

Darko Veljan

KOMBINATORNA I DISKRETNA MATEMATIKA

Ova je knjiga udžbenik kombinatorne i diskretne matematike, i premda je ponajprije namijenjena studentima matematičkih i računarskih znanosti, može poslužiti i studentima prirodnih, tehničkih, računarskih i drugih znanosti na dodiplomskom i poslijediplomskom studiju, a neki dijelovi knjige pogodni su i za rad sa srednjoškolcima.

Autor je veliku pažnju posvetio raznovrsnim primjerima i primjenama nastojeći s raznih aspekata dobro ilustrirati i opisati osnovne ideje, a budući da mnogi ljudi stvari doživljavaju vizualno, gdje god je to bilo uputno, nastojao je pored formalnog dokaza skicirati i njegovu vizualnu percepciju.

Osnovni cilj knjige, osim da čitatelja (naročito studente) poduči osnovnim idejama čitavog korpusa kombinatorne i diskretne matematike, je i taj, što je možda i najvažnije, da bude daljnji poticaj za samostalno precizno i rigorozno matematičko razmišljanje i zaključivanje.

Knjiga je prvenstveno namijenjena čitatelju koji katkad osjeti pravo intelektualno i estetsko zadovoljstvo u razumijevanju matematičkih pojmova i ideja i radost kad elegantno riješi neki teži problem.

ISBN 953-6450-74-7

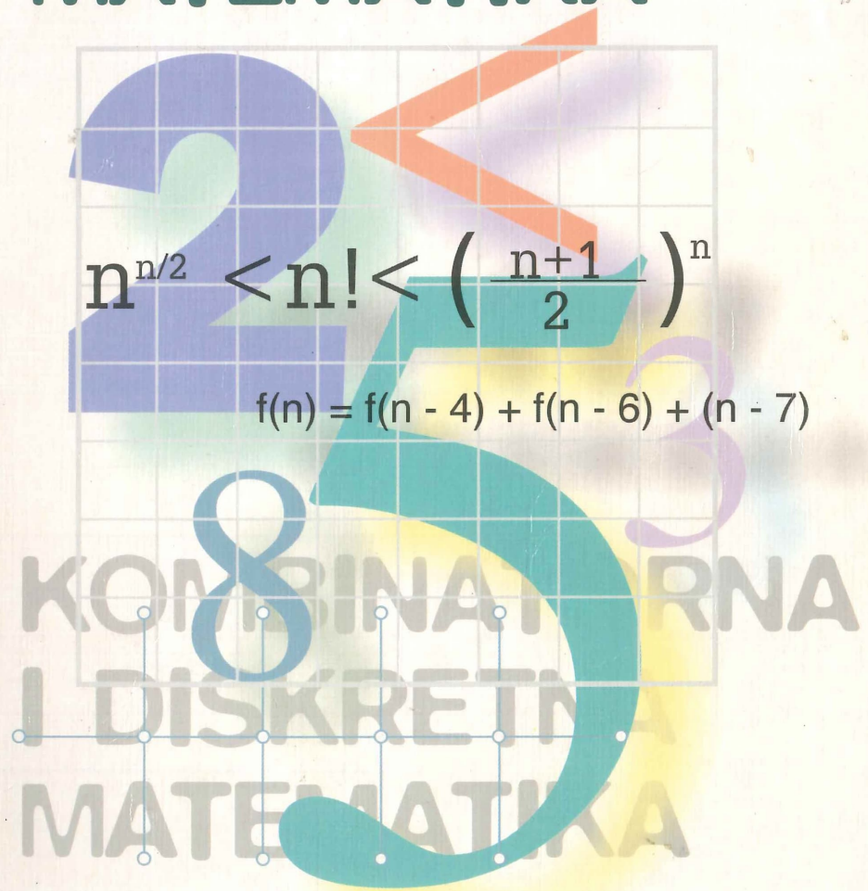
ISBN 953-6450-74-7

Darko Veljan

KOMBINATORNA I DISKRETNA MATEMATIKA

Darko Veljan

KOMBINATORNA I DISKRETNA MATEMATIKA



KOMBINATORNA I DISKRETNA MATEMATIKA

ALGORITAM

UDŽBENICI SVEUČILIŠTA U ZAGREBU
MANUALIA UNIVERSITATIS STUDIORUM ZAGRABIENSIS

INV. BR. 1864



Nakladnik: ALGORITAM d.o.o.
Zagreb, Gajeva 12

Za nakladnika: Mladen Kokolj

Urednik: Neven Antičević

Recenzija: Marko Petkovšek, Tomaž Pisanski,
Dragutin Svrtan, Andrej Dujella

Grafička priprema: Marcel Maretić, Ante Mijić

Ilustracije: Marcel Maretić

Design i priprema naslovne stranice: Bakal, d.o.o.

Lektura: Rosanda Kokanović

Tisak: ZT Zagraf

naklada 2000 primjeraka

CIP - Katalogizacija u publikaciji
Nacionalna i sveučilišna knjižnica, Zagreb

UDK 519.1(075.8)

VELJAN, Darko
Kombinatorna i diskretna matematika /
Darko Veljan. – Zagreb : Algoritam, 2001. –
(Udžbenici Sveučilišta u Zagrebu = Manualia
Universitatis studiorum Zagrabiensis)

ISBN 953-6450-74-7

410119121

ISBN 953-6450-74-7

Darko Veljan

KOMBINATORNA I DISKRETNA MATEMATIKA

ALGORITAM

Zagreb 2001.
prvo izdanje

Sadržaj

Predgovor vii

I. Uvod i osnovni pojmovi 1
1. Čime se bavimo u ovoj knjizi: neki primjeri 1
2. Osnovni pojmovi 14
3. Algoritmi 24
4. Dirichletov princip 31

II. Kombinatorna prebrojavanja 44
1. Osnovna pravila prebrojavanja 44
2. Prebrojavanje funkcija, podskupova, injekcija i bijekcija 47
3. Permutacije skupova 52
4. Kombinacije skupova 61
5. Kombinacije i permutacije multiskupova 69
6. Binomni i multinomni koeficijenti 78
7. Particije brojeva i skupova i još neke kombinatorne veličine 97

III. Neki rekurzivni problemi 110
1. Fibonaccijevi brojevi 114
2. Linearne rekurzije s konstantnim koeficijentima 122
3. Neke linearne rekurzije, svođenje na njih i neki sustavi rekurzija . . 127
4. Catalanovi brojevi 133
5. Dvoindeksne rekurzije i invertiranje polinomskih nizova i rekurzija . 139

IV. Formula uključivanja-isključivanja i Möbiusova formula inverzije 142
1. Formula uključivanja-isključivanja 142
2. Parcijalno uređeni skupovi i Möbiusova inverzija 157

V. Funkcije izvodnice 177
1. Osnovna ideja i jednostavni primjeri 177
2. Račun s funkcijama izvodnicama i neke primjene 181
3. Rekurzije i funkcije izvodnice 187
4. Simbolička metoda 195

5. Lagrangeova formula inverzije 202
6. Poopćeni binomni i eksponencijalni redovi i hipergeometrijski redovi 206
7. Još neke funkcije izvodnice 215
8. Tri osnovne vrste funkcija izvodnica 219

VI. Uvod u teoriju grafova **235**
1. Osnovni pojmovi teorije grafova 235
2. Ciklusi i stabla 253
3. Obilasci grafova i digrafova 277
4. Povezanost grafova 289
5. Bojenje grafova i kromatski broj 295
6. Planarni grafovi 306
7. Sparivanje u grafovima 327
8. Ekstremalna teorija grafova 340
9. Vjerojatnostne metode 343
10. Protoci u transportnim mrežama 351

VII. Odabrane teme kombinatorne i diskretne matematike **359**
1. Blok dizajni i konačne projektivne ravnine 359
2. Matroidi 367
3. Pólya-Redifieldova teorija 372
4. Simetrične funkcije 382

Literatura **395**

Indeks **407**

Predgovor

Ova je knjiga udžbenik kombinatorne i diskretne matematike, a ponajprije je namijenjena studentima matematičkih i računarskih znanosti. Knjiga je nastala na temelju autorovih predavanja kolegija *Kombinatorika* studentima druge godine i kolegija *Diskretna matematika* studentima druge i(li) treće godine studija na Matematičkom odjelu PMF-a Sveučilišta u Zagrebu, te nekih izbornih kolegija na višim godinama. Knjiga je također nastala potpunom preradom rasprodanog izdanja knjige

D. Veljan, *Kombinatorika s teorijom grafova*, Školska knjiga, Zagreb, 1989. (*)

Knjiga može poslužiti i studentima prirodnih, tehničkih, računarskih i drugih znanosti na dodiplomskom i poslijediplomskom studiju, a neki dijelovi knjige su pogodni i za rad sa srednjoškolcima. Vjerujem da će knjiga korisno poslužiti i svima onima koji se iz razno-raznih razloga zanimaju za kombinatoriku, teoriju grafova i srodne discipline.

U odnosu na prvotno izdanje (*), ova je knjiga sadržajno prilično drukčija. Osim što je obogaćena novim spoznajama, i što je mjestimice promijenjen redoslijed izlaganja, u ovom sam izdanju nastojao ugraditi svoja iskustva u vezi s poteškoćama koje studenti iskazuju oko razumijevanja ključnih pojmova i činjenica. Zato sam se odlučio da neke od njih objasnim iz nekoliko različitih aspekata. Na primjer, neke važne činjenice su dokazane na dva ili čak tri načina. Najčešće su to induktivan, algebarski i "čisto" kombinatorni dokaz u vidu bijekcije. Budući da mnogi ljudi stvari doživljavaju vizualno, gdje god je to bilo uputno, nastojao sam pored formalnog dokaza skicirati i njegovu "vizualnu percepciju" u duhu uzrečice "dobra slika je vrjednija od tisuća riječi". Osim toga, veliku sam pažnju posvetio raznovrsnim primjerima i primjenama nastojeći s raznih aspekata dobro ilustrirati i opisati osnovne ideje, katkad samo na intuitivnoj i neformalnoj razini. Važnost primjera je golema, jer se njima dobiva dinamičnost vječne igre "apstraktno - konkretno". Kako se takvih primjera nagomilalo, a znajući da mnogi ljudi ne vole debele knjige, odlučio sam (nažalost) iz ove knjige izbaciti zadatke (osim iz Uvoda) i napisati posebnu zbirku zadataka s uputama i rješenjima.

Osnovni cilj knjige, osim da čitatelja (naročito studente) poduči osnovnim idejama čitavog korpusa kombinatorne i diskretne matematike, je i taj, što je možda i najvažnije, da bude daljnji poticaj za samostalno precizno i rigorozno matematičko razmišljanje i zaključivanje.

Od predznanja potrebnih za uspješno svladavanje ove knjige navedimo poznavanje elementarne matematike i (barem djelomično) poznavanje nekih dijelova linearne algebre i matematičke analize, te ponešto iz računarstva.

Idealno bi bilo da je čitatelj prethodno već (uglavnom) svladao gradivo standardnih udžbenika iz tih područja. Na Matematičkom odjelu PMF-a Sveučilišta u Zagrebu to su S. Kurepa *Matematička analiza I, II*, K. Horvatić *Linearna algebra I, II* i B. Pavković, D. Veljan *Elementarna matematika I, II*.

No, bez obzira na predznanja, ova je knjiga prvenstveno namijenjena čitatelju koji katkad osjeti pravo intelektualno i estetsko zadovoljstvo u razumijevanju matematičkih pojmova i ideja i radost kad elegantno riješi neki teži problem. Nisu svi ljudi ovog svijeta jednaki. Kao što netko nema naročitog sluha za glazbu, slikarstvo ili npr. za financije, tako će onima s manje "sluha" za matematiku ova knjiga (i uopće matematika) uglavnom biti dosadna. Nadam se, međutim, da će i kod takvih čitatelja uz malo upornosti i volje uspjeti probuditi njihovu možda i zatomljenu pozitivnu "vibru" za matematiku.

Glavni sadržaji knjige su osnovne tehnike prebrojavanja, odnosno tzv. **enumerativna matematika** i osnovni pojmovi i metode **teorije grafova**. Ostali sadržaji kao što su simetrične funkcije, konačni skupovi i hipergrafovi, konačne projektivne ravnine i blok dizajni, matroidi, ekstremalna teorija grafova i kombinatorna geometrija, vjerojatnosne metode i druge, samo su ukratko obrađeni i opisani s uputom na odgovarajuću literaturu za čitatelja kojeg te teme zanimaju. Ti sadržaji mogu poslužiti i za neke izborne kolegije.

Što se tiče literature, u ovoj sam knjizi zadržao bez preinake popis literature [1]-[236] iz prošlog izdanja (*) i tome dodao popis novije literature označene s [1*],[2*],...Na samom kraju knjige dan je indeks pojmova i naziva. Kad se prvi put pojavljuju u knjizi, pojmovi i nazivi su otisnuti **debelim pismom**.

Sadržaji poput logike, konačnih automata, NP-potpunosti, asocijativnih shema, kombinatorne optimizacije i drugi samo su mjestimice uključeni, iako se mnogi od njih detaljno obrađuju u nekim udžbenicima kombinatorne i diskretne matematike. Razloga za to je više, a osnovni je da bi ovakav obični udžbenik (a ne monografija) tada bio preopsežan i nepraktičan, pa zato i preskup.

Na kraju, želim zahvaliti svim onim osobama koje su mi u bilo kojem vidu pripomogli u pisanju ovog udžbenika. U prvom redu su tu recenzenti, profesori M. Petkovšek i T. Pisanski iz Ljubljane i profesori A. Dujella i D. Svrtan iz Zagreba koji su svojim primjedbama i sugestijama pridonijeli znatnom poboljšanju teksta. Čitavu su knjigu znalački u LaTeX-u prepisali M. Maretić i A. Mijić.

Svima koji su mi pomogli oko prošlog izdanja (*) i ovom prilikom zahvaljujem.

Za lijepu opremu i ostale uredničke poslove zaslužan je g. N. Antičević, urednik poduzeća "Algoritam" koje je izdalo ovu knjigu.

Zahvaljujem i Ministarstvu znanosti i tehnologije Republike Hrvatske za subvenciju i potporu pri izdavanju ove knjige, a čiji je rezultat znatno niža prodajna cijena knjige, čime je mnogima kupnja postala pristupačnija.

Unaprijed zahvaljujem i svima onima koji pronađu i obavijeste me o preostalim materijalnim i drugim greškama "preživjelim" i nakon višestrukih korektura ove knjige.

Darko Veljan

I. Uvod i osnovni pojmovi

§ 1. Čime se bavimo u ovoj knjizi: neki primjeri

Kombinatorna i diskretna matematika ili kraće kombinatorika je matematička disciplina koja uglavnom proučava konačne skupove i strukture. Od davnina su se matematičari bavili problematikom prebrojavanja elemenata konačnih skupova, koja je danas samo jedan od vidova kombinatorike: naime, enumerativna kombinatorika. Često se u praksi susrećemo s problemima prebrojavanja elemenata konačnog skupa koji je čitav pred nama; na primjer slova i simboli na ovoj stranici ili sve stranice ove knjige ili sva drveća u nekom drvoredu itd. U tim je slučajevima lako prebrojiti sve elemente tog skupa i doći do prirodnog broja n (ili nule) koji označava broj elemenata tog skupa.

Međutim, često elementi skupa čine neku pravilnu konfiguraciju ili su pak zadani opisno pomoću nekih svojstava. Ako nas npr. zanima samo broj elemenata takvih skupova, onda ne moramo efektivno brojiti elemente, već se možemo poslužiti nekim enumerativnim metodama. Ti skupovi i svojstva kojima su im elementi opisani mogu biti najraznovrsniji, od posve jednostavnih do vrlo suptilnih. Stoga se u kombinatorici istražuju različite specijalne metode koje daju odgovore na pitanja kao što su: koliko ima objekata s danim svojstvima ili na koliko se načina može dogoditi izvjestan događaj itd.

Vjerujemo da će se čitatelj složiti s tim da se svatko od nas kad-tad susreo s kombinatornim problemima, i s onim svakodnevnim (npr. na koliko se načina može ispuniti listić sportske prognoze ili kako autom doći najkraćim putem od jednog do drugog mjesta u gradu ako je dan sustav jednosmjernih ulica itd.) i s "pravim" zadacima i problemima. Navedimo nekoliko tipičnih jednostavnih kombinatornih zadataka:

1. Na koliko se različitih načina 6 ploha kocke može obojiti ako imamo 4 boje? (Pritom smatramo da su dva načina bojenja ista ako ih rotacijama možemo dovesti do poklapanja).
2. Može li se svaki od 9 telefona spojiti s točno 3 od preostalih?
3. Koliko najviše ima registarskih tablica automobila ako na svakoj od njih pišu dva slova, a iza njih je broj s najviše 6 znamenaka?
4. Na koliko različitih načina može četvero ljudi sjesti za okrugli stol?

5. Koliko ukupno utakmica odigraju momčadi nogometne lige u kojoj ima 18 klubova, a svaki klub odigra po dvije utakmice sa svakim od preostalih klubova?
6. Na koliko načina može petoro ljudi među sobom podijeliti 24 kune?
7. Na koliko najviše dijelova 8 pravaca u ravnini dijeli tu ravninu?
8. Koliko ima (cijelih) brojeva između 1 i 100 koji nisu djeljivi ni s 2 ni s 3?
9. Na koliko se različitih načina može na šahovsku ploču 8×8 postaviti 8 topova, odnosno kraljica koje se međusobno ne napadaju?

Čitatelju se može učiniti da su to samo zgodne zagonetke i da služe samo za razonodu. Jest da je s nekim kombinatornim problemima doista i tako. I povijesno gledano, kombinatorika je kao znanstvena disciplina nastajala malo-pomalo, a svoje korijene vuče iz zabavne matematike, zagonetaka, igara, a naročito iz početaka teorije vjerojatnosti u 17.st. (vidi N. L. Biggs, The roots of combinatorics, Historia Math. 6(1979), 109-136 i Ku Tung-Hsin, W. D. Wallis, The development of combinatorics, Math. Scientist 11 (1986), 33-43). Tako je kombinatorika dugo vremena "vegetirala" na granici između znanosti i razbibrige. Mnogi problemi koji su se "do jučer" razmatrali prije svega samo radi zabave i svoje estetske privlačnosti, danas se ubrajaju u važne probleme teorijske i primijenjene znanosti. Danas je kombinatorika (kombinatorna teorija ili kombinatorna analiza, kako se ponegdje zove) vrlo važna grana matematike i njezina važnost i utjecaj i na matematiku i na ostale znanosti neprestano raste. Nesumnjivo je tome pridonio i pronalazak te intenzivan razvoj kompjutera i računarstva i njihov cjelokupni utjecaj na razvoj znanstvene misli i ljudsko društvo u cjelini. Kompjuteri ne rade sami od sebe; njih treba programirati. No osnovu za te programe često čine kombinatorni algoritmi za rješavanje problema. Postoje još i drugi razlozi za nagli razvoj kombinatorike počevši od 1960-ih godina. Tako se npr. spoznalo da se kombinatorika može primijeniti i na discipline za koje se smatralo da nemaju baš neke ozbiljne veze s matematikom. Tu ne mislimo na fiziku, astronomiju, tehniku i statistiku (discipline u kojima se matematika primijenjuje tradicionalno); mislimo ovdje i na biologiju (posebno genetiku i molekularnu biologiju), kemiju, elektroniku, medicinu, lingvistiku, sociologiju, antropologiju, ekonomske znanosti te na neke društvene znanosti. Zanimanje za kombinatornu i diskretnu matematiku i dalje neprestano raste. To se može potkrijepiti i činjenicom da danas u svijetu postoji barem 30-ak znanstvenih časopisa isključivo posvećenih kombinatornoj i diskretnoj matematici (npr. "Journal of Combinatorial Theory A,B", "Discrete Mathematics", "European Journal of Combinatorics", "Journal of Graph Theory", "Algorithmica" itd.)

Riječ **kombinatorika** dolazi od riječi kombinacija, a ova od lat. riječi combinare = slagati. Ljudi sa srednjim matematičkim obrazovanjem obično pod rječju "kombinatorika" razumijevaju "permutacije, kombinacije i varijacije". Pod permutacijom (od lat. permutare = promijeniti), obično razumijevaju neke vrste premještanja, odnosno promjena slijeda određenog broja stvari, pod kombinacijom svaku moguću skupinu određenog broja neke množine elemenata, a pod varijacijom (od lat. variatio=različitost) promjenu, mijenjanje, preinaku. No to je samo djelomično točno.

Riječ **diskretan** (od lat. discrenere = razlučiti, razlikovati) u ovom kontekstu znači da objekte koje proučavamo možemo jasno i nedvojbeno razlikovati po nekom redoslijedu (kao npr. elemente skupova $\{1, 2, \ldots, n\}$, $\mathbb{N}$ i $\mathbb{Z}$).

Kombinatorika se pretežno bavi razmještanjima objekata zadanog konačnog skupa u izvjesne konfiguracije (sheme). Najčešće tu imamo dva tipa problema:

1) *Egzistencija razmještaja.* Želimo li razmjestiti objekte nekog skupa na način propisan nekim uvjetima, prvo što se pitamo jest postoji li uopće takav razmještaj. Ako razmještaj nije uvijek moguć, pitamo se dalje, koji su nužni i dovoljni uvjeti za postojanje razmještaja danog tipa.

2) *Prebrojavanje i klasifikacija razmještaja.* Ako je određeni razmještaj moguć, pitanje je na koliko se načina on može postići ili kako te razmještaje klasificirati u određene tipove.

   Stoga upravo i najčešća pitanja u kombinatorici počinju ovako: "Je li moguće razmjestiti ...?" ili "Na koliko (najviše, najmanje ili točno) načina ...?" itd.

   Treći tip kombinatornih problema koji se pojavljuju, a u vezi su s problemima tipa 1), jest:

3) *Proučavanje poznatih razmještaja.* Nakon što je dokazana egzistencija i izvedena konstrukcija razmještaja koji zadovoljava određene uvjete, može se pristupiti proučavanju njegovih zakonitosti i strukture. Proučavanje tih struktura može imati primjene u problemima klasifikacije 2) i drugdje.

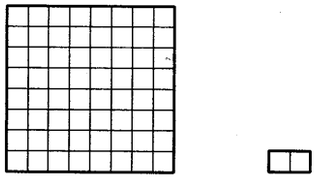
Sažeto, možemo reći da *kombinatorika proučava diskretne strukture i relacije.*

U rješavanju kombinatornih problema često se mora iznaći neka ad hoc metoda ili dosjetka za rješavanje, pa onda rezultat koji smo dobili (a koji ovisi o prirodnom broju n) valja provjeriti matematičkom indukcijom ili na neki drugi način. To ni u kom slučaju ne znači da u kombinatorici nema nekih općih načela i metoda kojima se možemo služiti u rješavanju kombinatornih problema. Bijektivna korespondencija, formula uključivanja - isključivanja, funkcije izvodnice, rekurzije, obilasci i bojenja grafova itd., samo su neke metode koje ćemo poslije sustavno upoznati.

Ono što ipak želimo istaći jest to da je prilikom rješavanja "elementarnih" kombinatornih problema potrebna izvjesna dovitljivost, oštroumnost i dosjetljivost.

Da bismo ilustrirali dosad rečeno, navest ćemo malo složenije kombinatorne probleme i primjere, načine njihovih rješavanja ili ćemo samo komentirati rješenja.

Primjer 1 (popločavanje šahovske ploče). Šahovsku ploču 8×8 kvadratića treba "popločati" pločicama tipa "domino", tj. pravokutnicima od kojih se svaki sastoji od 2 kvadratića sastavljenih duž zajedničke stranice (v. sl.).



Pitanje je je li moguće takvo popločenje s 32 domina, tako da se domina ne preklapaju?

Ovo je lagani problem razmještanja i svatko može odmah konstruirati nekoliko različitih popločavanja. Mnogo je teži problem izračunati broj različitih popločavanja. Taj je broj nađen tek 1961. god. i iznosi 12 988 816 ($= 2^4 901^2$). Ako umjesto šahovske ploče 8×8 razmatramo ploču $m \times n$, onda takvo popločenje s dominima ne mora uvijek postojati. Tako se npr. 3×3 ploča ne može popločiti dominima. Lako se vidi da se ploča $m \times n$ može popločiti s dominima na gornji način ako i samo ako je bar jedan od brojeva m ili n paran. Problem nalaženja broja različitih popločenja u tom slučaju je ekvivalentan **problemu dimera**, a nastao je u vezi s proučavanjem apsorpcije dvoatomnih molekula (dimera) u molekularnoj fizici.

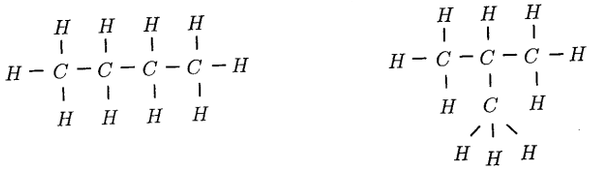
Zamislimo sada da smo od šahovske ploče 8×8 "otpilili" (odstranili) dva dijametralno suprotna kvadratića. Je li sada moguće popločiti ovu krnju šahovsku ploču? Pokazat ćemo da je to nemoguće. Dokaz je jednostavan i tipičan je primjer jedne ad hoc, ali lukave dosjetke u kombinatorici. Obična šahovska ploča 8×8 ima 64 kvadratića tako da boje tih kvadratića ("polja") alterniraju kad se ide od kvadratića do kvadratića preko zajedničkih stranica: bijeli - crni - bijeli - crni itd.: 32 bijela i 32 crna polja.

Međutim, kad odstranimo dva dijagonalno suprotna polja, odstranili smo dva polja iste boje, npr. bijela, pa preostaje 30 bijelih i 32 crna polja. No svaki domino pokriva jedno bijelo i jedno crno polje, pa 31 domino pokriva 31 crno i 31 bijelo polje, te nikako ne može pokriti 30 bijelih i 32 crna polja. Tu se odmah nameće pitanje o generalizaciji. Neka je dana $m \times n$ šahovska ploča čija su polja naizmjence bijela i crna. Odstranimo proizvoljno nekoliko polja. Preostaje "krnja" ploča. Uz koje uvjete se "krnja" ploča može popločiti dominima? Odmah vidimo, kao gore, da je nužan uvjet za to da krnja ploča ima jednak broj bijelih i crnih polja. Međutim, to nije i dovoljan uvjet jer postoje jednostavni protuprimjeri (nađite ih sami). Nužan i dovoljan uvjet za mogućnost popločenja krnje šahovske ploče dominima proizlazi iz teorije sistema različitih predstavnika. Tamo ćemo vidjeti još neke ekvivalentne formulacije tog problema.

Primjer 2 (broj vlasi na glavi). Poznato je da čovjek ima najviše 300 000 vlasi na glavi. U Hrvatskoj ima 4 700 000 stanovnika. Postoje li u Hrvatskoj postoje ljudi s "na dlaku" istim brojem vlasi na glavi? Možemo li sigurno tvrditi da postoji stanovit (maksimalan) broj ljudi u Hrvatskoj s "na dlaku" istim brojem vlasi na glavi? Koliki je to broj?

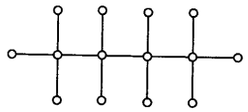
Ovo je tipičan primjer u kojem rabimo Dirichletov princip ili "princip kutija". Taj vrlo jednostavan i djelotvoran kombinatorni princip daje odmah i odgovore na gornja pitanja. Na posljednje pitanje odgovor je 16, jer kad bi bilo samo 15 ljudi s jednakim brojem vlasi, bilo bi u Hrvatskoj najviše $300\,001 \cdot 15 = 4\,500\,015$ stanovnika.

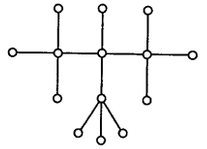
Primjer 3 (broj izomera). Taj je problem proučavao engleski matematičar Arthur Cayley (1821-1895), a riječ je o određivanju broja različitih izomera zasićenih ugljikovodika C_nH_{2n+2} za sve prirodne brojeve n. Na primjer C_4H_{10} može biti butan ili izobutan, čije strukturne formule izgledaju kao na idućoj slici:



Taj se problem grafički svodi na to da se pojedini atomi predstave točkama (vrhovima), a veze između njih dužinama (bridovima); time se dobiva **graf**. U tom grafu svaka dužina povezuje dvije točke, a svaka točka je sjecište ili jedne dužine ili četiriju dužina, a budući

da nema zatvorenih ciklusa sastavljenih od tih točaka i dužina, takav graf se još zove i **drvo** ili **stablo**:





Taj primjer ilustrira jednu često rabljenu metodu prebrojavanja, tzv. pravilo bijekcije. Naime, tom metodom zamjenjuje se jedan problem prebrojavanja drugim, lakšim, s tim da traženih objekata u prvom problemu ima točno koliko i u drugom, tj. postoji bijekcija među objektima prvog tipa s objektima drugog tipa. U spomenutom primjeru, postoji toliko izomera od C_nH_{2n+2} koliko i stabala u čijih se n vrhova sastaju četiri dužine, a preostalih $2n+2$ vrhova su krajevi jedne dužine. Broj takvih stabala nije sasvim lako naći, ali je to samo prvi korak u nalaženju traženog broja izomera. Za potpuno rješenje tog problema treba se upoznati s nekim metodama prebrojavanja koje je razvio oko 1937. g. američki matematičar mađarskog podrijetla Georg Pólya (1887 – 1985) . Teorija grafova bit će jedna od glavnih tema u knjizi. Odgovor na problem izomera za $n = 8$ je 18, za $n = 12$ odgovor je 355, a za $n = 40$ odgovor je približno $6,25 \cdot 10^{13}$.

Primjer 4 (izbori). Na izbornoj listi nekog društva predloženo je 12 ljudi od kojih treba izabrati predsjednika, potpredsjednika, tajnika i blagajnika. Ista osoba može obavljati i više od jedne dužnosti. Na koliko (različitih) načina se može provesti taj izbor?

Pridružimo svakoj od osoba na izbornoj listi, brojeve od 1 do 12 redom. Svakom izboru predsjednika, potpredsjednika, tajnika i blagajnika odgovara uređeni slog od četiriju brojeva od 1 do 12, s tim da se ti brojevi mogu i ponavljati, npr. $6, 10, 11, 10$. Dakle, na prvom mjestu može se pojaviti jedan od brojeva od 1 do 12, isto tako na drugom mjestu (neovisno o ostalim mjestima), pa isto tako na trećem i četvrtom mjestu. Stoga je traženi broj jednak broju svih uređenih četvorki brojeva od kojih je svaki između 1 i 12; te su četvorke $1, 1, 1, 1$; $1, 1, 1, 2$; $1, 1, 1, 3$; ...; $12, 12, 12, 11$; $12, 12, 12, 12$. Očito je da tih četvorki ima $12 \cdot 12 \cdot 12 \cdot 12 = 20\,736$. To je tipičan srednjoškolski zadatak iz kombinatorike.

Primjer 5 (marke na paketu). Za neku je paketnu pošiljku potrebno zalijepiti marke u vrijednosti od $n = 25$ kuna. No, jedine marke koje su nam na raspolaganju su marke s vrijednostima od $4, 6, 7$ kuna. Na koliko se različitih načina u nizu se mogu marke nalijepiti na paket, ako različite poretke (serije) maraka smatramo različitim načinima lijepljenja maraka?

Za $n \in \mathbb{N}_0$ označimo s $f(n)$ broj (različitih) načina lijepljenja maraka od $4, 6, 7$ kn, tako da im ukupna vrijednost, tj. zbroj iznosi n kn. Tvrdimo da vrijedi

$$f(n) = f(n-4) + f(n-6) + f(n-7) \qquad (*)$$

Zaista, zamislimo da smo već na neki način zalijepili marke čija je suma n i neka je posljednja marka vrijednosti 7 kn. Tada sve ostale marke stoje ukupno $n-7$ kn. I obratno, ako na bilo koju kombinaciju maraka čija je ukupna vrijednost $n-7$ kn dolijepimo još na kraju marku od 7 kn, dobivamo seriju čija je vrijednost n kn. Pritom različitim serijama čija je vrijednost $n-7$ kn odgovaraju dolijepljivanjem marke od 7 kn različite serije čija je suma n kn (pravilo bijekcije). Prema tome, broj različitih serija maraka kod kojih je posljednja u nizu maraka od 7 kn, a ukupna vrijednost n kn jest $f(n-7)$. Na isti se način dokaže da je broj različitih serija čija je ukupna vrijednost n kn, i koje završavaju markom od 6 kn $f(n-6)$, a broj onih koje završavaju markom od 4 kn $f(n-4)$. Odavde je jasno

(tzv. pravilo sume) da vrijedi (∗). Relacija (∗) omogućuje da se iz poznavanja broja serija maraka čija je ukupna vrijednost manja od n nađemo broj serija čija je ukupna vrijednost n. Relacija tipa (∗) zove se **rekurzivna relacija** ili kraće **rekurzija**. Problemima tog tipa posvećeno je 3. poglavlje, no spomenuti problem za $n = 25$ ovdje možemo potpuno riješiti, jer za male vrijednosti od n, $f(n)$ možemo odrediti izravnim računanjem. Imamo: $f(0) = 1$, $f(1) = f(2) = f(3) = 0$, $f(4) = 1$, $f(5) = 0$, $f(6) = 1$, $f(7) = 1$, $f(8) = 1$, $f(9) = 0$. $f(0) = 1$, znači da iznos 0 kn možemo uplatiti na jedan jedini način, naime da ne lijepimo ni jednu marku. Sume 1, 2, 3, 5, 9 ne možemo očito uopće isplatiti s markama od 4, 6 i 7 kn. Sada, s vrijednostima od $f(n)$ za $n = 0, 1, 2, 3, 4, 5, 6, 7, 8, 9$, izračunajmo $f(10)$. Iz (∗) izlazi

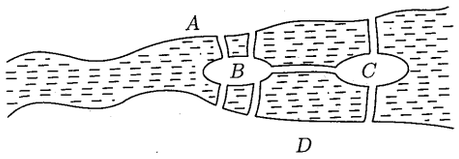
$$f(10) = f(6) + f(4) + f(3) = 1 + 1 + 0 = 2.$$

Dalje dobivamo $f(11) = f(7) + f(5) + f(4) = 2$, $f(12) = f(8) + f(6) + f(5) = 1 + 1 + 0 = 2$, pa dalje slično, $f(13) = 2$, $f(14) = 4$, itd. $f(25) = 28$.

Dakle, traženi broj različitih načina lijepljenja maraka od 4, 6 i 7 kn, čija je ukupna vrijednost 25 kn, iznosi 28. Npr. neki od tih načina su $7, 7, 7, 4$; $7, 4, 7, 7$; $6, 4, 7, 4, 4$ itd. (Ispišite sve te načine.)

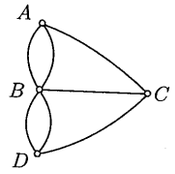
Primjer 6 (königsberški mostovi). Stari pruski grad Königsberg (sadašnji) Kalinjingrad u Rusiji (ili Królovec, Królowiec) smješten je na obalama rijeke Pregel. Dio grada smješten je na dva otoka, koji su bili povezani s kopnom i međusobno sa sedam mostova, kako je prikazano na idućoj slici.

Građani Königsberga voljeli su nedjeljne šetnje ili, kako su običavali reći "Spaziergangen" po gradu preko mostova. Neke je građane navodno ljutilo to što nisu mogli iznaći način kako da prošetaju gradom tako da prijeđu svaki most samo jedanput i vrate se kući, pa su na problem "Spaziergangena" upozorili čuvenog švicarskog matematičara Leonharda Eulera (1707 – 1783), koji je dugo djelovao u Petrogradu. Euler je taj problem dosta brzo i riješio 1736. god., pokazavši da je takva šetnja gradom nemoguća. Tim rješenjem on je i postavio temelje **teoriji grafova**, jednoj od najvažnijih grana kombinatorne i diskretne matematike.



Evo kako se možemo uvjeriti u nemogućnost "Spazierganga" koji su htjeli stanovnici Königsberga. Pretpostavimo da je takva šetnja moguća. Tada ona završava na kopnu, eventualno i na istoj komponenti kopna (A, B, C ili D) na kojoj je i započela. Prvo primijetimo da svaka komponenta kopna koja nije početak ni kraj šetnje mora biti povezana s drugim komponentama kopna s ukupno parnim brojem mostova. To je zato što svakom mostu kojim prilikom šetnje uđemo na tu komponentu, mora odgovarati točno jedan most kojim ćemo napustiti tu komponentu prilikom šetnje. Dakle, svakom "ulazećem" mostu mora odgovarati jedan "izlazeći" most. Stoga, svaka komponenta ima jednak broj ulazećih i izlazećih mostova, pa je ukupan broj mostova (ulazećih i izlazećih) paran broj. Zato svaka komponenta koja je povezana s drugim komponentama neparnim brojem mostova mora biti ili početak ili kraj šetnje. No u slučaju Königsberga svaka komponenta A, B, C ili D ima neparan broj mostova koji vode iz nje (ili u nju), a kako najviše dvije komponente mogu biti početak, odnosno kraj, šetnje, zaključujemo da je takva šetnja nemoguća.

Ako te komponente A, B, C, D "stisnemo" u točke ili vrhove, pa te točke spoji bridovima, linijama ili spojnicama (koje predstavljaju mostove), dobivamo pojednos vljenu shemu vrhova i njihovih spojnica u ravnini, tj. graf.



Problem mostova Königsberga ekvivalentan je problemu da se ovaj graf obiđe čit tako da krenemo iz jednog vrha i svaki brid prijeđemo točno jedanput.

Primjer 7 (magični kvadrati). To je jedan od najpopularnijih i najstarijih problem rekreativne matematike i zabave. **Magični kvadrat** reda n je kvadratna tablica (matrica) tipa $n \times n$ u koju su upisani brojevi $1, 2, \ldots, n^2$, tako da su sume brojeva u svi recima, stupcima i dvjema dijagonalama međusobno jednake. Ta se zajednička vrijednos s_n zove **magična suma** magičnog kvadrata reda n. Za $n = 3, 4, 5$ primjeri magični kvadrata su na idućoj slici.

2	7	6
9	5	1
4	3	8

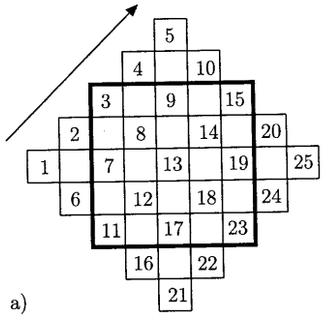
16	3	2	13
5	10	11	8
9	6	7	12
4	15	14	1

3	16	9	22	15
20	8	21	14	2
7	25	13	1	19
24	12	5	18	6
11	4	17	10	23

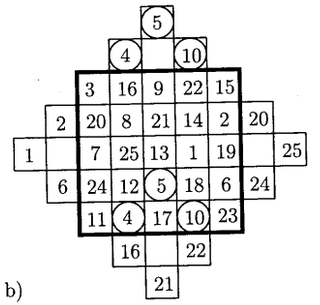
Magične sume su tu redom: $15, 34, 65$. U srednjem se vijeku vjerovalo u mističnu moć magičnih kvadrata i oni su nošeni u nekim ritualima kao zaštita od đavla.

Očito je da je suma svih brojeva u magičnom kvadratu reda n jednaka $1+2+\ldots+n^2 = n^2(n^2+1)/2$. Kako magični kvadrat reda n ima n redaka, a suma u svakom redu je s_n, proizlazi da je $n \cdot s_n = n^2(n^2+1)/2$. Stoga svi magični kvadrati reda n imaju istu magičnu sumu i ona je jednaka $s_n = n(n^2+1)/2$.

S time je u vezi sljedeći kombinatorni problem: odrediti za koje n postoji magični kvadrat reda n te naći opću metodu (**algoritam**) njihove konstrukcije. Odmah se vidi da ne postoji magični kvadrat reda 2 (magična bi suma trebala biti 5). No magični kvadrati reda n mogu se konstruirati za sve ostale vrijednosti od n. Objasnit ćemo ovdje kako se konstruiraju magični kvadrati neparnog reda. Provest ćemo konstrukciju za $n = 5$, a sasvim analogno se radi za ostale neparne brojeve (najbolje je za to uzeti papir s kvadratićima). Nad svakom stranicom kvadrata 5×5 konstruiramo "piramidu" kao na idućoj sl. a). Sada, počinjući od lijeve paralele dijagonalno prema gore upisujemo redom brojeve $1, 2, 3, 4, 5$ nastavljamo u sljedeću paralelu $(6, 7, 8, 9, 10)$, pa u sljedeću $(11, 12, 13, 14, 15)$ itd., dok ne iscrpimo sve brojeve $1, 2, \ldots, 25$. Sada se prazna mjesta u kvadratu popune jednostavno tako da se "piramide" translatiraju za 5 jedinica gore, dolje, lijevo, odnosno desno, tako da upadnu u kvadrat: sl. b). Kako se konstruiraju magični kvadrati parnih redova većih od 2, čitatelj može naći u knjizi [183] ili [53].



a)



b)

Primjer 8 (problem 36 časnika i latinski kvadrati). Iz svake od 6 vojnih jedinica poslano je na smotru 6 časnika i to po jedan svakog od 6 činova: poručnik, natporučnik, satnik, bojnik, pukovnik i general. Može li se tih 36 časnika svrstati u formaciju 6×6 tako da u svakom retku i svakom stupcu bude po jedan časnik svakog čina i po jedan časnik iz svake jedinice? Taj problem potječe iz 1772. g. od L. Eulera. Premda na prvi pogled spada u zabavnu matematiku, ovaj problem ima važne reperkusije u konačnim geometrijama, statistici, kombinatornim dizajnima i drugdje. Svakom časniku možemo pridružiti uređen par brojeva (i, j), gdje su $i, j \in \{1, 2, 3, 4, 5, 6\}$, pri čemu prva komponenta i kaže kojeg je čina taj časnik, a druga komponenta j iz koje je jedinice. Stoga je taj problem ekvivalentan problemu da se 36 uređenih parova $(i, j)(i = 1, 2, \ldots, 6; j = 1, 2, \ldots, 6)$ svrsta u kvadratnu tablicu ili matricu 6×6, tako da se u svakom retku i svakom stupcu pojave svi brojevi od 1 do 6 u prvim komponentama i isto tako svi brojevi od 1 do 6 u drugim komponentama. Takva se matrica može razbiti u dvije 6×6 matrice: jednu koja je sastavljena iz prvih komponenti matrice po činovima i drugu koja je sastavljena iz drugih komponenti (matrica po jedinicama). Sparivanjem tih dviju matrica (član po član), trebalo bi dobiti gornju matricu parova. Točnije, ako je na mjestu (k, l) (k-ti redak, l-ti stupac) prve matrice broj i, a na mjestu (k, l) druge matrice broj j, tada je na (k, l)-tom mjestu rezultantne matrice sparivanja uređen par (i, j) za $i, j, k, l \in \{1, 2, 3, 4, 5, 6\}$. Da budemo sasvim konkretni, pretpostavimo da je u pitanju 9 časnika triju činova i iz 3 različite jedinice. Tada je rješenje ovog "problema 9 časnika":

$$\underbrace{\begin{bmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \\ 2 & 3 & 1 \end{bmatrix}}_{\text{matrica po činovima}} \quad \underbrace{\begin{bmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \\ 3 & 1 & 2 \end{bmatrix}}_{\text{matrica po jedinicama}} \quad \rightarrow \quad \underbrace{\begin{bmatrix} (1,1) & (2,2) & (3,3) \\ (3,2) & (1,3) & (2,1) \\ (2,3) & (3,1) & (1,2) \end{bmatrix}}_{\text{matrica sparivanja}} \qquad (*)$$

Matrica po činovima i matrica po jedinicama primjeri su takozvanih **latinskih kvadrata** reda 3. Primjeri latinskih kvadrata reda 2 i 4 redom su

$$\begin{bmatrix} 1 & 2 \\ 2 & 1 \end{bmatrix}, \quad \begin{bmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \\ 3 & 4 & 1 & 2 \\ 2 & 3 & 4 & 1 \end{bmatrix}.$$

Latinski kvadrati reda 3 u $(*)$ zovu se **ortogonalni**, jer u matrici sparivanja dobivamo svih 9 mogućih uređenih parova $(i, j), i, j = 1, 2, 3$. Stoga se Eulerov problem 36 časnika može preformulirati ovako: Postoje li dva ortogonalna latinska kvadrata reda 6? Već je sam Euler razmatrao opći problem egzistencije dvaju ortogonalnih latinskih kvadrata reda

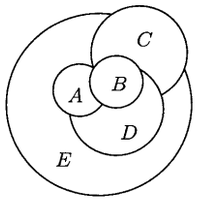
n. Lako se vidi da ne postoji par ortogonalnih latinskih kvadrata reda 2, jer osim gornjeg, još preostali latinski kvadrat reda 2 je

$$\begin{bmatrix} 2 & 1 \\ 1 & 2 \end{bmatrix},$$

a ta dva nisu ortogonalna. Euler je našao konstrukciju parova latinskih kvadrata reda n za sve neparne n kao i za n oblika $4k$. Nakon mnogih pokušaja, Euler je naslutio da ne postoji par ortogonalnih latinskih kvadrata reda 6, kao i da ne postoje parovi ortogonalnih latinskih kvadrata reda $n = 4k + 2$, $k \in \mathbb{N}$, tj. za $n = 6, 10, 14, 18, \ldots$. Za $n = 6$ Eulerova slutnja se pokazala točnom. Prvi dokaz za to je dao G. Tarry 1901. No tek 1960. Eulerova slutnja za $n > 6$ je oborena u radu triju matematičara-statističara: R. C. Bosea, E. T. Parkera, S. S. Shrikhandea (v. Canadian Journal Math., 12 (1960),189-203).

Oni su pokazali da za svako n oblika $n = 4k + 2$, $k = 2, 3, 4, \ldots$ postoje parovi ortogonalnih latinskih kvadrata reda n te su dali algoritam za njihovu konstrukciju. Oni upozoravaju na njihovu vezu s **konačnim aritmetikama**, kao i na njihovu primjenu u **kombinatornim dizajnima**. Razne rezultate, činjenice i primjere latinskih kvadrata čitatelj može naći u [64], a i mi ćemo se u ovoj knjizi povremeno osvrtati na njih. (VII, §1.)

Primjer 9 (problem četiriju boja). Zamislimo u ravnini ili na sferi zemljopisnu kartu na kojoj su ucrtane države (svaka se država sastoji od samo jedne regije na karti, a ne od više nepovezanih područja). Da bismo brzo razlikovali države, želimo ih obojiti tako da države sa zajedničkim granicama obojimo različitim bojama. Na primjer, na donjoj smo slici označili različitim slovima različite boje.



Problem četiri boje sastoji se u tome da se nađe najmanji broj boja koji će jamčiti da se svaka takva "zemljopisna karta" može obojiti na tako zadan način. Sve do 1976. to je bio jedan od najslavnijih neriješenih problema u matematici. Uz poznate klasične probleme kvadrature kruga i trisekcije kuta, taj su problem vrlo često "rješavali" laici-nematematičari. Razloge tome treba vjerojatno tražiti u činjenici da se problem može vrlo jednostavno formulirati, pa je samim tim pobudio pažnju među mnogim laicima i matematičarima-amaterima. Taj je problem postavio još kao postdiplomski student Francis Guthrie oko 1850. god., a pokušali su ga riješiti već u ono doba poznati matematičari kao A. Cayley, W. R. Hamilton, poslije A. B. Kempe, P. J. Heawood i drugi, razvivši tim pokušajima nove i važne metode u teoriji grafova. Odmah se uočilo da neke "zemljopisne karte" zahtijevaju 4 boje, na primjer ona na donjoj slici. Oko 1890. Heawood je dokazao da je svaku kartu moguće obojiti s 5 boja. I tako, više od 120 godina problem četiriju boja ostao je neriješen, sve dok nije ljeto 1976. došla vijest s University of Illinois da su K. Appel i W. Haken uspjeli dokazati da je svaku kartu u ravnini moguće obojiti četirima bojama. U svom dokazu oni su se intenzivno koristili kompjuterom, i to tako da su problem sveli na to da se ispita 1955 tipova grafova (tj. karata) i mogućnost njihova bojenja s 4 boje. Nakon golemog posla svođenja problema na te tipove i konstrukcije jednog vrlo ekonomičnog programa, tadašnjem kompjuteru je za to trebalo gotovo dva mjeseca neprekidnog i efektivnog

4. Nađite broj različitih popločavanja dominima "šahovske ploče" 3×4.

5. Zamislimo da se neki zatvor sastoji od 64 ćelije čiji tlocrt izgleda kao šahovska ploča 8×8. Između svakih dviju susjednih ćelija postoje vrata. Zatvoreniku u donjoj lijevoj ćeliji je rečeno da za sebe može izboriti slobodu ako uspije doći do desne gornje ćelije, tako da svaku od 64 ćelije obiđe samo jedanput. Može li taj zatvorenik za sebe izboriti slobodu?

6. Topovi (ili kule) u šahu napadaju se ako su u istom retku ili stupcu na šahovskoj ploči. Dokažite da se 8 topova može postaviti na šahovsku ploču a da se ne napadaju.

7. Lovci (ili lauferi) u šahu napadaju se ako se nalaze na istoj dijagonali. Dokažite da se na običnu šahovsku ploču može postaviti najviše 14 lovaca koji se međusobno ne napadaju. Dokažite da je analogan broj za ploču $n \times n$ jednak $2n - 2$.

8. Dokažite da se na šahovsku ploču može postaviti 8 dama, 8 topova, 14 lovaca i 21 skakač tako da se istovrsne figure međusobno ne napadaju.

9. Šahovska ploča 6×6 popločena je s 18 domina. Dokažite da postoji vodoravni ili okomiti pravac koji ne siječe ni jednu dominu, a dijeli šahovsku ploču na dvije neprazne manje ploče.

10. Koliko ima različitih izomera oktana C_8H_{18}?

11. U nekom društvu n se ljudi rukovalo s neparnim brojem ostalih. Dokažite da je n paran. (To je tzv. **"lema o rukovanju"**; s time ćemo se još puno puta sresti.)

12. Neka je n potpuni kvadrat. Tada n ima neparan broj djelitelja (uključujući 1 i n). Ako n nije potpun kvadrat, onda ima paran broj djelitelja.

13. Pariz je smješten na obalama Seine u kojoj su dva otočića A i B koji su spojeni jednim mostom. S jednom obalom Seine A je spojen s 4 i B s 3 mosta, dok je s drugom obalom A spojen s 5, a B s 2 mosta. Nađite Eulerovu šetnju na pripadnom grafu, tj. šetnju koja počinje u nekom vrhu i po bridovima obiđe čitavu figuru tako da svaki brid obiđe točno jedanput. Dokažite da na tom grafu Eulerova šetnja ne može početi i završiti u istoj točki, tj. da ne postoji zatvorena Eulerova staza na tom grafu.

14. Konstruirajte magične kvadrate reda a) 7, b) 9, c) 6.

15. Dokažite da magični kvadrat reda 3 mora imati na srednjoj poziciji broj 5. Dokažite odavde da postoji točno 8 različitih magičnih kvadrata reda 3.

16. Dokažite da ako u magičnom kvadratu reda n svaki broj a zamijenimo brojem n^2+1-a, dobivamo opet magični kvadrat reda n.

17. Konstruirajte latinske kvadrate reda a) 5, b) 6.

18. Nađite opću metodu konstrukcije latinskih kvadrata reda n.

19. Konstruirajte par ortogonalnih latinskih kvadrata reda 4.

20. Neka je $n \in \mathbb{N}$ i $A = (a_{ij})$, $B = (b_{ij})$ par ortogonalnih latinskih kvadrata reda n. Stavimo za svako $i, j \in \{1, 2, \ldots, n\}$ $m_{ij} = n(a_{ij} - 1) + b_{ij}$. Dokažite da je $M = (m_{ij})$ magični kvadrat reda n.

21. Jedan od 6 studenata A, B, C, D, E, F ukrao je knjigu iz knjižnice. Svatko od njih je pitan koga je od preostalih studenata vidio u knjižnici i svi su rekli istinu osim lopova. (Moguće je da je neki od studenata vidio nekog drugog, ali da sam nije primijećen od tog studenta, ali mi pretpostavljamo da ako su se dvojica našla u knjižnici u isto vrijeme, onda je jedan drugog vidio). A je rekao da je vidio B i E, B da je vidio A i F, C da je vidio D i F, D da je vidio A i F, E da je vidio A i D, F da je vidio C i B. Tko je lopov?

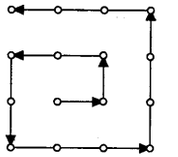
22. U društvu od četvero ljudi svaka dvojica imaju točno jednog zajedničkog prijatelja. Dokažite da u tom društvu postoji osoba koja je prijatelj svim ostalim članovima tog društva. Ovo je posebni slučaj tzv. **"Teorema o prijateljstvu"**, koji kaže da ako u nekom konačnom društvu svaka dva člana imaju točno jednog zajedničkog prijatelja, onda je netko iz tog društva prijatelj svih članova društva. (Za dokaz tog teorema vidi pogl. VI. §1.)

23. Od 100 članova nekog kolektiva može se formirati ukupno $2^{100} - 1$ delegacija (to ćemo poslije dokazati). Koliko se najviše delegacija može formirati istodobno od tog kolektiva pod uvjetom da svake dvije delegacije imaju bar jednog zajedničkog člana?

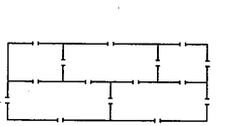
24. Svaki je član nekog kolektiva u točno dvije delegacije, a svake dvije delegacije imaju točno jednog zajedničkog člana. Ukupno, taj kolektiv ima 5 delegacija. Koliko članova ima taj kolektiv?

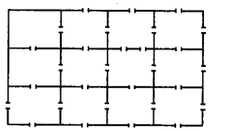
25. Savjet direktora jedne kompanije sastoji se od 15 ljudi, koji moraju ući u 20 komisija. Pri tome treba vrijediti: a) svaki direktor je član četiriju komisija, b) svaka se komisija sastoji od 3 direktora, c) svake dvije komisije imaju najviše jednog zajedničkog člana. Je li to moguće?

26. U ravnini je zadana kvadratna mreža od 3×3 točaka. Dokažite da postoji (povezana) izlomljena linija koja prolazi kroz svih $3 \cdot 3$ vrhova te mreže, a sastoji se od $2 \cdot 3 - 2 = 4$ dužine. Je li moguće općenito povući (povezanu) izlomljenu liniju koja prolazi kroz svih n^2 vrhova mreže $n \times n$, a koja se sastoji od $2n - 2$ dužina? (Na slici je za $n = 4$ nacrtana linija koja se sastoji od $2n - 1$ dužina).

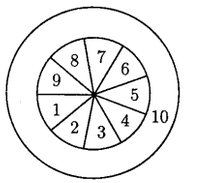


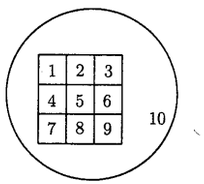
27. Na donjoj slici su tlocrti dviju kuća. Nađite (ako postoje) na svakom od tlocrta put koji prolazi kroz svaka vrata točno jedanput.





28. Dokažite da se "zemljopisne karte" na donjoj slici, koje se sastoje od 10 zemalja $1, 2, \ldots, 10$ mogu obojiti s 4 odnosno 3 boje, ali ne i s manje boja. Koliko ima različitih bojenja crvenom, bijelom i plavom bojom desne karte?





29. U ravnini je zadano n točaka koje leže tako da među udaljenostima po dvije od njih nema jednakih. Svaku od danih točaka spojimo dužinom s onom od preostalih točaka koja

joj je najbliža. Koliko najviše dužina prolazi (ili završava) u jednoj te istoj točki iz danog skupa?

30. a) Stari zadatak o čovjeku, vuku, kozi i zelju. Neki čovjek došao je do obale rijeke noseći glavicu zelja, i vodeći vuka i kozu. Dok je on prisutan, vuk neće pojesti kozu, niti koza zelje. Preko rijeke čovjek može prijeći sam, uzeti ili samo vuka, ili samo kozu, ili samo zelje. Može li on prelazeći rijeku više puta prenijeti na drugu obalu vuka, kozu i zelje, a da koza ne pojede zelje niti vuk kozu? Ako može, koji je najekonomičniji postupak, tj. postupak s najmanje prijelaza rijeke?

b) Sličan zadatak (pogodan za društvene igre) je ovaj: tri ljubomorne žene sa svojim supruzima dolaze na obalu rijeke. Društvo treba prijeći rijeku, a raspolažu čamčićem u koji može stati najviše dvoje ljudi. Postoji li (i ako postoji nađite) niz prelazaka čamčića preko rijeke kojim se svih 6 ljudi preveze preko rijeke tako da ni jedan suprug ne ostane sam (tj. bez svoje žene) u prisutnosti neke druge žene?

31. Između 9 zlatnika nalazi se jedan neispravni, manje težine. Kako ćemo u dva vaganja na vagi s dvije zdjelice konstatirati koji je zlatnik neispravan? (Pokušajte dokazati, ako se među 3^n zlatnika nalazi jedan neispravni manje težine, da ga onda možemo pronaći s n vaganja na vagi s dvije zdjelice.)

32. U nekom društvu od n mladića i n djevojaka svaki par mladić – djevojka je ili "skladan" ili "neskladan". Ako nema načina da mladići i djevojke sklope n "skladnih" brakova, dokažite da tada za neko $k > 0$ postoji skup od k mladića koji su "u skladu" sa samo $k-1$ djevojaka.

33. Dvoje ljudi ima kanistar od 8 l vina i dva prazna kanistra od 3 l i 5 l. Nađite najjednostavniji način da se podijeli vino na jednake dijelove.

34. U nekom društvu svaka dva znanca nemaju zajedničkih znanaca, a svaka dva neznanca imaju točno dva zajednička znanca. Dokažite da u tom društvu svi imaju jednak broj znanaca.

35. Skup S od n točaka u ravnini ima svojstvo da za svake dvije točke iz S postoji treća točka iz S koja je na pravcu određenom prvim dvjema. Tada sve točke iz S leže na jednom pravcu. Dokažite to rabeći Erdös-Gallai-Sylvestrov teorem.

§ 2. Osnovni pojmovi

Skupovi, funkcije, polinomi i formalni redovi

Podsjetimo se ukratko na osnovne pojmove i neke činjenice. Pojam **skupa** je osnovni pojam matematike, te se ne definira, tj. ne svodi se na još jednostavnije pojmove. Svaki skup čine njegovi **elementi** i skup je njima posve određen. Izjavu "x je element skupa S" bilježimo simbolički $x \in S$, a negaciju te izjave bilježimo $x \notin S$. Među skupove ubrajamo i **prazan skup** $\emptyset$, koji je bez elemenata. Skup S najčešće se opisuje pomoću nekim svojstvom P (predikatom), tako da elementima od S smatramo sve objekte x koji u danim okolnostima dolaze u obzir, a imaju svojstvo P. Tada to pišemo $S = \{x \mid x \text{ ima svojstvo } P\}$ ili $S = \{x \mid P(x)\}$ i čitamo "S je skup svih elemenata x sa svojstvom P". Ako je skup S sastavljen npr. od elemenata a, b, c, d, onda se piše $S = \{a, b, c, d\}$. Oznaka $S := \{x \mid P(x)\}$ znači da definiramo skup S kao skup svih x sa svojstvom P. Elementi skupova mogu biti

najrazličitiji, npr. stanovnici nekog grada, svi pravci neke ravnine, svi realni brojevi čiji je kvadrat veći od 2, pa konačno i neki skupovi mogu biti elementi nekog novog skupa. Kažemo da je skup S **podskup** ili **dio** skupa T (a skup T **nadskup** skupa S) i pišemo $S \subseteq T$ (čita se "S je sadržan u T") ili $T \supseteq S$ (čita se "T sadrži S") ako je svaki element $x \in S$ element od T, tj. $x \in T$. Prazan skup $\emptyset$ je podskup svakog skupa. Dva skupa S i T su **jednaka** i piše se $S = T$, ako je $S \subseteq T$ i $T \subseteq S$, tj. ako je svaki element od S element od T i svaki element od T ujedno i element od S. Ako je $S \subseteq T$ i $S \neq T$, kažemo da je S **pravi podskup** od T; pišemo $S \subset T$. Na primjer, $\{1,2,3\} = \{2,1,3\}$, ali $\{1,2,3\} \neq \{1,2\}$ i $\{1,2\} \subset \{1,2,3,4\}$. Uočite da je poredak elemenata unutar vitičastih zagrada nebitan. Relacija $\subseteq$ zove se **inkluzija**.

Sa skupom S posve je određen **partitivni skup** od S, čiji su elementi svi podskupovi skupa S. Taj se skup obično označava ili s $\mathcal{P}(S)$ ili s 2^S. Očito je $\emptyset, S \in \mathcal{P}(S)$. Podskup od $\mathcal{P}(S)$ se katkad zove **familija podskupova** od S. Za podskupove A i B nekog skupa U definiramo **uniju** $A \cup B := \{x \in U \mid x \in A \text{ ili } x \in B\}$, **presjek** $A \cap B := \{x \in U \mid x \in A \text{ i } x \in B\}$, **razliku** $A \setminus B := \{x \in U \mid x \in A \text{ i } x \notin B\}$ (katkad pišemo $A - B$), **simetričnu razliku** $A \triangle B := (A \setminus B) \cup (B \setminus A)$ i **komplement** $\overline{A} := U \setminus A$. Kažemo da su A i B **disjunktni** ako je $A \cap B = \emptyset$. Podsjetite se uobičajenih pravila za $\cup$ i $\cap$ i **de Morganovih formula**: $\overline{A \cup B} = \overline{A} \cap \overline{B}$, $\overline{A \cap B} = \overline{A} \cup \overline{B}$.

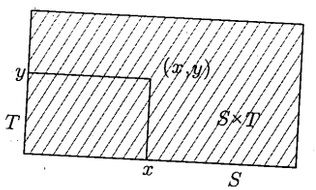
Koristit ćemo se standarnim oznakama za osnovne skupove brojeva, i to:

$\mathbb{N}$ = skup prirodnih brojeva $= \{1, 2, 3, \ldots, n, n+1, \ldots\}$,
$\mathbb{Z}$ = skup cijelih brojeva $= \{\ldots, -2, -1, 0, 1, 2, 3, \ldots\}$
$\mathbb{Q}$ = skup racionalnih brojeva $= \left\{\frac{m}{n} \mid m \in \mathbb{Z}, n \in \mathbb{N}\right\}$
$\mathbb{R}$ = skup realnih brojeva
$\mathbb{C}$ = skup kompleksnih brojeva $= \left\{x + iy \mid x, y \in \mathbb{R}\right\}$
$\mathbb{Z}^+$ = $\mathbb{N}_0 = \{0, 1, 2, 3 \ldots\}$
$[n]$ = $\{1, 2, 3, \ldots, n\}$ (ili katkad $\mathbb{N}_n$).

Direktni (ili **Kartezijev**) **produkt** dvaju skupova S i T je skup $S \times T$ svih **uređenih parova** (x, y) elemenata $x \in S$, $y \in T$, tj.

$$S \times T = \{(x, y) \mid x \in S, y \in T\}.$$

Za uređene parove je $(x, y) = (x', y')$ ako i samo ako je $x = x'$ i $y = y'$. Napomenimo da se uređeni par (x, y) općenito razlikuje od uređenog para (y, x). Nadalje, uređen par (x, y) se može definirati i kao skup $\{\{x\}, \{x, y\}\}$. Smatramo da je uvijek $\emptyset \times S = S \times \emptyset = \emptyset$.



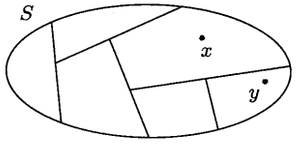
Općenito, ako imamo n skupova ($n \in \mathbb{N}$), $S_1, S_2, \ldots, S_n$ onda se njihov direktni produkt $S_1 \times S_2 \times \ldots \times S_n$ definira kao skup svih uređenih $n-$torki $(x_1, x_2, \ldots, x_n)$, $x_1 \in S_1, \ldots, x_n \in S_n$. Ako je $S_1 = S_2 = \ldots = S_n$, onda se $n-$struki direktni produkt $S \times S \times S \ldots \times S$ zapisuje još i kao S^n.

Svaki podskup $\rho \subseteq S \times S$ zove se **binarna relacija** na skupu S. Za elemente x, y kažemo da su u relaciji ρ, i piše se $\rho(x, y)$ ili $x\rho y$ ako je $(x, y) \in \rho$.

Relacija ρ je **refleksivna**, ako je $x\rho x$, za svako $x \in S$; relacija ρ je **simetrična** ako za svako $x, y \in S$, $x\rho y$ povlači $y\rho x$; relacija ρ je **tranzitivna** ako za svako $x, y, z \in S$, $(x\rho y)\&(y\rho z)$ povlači $x\rho z$. **Relacija ekvivalencije** ili **klasifikacije** je binarna relacija koja je istodobno refleksivna, simetrična i tranzitivna. Obično se relacija ekvivalencije bilježi s $\sim$. Na primjer, jednakost elemenata "=" nekog skupa S je relacija ekvivalencije na S.

Ako je $\sim$ relacija ekvivalencije na nekom skupu S, onda se S može prikazati na jedinstven način kao unija disjunktnih podskupova, tzv. **klasa ekvivalencije** s obzirom na relaciju $\sim$.

U istu klasu, po definiciji, ulaze svi međusobno ekvivalentni elementi od S. Za $x \in S$ označimo s $[x] = \{y \in S | y \sim x\}$ klasu ekvivalencije od x. Tada je očito $x \sim y \iff [x] = [y]$, te za svake dvije klase $[x], [y]$ vrijedi da se ili podudaraju ili su disjunktne. Unija svih klasa ekvivalencije je očito čitav skup S, pa relacija ekvivalencije $\sim$ na S definira jednu **particiju** skupa S na klase ekvivalencije. Shematski se ta situacija može prikazati ovako:



Skup svih klasa ekvivalencije s obzirom na relaciju ekvivalencije $\sim$ na S zove se **kvocijentni skup** i označava se sa $S/\sim$.

Drugi osnovni tip binarne relacije je relacija **parcijalnog uređaja** $\leq$ (manje ili jednako) na skupu S. To je binarna relacija na S koja je refleksivna, tranzitivna i **antisimetrična**, tj. ima svojstvo da za svako $x, y \in S$, $(x \leq y)\&(y \leq x)$ povlači $x = y$. Ako je osim toga za svaki $x, y \in S, (x \leq y)$ ili $(y \leq x)$, onda se govori o **relaciji uređaja** (ili **totalnog uređaja**). Skup S zajedno s relacijom $\leq$ parcijalnog uređaja zove se **parcijalno uređen skup** S. Ako je $\leq$ totalni uređaj na S, onda se S zajedno s $\leq$ (tj. uređen par $(S, \leq)$) zove **totalno uređen skup** ili **uređen skup**. Tako je npr. obična nejednakost $\leq$ na skupu $\mathbb{R}$ realnih brojeva totalni uređaj (katkad se još zove i **linearni uređaj**). Umjesto $x \leq y$ katkad se piše $y \geq x$ (y veće ili jednako od x). Ako je $x \leq y$ i $x \neq y$, piše se $x < y$ (x manje od y) ili $y > x$ (y veće od x).

Neka je $(S, \leq)$ parcijalno (ili totalno) uređen skup, a $X \subseteq S$ neprazan podskup od S. Kažemo da je $m \in S$ **donja međa** od X ako je $m \leq x$, $\forall x \in X$. Skup X je odozdo **omeđen** ako postoji bar jedna donja međa od X.

Najveća donja međa ili **infimum** odozdo omeđenog skupa $X \subseteq S$ je element $\inf S \in S$, ako vrijedi:

(1) $\inf X$ je donja međa skupa X
(2) za svaku donju među m skupa X vrijedi $m \leq \inf X$.

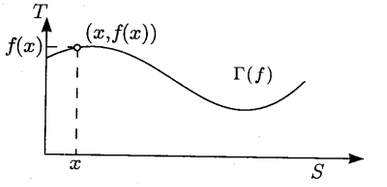
Ako $\inf X$ postoji, onda je jedinstven. Naime, pretpostavimo da imamo dva elementa $m_1, m_2 \in S$ sa svojstvima (1), (2). Tada bi vrijedilo $(m_1 \leq m_2)\&(m_2 \leq m_1)$, a odatle izlazi $m_1 = m_2$.

Najmanji element ili **minimum** skupa $X \subseteq S$ je element $\min X \in X$, koji je ujedno donja međa za X, tj. $\min X \leq x$, za svako $x \in X$. Ako minimum skupa X postoji, onda je opet jedinstven, te je očito $\inf X = \min X$.

Kažemo da je totalno uređen skup $(S, \leq)$ **dobro uređen**, ako svaki njegov neprazni podskup ima minimalni element. Tako je npr. skup $\mathbb{N}$ s obzirom na obični uređaj brojeva dobro uređen (vidi, npr. [153], str. 91), dok skup $\mathbb{R}$ s običnim uređajem to nije, jer npr. za skup $X = \{x \in Q \,|\, x^2 > 2\}, \inf X = \sqrt{2}$ nije najmanji element od X.

Posve analogno definiraju se pojmovi: **gornja međa**, **odozgo omeđen skup**, **najmanja gornja međa** ili **supremum** $\sup X$ i **najveći element** ili **maksimum** $\max X$ nepraznog skupa $X \subseteq S$. Ako je $X \subseteq S$ omeđen odozdo i odozgo, kažemo da je **omeđen**. Ako je $(S, \leq)$ parcijalno uređen skup, $a, b \in S, a \leq b$, onda se skup $[a, b] := \{x \in S \,|\, a \leq x \leq b\}$ zove **segment** u S, a ako je $a < b$, skup $\langle a, b\rangle := \{x \in S \,|\, a < x < b\}$ **interval** u S.

Neka su sada S i T dva skupa. **Preslikavanje** ili **funkcija** sa skupa S u skup T je uređena trojka (S, T, f), koja se sastoji od skupa S, koji se zove **područje definicije** ili **domena**, skupa T, koji se zove **područje vrijednosti** ili **kodomena**, te nekog pravila f, pomoću kojeg svakom elementu $x \in S$ pridružujemo neki element $y \in T$ (koji ovisi o x). Pridruženi element y zove se **vrijednost preslikavanja** na elementu x i označava se s $f(x)$. Katkad je zgodna i oznaka $x \mapsto f(x)$, $x \in S$, $f(x) \in T$ ili jednostavno $x \mapsto f(x)$, kojom se označava funkcija koja prevodi element x u $f(x)$. Npr. kvadriranje je funkcija $x \mapsto x^2$, $x \in \mathbb{R}, x^2 \in \mathbb{R}$.
Graf preslikavanja (S, T, f) je skup $\Gamma(f) = \{(x, f(x)) | x \in S\} \subseteq S \times T$ (v. sl.)



Uobičajena oznaka za preslikavanje ili funkciju je $f : S \to T$. Često se još o elementima $x \in S$ govori kao o **nezavisnoj varijabli** ili **argumentu**, a o elementima $y \in T$ kao o **zavisnoj varijabli** funkcije. Pojam funkcije se može alternativno definirati ovako. $f : S \to T$ je podskup $\Gamma \subseteq S \times T$, koji ima svojstvo da za svako $x \in S$ postoji jedan i samo jedan $y \in T$, tako da je $(x, y) \in \Gamma$. Tu smo, dakle, poistovjetili pojam funkcije s pojmom njezinog grafa i taj je pristup s logičke strane u prednosti jer se ne služi s nedefiniranim pojmom "pravilo" , ali je prvi pristup intuitivno bliži, a ne uzrokuje teškoće, jer se u njemu može gledati samo način govora, dok je matematički smisao iz ovog drugog pristupa.

Poučno je nacrtati grafove funkcija $\lfloor\,\rfloor, \lceil\,\rceil : \mathbb{R} \to \mathbb{Z}$, gdje je $\lfloor x \rfloor =$ **najveći cijeli**

broj $\leq x$ ("pod" od x), $\lceil x \rceil$ = **najmanji cijeli broj** $\geq x$ ("strop" od x). Uočite da je $\lceil x \rceil = -\lfloor -x \rfloor$.

Preslikavanja (S, T, f) i (S', T', f') su **jednaka** ako je $S = S'$, $T = T'$ i za svako $x \in S = S'$ je $f(x) = f(x')$. Vrlo je važno uočiti da za jednakost preslikavanja zahtijevamo da su im domene i kodomene jednaki skupovi. Npr. neka je $S \subseteq T$. Preslikavanje $i : S \to T$, definirano formulom $i(x) = x, x \in S$, zove se **inkluzija** (ili **ulaganje**). Ako je $S \subset T$, onda je inkluzija $i : S \to T$ različita od **identitete** $1_S : S \to S$, $1_S(x) = x$, $x \in S$. Naime, tada $i, 1_S$ imaju različite kodomene. Slijede još neki važniji primjeri preslikavanja. Neka su S i T skupovi. Tada definiramo **projekcije** $p_S : S \times T \to S$ i $p_T : S \times T \to T$, sa $p_S(x, y) = x$, $p_T(x, y) = y$ (zapravo bi trebalo pisati $p_S((x, y))$, ali te dvostruke zagrade obično izostavljamo); projekciju p_S zovemo prvom, a p_T drugom projekcijom. Nadalje, ako je $\sim$ relacija ekvivalencije na skupu S, onda definiramo **prirodnu projekciju** ili **kvocijentno preslikavanje** $q : S \to S/\sim$, formulom $q(x) = [x]$. Daljnji važni primjeri preslikavanja su **binarne operacije**. Binarna operacija na skupu S je svako preslikavanje skupa $S \times S$ u S. Npr. zbrajanje prirodnih brojeva je binarna operacija $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, $+(k, l) = k + l \in \mathbb{N}$. Ili, $\cup, \cap, \setminus$ su binarne operacije na partitivnom skupu $S = \mathcal{P}(U)$, jer svakom paru $(A, B) \in \mathcal{P}(U) \times \mathcal{P}(U)$ pridružuju novi element $A \cup B \in \mathcal{P}(U)$, $A \cap B \in \mathcal{P}$, $A \setminus B \in \mathcal{P}(U)$. **Kompozicija preslikavanja** $f : R \to S$ i $g : S \to T$ je preslikavanje $h : R \to T$, takvo da je za svako $x \in R, h(x) = g(f(g))$. Oznaka za kompoziciju od f i g je $g \circ f$, tj. $h = g \circ f$ ili jednostavno $h = gf$.

Ako su $f : P \to R$, $g : R \to S$, $h : S \to T$ preslikavanja, tada je $h \circ (g \circ f) = (h \circ g) \circ f$, tj. za kompoziciju preslikavanja vrijedi **zakon asocijacije** (dokažite to!). Nadalje, ako su $1_S : S \to S$ i $1_T : T \to T$ identička preslikavanja, a $f : S \to T$, onda je $f \circ 1_S = 1_T \circ f = f$.

Neka je $S' \subseteq S$, a $f : S \to T$. Tada je $f' : S' \to T$, $f'(x) = f(x)$, $x \in S'$, **restrikcija** (ili **suženje**) od f na podskup S' i pišemo $f|_{S'}$. Kažemo još da je f **proširenje** (ili **ekstenzija**) od f' na S.

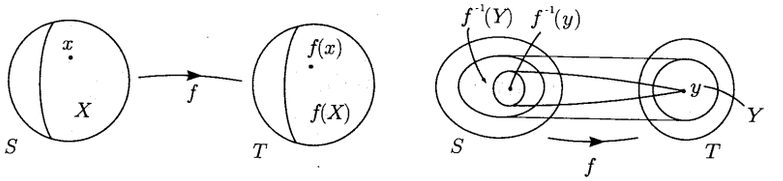
Vrlo korisna funkcija za ispitivanje pripada li neki element nekog ("velikog") skupa U nekom podskupu od U je tzv. **karakteristična funkcija** χ_S podskupa $S \subseteq U$. To je funkcija $\chi : U \to \{0, 1\}$ definirana s

$$\chi_S(x) = \begin{cases} 1, & \text{ako } x \in S \\ 0, & \text{ako } x \notin S. \end{cases}$$

Umjesto skupa $\{0, 1\}$ može se uzeti bilo koji dvočlani skup, npr. {istinito, lažno} itd. Ta je funkcija vrlo korisna za programiranje na kompjuterima.

Slika skupa $X \subseteq S$ pri preslikavanju $f : S \to T$ je skup $f(X) := \{y \in T | \exists x \in X \& y = f(x)\} \subseteq T$ ili kraće $f(X) = \{f(x) | x \in X\} \subseteq T$, a **slika od** f, $\operatorname{Im} f := f(S)$.

Inverzna slika (ili **original**) skupa $Y \subseteq T$ pri preslikavanju $f : S \to T$ je skup $f^{-1}(Y) = \{x \in S | f(x) \in Y\}$. Ako je $Y = \{y\}$ jednočlani skup, onda stavljamo $f^{-1}(y) := f^{-1}(\{y\}) = \{x \in S | f(x) = y\}$ i zovemo ga **originalom točke** y po f ili **vlakno** od f. Shematski možemo sliku, inverznu sliku i original točke ovako prikazati:



Oznaka za skup svih preslikavanja sa skupa S u skup T je T^S.

Za preslikavanje $f : S \to T$ kažemo da je **injekcija** (ili **1–1–preslikavanje**) ako $f(x) = f(x')$ povlači $x = x'$, a kažemo da je **surjekcija** (ili **preslikavanje na**) ako je $f(S) = T$ (tj. $(\forall y \in T)(\exists x \in S), f(x) = y$). f je **bijekcija** (ili **obostrano jednoznačno preslikavanje**) ako je f injekcija i surjekcija.

Kažemo da su skupovi S i T **ekvipotentni** ili **bijektivni** ako postoji bijekcija $f : S \to T$. Relacija ekvipotencije je relacija ekvivalencije, pa se skupovi svrstavaju u disjunktne klase; klasa kojoj pripada skup S zove se **kardinalni broj** skupa S i označava se sa $|S|$ ili card S ili $\#S$.

Neka je $f : S \to T$. Kažemo da je $g : T \to S$ **inverzno preslikavanje** ili **inverz** od f ako je $gf = 1_S$ i $fg = 1_T$. Odmah se vidi da za dano preslikavanje f može postojati najviše jedno inverzno preslikavanje. Dalje, ako za $f : S \to T$ postoji inverz, onda je f bijekcija, i obratno, svaka bijekcija f dopušta inverzno preslikavanje koje se označava s f^{-1}.

Kažemo da je skup S **konačan skup** ako S nije ekvipotentan ni s jednim svojim pravim podskupom. Kažemo da je skup S **beskonačan** ako nije konačan, tj. ako postoji pravi podskup $S' \subset S$ i bijekcija $f : S \to S'$. Prazan skup $\emptyset$ je konačan skup i stavljamo $|\emptyset| = 0$. Kardinalan broj konačnog skupa S se još zove i **broj elemenata** od S ili **brojnost** od S. Mi ćemo se u ovoj knjizi uglavnom baviti konačnim skupovima i njihovim brojnostima, pa ćemo stavljati za beskonačne skupove S da je njihov kardinalni broj $|S| = \infty$ (iako i za beskonačne skupove postoji odgovarajuća "aritmetika" i "kombinatorika"). Kao što smo već naglasili, kombinatorika i jest matematika konačnih skupova.

Osnovna svojstva konačnih skupova izričemo sljedećim teoremom.

TEOREM 1. *(a) Svaki podskup konačnog skupa je konačan.*

(b) Svaki skup bijektivan konačnom skupu je konačan.

(c) Ako je svaki pravi dio skupa S konačan skup, onda je i S konačan.

(d) Ako je S konačan skup, onda je i skup $T = S \cup \{t\}$ konačan.

(e) Za svako $n \in \mathbb{N}$, skup $[n] = \{1, 2, \ldots, n\}$ je konačan i stavljamo $|[n]| = n$.

(f) Neprazan skup S je konačan, ako i samo ako postoji $n \in \mathbb{N}$, tako da je S bijektivan s $[n]$.

(g) Skup S je konačan ako i samo ako je svaka injekcija $S \to S$ ujedno i surjekcija (pa stoga i bijekcija).

(h) Skup S je konačan ako i samo ako je svaka surjekcija $S \to S$ ujedno i injekcija (pa stoga i bijekcija).

(i) Skup S je konačan ako i samo ako postoji $n \in \mathbb{N}$ i surjekcija $[n] \to S$.

(j) Unija od konačno mnogo konačnih skupova je konačan skup.

(k) Direktni produkt od konačno mnogo konačnih skupova je konačan skup.

(l) Svaki konačan skup S se može (totalno) urediti; svaki uređaj na $S \neq \emptyset$ je dobar i diskretan uređaj.

Pritom kažemo da je $(S, \leq)$ **diskretno uređen** *ako svaki element koji nije minimalan ima direktnog prethodnika, a svaki element koji nije maksimalan ima direktnog sljedbenika; pritom kažemo da je b* **direktni sljedbenik** *od a ako je $a < b$ i nema elementa $x \in S$, takvog da je $a < x$ i $x < b$. Analogno se definira* **direktni prethodnik**.

Mi nećemo provesti dokaz ovog teorema, nego ga prepuštamo čitatelju.

Dakle, za svaki konačan skup $S \neq \emptyset$ postoji jedinstven prirodan broj n takav da je $|S| = n$; kažemo da S **ima** n **elemenata** ili da je S n**-člani skup**. Upravo je i jedno od najčešćih pitanja u kombinatorici "koliko elemenata ima skup S?" pa se i razne tehnike kombinatorike usmjeruju na to da se nađe taj broj elemenata.

Još jedan pojam će nam biti vrlo koristan, a to je particija skupa. Kažemo da neprazni različiti skupovi $S_1, S_2, \ldots, S_k$ čine **particiju** (konačnog) skupa $S \neq \emptyset$ ako je $S_1 \cup S_2 \cup \ldots \cup S_k = S$ i svaka dva skupa S_i, S_j su ili disjunktni ili se podudaraju, tj. $S_i \neq S_j \Rightarrow S_i \cap S_j = \emptyset$. To onda znači da za svako $x \in S$ postoji jedinstveni $i \in \{1, 2, \ldots, k\}$, takav da je $x \in S_i$. Skupovi S_i se zovu **blokovi particije**. Ako želimo istaknuti da imamo točno k blokova, govorimo o k-**particiji**. Napomenimo da svaka relacija ekvivalencije $\sim$ na konačnom skupu $S(\neq \emptyset)$ definira jednu particiju $S = S_1 \cup S_2 \cup \ldots \cup S_k$, gdje su S_i klase ekvivalencije, tj. kvocijentni skup $S/\sim$ je skup $\{S_1, S_2, \ldots, S_k\}$. Kvocijentno preslikavanje $q : S \to S/\sim$, koje svakom elementu $x \in S$ pridružuje jedinstvenu klasu ekvivalencije $[x]$ je surjekcija. No vrijedi i obratno: svaka particija $\{S_1, \ldots, S_k\}$ skupa S definira jednu relaciju ekvivalencije $\sim$ na S. Naime, $x \sim y :\iff \exists i \in \{1, 2, \ldots, k\}$ tako da je $x \in S_i, y \in S_i$.

Napose korisne particije dobivamo preslikavanjima. Vrijedi

TEOREM 2. *Neka su S i T konačni skupovi, a $f : S \to T$ neko preslikavanje. Tada skup svih nepraznih originala $f^{-1}(y), y \in T$ definira jednu particiju skupa S. Ta se particija na S zove* **particija inducirana preslikavanjem** *f ili* **jezgra** *od f i označava se s* $\ker f$.

Podsjetimo nadalje na **princip matematičke indukcije**. Neka je $S \subseteq \mathbb{N}$ podskup skupa prirodnih brojeva s ova sva svojstva:

$$\begin{aligned} &1 \in S && \text{(baza indukcije)} \\ &n \in S \Rightarrow n+1 \in S && \text{(korak indukcije).} \end{aligned}$$

Tada je $S = \mathbb{N}$. Ustvari, princip matematičke indukcije (kratko ćemo reći indukcije) je ekvivalentan tome da svaki neprazni podskup $S \subseteq \mathbb{N}$ ima najmanji element.

Principom indukcije služimo se i tada kada želimo definirati neko preslikavanje $x : \mathbb{N} \to S$ u skup S. Svako takvo preslikavanje zove se **niz** u S, a $x(n)$ se obično označava s x_n i zove **opći** ili n**−ti član niza** x s **indeksom** n. Niz se obično označava s $(x_n), n \in \mathbb{N}$ ili jednostavno $x_1, x_2, \ldots, x_n, \ldots$ Vrijedi sljedeće:

Princip definicije indukcijom (ili rekurzijom). Neka je S skup, $a \in S$, te neka je za svako $n \in \mathbb{N}$ dano neko preslikavanje $f_n : S \times S \times \ldots \times S \to S$. Tada postoji jedinstveni niz (x_n) u S, takav da je

$$\begin{aligned} x_1 &= a \\ x_{n+1} &= f_n(x_1, x_2, \ldots, x_n), \text{ za svako } n \in \mathbb{N}. \end{aligned} \qquad (*)$$

Posebno ako f_n ovisi samo o varijabli x_n, tj. ako je $f_n(x_1, \ldots, x_n) = f_n(x_n)$, onda zapravo imamo za svako $n \in \mathbb{N}$ preslikavanje $f_n : S \to S$, pa postoji jedinstven niz $x_1, x_2, \ldots, x_n, \ldots$ u S, takav da je $x_1 = a$ i $x_{n+1} = f_n(x_n)$, za svako $n \in \mathbb{N}$. $(*)$ se zove **rekurzivna formula** (ili **relacija**) ili kratko **rekurzija** za niz (x_n). Za dokaz vidi [153].

Neka je $S = \mathbb{N}$, $a = 1$ i neka je $f_n : \mathbb{N} \to \mathbb{N}$ dano sa $f_n(p) = p \cdot (n+1)$. Zaključujemo da postoji jedinstven niz u $\mathbb{N}$, takav da je $x_1 = 1$, te $x_{n+1} = f_n(x_n) = x_n(n+1)$, $n \in \mathbb{N}$. Očito je $x_2 = 1 \cdot 2$, $x_3 = 1 \cdot 2 \cdot 3$, ..., općenito $x_n = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$. Oznaka za $1 \cdot 2 \cdot 3 \cdot \ldots \cdot n$ je $n!$ i čita se n **faktorijela**. Po definiciji se stavlja da je $0! := 1$.

Sada ćemo precizno opisati što je to **suma** od m članova: $\sum_{i=1}^{m} x_i$, gdje su $x_1, \ldots, x_m$ dani brojevi. Neka je $S = \mathbb{R}$ (ili $\mathbb{C}$ ili bilo koji skup u kojem imamo asocijativno zbrajanje), $m \in \mathbb{N}$ i za $n \in \{1, 2, \ldots, m-1\}$ neka je $f_n : \mathbb{R} \to \mathbb{R}$, $f_n(x) = x + x_{n+1}$, a neka je $x_1 = a$. Tada postoji jedno jedino preslikavanje $g : \{1, 2, \ldots, m\} \to \mathbb{R}$ tako da je za svako $n \in \{1, 2, \ldots, m-1\}$, $g(1) = x_1$, $g(n+1) = f_n(g_n(n)) = g(n) + x_{n+1}$. Napose, posve je određen broj $g(m) \in \mathbb{R}$. Taj broj $g(m)$ ovako pridružen $m-$torki $(x_1, \ldots, x_m) \in \mathbb{R}^m$ označava se sa $\sum_{i=1}^{m} x_i$ ili s $x_1 + \ldots + x_m$. U toj oznaci gornja rekurzivna formula postaje $\sum_{i=1}^{1} x_i = x_1$, $\sum_{i=1}^{n+1} x_i = (\sum_{i=1}^{n} x_i) + x_{n+1}$. Općenitije, mogu se promatrati sume

$$\sum_{i_1, \ldots, i_k = 1}^{n} x_{i_1 \ldots i_k}.$$

Ovdje se sumira po $i_1, i_2, \ldots, i_k$ od 1 do n, bez ikakvih ograničenja, tj. i_1 ide slobodno od 1 do n, a istovremeno i_2 ide od 1 do n itd. Tako je npr. $\sum_{i_1, \ldots, i_k = 1}^{n} x_{i_1 \ldots i_k} = \sum_{i_1=1}^{n} \left(\sum_{i_2, \ldots, i_k = 1}^{n} x_{i_1 i_2 \ldots i_k} \right)$. No katkad imamo i ograničenje, npr. da je $i_1 \leq i_2 \leq \ldots \leq i_k$. Tada se takva suma zapisuje ovako: $\sum_{1 \leq i_1 \leq i_2 \leq \ldots \leq i_k \leq n} x_{i_1 i_2 \ldots i_k}$. Analogno se definiraju **produkti** $\prod_{i=1}^{n} x_i$ brojeva $x_1, \ldots, x_n$.

Podsjetimo se i na pojam polinoma.

Neka je $n \in \mathbb{N}_0$, $a_0, a_1, \ldots, a_n \in \mathbb{C}$. Tada se funkcija $P : \mathbb{C} \to \mathbb{C}$, definirana s

$$z \mapsto P(z) = a_0 + a_1 z + \ldots + a_n z^n = \sum_{i=0}^{n} a_i z^i,$$

zove **polinom** (nad poljem $\mathbb{C}$), a $a_0, a_1, \ldots, a_n$ zovu se **koeficijenti polinoma** P. Ako je $a_n \neq 0$, P je **polinom stupnja** n, u oznaci $\deg P = n$ ili $\mathrm{st}P = n$. Ako je $a_n = 1$, polinom P se zove **normiran**. Ako je $P : \mathbb{R} \to \mathbb{R}$, $P(x) = a_0 + a_1 x + \ldots + a_n x^n$, govorimo o **realnom polinomu** (ili nad $\mathbb{R}$). **Nultočka (korijen) polinoma** P je broj $z_0 \in \mathbb{C}$ takav da je $P(z_0) = 0$. **Nulpolinom** je polinom za koji je $P(x) = 0$ za sve x, a stupanj mu nije definiran (katkad stavljamo da je -1). Koeficijent uz x^k polinoma P bilježimo simbolom

$$\langle x^k \rangle P(x).$$

Primjerice, ako je $P(x) = 2x^3 - 5x^2 - 7x + 4$, onda je $\langle x^2 \rangle P(x) = -5$.

Podsjetimo se da su dva polinoma jednaka ako i samo ako su im stupnjevi jednaki i odgovarajući koeficijenti jednaki. Nadalje, svaki polinom stupnja $n \geq 1$ ima nultočku u $\mathbb{C}$ i ako su mu $x_1, x_2, \ldots, x_n$ sve (ne nužno različite) nultočke, onda je $P(x) = a_n(x - x_1)(x - x_2)\cdots(x - x_n)$.

Skup svih polinoma nad $\mathbb{R}$ označavamo s $\mathbb{R}[x]$, a nad $\mathbb{C}$ sa $\mathbb{C}[z]$. Polinome zbrajamo tako da zbrojimo odgovarajuće koeficijente, a množenje je definirano ovako. Ako je $P(x) = \sum_{i=0}^{m} a_i x^i$, a $Q(x) = \sum_{j=0}^{n} b_j x^j$, onda je $P(x) \cdot Q(x) = \sum_{k=0}^{m+n} c_k x^k$, gdje je koeficijent $c_k = a_0 b_k + a_1 b_{k-1} + \ldots + a_k b_0$. Na taj način $\mathbb{R}[x]$ (ili $\mathbb{C}[x]$) postaje komutativni prsten s jedinicom (bez djelitelja nule).

Skup svih polinoma s koeficijentima iz nekog komutativnog prstena P označavamo s $P[x]$. Uz zbrajanje i množenje kao gore i $P[x]$ je prsten.

Nadalje, skup svih polinoma u više varijabli $x_1, x_2, \ldots, x_n$, s koeficijentima u P označava se s $P[x_1, x_2, \ldots, x_n]$. Npr. u dvije varijable x, y prsten $P[x, y]$ ima tipične elemente $f = \sum a_{ij} x^i y^j$, $a_{ij} \in P$, gdje se sumira po nekom konačnom skupu parova $(i, j) \in \mathbb{N}_0 \times \mathbb{N}_0$. Umjesto da se specificira taj konačan skup, obično se uzima suma preko svih (i, j), ali s tim da je $a_{ij} = 0$, osim u nekom konačnom skupu parova.

Općenito se prsten polinom nad P u n varijabli definira induktivno s

$$P[x_1, x_2, \ldots, x_n] = P[x_1, \ldots, x_{n-1}][x_n].$$

Drugim riječima, na elemente od $R = P[x_1, \ldots, x_n]$ možemo gledati kao na polinome u varijabli x_n s koeficijentima koji su polinomi u varijablama $x_1, \ldots, x_{n-1}$ nad P. Iz te definicije se odmah dobiva da tipični element iz R izgleda ovako:

$$f = f(x_1, x_2, \ldots, x_n) = \sum a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$$

gdje je $a_{i_1 i_2 \ldots i_n} \in P$ jedinstveno određeni koeficijent uz monom $x_1^{i_1} \ldots x_n^{i_n}$. Može se (formalno) uzeti da je i ovdje sumiranje beskonačno, tj. da se sumira preko svih multiindeksa $i_1 i_2 \ldots i_n$, ali s time da su svi koeficijenti a_I ($I = i_1 i_2 \ldots i_n$ multiindeks), osim za konačno mnogo multiindeksa I, jednaki 0. Mi uvijek pretpostavljamo da

varijable međusobno komutiraju, kao i da komutiraju pri množenju s elementom od P pa stoga prsten R ovisi simetrično o $x_1, \ldots, x_n$, pa x_n nema neku posebnu ulogu; isto bismo tako mogli pisati polinom f kao polinom u x_1 s koeficijentima u $P[x_2, \ldots, x_n]$ itd. Svaki produkt $x_1^{i_1} \ldots x_n^{i_n}$ zove se **monom**, a odgovarajući član $a_{i_1 i_2 \ldots i_n} x_1^{i_1} x_2^{i_2} \ldots x_n^{i_n}$, **monomijalni član. Ukupni stupanj** (ili kratko: **stupanj**) tog monomijalnog člana je $i_1 + i_2 + \ldots + i_n$, a **stupanj po varijabli** x_k je i_k. **Stupanj polinoma** $\deg f$, od f je najveći stupanj njegovih ne-nul-monomijalnih članova.

Prirodno poopćenje polinoma su formalni redovi. **Formalni red** (nad $\mathbb{C}$ ili $\mathbb{R}$) u jednoj varijabli x je formalna beskonačna suma oblika

$$f(x) = f = \sum_{n=0}^{\infty} a_n x^n = \sum_{n \geq 0} a_n x^n = a_0 + a_1 x + a_2 x^2 + \ldots,$$

gdje su $a_n \in \mathbb{C}$ ili $a_n \in \mathbb{R}$ i opet se zovu **koeficijenti formalnog reda** f. Dva su formalna reda f i $g = \sum_{n=0}^{\infty} b_n x^n$ po definiciji **jednaka** ako je $a_n = b_n$ za svako $n \in \mathbb{N}_0$. Zbrajanje i množenje formalnih redova f i g definira se formulama

$$f + g = \sum_{n=0}^{\infty} (a_n + b_n) x^n \quad \text{i} \quad f \cdot g = \sum_{n=0}^{\infty} \Big(\sum_{i+j=n} a_i b_j \Big) x^n.$$

Formalni red f je polinom ako su mu svi koeficijenti, osim možda konačno mnogo njih, jednaki 0. Kraće se to još kaže: "Gotovo svi koeficijenti a_n su 0." Skup svih formalnih redova nad $\mathbb{R}$ u varijabli x označavamo s $\mathbb{R}[[x]]$, a nad $\mathbb{C}$ sa $\mathbb{C}[[x]]$.

To su opet prstenovi. Slično se mogu promatrati i formalni redovi nad bilo kojim komutativnim prstenom P. Na primjer, formalni red je

$$f = 1 + x + x^2 + \ldots = \sum_{n=0}^{\infty} x^n \in \mathbb{R}[[x]] \text{ ili } f = 1 + \frac{x}{1} + \frac{x^2}{2} + \frac{x^3}{3} + \ldots = 1 + \sum_{n=1}^{\infty} \frac{x^n}{n} \in \mathbb{R}[[x]]$$

itd.

Svaki red potencija oblika $\sum_{n=0}^{\infty} a_n x^n$ (nad $\mathbb{R}$) koji je konvergentan[1] na izvjesnom intervalu može se promatrati kao formalni red.

Uz neke uvjete realna se funkcija $f : \langle a, b \rangle \to \mathbb{R}$ može u okolini točke $c \in \langle a, b \rangle$ razviti u **Taylorov red**, tj. postoji otvoren interval $I \subset \langle a, b \rangle$, $c \in I$, tako da za svako $x \in I$ vrijedi[1]

$$f(x) = f(c) + \frac{f'(c)}{1!}(x - c) + \frac{f''(c)}{2!}(x - c)^2 + \ldots = \sum_{n=0}^{\infty} \frac{f^{(n)}(c)}{n!}(x - c)^n,$$

gdje $f^{(n)}(c)$ označava $n-$tu derivaciju funkcije f izračunatu u točki $x = c$. Posebno, ako je $c = 0$, onda se Taylorov red zove **Maclaurinov red**:

$$f(x) = \sum_{n=0}^{\infty} \frac{f^{(n)}(0)}{n!} x^n.$$

[1] O konvergenciji redova, Taylorovoj formuli itd., vidi npr. u [133]

Svakom formalnom redu $f(x) = \sum_{n=0}^{\infty} a_n x^n$ pridružujemo njegovu **formalnu derivaciju** $D(f)$, koja je opet formalni red definiran formulom

$$D(f) = \frac{df(x)}{dx} = \sum_{n=0}^{\infty} n a_n x^{n-1} = \sum_{n=0}^{\infty} (n+1) a_{n+1} x^n.$$

Isto tako formalnom redu $f(x) = \sum_{n\geq 0} a_n x^n$ pridružujemo njegov **formalni integral** $I(f)$, koji je opet formalni red:

$$I(f) = \int_0^x f(t)dt = \sum_{n=0}^{\infty} a_n \frac{x^{n+1}}{n+1}.$$

Nije teško provjeriti da je $D(I(f)) = f$ te da je $D(f \cdot g) = D(f) \cdot g + f \cdot D(g)$. Formalni redovi se, dakle, deriviraju, odnosno integriraju, "član po član". **Formalni red** f u n **varijabli** $x_1, x_2, \ldots, x_n$ nad $\mathbb{R}$ (ili $\mathbb{C}$) formalni je izraz oblika

$$f = f(x_1, x_2, \ldots, x_n) = \sum_{i_1, \ldots, i_n = 0}^{\infty} a_{i_1 i_2 \ldots i_n} x_1^{i_1} \cdots x_n^{i_n}$$

gdje su $a_{i_1 i_2 \cdots i_n} \in \mathbb{R}$ (ili $\mathbb{C}$) **koeficijenti** formalnog reda f. Skup svih formalnih redova u varijablama $x_1, \ldots, x_n$ nad $\mathbb{R}$ označavamo s $\mathbb{R}[[x_1, x_2, \ldots, x_n]]$. Katkad se kraće, ali preglednije, taj formalni red zapisuje, pomoću multiindeksa ovako:

$$f = \sum_{I \in \mathbb{N}_0^n} a_I x^I$$

gdje je $I = (i_1, i_2, \ldots, i_n) \in \mathbb{N}_0^n$; pri tome se x^I interpretira kao $x_1^{i_1} x_2^{i_2} \cdots x_n^{i_n}$. Slična svojstva onima za redove u jednoj varijabli vrijede i za takve redove.

§ 3. Algoritmi

Često se kolokvijalno kaže da se teorijska računarska znanost (engl. computer science) zapravo sastoji od nalaženja i proučavanja algoritama. U nekom smislu to je i točno, pa taj osnovni pojam zahtijeva i točnu definiciju. Definicije iz leksikona poput "... svaki pravilni postupak pri računanju" nisu zadovoljavajuće, jer ti pojmovi nisu dovoljno precizirani. Malo preciznije, ali još uvijek intuitivno, može se reći: **Algoritam**[2] je konačan niz propisanih postupaka, pravila, naredbi ili recepata (uglavnom računskih), koji, ako se dosljedno slijedi, izvršava, konkretan zadatak. Nadalje, svaki algoritam mora zadovoljavati sljedeće:

1) **Ulaz** (input). Algoritam ima nekoliko (možda i nula) ulaznih podataka, tj podataka koji su mu zadani izvana i prije samog početka rada.

[2]Sama riječ "algoritam" (prvobitno algorizam) čini se da dolazi od imena autora poznatog arapskog udžbenika iz matematike Abu Ja'far Mohammed ibn Musa **al-Khowârizmi** (oko 825.). Knjiga se zvala "Kitab **al jabr** w'almuqabala" ("Pravila postavljanja i pretvorbi"). Otuda i riječ **algebra**.

2) **Izlaz** (output). Algoritam izbacuje kao rezultat barem jednu veličinu, koja ima točno određen odnos prema ulaznim podacima.

3) **Određenost.** Svaka naredba algoritma mora biti jedinstveno određena, tj. jasna i nedvosmislena u svakom mogućem slučaju.

4) **Konačnost.** Kad se slijede pravila algoritma, tada, kakvi god bili ulazni podaci, algoritam završava nakon konačno mnogo koraka.

Kao posljednji, ali ne i nužan zahtjev, traži se:

5) **Efektivnost.** Naime, od algoritma se obično traži da bude i provediv, tj. da svaka naredba bude toliko jednostavna da je, barem načelno, svatko može izvršiti u konačnom vremenu (obično se koristeći samo papirom i olovkom).

Algoritmi se mogu zapisati na razne načine. Ako ih zapisujemo svakodnevnim jezikom, treba biti vrlo oprezan da ne bude nedoumica. Jedno poboljšanje je da se algoritam opiše pomoću tzv. **dijagrama toka** (engl. flowchart). Na taj način se svaki korak stavi u svoju "kutiju" i strelicama se naznačuje sljedeći korak. Kutije različitih oblika koriste se za različite vrste operacija. Za mnoge svakodnevne aktivnosti mogu se domisliti algoritmi. Tako su np. razne "kuharice" (tj. knjige recepata) pisane približno u stilu algoritama, samo što su često prilično neprecizne (npr. što je "prstohvat soli"?). Poanta je u tome da algoritam mora biti pisan tako da ga svatko, pa čak i kompjuter može shvatiti (a ne samo iskusna kuharica).

Formalno se algoritam definira na sljedeći način: **Računarski postupak** (ili **metoda**) je četvorka (Q, U, I, f), gdje je Q skup s podskupovima U, I, a $f : Q \to Q$ funkcija, za koju je $f(q) = q$, za sve $q \in I$. Skupovi Q, U, I redom se zovu **računska stanja, ulazi** i **izlazi**, a f se zove **pravilo računanja**. Nadalje, za svaki ulaz $x \in U$ definiramo **izračunljiv niz** $x_0, x_1, x_2, \ldots$ rekurzivno s $x_0 = x, x_{k+1} = f(x_k)$, za $k \geq 0$. Kažemo da se izračunljiv niz **završava** nakon p koraka, ako je $p \geq 0$ najmanji cijeli broj, za koji je $x_p \in I$, te u tom slučaju kažemo da on daje izlaz x_p za zadanu vrijednost ulaza x. (Uočite da $x_p \in I \Rightarrow x_{p+1} \in I$, jer je $x_{p+1} = x_p$.) **Algoritam** je računarski postupak koji završava za sve vrijednosti ulaza $x \in U$. **Program** je zapis algoritma (ili čak računarske metode) na jednom od programskih jezika. Nas u ovoj knjizi programi kao takvi neće zanimati, pa ćemo algoritme zapisivati svakodnevnim jezikom.

Tako, npr. jedan od najstarijih poznatih algoritama je **Euklidov algoritam** za nalaženje najveće zajedničke mjere (n.z.m. (m, n)) dvaju danih brojeva $m, n \in \mathbb{N}$.

Euklidov algoritam. Dana su dva broja $m, n \in \mathbb{N}$. Treba naći n.z.m. (m, n).

Podijeli se m s n, a ostatak neka je r $(0 \leq r < n)$. Ako je $r = 0$, algoritam završava, a n je traženi broj, a inače se m zamijeni s n, a n s r i s tim se vrijednostima vrati na početak.

Koncizno se taj algoritam zapisuje ovako:

Euklid [traži se n.z.m.(m, n)]

sve dok je $n \neq 0$ **radi**

$r \leftarrow$ ostatak pri dijeljenju m sa n

$m \leftarrow n$
$n \leftarrow r$

kraj. [tekuća vrijednost od m je traženi broj]

Simbol $\leftarrow$ čita se "postaje" ili "supstituira se". Npr. gore "$m \leftarrow n$" znači da vrijednost varijable m postaje tekuća vrijednost varijable n. Formalno, u Euklidovu algoritmu je skup Q računskih stanja jednak

$$\mathbb{N} \cup \mathbb{N} \times \mathbb{N} \cup (\{(m,n,r,1)\} \cup \{(m,n,r,2)\} \cup \{(m,n,p,3)\});\ m,n,p \in \mathbb{N},\ r \in \mathbb{N}_0),$$

ulaz $U = \mathbb{N} \times \mathbb{N}$, izlaz $I = \mathbb{N}$, a pravilo računanja $f : Q \to Q$ definirano je s $f(n) = n$, $f(m,n) = (m,n,0,1)$, $f(m,n,r,1) = (m,n,$ ostatak dijeljenja m s $n, 2)$,

$$f(m,n,r,2) = \begin{cases} n, & \text{ako je } r = 0 \\ (m,n,r,3), & \text{inače} \end{cases}, \qquad f(m,n,p,3) = (n,p,p,1).$$

Ova formalna definicija algoritma ne uključuje već spomenutu "efektivnost", pa se i neka ograničenja na Q, U, I, f u tom smislu mogu formalizirati unutar tzv. **teorije algoritma**, no u to nećemo ovdje ulaziti. Teorija algoritama uglavnom se bavi pitanjima egzistencije (efektivnih) algoritama za razrješenje određenih problema (vidi npr. [123], [154]).

Ono što je za praksu zanimljivo pripada tzv. **analizi algoritama.** Tu se uglavnom ispituju radne karakteristike algoritama, tj. njihova efikasnost i to prije svega vremenska složenost i prostorna složenost. (Ova posljednja nas manje zanima - to je pitanje u vezi s pohranom podataka). Vremenska složenost, ili jednostavno **složenost algoritma**, ili "vrijeme" računanja (ili rada) algoritma jest naprosto broj osnovnih računskih koraka koje algoritam izvodi prilikom prijelaza od ulaznih podataka do izlaznih rezultata.

Složenost algoritma općenito je, dakle, funkcija veličine ulaznih podataka ili **veličine problema**. Često je vrlo teško odrediti točnu vrijednost složenosti. Tako se npr. ona ne zna već za Euklidov algoritam, tj. koliki je broj dijeljenja kao funkcija od m i n. Najčešće se stoga pod složenošću $S_A(n)$ algoritma A misli na **složenost "najgoreg slučaja"**, tj. najveći broj osnovnih računskih koraka koje izvodi algoritam uz bilo koje ulazne podatke čiji je broj jednak n. Isto tako se često traži **prosječna složenost** $T_A(n)$. No, često je i to teško naći pa se zadovoljavamo donjim i gornjim međama za "najgori slučaj" ili "prosjek" ili njihovo **asimptotsko ponašanje** kada je broj ulaza velik, tj. procjene vrijednosti od $S_A(n)$ ili $T_A(n)$ za velike n, tj. kada $n \to \infty$.

Tako npr. neka je $T(m,n)$ broj dijeljenja u Euklidovu algoritmu za ulazne podatke m i n. Neka je T_n prosječni broj koraka dijeljenja za čvrsto n i proizvoljno m. Budući da je poslije prvog dijeljenja važno samo $m \mod n$ (tj. ostatak pri dijeljenju m s n), možemo pisati

$$T_n = \frac{1}{n} \sum_{k=0}^{n-1} T(k,n).$$

Pokazuje se tada da je ta prosječna složenost za dovoljno velike n dana približno s $T_n \approx 1.9405 \log_{10} n$ (vidi [123], vol.II). "Najgori slučaj" je u vezi s tzv. Fibonaccijevim brojevima (pogl. 3).

Složenosti dvaju algoritama za isti problem mogu se, naravno, razlikovati. Neka su npr. A_1 i A_2 dva algoritma i neka je npr. $S_{A_1}(n) = n^2/7$, a $S_{A_2}(n) = 4n$. Tada je očito A_2 brži i efikasniji algoritam od A_1 za sve probleme veličine $n > 28$. Uvijek će A_2 biti brži od A_1 za sve n počevši od nekog n_0, čak bez obzira na to koji su koeficijenti uz n^2 i n (umjesto 1/7 i 4). Kaže se da je tada A_2 **manjeg reda** nego A_1. Općenito za dvije funkcije $f, g : \mathbb{N} \to \mathbb{R}$ kažemo da je f manjeg reda od g ako postoje $K > 0$ i $n_0 \in \mathbb{N}$, tako da je $|f(n)| \leq K|g(n)|$, za sve $n \geq n_0$. U tom slučaju pišemo $f = O(g)$ ili $f(n) = O(g(n))$. f i g su **istog reda** ako je $f = O(g)$ i $g = O(f)$. Tako je npr. $n^2/7 + 3n = O(n^2)$, $100n^3 + 200n^2 - 9n = O(n^3)$, dok je $5n^2 \neq O(n)$. S druge strane, eksponencijalna funkcija a^n ($a > 1$ čvrst) nije manjeg reda ni od kojeg polinoma u n, tj. $a^n \neq O(n^r)$ za svako čvrsto $r \in \mathbb{N}$. To slijedi ovako. Iz binomnog teorema (vidi pogl. II) slijedi $a^n = (1+b)^n \geq \frac{1}{2}n(n-1)b^2$, $n \geq 2$, a odavde slijedi da je $\lim_{n\to\infty} n/a^n = 0$, pa stoga $\lim_{n\to\infty} n^r/a^n = \lim_{n\to\infty}(n/(a^{\frac{1}{r}})^n)^r = 0$ $\Rightarrow \lim_{n\to\infty} a^n/n^r = \infty$. Posebno stoga npr. 2^n puno brže raste, tj. većeg je reda od bilo kojeg polinoma od n. Odavde se (logaritmiranjem) lako dobiva da n puno brže raste od $\log_2 n$. Nadalje, $\lim_{n\to\infty} a^n/n! = 0$ jer je, npr. za $a = 2$

$$\frac{2^n}{n!} = \frac{2 \cdot 2 \cdot \ldots \cdot 2}{1 \cdot 2 \cdot \ldots \cdot n} < \frac{2}{1} \cdot \frac{2}{2} \cdot \frac{2}{3} \cdot \frac{2}{3} \cdot \ldots \cdot \frac{2}{3} = 2\left(\frac{2}{3}\right)^{n-3} \to 0, \text{ za } n \to \infty,$$

pa slijedi da je $n! \neq O(a^n)$, tj. $n!$ je većeg reda od eksponencijalne funkcije.

Asimptotska složenost određuje u biti najveći problem koji se može uraditi. Ako su dva algoritma za isti problem istog reda, onda, grubo govoreći, nijedan od njih ne obavlja zadatak bitno bolje od drugog. Za dovoljno velike n razlika postaje zanemariva s obzirom na razliku dvaju algoritama različitog reda. Ako je $S_A(n) = O(f(n))$, kažemo da je A **$O(f(n))$-algoritam**.

Jedan od razloga zašto je složenost algoritama važna "kompjuterašima" jest taj da sama egzistencija algoritma još ne jamči da se problem može praktički riješiti. Algoritam može biti tako neefikasan da bi čak i s kompjuterima novih generacija, sa sve većom brzinom, bilo nemoguće dobiti rezultate u nekom korisnom vremenu. Stoga treba karakterizirati "korisne" algoritme sa stajališta prakse. Spomenuta razmatranja i praksa pokazuju da su to **polinomski algoritmi**. Kažemo da je algoritam A **efikasan** ili **dobar** ako mu je složenost polinomska, tj. ako je $S_A(n) = O(P(n))$, gdje je $P(n)$ polinom.

Stoga eksponencijalni i pogotovo faktorijelni algoritmi nisu efikasni, dok je npr. algoritam sa složenošću $n \log_2 n$ efikasan i, štoviše, efikasniji od algoritma složenosti n^2. Tako npr. za $n = 50$, $n^2 = 2\,500$, a $n \log_2 n \approx 300$, a za $n = 500$, $n^2 = 250\,000$, dok je $n \log_2 n \approx 4\,500$. Uostalom $\lim_{n\to\infty}(n \log_2 n)/n^2 = 0$.

Ima međutim situacija, kao npr. u **linearnom programiranju** da su u praktičnoj upotrebi algoritmi (kao npr. razne **simpleks-metode**) koji u "najgorem slučaju" imaju eksponencijalnu složenost, ali u praksi pokazuju linearnu složenost, za što teorijsko objašnjenje nastoje dati radovi S. Smalea (Math. Programming 27

(1983), 241-262) i drugih (vidi [36]). S druge pak strane, poznati su polinomski algoritmi za linearno programiranje (vidi [97] i [62*]). Knjige posvećene raznim metodama analiza algoritama su [94], [123], [64*], [42*], [25*] i druge.

Zadaci

1. Neka je $S = \{1, 2, 3, 4\}$. Dokažite da za relacije $\rho \subseteq S \times S$ vrijedi

a) $\rho = \{(1,1),(2,2),(3,3),(4,4),(1,2),(2,1),(2,3),(3,2)\}$ je refleksivna i simetrična, a nije tranzitivna;

b) $\rho = \{(1,1),(2,2),(3,3),(4,4),(1,2)\}$ je refleksivna i tranzitivna, a nije simetrična;

c) $\rho = \{(1,1),(2,2),(1,2),(2,1)\}$ je simetrična i tranzitivna, a nije refleksivna.

2. Gdje je greška u ovom "dokazu": "Teorem. Neka je ρ simetrična i tranzitivna binarna relacija na S. Tada je ρ refleksivna. Dokaz. Neka je $(x, y) \in \rho$. Zbog simetričnosti je tada i $(y, x) \in \rho$. Zbog tranzitivnosti je onda i $(x, x) \in \rho$. Dakle je ρ refleksivna"?

3. Za sljedeće relacije ispitajte jesu li refleksivne, simetrične, tranzitivne i antisimetrične: a) ρ na $\mathbb{Z}$, $x\rho y$ ako je $x|y$; b) okomitost na skupu svih pravaca u ravnini; c) ρ na $\mathbb{Z}$, $x\rho y$ ako je $x + y$ paran (neparan); d) ρ na $\mathbb{Z}$, $x\rho y$ ako je $x - y$ paran (neparan); e) ρ na $\mathbb{Z} \times \mathbb{Z}$, gdje je $(x, y)\rho(u, v)$ ako je $x \leq u$.

Ako je neka od ovih relacija ekvivalencije, nađite kvocijentni skup.

4. Neka je S skup. Dokažite da je $(\mathcal{P}(S), \subseteq)$ partitivni skup od S s inkluzijom parcijalno uređeni skup.

5. Neka su $(S', \leq')$, $(S'', \leq'')$ dva parcijalno uređena skupa, a $S = S' \times S''$. Dokažite da je $\leq$ na S parcijalni uređaj, definiran s $(x', x'') \leq (y', y'')$ ako je $x' \leq x''$ & $y' \leq y''$.

6. Neka su $f : R \to S$, $g : S \to T$ preslikavanja. Dokažite da je f injekcija ako je $g \circ f : R \to T$ injekcija, a ako je $g \circ f$ surjekcija, da je onda i g surjekcija.

7. Na skupu $\mathbb{R}^S$ svih realnih funkcija $f : S \to \mathbb{R}$ definiramo $f \leq g$ sa $f(x) \leq g(x)$, $\forall x \in S$. Dokažite da je $\leq$ relacija parcijalnog uređaja na $\mathbb{R}^S$.

8. Neka je $A \subseteq S$, $B \subseteq T$, a $f : S \to T$. Dokažite da je $f^{-1}f(A) = A$ ako je f injekcija, a ako je f surjekcija onda je $ff^{-1}(B) = B$.

9. Dokažite Teorem 1.

10. Neka su $S, T \neq \emptyset$ skupovi. Dokažite da je $S \times T$ konačan skup ako i samo ako su S i T konačni.

11. Neka je S skup za koji je skup svih bijekcija $S \to S$ konačan. Dokažite da je i S konačan.

12. Neka su skupovi $S, T \neq \emptyset$ takvi da je skup svih surjekcija $\mathrm{Sur}(S, T)$ sa S na T također neprazan, a T nije jednočlan. Ako su $\mathrm{Sur}(S, T)$ i T konačni, dokažite da je i S konačan.

13. Neka su S, T konačni skupovi i neka postoje surjekcije $f : S \to T$, $g : T \to S$. Dokažite da su f i g injekcije i $|S| = |T|$.

14. Neka su skupovi $S, T \neq \emptyset$ takvi da je skup T^S svih funkcija sa S u T konačan. Dokažite da je tada i T konačan skup. Uz koji dodatni uvjet možemo tada tvrditi da je i S konačan?

15. Za bilo koje skupove X, Y oznaka $\operatorname{card} X \leq \operatorname{card} Y$ znači da postoji injekcija $X \to Y$. a) Dokažite da je $\operatorname{card} Y \leq \operatorname{card} X$ ako postoji surjekcija $f : X \to Y$; b) Dokažite da je relacija $\leq$ refleksivna i tranzitivna.

16. a) Dani su skupovi $X \subseteq Y \subseteq Z$. Dokažite da $\operatorname{card} X = \operatorname{card} Z \Rightarrow \operatorname{card} Y = \operatorname{card} Z$. (Neka je $f : Z \to X$ bijekcija. Induktivno definiramo $f^n : Z \to Z$ sa $f^0(z) = z$, $f^n(z) = f(f^{n-1}(z))$, $z \in Z$. Tada definirajte $g : Z \to Y$ sa $g(z) = f(z)$ za $z \in \cup f^n(Z \setminus Y)$, $n = 0, 1, 2, \ldots$, $g(z) = z$, za preostale $z \in Z$ i provjerite da je g bijekcija);

b) Rabeći a) dokažite **Cantor**[3]**-Bernsteinov** teorem:

$$\operatorname{card} X \leq \operatorname{card} Y \,\&\, \operatorname{card} Y \leq \operatorname{card} X \Rightarrow \operatorname{card} X = \operatorname{card} Y.$$

17. Neka je S skup, a $\mathcal{P}(S)$ partitivni skup od S. Dokažite da postoji injekcija $S \to \mathcal{P}(S)$, ali ne postoji surjekcija sa S na $\mathcal{P}(S)$. (Kad bi postojala surjekcija $f : S \to \mathcal{P}(S)$, promotrite skup $A := \{x \in S | x \notin f(x)\} \subseteq S$.) Zaključite odatle da je $\operatorname{card} \mathcal{P}(S) > \operatorname{card} S$, pa odatle da nema "najvećeg" kardinalnog broja.

18. a) Pri proučavanju beskonačnih skupova često se koristi ovaj **aksiom izbora**: Za svaki skup $S \neq \emptyset$ postoji funkcija $f : \mathcal{P}(S) \setminus \{\emptyset\} \to S$, tako da je $f(A) \in A$ za sve A (f se zove **funkcija izbora**). Dokažite da su sljedeće izjave ekvivalentne. (i) Skup S je beskonačan, (ii) Postoji injekcija $\mathbb{N} \to S$, (iii) Postoji injekcija $S \to S$, koja nije surjekcija.

b) Dokažite da su sljedeće izjave ekvivalentne (1) Aksiom izbora, (2) **Zornova lema**. Neka je P parcijalno uređen skup. Ako svaki lanac u P ima gornju među, onda P ima barem jedan maksimalni element; (3) **Zermelov**[4] **teorem**. Svaki skup se može dobro urediti. (vidi npr. [233]).

19. Neka je $f : S \to T$ neka funkcija. Neka je $\rho = \{(x, y) \in S \times S | f(x) = f(y)\}$. Dokažite da je ρ relacija ekvivalencije na S. Neka je $q : S \to S/\rho$ kvocijentno preslikavanje. Dokažite nadalje da je $f = q \circ f'$, gdje je $f' : S/\rho \to f(S)$ bijekcija.

20. Neka je S skup od n elemenata, tj. $|S| = n$. Dokažite (matematičkom) indukcijom da je $|\mathcal{P}(S)| = |2^S| = 2^n$. (vidi i pogl. 2)

21. Dokažite indukcijom:

a) $1^4 + 2^4 + \cdots + n^4 = \frac{1}{5}n^5 + \frac{1}{2}n^4 + \frac{1}{3}n^3 - \frac{1}{30}n$;

b) $1^5 + 2^5 + \cdots + n^5 = \frac{1}{6}n^6 + \frac{1}{2}n^5 + \frac{5}{12}n^4 - \frac{1}{12}n^2$.

22. Dokažite indukcijom da za sve realne brojeve $x > -1$ vrijedi $(1+x)^n > 1+nx$, $n \in \mathbb{N}$. Općenitije, dokažite da za sve $0 < x_i < 1$ vrijedi $(1 - x_1)(1 - x_2) \cdot \cdots \cdot (1 - x_n) \geq 1 - (x_1 + x_2 + \cdots + x_n)$.

23. Dokažite indukcijom

a) $\frac{1}{1\cdot 2} + \frac{1}{2\cdot 3} + \cdots + \frac{1}{n\cdot(n+1)} = \frac{n}{n+1}$; b) $\frac{1}{2} + \frac{2}{2^2} + \frac{3}{2^3} + \cdots + \frac{n}{2^n} = 2 - \frac{n+2}{2^n}$.

24. Dokažite da vrijede ove nejednakosti za pozitivne brojeve $x, y, z, x_1, x_2, \ldots, x_n$. Ispitajte kada vrijede jednakosti:

a) $\frac{x}{y} + \frac{y}{x} \geq 2$; b) $x^3 + y^3 + z^3 \geq 3xyz$; c) $(x + y + z)\left(\frac{1}{x} + \frac{1}{y} + \frac{1}{z}\right) \geq 9$;

d) $(1 + x_1)(1 + x_2) \cdot \cdots \cdot (1 + x_n) \geq 2^n$ ako je $x_1 + x_2 + \cdots + x_2 = 1$;

e) $\frac{x^p}{p} + \frac{y^q}{q} \geq xy$, gdje su p, q racionalni brojevi i $\frac{1}{p} + \frac{1}{q} = 1$;

f) $\left(\frac{p+q}{2}\right)^{p+q} \geq p^q q^p$ za $p, q \in \mathbb{N}$; g) $\frac{x_1}{x_2} + \frac{x_2}{x_3} + \frac{x_3}{x_4} + \cdots + \frac{x_{n-1}}{x_n} + \frac{x_n}{x_1} \geq n$;

h) $\left(\sum_{i=1}^n x_i\right)\left(\sum_{i=1}^n \frac{1}{x_i}\right) \geq n^2$; i) $\sum_{1\leq i<j\leq n} x_i x_j \leq \frac{n-1}{2n}\left(\sum_{i=1}^n x_i\right)^2$;

j) $\log\left(\frac{1}{n}\sum_{i=1}^n x_i\right) \geq \frac{1}{n}\sum_{i=1}^n \log x_i$; k) $\sum_{k=1}^n \frac{1}{\sqrt{k}} \geq \sqrt{n}$;

l) $(1 \cdot 2 \cdot 3 \cdot \cdots \cdot n)^2 < \left[\frac{(n+1)(2n+1)}{6}\right]^n$.

[3]Georg Cantor (1845 – 1918), njemački matematičar; osnivač teorije skupova.
[4]Ernst Zermelo (1871 – 1953), njemački matematičar

25. Ponderirana aritmetička, geometrijska i harmonijska sredina podataka (brojeva) $x_1, x_2, \ldots, x_n > 0$ s pripadnim kratnostima redom $f_1, f_2, \ldots, f_n \in \mathbb{N}$ definiraju se ovako:

$$A(x,f) = \frac{1}{f}\sum_{i=1}^{n} x_i f_i, \quad G(x,f) = \left(\prod_{i=1}^{n} x_i^{f_i}\right)^{1/f}, \quad H(x,f) = f\left(\sum_{i=1}^{n} \frac{f_i}{x_i}\right)^{-1},$$

gdje je $f = \sum_{i=1}^{n} f_i$. Dokažite da je $H(x,f) \le G(x,f) \le A(x,f)$.

26. Za $r \in \mathbb{N}$ i $x_1, x_2, \ldots, x_n > 0$ definira se r-ta **težinska sredina** $S_r := \left(\frac{1}{n}\sum_{i=1}^{n} x_i^r\right)^{1/r}$. Dokažite da težinske sredine monotono rastu, tj. $p \le q \Rightarrow S_p(x) \le S_q(x)$. Jednakost vrijedi ako i samo ako je $x_1 = x_2 = \cdots = x_n$. Dokažite nadalje ovu **Čebiševljevu nejednakost**. Za $0 < x_1 \le x_2 \le \cdots \le x_n$ i $0 < y_1 \le y_2 \le \cdots \le y_n$ vrijedi $S_r(x)S_r(y) \le S_r(xy)$ gdje je $xy = (x_1y_1, \ldots, x_ny_n)$. Što se dobiva za $r = 1$? (Težinske sredine S_r se mogu definirati i za svako $r \in \mathbb{R}$, pa i za $r = \pm\infty$; tako je npr. S_1 aritmetička sredina, S_0 (tj. $\lim_{r\to 0} S_r$) geometrijska, a S_{-1} harmonijska, dok je $S_{-\infty}$ minimum, a S_∞ maksimum brojeva $x_1, \ldots, x_n$).

27. Dokažite **Lagrangeov identitet** $(\sum a_k b_k)^2 = (\sum a_k^2)(\sum b_k^2) - \sum (a_k b_j - a_j b_k)^2$. Odatle izvedite **nejednakost Cauchy-Schwartza** $|\sum a_k b_k| \le (\sum a_k^2)^{1/2} \cdot (\sum b_k^2)^{1/2}$, gdje se sumira po j, k od 1 do n, te $j < k$.

28. Dokažite da za brojeve $a_i, b_j \in \mathbb{R}$, $i, j = 1 \ldots n$ vrijedi identitet

$$\left(\sum_{k=1}^{n} a_k\right)\left(\sum_{k=1}^{n} b_k\right) = n\sum_{k=1}^{n} a_k b_k - \sum_{1\le i<j\le n} (a_j - a_i)(b_j - b_i).$$

Odatle izvedite (još jedanput) **Čebiševljeve nejednakosti**:

$$\left(\sum_{k=1}^{n} a_k\right)\left(\sum_{k=1}^{n} b_k\right) \le n\sum_{k=1}^{n} a_k b_k, \quad \text{ako je } a_1 \le \ldots \le a_n \text{ i } b_1 \le \ldots \le b_n$$

$$\left(\sum_{k=1}^{n} a_k\right)\left(\sum_{k=1}^{n} b_k\right) \ge n\sum_{k=1}^{n} a_k b_k, \quad \text{ako je } a_1 \le \ldots \le a_n \text{ i } b_1 \ge \ldots \ge b_n.$$

(Ustvari, ako je $a_1 \le \cdots \le a_n$, a π neka permutacija od $\{1, \ldots, n\}$ (vidi pogl. II), onda je suma $\sum_{k=1}^{n} a_k b_{\pi(k)}$ najveća ako je $b_{\pi(1)} \le \cdots \le b_{\pi(n)}$, a najmanja ako je $b_{\pi(1)} \ge \cdots \ge b_{\pi(n)}$. Čebišev je tu nejednakost dokazao i za integrale umjesto suma:

$$\int_a^b f(x)dx \cdot \int_a^b g(x)dx \le (b-a)\int_a^b f(x)g(x)dx,$$

ako su f i g monotono rastuće funkcije.)

29. a) Napišite algoritam za rješavanje već spomenutog zadatka o čovjeku, vuku, kozi i zelju. Napišite program za rješenje tog zadatka u programskom jeziku prema izboru.

b) Isti zadatak kao a) za već spomenuti zadatak o tri ljubomorne supruge

c) Isti zadatak ako a) za već spomenuti zadatak o prelijevanju vina.

30. Napišite algoritam za nalaženje svih trojki $(x, y, z) \in \mathbb{N}_0^3$, takvih da je $x^2 + y^2 = z^2, z \le 100$.

31. Magični kvadrat $n \times n$, n neparan može se ovako konstruirati. Počinjemo s 1 u gornjem srednjem polju. Tada idemo gore–lijevo i upisujemo brojeve redom u rastućem poretku u prazna polja. Ako ispadnemo iz našeg kvadrata, zamišljamo da je to isto polje u popločavanju čitave ravnine i nastavimo. Ako je neko polje već popunjeno, spuštamo se dolje i nastavljamo. Napišite algoritam i program za tu konstrukciju.

32. Neka je $S = \{a_1, a_2, \ldots, a_n\}$ n–člani skup čiji elementi su u danom čvrstom poretku, a $\rho \subseteq S \times S$ binarna relacija na S. **Matrica relacije** ρ je $(n \times n)$–matrica $M := M(\rho) = [m_{ij}]$, gdje je $m_{ij} = 1$ ako je $(a_i, a_j) \in \rho$, $m_{ij} = 0$ inače. Za realne $(n \times n)$ matrice $A = [a_{ij}]$, $B = [b_{ij}]$, $A \le B$ znači $a_{ij} \le b_{ij}$ za sve i, j. I_n označava jediničnu $n \times n$ matricu, a $A^T = [a_{ij}^*]$ **transponiranu matricu** od A, tj. $a_{ij}^* = a_{ji}$. Dokažite sljedeće tvrdnje:

a) ρ je refleksivna $\iff I_n \le M$;

b) ρ je simetrična $\iff M = M^T$;

c) ρ je tranzitivna $\iff M \cdot M = M^2 \le M$;

d) ρ je antisimetrična $\iff M \times M^T \le I_n$ (ovo množenje $\times$ matrica je "član po član").

33. Na temelju prethodnog zadatka napišite algoritam i program (u programskom jeziku prema izboru) za prepoznavanje relacije ekvivalencije na konačnom skupu. Kolika je složenost tog algoritma?

§ 4. Dirichletov princip

Dirichletov princip ili poučak jedan je od najjednostavnijih elementarnih kombinatornih principa. U literaturi je još poznat pod raznim imenima: "princip pretinaca", "princip kutija" ili "princip golubinjaka" (od engl. "pigenhole principle") itd., ali mi ćemo ga zvati Dirichletov princip, prema njemačkom matematičaru G. Lejeune - Dirichletu (1805 – 1859), koji ga je prvi jasno formulirao i često se njime koristio pri svojim istraživanjima u teoriji brojeva i analizi. Slikovito rečeno, taj princip kaže da ako vrlo mnogo golubova doleti u nekoliko golubinjaka, onda će bar u jednom golubinjaku biti bar dva goluba. Malo preciznije, Dirichletov princip možemo ovako formulirati:

Dirichletov princip. *Ako $n+1$ predmeta bilo kako rasporedimo u n kutija (pretinaca), onda bar jedna kutija sadrži bar dva predmeta.*

Dokaz je gotovo nepotreban, a ide kontradikcijom. Pretpostavimo da svaka kutija sadrži najviše jedan predmet. Tada bi i predmeta najviše bilo n, a imamo ih $n+1$, pa je to kontradikcija.

Primijetimo da nam Dirichletov princip daje samo egzistenciju kutije s bar dva predmeta, a ne daje efektivni algoritam kako je naći.

Formalno:

Dirichletov princip. *Neka su S i T konačni skupovi, takvi da je $|S| > |T|$, a $f : S \to T$ neko preslikavanje. Tada f nije injekcija, tj. postoje $x, x' \in S$, $x \ne x'$, tako da je $f(x) = f(x')$.*

Još jedna (ekvivalentna) formulacija Dirichletovog principa je ova.

PROPOZICIJA 1. *Neka su S i T konačni skupovi sa $|S| = |T| = n$, a $f : S \to T$ neko preslikavanje. Tada je*

$$f \text{ injekcija} \iff f \text{ surjekcija}.$$

Dokaz. $\Rightarrow$: Ako je f injekcija, onda je očito $|S| = |f(S)|$. Prema pretpostavci je $|S| = |T|$, a kako je $f(S) \subseteq T$, te zbog $|f(S)| = |T|$ slijedi da je $f(S) = T$, jer je T konačan skup. Dakle, f je surjekcija.

$\Leftarrow$: Za svako preslikavanje $g : X \to Y$ među konačnim skupovima je očito $|g(X)| \leq |X|$. Neka su $x, x' \in S$, $x \neq x'$. Pretpostavimo da je $f(x) = f(x')$. Promotrimo restrikciju $f' : S \setminus \{x\} \to T$ od f, tj. $f' = f|_{S\setminus\{x\}}$. Očito je tada i f' surjekcija, pa je zbog gornje napomene tada $n = |f'(S \setminus \{x\})| \leq |S \setminus \{x\}| = n - 1$, što je nemoguće. □

Evo nekih jednostavnih primjera.

Primjer 11. Među 13 ljudi uvijek postoje dvoje rođenih u istom mjesecu.

Rješenje. Ako se skup S sastoji od 13 ljudi, a skup T od 12 mjeseci u godini, a $f : S \to T$, svakom članu od S pridružuje mjesec rođenja, onda f nije injekcija, pa postoje dva različita člana od S čije su vrijednosti po f jednake, tj. postoji dvoje ljudi rođenih u istom mjesecu. □

Primjer 12. Pet različitih pari rukavica nalazi se u jednom pretincu. Izvlačimo nasumce po jednu rukavicu i ne vraćamo ih natrag u pretinac. Koliko je najmanje izvlačenja potrebno da bismo bili sigurni da imamo obje rukavice istog para?

Rješenje. Ovdje je S = skup svih rukavica koje smo izvukli, T = skup svih parova rukavica, $f : S \to T$ pridružuje izvučenoj rukavici njezin par. Kako mora biti $|S| > |T| = 5$, to je najmanji takav broj $|S| = 6$. □

Primjer 13. Hrvatska ima 4,7 milijuna stanovnika. Čovjek ima najviše 300000 vlasi na glavi. Dokažite da postoje barem 16 ljudi u Hrvatskoj s "na dlaku" jednakim brojem vlasi na glavi.

Rješenje. Podijelimo sve stanovnike Hrvatske "u pretince" obzirom na broj vlasi na glavi, tj. na one koji imaju $0, 1, 2, 3, \ldots, 300\,000$ vlasi na glavi. Kad bi u svakom pretincu bilo ≤ 15 ljudi, bilo bi u Hrvatskoj $\leq 15 \cdot 300\,001 = 4\,500\,015$ stanovnika. □

Primjer 14. Neka su $a_1, a_2, \ldots, a_m$ cijeli brojevi. Tada postoje $k, l \in \{1, 2, \ldots, m\}$, $k < l$, tako da je $a_{k+1} + a_{k+2} + \cdots + a_l$ djeljivo s m. Drugim riječima, postoji nekoliko uzastopnih članova u nizu $a_1, a_2, \ldots, a_m$ čija je suma djeljiva s m.

Rješenje. Promatrajmo m suma: $a_1, a_1 + a_2, a_1 + a_2 + a_3, \ldots, a_1 + \cdots + a_m$. Ako je neka od tih suma djeljiva s m, onda smo gotovi. Stoga pretpostavimo da svaka od tih suma ima ne-nul-ostatak pri djeljenju s m. Ti ostaci su $1, 2, \ldots, m-1$. Kako imamo m suma, a $m-1$ ostataka, tada prema Dirichletovom principu postoje dvije sume $a_1 + a_2 + \cdots + a_k$ i $a_1 + a_2 + \cdots + a_l$ koje imaju isti ostatak r pri dijeljenju s m: $a_1 + \cdots + a_k = bm + r$, $a_1 + \cdots + a_l = cm + r$, pa odatle slijedi $a_{k+1} + \cdots + a_l = (c - b)m$, tj. $a_{k+1} + \cdots + a_l$ je djeljivo s m. □

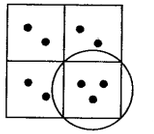
Primjer 15 (P. Erdös). Iz skupa $[2n] = \{1, 2, 3, \ldots, 2n\}$ odabran je podskup S od $n+1$ elemenata. Tada postoje $x, y \in S$, tako da je x djeljiv s y (tj. $y|x$).

Rješenje. Svaki prirodni broj može se napisati na jedinstven način kao $2^k \cdot a$, gdje je $k \geq 0$, a neparan, tj. izlučimo sve faktore 2 tog broja. Za brojeve između 1 i $2n$ vrijednosti od a su među n brojeva $1, 3, 5, \ldots, 2n-1$. Stoga u S koji ima $n+1$ elemenata postoje dva broja čiji su pripadni a jednaki. Neka su to brojevi $2^r a$ i $2^s a$. Ako je $r \leq s$, onda je $y = 2^r a | 2^s a = x$, a ako $r > s$, onda $y = 2^s a | 2^r a = x$. Primijetimo da je to najbolji mogući rezultat u tom smislu da tvrdnja više ne vrijedi ako makar malo oslabimo uvjete. Npr. ako je $|S| = n$ umjesto $|S| = n+1$, tvrdnja više ne vrijedi, tj. nijedan od njih ne mora dijeliti drugi broj iz S (promotrite $S = \{n+1, n+2, \ldots, 2n\}$). □

Primjer 16. U svakom konveksnom poliedru uvijek postoje dvije strane (plohe) s jednakim brojem bridova.

Rješenje. Uočimo stranu s najviše bridova. Neka je to n-terokut P. Zbog konveksnosti poliedra, nikoja dva brida iz P ne mogu istodobno biti bridovi i neke druge strane poliedra (Zašto?). Stoga poliedar osim P ima barem još n strana. Te strane mogu imati $3, 4, 5, \ldots, n$ bridova. Prema Dirichletovom principu, postoje stoga bar dvije strane s istim brojem bridova. □

Primjer 17. Unutar kvadrata stranice 1 dano je 9 točaka. Tada postoje 3 točke od danih 9 točaka koje su sadržane u krugu radijusa $2/5$.



Rješenje. Podijelimo kvadrat u četiri kvadratića kao na slici. "Najgori" raspored koji može imati 8 točaka jest da su u svakom kvadratiću dvije točke. Tada je prema Dirichletovom principu deveta točka u nekom od tih kvadratića, npr. u donjem desnom. Opišimo mu krug. Njegov radijus je

$$\frac{1}{2}\sqrt{\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2} = \frac{\sqrt{2}}{4} = \frac{1.4142\ldots}{4} < \frac{1.44}{4} = 0.36 = \frac{36}{100} = \frac{9}{25} < \frac{10}{25} = \frac{2}{5},$$

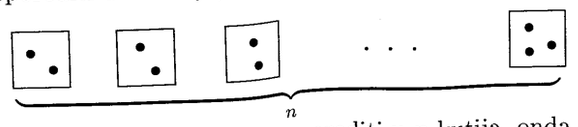
pa su u tom krugu 3 točke od danih 9. □

Primjer 18. Pripremajući se za svjetsko nogometno prvenstvo, nogometna je reprezentacija imala 11 tjedana pripreme. Stručni je štab odlučio da reprezentacija igra svaki dan bar jednu probnu utakmicu. No kako se igrači ne bi premorili, odlučeno je da se u svakom tjednu (= 7 dana) odigra najviše 12 probnih utakmica. Dokažite da će na tim pripremama reprezentacija odigrati u nekoliko uzastopnih dana točno 21 utakmicu.

Rješenje. Neka je a_1 = broj utakmica odigranih prvog dana priprema, a_2 = broj utakmica odigranih prvog i drugog dana priprema, a_3 = broj utakmica odigranih prvog, drugog i trećeg dana priprema itd. Niz $a_1, a_2, \ldots, a_{77}$ strogo raste jer je svakog dana odigrana bar jedna utakmica, tj . $a_1 < a_2 < \cdots < a_{77}$. Dalje, $a_1 \geq 1$, a kako je najviše 12 utakmica odigrano tijekom svakog tjedna, to je $a_{77} \leq 12 \cdot 11 = 132$. Niz $a_1 + 21, a_2 + 21, \ldots, a_{77} + 21$

je onda također strogo rastući i $a_{77}+21 \leq 132+21 = 153$. Prema tome, svaki od 154 broja $a_1, a_2, \ldots, a_{77}, a_1+21, a_2+21, \ldots, a_{77}+21$ je cijeli broj između 1 i 153. Prema Dirichletovom principu, postoje među njima dva koja su jednaka. Među prvih 77 nema jednakih, a isto tako ni među posljednih 77. Stoga postoje k, l, npr. $k < l$, tako da je $a_l = a_k + 21$. Dakle, u danima $k+1, k+2, \ldots, l$ reprezentacija će odigrati točno 21 utakmicu. □

Sada ćemo malo poopćiti Dirichletov princip. Primijetimo da ako $2n+1$ predmeta treba rasporediti u n kutija, tada će (bar) jedna kutija imati bar 3 predmeta:



Dalje, ako $3n+1$ predmeta treba rasporediti u n kutija, onda će u (bar) jednoj kutiji biti bar 4 predmeta itd. Općenito, ako je $n(r-1)+1$ predmeta razmješteno u n kutija, tada će bar u jednoj kutiji biti barem r predmeta. Drukčije rečeno, vrijedi

Dirichletov princip - jaka forma. *Ako je m predmeta razmješteno u n kutija, onda bar jedna kutija sadrži $\left\lfloor \frac{m-1}{n} \right\rfloor + 1$ predmet.*

Zaista, najveći multipl od n, manji od m nađe se tako da se multiplicira n s $1, 2, 3 \ldots$, sve dok se ne dođe do $m-1$, a ostatak se odbaci. Taj je jednak $\left\lfloor \frac{m-1}{n} \right\rfloor$. Kad bi bilo točno $n \cdot \left\lfloor \frac{m-1}{n} \right\rfloor \leq m-1 < m$ predmeta, stavili bismo $\left\lfloor \frac{m-1}{n} \right\rfloor$ njih u svaku kutiju, ali kako imamo m predmeta, moramo imati više od toga bar u jednoj kutiji.

Evo odgovarajućega matematičkog opisa:

PROPOZICIJA 2. *Neka su S i T konačni skupovi, $|S| = m$, $|T| = n$, a $f : S \to T$. Tada postoji $y \in T$, tako da je*

$$|f^{-1}(y)| \geq \left\lfloor \frac{m-1}{n} \right\rfloor + 1.$$

Primjer 19. Među 44 ljudi bar je četvero rođeno u istom mjesecu.

Rješenje. Prema gornjem je barem $\left\lfloor \frac{44-1}{12} \right\rfloor + 1 = \lfloor 3.583 \rfloor + 1 = 4$ rođeno u istom mjesecu. □

Sada još malo poopćimo Dirichletov princip.

Opći Dirichletov princip. *Neka je $n \in \mathbb{N}$ i $r_1, r_2, \ldots, r_n \in \mathbb{N}$. Ako je $r_1 + r_2 + \cdots + r_n - n + 1$ predmeta razmješteno u n kutija $K_1, K_2, \ldots, K_n$, onda bar jedna kutija K_i sadrži $\geq r_i$ predmeta, tj. ili K_1 sadrži $\geq r_1$ predmeta ili K_2 sadrži $\geq r_2$ predmeta,..., ili K_n sadrži $\geq r_n$ predmeta.*

Dokazujemo opet kontradikcijom. Kad bi svaka kutija K_i sadržavala $< r_i$ predmeta, onda bi ukupan broj predmeta bio $\leq (r_1 - 1) + (r_2 - 1) + \cdots + (r_n - 1) = r_1 + \cdots + r_n - n$, što ne može biti.

Napomenimo da je $r_1 + r_2 + \cdots + r_n - n$ predmeta moguće rasporediti u n kutija, tako da svaka K_i sadrži $< r_i$ predmeta: $r_1 - 1$ u K_1, $r_2 - 1$ u K_2,..., $r_n - 1$ u K_n. Nadalje, primijetimo da za $r_1 = r_2 = \cdots = r_n = r$ dobivamo jaku formu

Dirichletova principa, a ako je k tome još i $r = 2$, dobivamo obični Dirichletov princip.

Primjer 20. Neka je n^2+1 vojnika poredano u vrstu. Tada je uvijek moguće odabrati $n+1$ njih u nizu, tako da idući slijeva na desno, njihove visine ili rastu ili padaju.

Ovo je samo jedna zgodna formulacija sljedeće činjenice.

(P. Erdös, G. Szekeres, 1935): Neka je $a_1, a_2, \ldots, a_{n^2+1}$ niz od n^2+1 realnih brojeva. Tada u tom nizu postoji rastući ili padajući podniz duljine $n+1$.

Naprimjer, za $n = 2$ promatrajmo niz duljine pet $16, 7, 39, 4, 25$. U ovom nizu imamo jedan tročlani padajući podniz: $16, 7, 4$.

Rješenje. Pretpostavimo da ne postoji $(n+1)$-člani rastući podniz našeg niza, pa dokažimo da postoji padajući niz duljine $n+1$. Za $k = 1, 2, 3, \ldots, n^2+1$ neka je p_k =duljina najvećeg rastućeg podniza našeg niza koji počinje s a_k. Zbog naše pretpostavke je $p_k \leq n$ za svako $k = 1, 2, \ldots, n^2+1$, a očito je $p_k \geq 1$ za svako k. Dakle, $p_1, p_2, \ldots, p_{n^2+1}$ je niz od n^2+1 prirodnih brojeva između 1 i n. Prema Dirichletovom principu (jake forme) za $r-1 = n$, tj. $r = n+1$, slijedi da postoji bar $n+1$ od tih brojeva koji su jednaki, tj. postoje $k_1, \ldots, k_{n+1}$, $1 \leq k_1 < k_2 < \cdots < k_{n+1} \leq n^2+1$, tako da je $p_{k_1} = p_{k_2} = \cdots = p_{k_{n+1}}$. Pretpostavimo da je za neko $i \in \{1, 2, \ldots, n\}$, $a_{k_i} < a_{k_{i+1}}$. Tada zbog $k_i < k_{i+1}$ možemo uzeti najveći rastući podniz koji počinje s $a_{k_{i+1}}$ i staviti a_{k_i} na početak. Tako dobijemo rastući podniz koji počinje s a_{k_i}. No zbog definicije brojeva p_k, to povlači da je $p_{k_i} > p_{k_{i+1}}$, što je nemoguće. Stoga zaključujemo da je $a_{k_i} \geq a_{k_{i+1}}$ za svako $i = 1, 2, \ldots, n$. Dakle, $a_{k_1} \geq a_{k_2} \geq \cdots \geq a_{k_{n+1}}$, pa $a_{k_1}, a_{k_2}, \ldots, a_{k_{n+1}}$ tvore padajući podniz duljine $n+1$. Posve analogno zaključujemo u preostalom slučaju. Time je ta činjenica dokazana.

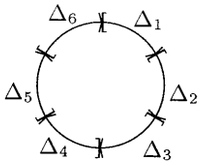
Napomenimo da je ovo najbolji mogući rezultat u smislu da rezultat više ne vrijedi ako umjesto n^2+1 brojeva promatramo samo n^2 brojeva. Npr. za $n = 3$, u 9-članom nizu $3, 2, 1, 8, 9, 5, 7, 4, 6$ najdulji rastući ili padajući podnizovi imaju duljinu 3. No ako bilo gdje ubacimo, recimo, broj 10, dobit ćemo ili rastući ili padajući podniz duljine 4. Nadalje, isti dokaz daje da tvrdnja vrijedi za $mn+1$ $(m \geq n)$ umjesto n^2+1 brojeva. □

Na kraju, evo još jedne primjene Dirichletova principa u matematičkoj analizi.

Primjer 21. Neka je $\alpha \in \mathbb{R}$, $\frac{\alpha}{2\pi} \in \mathbb{R} \setminus \mathbb{Q}$, $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ jedinična kružnica u kompleksnoj ravnini, a $f : S^1 \to S^1$ rotacija (npr. u pozitivnom smjeru) za kut α, $z \in S^1$. Tada je skup $P = \{f^n(z) \mid n \in \mathbb{N}_0\}$ gust na S^1. Pritom je $f^0(z) = z, f^1(z) = f(z), f^2(z) = f(f(z)), f^3(z) = f(f(f(z))), \ldots$ i općenito $f^{n+1}(z) = f(f^n(z))$.

Rješenje. Da je skup $P \subseteq S^1$ **gust** na S^1 znači da u svakom otvorenom luku lučne duljine $\varepsilon > 0$ postoji točka iz P. Opisno govoreći, taj teorem kaže da rotiramo li neku točku (u pozitivnom smjeru) za kutove $\alpha, 2\alpha, 3\alpha, \ldots$, onda se ovako dobivene točke nalaze "gotovo svuda" na kružnici, tj. u svakom netrivijalnom luku. Očito da to neće biti tako ako je kut α sumjerljiv s 2π, tj. $\frac{\alpha}{2\pi} \in \mathbb{Q}$. Npr. ako je $\alpha = \frac{\pi}{2}$, a $z = 1$, onda je skup $\{f^n(z) \mid n \in \mathbb{N}_0\} = \{1, i, -1, -i\}$.

Podijelimo kružnicu S^1 na n jednakih poluintervala $\Delta_1, \Delta_2, \ldots, \Delta_n$ lučne duljine $2\pi/n$.

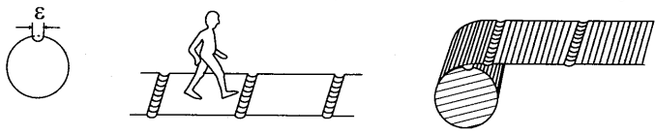


Promatrajmo skup točaka $\{z, f(z), \ldots, f^n(z)\}$. Tu se zaista radi o $n+1$ različitih točaka, jer ako je npr. $f^k(z) = f^l(z)$, $0 \le k < l \le n$, onda, budući da je rotacija f očito bijekcija, slijedi da je $f^{l-k}(z) = z$. Svaku točku na S^1 možemo napisati u obliku $e^{i\varphi} = \cos\varphi + i\sin\varphi$. Stoga je $f^{l-k}(z) = e^{i(\varphi+(l-k)\alpha)}$, pa postoji $r \in \mathbb{N}$, takav da je $\varphi + 2r\pi = \varphi + (l-k)\alpha$, pa je $\frac{\alpha}{2\pi} \in \mathbb{Q}$, što je suprotno pretpostavci. Dakle, točke $z, f(z), \ldots, f^n(z)$ su sve različite, pa prema Dirichletovom principu postoje dvije od njih u jednom te istom podintervalu Δ_k. Neka su to $f^i(z)$, $f^j(z)$, $j > i$. Neka je $d = j - i \in \mathbb{N}$. Kut $d\alpha$ je lučna udaljenost između $f^i(z)$, $f^j(z)$, pa je $d\alpha < \frac{2\pi}{n}$. U nizu točaka $z, f^d(z), f^{2d}(z), f^{3d}(z), \ldots$ svake dvije su jednako udaljene, i to u lučnoj mjeri za $d\alpha < \frac{2\pi}{n}$. Neka je sada $\varepsilon > 0$ i neka je n odabran tako da je $\frac{2\pi}{n} < \varepsilon$. Ako sada uzmemo ε-okolinu bilo koje točke na S^1 (tj. otvoreni luk sa središtem u toj točki i lučne duljine ε), onda postoji točka $f^{sd}(z)$ koja je u toj okolini. To znači da je skup P gust na S^1. □

Ovaj primjer možemo i ovako protumačiti: ako u svakom kvadratiću beskonačnog kvadratičnog polja sjedi jedan zec, i to tako da je svaki smješten u istu točku kvadratića, pa ako lovac koji je u ishodištu nacilja u smjeru čiji je tangens kuta s obzirom na koordinatne osi iracionalan, onda će lovac pogoditi bar jednog zeca. To drugim riječima znači da će pravac s jednadžbom $y = \omega x$ u xy-ravnini, $\omega \in \mathbb{R} \setminus \mathbb{Q}$ proći po volji blizu nekim cjelobrojnim točkama, odnosno namotat će se na torus svuda gusto (tj. u svakoj okolini svake točke torusa bit će točka namotanog pravca). **Torus** je kvocijentni skup $\mathbb{R}^2/\sim$, gdje je $(x,y) \sim (x',y') \iff x - x' \in \mathbb{Z}$ i $y - y' \in \mathbb{Z}$. Torus je (topološki) ekvivalentan sa $S^1 \times S^1$. Ova činjenica ima važnih reperkusija u diferencijalnim jednadžbama i u teoriji ergodičnosti. (v. [228]).

Primjer 22. Čovjek korača cestom koracima dugim 1 m. Na pravilnim razmacima od $\sqrt{2}$m iskopani su na cesti poprečni uski kanalići. Dokažite da će čovjek kad-tad stupiti na neki od kanalića (pritom možemo zanemariti ili duljinu čovjekova stopala ili širinu kanalića, ali ne oboje).

Rješenje. Zamislimo da smo cestu "namotali" na valjak čiji je opseg baze $\sqrt{2}$ m. Tada svi kanalići na valjku padnu na isto mjesto na valjku, tj. u projekciji na kružnici. Stoga svi ti kanalići (gledano u projekciji) "padnu" na jedan mali luk kružnice duljine ε (v. sliku).



Koračanje čovjeka po cesti odgovara (pri namotavanju) rotaciji neke točke po kružnici za kut (tj. luk od) 1 m, 2 m, 3 m,... u pozitivnom smjeru. Kako je $1/\sqrt{2}$ iracionalan broj, onda iz Primjera 21. slijedi da će neke od zarotiranih točaka upasti u ε-luk, što onda znači da će čovjek stupiti na neki od kanalića. □

Primjer 23. Dokažite da postoji potencija broja 2, koja u dekadskom zapisu počinje s 5 devetki: $2^n = 99999\ldots$.

Rješenje. Traže se $k, n \in \mathbb{N}$, tako da je $99999 \cdot 10^k \le 2^n < 10^{k+5} \iff k + \log 99999 \le n \cdot \log 2 < k+5$. U smislu prethodnog primjera, ovdje je "duljina koraka" $\log 2$, a udaljenost među "susjednim kanalićima" (kojima je širina $5 - \log 99999$) jednaka je 1. Tvrdnja sada izlazi kao u prethodnom primjeru, jer je $\log 2$ iracionalan broj. □

Primjer 24. Neka je $\alpha \in \mathbb{R}$ i $n \in \mathbb{N}$. Tada postoje $x, y \in \mathbb{Z}$, tako da je

$$|x - \alpha y| < \frac{1}{n},\ 1 \le y \le n.$$

Rješenje. Promatrajmo brojeve $u - \alpha v$ gdje je $v = 0, 1, \ldots, n$, $u = \lfloor \alpha v \rfloor + 1$. Tada je $0 < u - \alpha v \le 1$. (Ako je $\alpha \in \mathbb{R} \setminus \mathbb{Q}$, onda će $n+1$ brojeva $u - \alpha v$ biti svi različiti.) Barem jedan od intervala $\langle \frac{i}{n}, \frac{i+1}{n}]$, $i = 0, 1, \ldots, n-1$ sadrži tada bar dva od tih $n+1$ brojeva (prema Dirichletovom principu), tj. $\exists v_1, v_2$, $0 \le v_1 < v_2 \le n$ i u_1, u_2, tako da je $\frac{i}{n} < u_1 - \alpha v_1 \le \frac{i+1}{n}$, $\frac{i}{n} < u_2 - \alpha v_2 \le \frac{i+1}{n}$. Oduzimanjem slijedi

$$-\frac{1}{n} < (u_2 - u_1) - \alpha(v_2 - v_1) < \frac{1}{n}$$

$\Rightarrow |(u_2 - u_1) - \alpha(v_2 - v_1)| < \frac{1}{n}$. Tada je $y = v_2 - v_1$, $x = u_2 - u_1$. Očito je $0 < y \le n$. □

Dirichletov princip se može poopćiti do neslućenih razmjera. Prvi je to uočio Ramsey[5] pa se po njemu i osnovni teorem koji je dokazao zove **Ramseyev teorem**, a cijela teorija koja se time bavi **Ramseyeva teorija**. Taj teorem se neformalno može izreći ovako.

Ramseyev teorem. *Za svako $r, m \in \mathbb{N}$ i sve prirodne brojeve $r_1, r_2, \ldots, r_m \ge r$ postoji najmanji prirodni broj $N = R(r_1, r_2, \ldots, r_m; r)$ tako velik da ako imamo skup od $n \ge N$ elemenata i ako u tom (golemom) skupu razvrstamo sve r-podskupove u m klasa $K_1, K_2, \ldots, K_m$, onda postoji*

ili r_1 elemenata čiji su svi r-podskupovi u klasi K_1,
ili r_2 elemenata čiji su svi r-podskupovi u klasi K_2,
$\vdots$
ili r_m elemenata čiji su svi r-podskupovi u klasi K_m.
Broj $R(r_1, r_2, \ldots, r_m; r)$ zove se (opći) **Ramseyev broj**.

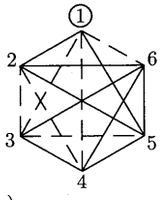
Na primjer, ako je $r = 1$, onda je $N = R(r_1, r_2, \ldots, r_m; 1)$ najmanji broj sa svojstvom da ako imamo npr. n kuglica, $n \ge N$, koje treba staviti u m kutija $K_1, \ldots, K_m$, onda je ili u kutiji K_1 barem r_1 kuglica, ili je u K_2 barem r_2 kuglica itd., ili je u kutiji K_m barem r_m kuglica. Prema općem Dirichletovom principu, taj broj je $N = R(r_1, \ldots, r_m; 1) = r_1 + r_2 + \cdots + r_m - m + 1$. Tako je, dakle, Dirichletov princip jedan sićušni poseban slučaj Ramseyeva teorema.

Mi se nećemo upuštati u dokaz Ramseyeva teorema, nego ćemo pokazati samo neke primjere koji će pokazati gdje i kako se on rabi. Osnovna ideja dokaza je zapravo vrlo jednostavna: indukcijom po r (za $r = 1$ to je opći Dirichletov princip), pa onda indukcijom po m (i po svim brojevima $r_1, \ldots, r_m \ge r$), dokažu se izvjesne nejednakosti koje induktivno osiguravaju egzistenciju Ramseyevih brojeva.

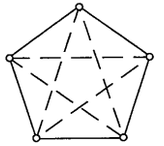
"Od troje običnih ljudi, dvoje moraju biti istog spola." Ova očita činjenica u neku ruku parafrazira Ramseyev teorem. Ovdje je broj 3 očito najmanji broj n sa svojstvom da ako imamo n ljudi i svrstamo ih u dvije "kutije" (muški i ženski), onda će u bar jednoj biti bar dvoje ljudi. To znači da je $R(3, 2; 2) = 3$. Jasno je i

[5] Frank P. Ramsey (1903–1930), engleski logičar i matematičar

$R(p,2;2) = p = R(2,p;2)$. Pokažimo sada da je $R(3,3;2) = 6$. Broj $R(3,3;2)$ je najmanji broj ljudi u nekom društvu, tako da među njima postoji ili trojka međusobnih znanaca ili trojka međusobnih neznanaca. Pokažimo prvo da je $R(3,3;2) \leq 6$. To znači da u svakom društvu od šestero ljudi uvijek postoji ili trojka znanaca ili trojka neznanaca. Najbolje je to ilustrirati crtežom, odnosno grafom. **Graf** se sastoji od **vrhova** (ili čvorova) i **bridova** – to su spojnice vrhova, a **podgraf** je dio grafa. **Potpun graf** K_n je graf s n vrhova u kojem su svaka dva vrha spojena jednim bridom (vidi iduću točku, a više o tome u poglavlju o grafovima). Sada označimo ljude brojevima $1, 2, \ldots, 6$ (uz ispriku) i promotrimo potpun graf K_6 s vrhovima $1, 2, \ldots, 6$. Obojimo svaki brid toga grafa K_6 ili plavom bojom (ili punom crtom) ili crvenom bojom (ili crtkano) i to tako da brid koji spaja dvoje poznanika obojimo plavo, a onaj koji spaja neznance crveno. Stoga mi tvrdimo da kako god obojili bridove od K_6 dvjema bojama, uvijek imamo jednobojni trokut, tj. podgraf K_3 u K_6 koji je ili plavi ili crveni. To se ovako može pokazati. Istaknimo jedan vrh (tj. jednog čovjeka iz tog društva), npr. 1. Ostalih 5 vrhova $\{2,3,4,5,6\}$ razvrstamo u dvije skupine C i P. U C su oni vrhovi koji su spojeni crvenom, a u P oni koji su spojeni plavim bridom s 1, dakle, $C \cup P = \{2,3,4,5,6\}$. Očito bar jedan od skupova C ili P ima ≥ 3 elementa (ustvari; bar jedan ima $\lfloor (5-1)/2 \rfloor + 1 = 3$ elementa po Dirichletovom principu). Na slici a) je $C = \{3,4,6\}$, $P = \{2,5\}$.



a)


b)

Ako je $|C| \geq 3$, onda među vrhovima od C ili imamo sve plave bridove (stoga i plavi trokut) ili među vrhovima od C imamo crveni brid. U potonjem slučaju krajevi tog brida i vrh 1 određuju crveni trokut. Na isti način zaključujemo ako je $|P| \geq 3$. Tako smo dokazali da je $R(3,3;2) \leq 6$. Međutim, slika b) pokazuje da je $R(3,3;2) > 5$, jer tu nema ni plavog ni crvenog trokuta.

Na sličan se način može pokazati da je $R(3,4;2) = R(4,3;2) = 9$, tj. da je $R(3,4;2) \leq 9$ i $R(3,4;2) > 8$.

Da je $R(3,4;2) \leq 9$ vidi se ovako. Ako bridove od K_9 opet obojimo crveno ili plavo i opet istaknemo vrh 1, onda ostalih 8 vrhova kao i prije razvrstamo u skupove C i P. Tada je ili $|C| \geq 4$ ili $|P| \geq 4$. Ako je $|P| \geq 4$, onda među vrhovima od P imamo ili same crvene bridove (pa smo gotovi) ili postoji plavi brid, a tada imamo plavi trokut određen krajevima tog brida i vrhom 1. Ako je $|P| \leq 3$, onda je $|C| \geq 5$. Ako je $|C| \geq 6$, onda zbog malo prije dokazanog da je $R(3,3;2) = 6$ slijedi da među vrhovima od C imamo jednobojni trokut K_3 i tada je jasno da je $R(3,4;2) = R(4,3;2) \leq 9$. Još preostaje slučaj $|C| = 5$ i $|P| = 3$. No tada se (s malo crtanja) lako vidi da je jedini nerazmatrani preostali slučaj taj da svaki od 9 vrhova spojimo s preostalima s po 3 plava brida i 5 crvenih. No tada bi ukupno imali $9 \cdot 3/2$ plavih i $9 \cdot 5/2$ crvenih bridova, što je očito nemoguće.

Da je $R(3,4;2) > 8$, uzmemo graf K_8 s vrhovima $0, 1, 2, 3, 4, 5, 6, 7$. Vrhove i, j spojimo crvenim bridom ako je $i-j \equiv 1, 4, 7 \pmod 8$, a plavim ako je $i-j \equiv 2, 3, 5, 6 \pmod 8$. U tom grafu nema crvenog podgrafa K_3 ni plavog podgrafa K_4 (nacrtajte sliku). Dakle, $R(3,4;2) = 9$.

Već i iz ovoga je vidljivo da je određivanje točnih vrijednosti Ramseyevih brojeva vrlo teško. Znaju se samo neke točne vrijednosti; npr. $R(3,5;2) = 14$, $R(4,4;2) = 18$, $R(3,6;2) = 18$, $R(3,7;2) = 23$, kao i neke gornje međe koje uglavnom slijede iz osnovne nejednakosti za $p, q \geq 2$:

$$R(p,q;2) \leq R(p-1,q;2) + R(p,q-1;2),$$

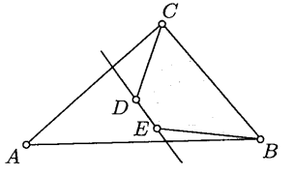
uz očitu činjenicu da je $R(p,2;2) = p$. Ova se nejednakost dokazuje slično kao što smo dokazali da je $R(3,3;2) \leq 6$ i $R(3,4;2) \leq 9$, a zapravo je polazna u dokazu samog Ramseyeva teorema.

Pokažimo na par primjera kako i gdje se sve koristi Ramseyev teorem. Prvo u geometriji.

Primjer 25 (Erdös-Szekereszov teorem). , 1935.] Za svako $m \geq 3$ postoji najmanji broj C_m tako da za $n \geq C_m$ vrijedi sljedeće: ako od n točaka u ravnini nijedna trojka nije kolinearna, onda među njima postoji m točaka koje su vrhovi konveksnog m-terokuta.

Rješenje. Prvo je jasno da je $C_3 = 3$, jer je svaki trokut konveksan. Drugo, dokažimo da je $C_4 = 5$. To znači da od 5 točaka u ravnini (bez kolinearnih trojki) uvijek postoje četiri koje su vrhovi konveksnog četverokuta.

Neka su te točke A, B, C, D, E. Ako je konveksna ljuska $\text{conv}\{A,B,C,D,E\}$ (konveksni) četverokut ili peterokut, tvrdnja je dokazana. Neka je ta konveksna ljuska trokut, npr. $\triangle ABC$. Tada su ostale dvije točke D, E unutar trokuta, a pravac DE siječe dvije stranice npr. $\overline{AB}$ i $\overline{AC}$ (pa ne siječe $\overline{BC}$ — Paschov aksiom) i četverokut $BCDE$ stoga je konveksan.



LEMA 1. *Ako među m točaka u ravnini bez kolinearnih trojki, svaka četvorka čini vrhove konveksnog četverokuta, onda sve te točke čine vrhove konveksnog m-terokuta.*

Dokaz Leme. Neka su to vrhovi $A_1, A_2, \ldots, A_m$. Možemo bez smanjenja općenitosti pretpostaviti da je konveksna ljuska $\text{conv}\{A_1, \ldots, A_m\}$ poligon $A_1A_2 \ldots A_s$. Treba dokazati da je $s = m$. Pretpostavimo da je $s < m$. Tada je vrh A_{s+1} u unutrašnjosti jednog od trokuta $A_1A_2A_3$, $A_1A_3A_4$, $\ldots$, $A_1A_{s-1}A_s$ jer nema kolinearnih trojki. Recimo da je u unutrašnjosti trokuta $A_1A_{i-1}A_i$. Tada točke A_1, A_{i-1}, A_i, A_{s+1} ne čine vrhove konveksnog četverokuta, suprotno pretpostavci. Dakle, $s = m$. Time je Lema dokazana. □

Sada dovršimo dokaz tvrdnje. Za $m \geq 4$, promotrimo Ramseyev broj $R(m, 5; 4)$ i neka je $n \geq R(m, 5; 4)$, a S skup od n točaka u ravnini bez kolinearnih trojki. Skup svih četvorki točaka iz S rastavimo u dvije klase K_1 i K_2. U K_1 neka su sve one četvorke koje čine vrhove konveksnog četverokuta, a u K_2 sve ostale četvorke. Prema Ramseyevu teoremu ili postoji m točaka iz S čije su sve četvorke u K_1 ili postoji pet točaka iz S čije su sve četvorke iz K_2. Ovo potonje znači da postoji pet točaka čije su sve četvorke nekonveksni četverokuti, što ne može biti jer smo pokazali da je $C_4 = 5$. Preostaje, dakle, prva mogućnost, a prema Lemi onda tih m točaka čini vrhove konveksnog m-terokuta. Time je dokaz gotov. Uočite da smo dokazali da je $C_m \leq R(m, 5; 4)$.

Točan broj C_m se ne zna, ali je slutnja da je $C_m = 2^{m-2} + 1$, što se pokazalo ispravnim za $m = 3, 4, 5, 6$. □

Primjer 26 (I. Schur[6]). Za svako $m \in \mathbb{N}$ postoji najmanji broj S_m, takav da ako je $n \geq S_m$ i skup $[n]$ particioniran u m blokova $B_1, \ldots, B_m$, onda postoji blok B_k i tri broja $x, y, z \in B_k$, tako da je $x + y = z$.

(Ako na B_k gledamo kao na točke obojene bojom k, onda ta tvrdnja pokazuje da jednadžba $x + y = z$ ima jednobojno (monokromatsko) rješenje.)

Rješenje. Promotrimo Ramseyev broj $R(3, 3, \ldots, 3; 2)$ s m trojki i neka je $n \geq R(3, 3, \ldots, 3; 2)$. Sve dvočlane podskupove od $[n]$ razvrstajmo u m klasa $K_1, K_2, \ldots, K_m$ ovako:

$$\{a, b\} \in K_i \iff |a - b| \in B_i,\ i = 1, 2, \ldots, m.$$

Prema Ramseyevu teoremu postoji podskup $T = \{x_1, x_2, x_3\} \subseteq [n]$ i indeks $k \in \{1, 2, \ldots, m\}$ tako da je $\{x_1, x_2\}, \{x_2, x_3\}, \{x_1, x_3\} \in K_k$. Uzmimo da je $x_1 < x_2 < x_3$. Tada su brojevi $x = x_2 - x_1$, $y = x_3 - x_2$, $z = x_3 - x_1$ svi u B_k i vrijedi $x + y = z$. Dokazali smo, dakle, da je $S_m \leq R(3, 3, \ldots, 3; 2)$, ali se ne zna koliki je S_m. □

Sljedeća tvrdnja (teorem) također je posljedica Ramseyeva teorema, ali je nećemo dokazivati, a također govori o jednobojnosti. Neka je skup $[n]$ obojen s r boja (tj. zadana je funkcija bojanja $\beta : [n] \to [r]$, tzv. r-**bojenje** od $[n]$).

Primjer 27 (van der Waerden[7], 1927). Za svako $k, r \in \mathbb{N}$ postoji najmanji broj $W(k, r) \in \mathbb{N}$, tako da za $n \geq W(k, r)$ i svako r-bojenje skupa $[n]$ postoji jednobojni aritmetički niz u $[n]$ duljine k.

Pokazuje se da je ova tvrdnja ekvivalentna s ovom:

Ako je skup $\mathbb{N}$ particioniran u dva bloka, onda jedan od njih sadrži po volji dugačak aritmetički niz.

U vezi s tim spomenimo i sljedeći čuveni teorem iz kombinatorne teorije brojeva kojom je odgovoreno na 40 godina staru slutnju Erdösa i Turana.

Szemerédijev teorem (1975). *Ako skup $A \subseteq \mathbb{N}$ ima asimptotski pozitivnu gornju gustoću (tj. $\limsup_{n\to\infty} \frac{|A \cap [n]|}{n} > 0$), onda A sadrži po volji dugačke konačne aritmetičke nizove.*

[6] Issai Schur (1875 – 1914), njemački matematičar

[7] Bartel L. van der Waerden (1903 – 1996), nizozemski matematičar

Unatoč ovom teoremu, još uvijek nije razriješena čuvena **Erdösova slutnja** (za čije je rješenje nudio 3 000 američkih dolara): Ako je $A \subseteq \mathbb{N}$ skup za koji je $\sum_{a \in A} 1/a = \infty$, onda A sadrži po volji dug aritmetički niz. Posebno se odgovor ne zna ako je $A = \mathbb{P}$ skup svih prostih brojeva.

Spomenimo na kraju da Ramseyev teorem ima i beskonačan analogon.

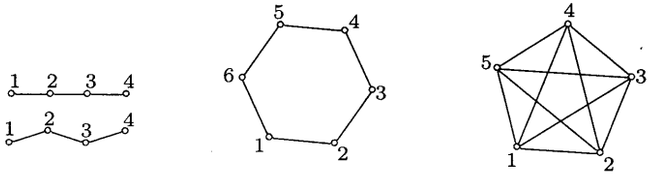
Ramseyev teorem. *Neka je S beskonačan skup. Za svako $k \in \mathbb{N}$ i svaku particiju k-članih podskupova od S u konačno mnogo blokova, postoji beskonačan podskup od S čiji su svi k-člani podskupovi u jednom bloku.*

Na kraju kažimo da opću "filozofiju" Ramseyeve teorije možemo sažeti ovako: Vrlo kaotični veliki sustavi sadrže relativno male podsustave koji su vrlo pravilni. To potkrepljuje i jedan Szemeredijev teorem iz 1978. godine, koji, grubo govoreći, kaže da se i najkaotičniji sustav može rastaviti u relativno mali broj (gotovo) pravilnih podsustava. Zainteresiranog čitatelja za Ramseyevu teoriju upućujemo na knjige [90], [88], [185] ili na pregledni članak u [36*].

Grafovi

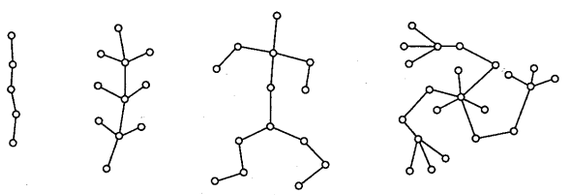
Na kraju ovog uvoda opišimo kratko i neformalno pojam grafa. Sustavno ćemo ih proučavati u VI. poglavlju.

Graf $G = (V, E)$ se sastoji od skupa $V = V(G)$ **vrhova** (ili **čvorova**) i skupa $E = E(G)$ **bridova** — spojnica među vrhovima. To je osnovna kombinatorna konfiguracija. Ako ne kažemo drukčije, smatramo da je graf **konačan**, tj. V i E su konačni skupovi. Graf obično crtamo u ravnini tako da su vrhovi točke, a bridovi dužine (ili krivulje) koje spajaju te točke. Svaki brid koji spaja dva vrha je **incidentan** s tim vrhovima, a oni su **susjedni**. Dva grafa G i H su **izomorfna** ako postoje bijekcije među vrhovima i među bridovima tako da susjedni vrhovi prelaze u susjedne; pišemo $G \approx H$. Graf je **jednostavan** ako su svaka dva vrha spojena s najviše jednim bridom i nema **petlji** (tj. bridova koji spajaju vrh sa samim sobom). Graf H je **podgraf** grafa G, ako je $V(H) \subseteq V(G)$ i $E(H) \subseteq E(G)$. Na idućoj su slici nacrtani neki važni jednostavni grafovi.



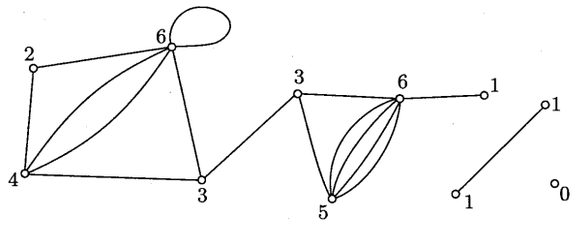
P_4 put s 4 vrha — C_6 ciklus sa 6 vrhova — K_5 potpun graf s 5 vrhova

Graf je **povezan** ako su svaka dva vrha povezana nekim putom. Povezani graf bez ciklusa zove se **stablo** (ili **drvo**). Na donjoj su slici neka stabla.



Stupanj vrha $v \in V(G)$ u grafu G je broj bridova s kojima je v incidentan. Označimo ga s $\deg_G v$ ili $d_G(v)$ ili još kraće $d(v)$ (ako je jasno ili nije važno o kojem se grafu radi).

Intuitivno, stupanj vrha je broj sjecišta male kružnice oko vrha s linijama koje izlaze iz vrha (uočite da se petlja računa dva puta). Na idućoj smo slici nacrtali graf i kod svakog vrha označili njegov stupanj:



Sljedeća važna i jednostavna činjenica ima mnoge primjene.

PROPOZICIJA 3. *Zbroj svih stupnjeva vrhova grafa jednak je dvostrukom broju bridova, tj.*

$$\sum_{v \in V(G)} d_G(v) = 2|E(G)|. \qquad (*)$$

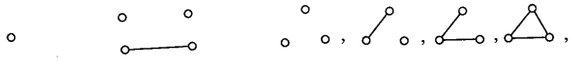
Naime, stupanj vrha je broj bridova koji ga sadrže (petlju računamo dvaput), a svaki brid ima dva kraja, pa zbrajanjem svih stupnjeva dobivamo dvostruki broj bridova.

Kao posljedicu dobivamo sljedeću činjenicu, koja je vrlo korisna pri određivanju parnosti (ili neparnosti) nekog broja objekata.

Lema o rukovanju ("Handshaking lemma"). *U svakom je grafu broj vrhova neparnog stupnja paran broj.*

Ili: na svakoj je zabavi ("tulumu" ili "partyju") broj onih koji su se rukovali s neparnim brojem ostalih paran broj.

U to se možemo uvjeriti tako da konstruiramo graf "tuluma" G ovako: Vrhovi su svi članovi "tuluma", a dva vrha (člana) spojimo bridom ako i samo ako su se ti članovi rukovali. Lema je očito istinita za "male tulume":



"solo tulum" "tulum u dvoje" "tročlani tulumi"

Općenito (za "velike tulume"), neka je V_1 skup onih koji su se rukovali s neparnim brojem drugih (tj. skup vrhova čiji je stupanj u G neparan), a V_2 skup ostalih

članova "tuluma". Tada iz $(*)$ imamo

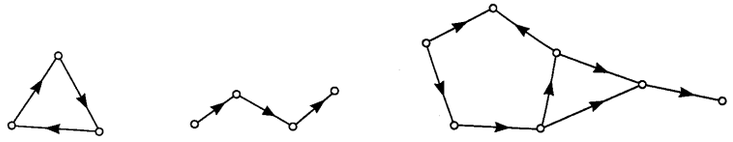
$$\sum_{v \in V_1} d(v) + \sum_{v \in V_2} d(v) = \sum_{v \in V(G)} d(v) = 2|E(G)|.$$

Kako je $\sum_{v \in V_2} d(v)$ paran, slijedi da je i $\sum_{v \in V_1} d(v)$ paran. Svaki sumand potonje sume je neparan, pa stoga $|V_1|$ mora biti paran.

Uočimo da lema o rukovanju ne vrijedi za "beskonačni tulum":



Usmjereni (ili **orijentirani**) **graf** je poput grafa, samo što su bridovi usmjereni (ili orijentirani), tj. svaki brid dobiva "strelicu". Točnije, bridovi, koji se tu zovu **lûkovi**, uređeni su parovi vrhova; dakle, svaki **lûk** $a = (u, v)$ je uređeni par svojih krajeva, što znači da "strelica" ide od u prema v. Na primjer:



II. Kombinatorna prebrojavanja

§ 1. Osnovna pravila prebrojavanja

Kao što smo već istaknuli, jedan od najvažnijih i najčešćih problema s kojima se susrećemo u kombinatorici jest problem određivanja broja elemenata konačnog skupa S, odnosno problem prebrojavanja raznih konfiguracija. **Broj elemenata** od S označava se sa $|S|$, $\operatorname{card} S$ ili $\#S$ i katkad se zove **kardinalni broj** od S (obično za beskonačne skupove). Kod određivanja broja $|S|$ često se susrećemo s tri vrste postupaka. Prvi je postupak da uspostavimo bijekciju s nekim skupom T čiji broj elemenata poznamo, drugi je da znamo dijelove od S, a treći da znamo faktore od S. Pojednostavljeno, prvi način kaže da nije važno kako prebrojavamo sve elemente, drugi kaže da je cjelina jednaka zbroju dijelova, a treći da je veličina umnoška (produkta) jednaka umnošku (produktu) faktora. Točnije, vrijede sljedeća pravila (načela ili principi).

PROPOZICIJA 1 (Osnovna pravila prebrojavanja).

1. **Pravilo jednakosti** *(ili* **bijekcije***).* *Neka su S i T konačni skupovi. Tada je $|S| = |T|$ ako i samo ako postoji bijekcija među skupovima S i T.*

2. **Pravilo zbroja** *(***sume***).* *Neka je $n \in \mathbb{N}$, a $S_1, S_2, \ldots, S_n$ konačni međusobno disjunktni skupovi (tj. $S_i \cap S_j = \emptyset$ za $i \neq j$). Tada je njihova unija $S_1 \cup S_2 \cup \cdots \cup S_n = \bigcup_{i=1}^{n} S_i$ konačan skup i vrijedi*

$$\Big|\bigcup_{i=1}^{n} S_i\Big| = \sum_{i=1}^{n} |S_i|.$$

3. **Pravilo množenja** *(ili* **produkta***).* *Neka je $n \in \mathbb{N}$, a $S_1, S_2, \ldots, S_n$ konačni skupovi. Tada je Kartezijev produkt $S_1 \times S_2 \times \cdots \times S_n = \prod_{i=1}^{n} S_i$ konačan skup i vrijedi*

$$\Big|\prod_{i=1}^{n} S_i\Big| = \prod_{i=1}^{n} |S_i|.$$

Dokaz. Dokazi ovih gotovo očitih pravila vrlo su jednostavni. Pravilo bijekcije vrijedi po definiciji. Pravilo zbroja vrijedi za $n = 2$, jer ako je $S_1 = \{a_1, a_2, \ldots, a_r\}$, a $S_2 = \{b_1, b_2, \ldots, b_s\}$ pri čemu je $a_i \neq b_j$, za sve i, j, onda je očito $S_1 \cup S_2 = \{a_1, \ldots a_r, b_1, \ldots, b_s\}$ i stoga $|S_1 \cup S_2| = r + s = |S_1| + |S_2|$. Pravilo množenja za $n = 2$ slijedi iz toga što sve uređene parove (a_i, b_j) možemo svrstati u tablicu (matricu) tipa $r \times s$:

$$\begin{bmatrix} (a_1,b_1) & (a_1,b_2) & \cdots & (a_1,b_s) \\ \vdots & & & \\ (a_r,b_1) & (a_r,b_2) & \cdots & (a_r,b_s) \end{bmatrix},$$

odakle slijedi da je $|S_1 \times S_2| = r \cdot s = |S_1| \cdot |S_2|$. Pravila zbroja i množenja dalje se lako dokazuju indukcijom po n. □

Svakodnevnim se jezikom pravilo množenja za $n = 2$ može i ovako rastumačiti. Ako za neki događaj imamo r mogućnosti, a svaka od mogućnosti s ishoda, onda je ukupan broj svih mogućih ishoda jednak $r \cdot s$.

Navedimo sada neke jednostavne primjene "**umjetnosti prebrojavanja**" koji se mogu riješiti "zdravorazumski" (uz malo oštroumnosti i dosjetljivosti).

Primjer 1. Na koliko načina (kratko: NKN) se između 5 muškaraca, 7 žena, 3 dječaka i 4 djevojčice može izabrati:

a) jedna osoba?

b) po jedan muškarac, jedna žena, jedan dječak i jedna djevojčica?

Rješenje. a) Iz pravila zbroja slijedi da je taj broj jednak $5 + 7 + 3 + 4 = 19$.

b) Prema pravilu množenja taj je broj jednak $5 \cdot 7 \cdot 3 \cdot 4 = 420$.

□

Primjer 2. Netko želi poslati svakome od svojih 5 prijatelja po jednu od 20 (različitih) razglednica. Na koliko je to načina moguće učiniti?

Rješenje. Za svakog se prijatelja razglednica može izabrati na 20 načina i pet izbora razglednica je neovisno (izbor jedne očito ne utječe na izbor drugih). Stoga je odgovor (prema pravilu množenja) jednak $20 \cdot 20 \cdot 20 \cdot 20 \cdot 20 = 20^5 = 3\,200\,000$. Kao što ćemo poslije pokazati, to je isto kao i prebrojiti sve funkcije iz 5-članog skupa (prijatelji) u 20-člani skup (razglednice). □

Primjer 3. Registarska tablica na vozilima sastoji se nakon oznake mjesta od 3 ili 4 brojke te jednog ili dva slova abecede (njih 30). Koliko ima takvih tablica?

Rješenje. Prema pravilima zbroja i množenja traženi je broj jednak $10^3 \cdot 30 + 10^3 \cdot 30^2 + 10^4 \cdot 30 + 10^4 \cdot 30^2 = 1\,023\,000$. □

Primjer 4. Svaki od četvorice dečka izabere jednu od šest djevojaka kao partnericu za ples. Na koliko se to načina može učiniti?

Rješenje. Jedan dečko može izabrati bilo koju od 6 djevojaka. Drugome tada preostaje izbor od 5 djevojaka, trećem preostaje izbor od 3 djevojke, a četvrtom izbor od 3 djevojke. Prema pravilu množenja, traženi je broj jednak $6 \cdot 5 \cdot 4 \cdot 3 = 360$. □

Primjer 5. Na polici su hrpe od: 8 jabuka, 10 kruški, 7 breskvi, 6 banana i 3 ananasa. Za spremanje voćne salate potrebno je nekoliko komada voća (uključujući i "praznu salatu"). Koliko se ukupno voćnih salata može spraviti od ponuđenog voća?

Rješenje. Svaka voćna salata odgovara izboru od nekoliko komada (moguće i 0) svake od ponuđene vrste voća. Tako dobivamo prirodnu bijekciju

$$\left\{ \begin{array}{c} \text{voćne} \\ \text{salate} \end{array} \right\} \to \{0,1,2,\ldots,8\} \times \{0,1,\ldots,10\} \times \{0,1,\ldots,7\} \times \{0,1,\ldots,6\} \times \{0,1,2,3\}.$$

Prema tome, voćnih salata imamo toliko koliko ima elemenata skup na desnoj strani. Prema pravilu množenja, potonji skup ima $9 \cdot 11 \cdot 8 \cdot 7 \cdot 4 = 22\,176$ elemenata. □

Primjer 6. Osnovni teorem aritmetike kaže da se svaki prirodni broj $n > 1$ može jednoznačno napisati u obliku $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$, gdje su $p_1 < p_2 < \cdots < p_k$ prosti brojevi, a $\alpha_1, \alpha_2, \ldots, \alpha_k$ prirodni brojevi. Odredite broj $\tau(n)$ svih djelitelja od n (uključujući 1 i n).

Rješenje. Svaki je djelitelj od n oblika $p_1^{\beta_1} p_2^{\beta_2} \ldots p_k^{\beta_k}$, gdje je $0 \le \beta_1 \le \alpha_1, \ldots, 0 \le \beta_k \le \alpha_k$. Dakle, skup svih djeljitelja od n je u bijekciji sa skupom uređenih k-torki cijelih brojeva $\{(\beta_1, \beta_2, \ldots, \beta_k) | 0 \le \beta_1 \le \alpha_1, \ldots, 0 \le \beta_k \le \alpha_k\}$, a ovaj je u bijekciji s $\{0,1,\ldots,\alpha_1\} \times \cdots \times \{0,1,\ldots,\alpha_k\}$. Stoga je broj djelitelja $\tau(n)$ broja n jednak broju $\tau(n) = (\alpha_1 + 1) \cdot (\alpha_1 + 1) \cdot \cdots \cdot (\alpha_k + 1)$. Tako npr. broj $n = 349272 = 2^3 \cdot 3^4 \cdot 7^2 \cdot 11$ ima $(3+1) \cdot (4+1) \cdot (2+1) \cdot (1+1) = 120$ djelitelja. □

Primjer 7. Dvanaestero djece treba prijeći ulicu, pa ih teta iz vrtića želi razvrstati u 6 grupa po dvoje (tj. u 6 parova). Na koliko to načina teta može učiniti?

Rješenje. U paru s jednim djetetom može biti bilo koje od 11 preostale djece. Kad smo jednom utvrdili jedan par, onda s ostalih 10 djece rezoniramo na isti način itd. Stoga je odgovor $11 \cdot 9 \cdot 7 \cdot 5 \cdot 3 \cdot 1 = 10\,395$. □

Primjer 8. Koliko ima (prirodnih) brojeva manjih od bilijun ($= 10^{12}$) koji sadrže znamenku 2 u svom dekadskom zapisu? Kojih brojeva ima više, onih koji sadrže ili onih koji ne sadrže 2?

Rješenje. Odredimo prvo broj onih brojeva $< 10^{12}$ koji ne sadrže brojku 2. Taj je broj jednak broju slogova od 12 simbola iz skupa $\{0,1,3,4,5,6,7,8,9\}$. Tih brojeva prema pravilu množenja ima 9^{12} (uključujući $00\ldots0$). Stoga, brojeva koji sadrže brojku 2 ima $10^{12} - 9^{12}$. Dakle, oko 98 posto brojeva manjih od bilijun sadrži brojku 2. □

Primjer 9. Koliko ima neparnih brojeva između 1000 i 10000, od kojih svaki ima različite znamenke?

Rješenje. Svaki broj između 1000 i 9999 uređena je četvorka svojih znamenaka ili brojaka. Zadnja brojka mora biti iz $\{1,3,5,7,9\}$, dakle imamo 5 mogućnosti. Kad je jednom zadnja brojka izabrana, prvu brojku možemo odabrati na 8 načina (svaka iz $\{1,\ldots,9\}$ osim izabrane zadnje, jer brojke moraju biti različite). Kad su ove dvije već izabrane, za drugu brojku imamo 8 mogućnosti (svaka iz $\{0,1,\ldots,9\}$ osim već dvije izabrane), pa nakon izbora tih triju imamo još 7 mogućnosti za izbor treće brojke. Prema pravilu množenja, traženih brojeva ima $5 \cdot 8 \cdot 8 \cdot 7 = 2\,240$. □

Uočimo da smo ove probleme riješili tako da smo zapravo uspostavili bijekciju (katkad i prešutno) između skupa čiji broj elemenata tražimo i nekog skupa kojem znamo broj elemenata. Tako je u kombinatorici i uvijek poželjno zaključivati. Da bismo dokazali da je $|S| = n$, mi ćemo uvijek nastojati naći neku bijekciju između skupa S i skupa $[n] = \{1,2,\ldots,n\}$ za koji znamo da ima n elemenata. Takav postupak se onda i zove **kombinatorni** (ili **bijektivni**) **dokaz**. Uza sva umijeća i pamet, takav izravni ("najčišći") dokaz je često vrlo teško naći. Zato ćemo razviti druge tehnike kojima ćemo zaobići tu teškoću.

§ 2. Prebrojavanje funkcija, podskupova, injekcija i bijekcija

Sada ćemo manirama kombinatornog zaključivanja izvesti važne formule za broj funkcija i broj injekcija među konačnim skupovima, za broj bijekcija nekog konačnog skupa, kao i broj svih podskupova nekog konačnog skupa i broj k-članih podskupova konačnog skupa. Skupovi i funkcije su, uostalom, fundamentalni objekti proučavanja u matematici. Krenimo redom.

Ako su S i T neki skupovi onda se skup svih preslikavanja ili funkcija $f : S \to T$ sa skupa S u skup T označava s T^S.

PROPOZICIJA 2. *Neka su N i X konačni skupovi $|N| = n$, $|X| = x$. Tada je*

$$|X^N| = |X|^{|N|} = x^n.$$

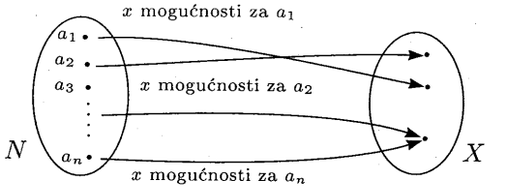
Dokaz. Neka je $N = \{a_1, a_2, \ldots, a_n\}$. Prema pravilu množenja, skup $X^n = X \times X \times \cdots \times X$ ima $|X|^n = x^n = |X|^{|N|}$ elemenata. Konstruirajmo bijekciju $\varphi : X^N \to X^n$. Definirajmo za $f \in X^N$ (tj. $f : N \to X$)

$$\varphi(f) = (f(a_1), f(a_2), \ldots, f(a_n)). \qquad (*)$$

Sada se lako provjeri da je φ doista bijekcija (učinite to!). Time je dokaz gotov. □

Napomena 1. Uočite da smo bijekciju φ mogli zadati npr. i ovako: $\varphi(f) = (f(a_3), f(a_n), \ldots, f(a_2))$. No odabirom nekog čvrstog poretka elemenata od N, npr. $a_1 \prec a_2 \prec \cdots \prec a_n$, formulom $(*)$ dobro je definirano preslikavanje φ.

Napomena 2. Ovaj elegantni i kratki dokaz možemo riječima još kraće izreći ovako. S bilo kojom funkcijom $f : N \to X$, element a_1 se može preslikati u bilo koji od x elemenata iz X. Bez obzira na to kamo poslali a_1, element a_2 također možemo poslati na x mjesta, itd. sve do a_n. Prema pravilu množenja, f možemo zadati na $x \cdot x \cdot \cdots \cdot x = x^n$ načina. Za vizualnog čitatelja, dajemo i donju sliku.



Ustvari, ovako bi se Propozicija 2 mogla dokazati indukcijom po n (i time izbjeći specifikacija uređaja elemenata iz N; za vježbu provedite sa svim potankostima i taj dokaz).

Katkad se dodatno definira da je $|\emptyset^\emptyset| := 1$.

S pomoću Propozicije 2 kombinatorno protumačite poznate formule $x^m \cdot x^n = x^{m+n}$ i $(x \cdot y)^n = x^n \cdot y^n$.

PROPOZICIJA 3. *Broj svih podskupova n-članog skupa je jednak 2^n.*

Dokaz. Neka je $|S| = n$. Treba dokazati da je

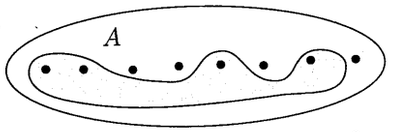
$$|2^S| = 2^{|S|} = 2^n.$$

To ćemo dokazati uporabom prethodne Propozicije i to tako da ćemo konstruirati jednu bijekciju između skupa 2^S svih podskupova iz S i skupa svih preslikavanja $\{0,1\}^S$. U tu svrhu svakom podskupu $A \subseteq S$ pridružimo njegovu **karakterističnu funkciju** $\chi_A : S \to \{0,1\}$ definiranu ovako:

$$\chi_A(x) = \begin{cases} 1\,, & \text{za } x \in A \\ 0\,, & \text{za } x \notin A \end{cases}$$

Pridruživanje $\varphi : A \mapsto \chi_A$ je bijekcija sa 2^S u $\{0,1\}^S$. Zaista, ako su A i B različiti podskupovi od S, onda se oni razlikuju u barem jednom elementu x. Ako je npr. $x \in A$, $x \notin B$, onda je $\chi_A(x) = 1$, $\chi_B(x) = 0$, pa je $\chi_A \neq \chi_B$. Dakle, različiti podskupovi imaju različite karakteristične funkcije, pa je φ injekcija. Ako je $f : S \to \{0,1\}$ zadana funkcija (tj. $f \in \{0,1\}^S$), onda ona potpuno određuje podskup A za koji je $\chi_A = f$; naime, $A = f^{-1}(1)$ = skup svih $x \in S$ za koji je $f(x) = 1$. Dakle, $\varphi(A) = f$, pa je φ i surjekcija. Zato je φ bijekcija. Prema Propoziciji 2 je $|\{0,1\}^S| = 2^n$, pa je stoga i $|2^S| = 2^n$. □

Napomena 3. I ovaj dokaz kratko možemo izreći ovako. Svaki podskup $A \subseteq S$ je *kodiran* svojom karakterističnom funkcijom χ_A (koja, dakle, "raspoznaje" skup A). Drugim riječima, poredamo li nekako elemente iz S, onda je A potpuno određen uređenom n-torkom nula i jedinica. Za "vizualce" slika:



χ_A 1 1 0 0 1 0 1 0

Bez specifikacije uređaja Propozicija 3 se može dokazati indukcijom po n (za vježbu provedite sa svim potankostima i taj dokaz). Vrlo sažeto gornji dokaz možemo ovako izreći. 2^n broji sve podskupove od S, jer za svaki od n elemenata imamo dvije mogućnosti: ili jest u podskupu ili nije.

Napomena 4. Za sve $n \in \mathbb{N}$ vrijedi $2^n > n$ (što se npr. može provjeriti indukcijom), pa je za skup S od n elemenata $|2^S| > |S|$. No kombinatorno se ova nejednakost vidi tako što partitivni skup 2^S sadrži među inim i sve jednočlane podskupove od S, a tih

je upravo $|S|$. Točnije, postoji injekcija $\varphi : S \to 2^S$, $\varphi(x) = \{x\}$, koja nije surjekcija. Za $S = \mathbb{N}$, "Cantorov dijagonalni postupak" pokazuje da je $\operatorname{card}\{0,1\}^{\mathbb{N}} > \operatorname{card}\mathbb{N}$, tj. $c = 2^{\aleph_0} > \aleph_0$, čime se pokazuje da realnih brojeva "ima više" od prirodnih.

KOROLAR 1. *Broj svih parnih podskupova (tj. onih s parno mnogo elemenata) n-članog skupa jednak je broju svih neparnih podskupova (tj. onih s neparno mnogo elemenata). Oba su ta broja jednaka 2^{n-1}.*

Dokaz. Neka je S skup sa $|S| = n$. Nađimo bijekciju između parnih i neparnih podskupova od S. Neka je $a \in S$ neki čvrsti element. Neka je $A \subseteq S$. Pridružimo mu $A' \subseteq S$ na sljedeći način. Ako A sadrži a, neka je $A' = A \setminus \{a\}$, a ako A ne sadrži a, neka je $A' = A \cup \{a\}$. Bijekcijom $A \mapsto A'$ parni podskupovi prelaze u neparne i obrnuto. Kako parnih i neparnih zajedno ima 2^n prema Propoziciji 3, to slijedi da i parnih i neparnih podskupova od S ima $\frac{2^n}{2} = 2^{n-1}$. □

Navedimo neke primjere gdje se prirodno javljaju potencije s bazama $2, 3, \ldots$.

Primjer 10. Binarni broj duljine n je uređena n-torka sastavljena od 0 i 1. Koliko ima binarnih brojeva duljine n? (Računala primaju i izbacuju rezultate u binarnim brojevima, tzv. **bitovima** - od engl. **binary digit**; taj je pojam uveo američki matematičar Claude Shannon r. 1916., jedan od utemeljitelja teorijske informatike i suvremenog računarstva.)

Rješenje. Binarne "riječi" duljine n su uređene n-torke $i_1 i_2 \ldots i_n$, gdje su svi $i_k \in \{0,1\}$. Ako su na mjestima s indeksima $j_1, j_2, \ldots, j_k$ jedinice, a na ostalim mjestima nule, onda toj riječi pridružujemo podskup $\{j_1, j_2, \ldots, j_k\} \subseteq \{1, 2, \ldots, n\}$, a "praznoj" riječi $00\ldots0$ pridružujemo prazan skup $\emptyset$. To pridruživanje je očito bijekcija, pa binarnih riječi duljine n ima koliko i podskupova od $\{1, 2, \ldots, n\}$, a tih je 2^n. □

Primjer 11. U glavnoj memoriji računala podaci se smještaju u tzv. memorijske ćelije. Svaka ćelija ima svoju *adresu*. Binarni broj duljine 8 zove se **bajt** (engl. byte). Adresa je obično kodirana s jednim bajtom. No neka računala rabe dvobajtno adresiranje, tj. adresa memorijske ćelije sastoji se od dva uzastopna bajta, a neka rabe adresiranje ćelija sa četiri bajta, dok najnovija koriste osam bajta.

Izračunajte koliki je ukupan broj adresa dostupnih za pohranjivanje informacija u memorijske ćelije u svakom od slučajeva.

Rješenje. U slučaju jednog bajta imamo $2^8 = 256$ adresa, u 2-bajtnom slučaju broj adresa je $2^8 \cdot 2^8 = 65536$, u 4-bajtnom slučaju je $(2^8)^4 = 4294967296$ (dakle, oko 4.3 milijarde), a u 8-bajtnom slučaju $(2^8)^8 = 2^{64} \approx 1.8 \cdot 10^{24}$. □

Primjer 12. Booleova funkcija od n varijabli je funkcija $f : \{0,1\}^n \to \{0,1\}$. Koliko ih ima ukupno?

Rješenje. Iz Propozicije 2 za $N = \{0,1\}^n$ i $X = \{0,1\}$ slijedi da je odgovor jednak 2^{2^n}. Tako primjerice, Booleovih funkcija s dvije varijable ima ukupno $2^{2^2} = 2^4 = 16$, s tri varijable $2^{2^3} = 2^8 = 256$, s četiri varijable $2^{2^4} = 2^{16} = 65536$, s pet varijabli $2^{2^5} = 2^{32} \approx 4.3$ milijarde itd. □

Primjer 13. Neka je S skup od n elemenata. Koliko ima binarnih relacija na S? (Binarna relacija na S je podskup od $S \times S$.)

Rješenje. Skup $S \times S$ ima n^2 elemenata, a mi tražimo $|2^{S\times S}|$. Prema Propoziciji 3 taj je broj 2^{n^2}. Tako skup od 6 elemenata ima $2^{36} \approx 69$ milijardi binarnih relacija. Kao što vidimo u ovim primjerima, rezultati strahovito brzo rastu kako raste parametar n. Takav brz rast se katkad zove **kombinatorna eksplozija**. □

Primjer 14. Koliko će sumanada biti u izrazu $(x_1+1)(x_2+1)(x_3+1)\dots(x_n+1)$ nakon svih provedenih množenja?

Rješenje. Svaki sumand (osim 1) nakon izvršenog množenja izgleda ovako: $x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_k}$, gdje je $1 \le i_1 < i_2 < \dots < i_k \le n$. Svaki takav niz $i_1 i_2 \dots i_k$ odgovara nekom podskupu ($\neq \emptyset$) skupa $[n] = \{1, 2, \dots, n\}$, a sumand 1 odgovara praznom podskupu. Traženi je broj dakle $|2^{[n]}| = 2^n$. □

Primjer 15. Sportska prognoza ima 12 redaka. U svaki redak treba upisati 0, 1 ili 2 (neriješeno, pobjeda domaćina, pobjeda gosta). Na koliko se načina može ispuniti sportska prognoza?

Rješenje. Jedan stupac sportske prognoze je zapravo funkcija $[12] \to \{0,1,2\}$. Dakle sportska prognoza se može ispuniti na toliko načina koliko ima ovih funkcija, a njih prema Propoziciji 2 ima $3^{12} = 531441$. □

Primjer 16. Lokot na šifru ima 4 koluta s po 10 brojki $0, 1, 2, \dots, 9$. Lokot se može otvoriti samo onda ako je na svakom kolutu postavljena ispravna brojka. Koliko šifri može imati takav lokot?

Rješenje. Svaka šifra je funkcija $[4] \to \{0, 1, \dots, 9\}$, a takvih funkcija ima ukupno $10^4 = 10000$. □

Primjer 17. Trijadski broj duljine n je uređena n-torka koja se sastoji od brojeva 0, 1 i 2, s tim da na prvom mjestu ne stoji 0. Koliko ih ima ukupno?

Rješenje. Trijadski broj duljine n je zapravo funkcija $f : [n] \to \{0,1,2\}$, s tim da je $f(1) \neq 0$. Stoga od broja $\#\{0,1,2\}^{[n]} = 3^n$ treba oduzeti broj $\#\{0,1,2\}^{[n-1]} = 3^{n-1}$, pa je odgovor $3^n - 3^{n-1} = 2 \cdot 3^{n-1}$. □

Primjer 18. Koliko ukupno ima različitih riječi od 6 slova koje možemo načiniti od 30 slova hrvatske abecede a b c č ... z ž (uključujući i besmislene riječi kao što je bmčzaz[1])?

Rješenje. Na svaku od 6 pozicija slobodno možemo staviti bilo koje od 30 slova, pa je zato odgovor $30^6 = 729$ milijuna. Na drugi način možemo zaključivati ovako. Svaka 6-slovčana riječ je zapravo preslikavanje $[6] \to \{a, b, \dots, \check{z}\}$ koje svakom od 6 mjesta označenih s $1, 2, \dots, 6$ pridružuje neko slovo abecede. Zato je (opet) odgovor 30^6. □

Do sada smo prebrojili sve funkcije $N \to X$, tj. našli da je $|X^N| = |X|^{|N|}$, a sada ćemo prebrojiti sve injekcije $N \to X$.

Ako su S i T neki skupovi, onda se skup svih injekcija $S \to T$ označava simbolom $T^{\underline{S}}$ (ili $\mathrm{Inj}(S,T)$).

[1] Tko može reći da je neka riječ besmislena ili bez značenja? Možda ona ipak ima neko značenje u, recimo, bušbumbuju jeziku.

PROPOZICIJA 4. *Neka su N i X konačni skupovi, $|N| = n$, $|X| = x$. Tada je*

$$|X^{\underline{N}}| = x(x-1)(x-2)\cdot\dots\cdot(x-n+1) := x^{\underline{n}}.$$

Broj $x^{\underline{n}} := x(x-1)\cdot\dots\cdot(x-n+1) = \prod_{i=0}^{n-1}(x-i)$ se zove **padajuća potencija** ili **padajući faktorijel**. Njegova baza x određuje od kojeg mjesta počinjemo, a "eksponent" n za koliko se mjesta spustimo dolje i sve uzastopne brojeve pomnožimo. Slično se definira **rastuća potencija** ili **rastući faktorijel**

$$x^{\overline{n}} := x(x+1)(x+2)\cdot\dots\cdot(x+n-1).$$

Ove definicije padajućeg i rastućeg faktorijela očito imaju smisla i za realne (ili kompleksne) brojeve x i sve prirodne brojeve n. Definiramo li nadalje

$$x^{\underline{0}} := 1 \quad \text{i} \quad x^{\underline{-n}} := \frac{1}{(x+1)(x+2)\cdot\dots\cdot(x+n)} \text{ za } n > 0,$$

dobivamo $x^{\underline{n}}$ definirano za sve cijele brojeve n. Veza između padajućeg i rastućeg faktorijela je sljedeća (recipročnost):

$$x^{\overline{n}} = (-1)^n(-x)^{\underline{n}} = (x+n-1)^{\underline{n}} = 1/(x-1)^{\underline{-n}},$$

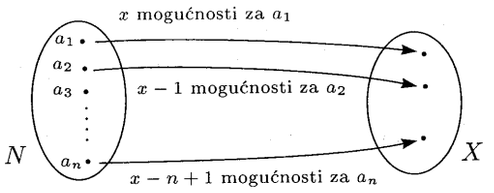
$$x^{\underline{n}} = (-1)^n(-x)^{\overline{n}} = (x-n+1)^{\overline{n}} = 1/(x+1)^{\overline{-n}},$$

pri čemu je $x^{\overline{-n}} = 1/(x-n)^{\overline{n}} = 1/(x-1)^{\underline{n}}$, za sve $n \in \mathbb{Z}$ (provjerite te formule). Stoga na $x^{\underline{n}}$ (ili $x^{\overline{n}}$) možemo gledati kao na polinom za $n \ge 0$, odnosno kao na racionalnu funkciju za $n < 0$ u varijabli x.

No vratimo se na injekcije i dokažimo da njihov broj daje kombinatorno značenje padajućih faktorijela. Dat ćemo dva (u biti ista) dokaza.

Dokaz I Propozicije 4. Neka je $N = \{a_1, a_2, \dots, a_n\}$ i neka je $a_1 \prec a_2 \prec \dots \prec a_n$ opet neki čvrsti poredak elemenata. Sada prvi element a_1 možemo preslikati u bilo koji od x elemenata iz X, tj. mi imamo x mogućnosti za sliku od a_1. Kad smo a_1 negdje preslikali, slika od a_2 može biti bilo koji od preostalih $x-1$ elemenata iz X, tj. za sliku od a_2 imamo $x-1$ mogućnosti, jer se radi o injekciji. Kad smo i a_2 negdje preslikali, za a_3 imamo $x-2$ mogućnosti itd., kad smo i a_{n-1} nekud preslikali, onda za sliku od a_n imamo još $x-(n-1) = x-n+1$ mogućnosti. Prema pravilu množenja svih mogućnosti, tj. svih injekcija $N \to X$ ima $x(x-1)(x-2)\dots(x-n+1)$. □

"Vizualni dokaz" je na idućoj slici.



Napomena 5. Za $n > x$ uopće nema injekcije $N \to X$, tj. broj injekcija je tada nula, što je u skladu s formulom (jer tada produkt prolazi kroz 0). Dakle, formula je smislena i za $n \geq x$.

Dokaz II Propozicije 4. (Indukcijom po n). Za $n = 1$ tvrdnja je jasna (pa čak i za $n = 0$ – zašto?). Neka je $n \geq 1$. Neka je $a \in N$ neki čvrsti element, odaberimo vrijednost $f(a) \in X$ kao bilo koji od x elemenata. Preostaje odabrati injekciju $N \setminus \{a\} \to X \setminus \{f(a)\}$. Po pretpostavci indukcije to se može učiniti na $(x-1)^{\underline{n-1}}$ načina. Stoga ukupno imamo $x \cdot (x-1)^{\underline{n-1}} = x^{\underline{n}}$ injekcija $N \to X$. □

Pogledajmo sada vrlo važan poseban slučaj kada je $x = n$. Tada je $n^{\underline{n}} = n(n-1)(n-2)\cdot\cdots\cdot 1$. Kao što znamo, to je (uz dogovor $0! := 1$) n **faktorijela**:

$$n! = 1 \cdot 2 \cdot \cdots \cdot n.$$

Uočite da je za $n, x \in \mathbb{N}$, $n \leq x$, broj injekcija $N \to X$, $|N| = n$, $|X| = x$ jednak

$$x^{\underline{n}} = \frac{x!}{(x-n)!}.$$

Umjesto injekcija, običnim riječima rečeno, $x^{\underline{n}}$ je broj načina da se od x (različitih) predmeta izabere njih n, pri čemu je poredak bitan, a ponavljanja nema.

KOROLAR 2. *Broj bijekcija n-članog skupa u samog sebe je jednak $n!$.*

Dokaz. Ako u Propoziciji 4 stavimo $x = n$, dobivamo upravo $n!$. Međutim, svaka injekcija n-članog skupa u samog sebe je i bijekcija. □

Bijekcija skupa u samog sebe zove se još i **permutacija**[2] tog skupa.

Bilješka. Često je vrlo teško dokazati i da *ne* postoji bijekcija među nekim skupovima. Tako je npr. poznato da produkt od ≥ 2 uzastopna prirodna broja nikad nije potencija prirodnog broja (vidi P. Erdös, J. Selfridge, Illinois Journal of Math. 19 (1975), 292–301). Stoga za konačne skupove N, X, Y, M s bar dva elementa nikad ne postoji bijekcija između X^N i $Y^{\underline{M}}$, tj. uvijek je $X^N \not\approx Y^{\underline{M}}$. Bilo bi vrlo zanimljivo to dokazati i kombinatorno.

§ 3. Permutacije skupova

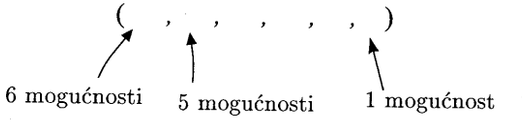
Neka je $S = \{a_1, a_2, \ldots, a_n\}$ neki n-člani skup. Permutacija od S je bijekcija $f : S \to S$, pa odabirom nekog uređaja elemenata od S, npr. $a_1 \prec a_2 \prec \cdots \prec a_n$, permutacijom f ti elementi prelaze redom u $f(a_1), f(a_2), \ldots, f(a_n)$, dakle u jedan novi niz (točnije uređenu n-torku) različitih elemenata iz S, npr. $a_{i_1}, a_{i_2}, \ldots, a_{i_n}$. Time se dobiva jedan novi (linearni) uređaj na S: $a_{i_k} \prec a_{i_l} \iff k < l$. Tako dobivamo da na S ima $n!$ različitih linearnih uređaja.

Skup svih bijekcija (tj. permutacija) $S \to S$ s kompozicijom kao grupovnom operacijom očito čini grupu. Ako je $S = [n] = \{1, 2, \ldots, n\}$, onda se ta grupa označava sa S_n i zove **simetrična grupa**. Red te grupe je $|S_n| = n!$.

[2]Od lat. *permutare* – promijeniti, premjestiti. Hrvatski bi se stoga za permutaciju reklo premjestba, ali se to nije udomaćilo

Primjer 19. Na koliko načina 6 ljudi može stati u red (primjerice pred kino-blagajnom)?

Rješenje. Označimo ljude (uz dužnu ispriku) brojevima $1, 2, 3, 4, 5, 6$. Mi se zapravo pitamo koliko ima linearnih uređaja (poredaka) ovih 6 elemenata, tj. na koliko načina možemo popuniti tablicu (, , , , ,) različitim elementima iz [6]. Sljedeća slika pokazuje da je odgovor $6! = 720$ (i to je još jedan dokaz Korolara 2):



□

Primjer 20. 6 muškaraca i 5 žena trebaju stati u red pred trgovinu tako da alterniraju muškarac–žena–muškarac–žena–... Na koliko je to načina moguće?

Rješenje. 6 muškaraca možemo poredati na 6! načina, a 5 žena na 5! načina. Ako najprije stavimo u red muškarce, pa se malo razmaknu, tako da između susjedne dvojice stane po jedna žena, onda se uz svaki poredak muškaraca, žene mogu (uz propisanu alternaciju) stati u red na 5! načina. Prema pravilu množenja, traženi je broj jednak $6! \cdot 5! = 720 \cdot 120 = 86400$. □

Primjer 21. a) Na koliko se načina može razmjestiti 8 topova (kula) na šahovsku ploču tako da se nikoja dva međusobno ne napadaju?

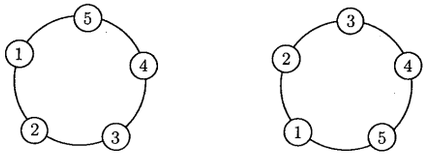
b) Isto pitanje kao a), pod uvjetom da se topovi međusobno razlikuju?

Rješenje. a) U prvi red možemo staviti top na 8 mjesta; kad smo fiksirali top u prvom redu, onda u drugi red možemo topa postaviti na 7 mjesta; nakon ovako fiksirana dva topa u prva dva reda, u treći red možemo postaviti top na 6 načina itd., pa je traženi broj 8!.

b) Označimo topove npr. s $T_1, \ldots, T_8$. Odgovor je tada očito $(8!)^2$ jer još svakom rasporedu topova iz a) odgovara 8! permutacija topova $T_1, \ldots, T_8$.

□

Primjer 22. Na koliko bitno različitih načina n ljudi može sjesti za okrugli stol? Pritom dva načina smatramo bitno istim ako jedan iz drugog možemo dobiti rotacijom, a inače bitno različitim. Primjerice za $n = 5$ na slici su dva zaposjedanja u biti ista:



Rješenje. Označimo ljude s $1, 2, \ldots, n$. Uspostavit ćemo bijekciju između skupova svih kružnih razmještaja (tj. oko okruglog stola) n ljudi i skupa svih (linijskih) razmještaja $n-1$ ljudi u red. Neka je n ljudi sjelo za okrugli stol. S obzirom na osobu 1, nazovimo prvu osobu njoj zdesna a_1, drugu osobu njoj zdesna a_2 itd., a $(n-1)$-vu osobu njoj zdesna a_{n-1}. Tada je $(a_1, a_2, \ldots, a_{n-1})$ jedna permutacija skupa $\{2, 3, \ldots, n\}$, tj. razmještaj tih osoba u red. Obratno, ako su osobe $2, 3, \ldots, n$ stale u red $a_1, a_2, \ldots, a_{n-1}$, a osobu 1 stavimo bilo

gdje za okrugli stol, onda na prvo mjesto zdesna od nje stavimo osobu a_1, zdesna od nje osobu a_2 itd. Lako se provjeri da je to pridruživanje bijekcija, pa je traženi broj jednak $(n-1)!$. □

Svaku permutaciju $\pi \in S_n$ skupa $[n] = \{1, 2, \ldots, n\}$ možemo zapisati kao

$$\pi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ i_1 & i_2 & i_3 & \ldots & i_n \end{pmatrix},$$

gdje je $\pi(1) = i_1, \pi(2) = i_2, \ldots, \pi(n) = i_n$ ili kraće kao $\pi = i_1 i_2 \ldots i_n$ tj. kao "riječ" nad "alfabetom" $[n]$, izostavljajući gornji red koji je uvijek $12 \ldots n$. Pokažimo primjerom kako se množe (tj. komponiraju) permutacije i kako se nalazi inverz dane permutacije.

Uzmimo npr. $\pi = 51423, \rho = 41253 \in S_5$ i neka je $\sigma = \rho \circ \pi$ njihova kompozicija. Tada zbog $\pi(1) = 5$, $\rho(5) = 3$ slijedi $\sigma(1) = 3$, pa zbog $\pi(2) = 1$, $\rho(1) = 4$ slijedi $\sigma(2) = 4$ itd. Tako dobivamo da je $\sigma = 34512$. Nadalje, kako je $\pi(1) = 5$, $\pi(2) = 1$, $\pi(3) = 4$, $\pi(4) = 2$, $\pi(5) = 3$, to odavde slijedi da je $\pi^{-1}(5) = 1$, $\pi^{-1}(1) = 2$, $\pi^{-1}(4) = 3$, $\pi^{-1}(2) = 4$, $\pi^{-1}(3) = 5$, pa je $\pi^{-1} = 24531$.

Drugi način zapisa permutacije je pomoću tzv. ciklusa permutacije. Naime, permutacija nekog skupa S je bijekcija $\pi : S \to S$, pa ako uzmemo neki element $x \in S$, onda je prirodno promatrati niz $x, \pi(x), \pi^2(x), \pi^3(x), \ldots$, gdje je $\pi^2 = \pi \circ \pi, \pi^3 = \pi^2 \circ \pi$ itd. Kako je π bijekcija, a S konačan skup, taj niz se kad-tad mora vratiti u x. Stoga postoji jednoznačno određen $k \geq 1$ takav da je $\pi^k(x) = x$, a elementi $x, \pi(x), \ldots, \pi^{k-1}(x)$ međusobno različiti. Takav niz $(x, \pi(x), \ldots, \pi^{k-1}(x))$ nazivamo **ciklus permutacije** π **duljine** k. Cikluse $(x, \pi(x), \ldots, \pi^{k-1}(x))$ i $(\pi^i(x), \pi^{i+1}(x), \ldots, \pi^{k-1}(x), x, \ldots, \pi^{i-1}(x))$ smatramo ekvivalentnim ("istim"). Svaki element iz S se javlja u jedinstvenom ciklusu od π i permutaciju π možemo rastaviti na disjunktnu uniju (zvanu produkt) različitih ciklusa $C_1, C_2, \ldots, C_r$. To zapisujemo kao $\pi = C_1 C_2 \ldots C_r$ i zovemo **ciklički rastav** od π.

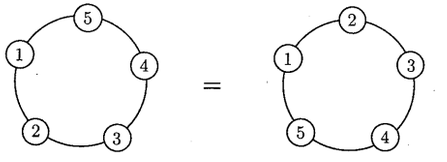
Uzmimo jedan primjer. Neka je npr. $\pi \in S_7$ definirana ovako $\pi(1) = 3$, $\pi(2) = 4$, $\pi(3) = 7$, $\pi(4) = 2$, $\pi(5) = 1$, $\pi(6) = 6$, $\pi(7) = 5$, tj. $\pi = 3472165$. Prvo pogledajmo sliku od 1, tj. $\pi(1) = 3$, pa onda $\pi(3) = 7$, pa $\pi(7) = 5$ i zbog $\pi(5) = 1$ ciklus se zatvara. Tako dobivamo ciklus $(1, 3, 7, 5)$. Sljedeći element koji nije obuhvaćen je 2. Zbog $\pi(2) = 4$, $\pi(4) = 2$, dobivamo ciklus $(2, 4)$. Preostaje još element 6, a zbog $\pi(6) = 6$ imamo ciklus (6). Prema tome, π možemo rastaviti na cikluse ovako $\pi = (1, 3, 5, 7)(2, 4)(6)$. Naravno, to nije i jedini prikaz. Tako su npr. $\pi = (4, 2)(6)(3, 5, 7, 1)$, $\pi = (6)(2, 4)(7, 1, 3, 5)$ još neki rastavi od π u disjunktne cikluse.

Ciklus duljine k zove se još i **k-ciklus**, a 1-ciklus je **trivijalni ciklus**. Trivijalni ciklusi su naprosto fiksne točke permutacije i oni se obično izostavljaju u rastavu permutacije na cikluse. Permutacija $\pi \in S_n$ koja se sastoji od samo jednog k-ciklusa i ostalih trivijalnih ciklusa zove se **k-ciklička**, a n-ciklička se naprosto zove **ciklička permutacija**. 2-ciklus se zove **transpozicija**; dakle, transpozicija $\pi = (i\ j) \in S_n$ djeluje ovako: $\pi(i) = j$, $\pi(j) = i$, $\pi(k) = k$ za sve $k \neq i, j$. **Standardna transpozicija** je oblika $(i, i+1)$, tj. ona izmijeni samo dva susjedna elementa.

Ciklička permutacija $\pi \in S_n$ je, dakle, oblika $\pi = (1\ \pi(1)\ \pi^2(1) \ldots \pi^{n-1}(1))$, što znači da π djeluje ovako: $1 \mapsto \pi(1)$, $\pi(1) \mapsto \pi(\pi(1)) = \pi^2(1), \ldots, \pi^{n-1}(1) \mapsto 1$, tj. zatvara se ciklus. Tako je npr. $\pi \in S_5$ zadana s $\pi(1) = 2$, $\pi(2) = 3$, $\pi(3) = 4$, $\pi(4) = 5$, $\pi(5) = 1$ ciklička permutacija (12345), i očito vrijedi $(12345) = (23451) = (34512) = (45123) = (51234)$. Dakle, cikličke permutacije ostaju iste obzirom na "rotaciju".

Primjer 23. Koliko se različitih ogrlica može napraviti od $n\,(\geq 3)$ perli (bisernih kuglica) koje su sve različito obojene (koriste se sve perle)?

Rješenje. Ogrlica se očito ne mijenja pri cikličkoj permutaciji perla, a ni pri preokretanju ogrlica, tj. pri zrcaljenju.



Ovdje onda očito imamo upola manje mogućnosti nego u prethodnom primjeru. Stoga je traženi broj $\frac{1}{2}(n-1)!$. □

Primjer 24. Svaku permutaciju f od $[n]$ možemo zapisati kao $f = \begin{pmatrix} 1 & 2 & \ldots & n \\ i_1 & i_2 & \ldots & i_n \end{pmatrix}$ ili naprosto $f = i_1 i_2 \ldots i_n$. Skup svih tih permutacija možemo urediti na prirodan način, tzv. **leksikografskim** (ili **abecednim**) **uređajem** ovako: permutacija $i_1 i_2 \ldots i_n$ manja je od permutacije $j_1 j_2 \ldots j_n$, što pišemo $i_1 i_2 \ldots i_n <_L j_1 j_2 \ldots j_n$ ako je ili $i_1 < j_1$ ili za neko k, $i_1 = j_1, \ldots, i_{k-1} = j_{k-1}$, $i_k < j_k$. Npr. za $n = 5$, $14352 <_L 14523$. (Ime "leksikografski" dolazi otuda što su u rječniku ili leksikonu tako poredane riječi, koje tamo dolaze abecednim redom, s time da tu dopuštamo ponavljanje slova i smatramo da su sve riječi jednako duge i da je ta duljina jednaka duljini najduže riječi koja se uopće pojavljuje, a to postižemo uvođenjem dodatnog simbola, manjeg od svih slova $a, b, \ldots, \check{z}$ koji pripisujemo na kraju koliko treba, ali ga naravno ne pišemo; npr. baba$<_L$babama$<_L$banana).

Kako se algoritamski može načiniti lista svih permutacija od $[n]$ u leksikografskom poretku?

Rješenje. Počinjemo s leksikografski najmanjom permutacijom $123 \ldots n$. Nadalje, treba znati koja permutacija neposredno slijedi iza dane permutacije $f = i_1 i_2 \ldots i_n$. Ako je $i_{n-1} < i_n$, onda izmjenom mjesta i_{n-1} i i_n dobivamo neposrednog sljedbenika; npr. iza 14325 dolazi odmah 14352. Ako je $i_{n-1} > i_n$, onda izmjenom pozicije od i_{n-1} i i_n u f dobivamo leksikografski manju permutaciju, pa stoga treba ići na i_{n-2}. Ako je $i_{n-2} < i_{n-1}$, onda zadnja tri broja od f treba ispremještati tako da se dobije leksikografski veći niz. Da bi "povećali" naš niz što je moguće manje, na poziciju $n-2$ trebalo bi staviti sljedeći veći broj (tj. veći od i_{n-2}), odabran među i_{n-1} i i_n. Ostala dva među originalnim zadnjim brojevima stave se na pozicije $n-1$ i n u rastućem poretku. Npr., odmah iza 14352 dolazi 14523, a odmah iza 14253 dolazi 14325. Ako je $i_{n-2} > i_{n-1}$ (a istovremeno $i_{n-1} > i_n$), moramo pogledati i_{n-3}.

Općenito, počinjemo zdesna i gledamo prvi par i_k, i_{k+1} tako da je $i_k < i_{k+1}$ (te $i_{k+1} > i_{k+2} > \cdots > i_{n-1} > i_n$). Tada se neposredni sljedbenik dobije tako da se na poziciju k stavi $\min\{i_l | i_l > i_k, l > k\}$, a ostali brojevi $i_k, i_{k+1}, \ldots, i_n$ (osim broja već stavljenog na poziciju k) stave na pozicije $k+1$ do n u rastućem poretku. Tim pravilom za neposrednog

sljedbenika lako se može napisati program za leksikografsku listu svih permutacija od $\{1, 2, \ldots, n\}$. Npr. za $n = 3$ ta je lista 123, 132, 213, 231, 312, 321. Postoje i "brži" algoritmi za listu svih permutacija. Takvi algoritmi nalaze neposrednog sljedbenika na listi s manje koraka (čak sa samo jednom izmjenom i_k i i_l), ali takvi algoritmi "listaju" permutacije ne u leksikografskom, nego u nekom drugom "neprirodnom" poretku. Više o tome može se naći u knjigama [123], [124]. □

Budući da permutaciju možemo na više načina prikazati u obliku produkta disjunktnih ciklusa, obično se stoga odlučujemo za tzv. **standardni ciklički zapis permutacije**. Tu zahtijevamo da svaki ciklus počne s najvećim elementom i da su ciklusi zapisani po uzlaznom redu najvećih (prvih) elemenata.

Na primjer, permutacija $\pi \in S_9$, $\pi = 579482613$ ima standardni ciklički zapis $\pi = (4)(762)(815)(93)$.

Ako u standardnom cikličkom zapisu permutacije π izbrišemo sve zagrade, dobijemo riječ (tj. permutaciju) π'. Na primjer, ako je $\pi = (4)(762)(815)(93)$, onda je $\pi' = 476281593$. No, uočite da se π može rekonstruirati iz π' i to tako da se u $\pi' = i_1 i_2 \ldots i_n$ prvo umetnu lijeve zagrade prije pojave svakog elementa i_k takvog da je $i_k > i_l$ za svako $l < k$ (takav i_k se zove **maksimum slijeva na desno**), pa se nakon toga umetnu desne zagrade prije svake unutarnje lijeve i na sam kraj. Na primjer, ako pođemo od permutacije $\pi' = 476281593$, onda prvo stavimo lijeve zagrade prema gornjem algoritmu: (4(762(815(93, pa onda na odgovarajuća mjesta desne zagrade: (4)(762)(815)(93). Tako smo dobili standardni ciklički zapis permutacije π kao gore. Jasno je stoga da smo time dobili jednu bijekciju $\pi \mapsto \pi'$ iz S_n u samu sebe.

Neka je $\pi \in S_n$ bilo koja permutacija. Označimo s $c_i = c_i(\pi)$ broj ciklusa od π duljine i (dakle, c_1 je broj 1-ciklusa, tj. fiksnih točaka od π, c_2 broj 2-ciklusa, tj. transpozicija, c_3 broj 3-ciklusa, ..., a c_n broj n-ciklusa od π). Očito je $c_1, c_2, \ldots, c_n \geq 0$ i $c_1 + 2c_2 + \cdots + nc_n = n$. Definiramo **ciklički tip** od π kao niz $(c_1, c_2, \ldots, c_n)$. Ukupni broj ciklusa od π tada je $c_1 + c_2 + \cdots + c_n$. Na primjer, permutacija $\pi \in S_9$, $\pi = 437186295$ ima ciklički rastav $\pi = (41)(6)(723)(958)$. Ciklički tip od π je $(1, 1, 2, 0, 0, 0, 0, 0, 0)$.

Prirodno pitanje je koliko ima permutacija zadanog cikličkog tipa?

PROPOZICIJA 5. *Broj permutacija od n elemenata cikličkog tipa $(c_1, \ldots, c_n)$ jednak je*

$$\frac{n!}{1^{c_1} c_1! 2^{c_2} c_2! \ldots n^{c_n} c_n!}.$$

Dokaz. Svaku permutaciju iz S_n cikličkog tipa $(c_1, \ldots, c_n)$ možemo ovako predstaviti:

$$\underbrace{(*)(*)\ldots(*)}_{c_1}\ \underbrace{(**)(**)\ldots(**)}_{c_2}\ \cdots\ \underbrace{(*\,*\cdots*)\ldots(*\,*\cdots*)}_{c_n}.$$

Tih n simbola $*$ (tj. n mjesta) možemo ukupno popuniti brojevima od 1 do n na $n!$ načina. Među tih $n!$ zapisa bit će i različitih zapisa iste permutacije, pa izbrojimo koliko takvih ima. Kao što već znamo, svaki ciklus duljine i možemo unutar dane zagrade napisati na i načina, pa c_i takvih ciklusa možemo zapisati na

i^{c_i} načina. Svih c_i ciklusa duljine i možemo ispremiješati na $c_i!$ načina, pa prema pravilu množenja, cikluse duljine i možemo zapisati ukupno na $i^{c_i} \cdot c_i!$ načina. To vrijedi za svako $i \in [n]$, pa opet prema pravilu množenja dobivamo da ukupno imamo $N = 1^{c_1} c_1! 2^{c_2} c_2! \ldots n^{c_n} c_n!$ načina zapisa svake permutacije cikličkog tipa $(c_1, c_2, \ldots, c_n)$. Zato $n!$ treba podijeliti s N da se dobije broj permutacija tog tipa, pa je $\frac{n!}{N}$ broj permutacija cikličkog tipa $(c_1, \ldots, c_n)$. □

Kako svih permutacija od $[n]$ ima $n!$, zbrajanjem svih izraza iz Propozicije 5 dobivamo $n!$, pa skraćivanjem s $n!$ slijedi tzv. **Cauchyjev identitet**

$$\sum \frac{1}{1^{c_1} c_1! 2^{c_2} c_2! \ldots n^{c_n} c_n!} = 1,$$

gdje se sumira po svim $(c_1, \ldots, c_n) \in \mathbb{N}_0^n$ za koje je $\sum i c_i = n$.

Za opis permutacije često nam je važno znati koliko ima permutacija u S_n sa zadanim brojem ciklusa. Zato definiramo broj $c(n, k)$ kao broj permutacija $\pi \in S_n$ s točno k ciklusa, a

$$s(n, k) := (-1)^{n-k} c(n, k).$$

$c(n, k)$ se zove **Stirlingov** [3] **broj prve vrste** ili **Stirlingov ciklički broj**, a $s(n, k)$ **Stirlingov broj prve vrste s predznakom**. Za $c(n, k)$ je često u literaturi u upotrebi i simbol $\left[{n \atop k}\right]$. O tim će brojevima više riječi biti poslije.

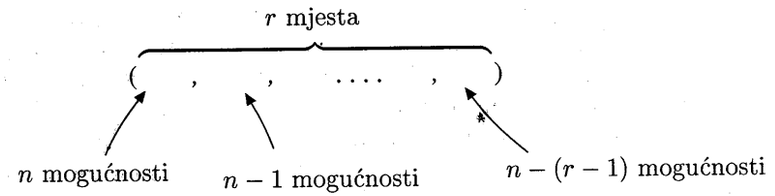
Još jedna interpretacija padajućih faktorijela je sljedeća. Neka je S skup od n elemenata, a $r \in \mathbb{N}$. Definiramo da je **r-permutacija** skupa S uređena r-torka $(x_1, x_2, \ldots, x_r)$ međusobno različitih elemenata x_i iz S. Označimo s $P(n, r)$ broj r-permutacija n-članog skupa. Dodatno definiramo da je $P(n, 0) := 1$. n-permutacija n-članog skupa je očito permutacija tog skupa, pa je $P(n, n) = n!$, a za $r > n$ je jasno da je $P(n, r) = 0$, jer je očito da ne postoje npr. 3-permutacije 2-članog skupa, pa je njihov broj nula. Sve 2-permutacije 3-članog skupa $S = \{a, b, c\}$ su ab, ac, ba, ca, bc, cb (ovdje bi trebalo pisati (a, b) umjesto ab itd.), a sve 3-permutacije ili naprosto permutacije od $\{a, b, c\}$ su abc, acb, bac, bca, cab, cba. Vidimo da je $P(3, 2) = P(3, 3) = 6$. Očito je $P(n, 1) = n$. Spomenimo da se u starijoj literaturi r-permutacija n-članog skupa zove još i **varijacija** r-tog **razreda bez ponavljanja od n elemenata**.

PROPOZICIJA 6. *Broj r-permutacija n-članog skupa jednak je*

$$n^{\underline{r}} = n(n-1)\ldots(n-r+1).$$

Dokaz I. Pitamo se na koliko načina možemo popuniti tablicu (, , ... ,) od r mjesta s različitim elementima n-članog skupa S (usp. rješenje Primjera 19). Na prvo mjesto (komponentu) možemo odabrati bilo koji od n elemenata iz S. Nakon što smo odabrali prvu komponentu, na drugo mjesto možemo odabrati bilo koji od preostalih $n - 1$ elemenata iz S itd. Shematski:

[3] James Stirling (1692 – 1770), škotski matematičar



Ukupno, dakle, imamo prema pravilu produkta $n(n-1)\dots(n-r+1) = n^{\underline{r}}$ mogućnosti. □

Dokaz II. (Svođenje na poznati rezultat). Neka je $|S| = n$. Označimo s $\mathrm{Per}(r,S)$ skup svih r-permutacija od S. Nađimo bijekciju između tog skupa i skupa $S^{\underline{[r]}}$ svih injekcija $[r] \to S$. Za $x = (x_1, x_2, \dots, x_r) \in \mathrm{Per}(r,S)$ definirajmo $\varphi(x) = f \in S^{\underline{[r]}}$ sa $f(i) = x_i$, $i = 1, 2, \dots, r$. Sada je lako provjeriti da je $\varphi : \mathrm{Per}(r,S) \to S^{\underline{[r]}}$ bijekcija (što je inverz?), pa tvrdnja slijedi iz Propozicije 4. □

Primjer 25. Koliko ima uređenih parova različitih slova abecede od 30 slova, tj. "riječi" s dva različita slova. Koliko ima takvih "riječi" s 3, 4, 5 i 6 slova?

Rješenje. Takvih riječi od 2 slova očito ima $P(30,2) = \frac{30!}{(30-2)!} = \frac{30!}{28!} = 30 \cdot 29 = 870$. Takvih "riječi" s 3 slova ima $P(30,3) = \frac{30!}{(30-3)!} = \frac{30!}{27!} = 30 \cdot 29 \cdot 28 = 24360$, s četiri slova $P(30,4) = 24360 \cdot 27 = 657720$, s pet slova $P(30,5) = 657720 \cdot 26 = 17100720$, a onih sa šest slova $P(30,6) = P(30,5) \cdot 25 = 427518000$ (dakle, oko pola milijarde). Neke riječi od 6 različitih slova su primjerice *abcdef*, *bacdef*,..., *fedbac*, ..., *mozaik*, ..., *žzvutš* (i ove 6-permutacije od 30 slova se na sličan način mogu leksikografski izlistati kao i sve permutacije nekog skupa). □

Iz ovog je primjera jasno da i općenito za $k \le n$ vrijedi rekurzija:

$$P(n,k) = (n-k+1)P(n,k-1),$$

što se lako dokaže (za čvrsto n) indukcijom po k. Ako izmnožimo sve ove jednakosti za $k = 1, 2, \dots, r$, dobivamo još jedan dokaz Propozicije 6. A ako pak redom uvrštavamo $k = n, n-1, \dots, 1$ dobivamo još jedan dokaz Korolara 2 da permutacija od n objekata ima $n!$. Prve dokumentirane primjere Propozicija 4 i 6 i Korolara 2 nalazimo već u anonimnom hebrejskom mističnom djelu "Sefer Yetzirah" ("Knjiga postanka") pisanom između III. i VI. st.

Osim običnih faktorijela definiraju se i tzv. **dvostruki faktorijeli**

$$(2n)!! := 2 \cdot 4 \cdot 6 \cdot \dots \cdot 2n = 2^n \cdot n! \text{ i } (2n-1)!! := 1 \cdot 3 \cdot 5 \cdot \dots \cdot (2n-1);$$

množenjem i dijeljenjem s $2 \cdot 4 \cdot \dots \cdot 2n$, odavde dobivamo

$$(2n-1)!! = \frac{(2n)!}{2^n \cdot n!}.$$

Bilješka. S permutacijama (i faktorijelima) još ćemo se puno susretati. One su, primjerice, važne u analizi raznih algoritama sortiranja. Neki efikasni algoritmi o grafovima ili geometrijskim objektima često počinju tako da ulazne objekte preurede

u slučajni poredak, tj. u slučajnu permutaciju. Tako se one prirodno javljaju u (teorijskom) računarstvu. Grupe permutacija su važne ne samo u teoriji grupa, nego u gotovo čitavoj matematici, ali i suvremenoj fizici. Ustvari, svaka konačna grupa G reda n je izomorfna nekoj podgrupi simetrične grupe S_n. Naime, neka je $S(G)$ grupa bijekcija od G. Definirajmo $\varphi : G \to S(G)$ sa $\varphi(x) = f_x \in S(G)$, gdje je $f_x(a) = xax^{-1}$ za $x, a \in G$. φ je monomorfizam, pa je $G \approx \varphi(G)$, a $\varphi(G)$ je podgrupa od $S(G) \approx S_n$. To je poznati **Cayleyev teorem**. Osnovni razlog algebarske nerješivosti opće algebarske jednadžbe stupnja ≥ 5 leži u činjenici da je grupa permutacija S_5 nerješiva. Prebrojavanje izvjesnih izomera organskih molekula u kemiji, analiza miješanja igraćih karata itd. još su neke "konkretne" instance gdje je proučavanje permutacija od osnovne važnosti.

Osim cikličke strukture permutacije $\pi \in S_n$, osnovne statistike koje dobro opisuju permutaciju su inverzije i padovi. Mi ćemo sada samo definirati te pojmove, a njihova važna svojstva ćemo proučavati kasnije.

Dakle, **inverzija** permutacije $\pi = i_1 i_2 \dots i_n \in S_n$ je par (i_k, i_l) za koji je $k < l$, a $i_k > i_l$. $a_j := \#\{i \in [n] | (i,j) \text{ je inverzija od } \pi\}$, a $I(\pi) = (a_1, a_2, \dots, a_n)$ se zove **niz inverzija** od π, dok je $i(\pi) = |I(\pi)| = a_1 + a_2 + \dots + a_n$ **broj inverzija** od π. **Skup padova** od $\pi \in S_n$ definira se kao skup $D(\pi) = \{k \in [n] | i_k > i_{k+1}\}$, a broj $d(\pi) = |D(\pi)|$ kao **broj padova** od π. Na to ćemo se još vratiti.

O procjeni $n!$

Koliko je zapravo velik $n!$?

Funkcija $n \mapsto n!$ vrlo brzo raste, npr. $7! = 5040$, $10! = 3628800$, $20! = 2432902008176640000$. Ona raste brže od eksponencijalne funkcije, jer za $n \ge 3$ je očito $2 \cdot 2 \cdot \dots \cdot 2 = 2^{n-1} < n(n-1) \cdot \dots \cdot 2 = n! < n \cdot n \cdot \dots \cdot n = n^n$. No, vrijedi i bolja procjena

$$n^{n/2} < n! < \left(\frac{n+1}{2}\right)^n.$$

Desna nejednakost je aritmetičko-geometrijska za brojeve $1, 2, \dots, n$, a lijeva slijedi iz toga što je $k(n-k+1) \ge n$, tj. $(k-1)(k-n) \le 0$, pa imamo:

$$(n!)^2 = [1 \cdot n] \cdot [2 \cdot (n-1)] \cdot \dots \cdot [k \cdot (n-k+1)] \cdot \dots \cdot [n \cdot 1] = \prod_{k=1}^{n} [k \cdot (n-k+1)] \ge \prod_{k=1}^{n} n = n^n.$$

Ova procjena je prilično gruba. Bolja procjena je ova

$$e\left(\frac{n}{e}\right)^n \le n! \le e\sqrt{n}\left(\frac{n}{e}\right)^n. \qquad (*)$$

Osnovni razlog za ovu procjenu su sljedeće nejednakosti:

$$1 + x \le e^x, 1 + x + x^2/2 \le e^x, \text{ itd. , za svaki } x \ge 0.$$

Ove nejednakosti "vidimo" tako da nacrtamo grafove funkcija $y = 1 + x$ i $y = e^x$ (nacrtajte sliku).

Sada rabeći tu nejednakost nije teško indukcijom dokazati (∗). Mi ćemo desnu nejednakost u (∗) izvesti drukčije (lijevu je lakše izvesti).

Logaritmirajmo $n! = 1 \cdot 2 \cdot \cdots \cdot n$. Tada dobivamo

$$\ln n! = \ln 1 + \ln 2 + \cdots + \ln n.$$

Izraz na desnoj strani je površina ispod stepeničaste krivulje $y = \ln\lfloor x \rfloor$ na segmentu $[1, n+1]$. Kako je $\lfloor x \rfloor \leq x$, slijedi da je ta površina $\leq$ površine ispod grafa funkcije $y = \ln x$ na $[1, n+1]$. Stoga je (vidi donju sliku):

$$\ln n! \leq \int_1^{n+1} \ln x dx = (n+1)\ln(n+1) - n,$$

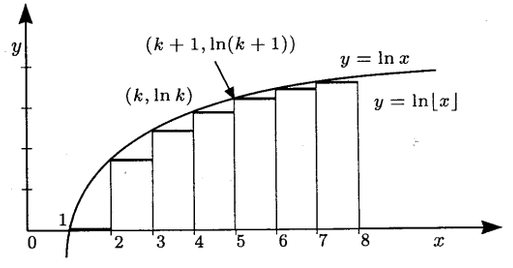
a odatle

$$n! \leq e^{(n+1)\ln(n+1)-n} = \frac{(n+1)^n}{e^n},$$

tj. (pišemo li $n-1$ umjesto n), dobivamo

$$n! = n \cdot (n-1)! \leq n \cdot \frac{n^n}{e^{n-1}} = e \cdot n \left(\frac{n}{e}\right)^n.$$

To još nije desna strana od (∗). Uočimo da zbog konkavnosti krivulje $y = \ln x$, svi trokutići s vrhovima $(k, \ln k), (k+1, \ln k), (k+1, \ln(k+1))$ leže ispod krivulje $y = \ln x$, pa je zbroj površina pravokutnika i trokutića $\leq$ površine ispod $y = \ln x$ na $[1, n+1]$.



Kako je površina trokutića $\frac{1}{2}(\ln(k+1) - \ln(k)$, slijedi (kao gore):

$$\ln n! \leq \ln n + \int_1^n \ln x dx - \frac{1}{2}\sum_{k=1}^{n-1}(\ln(k+1) - \ln k).$$

Odavde (s malo računanja) slijedi desna strana (∗):

$$n! \leq e\sqrt{n}\left(\frac{n}{e}\right)^n.$$

Ovaj izvod potječe od W. Fellera[4]. Ta je procjena već vrlo bliska **Stirlingovoj aproksimaciji (asimptotskoj formuli)** (za dokaz vidi [123]):

$$n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n,$$

ili još točnije

$$n! = \sqrt{2\pi n}\left(\frac{n}{e}\right)^n (1 + \frac{1}{12n} + \frac{1}{128n^2} + O(\frac{1}{n^3})).$$

(Podsjetimo, $f(n) \sim g(n)$, ako $\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1$, a $f(n) = O(g(n))$ ako postoji konstanta K tako da je $\frac{f(n)}{g(n)} \leq K$ za gotovo sve n.) Proširenje od $n!$ je tzv. **gama funkcija** Γ, koja je za $x > 0$ definirana s

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt.$$

Parcijalnom se integracijom lako dobiva da je $\Gamma(x+1) = x\Gamma(x)$, a zbog $\Gamma(1) = 1$ slijedi $\Gamma(n+1) = n!$.

§ 4. Kombinacije skupova

Neka je S bilo koji skup, a $r \geq 0$ cijeli broj. Bilo koji r-člani podskup od S zove se r-**kombinacija** [5] **skupa** S. Drugim riječima r-kombinacija od S je (neuređeni) izbor od r elemenata iz S. Skup svih r-kombinacija od S bilježimo simbolom

$$\binom{S}{r},$$

ili katkada $\mathcal{P}_r(S)$.

Na primjer, $\binom{\{a,b,c,d\}}{3} = \{\{a,b,c\}, \{a,b,d\}, \{a,c,d\}, \{b,c,d\}\}$.

S druge strane, broj svih r-kombinacija n-članog skupa bilježimo simbolom (čitaj n povrh r, ili n iznad r, engleski se čita "n choose r"):

$$\binom{n}{r},$$

i zovemo ga **binomni koeficijent** (poslije će postati jasno zašto taj naziv). Dodatno definiramo $\binom{0}{0} := 1$. Ako je $r > n$, onda je jasno da je $\binom{n}{r} = 0$, a ako je $n = 0$, a $r \in \mathbb{N}$, onda je $\binom{0}{r} = 0$. Isto je tako jasno da je $\binom{n}{0} = 1$, $\binom{n}{1} = n$, a $\binom{n}{n} = 1$.

Pojam kombinacije toliko je fundamentalan da se čitava grana matematike kojom se ovdje bavimo naziva prema tome pojmu kombinatorna matematika ili kombinatorika.

Katkad se (punim nazivom) r-kombinacija skupa S zove i r-**kombinacija od** S **bez ponavljanja**. Poslije ćemo promatrati i r-kombinacije s ponavljanjem.

Sada izvedimo osnovnu formulu za broj kombinacija (bez ponavljanja).

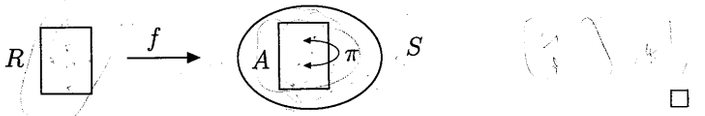
[4] William (Vilim) Feller (1906 – 1970), američki matematičar hrvatskog podrijetla. Rođen u Zagrebu, gdje je započeo studij. 1925. studij nastavlja u Göttingenu i poslije emigrira u SAD. Osnivač referalnog časopisa *Mathematical Reviews* 1939. godine. Profesor na Princeton University 1950. – 1970.

[5] Od lat. *combinare* – slagati, odabirati, izabirati. Hrvatski bi se stoga za kombinaciju moglo reći odabir, ali se to nije udomaćilo.

PROPOZICIJA 7. *Neka je S konačni skup, $|S| = n$, a $r \geq 0$ cijeli broj. Tada je broj r-kombinacija od S jednak*

$$\binom{n}{r} = \frac{n^{\underline{r}}}{r!} = \frac{n(n-1)(n-2)\cdot\cdots\cdot(n-r+1)}{r!}. \qquad (*)$$

Dokaz. Dovoljno je dokazati jednakost $\binom{n}{r} r! = n^{\underline{r}}$. Neka je R skup sa $|R| = r$ elemenata. Desna strana ove jednakosti (prema Propoziciji 4) broji sve injekcije $f : R \to S$. S druge strane, svaku injekciju $f : R \to S$ dobijemo tako da prvo odaberemo neki r-člani podskup A od S, što možemo učiniti na $\binom{n}{r}$ načina, pa onda taj podskup "ispremiješamo" (tj. permutiramo s permutacijom π) na sve moguće načine, što možemo učiniti na $r!$ načina. Time je navedena jednakost dokazana. Formalno, $f \mapsto (A, \pi)$ je bijekcija $S^{\underline{R}} \to \binom{S}{r} \times S_r$. Sugestivna sličica za "vizualce":



□

Simbolima i kratko, Propozicija 7 kaže naprosto

$$\left|\binom{S}{r}\right| = \binom{|S|}{r}.$$

Ako desnu stranu formule $(*)$ pomnožimo i podijelimo s $(n-r)!$ dobijemo

$$\binom{n}{r} = \frac{n!}{r!(n-r)!}.$$

Vezu između r-permutacije i r-kombinacije možemo sada slobodno iskazati ovako: sve r-permutacije dobivamo tako da ispermutiramo (na sve moguće načine) sve r-kombinacije.

Sam pojam kombinacije je također vrlo star, no izgleda da je oznaku $\binom{n}{r}$ prvi uveo Andreas von Ettingshausen (1796 - 1878).

Primjer 26. a) Od 12 košarkaša u igri je uvijek samo njih 5. Koliko takvih petorki ima ukupno?

b) Izbornik nogometne reprezentacije "Ć" mora od 22 nogometaša izabrati njih 11, ali za petoricu svojih favorita već je odlučio. Na koliko načina "Ć" može izabrati momčad?

Rješenje. a) Traženi je broj jednak broju 5-kombinacija skupa od 12 elemenata, a taj je broj jednak

$$\binom{12}{5} = \frac{12\cdot 11\cdot 10\cdot 9\cdot 8}{1\cdot 2\cdot 3\cdot 4\cdot 5} = 792;$$

b) Nakon dugog i dubokoumnog razmišljanja te neprospavane noći, izbornik "Ć" je napokon shvatio da je broj načina da izabere momčad jednak

$$\binom{22-5}{11-5} = \binom{17}{6} = \frac{17\cdot 16\cdot 15\cdot 14\cdot 13\cdot 12}{1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6} = 12376.$$

□

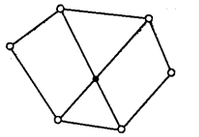
Primjer 27. Na šahovskom turniru svaki je igrač odigrao sa svakim od preostalih jednu partiju. Ukupno je odigrano 78 partija. Koliko je šahista sudjelovalo na turniru?

Rješenje. Neka je n broj šahista na turniru. Tada je broj odigranih partija jednak $\binom{n}{2}$. Dakle $\binom{n}{2} = 78$, tj. $\frac{n(n-1)}{2} = 78$, a odatle se dobije traženi broj $n = 13$. □

Primjer 28. Koliko ima dužina, a koliko trokuta s vrhovima u n zadanih točaka u ravnini koje su u **općem položaju** (tj. nikoje 3 nisu na istom pravcu)?

Rješenje. Nikoja trojka točaka nije kolinearna, pa svaki par točaka određuje jedinstvenu dužinu (pa stoga i pravac). Zato je broj dužina jednak $\binom{n}{2}$. Zbog općeg položaja, svaka trojka točaka određuje jedinstveni trokut, pa je broj trokuta jednak $\binom{n}{3} = \frac{n(n-1)(n-2)}{6}$. □

Primjer 29. Neka je konveksni n-terokut takav da se nikoje tri dijagonale ne sijeku u jednoj (unutrašnjoj) točki. Koliko ima presječnih točaka dijagonala?



Rješenje. Svakoj unutrašnjoj presječnoj točki odgovara skup od 4 vrha poligona (krajevi dviju dijagonala), a svaka četvorka vrhova daje jednu takvu presječnu točku. Stoga je traženi broj jednak broju četvorki vrhova n-terokuta, tj. $\binom{n}{4}$. □

Primjer 30. Od 7 žena i 4 muškaraca treba izabrati delegaciju. Na koliko se načina može izabrati delegacija tako da se ona sastoji od

a) petero ljudi, i to 3 žene i 2 muškarca,

b) bilo kojeg broja ljudi, ali mora biti jednako žena i muškaraca,

c) petero ljudi, od kojih su bar dvije žene,

d) petero ljudi, s tim da jedan od njih bude već unaprijed određena žena,

e) šestero ljudi, po troje oba spola, s tim da u delegaciju ne mogu ući zajedno po jedan unaprijed određeni muškarac i žena?

Rješenje. a) 3 žene mogu se izabrati na $\binom{7}{3}$ načina, a 2 muškarca na $\binom{4}{2}$ način. Prema pravilu produkta traženi je broj $\binom{7}{3}\cdot\binom{4}{2} = 210$.

b) Mogućnosti su da se izabere po jedna osoba svakog spola, po dvije, tri i četiri. Primjenom pravila produkta i sume nalazimo da je traženi broj jednak

$$\binom{7}{1}\binom{4}{1} + \binom{7}{2}\binom{4}{2} + \binom{7}{3}\binom{7}{3} + \binom{7}{4}\binom{4}{4} = 329.$$

c) Moglo bi se pomisliti da se taj problem može riješiti jednostavno ovako: odaberemo prvo dvije žene, to se može učiniti na $\binom{7}{2} = 21$ način, pa onda još tri od preostalih 9 osoba (5 žena i 4 muškarca) na $\binom{9}{3} = 63$ načina. Odgovor bi tada bio $21\cdot 63 = 1296$. No to nije dobro (zašto?). Ispravno se rješenje dobije opet tako da se razmatraju razne mogućnosti kao u b), tj. da se problem razbije na 3 podslučaja: 2 žene i 3 muškarca, 3 žene i 2 muškarca, 4 žene i 1 muškarac te 5 žena. Stoga je traženi broj jednak: $\binom{7}{2}\binom{4}{3} + \binom{7}{3}\binom{4}{2} + \binom{7}{4}\binom{4}{1} + \binom{7}{5} = 455$.

d) Ako već određena žena mora biti u delegaciji, to jednostavno znači da se od preostalih 10 ljudi (6 žena i 4 muškarca) mora odabrati četvero. Traženi je broj stoga $\binom{10}{4} = 210$.

e) Tri žene i tri muškarca mogu se izabrati na $\binom{7}{3}\binom{4}{3}$ načina. Od tog broja treba oduzeti broj onih delegacija u kojima već jesu odabrani muškarac i žena. Njih je $\binom{6}{2}\binom{3}{2}$. Traženi je broj jednak $\binom{7}{3}\binom{4}{3} - \binom{6}{2}\binom{3}{2} = 95$.

□

Primjer 31. Zadan je skup $V = \{v_1, v_2, \ldots, v_n\}$ od n vrhova. Koliko ima jednostavnih grafova kojima je V skup vrhova?

Rješenje. Jednostavni graf sa skupom vrhova V potpuno je određen time koje dvočlane podskupove $\{v_i, v_j\}$ uzimamo kao bridove. Prema tome, tih grafova ima koliko i svih podskupova skupa $\binom{V}{2}$ svih 2-članih podskupova od V. Zato je traženi broj jednak $2^{\binom{n}{2}}$. I ovdje imamo "kombinatornu eksploziju", jer npr. već za $n = 7$ imamo više od 268 milijuna grafova sa 7 vrhova (od kojih su mnogi izomorfni). □

Primjer 32. a) Koliko se osmoslovnih različitih riječi može načiniti od 30 slova abecede?

b) Isto pitanje kao a), ali tako da svaka riječ mora sadržavati točno 3 različita (od ukupno 5) samoglasnika i točno 5 (od ukupno 25) različitih suglasnika.

c) Isto pitanje kao a), ali tako da svaka riječ sadrži ili 3 ili 4 ili 5 (ne nužno različitih) samoglasnika?
(U problemima a) i c) smatramo da nema restrikcija u ponavljanju slova u riječi.)

Rješenje. a) Na svaku od 8 pozicija možemo stavljati bilo koje od 30 slova (a,b,...,ž). Prema pravilu produkta, takvih riječi ima $30 \cdot 30 \cdot \cdots \cdot 30 = 30^8 = 656,1 \cdot 10^9$, tj. više od 656 milijardi.

b) 3 različita samoglasnika možemo birati na $\binom{5}{3}$ načina, a 5 različitih suglasnika na $\binom{25}{5}$ načina. Od 8 slova (3 samoglasnika i 5 suglasnika) možemo načiniti 8! poredaka. Prema pravilu produkta, traženi je broj jednak $\binom{5}{3}\binom{25}{5}8! = 21422000000$.

c) Računajmo broj riječi s obzirom na broj samoglasnika koje sadrži.

Tri samoglasnika: 3 pozicije (od njih 8) na kojima su samoglasnici možemo izabrati na $\binom{8}{3}$ načina. Na ostalih su 5 mjesta suglasnici. Na mjestima samoglasnika možemo slobodno stavljati bilo koji od njih 5; dakle, s njima (na nekoj određenoj poziciji) imamo 5^3 mogućnosti, a na preostalih 5 mjesta možemo slobodno birati suglasnike na 25^5 načina. Prema pravilu produkta, broj riječi s točno 3 samoglasnika je $\binom{8}{3}5^3 25^5$.

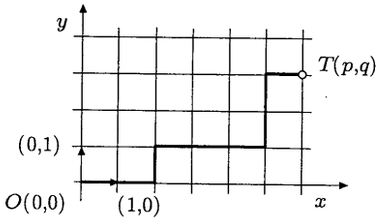
Četiri samoglasnika: Sličnim argumentiranjem dobijemo $\binom{8}{5}5^4 25^4$. Pet samoglasnika: $\binom{8}{5}5^5 25^3$.

Prema pravilu sume traženi je broj

$$\binom{8}{3}5^3 25^5 + \binom{8}{4}5^4 25^4 + \binom{8}{5}5^5 25^3 = 88182300000, \text{ tj. više od 88 milijardi.}$$

□

Primjer 33. Cjelobrojna mreža u koordinatnom sustavu u ravnini je unija pravaca paralelnih s osima kroz sve cjelobrojne točke. (Točnije, to je beskonačni graf sa skupom vrhova $V = \mathbb{Z}^2$, a bridovi su sve dužine s jednim krajem u (x, y), a drugim $(x \pm 1, y)$ ili $(x, y \pm 1)$, pri čemu su $x, y \in \mathbb{Z}$.) **Najkraći put** u toj mreži od ishodišta $O(0,0)$ do $T(p,q)$ je niz bridova te mreže koji počinje u O, a završava u T i kod kojeg su dopušteni pomaci tipa $(1,0)$ ili $(0,1)$. Koliko ima takvih najkraćih putova?



x x y x x x y y y x

Rješenje. Svaki takav put sastoji se od p pomaka u smjeru x (tj. tipa $(1,0)$) i q pomaka u smjeru y (tj. tipa $(0,1)$). Prema tome, svaki put možemo kodirati nizom x-ova i y-ova, ukupno njih $p+q$, od čega je p x-ova (i stoga q y-ova). Traženi je broj stoga jednak $\binom{p+q}{p}$. □

Navedimo sada neka jednostavna i važna svojstva binomnih koeficijenata. Mi ćemo uvijek nastojati dati kombinatorne dokaze, iako se mnoge formule mogu dokazati i algebarskim manipuliranjem rabeći formulu $\binom{n}{r} = \frac{n!}{r!(n-r)!}$.

PROPOZICIJA 8. *Za cijele brojeve $n, r \geq 0$ vrijedi:*

a) $\binom{n}{r} = \binom{n}{n-r}$ *(tj.* **simetrija binomnih koeficijenata***);*

b) $\sum_{k=0}^{n} \binom{n}{k} = 2^n$ *(tj. zbroj binomnih koeficijenata s "brojnikom" n je 2^n);*

c) $\binom{n}{r} = \frac{n}{r}\binom{n-1}{r-1}$, $r \neq 0$, *odnosno* $r\binom{n}{r} = n\binom{n-1}{r-1}$ *za sve r, n (pri tome smatramo da je* $\binom{p}{-1} = 0$*) (***svojstvo apsorpcije binomnih koeficijenata***);*

d) $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$ *(***Pascalova formula***);*

e) $\sum_{k=0}^{r} \binom{n+k}{k} = \binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+r}{r} = \binom{n+r+1}{r}$ *(tj. razlika "brojnika" i "nazivnika" je stalna);*

f) $\sum_{k=0}^{n-r} \binom{r+k}{r} = \binom{r}{r} + \binom{r+1}{r} + \cdots + \binom{n}{r} = \binom{n+1}{r+1}$ *(tj. "nazivnik" je stalan);*

g) $\binom{n}{r}\binom{r}{k} = \binom{n}{k}\binom{n-k}{r-k}$, *za svako k. (***pravilo produkta za binomne koeficijente***);*

Dokaz. a) Algebarski: $\binom{n}{r} = \frac{n!}{r!(n-r)!} = \frac{n!}{(n-(n-r))!(n-r)!} = \binom{n}{n-r}$. Kombinatorno: Neka je S n-člani skup. Preslikavanje $\binom{S}{r} \to \binom{S}{n-r}$, $A \mapsto S \setminus A$ koje r-članom skupu pridružuje njegov komplement je bijekcija. Drugi kombinatorni dokaz slijedi iz rješenja prethodnog primjera. Naime, ako od $p+q$ mjesta na kojima su x i y biramo q mjesta na kojima je y, opet dobivamo broj najkraćih putova po cjelobrojnoj mreži $\binom{p+q}{q}$. Stoga je $\binom{p+q}{p} = \binom{p+q}{q}$. Stavimo li ovdje $p+q = n$ i $p = r$, opet dobivamo a).

b) Svi podskupovi od $[n]$ mogu biti 0-člani, 1-člani, 2-člani, itd. ili n-člani. Stoga je lijeva strana ukupni broj podskupova od $[n]$. Znamo (Propozicija 3) da je ukupni broj podskupova od $[n]$ također jednak 2^n, pa odatle slijedi tvrdnja. Algebarski dokaz dat ćemo poslije.

c) $r\binom{n}{r}$ je broj uređenih parova (A, x), gdje je $A \in \binom{[n]}{r}$, a $x \in A$, dok je $n\binom{n-1}{r-1}$ broj uređenih parova (y, B), gdje je $y \in [n]$, a $B \in \binom{[n]\setminus\{y\}}{r-1}$. Bijekcija među ovim skupovima uređenih parova je:

$$(A, x) \mapsto (x, A \setminus \{x\}).$$

Inverzno preslikavanje mu je (provjerite to):

$$(y, B) \mapsto (B \cup \{y\}, y).$$

Algebarski dokaz formule c) je trivijalan.

d) I Pascalova formula se može jednostavno provjeriti algebarski. Kombinatorni dokaz je ovaj. Neka je S skup od n elemenata (npr. jabuka). Lijeva strana je broj r-podskupova od S. Neka je $a \in S$ neki čvrst element (npr. trula jabuka). Rastavimo skup $\binom{S}{r}$ svih r-kombinacija od S u dvije (disjunktne) klase A i B. $A = \{R \in \binom{S}{r} | a \in R\}$, tj. u A su sve r-kombinacije od S koje sadrže a (trulu jabuku), dok su u B sve ostale, tj. one koje ne sadrže a. Očito je $|A|$ = broj $(r-1)$-kombinacija $R \setminus \{a\}$ od $S \setminus \{a\}$, a njih je $\binom{n-1}{r-1}$, dok je $|B|$ = broj r-kombinacija od $S \setminus \{a\}$, a njih je $\binom{n-1}{r}$. Prema pravilu zbroja, imamo $\binom{n}{r} = \binom{n-1}{r-1} + \binom{n-1}{r}$.

e) Iz Pascalove formule imamo redom $\binom{n+r+1}{r} = \binom{n+r}{r} + \binom{n+r}{r-1} = \binom{n+r}{r} + \binom{n+r-1}{r-1} + \binom{n+r-1}{r-2} = \binom{n}{r} + \binom{n+r-1}{r-1} + \binom{n+r-2}{r-2} + \binom{n+r-2}{r-3} = \cdots = \binom{n+r}{r} + \binom{n+r-1}{r-1} + \cdots + \binom{n+1}{1} + \binom{n}{0}$.

f) Ustvari, formule e) i f) su ekvivalentne, što slijedi iz simetrije $\binom{r+k}{r} = \binom{r+k}{k}$ i uz zamjene $n \leftrightarrow r$, odnosno $r \leftrightarrow n - r$. Dokažimo sada kombinatorno formulu f). Zapišimo je prvo u ekvivalentnom obliku

$$\sum_{o \le m \le n} \binom{m}{r} = \binom{0}{r} + \binom{1}{r} + \cdots + \binom{r-1}{r} + \binom{r}{r} + \cdots + \binom{n}{r} = \binom{n+1}{r+1}.$$

Desna strana kaže na koliko načina možemo odabrati $r+1$ kino-karata od njih $n+1$ koje su numerirane brojevima od 0 do n. Ako je najveća odabrana karta m, onda je broj takvih izbora $\binom{m}{r}$. Iz pravila sume slijedi tvrdnja.

g) Lijeva strana $\binom{n}{r}\binom{r}{k}$ broji uređene parove (A_1, A_2) skupova, gdje je A_1 r-člani podskup od $[n]$, a A_2 k-člani podskup od A_1. Desna strana $\binom{n}{k}\binom{n-k}{r-k}$ broji uređene parove (B_1, B_2) skupova, gdje je B_1 k-člani podskup od $[n]$, a B_2 $(r-k)$-člani podskup iz $[n] \setminus B_1$. Između skupova objekata koji prebrojavaju lijevu i desnu stranu jednakosti imamo prirodnu bijekciju

$$(A_1, A_2) \mapsto (A_2, A_1 \setminus A_2),$$

čiji je inverz

$$(B_1, B_2) \mapsto (B_1 \cup B_2, B_1).$$

Algebarski dokaz formule g) je jednostavan, pa ga prepuštamo čitatelju.

Uočite da zbog simetrije (svojstvo a)) svaki od produkata iz g) možemo napisati na još tri načina. Stoga pravilo produkta možemo napisati na 48 raznih načina. To pokazuje svu "*kameleonsku prirodu*" binomnih koeficijenata.

□

Pascal je do svoje formule došao tako da je binomne koeficijente $\binom{n}{r}$ za male vrijednosti n i r napisao u obliku tablice koja se zove **Pascalov trokut**:

n	$\binom{n}{0}$	$\binom{n}{1}$	$\binom{n}{2}$	$\binom{n}{3}$	$\binom{n}{4}$	$\binom{n}{5}$	$\binom{n}{6}$	$\binom{n}{7}$	$\binom{n}{8}$	$\binom{n}{9}$	$\binom{n}{10}$	$\cdots$
0	1											
1	1	1										
2	1	2	1									
3	1	3	3	1								
4	1	4	6	4	1							
5	1	5	10	10	5	1						
6	1	6	15	20	15	6	1					
7	1	7	21	35	35	21	7	1				
8	1	8	28	56	70	56	28	8	1			
9	1	9	36	84	126	126	84	36	9	1		
10	1	10	45	120	210	252	210	120	45	10	1	
$\vdots$	$\vdots$											

Pascalova formula je zapravo rekurzija za binomne koeficijente, jer se njome počevši s prva dva stupca može izračunati svaki daljnji član Pascalova trokuta. Pascalov trokut je izvor i mnogih drugih identiteta i formula za binomne koeficijente. No njima ćemo se vratiti poslije.

Opišimo sada vezu između podskupova skupa i rastava prirodnih brojeva. **Rastav** (ili **kompozicija**) **prirodnog broja** n u r dijelova je *uređena* r-torka prirodnih brojeva čiji je zbroj n. Tako, primjerice, imamo ukupno 8 rastava broja 4: $1+1+1+1$, $2+1+1$, $1+2+1$, $1+1+2$, $3+1$, $1+3$, $2+2$, 4, od toga je jedan u 4 dijela, tri u 3 dijela, tri u 2 dijela i jedan u 1 dio.

Neka je $(a_1, a_2, \ldots, a_r)$ rastav od n u r dijelova. Tome rastavu pridružimo $(r-1)$-člani podskup $\{a_1, a_1+a_2, \ldots, a_1+a_2+\cdots+a_{r-1}\} \subseteq [n-1]$, koji se sastoji od svih

parcijalnih suma (osim konačne koja je n). Lako je provjeriti da je to pridruživanje bijekcija između svih rastava od n u r dijelova i $(r-1)$-članih podskupova od $[n-1]$.

Odatle zaključujemo da je broj rastava od n u r dijelova jednak $\binom{n-1}{r-1}$, a ukupan broj rastava od n jednak (zbog Propozicije 8b))

$$\sum_{r=1}^{n}\binom{n-1}{r-1}=\binom{n-1}{0}+\binom{n-1}{1}+\cdots+\binom{n-1}{n-1}=2^{n-1}.$$

"Apstraktni" rezultat $\binom{n-1}{r-1}$ o broju rastava broja n u r dijelova grafički možemo doživjeti i dokazati ovako. Nanižimo u jednoj liniji n točaka (možemo zamisliti i kuglice). Ovisno o tome koji su dijelovi rastava, između točaka (ili kuglica) stavimo $r-1$ pregrada između $n-1$ mjesta među točkama (ili kuglicama). Tako primjerice

$$\bullet\bullet\,|\,\bullet\bullet\bullet\,|\,\bullet\,|\,\bullet\bullet\bullet\,|\,\bullet\,|\,\bullet\bullet\bullet\bullet$$

predstavlja rastav $2+3+1+3+1+4$ (broja 14) u šest dijelova. Odavde jednostavno "vidimo" da je broj rastava broja n u r dijelova $\binom{n-1}{r-1}$.

Sličan je problem određivanja broja uređenih r-torki $(x_1,x_2,\dots x_r)$ nenegativnih cijelih brojeva koji zadovoljavaju jednadžbu

$$x_1+x_2+\cdots+x_r=n. \tag{1}$$

Svako rješenje $(x_1,\dots,x_r)$ te jednadžbe zove se **slabi rastav broja** n u r dijelova. Označimo li $y_i=x_i+1$, $i=1,2,\dots,r$, iz (1) slijedi

$$y_1+y_2+\cdots+y_r=n+r. \tag{2}$$

Prema tome, broj rješenja $(x_1,\dots,x_r)\in\mathbb{N}_0^r$ od (1) jednak je broju rješenja $(y_1,\dots,y_r)\in\mathbb{N}^r$ od (2), a to je broj rastava od $n+r$ u r dijelova. Taj je broj, kao što znamo, jednak $\binom{n+r-1}{r-1}$. Zaključimo ovo razglabanje.

PROPOZICIJA 9. *a) Broj svih rastava broja n u r dijelova jednak je $\binom{n-1}{r-1}$.*

b) Broj svih slabih rastava od n u r dijelova, tj. broj svih uređenih r-torki $(x_1,\dots,x_r)$ cijelih brojeva $x_i\geq 0$ za koje je $x_1+x_2+\cdots+x_r=n$ jednak je

$$\binom{n+r-1}{r-1}.$$

Primjer 34. Na koliko se načina među r djece može raspodijeliti a) točno n bombona; b) najviše n bombona? (Bombone smatramo jednakim.) Posebno izračunajte to za $n=50$, $r=5$.

Rješenje. a) Označimo djecu s $D_1,D_2,\dots,D_r$ i neka je x_i broj bombona koje dobije dijete D_i, $i=1,\dots,r$. I ovdje se pitamo za broj uređenih rješenja $(x_1,\dots,x_r)$ u nenegativnim cijelim brojevima jednadžbe $x_1+\cdots+x_r=n$, a njih prema Propoziciji 9 ima $\binom{n+r-1}{r-1}$. Za $n=50$, $r=5$ odgovor je $\binom{50+5-1}{5-1}=\binom{54}{4}=316251$.

b) Slično kao u a) ovdje tražimo broj (uređenih) rješenja $(x_1,\dots,x_r)$ nejednadžbe $x_1+x_2+\cdots+x_r\leq n$. Taj je broj jednak sumi brojeva rješenja jednadžbi $x_1+x_2+\cdots+x_r=m$, za $m=0,1,\dots,n$. Traženi broj je stoga jednak (rabeći a) i Propoziciju 8f)):

$$\sum_{m=0}^{n}\binom{m+r-1}{r-1}=\binom{n+r-1+1}{r}=\binom{n+r}{r}.$$

Za $n=50$, $r=5$ odgovor je $\binom{50+5}{5}=\binom{55}{5}=\frac{55}{5}\binom{54}{4}=11\binom{54}{4}=3478761$. □

Primjer 35. Kombinatorno interpretirajte jednakosti

$$k\binom{n}{k}=k\binom{n}{n-k}=(n-k+1)\binom{n}{k-1}=(n-k+1)\binom{n}{n-k+1}.$$

Rješenje. Ove se jednakosti lako dokazuju uporabom formule $\binom{n}{k}=\frac{n!}{k!(n-k)!}$. No izravna kombinatorna interpretacija je ova. Veličina sasvim lijevo broji sve uređene parove (A,x), gdje je $A\in\binom{[n]}{k}$, $x\in A$, dok veličina sasvim desno broji sve uređene parove (B,y), gdje je $B\in\binom{[n]}{n-k+1}$, $y\in B$. Bijekcija je ova: $(A,x)\mapsto(\overline{A}\cup\{x\},x)$, s inverzom $(B,y)\mapsto(\overline{B\setminus\{y\}},y)$. □

§ 5. Kombinacije i permutacije multiskupova

Kao što smo rekli, r-podskup nekog n-članog skupa S zove se r-kombinacija od S bez ponavljanja. Već i ovaj naziv upućuje na problem prebrojavanja r-kombinacija od S *s ponavljanjem*. Točnije, problem je na koliko načina možemo odabrati r elemenata iz S, bez obzira na poredak, ali dopuštamo ponavljanje elemenata. Označimo taj broj simbolom

$$\left(\!\binom{n}{k}\!\right).$$

Na primjer, neka je $S=\{a,b,c,d\}$. Odredimo $\left(\!\binom{4}{2}\!\right)$. Treba, dakle odrediti sve 2-kombinacije s ponavljanjem od S. Tako su $\{a,a\}$, $\{a,b\}$ dvije takve. Sve 2-kombinacije s ponavljanjem od S su (pisane bez zagrada): *aa*, *ab*, *ac*, *ad*, *bb*, *bc*, *bd*, *cc*, *cd*, *dd*.

Formalni pristup ovome problemu (i još nekim) izvodi se iz pojma multiskupa. Multiskup je objekt poput skupa u kojem se neki elementi ponavljaju. Primjerice $\{a,a,b,c,c,d,d,d\}$.

Precizno, **konačni multiskup** M na skupu S je uređeni par $M=(S,m)$, gdje je $m:S\to\mathbb{N}_0$ funkcija za koju je $\sum_{x\in S}m(x)$ konačan broj. Za $x\in S$ se broj $m(x)$ zove **kratnost** (ili **ponavljanje** ili **multiplicitet**) od x. **Broj elemenata** (ili **kardinalnost**) **multiskupa** M, u oznaci $|M|$, $\#M$ ili $\operatorname{card}M$ je

$$\sum_{x\in S}m(x).$$

Ako je $S=\{x_1,x_2,\dots,x_n\}$, a element x_i ima kratnost $m(x_i)=m_i$, $i=1,\dots,n$, onda se M zapisuje kao $M=\{x_1^{m_1},x_2^{m_2},\dots,x_n^{m_n}\}$ i kaže da se x_1 ponavlja m_1

puta, ..., x_n se ponavlja m_n puta. Tako npr. umjesto $\{a,a,b,c,c,d,d,d\}$ pišemo $\{a^2,b,c^2,d^3\}$. Broj elemenata ovog multiskupa je $\#\{a^2,b,c^2,d^3\} = 2+1+2+3 = 8$. Ako je $m(x) = 1$, $\forall x \in S$, multiskup je naprosto skup.

Skup svih r-članih multiskupova nad skupom S označavamo simbolom

$$\left(\!\binom{S}{r}\!\right).$$

Ako su $M = (S,m)$ i $M' = (S,m')$ dva multiskupa na istom skupu S, onda kažemo da je M' **podmultiskup** od M i pišemo $M' \subseteq M$, ako je $m(x) \leq m'(x)$, za svako $x \in S$. Primjerice, $\{a,b,c^2\} \subseteq \{a^2,b,c^2,d^3\}$. Dva multiskupa $M = (S,m)$ i $M' = (S,m')$ nad S su **jednaka** ako je $M \subseteq M'$ i $M' \subseteq M$, tj. ako je $m = m'$.

Kažemo (definiramo) da je r-**kombinacija s ponavljanjem** skupa S neki r-člani multiskup na skupu S, tj. element skupa $\left(\!\binom{S}{r}\!\right)$, te

$$\left(\!\binom{n}{r}\!\right) := \#\left(\!\binom{S}{r}\!\right).$$

Pokazat ćemo da je ovaj dvostruko zagrađeni binomni koeficijent zapravo transformirani obični binomni koeficijent. No prije toga izračunajmo ukupni broj podmultiskupova zadanog multiskupa $M = (S,m)$. Naime, ako je $M = \{x_1^{m_1}, \ldots, x_n^{m_n}\}$, onda je tipični podmultiskup od M oblika $\{x_1^{k_1}, \ldots x_n^{k_n}\}$, gdje je $0 \leq k_i \leq m_i$, $i = 1, \ldots, n$, pa je skup svih podmultiskupova od M u bijekciji sa skupom $\{0,1,\ldots, m_1\} \times \{0,1,\ldots,m_2\} \times \cdots \times \{0,1,\ldots,m_n\}$. Iz pravila produkta slijedi da je broj podmultiskupova od M jednak

$$\prod_{i=1}^{n}(m_i+1) = \prod_{x\in S}(m(x)+1).$$

Ako je $m(x) = 1$, za sve $x \in S$, dobivamo broj 2^n svih podskupova (Propozicija 3).

Napomena 6. I ovdje smo (prešutno) diskretno uredili skup S: $x_1 \prec x_2 \prec \cdots \prec x_n$.

PROPOZICIJA 10. *Broj r-kombinacija s ponavljanjem n-članog skupa S je jednak $\binom{n+r-1}{r}$, tj. vrijedi*

$$\#\left(\!\binom{S}{r}\!\right) = \left(\!\binom{n}{r}\!\right) = \binom{n+r-1}{r}.$$

Dokaz I. Neka je $S = \{y_1, y_2, \ldots, y_n\}$. Zanima nas koliko ima r-članih multiskupova na S. Neka su kratnosti elemenata $m(y_1) = x_1, \ldots, m(y_n) = x_n$. Tada je $x_1 + x_2 + \cdots + x_n = r$, a znamo (Propozicija 9) da ova jednadžba ima $\binom{r+n-1}{n-1} = \binom{n+r-1}{r}$ rješenja. □

Dokaz II. Izravni kombinatorni dokaz da je $\left(\!\binom{n}{r}\!\right) = \binom{n+r-1}{r}$ je ovaj. Neka je $1 \leq a_1 < a_2 < \cdots < a_r \leq n+r-1$ neki r-podskup od $[n+r-1]$. Definirajmo $b_i := a_i - i + 1$, $i = 1,2,\ldots,r$. Tada je $\{b_1, b_2, \ldots, b_r\}$ neki r-člani multiskup na

skupu $[n]$ jer je $1 \leq b_1 \leq b_2 \leq \cdots \leq b_r \leq n$ (tj. neki b_i-ovi su mogu ponavljati). Obrnuto, ako je zadan r-člani multiskup $1 \leq b_1 \leq b_2 \leq \cdots \leq b_r \leq n$ na $[n]$, onda definiramo $a_i := b_i + i - 1$, $i = 1,\ldots,r$. Time dobivamo r-člani podskup $\{a_1, a_2, \ldots, a_r\} \subseteq [n+r-1]$, jer je $1 \leq a_1 < a_2 < \cdots < a_r \leq n+r-1$. Ova dva pridruživanja su inverzna jedan drugom, pa smo time našli bijekciju

$$\left(\!\binom{[n]}{r}\!\right) \to \binom{[n+r-1]}{r}.$$

□

Tako npr. 3-kombinacije s ponavljanjem na skupu $\{a,b\}$ su sljedeće (pisane bez $\{\}$ i zareza): aaa, aab, abb, bbb. I to su sve jer ih ima $\binom{2+3-1}{3} = \binom{4}{3} = 4$. 4-kombinacije s ponavljanjem nad $\{a,b\}$ su: $aaaa, aaab, aabb, abbb, bbbb$. I to su sve jer ih ima $\binom{4+2-1}{4} = \binom{5}{4} = 5$.

Primjer 36. a) Na koliko se načina među četvero djece može raspodijeliti 10 jabuka, 8 krušaka i 9 banana?

b) Na koliko se načina među r djece može raspodijeliti n_1 predmeta prve vrsta, n_2 predmeta druge vrste, ..., n_k predmeta k-te vrste (smatramo da su predmeti i-te vrste jednaki, $i = 1,\ldots,k$)?

Rješenje. a) Neka su D_1, D_2, D_3, D_4 djeca, a x_i, y_i, z_i redom brojevi jabuka, krušaka i banana koje dobije dijete D_i, $i = 1,2,3,4$. Traženi je broj jednak produktu broja rješenja jednadžbi $x_1 + x_2 + x_3 + x_4 = 10$, $y_1 + y_2 + y_3 + y_4 = 8$, $z_1 + z_2 + z_3 + z_4 = 9$ u cijelim brojevima ≥ 0. Iz Propozicije 9 slijedi da je broj jednak

$$\binom{10+4-1}{4-1}\cdot\binom{8+4-1}{4-1}\cdot\binom{9+4-1}{4-1} = \binom{13}{3}\binom{11}{3}\binom{12}{3} = 10\,381\,800.$$

b) Potpuno isto zaključivanje kao u a) daje rezultat

$$\prod_{i=1}^{k}\binom{n_i+r-1}{r-1}.$$

□

Primjer 37. Koliko ima nepadajućih nizova duljine r čiji su članovi iz $\{1,2,\ldots,n\}$?

Rješenje. Svaki takav niz $1 \leq a_1 \leq a_2 \leq \cdots \leq a_r \leq n$ zapravo je jedna r-kombinacija s ponavljanjem na skupu $[n]$. Prema Propoziciji 10, traženi je broj jednak

$$\binom{n+r-1}{r}.$$

□

Primjer 38. Koliko ima nesukladnih trokuta čije duljine stranica imaju vrijednosti u skupu $\{5,6,7,8\}$?

Rješenje. Ovdje se očito radi o tome da moramo prebrojiti 3-kombinacije s ponavljanjem na skupu $\{5,6,7,8\}$. Takvih ima $\binom{4+3-1}{3} = 20$. □

Primjer 39. Polinom od n varijabli je **homogen** ako svaki sumand (monom) ima isti stupanj. Npr. $x^3y + x^2y^2 + 4xz^3 + 5z^4$ homogeni je polinom stupnja 4 od 3 varijable x, y, z. Koliko najviše članova (tj. monoma) ima homogeni polinom r-tog stupnja od n varijabli? (Homogeni polinomi zovu se još **forme**.)

Rješenje. Tipični monom (do na konstantu) od n varijabli $x_1, \ldots, x_n$ stupnja r je oblika

$$x_1^{k_1} x_2^{k_2} \ldots x_n^{k_n},\ k_1, \ldots, k_n \geq 0,\ k_1 + \cdots + k_n = r.$$

Stoga takvih monoma ima koliko ima rješenja $(k_1, \ldots, k_n) \in \mathbb{N}_0^n$ jednadžbe $k_1 + \cdots + k_n = r$, a prema Propoziciji 9, tih rješenja ima $\binom{r+n-1}{n-1} = \binom{n+r-1}{r}$. □

Primjer 40. Na koliko se načina n jednakih kuglica može rasporediti u r različitih kutija, tako da nijedna kutija ne bude prazna?

Rješenje. Neka su $K_1, K_2, \ldots, K_r$ (različite) kutije i neka je x_i broj kuglica koje stavljamo u kutiju K_i, $i = 1, \ldots, r$. Stoga je traženi broj jednak broju rješenja jednadžbe $x_1 + x_2 + \cdots + x_r = n$ u skupu $\mathbb{N}^n$, tj. broju rastava od n u r dijelova, a taj je jednak $\binom{n-1}{r-1}$. □

Primjer 41. Koliko ima onih r-članih podskupova iz $[n]$ koji ne sadrže dva uzastopna broja?

Rješenje. Primijenit ćemo sličnu ideju kao u dokazu II Propozicije 10. Ako je $A = \{a_1, a_2, \ldots a_r\} \subseteq [n]$ takav podskup $1 \leq a_1 < a_2 < \cdots < a_r \leq n$, onda je $a_{i+1} - a_i \geq 2$, $i = 1, \ldots, r-1$. Tome podskupu pridružimo r-člani skup $B = \{b_1, b_2, \ldots, b_r\}$, gdje je $b_i = a_i - (i-1)$, $i = 1, 2, \ldots, r$. tada je $1 \leq b_1 < b_2 < \cdots < b_r \leq n - r + 1$. Ovo pridruživanje $A \mapsto B$ je bijekcija (što mu je inverz?), pa je traženi broj jednak broju r-podskupova iz $[n - r + 1]$, a taj je jednak $\binom{n-r+1}{r}$. □

Primjer 42. Koliko ima svih podskupova iz $[n]$ koji ne sadrže dva uzastopna broja?

Rješenje. Takvih r-članih podskupova ima prema prethodnom primjeru $\binom{n-r+1}{r}$. Prema pravilu sume, takvih podskupova ima

$$f_n := \sum_{r \geq 0} \binom{n-r+1}{r} = \binom{n+1}{0} + \binom{n}{1} + \binom{n-1}{2} + \binom{n-2}{3} + \cdots + \binom{0}{n-1}.$$

Ovdje se zapravo sumira po $r \geq 0$ "dokle ide" (tj. dok je $n - r + 1 \geq r \iff r \leq \lfloor \frac{n+1}{2} \rfloor$). Uočite da je u ovoj sumi binomnih koeficijenata suma "brojnika" i "nazivnika" stalna.

Dokažimo da je $f_{n-2} + f_{n-1} = f_n$. Rabeći Pasacalovu formulu imamo

$$\begin{aligned}
f_{n-1} + f_{n-2} &= \binom{n-1}{0} + \binom{n-2}{1} + \binom{n-3}{2} + \cdots + \binom{n-r}{r-1} + \cdots + \binom{0}{n-1} + \\
&+ \binom{n}{0} + \binom{n-1}{1} + \binom{n-2}{2} + \cdots + \binom{n-r}{r} + \cdots + \binom{0}{n} = \\
&= \binom{n}{0} + \left[\binom{n-1}{1} + \binom{n-1}{0}\right] + \left[\binom{n-2}{2} + \binom{n-2}{1}\right] + \cdots + \\
&+ \left[\binom{n-r}{r-1} + \binom{n-r}{r}\right] + \cdots + \left[\binom{0}{n-1} + \binom{0}{n}\right] = \\
&= \binom{n+1}{0} + \binom{n}{1} + \binom{n-1}{2} + \cdots + \binom{n-r+1}{r} + \cdots + \binom{0}{n+1} = \\
&= f_n
\end{aligned}$$

Kako je $f_1 = 2$ (jer su $\emptyset$ i $\{1\}$ takvi podskupovi), a $f_2 = 3$ (jer su $\emptyset$, $\{1\}$, $\{2\}$ takvi podskupovi), dobivamo da je $f_n = F_{n+2}$, gdje je $F_0, F_1, F_2, \ldots, F_n, \ldots$ niz **Fibonaccijevih brojeva** za koje je $F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_n + F_{n+1}$, $n \geq 0$. (Drugo rješenje vidi Primjer 8 u poglavlju 3.) □

Primjer 43. Koliko ima onih r-članih podskupova iz $[n]$ koji ne sadrže t uzastopnih brojeva?

Rješenje. Neka je $f_t(n, r)$ traženi broj. U Primjeru 41 smo izračunali $f_2(n, r)$. Ovdje je ideja slična. Ako je $A = \{a_1, a_2, \ldots, a_r\} \subseteq [n]$ takav skup, $1 \leq a_1 < a_2 < \cdots < a_r \leq n$, onda mora biti $a_{i+1} - a_i \geq t$, $i = 1, \ldots, r-1$. Tome skupu pridružimo r-člani skup $B = \{b_1, b_2, \ldots, b_r\}$, gdje je $b_i := a_i - (i-1)(t-1)$, $i = 1, \ldots, r$. Tada je $1 \leq b_1 < b_2 < \cdots < b_r \leq n - (r-1)(t-1)$. Pridruživanje $A \mapsto B$ je bijekcija (što mu je inverz?), pa je $f_t(n, r)$ jednak broju r-podskupova iz $[n - (r-1)(t-1)]$. Stoga je

$$f_t(n, r) = \binom{n - (r-1)(t-1)}{r}.$$

□

Primjer 44. Koliko ima monotono rastućih funkcija $f : [n] \to [n]$ (tj. takvih da $i \leq j \Rightarrow f(i) \leq f(j)$)?

Rješenje. Neka je f takva funkcija. Stavimo $k_i = f(i+1) - f(i)$, $i = 1, \ldots, n-1$, $k_0 = f(1) - 1$ i $k_n = n - f(n)$. Traženi je broj jednak broju rješenja $(k_0, k_1, \ldots, k_n)$ u cijelim brojevima $k_i \geq 0$ jednadžbe $k_0 + k_1 + \cdots + k_n = n - 1$. Prema Propoziciji 9, tih rješenja ima $\binom{n-1+n+1-1}{n} = \binom{2n-1}{n}$. □

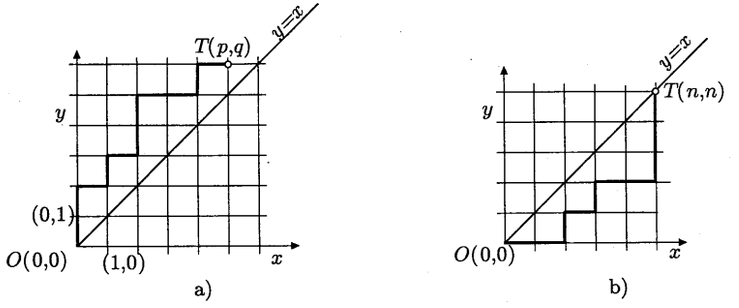
Primjer 45. ("**Princip zrcaljenja**")

a) Dokažite da je broj (najkraćih) putova u cjelobrojnoj mreži koordinatne ravnine Oxy od $O(0,0)$ do $T(p,q)$ $(p < q)$ s koracima $(1,0)$ i $(0,1)$ a koji nigdje osim u O ne sijeku pravac $y = x$ jednak (slika a)

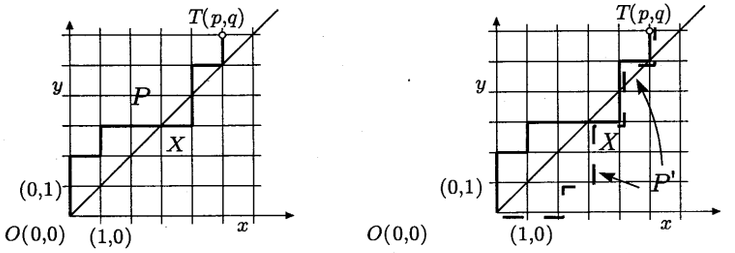
$$\binom{p+q-1}{p} - \binom{p+q-1}{p-1} = \frac{q-p}{q+p}\binom{p+q}{p}.$$

b) Dokažite nadalje da je broj takvih putova od $O(0,0)$ do $T(n,n)$ koji su čitavi ispod $y=x$ (a dotiču je samo u O i T) jednak Catalanovu broju C_{n-1} (slika b)). Pritom je $C_n = \frac{1}{n+1}\binom{2n}{n}$ n-ti **Catalanov**[6] **broj**.

c) Koliko ima takvih putova od $(0,0)$ do (n,n) koji nikad ne prijeđu iznad pravca $y=x$?



Rješenje. a) Podsjetimo se da je broj (najkraćih) putova od $(0,0)$ do (p,q) s koracima $(1,0)$ i $(0,1)$ jednak $\binom{p+q}{p}$ (Primjer 33). Putovi koji su iznad pravca $y=x$ moraju uvijek početi s $(0,1)$. Broj svih putova od $(0,1)$ do (p,q) stoga je $\binom{p+q-1}{p}$. Od toga broja treba oduzeti broj putova od $(0,1)$ do (p,q) koji dotiču ili sijeku $y=x$. Na takvom putu P uočimo prvu točku X presjeka s $y=x$ nakon O.



Dio puta P od O do X zrcalimo preko $y=x$ i dalje od X do T nastavimo istim putem kao P. Tako smo dobili put P' (crtkani na slici). Pridruživanje $P \mapsto P'$ je bijekcija između skupa svih putova od $(0,1)$ do (p,q) koji dotiču ili sijeku $y=x$ i skupa svih putova iz $(1,0)$ do (p,q). Inverzno pridruživanje je opet zrcaljenje do prvog presjeka s $y=x$. Svih putova od $(1,0)$ do (p,q) ima $\binom{p-1+q}{p-1}$. Oduzimanjem slijedi tvrdnja kao što je navedeno.

b) Ova tvrdnja slijedi ovako. Putova koji su ispod $y=x$ ima koliko i takvih od O do $(n,n-1)$, a takvih je (zrcaljenjem preko $y=x$) koliko i svih od O do $(n-1,n)$ koji su potpuno iznad $y=x$. Iz a) za $p=n-1$, $q=n$ slijedi da je njihov broj

$$\frac{1}{2n-1}\binom{2n-1}{n-1} = \frac{1}{2n-1}\frac{(2n-1)!}{(n-1)!n!} = \frac{1}{n}\frac{(2n-2)!}{(n-1)!^2} = \frac{1}{n}\binom{2n-2}{n-1} = C_{n-1}.$$

c) Odgovor je C_n. To dobivamo tako da putove iz c) translatiramo udesno za 1 i time dobivamo bijekciju s putovima iz b) s $n+1$ umjesto n.

□

[6]Eugene Charles Catalan (1814-1894), francuski matematičar

Primjer 46. Koliko ima monotono rastućih funkcija $f:[n]\to[n]$ (v. Primjer 44), takvih da je $f(k)\le k$, za svako k?

Rješenje. Problem je ekvivalentan sljedećem: koliko ima nizova $1\le a_1\le\cdots\le a_n$ cijelih brojeva za koje je $a_k\le k$ za svako k?

Neka je P jedan put iz prethodnog primjera c), dakle put u cjelobrojnoj mreži s koracima $(1,0)$ i $(0,1)$ od $(0,0)$ do (n,n) koji nikad ne prijeđe iznad pravca $y=x$. Neka je a_k površina iznad osi x između $x=k-1$ i $x=k$, a ispod P. Pridruživanje $P\mapsto(a_1,\dots a_n)$ je bijekcija, pa je odgovor opet Catalanov broj

$$C_n = \frac{1}{n+1}\binom{2n}{n}.$$

(O njima će još biti riječi, naročito u idućem poglavlju; usp. III, Propozicija 6) □

Kao što znamo, permutacija skupa je neki linearni poredak elemenata skupa. Potpuno analogno definiramo i permutacije multiskupa.

Neka je M multiskup kardinalnosti n. Tada je svaki linearni poredak $x_1x_2\dots x_n$ "elemenata" iz M permutacija od M. Točnije, ako je $M=(S,m)$ konačni multiskup, a $m:S\to\mathbb{N}_0$ funkcija kratnosti i $\sum_{x\in S}m(x)=n$, onda se svaka uređena n-torka $(x_1,x_2,\dots,x_n)$ elemenata iz S zove **permutacija multiskupa** M. Svaki element $x\in S$ javlja se u permutaciji od M točno $m(x)$ puta.

Na primjer, neka je $\{a,b^2,c\}$ multiskup. Sve njegove permutacije su: *abbc*, *abcb*, *acbb*, *babc*, *bacb*, *bbac*, *bbca*, *bcab*, *bcba*, *cabb*, *cbab*, *cbba*. Ukupno ih je 12.

Izračunajmo sada koliko permutacija ima konačan multiskup.

PROPOZICIJA 11. *Neka je $M=\{x_1^{n_1},x_2^{n_2},\dots,x_k^{n_k}\}$ multiskup s kratnostima elemenata $n_1,\dots,n_k$ i neka je $n_1+n_2+\cdots+n_k=n$. Tada je broj permutacija od M jednak*

$$\binom{n}{n_1,n_2,\dots,n_k} := \frac{n!}{n_1!n_2!\cdot\dots\cdot n_k!} = \frac{(n_1+n_2+\cdots+n_k)!}{n_1!n_2!\cdot\dots\cdot n_k!}.$$

Dokaz. Imamo n mjesta u nizu i na svako mjesto trebamo staviti po jedan element iz M. Prvo odaberimo na koja ćemo mjesta staviti elemente x_1. Kako ima n_1 elemenata x_1 u M, moramo odabrati podskup od n_1 mjesta u skupu od n mjesta. To se može odabrati na $\binom{n}{n_1}$ načina. Dalje odredimo na koja ćemo mjesta staviti x_2. Nakon postavljanja elemenata x_1 preostalo je $n-n_1$ mjesta, a moramo odabrati n_2 od njih. To je moguće na $\binom{n-n_1}{n_2}$ načina. Dalje nalazimo da ima $\binom{n-n_1-n_2}{n_3}$ načina da se odaberu mjesta za x_3 itd. (indukcija!). Prema pravilu produkta, dobivamo

da je ukupan broj permutacija od M jednak

$$\binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdot\ldots\cdot\binom{n-n_1-n_2-\cdots-n_{k-1}}{n_k}=$$
$$=\frac{n!}{n_1!(n-n_1)!}\cdot\frac{(n-n_1)!}{n_2!(n-n_1-n_2)!}\cdot\frac{(n-n_1-n_2)!}{n_3!(n-n_1-n_2-n_3)!}\cdot\ldots$$
$$\ldots\cdot\frac{(n-n_1-\cdots-n_{k-1})!}{n_k!(n-n_1-\cdots-n_k)!}=$$
$$=\frac{n!}{n_1!n_2!\ldots n_k!0!}=\frac{n!}{n_1!n_2!\ldots n_k!}.$$

□

Drugim riječima, ako imamo n kuglica (za bilijar, recimo), od kojih je n_1 njih jedne boje (npr. crvene), n_2 njih druge boje (npr. plave), n_3 treće boje (npr. bijele), ..., n_k njih k-te boje (npr. ?), onda je broj načina na koji možemo te kuglice postaviti u niz jednak

$$\binom{n}{n_1,\ldots,n_k}=\frac{n!}{n_1!n_2!\ldots n_k!}.$$

Taj se broj katkad zove i **broj permutacija s ponavljanjem**, odnosno **multinomni koeficijent**.

Uočite da je za $k=2$, multinomni koeficijent zapravo binomni:

$$\frac{n!}{n_1!n_2!}=\frac{n!}{n_1!(n-n_1)!}=\binom{n}{n_1}.$$

Primjer 47. Koliko različitih riječi[7] možemo napraviti od slova u riječima a) BANANA; b) OUAGADOUGOU (glavni grad Gornje Volte); c) MISSISSIPPI (omiljeno pitanje u američkim udžbenicima); d) MISSISSIPPI, ali da četiri slova S ne budu zajedno?

Rješenje. a) Treba izračunati broj permutacija multiskupa $\{A^3,B,N^2\}$. Prema Propoziciji 11 njih ima $\frac{6!}{3!1!2!}=60$.

Slično je odgovor b) $\frac{11!}{3!3!2!2!1!}=277200$, c) $\frac{11!}{4!4!2!1!}=34650$.

d) Odgovor je $\frac{11!}{4!4!2!1!}-\frac{8!}{4!2!1!1!}=33810$. □

Primjer 48. Nađite broj a) 8-cifrenih, b) 5-cifrenih brojeva koji se mogu načiniti od broja 62 724 277.

Rješenje. a) To su sve permutacije multiskupa $\{2,2,4,6,7,7,7\}$. Stoga je odgovor $8!/4!2!1!1!1!=1180$.

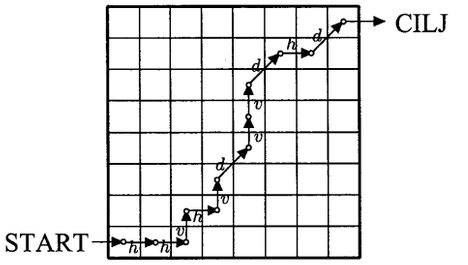
b) 5-cifreni broj se može sastojati od 4 jednake cifre i jedne različite: (77772), (77774), (77776); od 3 jednake i druge dvije jednake (77722); od 3 jednake i 2 različite: (77724), (77726), (77746); od 2 para jednakih i jedne različite: (77224), (77226) ili od dvije jednake i 3 različite cifre: (77246), (22467). Prema pravilu sume, traženi je broj

$$3\cdot\frac{5!}{4!1!}+\frac{5!}{3!2!}+3\cdot\frac{5!}{3!1!1!}+2\cdot\frac{5!}{2!2!1!}+2\cdot\frac{5!}{2!1!1!1!}=265.$$

□

[7] U zabavnoj se matematici "smislena" permutacija slova neke riječi (ili rečenice) zove **premetaljka** ili **anagram**. Tako su npr. neki anagrami imena i prezimena autora ove knjige Dejan Lovrak, Jadranko Lev, Ena Vrdoljak, vjerna klado, orden valjak, roljav dekan, valjan koder itd.

Primjer 49. Na koliko načina može kralj iz donjeg lijevog polja šahovske ploče doći u njezino desno gornje polje, ako se mora pomicati tako da nakon svakog pokreta bude bliži cilju?



Rješenje. Pomičući se bliže cilju, kralj se može kod svakog pomaka pomicati za jedno polje ili u horizontalnom smjeru h ili u vertikalnom smjeru v ili dijagonalno d. Jedan takav put (na slici) je *hhvhvdvvdhd*. Dijagonalnih pomaka d može biti najviše 7. Ako je broj dijagonalnih koraka d čvrst broj k, $0\le k\le 7$, onda horizontalnih koraka h ima $7-k$, a isto tako i vertikalnih v. Nas stoga zanima koliko ima permutacija multiskupa $\{k\cdot d,(7-k)\cdot h,(7-k)\cdot v\}$ za čvrsto k. Njih ima $\frac{(14-k)!}{k!(7-k)!(7-k)!}$, pa je traženi broj $\sum_{k=0}^{7}\frac{(14-k)!}{k![(7-k)!]^2}=48639$.

Interpretirajte taj rezultat i kao $\sum_{k=0}^{7}\binom{14-k}{k}\binom{14-2k}{7-k}$. □

Primjer 50. Na koliko načina možemo n (jednakih) bombona raspodijeliti među r djece? (To je primjer 34 a), ali ćemo ga sada riješiti uporabom permutacija s ponavljanjem.)

Rješenje. Naničimo bombone ispred djece $D_1,D_2,\ldots,D_r$.

$$\underbrace{\bowtie\ \bowtie\ \bowtie}_{D_1}\Big|\underbrace{\bowtie\ \bowtie}_{D_2}\Big|\underbrace{\ }_{D_3}\Big|\underbrace{\bowtie\ \bowtie}_{D_4}\Big|\ \cdots\ \Big|\underbrace{\bowtie\ \bowtie}_{D_r}$$

Svakom djetetu D_i damo pregradu da njome zagrabi nekoliko bombona (može biti i ništa), osim zadnjem djetetu D_r, jer njemu damo preostale bombone. Stoga je traženi broj jednak broju permutacija s ponavljanjem od n bombona i $r-1$ pregrada, pa je odgovor (opet)

$$\frac{(n+r-1)!}{n!(r-1)!}=\binom{n+r-1}{r-1}.$$

□

Uređena k-torka $(A_1,A_2,\ldots,A_k)$ međusobno disjunktnih podskupova $A_i\subseteq S$ čija je unija čitav S zove se **rastav** od S na k dijelova. Ako je $|S|=n$, onda je broj

rastava od S na k dijelova $(A_1, \ldots, A_k)$ s $|A_i| = n_i$, $i = 1, \ldots, k$, $n_1 + \cdots + n_k = n$, $n_1, \ldots n_k \geq 0$, također jednak (indukcijom po k):

$$\binom{n}{n_1, \ldots, n_k}.$$

Uočite da je taj broj jednak i broju svih funkcija $f : [n] \to [k]$ takvih da je $\#f^{-1}(i) = n_i$, $i = 1, 2, \ldots, k$.

Ako je multiskup veličine n, a $r < n$, onda je **r-permutacija** od M uređena r-torka "elemenata" iz M. Broj r-permutacija nekog multiskupa najlakše je izračunati pomoću funkcija izvodnica (v. poglavlje 5). Razna netrivijalna kombinatorna svojstva permutacija multiskupova mogu se naći u knjizi [123], vol. III. 5.1.

Primjer 51. Imamo 3 jabuke, 3 kruške i 4 breskve. Za spravljanje voćne salate uzimamo 8 komada voća, jedan po jedan. Na koliko je načina to moguće učiniti?

Rješenje. Treba izračunati broj 8-permutacija multiskupa $\{J^3, K^3, B^4\}$. Ako smo uzeli n_1 jabuka (J), n_2 krušaka (K) i n_3 bresaka (B), rezultat je $\sum \binom{8}{n_1, n_2, n_3}$, gdje se sumira po svim $n_1, n_2, n_3 \geq 0$, $n_1 + n_2 + n_3 = 8$ i $n_1, n_2 \leq 3$, $n_3 \leq 4$. Jedina rješenja ovog sustava su $(n_1, n_2, n_3) = (1, 3, 4)$, $(3, 1, 4)$, $(2, 3, 3)$, $(3, 2, 3)$, $(3, 3, 2)$, $(2, 2, 4)$, pa je stoga traženi broj jednak

$$2\binom{8}{1, 3, 4} + 3\binom{8}{2, 3, 3} + \binom{8}{2, 2, 4} = 2660.$$

□

§ 6. Binomni i multinomni koeficijenti

Binomna formula

Binomni koeficijenti su dobili ime po tome što se pojavljuju kao koeficijenti u **binomnom teoremu** ili **binomnoj formuli**. To je jedan od najvažnijih algebarsko-kombinatornih rezultata, a njegov najjednostavniji slučaj $(x + y)^2 = x^2 + 2xy + y^2$ datira i prije Euklida oko 300 g. pr. Kr. Formula za $(x + y)^n$ znala se je u nekom smislu i prije Sir Isacca Newtona, ali ju je on oko 1676. g. prvi (korektno) dokazao i poopćio razvivši u red potencija $(1 + x)^\alpha$, $\alpha \in \mathbb{R}$. O tome poslije, a sada ćemo na tri načina dokazati osnovnu i vrlo važnu formulu za $(x + y)^n$.

TEOREM 1 (Binomni teorem). *Za svako $n \in \mathbb{N}_0$ i svako $x, y \in \mathbb{R}$ (ili čak $x, y \in \mathbb{C}$) vrijedi*

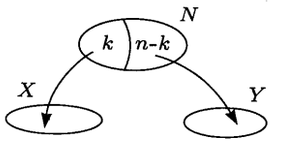
$$(x+y)^n = x^n + \binom{n}{1}x^{n-1}y + \cdots + \binom{n}{k}x^k y^{n-k} + \cdots + y^n = \sum_{k=0}^{n}\binom{n}{k}x^k y^{n-k}. \quad (3)$$

Dokaz I. Indukcijom po n, formula se lako dokazuje uporabom Pascalove formule. □

Dokaz II. $(x + y)^n = (x + y)(x + y) \ldots (x + y)$. Nakon svih množenja (tj. kad se "riješimo zagrada"), kao rezultat dobivamo zbroj svih monoma oblika $x^k y^{n-k}$. Za čvrst k, tih je sumanada toliko koliko iz n faktora možemo izabrati k njih jednakih x (a $n - k$ njih y), pa ih ima $\binom{n}{k}$. □

Dokaz III (Kombinatorni). Mi želimo dokazati jednakost polinoma (u dvije varijable x i y i čvrsto $n \geq 0$). Jednakost dvaju polinoma se obično dokazuje na tri načina: prvo, da su jednaki kao funkcije; drugo, da su im odgovarajući koeficijenti jednaki ili treće, da se podudaraju u dovoljno mnogo (konačno) točaka. Mi ćemo se ovdje poslužiti trećim načinom. Prema tome, dovoljno je dokazati da binomna formula vrijedi za sve prirodne brojeve x, y (dakle, da se lijeva i desna strana podudaraju u beskonačno točaka (x, y)). Sjetimo se da nam a^n za $n, a \in \mathbb{N}$ znači broj funkcija s n-članog u a-člani skup (Propozicija 2). Nakon ovog malog podsjetnika sada zapravo počinje dokaz.

Neka su X, Y i N konačni skupovi $|X| = x$, $|Y| = y$ i $|N| = n$, a X i Y disjunktni. Lijeva strana $(x + y)^n$ kombinatorno znači broj funkcija $N \to X \cup Y$, a opći član $\binom{n}{k}x^k y^{n-k}$ na desnoj strani koliko ima izbora k-članih podskupova iz N koji se preslikavaju u X (a ostalih $n - k$ elemenata u Y). Iz pravila zbroja tada slijedi jednakost. Sličica za "vizualce" (uostalom, "prava slika vrijedi tisuće riječi"):



"Dokaz bez riječi" binomnog teorema

□

Napomena 7. Uočite (npr. iz dokaza I) da x i y mogu biti iz bilo kojeg komutativnog prstena.

Posebno, za $y = 1$ dobivamo (jednakost polinoma u jednoj varijabli x)

$$(x+1)^n = \sum_{k=0}^{n}\binom{n}{k}x^k. \quad (4)$$

Ova formula vrijedi za svaki realni (ili kompleksni) broj x, pa ako u nju uvrstimo neke brojeve, dobivamo razne identitete s binomnim koeficijentima. Primjerice, za $x = 1$, dobivamo formulu (Propozicija 8 b))

$$\sum_{k=0}^{n}\binom{n}{k} = 2^n, \quad (5)$$

i to je još jedan dokaz da svih podskupova iz $[n]$ ima 2^n.

Za $x = -1$ dobivamo također nešto što već znamo (Korolar 1) da parnih i neparnih podskupova n-članog skupa ima jednako mnogo, i to 2^{n-1}. Naime, stavimo li $x = -1$ u (4), dobivamo

$$\sum_{k=0}^{n}(-1)^k\binom{n}{k} = 0, \quad (6)$$

što je ekvivalentno s

$$\sum_{k\geq 0}\binom{n}{2k}=\sum_{k\geq 0}\binom{n}{2k+1},$$

a to zajedno s (5) dokazuje navedenu tvrdnju.

Doslovno, milijuni zanimljivih formula i identiteta s binomnim koeficijentima (kao (5) i (6)) slijede iz binomne formule ili drugih sličnih formula i tome su posvećeni mnogi znanstveni članci, knjige i knjižurine. Mi ćemo ovdje i u drugim poglavljima (posebno kad naučimo funkcije izvodnice) navesti samo neke od njih.

Prvo, izvedimo analognu formulu binomnoj kada eksponente "podvučemo", tj. formulu za $(x+y)^{\underline{n}}$. Podsjetimo se da je padajući faktorijel (ili potencija) definiran s

$$x^{\underline{n}}=x(x-1)\cdot\dots\cdot(x-n+1), \tag{7}$$

a kombinatorno značenje mu je (za $n,x\in\mathbb{N}$, Propozicija 4) broj injekcija. Slično je i rastući faktorijel (potencija)

$$x^{\overline{n}}=x(x+1)\cdot\dots\cdot(x+n-1). \tag{8}$$

PROPOZICIJA 12 (Vandermondeova[8] formula). *Za svako $n\in\mathbb{N}_0$ i svako $x,y\in\mathbb{R}$ (ili čak $x,y\in\mathbb{C}$) vrijedi*

$$(x+y)^{\underline{n}}=\sum_{k=0}^{n}\binom{n}{k}x^{\underline{k}}y^{\underline{n-k}}, \tag{9}$$

$$(x+y)^{\overline{n}}=\sum_{k=0}^{n}\binom{n}{k}x^{\overline{k}}y^{\overline{n-k}}. \tag{10}$$

Dokaz I. Algebarski dokaz formule (9) ide slično kao i binomna formula indukcijom po n. Ovaj put to provedimo rabeći Pascalovu formulu. Za $n=1$ (i $n=0$) formula očito vrijedi. Neka je $n\geq 2$ i pretpostavimo da (9) vrijedi za sve brojeve $\leq n-1$. Tada redom imamo (uvjerite se u svaki korak):

$$\begin{aligned}(x+y)^{\underline{n}}&=(x+y)^{\underline{n-1}}(x+y-n+1)=\\&=\sum_{k=0}^{n-1}\binom{n-1}{k}x^{\underline{k}}y^{\underline{n-k-1}}(x-k+y-n+k+1)=\\&=\sum_{k=0}^{n-1}\binom{n-1}{k}x^{\underline{k+1}}y^{\underline{n-k-1}}+\sum_{k=0}^{n-1}\binom{n-1}{k}x^{\underline{k}}y^{\underline{n-k}}=\\&=\sum_{k=0}^{n}\left[\binom{n-1}{k-1}+\binom{n-1}{k}\right]x^{\underline{k}}y^{\underline{n-k}}=\sum_{k=0}^{n}\binom{n}{k}x^{\underline{k}}y^{\underline{n-k}}.\end{aligned}$$

[8] Alexandre Vandermonde (1735 – 1796), francuski matematičar

Formula (10) (koja se ponegdje naziva i **Nörlundova formula**) također se može tako dokazati, ali ona slijedi i iz (9) pomoću "reciprociteta"

$$x^{\overline{n}}=(-1)^n(-x)^{\underline{n}}.$$

□

Dokaz II. Kombinatorni dokaz formule (9) doslovno se provodi na isti način kao i kombinatorni dokaz binomne formule, samo što umjesto skupa funkcija $(X\cup Y)^N$ ovdje gledamo skup injekcija $(X\cup Y)^{\underline{N}}$. Dakle, isto zaključivanje i ista sličica daje formulu (9) (a bogme i (10) uz odgovarajuću zamjenu slova). □

I ove dvije formule imaju, naravno, silne zanimljive posljedice (milijuni i milijuni ...). Ukažimo na samo neke od njih. No prvo ćemo definirati opći binomni koeficijent. Za realni (ili kompleksni) broj x i nenegativni cijeli broj n, **opći binomni koeficijent** $\binom{x}{n}$ definira se kao

$$\binom{x}{n}:=\frac{x(x-1)(x-2)\cdot\dots\cdot(x-n+1)}{n!}, \tag{11}$$

tj. s (ekvivalentnom jednakošću, i to jednakošću polinoma za čvrsto n):

$$n!\binom{x}{n}=x^{\underline{n}}. \tag{12}$$

Ako je x prirodan broj (ili 0), opći se binomni koeficijent podudara s običnim binomnim koeficijentom (Propozicija 7) i ima svoje kombinatorno značenje.

Izrazimo sada i rastući faktorijel pomoću općeg binomnog koeficijenta. Prvo, iz definicije (11) imamo

$$\begin{aligned}\binom{-x}{n}&=\frac{(-x)(-x-1)(-x-2)\dots(-x-n+1)}{n!}=\\&=(-1)^n\frac{x(x+1)\dots(x+n-1)}{n!}=(-1)^n\binom{x+n-1}{n},\end{aligned}$$

pa odavde slijedi tzv. **zakon recipročnosti za binomne koeficijente**:

$$\binom{x+n-1}{n}=(-1)^n\binom{-x}{n} \tag{13}$$

koji (za prirodni x) izražava broj kombinacija s ponavljanjem. Sada imamo, rabeći (12) i (13):

$$x^{\overline{n}}=(-1)^n(-x)^{\underline{n}}=(-1)^n n!\binom{-x}{n}=n!\binom{x+n-1}{n},$$

tj.

$$x^{\overline{n}}=n!\binom{x+n-1}{n}. \tag{14}$$

KOROLAR 3 (Vandermondeove konvolucije). *Za $m,n,r \in \mathbb{N}$ vrijedi*

$$\sum_{k=0}^{r} \binom{m}{k}\binom{n}{r-k} = \binom{m+n}{r}, \tag{15}$$

$$\sum_{k\geq 0} \binom{m}{k}\binom{n}{k} = \binom{m+n}{n}. \tag{16}$$

(Ovdje se zapravo sumira po k od 0 do $\min(m,n)$; ostali sumandi su 0.) Kao poseban (zanimljiv) slučaj od (16) *za $m=n$ je formula*

$$\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}. \tag{17}$$

Dokaz I. (Kao posljedica Vandermondeovih formula). Iz Propozicije 12, to slijedi odmah iz definicije (12) općeg binomnog koeficijenta. Naime, primijenimo li (12) na lijevu i desnu stranu od (9), imamo

$$n!\binom{x+y}{n} = \sum_{k=0}^{n} \binom{n}{k} k! \binom{x}{k} (n-k)! \binom{y}{n-k} = n! \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k},$$

pa skraćivanje s $n!$ povlači

$$\binom{x+y}{n} = \sum_{k=0}^{n} \binom{x}{k}\binom{y}{n-k}. \tag{15'}$$

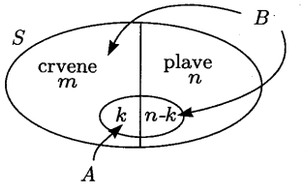
Ovo je zapravo već formula (15), uz očite zamjene slova: $x \leftrightarrow m$, $y \leftrightarrow n$, $n \leftrightarrow r$. Uočite da je (15) formula za sumu produkata od po dva binomna koeficijenta kod kojih su "brojnici" čvrsti, a zbroj "nazivnika" također stalan. Formula (16) slijedi iz (15) zbog simetrije binomnih koeficijenata. Imamo

$$\sum_{k=0}^{n} \binom{m}{k}\binom{n}{k} = \sum_{k=0}^{n} \binom{m}{m-k}\binom{n}{k} = \binom{m+n}{n}.$$

□

Dokaz II. Formula (15), tj. (15') kombinatorno se može i ovako protumačiti. Za $x,y \in \mathbb{N}$, lijeva strana od (15') broji sve načine na koje od x muškaraca i y žena možemo izabrati n ljudi. Na desnoj strani svaki sumand je broj načina da se odabere k muškaraca i $n-k$ žena. Sumiranje po svim k broji svaku mogućnost točno jedanput.

A formula (16) ide ovako. Ovaj put brojimo npr. kuglice. Uzmimo da imamo skup S od m crvenih i n plavih kuglica. Desna strana od (16) kaže koliko ima n-članih podskupova od tih $m+n$ kuglica. Lijeva strana od (16) kaže na koliko načina možemo odabrati podskup od $m+n$ kuglica u kojem je jednako mnogo k crvenih i k plavih kuglica, $k = 0,1,\ldots,\min(m,n)$. Neka je $A \subseteq S$ n-člani podskup. Ako A ima k crvenih kuglica (pa stoga $n-k$ plavih), onda skupu A pridružimo skup B od $m-k$ neodabranih crvenih i odabranih $n-k$ plavih kuglica. $A \mapsto B$ je bijekcija.



Stoga je (zbog simetrije binomnih koeficijenata):

$$\sum_{k\geq 0} \binom{m}{m-k}\binom{n}{n-k} = \sum_{k\geq 0} \binom{m}{k}\binom{n}{k} = \binom{m+n}{n}.$$

□

Dokaz III (Algebarski). (15) možemo dokazati i tako da u identitetu

$$(1+x)^m(1+x)^n = (1+x)^{m+n}$$

nađemo koeficijent uz x^r nakon razvoja po binomnoj formuli (4). Imamo:

$$\langle x^r\rangle (1+x)^m(1+x)^n = \langle x^r\rangle \left(\sum_{k=0}^{m}\binom{m}{k}x^k \cdot \sum_{l=0}^{n}\binom{n}{j}x^l\right) =$$

$$= \sum_{k+l=r}\binom{m}{k}\binom{n}{l} = \sum_{k=0}^{r}\binom{m}{k}\binom{n}{r-k}.$$

S druge je strane zbog binomne formule također

$$\langle x^r\rangle (1+x)^{m+n} = \binom{m+n}{r}.$$

Izjednačavanjem se dobije (15). Pokušajte slično dokazati i (16). □

Cijelu seriju svojstava i identiteta dobijemo kada jednakost (4) među polinomima deriviramo (po x), dvaput deriviramo, integriramo itd. ili pak ako (3) parcijalno deriviramo itd. , pa nakon toga uvrstimo neke posebne vrijednosti. Slično i s Vandermondeovim formulama, možemo derivirati (11) (ili (12)) itd. Evo samo nekih primjera.

Primjer 52. Dokažite da vrijedi

a) $\sum_{k=0}^{n} k\binom{n}{k} = n2^{n-1}$; b) $\sum_{k=0}^{n} k^2\binom{n}{k} = n(n+1)2^{n-2}$;

c) $\sum_{k=0}^{n} \frac{1}{k+1}\binom{n}{k} = \frac{2^{n+1}-1}{n+1}$; d) $\sum_{k=0}^{n} \frac{k}{2^k}\binom{n}{k} = \frac{n3^{n-1}}{2^n}$;

e) $\sum_{k=0}^{n} k\binom{n}{k}^2 = n\binom{2n-1}{n-1}$.

Rješenje. a) Deriviranje obje strane jednakosti (4) po x daje

$$n(1+x)^{n-1} = \sum_{k=1}^{n} \binom{n}{k} k x^{k-1}. \qquad (*)$$

Ako tu uvrstimo $x = 1$, dobivamo a).

b) Ako gornju jednakost $(*)$ pomnožimo s x, zatim opet deriviramo i na kraju opet uvrstimo $x = 1$, dobivamo b).

c) Integriranjem jednakosti (4) po x od 0 do 1 dobivamo

$$\int_0^1 (1+x)^n dx = \sum_{k=0}^{n} \binom{n}{k} \int_0^1 x^k dx,$$

a odatle

$$\frac{1}{n+1}(2^{n+1}-1) = \sum_{k=0}^{n} \binom{n}{k} \frac{1}{k+1}.$$

d) Ako $(*)$ pomnožimo s x i zatim uvrstimo $x = \frac{1}{2}$, dobivamo d).

e) Pomnožimo lijeve i desne strane od (4) i $(*)$, pa tada izjednačimo koeficijente uz x^{n-1}. □

Ako pak u binomnu formulu (4) uvrstimo neki kompleksni broj, onda izjednačavanjem realnih (ili imaginarnih) dijelova dobivamo nove identitete. U idućem primjeru tako ćemo izračunati sume poput

$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \dots, \quad \binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \dots, \quad \binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \dots \text{ itd.}$$

Primjer 53. Neka su $n, q \in \mathbb{N}$, $1 \le q \le n-1$, $r \in \{0, 1, \dots, q-1\}$. Tada vrijedi

$$\binom{n}{r} + \binom{n}{r+q} + \binom{n}{r+2q} + \binom{n}{r+3q} + \dots = \frac{1}{q} \sum_{k=0}^{q-1} \left(2\cos\frac{k\pi}{q}\right)^n \cos\frac{k(n-2r)\pi}{q}.$$

(Suma na lijevoj strani ide "dok može", tj. dok "nazivnik" ne prijeđe n.)

Rješenje. Neka je $\varepsilon = e^{\frac{2\pi i}{q}} = \cos\frac{2\pi}{q} + i\sin\frac{2\pi}{q}$, tj. $\varepsilon(\neq 1)$ je q-ti korijen iz jedinice. Tada je $\varepsilon^q = 1 \Rightarrow \varepsilon^q - 1 = 0 \Rightarrow (\varepsilon-1)(\varepsilon^{q-1}+\varepsilon^{q-2}+\dots+\varepsilon+1) = 0 \Rightarrow \varepsilon^{q-1}+\varepsilon^{q-2}+\dots+\varepsilon+1 = 0$. Sada u (4) uvrstimo redom $x = 1, \varepsilon, \varepsilon^2, \dots, \varepsilon^{q-1}$ (napišite sami te jednakosti). Sada te jednakosti redom pomnožimo s $\varepsilon^0, \varepsilon^{-r}, \varepsilon^{-2r}, \dots, \varepsilon^{-(q-1)r}$ i tako dobivene izraze zbrojimo. Tada dobivamo

$$\sum_{k=0}^{q-1} (1+\varepsilon^k)^n \varepsilon^{-rk} = q\left[\binom{n}{r} + \binom{n}{r+q} + \binom{n}{r+2q} + \dots\right]. \qquad (+)$$

Pritom smo se koristili činjenicom da je

$$1 + \varepsilon^{k-r} + \varepsilon^{2(k-r)} + \dots + \varepsilon^{(q-1)(k-r)} = \begin{cases} 0 & , \text{za } k \not\equiv r \pmod q \\ q & , \text{za } k \equiv r \pmod q, \end{cases}$$

a to lako slijedi iz toga da je $\varepsilon^p = 1 \iff q$ dijeli p. Lijevu stranu od $(+)$ možemo napisati i ovako

$$\sum_{k=0}^{q-1} \left(\varepsilon^{\frac{k}{2}} + \varepsilon^{-\frac{k}{2}}\right)^n \varepsilon^{\frac{kn}{2}-kr},$$

a to je zbog $(e^{i\varphi})^n = (\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi$, jednako

$$\sum_{k=0}^{q-1} \left(2\cos\frac{k\pi}{q}\right)^n \left[\cos\frac{k(n-2r)}{q}\pi + i\sin\frac{k(n-2r)}{q}\pi\right]. \qquad (++)$$

No lijeva strana od $(+)$ je realan broj, jer je očito desna strana takva, pa je imaginarni dio od $(++)$ jednak nuli, i odatle slijedi tvrdnja.

Tako na primjer, uzmemo li $q = 2$, onda za $r = 0$ dobivamo $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \dots = \frac{1}{2}2^n = 2^{n-1}$, a za $r = 1$, $\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \dots = \frac{1}{2}2^n = 2^{n-1}$ (što već znamo od prije). Za $q = 3$ za $r = 0$ dobivamo $\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \dots = \frac{1}{3}(2^n + 2\cos\frac{n\pi}{3})$, za $r = 1$ dobivamo $\binom{n}{1} + \binom{n}{4} + \binom{n}{7} + \dots = \frac{1}{3}(2^n + 2\cos\frac{(n-2)\pi}{3})$ itd.

Primjerice, za $n = 15$ (bez puno računanja) nalazimo

$$\binom{15}{1} + \binom{15}{4} + \binom{15}{7} + \binom{15}{10} + \binom{15}{13} = \frac{1}{3}(2^{15} + 2\cos\frac{13\pi}{3}) = \frac{1}{3}(2^{15}+1) = 10923.$$

□

Kako smo već istaknuli, binomni koeficijenti su specijalni slučajevi multinomnih koeficijenata, a ovi se pojavljuju kao koeficijenti u prirodnoj generalizaciji binomnog teorema s više sumanada. Naime, vrijedi sljedeće.

TEOREM 2 (Multinomni teorem). *Za $n, k \in \mathbb{N}$ i bilo koje realne (ili kompleksne) brojeve $x_1, x_2, \dots, x_k$ vrijedi*

$$(x_1 + x_2 + \dots + x_k)^n = \sum_{\substack{n_1+\dots+n_k=n \\ n_1,\dots,n_k \ge 0}} \binom{n}{n_1, n_2, \dots, n_k} x_1^{n_1} x_2^{n_2} \dots x_k^{n_k}. \qquad (18)$$

Dokaz I. Indukcijom po n. Za $n = 1$ tvrdnja je trivijalna, a za korak indukcije treba nam "**multinomna Pascalova formula**" za multinomne koeficijente:

$$\binom{n}{n_1, n_2, \dots, n_k} = \sum_{i=1}^{k} \binom{n-1}{n_1, \dots, n_i - 1, \dots, n_k}.$$

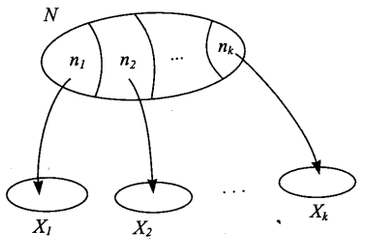
Ova se pak formula algebarski dokazuje jednostavno iz definicije multinomnih koeficijenata, dok se ona kombinatorno može ovako protumačiti. Njezina lijeva strana je broj različitih poredaka od n kuglica među kojima je n_i njih boje i, $i = 1, \dots, k$, dok njezina desna strana kaže na koliko načina možemo poredati ostalih $n-1$ kuglica, nakon što smo odabrali koja vrsta kuglica će biti na prvoj poziciji.

Sada induktivni korak nije nimalo teško provesti detaljno, pa to prepuštamo čitatelju. □

Dokaz II. Slično zaključivanje kao i dokaz II binomnog teorema provedite sami. □

Dokaz III (kombinatorni). I ovdje je ideja ista kao i (kombinatorni) dokaz III binomnog teorema.

Stoga uzmimo konačne skupove N i $X_1, X_2, \ldots, X_k$, $|N| = n$, $|X_i| = x_i$, $i = 1, \ldots, k$, X_i međusobno disjunktni. Tada lijeva strana od (18) broji sve funkcije $N \to \cup_{i=1}^{k} X_i$, a na desnoj opći član pod znakom sume broji koliko ima onih funkcija koje n_1 elemenata iz N preslikavaju u X_1, ..., n_k elemenata iz N preslikavaju u X_k. Prema tome, iz pravila sume slijedi tvrdnja. Sličica za "vizualce" je sljedeća:



□

Formula (18), dakle, kaže kako se $(x_1 + \cdots + x_k)^n$ "razvija" po potencijama od $x_1, x_2, \ldots, x_k$. Desna strana od (18) ima vrlo mnogo sumanada (toliko koliko i rješenja jednadžbe $n_1 + \cdots + n_k = n$ u cijelim ≥ 0 brojevima, a tih prema Propoziciji 9 ima $\binom{n+k-1}{n}$). No, teorem precizno služi za određivanje konkretnih koeficijenata. Tako, primjerice, želimo li odrediti koeficijent uz $x^2y^5z^5$ u razvoju od $(x+y+z)^{12}$, imamo prema (18):

$$\langle x^2y^5z^5\rangle(x+y+z)^{12} = \binom{12}{2,5,5} = \frac{12!}{2!5!5!} = 16632.$$

Ili, ako nas zanima koeficijent uz x^4yz^7 u razvoju od $(3x-5y+2z)^{12}$, onda je taj koeficijent jednak

$$\langle x^4yz^7\rangle(3x-5y+2z)^{12} = \binom{12}{4,1,7}3^4(-5)2^7 = -20528 \cdot 10^8,$$

slično je (provjerite):

$$\langle x^3y^4z^6\rangle(2x-y^2+2xy-3z^3)^7 = 15120.$$

Za $n = 2$ i $n = 3$, multinomni teorem daje "praktične" formule:

$$(x_1 + x_2 + \ldots)^2 = \sum_i x_i^2 + 2\sum_{i<j} x_ix_j,$$

$$(x_1 + x_2 + \ldots)^3 = \sum_i x_i^3 + 3\sum_{i<j} x_i^2x_j + 3\sum_{i<j} x_ix_j^2 + 6\sum_{i<j<k} x_ix_jx_k.$$

Ako binomna formula ima milijune zanimljivih posljedica, onda je malo reći da multinomna ima više od trilijun na trilijun: "think big" (šalu na stranu, ima ih beskonačno mnogo, prebrojivo ili više?).

Na primjer, ako u (18) stavimo $x_1 = x_2 = \cdots = x_k = 1$, dobivamo da je zbroj svih multinomnih koeficijenata

$$\sum_{\substack{n_1+\cdots+n_k=n \\ n_1,\ldots,n_k\geq 0}} \binom{n}{n_1,\ldots,n_k} = k^n.$$

A sada malo teorije brojeva.

Primjer 54. a) ("San brucoša"[9]). Ako je p prost broj, a $x_1, x_2, \ldots, x_k$ cijeli, onda dokažite da je

$$(x_1 + x_2 + \cdots + x_k)^p \equiv x_1^p + x_2^p + \cdots + x_k^p \pmod{p};$$

b) Za prirodan broj k i prost broj p dokažite tzv. **mali Fermatov teorem**

$$k^p \equiv k \pmod{p}.$$

Rješenje. a) Iz multinomnog teorema imamo

$$\left(\sum_{i=1}^{k} x_i\right)^p = x_1^p + x_2^p + \cdots + x_k^p + \sum \frac{p!}{n_1!n_2!\ldots n_k!}x_1^{n_1}x_2^{n_2}\ldots x_k^{n_k}.$$

U posljednjoj se sumi zbraja po svim $n_1, n_2, \ldots, n_k < p$, pa kako je p prost broj, očito je onda svaki njezin pribrojnik djeljiv s p. Odatle slijedi "tvrdnja brucoša".

b) Stavimo $x_1 = x_2 = \cdots = x_k = 1$ u a).

□

(Mala digresija: Za razliku od malog, tzv. **veliki Fermatov teorem** tvrdi da za cijeli broj $n \geq 3$, jednadžba $x^n + y^n = z^n$, $xyz \neq 0$, nema rješenja u cijelim brojevima. Prvi je to dokazao engleski matematičar Andrew Wiles 1994. godine. Dokaz je vrlo složen (oko 100 stranica), a zasniva se na suvremenim tehnikama eliptičkih krivulja i algebarske geometrije.)

Primjer 55. Dokažite da je $(k!)!$ djeljiv s $((k-1)!)!^k$.

Rješenje. Stavimo li u multinomni teorem $n_1 = n_2 = \cdots = n_k = (k-1)!$, onda je $n = n_1 + \cdots + n_k = k \cdot (k-1)! = k!$, pa je

$$\binom{n}{n_1,\ldots,n_k} = \frac{(k!)!}{((k-1)!)!\ldots((k-1)!)!} = \frac{(k!)!}{((k-1)!)!^k}.$$

Kako je multinomni koeficijent cijeli broj (npr. i zato jer ima kombinatorno značenje), tvrdnja slijedi. Već za $k = 4$ nije odmah evidentno da je $(4!)! = 24!$ djeljivo s $(3!)!^4 = 720^4$.

□

[9] Navodno, naivni brucoš na pitanje: kolika je p-ta potencija sume, odgovara: suma p-tih potencija. Donekle je i u pravu, ali samo do na $\equiv \pmod{p}$.

Ako u multinomnom teoremu "podvučemo" (ili "nadvučemo") sve eksponente, formula i dalje ostaje valjana s praktički istim (kombinatornim) dokazom, samo što tu imamo posla s injekcijama umjesto funkcijama. Dakle, vrijede sljedeće Vandermondeove formule u više varijabli.

PROPOZICIJA 13. *Za $n \in \mathbb{N}_0$ i $x_1, \ldots, x_k \in \mathbb{R}$ (ili $\mathbb{C}$) vrijedi*

$$\left(\sum_{i=1}^{k} x_i\right)^{\underline{n}} = \sum_{\substack{n_1+\cdots+n_k=n \\ n_1,\ldots,n_k \geq 0}} \binom{n}{n_1, \ldots, n_k} x_1^{\underline{n_1}} x_2^{\underline{n_2}} \ldots x_k^{\underline{n_k}}.$$

(I slična formula za "nadvučene" eksponente.)

Binomni red

Vratimo se opet malo binomnim koeficijentima. Zakon recipročnosti za binomne koeficijente (13) omogućuje nam da za zadane $n, t \in \mathbb{N}$ izračunamo alterniranu sumu $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} - \cdots + (-1)^t \binom{n}{t}$. Zaista, iz (13), Propozicije 8e) i opet iz (13) imamo redom

$$\sum_{k=0}^{t} (-1)^k \binom{n}{k} = \sum_{k=0}^{t} \binom{-n+k-1}{k} = \binom{-n+t}{t} = (-1)^t \binom{n-1}{t}. \qquad (19)$$

Tu se prirodno nameće pitanje: možemo li za zadane $n, t \in \mathbb{N}$ tako izračunati i zbroj $\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{t}$, tj. taj zbroj izraziti u obliku "zatvorene" formule pomoću n i t? Odgovor je: ne! To je dokazano tek 1977. godine s tzv. Gosperovim algoritmom koji omogućuje da se odluči je li nešto zbrojivo ili nije u terminima tzv. hipergeometrijskih redova potencija.

Prije nego što kažemo nešto o njima, navedimo dva primjera u kojima se "prirodno" i pojavljuju parcijalne sume binomnih koeficijenata (poslije ćemo vidjeti još neke; npr. Schläflijev teorem u idućem poglavlju).

Primjer 56. Binarne **n-kodirane riječi** čine neki skup "riječi" binarnih brojeva duljine n. Udaljenost između dviju kodiranih riječi definira se kao broj bitova u kojima se riječi razlikuju. Npr. udaljenost između 1001100100 i 0100111010 je 7. U prijenosu kodirane riječi postoji mogućnost pogreške. Ako je kompjuter pokazao riječ od n bitova, a ta riječ nije kodirana, pitanje je koju je riječ kompjuter trebao izbaciti? Kad bi postojala najbliža kodirana riječ (najmanje udaljena) od pokazane iskrivljene riječi, mogli bismo pretpostaviti da je upravo tu susjednu riječ kompjuter trebao iskazati. Problem je u tome da se provede takvo kodiranje da riječi budu dovoljno daleko, tako da se iskrivljene riječi mogu lako dešifrirati.

U hrvatskom jeziku neke riječi su dovoljno daleko jedna od druge i lako ih se dešifrira. Npr. ako nam se u brzojavu pojavi niz slova "ROĐENBAN", onda se on lako identificira kao iskrivljeno napisana korektna riječ. No postoje i riječi koje su bliske. Npr. niz slova "MZK" može biti iskrivljeno napisana riječ od više ispravnih različitih riječi. Spomenuta definicija udaljenosti zove se **Hammingova udaljenost**.

Ako je najmanja udaljenost između bilo kojih dviju kodiranih riječi $2r+1$, onda nijedan bezvezni niz slova (tj. "ne-riječ") ne može biti istodobno na udaljenosti $\leq r$ od dviju

različitih kodiranih riječi. U tom se slučaju taj skup zove **kodiranje s ispravljanjem grešaka reda r** (engl. r-error-correcting code). Drugim riječima, ako dobijemo riječ s najviše r grešaka, onda će ona biti najbliža točno jednoj pravoj kodiranoj riječi. S druge strane, da bismo riječi stavili dovoljno daleko jednu od druge, potrebno je mnogo bitova pa da dobijemo kodiranje s bogatim rječnikom.

Označimo s $M = M(n, r)$ najveći broj n-kodiranih riječi u kodiranju s ispravljanjem grešaka reda r. Kako velik može biti M? To pitanje je prema svojoj naravi kombinatorno i, ustvari, možemo se zapitati: koja su najbolja kodiranja s ispravljanjem grešaka? Mi ćemo se zadovoljiti jednom približnom ocjenom od M.

Za svaku od M kodiranih riječi ima više nizova koje ne mogu biti kodirane riječi. To su nizovi na udaljenosti 1 od nje, na udaljenosti 2 od nje, ..., na udaljenosti r od nje (i sama ta riječ na udaljenosti 0). n-nizova u bitovima koji su točno k daleko od dane riječi ima $\binom{n}{k}$, jer jednom kad ustanovimo koje k bitove treba mijenjati, onda je promjena jedinstvena, tj. 1 prelazi u 0, a 0 u 1. Svaka kodirana riječ eliminira točno

$$\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}$$

mogućih nizova. M kodiranih riječi tada eliminira

$$M\left[\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}\right]$$

riječi. Taj broj mora biti manji od 2^n = ukupan broj svih binarnih nizova duljine n. Stoga je

$$M \leq \frac{2^n}{\binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{r}}.$$

Ta se ograda zove **Hammingova ograda**.

Recimo da želimo promatrati riječi od 6 bitova i da možemo ispraviti jednu grešku. Neka je 100101 kodirana riječ. Tada se sve riječi s jednom promjenom (na udaljenosti 1) korigiraju na tu riječ. To su 000101, 110101, 101101, 100001, 100111, 100100. Na taj način svaka riječ eliminira ne samo sebe, nego i šest drugih riječi da budu kodirane. Ako ima M riječi u kodiranju (tj. $M = M(6,1)$), onda mora biti $7M \leq 2^6 = 64 \Rightarrow M \leq 9$, pa u kodiranju može biti najviše 9 riječi.

(O teoriji kodiranja vidi knjige [10], [141] [12*], [72*], [58*] i dr.)

Primjer 57. Hipergraf $H = (V(H), E(H))$ se sastoji od konačnog skupa vrhova $V(H)$ i familije $E(H)$ podskupova od $V(H)$ koji se zovu **hiperbrid** od H. Skup vrhova $A \subseteq V(H)$ se zove **raspršen** ako za svako $B \subseteq A$ postoji hiperbrid $E \in E(H)$, tako da je $E \cap A = B$. **Vapnik - Chernovenkisova dimenzija** (ili **VC-dimenzija**) od H je veličina najvećeg raspršenog podskupa od $V(H)$. Oznaka je VC-dim(H).

Ako hipergraf H ima n vrhova i VC-dim$(H) = d$, onda hiperbridova ima najviše

$$|E(H)| \leq \binom{n}{0} + \binom{n}{1} + \cdots + \binom{n}{d}.$$

Rješenje. Indukcijom. Prvo, tvrdnja je trivijalna za $d = 0$ ili $n \leq d$. Pretpostavimo da tvrdnja vrijedi za sve hipergrafove $\bar{H}$ za koje je VC-dim$(\bar{H}) < d$ i sve hipergrafove $\bar{H}$ za koje je VC-dim$(\bar{H}) = d$ i $|V(H)| < n$.

Neka je H hipergraf s $|V(H)| = n$ i VC-dim$(H) = d$. Neka je $x \in V(H)$ neki čvrsti vrh. Definirajmo dva nova hipergrafa H_1i H_2 ovako. $V(H_1) = V(H_2) = V(H) \setminus \{x\}$, a $E(H_1) = \{E \setminus \{x\} | E \in E(H)\}$, $E(H_2) = \{E \in E(H) | x \notin E, E \cup \{x\} \in E(H)\}$.

Tada je očito VC-dim$(H_1) \leq d$ i VC-dim$(H_2) \leq d-1$. Iz pretpostavke indukcije i Pascalove formule tada dobivamo:

$$|E(H)| = |E(H_1)| + |E(H_2)| \leq \sum_{i=0}^{d} \binom{n-1}{i} + \sum_{i=0}^{d-1} \binom{n-1}{i} = \sum_{i=0}^{d} \binom{n}{i}.$$

To je i najbolja ograda, jer ako je $E(H) = \{U \in V(H) | |U| \leq d\}$, onda je VC-dim$(H) = d$.

(Pojam VC-dimenzije je važan u teoriji vjerojatnosti, kombinatornoj geometriji i npr. sociologiji gdje je $V(H)$ uzorak društva, a $E(H)$ razne društvene skupine.) □

Hipergeometrijski red potencija proučavali su već i Euler i Gauss i Riemann, a definira se kao red potencija po z uz zadane parametre $a_1, \ldots, a_m, b_1, \ldots, b_n$ kao

$$F\left(\begin{matrix} a_1, \ldots, a_m \\ b_1, \ldots, b_n \end{matrix} \middle| z \right) = \sum_{k \geq 0} \frac{a_1^{\overline{k}} \ldots a_m^{\overline{k}}}{b_1^{\overline{k}} \ldots b_n^{\overline{k}}} \cdot \frac{z^k}{k!}.$$

To su vrlo općeniti i korisni redovi potencija koji uključuju mnoge poznate razvoje u red potencija, kao što su

$$F\left(\begin{matrix} \\ \end{matrix} \middle| z \right) = \sum_{k \geq 0} \frac{z^k}{k!} = e^z, \quad F\left(\begin{matrix} 1,1 \\ 1 \end{matrix} \middle| z \right) = \sum_{k \geq 0} z^k = \frac{1}{1-z}$$

$$F\left(\begin{matrix} a,1 \\ 1 \end{matrix} \middle| -z \right) = \sum_{k \geq 0} a^{\overline{k}} \frac{z^k}{k!} = \sum_{k \geq 0} \binom{a+k-1}{k} z^k = \frac{1}{(1-z)^a}$$

$$F\left(\begin{matrix} -a,1 \\ 1 \end{matrix} \middle| -z \right) = (1+z)^a, \quad zF\left(\begin{matrix} 1,1 \\ 2 \end{matrix} \middle| -z \right) = \ln(1+z) \text{ itd.}$$

Uostalom, kako smo već rekli, Newton je prvi promatrao beskonačne redove *formalno* poopćivši binomnu formulu: $(1+x)^a = 1 + \binom{a}{1}x + \binom{a}{2}x^2 + \ldots$. Pitanja oko konvergencije razriješena su tek mnogo kasnije. Podsjetimo se prvo tog važnog rezultata (za dokaz vidi npr. [133]) čime objašnjavamo i neke od gornjih formula.

TEOREM 3 (Binomni red). *Za sve $z \in \mathbb{C}$, $|z| < 1$ i sve $a \in \mathbb{R}$ vrijedi*

$$(1+z)^a = \sum_{k=0}^{\infty} \binom{a}{k} z^k = 1 + \binom{a}{1}z + \binom{a}{2}z^2 + \binom{a}{3}z^3 + \ldots. \tag{20}$$

Tako, na primjer, vrijede ovi razvoji u red potencija:

$$\frac{1}{1+z} = \sum_{k \geq 0} (-1)^k z^k = 1 - z + z^2 - \ldots; \quad \frac{1}{1-z} = \sum_{k \geq 0} z^k = 1 + z + z^2 + \ldots;$$

$$\frac{1}{(1+z)^{n+1}} = \sum_{k \geq 0} (-1)^k \binom{n+k}{n} z^k \ (n \in \mathbb{N}_0);$$

$$\frac{1}{(1-z)^{n+1}} = \sum_{k \geq 0} \binom{n+k}{n} z^k \ (n \in \mathbb{N}_0);$$

$$(1+z)^{1/2} = \sqrt{1+z} = 1 + \sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k \cdot 2^{2k-1}} \binom{2k-2}{k-1} z^k;$$

$$(1-4x)^{-1/2} = \frac{1}{\sqrt{1-4x}} = \sum_{k=0}^{\infty} \binom{2k}{k} x^k \text{ (tu je } a = -1/2,\ z = -4x,\ |x| < 1/4\text{), itd.}$$

Pri ovim smo razvojima prvo izračunali neke binomne koeficijente. Neki binomni koeficijenti koji se tu često javljaju su:

$$\binom{-1}{k} = (-1)^k, \ \binom{-(n+1)}{k} = (-1)^k \binom{n+k}{k},$$

$$\binom{1/2}{k} = \frac{1/2(1/2-1)\ldots(1/2-k+1)}{k!} = \frac{(-1)^{k-1} 1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2k-3)}{2^k \cdot k!} =$$

$$= (-1)^{k-1} \frac{1}{2^{2k-1}} \frac{1}{k} \binom{2k-2}{k-1},$$

i slično

$$\binom{-1/2}{k} = \frac{(-1)^k}{2^{2k}} \binom{2k}{k}, \quad \binom{-3/2}{k} = \frac{(-1)^k (2k+1)}{2^{2k}} \binom{2k}{k}.$$

Pokažimo na nekoliko primjera kako se neki (konačni) identiteti mogu (jednostavno) izvesti iz (beskonačnih) redova. Osnovna (prirodna) ideja je ova:

$$a_n = b_n, \ \forall n \in \mathbb{N}_0 \iff f(x) := \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} b_n x^n =: g(x)$$

tj. želimo li dokazati identitet $a_n = b_n$, nužno je i dovoljno dokazati $f(x) = g(x)$.

Primjer 58. Dokažite da za svako $n \in \mathbb{N}_0$ vrijedi:

a) $\sum_{k=0}^{n} \frac{1}{2^{2k}} \binom{2k}{k} = \frac{2n+1}{2^{2n}} \binom{2n}{n}$;

b) $\sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k} = \frac{1}{3}(2^{2n+1}+1)$;

c) $\sum_{k=0}^{n} \left(-\frac{1}{2}\right)^k \binom{n}{k} \binom{2k}{k} = \begin{cases} 0 & , n \text{ neparan} \\ \frac{1}{2^n}\binom{n}{n/2} & , n \text{ paran.} \end{cases}$

Rješenje. a) Označimo lijevu stranu s a_n i promotrimo red $f(x) := \sum_{n=0}^{\infty} a_n x^n$. Tada imamo:

$$\begin{aligned}
f(x) &= \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty}\sum_{k=0}^{n} \frac{1}{2^{2k}}\binom{2k}{k} x^n = \text{(zamjena redoslijeda sumacije)} = \\
&= \sum_{k=0}^{\infty} \frac{1}{2^{2k}}\binom{2k}{k} \sum_{n=k}^{\infty} x^n = \sum_{k=0}^{\infty} \frac{1}{2^{2k}}\binom{2k}{k}(x^k + x^{k+1} + x^{k+2} + \dots) = \\
&= \sum_{k=0}^{\infty} \frac{1}{2^{2k}}\binom{2k}{k} x^k(1 + x + x^2 + \dots) = \text{(binomni red za } a = -1) = \\
&= \sum_{k=0}^{\infty} \frac{1}{2^{2k}}\binom{2k}{k} x^k \frac{1}{1-x} = \frac{1}{1-x}\sum_{k=0}^{\infty} \frac{1}{2^{2k}}\binom{2k}{k} x^k = \\
&= \frac{1}{1-x}\sum_{k=0}^{\infty} \binom{2k}{k}\left(\frac{x}{4}\right)^k = \text{(binomni red za } a = -1/2) = \\
&= \frac{1}{1-x}\cdot\frac{1}{(1-x)^{1/2}} = \frac{1}{(1-x)^{-3/2}} = \text{(binomni red za } a = -3/2) = \\
&= \sum_{n=0}^{\infty}\binom{-3/2}{n}(-x)^n = \sum_{n=0}^{\infty}\frac{2n+1}{2^{2n}}\binom{2n}{n}x^n =: g(x).
\end{aligned}$$

Izjednačavanjem koeficijenata uz x^n od $f(x)$ i $g(x)$ slijedi tvrdnja.

b) Postupamo slično kao u a). Neka je opet lijeva strana a_n, te $f(x) := \sum_{n\geq 0} a_n x^n$. Tada je (obrazložite svaki korak):

$$\begin{aligned}
f(x) &= \sum_{n=0}^{\infty} a_n x^n = \sum_{n=0}^{\infty} x^n \sum_{k=0}^{n}\binom{n+k}{2k}2^{n-k} = \\
&= \sum_{k=0}^{\infty} 2^{-k}\sum_{n=k}^{\infty} 2^n x^n \binom{n+k}{2k} = \sum_{k=0}^{\infty} 2^{-k}(2x)^{-k}\sum_{n=0}^{\infty}\binom{n+k}{2k}(2x)^{n+k} = \\
&= \sum_{k=0}^{\infty} 2^{-k}(2x)^{-k}\frac{(2x)^{2k}}{(1-2x)^{2k+1}} = \frac{1}{1-2x}\sum_{k=0}^{\infty}\left(\frac{x}{1-2x}\right)^k = \\
&= \frac{1-2x}{(1-4x)(1-x)} = \frac{2}{3(1-4x)} + \frac{1}{3(1-x)} = \frac{2}{3}\sum_{n=0}^{\infty}(4x)^n + \frac{1}{3}\sum_{n=0}^{\infty}x^n = \\
&= \frac{1}{3}\sum_{n=0}^{\infty}(2\cdot 4^n + 1)x^n =: g(x),
\end{aligned}$$

i odavde opet izjednačavanjem koeficijenata uz x^n slijedi tvrdnja.

c) I ovdje možemo postupiti slično kao u a) i b) (pokušajte), ali je jednostavnije na sljedeći način. Prvo uočimo da iz binomne formule slijedi da je koeficijent uz x^0 od $(x+x^{-1})^{2k}$ jednak $\binom{2k}{k}$, tj.

$$\langle x^0\rangle(x+x^{-1})^{2k} = \binom{2k}{k}.$$

Odavde odmah slijedi da je lijeva strana (označena s a_n) jednaka

$$a_n = \langle x^0\rangle\left(1 - \frac{(x+x^{-1})^2}{2}\right)^n.$$

No, iz binomne formule je

$$\left(1 - \frac{(x+x^{-1})^2}{2}\right)^n = \frac{(-1)^n}{2^n}(x^2+x^{-2})^n = \frac{(-1)^n}{2^n}\sum_{k=0}^{n}\binom{n}{k}x^{4k-2n},$$

pa tvrdnja slijedi, uzmemo li koeficijent uz x^0 na desnoj strani. □

Iz ovih je primjera već jasno da prirodni okvir za formalne manipulacije s binomnim koeficijentima (i drugim) predstavljaju redovi i to tzv. formalni redovi potencija, a njih ćemo sustavno upoznati u poglavlju V funkcije izvodnice.

Binomni koeficijent

$\binom{n}{\lfloor n/2\rfloor}$.

Promotrimo sada jedan redak binomnih koeficijenata iz Pascalova trokuta:

$$\binom{n}{0}, \binom{n}{1}, \binom{n}{2}, \dots, \binom{n}{n}.$$

Kako se ponaša taj niz i koji je najveći član? Iz osnovne formule

$$\binom{n}{k} = \frac{n!}{k!(n-k)!},$$

odmah slijedi da je (vidi i Primjer 35):

$$\binom{n}{k} = \frac{n-k+1}{k}\binom{n}{k-1}.$$

Odavde odmah vidimo da je za $n-k+1 \geq k$, $\binom{n}{k} \geq \binom{n}{k-1}$, tj. za $k \leq n/2$ vrijedi $\binom{n}{k} > \binom{n}{k-1}$. Obrnuto, za $k \geq n/2$ je $\binom{n}{k} > \binom{n}{k+1}$. Prema tome, za dano n, najveći od binomnih koeficijenata $\binom{n}{k}$ je srednji. Za n paran, $\binom{n}{n/2}$ je veći od ostalih, a za n neparan dva najveća su $\binom{n}{\lfloor n/2\rfloor} = \binom{n}{\lceil n/2\rceil}$.

Kao funkcija od k, niz $\binom{n}{0}, \binom{n}{1}, \dots, \binom{n}{k}, \dots, \binom{n}{n}$ se ponaša tako da do sredine (tj. do $k = \lfloor n/2\rfloor$) niz raste, a dalje pada.

Općenito kažemo da je (konačan) niz realnih brojeva

$$a_0, a_1, a_2, \dots, a_n$$

unimodalan ako do nekog mjesta raste, pa onda pada; točnije ako postoji j, tako da je $a_0 \leq a_1 \leq \dots \leq a_{j-1} \leq a_j \geq a_{j+1} \geq \dots \geq a_n$. Broj j se zove **vrhunac** takvog niza. Dokazali smo, dakle:

PROPOZICIJA 14. *Niz binomnih koeficijenata* $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$ *je unimodalan i vrhunac mu je za* $k = \lfloor n/2 \rfloor$.

O nizu $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ se može reći i nešto više, a to je da je log-konkavan. Kažemo da je niz (nenegativnih) brojeva $a_0, a_1, \ldots, a_n$ **log-konkavan** ako je $a_k^2 \geq a_{k-1}a_{k+1}$ za svako k, a **log-konveksan** ako je $a_k^2 \leq a_{k-1}a_{k+1}$, za svako k. Lako je provjeriti da za svako k vrijedi

$$\binom{n}{k}^2 \geq \binom{n}{k-1}\binom{n}{k+1},$$

pa je, dakle, $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{n}$ i log-konkavan niz. Niz pozitivnih brojeva (a_k) je log-konkavan ako i samo ako je (a_{k+1}/a_k) padajući, pa stoga log-konkavnost povlači unimodalnost. Obrat ne vrijedi, npr. za niz $1, 1/2, \ldots, 1/n$.

Kako je velik srednji binomni koeficijent? Gruba procjena je

$$\frac{2^n}{n+1} \leq \binom{n}{\lfloor n/2 \rfloor} \leq 2^n,$$

što odmah izlazi odatle da je suma svih $n+1$ binomnih koeficijenata $\binom{n}{k}$ jednaka 2^n, a srednji je najveći. Dokažimo i bolju procjenu. Uzmimo parni "brojnik" (za neparni je slično). Tada vrijedi ova aproksimacija

$$\frac{2^{2m}}{2\sqrt{m}} \leq \binom{2m}{m} \leq \frac{2^{2m}}{\sqrt{2m}}. \qquad (*)$$

Zaista, promotrimo broj

$$P = \frac{1 \cdot 3 \cdot 5 \cdot \cdots \cdot (2m-1)}{2 \cdot 4 \cdot 6 \cdot \cdots \cdot 2m} = \frac{(2m-1)!!}{(2m)!!} = \frac{(2m)!}{2^{2m}m!^2} = \frac{1}{2^{2m}}\binom{2m}{m}.$$

Tada je $(*)$ ekvivalentno s

$$\frac{1}{2\sqrt{m}} \leq P \leq \frac{1}{\sqrt{2m}}. \qquad (**)$$

Gornju ogradu u $(**)$ dobijemo tako da promotrimo produkt

$$\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{4^2}\right)\cdots\left(1-\frac{1}{(2m)^2}\right) = \left(\frac{1\cdot 3}{2^2}\right)\cdot\left(\frac{3\cdot 5}{4^2}\right)\cdots \cdots\left(\frac{(2m-1)\cdot(2m+1)}{(2m)^2}\right) = (2m+1)P^2.$$

Vrijednost produkta na lijevoj strani je ≤ 1, pa slijedi $P \leq 1/\sqrt{2m}$. Donju ogradu u $(**)$ dobijemo tako da promotrimo produkt

$$\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\cdots\left(1-\frac{1}{(2m-1)^2}\right) = \left(\frac{2\cdot 4}{3^2}\right)\cdot\left(\frac{4\cdot 6}{5^2}\right)\cdots \cdots\left(\frac{(2m-2)\cdot(2m)}{(2m-1)^2}\right) = \frac{1}{2\cdot 2m\cdot P^2}.$$

Opet je lijeva strana ≤ 1, pa dobivamo donju ogradu u $(**)$.

Ustvari, iz Stirlingove aproksimacije za $n!$ slijedi $\binom{2m}{m} \sim 4^m/\sqrt{\pi m}$, odnosno

$$\binom{n}{\lfloor n/2 \rfloor} \sim \sqrt{\frac{2}{\pi n}}2^n,$$

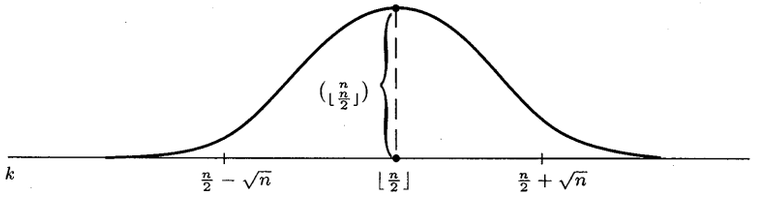
ili još točnije

$$\binom{n}{\lfloor n/2 \rfloor} \sim \sqrt{\frac{2}{\pi n}}2^n\left(1 - \frac{1}{4n} + \frac{1}{64n^2} + O(n^{-3})\right).$$

Važno kombinatorno značenje srednjeg binomnog koeficijenta vidjet ćemo poslije (Spernerov teorem u poglavlju IV).

Bilješka. Ponašanje niza $\binom{n}{0}, \binom{n}{1}, \ldots, \binom{n}{k}, \ldots, \binom{n}{n}$ kao funkcije od k za "velike" n, a k blizu $n/2$ pokazano je na donjoj slici. Graf od $\binom{n}{k}$ nije, doduše, neprekidna krivulja (jer $\binom{n}{k}$ je definiran samo za cijele k), ali ako je n vrlo velik, onda se vizualno puno točaka stopi u jednu krivulju. Visina te "zvonolike" krivulje je $\binom{n}{\lfloor n/2 \rfloor}$, a širina "zvona" od sredine je otprilike $1.5\sqrt{n}$ (tj. cijelog zvona $\approx 3\sqrt{n}$).

S druge strane, graf funkcije $x \mapsto e^{-x^2/2}$ izgleda isto tako "zvonoliko". Ta krivulja (tzv. **Gaussova krivulja**) je u izvjesnom smislu limes krivulja binomnih koeficijenata kada $n \to \infty$. Ta je krivulja od presudne važnosti u teoriji vjerojatnosti, matematičkoj statistici i drugdje, jer opisuje tipičnu razdiobu odstupanja, tj. grešaka u obradi podataka od neke srednje (normalne) vrijednosti, ako se radi o tzv. normalnoj razdiobi (ili normalnoj distribuciji), vidi npr. knjige [73], [206], [214].



q-binomni koeficijenti (ili Gaussovi binomni koeficijenti)[10]

Neka je $\mathbb{F}_q$ konačno polje od q elemenata (znamo da je $\mathbb{F}_q \approx (\mathbb{Z}_p)^r$, pa je $q = p^r$ potencija nekog prostog broja p). Neka je $V_n(q)$ n-dimenzionalni vektorski prostor nad $\mathbb{F}_q$, tj. $V_n(q)$ je izomorfan s $\mathbb{F}_q^n = \{(\alpha_1, \ldots, \alpha_n) | \alpha_i \in \mathbb{F}_q\}$ i ima q^n elemenata. Zanima nas koliko ima k-dimenzionalnih potprostora u $V_n(q)$. Taj broj označavamo s

$$\binom{n}{k}_q$$

i zovemo **q-binomni koeficijent** ili **Gaussov binomni koeficijent**.

[10] Čitatelj koji ne zna ništa o konačnim poljima, u prvom čitanju može preskočiti ovu točku.

Obični binomni koeficijent prebrojava k-podskupove konačnog n-članog skupa, a q-binomni koeficijent prebrojava k-dimenzionalne potprostore n-dimenzionalnog vektorskog prostora nad konačnim poljem od q elemenata. Osnovna veza među binomnim koeficijentima i (padajućim) faktorijelima je (Propozicija 7):

$$k!\binom{n}{k} = n^{\underline{k}}.$$

To smo dokazali tako da smo na dva načina prebrojili injekcije $[k] \to [n]$. Na isti način postupimo i ovdje. Prvo označimo s $[n^{\underline{k}}]_q$ broj monomorfizama (tj. linearnih injekcija) $V_k(q) \to V_n(q)$, za $k \leq n$. Dalje, q-**faktorijel broja** n definiramo kao

$$n!_q = (1)_q \cdot (2)_q \cdot \cdots \cdot (n)_q,$$

gdje je $(j)_q = 1 + q + \cdots + q^{j-1} = \frac{q^j-1}{q-1}$ i $0!_q := 1$.

LEMA 1. $[n^{\underline{k}}]_q = (q^n-1)(q^n-q)\cdot\cdots\cdot(q^n-q^{k-1}) = \frac{n!_q}{(n-k)!_q}$. *Posebno, za* $n = k$ *je* $[k^{\underline{k}}]_q = k!_q = (q^k-1)(q^k-q)\cdot\cdots\cdot(q^k-q^{k-1})$.

Dokaz. Ako je $(e_1, \ldots, e_k)$ baza od $V_k(q)$, onda je monomorfizam $f : V_k(q) \to V_n(q)$ potpuno određen s uređenom k-torkom $(f(e_1), \ldots, f(e_k)) = (v_1, \ldots, v_k)$ linearno nezavisnih vektora iz $V_n(q)$. Vektor v_1 možemo izabrati na $q^n - 1$ načina (svi osim nulvektora), pa onda v_2 na $q^n - q$ načina (svi osim λv_1, gdje je $\lambda \in \mathbb{F}_q$), v_3 na $q^n - q^2$ načina (svi osim $\lambda v_1 + \mu v_2$, gdje su $\lambda, \mu \in \mathbb{F}_q$) itd. Dakle, ukupno na $(q^n-1)(q^n-q)\cdot\cdots\cdot(q^n-q^{k-1})$ načina. □

PROPOZICIJA 15.

$$\binom{n}{k}_q = \frac{(q^n-1)(q^n-q)\ldots(q^n-q^{k-1})}{(q^k-1)(q^k-q)\ldots(q^k-q^{k-1})} = \frac{(q^n-1)(q^{n-1}-1)\ldots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\ldots(q-1)}. \tag{21}$$

Dokaz. Tvrdimo da je

$$k!_q \cdot \binom{n}{k}_q = [n^{\underline{k}}]_q.$$

Svaki monomorfizam $f : V_k(q) \to V_n(q)$ je potpuno određen izborom k-dimenzionalnog potprostora $W \subseteq V_n(q)$, što možemo odabrati na $\binom{n}{k}_q$ načina, pa potom izborom jednog izomorfizma $\pi : W \to W$, što možemo odabrati na $k!_q$ načina. Pridruživanje $f \mapsto (W, \pi)$ je bijekcija (opišite inverz), pa tvrdnja slijedi. Propozicija tada slijedi iz Leme 1. □

Zbog $q^j - 1 = (q-1)(1 + q + \cdots + q^{j-1})$, formulu (21) možemo napisati u potpunoj analogiji s običnim binomnim koeficijentima:

$$\binom{n}{k}_q = \frac{n!_q}{k!_q \cdot (n-k)!_q}. \tag{22}$$

Očito je $\binom{n}{0}_q = 1$, te (q-simetrija): $\binom{n}{k}_q = \binom{n}{n-k}_q$. Nadalje, izravnom provjerom se može lako pokazati q-**Pascalova formula**:

$$\binom{n}{k}_q = \binom{n-1}{k}_q + q^{n-k}\binom{n-1}{k-1}_q.$$

Odavde i iz "početnog uvjeta" $\binom{n}{0}_q = 1$, indukcijom se pokazuje da je $\binom{n}{k}_q$ polinom u varijabli q s nenegativnim cijelim koeficijentima, stupnja $k(n-k)$. Na primjer $\binom{5}{2}_q = 1 + q + 2q^2 + 2q^3 + 2q^4 + q^5 + q^6$. Pustimo li $q \to 1$, iz (21) odmah dobivamo

$$\lim_{q\to 1}\binom{n}{k}_q = \binom{n}{k}.$$

(U nekom smislu možemo reći da "vektorski prostori nad jednočlanim poljima postaju skupovi", iako svako polje ima bar dva elementa: 0 i 1.)

Mnoga svojstva binomnih koeficijenata imaju svoje q-analogone. Tako npr. vrijedi q-unimodalnost, q-Vandermondeova konvolucija, q-binomni teorem (vidi Primjer 17 pogl. IV),

$$b_n = \sum_{k=0}^{n}\binom{n}{k}_q a_k \iff a_n = \sum_{k=0}^{n}(-1)^{n-k}q^{\binom{n-k}{2}}\binom{n}{k}_q b_k,$$

itd., što sve za $q \to 1$ prelazi u udgovarajuće tvrdnje za binomne koeficijente.

q-**multinomni koeficijent** za $n_1, \ldots, n_k \in \mathbb{N}_0$ i $n = n_1 + \cdots + n_k$ se definira kao

$$\binom{n}{n_1, \ldots, n_k}_q := \frac{n!_q}{n_1!_q n_2!_q \ldots n_k!_q}. \tag{23}$$

Sada iz (22) nije teško provjeriti da vrijedi q-analogon Propozicije 11:

$$\binom{n}{n_1, \ldots, n_k}_q = \binom{n}{n_1}_q \binom{n-n_1}{n_2}_q \binom{n-n_1-n_2}{n_3}_q \cdots \binom{n_k}{n_k}_q, \tag{24}$$

prema tome, i to je polinom u q s cijelim ≥ 0 koeficijentima.

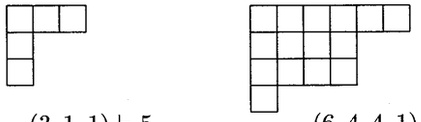
Kombinatorno značenje q-multinomnog koeficijenta (23) jest broj uređenih k-torki potprostora $(W_1, \ldots, W_k)$ od $V_n(q)$, $\dim W_i = n_i$, $i = 1, \ldots, k$, tako da je $V_n(q)$ Kartezijev produkt $W_1 \times \cdots \times W_k$.

§ 7. Particije brojeva i skupova i još neke kombinatorne veličine

Particije brojeva

Za razliku od rastava prirodnog broja, sada ćemo definirati particiju broja. **Particija broja** $n \in \mathbb{N}$ je prikaz broja n kao zbroja (sume) prirodnih brojeva. Pritom poredak sumanada nije važan. Na primjer, sve particije broja 5 su: $5 = 1 + 1 +$

$1+1+1$, $5=2+1+1+1$, $5=2+2+1$, $5=3+1+1$, $5=3+2$, $5=4+1$, te $5=5$. Kako poredak sumanada nije važan, mi ćemo uvijek smatrati da padaju (točnije, ne rastu). Dakle, particija od n je niz $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_k)\in\mathbb{N}^k$ pri čemu je $\lambda_1\geq\cdots\geq\lambda_k\geq 1$ i $\lambda_1+\lambda_2+\cdots+\lambda_k=n$. Kažemo da tada particija λ ima k **dijelova** $\lambda_1,\ldots,\lambda_k$. Ako je λ particija od n, pišemo $\lambda\vdash n$. Na primjer, $\lambda=(3,1,1)\vdash 5$. Particiju broja često je pogodno crtati pomoću tzv. **Ferrerovog** (ili **Youngovog**) **dijagrama**. Ako je $\lambda=(\lambda_1,\lambda_2,\ldots,\lambda_k)\vdash n$, onda je Ferrerov dijagram tablica koja ima u prvom retku λ_1 kvadratića, u drugom λ_2 kvadratića itd. Primjeri su na idućoj slici.



$(3,1,1)\vdash 5$ $\qquad$ $(6,4,4,1)\vdash 15$

Već vam je jasno što bi mi željeli izračunati: broj particija broja n i isto tako broj particija od n pod raznim dodatnim uvjetima. Najčešće su ove oznake u uporabi:

$p(n)$:= ukupni broj particija od n,
$p_k(n)$:= broj particija od n u točno k dijelova,
$p'_k(n)$:= broj particija od n u najviše k dijelova,
$p(n,k,r)$:= broj particija od n u najviše k dijelova, svaki $\leq r$,
$\bar{p}(n)$:= broj particija od n u različite dijelove,

zatim za zadani podskup $S\subseteq\mathbb{N}$ (npr. parni; prosti itd.)

$p_S(n)$:= broj particija od n čiji su dijelovi iz S,
$p_{S,k}(n)$:= broj particija od n u točno k dijelova, a svaki iz S,
$\bar{p}_S(n)$:= broj particija od n u različite dijelove, svaki iz S itd.

Tako je, npr. $p(5)=7$, $p_3(5)=2$, $p(5,3,3)=3$ itd. Po definiciji je još $p_0(0)=p(0)=1$. Odmah kažimo da je vrlo teško naći eksplicitne formule za te veličine, ali su poznate razne veze među tim veličinama i neke posebne vrijednosti.

Tako je, primjerice, jasno sljedeće: $p_n(n)=1$, $p_{n-1}(n)=1$ $(n>1)$, $p_1(n)=1$, $p_2(n)=\lfloor n/2\rfloor$, $p(n)=p_1(n)+p_2(n)+\cdots+p_n(n)$, $p'_k(n)=p_1(n)+p_2(n)+\cdots+p_k(n)$. Brojevi $p(n)$ vrlo brzo rastu, pa je tako $p(10)=42$, $p(20)=627$, $p(50)=204226$, $p(100)=190569292$, $p(200)\approx 4\cdot 10^{12}$ itd. **Hardy-Ramanujanova asimptotska formula** glasi (vidi [9] ili [203]):

$$p(n)\sim\frac{1}{4n\sqrt{3}}e^{\pi\sqrt{2n/3}}.$$

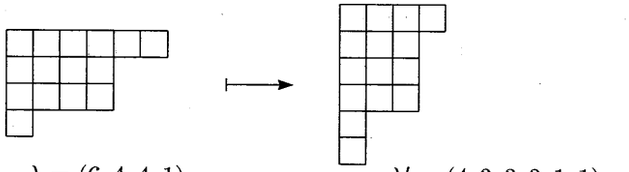
PROPOZICIJA 16. *a) Broj particija od n u najviše k dijelova (tj. $p'_k(n)$) jednak je broju particija od n u dijelove, od kojih je svaki $\leq k$;*

b) $p_k(n)=p_{k-1}(n-1)+p_k(n-k)$ (rekurzija za brojeve $p_k(n)$);

c) $p(n)=p_n(2n)$

*d) (**Euler**) Broj particija od n u neparne dijelove jednak je broju particija od n u različite dijelove.*

Dokaz. a) Konstruirat ćemo bijekciju između pripadnih skupova particija. Prvo nam treba pojam konjugirane particije. Ako je $\lambda=(\lambda_1,\lambda_2,\ldots)$ neka particija od n, pa ako u pripadnom Ferrerovom dijagramu zamijenimo retke i stupce (tj. transponiramo ga), dobijemo **konjugiranu particiju** $\lambda'=(\lambda'_1,\lambda'_2,\ldots)$ od n. Očito je $\lambda'_i=\#\{j|\lambda_j\geq i\}$. $\lambda\mapsto\lambda'$ je tražena bijekcija (inverz je opet konjugiranje i $(\lambda')'=\lambda$); npr. na idućoj slici je $k=4$.



$\lambda=(6,4,4,1)$ $\qquad$ $\lambda'=(4,3,3,3,1,1)$

b) Ako particija od n u k dijelova ima jedinicu (kao dio), onda ostatak $n-1$ možemo particionirati na $p_{k-1}(n-1)$ načina, a ako pak nema jedinicu, onda svakom dijelu oduzmimo jedinicu i imamo $p_k(n-k)$ particija ostatka $n-k$ u k dijelova. I ovo je bijekcija.

c) Slijedi iz b). Naime, $p_n(2n)=p_{n-1}(2n-1)+p_n(n)=p_{n-2}(2n-2)+p_{n-1}(n)+p_n(n)=\cdots=p_1(n)+p_2(n)+\cdots+p_n(n)=p(n)$.

d) Bijekciju definiramo ovako. Neka je $n=r_1\cdot 1+r_3\cdot 3+r_5\cdot 5+\ldots$ particija broja n u neparne dijelove (r_1 jedinica, r_3 trojki itd.) Sada svaki r_i napišemo u binarnome zapisu, pa imamo

$$n=(2^{a_1}+2^{b_1}+\ldots)\cdot 1+(2^{a_3}+2^{b_3}+\ldots)\cdot 3+(2^{a_5}+2^{b_5}+\ldots)\cdot 5+\ldots.$$

Tada dobivamo

$$n=2^{a_1}+2^{b_1}+\cdots+2^{a_3}\cdot 3+2^{b_3}\cdot 3+\cdots+2^{a_5}\cdot 5+2^{b_5}\cdot 5+\ldots,$$

a ovo je particija od n u različite dijelove, jer je $a_i>b_i>\ldots$. Ovo pridruživanje očito možemo invertirati, pa je bijekcija. (Drugi dokaz ćemo dati pomoću funkcija izvodnica u pogl. V.)

□

Zanimljiva je veza između brojeva particija i q-binomnih koeficijenata. Rekli smo da su ovi potonji polinomi u q. Tada je $p(n,k,r)$ jednak koeficijentu uz q^n od $\binom{r+k}{k}_q$. To se može dokazati indukcijom iz q-Pascalove formule, a može se i kombinatorno. Mi ćemo se na particije brojeva vratiti u pogl. V funkcije izvodnice.

Particije skupova i Stirlingovi brojevi prve i druge vrste

Podsjetimo se da je **particija** n-članog **skupa** familija nepraznih disjunktnih podskupova čija je unija čitav n-člani skup. Ti podskupovi se zovu **blokovi particije**, a ako ih ima k, govorimo o particiji n-članog skupa u k blokova ili o k-particiji skupa. Npr., $\{\{1,4\},\{2\},\{3,5\}\}$ je 3-particija 5-članog skupa [5].

Označimo sa $S(n,k)$ broj k-particija n-članog skupa. Dodatno definiramo $S(0,0) := 1$. Broj $S(n,k)$ zove se **Stirlingov broj druge vrste** ili **Stirlingov particijski broj**. U uporabi je često i simbol $\left\{ {n \atop k} \right\}$.

Drugim riječima, $S(n,k)$ (ili $\left\{ {n \atop k} \right\}$) je broj relacija ekvivalencije s točno k klasa ekvivalencije na n-članom skupu. Ili, još jednostavnijim riječima, $S(n,k)$ je broj načina da se n različitih kuglica (npr. numeriranih s $1,2,\ldots,n$) stavi u k jednakih kutija (poredak kutija nije bitan) tako da nijedna kutija ne ostane prazna.

Očito je $S(n,k) = 0$ za $k > n \geq 1$, a $S(n,0) = S(0,k) = 0$ za $k,n \in \mathbb{N}$. Dalje, jasno je da je $S(n,n) = 1$, a $S(n,n-1) = \binom{n}{2}$, jer $n-1$ blokova n-članog skupa znači da su u samo jednom bloku dva elementa, a u ostalima po jedan, pa je $S(n,n-1)$ broj 2-članih podskupova n-članog skupa. $S(n,2) = 2^{n-1} - 1$, jer particija u samo dva bloka potpuno je određena jednim blokom, a taj može biti bilo koji neprazan pravi podskup, pa izbora za jedan od blokova ima $2^n - 2$, a kako je poredak blokova nebitan, slijedi $S(n,2) = (2^n - 2)/2 = 2^{n-1} - 1$.

Kako dalje računati $S(n,k)$-ove (ili ako više volite $\left\{ {n \atop k} \right\}$-ove)? Jedan je način pomoću osnovne rekurzije za te brojeve:

PROPOZICIJA 17 (Osnovna rekurzija za $S(n,k)$). *Za $k,n \in \mathbb{N}$ vrijedi*

$$S(n,k) = S(n-1,k-1) + kS(n-1,k). \tag{25}$$

Dokaz. Želimo particionirati n-člani skup, recimo $[n]$, u k blokova. Uočimo jedan istaknuti element u našem skupu, npr. $n \in [n]$. Sada imamo dvije vrste k-particija od $[n]$: one u kojima je $\{n\}$ blok, pa ostatak možemo particionirati na $S(n-1,k-1)$ načina i one u kojima je n u bloku s drugim elementima iz $[n-1]$. Imamo $S(n-1,k)$ k-particija od $[n-1]$, pa n možemo ubaciti u neki od blokova na k načina, čime dobivamo $kS(n-1,k)$ načina. Prema tome (iz pravila sume), slijedi formula. □

S ovom rekurzijom i početnim vrijednostima možemo načiniti tablicu za brojeve $S(n,k)$, tzv. **Stirlingov trokut** (kao Pascalov trokut za binomne koeficijente; zbog prostora ovdje umjesto $S(n,k)$ pišemo $\left\{ {n \atop k} \right\}$, a ovaj simbol i više nalikuje na $\binom{n}{k}$):

n	$\left\{ {n \atop 0} \right\}$	$\left\{ {n \atop 1} \right\}$	$\left\{ {n \atop 2} \right\}$	$\left\{ {n \atop 3} \right\}$	$\left\{ {n \atop 4} \right\}$	$\left\{ {n \atop 5} \right\}$	$\left\{ {n \atop 6} \right\}$	$\left\{ {n \atop 7} \right\}$	$\left\{ {n \atop 8} \right\}$	$\left\{ {n \atop 9} \right\}$	$\cdots$
0	1										
1	0	1									
2	0	1	1								
3	0	1	3	1							
4	0	1	7	6	1						
5	0	1	15	25	10	1					
6	0	1	31	90	65	15	1				
7	0	1	63	301	350	140	21	1			
8	0	1	127	966	1701	1050	266	28	1		
9	0	1	255	3025	7770	6951	2646	462	36	1	
⋮											

Primjer 59. Svaku od $n = 10$ različitih razglednica želimo poslati svojim prijateljima kojih je $k = 7$ i to tako da svaki prijatelj dobije bar jednu razglednicu. Na koliko načina to možemo učiniti?

Rješenje. Skup $R = \{R_1,\ldots,R_n\}$ od n razglednica moramo "razbiti" na k blokova. Iz svake takve particije imamo $k!$ načina da pošaljemo razglednice. Stoga je odgovor (prema pravilu produkta) jednak $k!S(n,k)$. U posebnom slučaju, iz rekurzije (25) nađemo prvo $S(10,7) = S(9,6) + 7 \cdot S(9,7) = $ (iz tablice) $= 2646 + 7 \cdot 462 = 5880$, pa je odgovor $7!S(10,7) = 29635200$ (zamalo 30 milijuna!). □

Sljedeća formula nam daje još bolji kombinatorni uvid u Stirlingove brojeve (kao binomna formula (4) za binomne koeficijente):

PROPOZICIJA 18. *Za svako $n \in \mathbb{N}_0$ i sve $x \in \mathbb{R}$ (ili iz $\mathbb{C}$) vrijedi*

$$x^n = \sum_{k=0}^{n} S(n,k)x^{\underline{k}}. \tag{26}$$

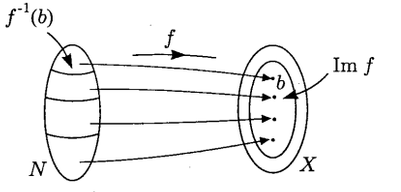
Dokaz I. Indukcijom po n. Za $n = 0$ (i $n = 1$) formula je očita. Pretpostavimo da vrijedi za brojeve $\leq n-1$. Tada iz $x^{\underline{k+1}} = x^{\underline{k}}(x-k)$ slijedi $x \cdot x^{\underline{k}} = x^{\underline{k+1}} + kx^{\underline{k}}$, pa uporabom rekurzije (25) imamo

$$\begin{aligned} x^n = x \cdot x^{n-1} &= x\sum_k S(n-1,k)x^{\underline{k}} = \sum_k S(n-1,k)x^{\underline{k+1}} + \\ &+ \sum_k S(n-1,k)kx^{\underline{k}} = \sum_k S(n-1,k-1)x^{\underline{k}} + \sum_k kS(n-1,k)x^{\underline{k}} = \\ &= \sum_k (S(n-1,k-1) + kS(n-1,k))x^{\underline{k}} = \sum_k S(n,k)x^{\underline{k}}. \end{aligned}$$

□

Dokaz II (kombinatorni). (26) je jednakost dvaju polinoma u varijabli x, pa je dovoljno dokazati da ona vrijedi za svaki prirodni broj x. Neka su N i X skupovi s $|N| = n$ i $|X| = x$. Lijeva strana od (26) broji sve funkcije $f : N \to X$. Tvrdimo da sve te funkcije možemo prebrojiti i desnom stranom.

Neka je $f : N \to X$ i neka je slika od f, tj. $\operatorname{Im} f$ neki k-člani skup u X. Tada skup svih originala $\{f^{-1}(b) | b \in \operatorname{Im} f\} =: \operatorname{Ker} f$. (tzv. **jezgra** od f) očito definira jednu k-particiju od N i prirodnu injekciju $f' : \operatorname{Ker} f \to X$ definiranu s $f'(f^{-1}(b)) = b$. No, k-particije od N možemo odabrati na $S(n,k)$ načina, a onda ovih injekcija f' na $x^{\underline{k}}$ načina. Stoga ukupno uređenih parova $(\operatorname{Ker} f, f')$ ima $S(n,k)x^{\underline{k}}$. Za čvrsto k je $f \mapsto (\operatorname{Ker} f, f')$ bijekcija, pa zbog pravila sume i svih funkcija $N \to X$ ima kao na desnoj strani od (26). Sličica za "vizualce":



□

Kao posljedicu odmah dobivamo

KOROLAR 4. *Broj svih surjekcija n-članog na x-člani skup je jednak*

$$x!S(n,x).$$

Dokaz. Naime, kao u prethodnom dokazu II, ako je $f : N \to X$ surjekcija, onda je $\operatorname{Im} f = X$, pa je i $|\operatorname{Ker} f| = x$ i stoga $f' : \operatorname{Ker} f \to X$ bijekcija, a ovih ima $x!$. Odatle slijedi tvrdnja kao i u dokazu II. (Ovo je, zapravo, isto zaključivanje kao rješenje prethodnog primjera, samo izrečeno "učeno".) □

Osim osnovne rekurzije (25), Stirlingovi particijski brojevi zadovoljavaju i druge rekurzije ili identitete (pišemo ih s pomakom indeksa, jer tako postaju ljepše):

PROPOZICIJA 19. *Za $n, m \in \mathbb{N}_0$ vrijedi*

a) $S(n+1,m+1) = \sum_{k=0}^{n} \binom{n}{k} S(k,m)$;

b) $S(m+n+1,m) = \sum_{k=0}^{n} kS(n+k,k)$;

c) $S(n+1,m+1) = \sum_{k=0}^{n} (m+1)^{n-k} S(k,m)$.

Dokaz. a) Sve particije od $[n+1]$ u $m+1$ blokova možemo izvršiti i tako da prvo uklonimo blok B koji sadrži $n+1$. Ako B ima k elemenata, onda ostatak od $n+1-k$ možemo particionirati u m blokova na $S(n+1-k,m)$ načina, a blok B možemo izabrati na $\binom{n+1-1}{k-1} = \binom{n}{k-1}$ načina, pa ukupno tu ima $\binom{n}{k-1} S(n+1-k,m)$ izbora. Sumiranjem po k, pa onda zamjenom $n+1-k \leftarrow k$, slijedi tvrdnja.

b) To slijedi višestrukom primjenom osnovne rekurzije (25) (a može i izravno – pokušajte).

c) Prepuštamo čitatelju.

□

U pogl. IV o formuli uključivanja–isključivanja izračunat ćemo $S(n,m)$ pomoću binomnih koeficijenata.

Označimo s B_n ukupni broj particija (ili relacija ekvivalencija) na n-članom skupu. Taj se broj zove n-ti **Bellov**[11] **broj**. Dodatno definiramo $B_0 := 1$. Očito je $B_n = \sum_{k=1}^{n} S(n,k)$, $n \geq 1$. Bellovi brojevi su tako izraženi preko Stirlingovih, ali oni se rekurzivno mogu računati na sljedeći način.

PROPOZICIJA 20. *Za svako $n \in \mathbb{N}_0$ vrijedi*

$$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k.$$

[11] Eric Temple Bell (1883 -1960), američki matematičar

Dokaz. Opet možemo istaknuti element $(n+1)$-članog skupa na kojem gledamo sve particije, npr., $n+1 \in [n+1]$. Blok koji ga sadrži neka ima još k elemenata. Taj se blok može izabrati na $\binom{n+1-1}{k+1-1} = \binom{n}{k}$ načina, a preostali skup od $n-k$ elemenata particionirati na B_{n-k} načina, pa za čvrsto k imamo $\binom{n}{k} B_{n-k}$ particija. Pravilo sume povlači tvrdnju. □

Ova rekurzija (tzv. binomnog tipa) seže "duboko u prošlost", no ipak se za relativno male n brojevi B_n mogu lako izračunati:

n	0	1	2	3	4	5	6	7	8	9	10	...
B_n	1	1	2	5	15	52	203	877	4140	21147	116335	...

Povežimo Stirlingove brojeve I i II vrste. Sjetimo se da je $c(n,k)$ (ili $\left[{n \atop k}\right]$) broj permutacija π od n elemenata (tj. $\pi \in S_n$) s točno k ciklusa, a $s(n,k) = (-1)^{n-k} c(n,k)$. "Rubni uvjeti" su: $c(n,k) = 0$ za $n \leq 0$ ili $k \leq 0$, osim što dodatno definiramo $c(0,0) := 1$, te $c(n,n) = 1$ i $c(n,k) = 0$ za $k > n \geq 0$. Također je jasno da je $\sum_{k=0}^{n} c(n,k) = n!$.

LEMA 2 (Osnovna rekurzija za $c(n,k)$). *Za $k, n \in \mathbb{N}$ vrijedi*

$$c(n,k) = c(n-1,k-1) + (n-1)c(n-1,k), \tag{27}$$

odnosno

$$s(n,k) = s(n-1,k-1) - (n-1)s(n-1,k). \tag{27'}$$

Dokaz. Rasuđivanje je slično onom za $S(n,k)$. Svaku permutaciju od $[n]$ s k ciklusa restringirajmo na $[n-1]$. Ako je n fiksna točka, onda izostavimo ciklus (n) i dobijemo permutaciju od $[n-1]$ s $k-1$ ciklusa, a takvih ima $c(n-1,k-1)$. Ako pak n nije fiksna točka, onda ga izostavimo iz ciklusa koji ga sadrži (taj je duljine ≥ 2). Na taj je način svaka permutacija od $[n-1]$ s $k-1$ ciklusa dobivena točno jedanput, a svaka permutacija od $[n-1]$ s k ciklusa dobivena točno $n-1$ puta, jer se n može ubaciti poslije svakog od brojeva $1, 2, \ldots, n-1$, pa takvih im $(n-1)c(n-1,k)$. Odatle slijedi tvrdnja. □

Tako npr., za $k=1$, dobivamo $c(n,1) = (n-1)c(n-1,1) = (n-1)(n-2)c(n-2,1) = \cdots = (n-1)!$, što je još jedna potvrda da cikličkih permutacija na $[n]$ ima $(n-1)!$.

PROPOZICIJA 21. *Za svako $n \in \mathbb{N}_0$ i sve $x \in \mathbb{R}$ (ili $\mathbb{C}$) vrijedi*

$$\sum_{k=0}^{n} c(n,k) x^k = x^{\overline{n}} (= x(x+1)\ldots(x+n-1)). \tag{28}$$

Dokaz I. Indukcijom po n uporabom Leme 2. Korak indukcije je:

$$\begin{aligned}\sum_{k=0}^{n} c(n,k)x^k &= \sum_{k=0}^{n} [c(n-1,k-1) + (n-1)c(n-1,k)]x^k = \\ &= x \cdot \sum_{k=1}^{n} c(n-1,k-1)x^{k-1} + (n-1)\sum_{k=0}^{n-1} c(n-1,k)x^k = \\ &= x \cdot x^{\overline{n-1}} + (n-1) \cdot x^{\overline{n-1}} = (x+n-1)x^{\overline{n-1}} = x^{\overline{n}}.\end{aligned}$$

□

Dokaz II (kombinatorni). Opet je dovoljno tvrdnju dokazati za bilo koji prirodni broj x. Opći sumand lijeve strane broji sve uređene parove (π, f), gdje je $\pi \in S_n$ permutacija s k ciklusa, a $f : C(\pi) \to [x]$ funkcija sa skupa ciklusa $C(\pi) = \{C_1, \ldots, C_k\}$ u $[x] = \{1, 2 \ldots, x\}$. Desna strana broji sve uređene n-torke cijelih brojeva $(a_1, a_2, \ldots, a_n)$, pri čemu je $0 \leq a_1 \leq x+n-2$, $0 \leq a_2 \leq x+n-1, \ldots,$ $0 \leq a_i \leq x+n-i-1, \ldots,$ $0 \leq a_n \leq x-1$. Sljedeći jednostavni algoritam definira pridruživanje $(a_1, \ldots, a_n) \mapsto (\pi, f)$.

Počinjemo s ciklusom $C_1 = (n)$ od π i neka je $f(C_1) = a_n + 1$. Pretpostavimo da smo već umetnuli brojeve $n, n-1, \ldots, n-i+1$ u ciklički zapis od π. Sada želimo umetnuti broj $n-i$. Imamo dvije mogućnosti:

1) Ako je $0 \leq a_{n-i} \leq x-1$, onda otvorimo s brojem $n-i$ novi ciklus C_j i to lijevo od prethodno umetnutih brojeva, te stavimo $f(C_j) = a_{n-i} + 1$.

2) Ako je $a_{n-i} = x+r$, za neko r, $0 \leq r \leq i-1$ (uostalom, mora biti $a_{n+i} \leq x+i-1$), onda broj $n-i$ umetnimo u neki stari ciklus, tako da mu nije početni element te tako da je udesno od $r+1$ prethodno umetnutih brojeva.

Ovaj proces (algoritam) se može i obrnuti, pa se dobiva bijekcija. □

Pokažimo na dobro odabranom primjeru kako radi gornji algoritam (kao što je dobro poznato, ta metoda učenja je vrlo učinkovita).

Primjer 60. Neka je $n = 10$, $x = 4$ i $(a_1, a_2, \ldots, a_{10}) = (6, 8, 10, 4, 3, 6, 5, 5, 3, 2)$. Nađite algoritmom iz kombinatornog dokaza Propozicije 21 pripadni (π, f). Tada obrnite proces.

Rješenje. Napišimo etape algoritma (odozgo prema dolje) kojima se gradi permutacija π. Dakle, počinjemo skraja (zdesna), pa redom imamo:

(10)
(9)(10)
(9)(10 8)
(9)(10 7 8)
(9)(10 7 6 8)
(5)(9)(10 7 6 8)
(5 4)(9)(10 7 6 8)
(5 4)(9)(10 7 6 8 3)
(5 4)(9)(10 7 2 6 8 3)
(5 4)(9 1)(10 7 2 6 8 3) $= \pi$.
Usput dobivamo $f(10\,7\,2\,6\,8\,3) = 3$, $f(9\,1) = 4$, $f(5\,4) = 4$. □

Za $x = 1$ kombinatorni dokaz Propozicije 21 nam daje i kombinatorni dokaz sljedećeg (još jednog) kombinatornog značenja brojeva $c(n, k)$.

KOROLAR 5. *Za sve $n, k \in \mathbb{N}$, broj cjelobrojnih uređenih n-torki $(a_1, a_2, \ldots, a_n)$ za koje je $0 \leq a_i \leq n-i$, a među njima točno k brojeva $a_i = 0$ je jednak $c(n, k)$.*

Dakle, za $x = 1$, dokaz II Propozicije 21 permutaciji $\pi \in S_n$ bijektivno pridružuje n-torku cijelih brojeva $(a_1, \ldots, a_n)$, $0 \leq a_i \leq n-i$. Iz zadanog niza $(a_1, \ldots, a_n)$ dobijemo permutaciju $\pi = i_1 i_2 \ldots i_n \in S_n$ shvaćenu kao riječ (a ne produkt ciklusa) ovako. Opet počinjemo s n, a nakon što smo umetnuli $n, n-1, \ldots, n-i+1$, onda broj $n-i$ umetnemo tako da mu je a_{n-i} elemenata ulijevo. Prema tome, a_j je broj članova $i \in [n]$ koji su lijevo od j, a za koje je $j > i$. Stoga je niz $I(\pi) = (a_1, \ldots, a_n)$ niz inverzija od π. Gornji algoritam nam stoga omogućava da permutaciju π rekonstruiramo iz niza inverzija.

Primjer 61. Nađite permutaciju $\pi \in S_9$ čiji je niz inverzija $I(\pi) = (3, 0, 5, 1, 4, 0, 2, 1, 0)$.

Rješenje. Opet počinjemo zdesna s brojem 9 i onda redom umećemo $8, 7, \ldots, 1$ prema gornjem pravilu da $9-i$ umetnemo tako da mu je a_{9-i} elemenata lijevo, $i = 0, 1, \ldots, 8$. Etape algoritma su:

9
98
987
6987
69875
649875
6498735
26498735
264198735 $= \pi$.

□

Sada se vratimo vezi Stirlingovih brojeva I i II vrste. Iz $s(n,k) = (-1)^{n-k} c(n,k)$ i $x^{\overline{n}} = (-1)^n (-x)^{\underline{n}}$, iz (28) dobivamo

$$x^{\underline{n}} = \sum_{k=0}^{n} s(n,k) x^k. \tag{29}$$

Formule (26) i (29) možemo ovako tumačiti. Skup $\mathbb{R}[x]$ svih polinoma nad $\mathbb{R}$ (a i nad $\mathbb{C}$) u varijabli x je vektorski prostor u kojem imamo dvije baze $B_1 = \{1, x, x^2, \ldots\}$ i $B_2 = \{1, x^{\underline{1}}, x^{\underline{2}}, \ldots\}$. Tada te formule izražavaju vektore jedne baze pomoću druge. Matrice prijelaza su (beskonačne) matrice $A_1 = [S(n,k)]_{n,k \in \mathbb{N}_0}$ i $A_2 = [s(n,k)]_{n,k \in \mathbb{N}_0}$ i stoga su jedna drugoj inverzne.

Prema tome, vrijedi sljedeća **Stirlingova inverzija**:

KOROLAR 6. *Za svako $m, n \in \mathbb{N}_0$ vrijedi*

$$\sum_{k \geq 0} S(m,k) s(k,n) = \begin{cases} 1 & , \text{za } m = n \\ 0 & , \text{za } m \neq n \end{cases} \quad (= \delta_{m,n}). \tag{30}$$

Dokaz. Kako su A_1 i A_2 međusobno inverzne (donje trokutaste) matrice, to je njihov produkt jednak jediničnoj matrici $I = [\delta_{m,n}]$. Odatle slijedi tvrdnja. □

Kao i za binomne koeficijente, i za Stirlingove se brojeve postavlja slično pitanje kako se ponaša niz $c(n,0), c(n,1), \ldots, c(n,n)$ i slično $S(n,0), S(n,1), \ldots, S(n,n)$; je li unimodalan ili čak log-konkavan? Odgovor je da. Poslužit ćemo se jednom Newtonovom lemom.

LEMA 3 (Newton). *Ako realni polinom $P(x) = \sum_{k=0}^{n} a_k x^k$ stupnja n ima samo realne nultočke, onda su mu koeficijenti log-konkavni, tj. vrijedi $a_k^2 \geq a_{k-1}a_{k+1}$. (Štoviše, $a_k/\binom{n}{k}$ su log-konkavni.)*

Sada, iz desne se strane formule (28) vidi da polinom na njezinoj lijevoj strani ima same realne nultočke (to su: $0, -1, -2, \ldots, -(n-1)$). Zato je $c(n,k)^2 \geq c(n,k-1)c(n,k+1)$. Stoga je niz $c(n,0), c(n,1), \ldots, c(n,n)$ unimodalan.

Za brojeve $S(n,k)$ stvar je malo složenija. Naime, tvrdimo da polinom

$$P_n(x) = \sum_{k=0}^{n} S(n,k)x^k$$

ima sve realne ≤ 0 različite nultočke. Prvo, $P_0(x) = 1$, a iz rekurzije (25) slijedi $P_n(x) = x[P'_{n-1}(x) + P_{n-1}(x)]$. Funkcija $Q_n(x) := P_n(x)e^x$ ima iste nultočke kao i P_n, a vrijedi $Q_n(x) = xQ'_{n-1}(x)$. Odavde se lako indukcijom po n i uporabom Rolleovog teorema zaključi da Q_n, pa stoga i P_n, ima sve realne ≤ 0 različite nultočke. Dakle, dokazali smo

PROPOZICIJA 22. *Nizovi $c(n,0)$, $c(n,1)$, $\ldots$,$c(n,n)$ te $S(n,0)$, $S(n,1)$,$\ldots$, $S(n,n)$ su log-konkavni; pa stoga i unimodalni.*

Vrhunce tih nizova je teže odrediti. Zna se da se vrhunac za $S(n,k)$ postiže za $k \approx n/\log n$ (za velike n).

Potpunosti radi, dokažimo i vrlo korisnu Newtonovu lemu.

Dokaz Leme 3. Podsjetimo da Rolleov teorem kaže da ako je f glatka funkcija na $[a,b]$ i $f(a) = f(b) = 0$, onda u intervalu $\langle a,b\rangle$ postoji točka c, tako da je derivacija $Df(c) = 0$. (Pišemo D za $\frac{d}{dx}$.) Neka je $Q(x) := D^k P(x)$ (k-ta derivacija). Iz Rolleovog teorema slijedi da $Q(x)$ ima samo realne nultočke. Neka je $Q_1(x) := x^{n-k}Q(x^{-1})$. Tada su nultočke od Q_1 recipročne od nultočaka od Q, pa stoga opet realne. Neka je $R(x) := D^{n-k-2}Q_1(x)$. To je kvadratni polinom. Iz Rolleovog teorema opet slijedi da su nultočke od R realne. No, malo računanja daje

$$R(x) = k!\frac{(n-k)!}{2}a_k x^2 + (k+1)!(n-k-1)!a_{k+1}x + \frac{(k+2)!}{2}(n-k-2)!a_{k+2} =$$
$$= \frac{1}{2}k!\left[\frac{a_k}{\binom{n}{k}}x^2 + \frac{a_{k+1}}{\binom{n}{k+1}}2x + \frac{a_{k+2}}{\binom{n}{k+2}}\right].$$

Nultočke ovog polinoma su realne ako i samo ako je diskriminanta ≥ 0, tj.

$$\left(\frac{a_{k+1}}{\binom{n}{k+1}}\right)^2 - \frac{a_k}{\binom{n}{k}}\frac{a_{k+2}}{\binom{n}{k+2}} \geq 0.$$

Odavde odmah slijedi tvrdnja leme. □

Ako osnovne rekurzije (25) i (27) formalno proširimo na sve parove n, k cijelih brojeva, s tim da vrijede isti "rubni uvjeti" $S(0,k) = c(0,k) = 0$ za $k \neq 0$ i $S(n,0) = c(n,0) = 0$ za $n \neq 0$, te $S(0,0) = c(0,0) = 1$, onda je lako provjeriti da $c(n,k)$ i $S(-k,-n)$ zadovoljavaju istu rekurziju (s istim rubnim uvjetima), pa se stoga podudaraju. Tako dobivamo **recipročnost za Stirlingove brojeve**: za sve $k, n \in \mathbb{Z}$

$$c(n,k) = S(-k,-n), \text{ ili } S(n,k) = c(-k,-n). \tag{31}$$

Eulerovi brojevi za permutacije

Neka je $\pi \in S_n$ permutacija na skupu $[n]$, zapisana kao riječ $\pi = i_1 i_2 \ldots i_n$. **Skup uspona** od π je $U(\pi) = \{k \in [n] | i_k < i_{k+1}\}$, a $|U(\pi)|$ **broj uspona permutacije** π. Označimo s $E(n,k)$ ili $\left\langle {n \atop k} \right\rangle$ broj permutacija $\pi \in S_n$ s točno k uspona. Taj se broj zove **Eulerov broj**. Skupovi uspona $U(\pi)$ i padova $D(\pi)$ su disjunktni i $U(\pi) \cup D(\pi) = [n-1]$. Na primjer, za $n = 4$ i $k = 2$ imamo 11 permutacija s dva uspona: 1324, 1423, 2314, 2413, 3412, 1243, 1342, 2341, 2134, 3124, 4123. Stoga je $E(4,2) = 11$.

Očito permutacija ima najviše $n-1$ uspona, pa je $E(n,n) = 0$ za $n \geq 1$, a dodatno definiramo $E(0,0) := 1$, te $E(n,k) = 0$ za $k \geq n \geq 1$. Za te brojeve vrijedi *simetrija*: $E(n,k) = E(n,n-1-k)$ ili u drugoj simbolici

$$\left\langle {n \atop k} \right\rangle = \left\langle {n \atop n-1-k} \right\rangle,$$

jer permutacija $\pi = i_1 i_2 \ldots i_n$ ima $n-1-k$ uspona ako i samo ako "zrcalna" permutacija $\bar{\pi} = i_n \ldots i_2 i_1$ ima k uspona. Nadalje vrijedi $E(n,0) = 1$ i $E(n,1) = 2^n - n - 1$ (zašto?). Očito vrijedi i

$$E(n,0) + E(n,1) + \cdots + E(n,n) = n!.$$

LEMA 4 (Osnovna rekurzija za $E(n,k)$). *Za $k, n \in \mathbb{N}$ vrijedi*

$$E(n,k) = (k+1)E(n-1,k) + (n-k)E(n-1,k-1). \tag{32}$$

Dokaz. Sve permutacije od $[n]$ dobivamo umetanjem broja n na sve moguće pozicije permutacija od $[n-1]$. Pretpostavimo da smo broj n umetnuli na poziciju t permutacije $\rho = i_1 i_2 \ldots i_{n-1}$ od $[n-1]$. Tada dobivamo permutaciju $\pi = i_1 \ldots i_{t-1} n i_t \ldots i_{n-1}$ od $[n]$. Za broj uspona $|U(\pi)|$ od π tada očito vrijedi

$$|U(\pi)| = \begin{cases} |U(\rho)| & , \text{za } t = 1 \text{ ili } i_{t-1} < i_t \\ |U(\rho)| + 1 & , \text{za } t = n \text{ ili } i_{t-1} > i_t. \end{cases}$$

Ako je $|U(\pi)| = k$, onda u prvom slučaju imamo $(k+1)E(n-1,k)$ mogućnosti (k uspona od ρ plus jedna), a u drugom $(n-k)E(n-1,k-1)$ ($k-1$ padova od ρ, tj. $n-2-(k-1) = n-k-1$ uspona plus jedna). □

Ova rekurzija se može proširiti i na sve $k, n \in \mathbb{Z}$, stavimo li $E(0,k) = 0$ za $k \neq 0$ i $E(n,k) = 0$ za $k < 0$.

Osnovna formula za Eulerove brojeve je sljedeća.

PROPOZICIJA 23. *Za svako $n \in \mathbb{N}_0$ i sve $x \in \mathbb{R}$ vrijedi*

$$x^n = \sum_{k=0}^{n} E(n,k) \binom{x+k}{n}. \tag{33}$$

Dokaz I. Indukcijom po n uporabom osnovne rekurzije (32), što prepuštamo čitatelju. □

Dokaz II (kombinatorni). Tvrdnju je dovoljno dokazati za bilo koji $x \in \mathbb{N}$. Lijeva strana broji sve funkcije $f : [n] \to [x]$, a desna sve uređene parove (π, A), gdje je $\pi \in S_n$ permutacija na skupu $[n]$ s k uspona, a A n-člani podskup od $[x+k]$, za neko $k \geq 0$. Nađimo prirodnu bijekciju $f \mapsto (\pi, A)$.

Neka je $f : [n] \to [x]$ zadana funkcija i neka je $f(i) = a_i$, $i = 1, \ldots, n$. Uredimo $a_1, \ldots, a_n$ u rastućem poretku

$$1 \leq a_{i_1} \leq a_{i_2} \leq \cdots \leq a_{i_n} \leq x, \tag{$*$}$$

s tim da ako je na nekom mjestu $a_{i_j} = a_{i_{j+1}}$, pišemo $a_{i_j} \leq a_{i_{j+1}}$ ako je $i_j < i_{j+1}$. Dakle, $i_j > i_{j+1} \Rightarrow a_{i_j} < a_{i_{j+1}}$. Time smo dobili permutaciju $\pi = i_1 i_2 \ldots i_n \in S_n$.

Očito π ima k padova (tj. $n-k-1$ uspona) ako i samo ako u nizu $a_{i_1} \leq a_{i_2} \leq \cdots \leq a_{i_n}$ ima k strogih nejednakosti. Označimo $b_j := a_{i_j}$, pa imamo $1 \leq b_1 \leq b_2 \leq \cdots \leq b_n \leq x$. Uzmimo da stroge nejednakosti nastupaju tu na mjestima $r_1, \ldots, r_k$. Tada $(*)$ izgleda ovako

$$1 \leq b_1 \leq \cdots \leq b_{r_1} < b_{r_1+1} \leq \cdots \leq b_{r_2} < b_{r_2+1} \leq \cdots \leq b_{r_k} < b_{r_k+1} \leq \cdots \leq b_n \leq x.$$

Sada formiramo niz

$$1 \leq c_1 < c_2 < \cdots < c_n \leq x + k$$

na sljedeći način

$$c_1 = b_1,\ c_2 = b_1 + 1, \ldots,\ c_{r_1} = b_{r_1} + (r_1 - 1),\ c_{r_1+1} = b_{r_1+1} + (r_1 - 1), \ldots$$

Drugim riječima, c-ove definiramo tako da minimalno razdvoje b-ove. Tada je najveći c_n najviše za k narastao od najvećeg b_n, pa je $c_n \leq x + k$. Stavimo $A = \{c_1, \ldots, c_n\}$.

Permutacije π možemo birati na $E(n, n-k-1) = E(n,k)$ načina (to je zbog svojstva simetrije), a podskup A na $\binom{x+k}{n}$ načina.

Pridruživanje $f \mapsto (\pi, A)$ je bijekcija. Inverzno pridruživanje dobivamo obrnutim postupkom (algoritmom). □

Formula (33) izražava potencije pomoću uzastopnih binomnih koeficijenata, a oni također čine bazu prostora polinoma $\mathbb{R}[x]$. Primjerice,

$$x^2 = \binom{x}{2} + \binom{x+1}{2}, \quad x^3 = \binom{x}{3} + 4\binom{x+1}{3} + \binom{x+2}{3} \quad \text{itd.}$$

Konačno, veza između Stirlingovih i Eulerovih brojeva jest sljedeća.

KOROLAR 7. *Za sve $n, x \in \mathbb{N}$ vrijedi*

$$x!S(n,x) = \sum_k E(n,k) \binom{k}{n-x}. \tag{34}$$

Dokaz. Dokaz je sličan prethodnom, ali sada lijeva strana broji sve surjekcije $f : [n] \to [x]$(v. Korolar 4), pa ga prepuštamo čitatelju. □

Dvanaest načina

Zaključno ćemo sve osnovne rezultate kombinatornih prebrojavanja sažeti u jednu preglednu tablicu koja ima 12 članova i odatle joj i ime.

Mi prebrajamo sve funkcije $f : N \to X$ između konačnih skupova N i X s $|N| = n$ i $|X| = x$, ali pod nekim dodatnim zahtjevima. Tri su zahtjeva na samu funkciju (bilo koja, injekcija i surjekcija), te po dva zahtjeva na N i X, tj. ukupno četiri, s obzirom na to razlikujemo li ili ne razlikujemo elemente. To je zgodno zamišljati tako da je N skup kuglica, a X skup kutija, a funkcija $f : N \to X$ stavlja svaku kuglicu u neku kutiju. Ako kuglice razlikujemo (npr. ako su označene s $1, 2, \ldots, n$), onda elemente od N smatramo "različitim" i u tablici ćemo pisati "razl.", a ako ih ne razlikujemo, tj. ako su "nerazlučive", pisat ćemo "nerazl.". Slično je i s elementima od X (kutije razlikujemo ili ne). Ovo se može i formalizirati, ali se u to nećemo upuštati.

Dvanaest načina za broj funkcija $f : N \to X$, $|N| = n$, $|X| = x$

Elementi od N	Elementi od X	f bilo koja	f injekcija	f surjekcija
razl.	razl.	① x^n	② $x^{\underline{n}}$	③ $x!S(n,x)$
nerazl.	razl.	④ $\binom{x+n-1}{n}$	⑤ $\binom{x+n-1}{n}$	⑥ $\binom{n-1}{x-1}$
razl.	nerazl.	⑦ $S(n,1)+S(n,2)+\cdots+S(n,x)$	⑧ $\begin{cases} 1, & \text{za } n \leq x \\ 0, & \text{za } n > x \end{cases}$	⑨ $S(n,x)$
nerazl.	nerazl.	⑩ $p_1(n)+p_2(n)+\cdots+p_x(n)$	⑪ $\begin{cases} 1, & \text{za } n \leq x \\ 0, & \text{za } n > x \end{cases}$	⑫ $p_x(n)$

Objasnimo samo ⑦ i ⑩. Ostale stavke smo ili dokazali ili vrijede po definiciji. U ⑦ želimo n različitih kuglica staviti u x jednakih kutija. Zato je funkcija $f : N \to X$ određena jezgrom, tj. nepraznim skupovima $f^{-1}(b)$, $b \in X$, a oni čine particiju od N s najviše x blokova. Broj takvih particija je $S(n,1)+S(n,2)+\cdots+S(n,x)$. U ⑩ stavljamo jednake kuglice u jednake kutije, pa je takva funkcija $f : N \to X$ određena samo brojem elemenata u svakom bloku jezgre od f, pa je broj takvih funkcija jednak broju particija broja n u najviše x dijelova, tj. $p_1(n) + p_2(n) + \cdots + p_x(n)$.

III. Neki rekurzivni problemi

Već smo se u više navrata susreli s pojmom **rekurzivne relacije** (**rekurzivne formule** ili **rekurzije**). Grubo govoreći, to je relacija (često formula), pomoću koje se $n-$ti član nekog niza a_n izražava pomoću nekoliko prethodnih članova $a_k, k < n$. Precizna matematička podloga za taj pojam jest princip definicije indukcijom (vidi Uvod), a opći pojam rekurzije precizno se može definirati u matematičkoj logici u sklopu teorije izračunljivih funkcija, no mi se nećemo ovdje u to upuštati. Rekurzivne formule često daju djelotvoran način da se izračuna opći član a_n nekog niza iz poznavanja (nekih ili svih) prethodnih članova $a_k, k < n$, počevši od nekog indeksa n_0. Na primjer, vrlo jednostavna rekurzivna relacija je $a_n = 2a_{n-1}$. Ako zahtijevamo da ta relacija vrijedi za sve $n \in \mathbb{N}$, onda imamo redom $a_1 = 2a_0, a_2 = 2a_1, a_3 = 2a_2, \ldots$, pa ponovljenim uvrštavanjem dobivamo $a_2 = 2^2 a_0$, $a_3 = 2^3 a_0$, ...i , općenito, $a_n = 2^n a_0$. Da eksplicitno izračunamo a_n, treba poznavati još i tzv. **početne uvjete**. Ako je npr. $a_0 = 1$, dobivamo da je $a_n = 2^n$, za sve $n \in \mathbb{N}_0$. Tipične rekurzivne relacije kojima ćemo se ovdje baviti izgledat će ovako:
$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_r a_{n-r}$, gdje su c_i neke (zadane) konstante, te $r \in \mathbb{N}$ dani čvrst broj;
$a_n = ca_{n-1} + f(n)$, gdje je c zadana konstanta, a f zadana funkcija;

$$a_n = a_0 a_{n-1} + a_1 a_{n-2} + \ldots + a_{n-1} a_0;\ a_{n,k} = a_{n-1,k} + a_{n-1,k-1}$$

(ovo potonje je primjer "dvoindeksne" rekurzije kao Pascalova formula) itd.

Rekurzivne su relacije vrlo pogodne za rad na kompjuteru, pa možemo slobodno reći da, ako kompjuteri nešto vole, onda su to iterativne metode, uključujući i rekurzivne relacije.

Primjer 1. Nađite rekurziju za broj $P(n)$ permutacija skupa $[n]$ i izračunajte ga.

Rješenje. Svaka permutacija $i_1, i_2, \ldots, i_n$ od $[n] = \{1, 2, \ldots, n\}$ dobiva se na jedinstven način iz permutacije elemenata skupa $[n-1] = \{1, 2, \ldots, n-1\}$ umetanjem elementa n na ili prvo mjesto, ili između prvog i drugog mjesta itd., ili na zadnje ($n-$to) mjesto. Stoga je za $n \geq 2$

$$P(n) = nP(n-1).$$

To zajedno s početnom vrijednosti $P(1) = 1$ daje

$$P(n) = nP(n-1) = n(n-1)P(n-2) = \ldots = n(n-1)(n-2)\ldots 2P(1) =$$
$$n(n-1)(n-2)\cdot \ldots \cdot 2 \cdot 1 = n!$$

□

Primjer 2. Za $n \in \mathbb{N}_0$ označimo s $h_1(n)$ broj dijelova na koji n različitih točaka na pravcu dijeli taj pravac, s $h_2(n)$ označimo broj dijelova ravnine na koji je dijeli n pravaca u **općem položaju** (tj. svaka dva pravca sijeku se točno u jednoj točki, a nikoja tri ne prolaze istom točkom).

a) Nađite rekurzivnu relaciju među brojevima $h_1(n)$ i odredite ih.

b) Nađite rekurzivnu relaciju među brojevima $h_2(n)$. Koliko je $h_2(4)$, $h_2(5)$, $h_2(10)$?

c) Nađite opći član $h_2(n)$. (Točnije, treba odrediti broj komponenti povezanosti skupa $\mathbb{R}^2 \setminus \cup_{i=1}^n p_i$, gdje su $p_1, p_2, \ldots, p_n$ pravci u općem položaju.)

Rješenje. a) Očito je $h_1(0) = 1$, $h_1(1) = 2$, $h_1(2) = 3$. Za $n \geq 1$, pravac je s $n-1$ točaka razdijeljen na $h_1(n-1)$ dijelova. Dodajmo sada $n-$tu točku. Gdje god je umetnemo, ona će jedan od već postojećih $h_1(n-1)$ dijelova razbiti na dva dijela, tj. nastat će jedno novo područje. Stoga je

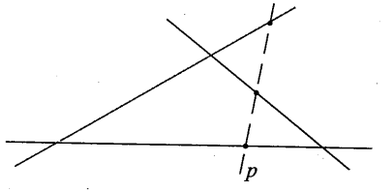
$$h_1(n) = h_1(n-1) + 1.$$

Iteriramo li tu formulu, tj. pišemo li umjesto n redom $n-1, n-2, \ldots, 1$ dobivamo

$$\begin{aligned} h_1(n-1) &= h_1(n-2) + 1 \\ h_1(n-2) &= h_1(n-3) + 1 \\ &\vdots \\ h_1(1) &= h_1(0) + 1. \end{aligned}$$

Zbrajanjem svih formula[1] slijedi $h_1(n) = h_1(0) + n = n + 1$. Taj rezultat se inače lako provjeri i indukcijom.

b) $h_2(0) = 1$, $h_2(2) = 4$, $h_2(3) = 7$. Neka je $n \geq 1$. Promatrajmo prvo $n-1$ pravaca u općem položaju. Oni dijele ravninu na $h_2(n-1)$ dijelova. Dodamo li tom skupu $n-$ti pravac, nazovimo ga p, tako da i skup od n pravaca bude u općem položaju, onda prvih $n-1$ pravaca siječe p u $n-1$ različitih točaka, pa ga dijeli na $h_1(n-1)$ dijelova. Svaki od tih dijelova na p povećava broj područja za jedan već postojećim $h_2(n-1)$, jer "staro" područje p dijeli na dva nova područja (v. sl. za $n = 4$).



Stoga dobivamo

$$h_2(n) = h_2(n-1) + h_1(n-1),$$

pa zbog a) odavde slijedi

$$h_2(n) = h_2(n-1) + n.$$

Zbog toga je $h_2(4) = h_2(3) + 4 = 7 + 4 = 11$, pa $h_2(5) = 11 + 5 = 16$, i slično se dobije $h_2(10) = 56$.

[1] Ta se metoda katkad zove i **teleskopiranje**.

c) Da se nađe ekplicitni izraz za $h_2(n)$ opet se iterira ta rekurzija, tj. napiše se za n, $n-1$, ..., 1 i sve skupa zbroji:

$$\left.\begin{array}{rcl} h_2(n) & = & h_2(n-1)+n \\ h_2(n-1) & = & h_2(n-2)+n-1 \\ h_2(n-2) & = & h_2(n-3)+n-2 \\ \vdots & & \\ h_2(2) & = & h_2(1)+2 \\ h_2(1) & = & h_2(0)+1. \end{array}\right\} + \Rightarrow$$

$$h_2(n) = h_2(0)+n+(n-1)+(n-2)+\ldots+2+1 =$$
$$= 1+\frac{n(n+1)}{2} = \binom{n}{0}+\binom{n}{1}+\binom{n}{2} = \frac{1}{2}(n^2+n+2)$$

□

Primjer 3. Označimo s $h_3(n)$ broj područja na koji je podijeljen prostor s n ravnina u **općem položaju**; tj. svaki par ravnina se siječe u jednom pravcu, ali nikoje tri se ne sijeku u jednom pravcu, već samo u jednoj točki i nikoje četiri ne prolaze jednom točkom. Nađite rekurziju za brojeve $h_3(n)$ i odredite ga (tj. $h_3(n)$ je broj komponenti povezanosti skupa $\mathbb{R}^3 \setminus \cup_{i=1}^n \pi_i$, gdje su $\pi_1, \ldots, \pi_n$ te ravnine).

Rješenje. Istim zaključivanjem kao u Primjeru 2 promatramo prvo $n-1$ ravnina u općem položaju koje dijele prostor na $h_3(n-1)$ područja. Dodavanjem n–te ravinine, tako da je svih n ravnina u općem položaju, prvih $n-1$ ravnina sijeku tu n–tu ravninu u $n-1$ pravaca koji su u općem položaju u n–toj ravnini. Tih $n-1$ pravaca dijele tu ravninu na $h_2(n-1)$ ravninskih dijelova, od kojih svaki dijeli već postojeća prostorna područja na dva dijela, pa stoga pridonese novih $h_2(n-1)$ područja. Dakle,

$$h_3(n) = h_3(n-1)+h_2(n-1).$$

Opet kao u Primjeru 2, iteriranjem i zbrajanjem (tj. teleskopiranjem) dobivamo zbog $h_3(0)=1$ i zbog rezultata c) Primjera 2:

$$h_3(n) = h_3(0)+\sum_{i=0}^{n-1} h_2(i) = 1+\sum_{i=0}^{n-1}\left[\binom{i}{0}+\binom{i}{1}+\binom{i}{2}\right],$$

a odavde se lakim računom dobije da je

$$h_3(n) = \binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\binom{n}{3} = \frac{1}{6}(n^3+5n+6).$$

□

Napomena 1. Rezultati Primjera 2. i 3. mogu se generalizirati na višedimenzionalne prostore. Za $k \in \mathbb{N}$ označimo s $h_k(n)$ broj područja na koje je k-dimenzionalni euklidski prostor $\mathbb{R}^k$ podijeljen s n $(k-1)$-dimenzionalnih hiperravnina π_1, π_2, ..., π_n u **općem položaju**. To znači da je presjek svakih d od tih hiperravnina $(k-d)$-dimenzionalna ravnina, $d = 1, 2, \ldots, n$, pri čemu negativna dimenzija znači

prazan skup. Tada analognim zaključivanjem kao u Primjerima 2. i 3. dobivamo "dvoindeksnu" rekurziju

$$h_k(n) = h_k(n-1)+h_{k-1}(n-1).$$

Odavde iteriranjem i zbrajanjem (tj. teleskopiranjem) dobivamo

$$h_k(n) = h_k(0)+\sum_{i=0}^{n-1} h_{k-1}(i).$$

Znamo da je $h_k(0)=1$. Pretpostavimo induktivno (po k) da je

$$h_{k-1}(n) = \binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{k-1},$$

onda iz $\sum_{j=0}^{n-k}\binom{k+j}{k} = \binom{n+1}{k+1}$ i činjenice da je $\binom{s}{t}=0$ za $t>s$ dobivamo **Schläflijev teorem**[2]:

$$h_k(n) = \binom{n}{0}+\binom{n}{1}+\binom{n}{2}+\ldots+\binom{n}{k},$$

tj. $h_k(n)$ je parcijalna suma prvih $k+1$ binomnih koeficijenata s "brojnikom" n. Uočite da je $h_k(n) = 2^n - \sum_{j=0}^{n-k-1} 2^j\binom{n-j-1}{k}$, a broj omeđenih područja $\binom{n-1}{k}$.

Primjer 4. Banka plaća štedišama 7% kamata na godinu na uloženi novac. Nađite rekurzivnu relaciju za iznose uštedenog novca nekog štediše nakon n godina, ako je njegova strategija ulaganja bila sljedeća:

a) Uložio je 100 000 kuna i ostavio taj novac nedirnut n godina

b) Na kraju svake godine uložio je 10 000 kuna.

Izračunajte iznose koje je imao štediša nakon 10 godina u oba slučaja.

Rješenje. Ako je na početku neke godine štediša ima x kuna, pa ako kroz tu godinu nije više niti dodavao niti oduzimao novac sa svog računa, onda je na kraju te godine (tj. na početku slijedeće) imao x kuna plus kamate na tih x kuna. Označimo s a_n iznos koji je imao na kraju n–te (tj. na početku $n+1$-ve)godine. Tada imamo

a) $a_n = a_{n-1}+0,07a_{n-1} = 1,07a_{n-1}$, uz početni uvjet $a_0 = 100\,000$;

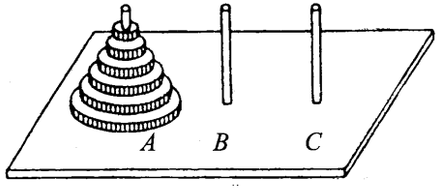
b) Kako je novac ulagan na kraju svake godine, to neće biti ni kamata na taj iznos u toj godini. Stoga je

$$a_n = 1,07a_{n-1}+10\,000, \text{uz početni uvjet } a_0 = 0.$$

U slučaju a) $a_{10} = 1,07^{10}\cdot 100\,000 = 196\,715$.
U slučaju b) $a_{10} = (1,07^9+\ldots+1,07+1)\cdot 10\,000 = \frac{1,07^{10}-1}{1,07-1}\cdot 10\,000 = 138\,164$. □

[2]Ludwig Schläfli (1814–1895), njemački matematičar

Primjer 5. Poznata igra "Tornjevi Hanoja" sastoji se od sljedećeg: na jednom od triju štapova A, B, C, npr. na A, nalazi se n kolutova različite veličine nanesenih tako da je svaki kolut (osim najnižeg) manji od onog ispod njega (v.sl.). Sve kolutove treba premjestiti na štap B, tako da i tamo budu u istom položaju. Pritom se kolutovi prenose sa štapa na štap tako da se svaki put prenese samo jedan kolut i da se nikad veći kolut ne stavi na manji. Pritom se možemo služiti trećim pomoćnim štapom C. Nađite rekurzivnu formulu za najmanji potrebni broj prijenosa kolutova da se provede premještaj s A na B i odredite taj broj.



Rješenje. Označimo s N_n traženi minimalni broj premještanja n kolutova sa štapa A na B. Očito je $N_0 = 0$ i $N_1 = 1$ (jednostavno prenesemo taj jedan jedini kolut izravno s A na B). Neka je $n \geq 2$. Da bismo s A uopće mogli skinuti najdonji (n–ti kolut), moramo prethodno premjestiti prvih $n-1$ kolutova na B i C. Kako n–ti kolut ne smije doći na neki manji, moramo prethodno prvih $n-1$ sve smjestiti na C. Za to je potrebno N_{n-1} prijenosa. Nakon toga možemo $n-ti$ kolut staviti na štap B (i to je $(N_{n-1}+1)$-vi prijenos). Sada moramo "piramidu" s C od $n-1$ kolutova prenijeti na B, pa koristeći se sada štapom A kao s pomoćnim, treba još N_{n-1} prijenosa. Stoga je

$$N_n = (N_{n-1}+1) + N_{n-1} = 2N_{n-1} + 1.$$

Dalje iteriranjem dobivamo

$$\begin{aligned} N_n &= 2N_{n-1}+1 = 2(2N_{n-2}+1)+1 = 2^2N_{n-2}+2+1 = 2^2(2N_{n-3}+1)+2+1 = \\ &= 2^3N_{n-3}+2^2+2+1 = \ldots = 2^nN_0+2^{n-1}+\ldots+2+1 = 2^{n-1}+\ldots+1 = \\ &= 2^n-1 \quad \text{što se lako dokaže i indukcijom po } n. \end{aligned}$$

□

§ 1. Fibonaccijevi brojevi

U svojoj knjizi *Liber Abaci* (knjiga o abakusu) iz 1202. godine Leonardo od Pise (1170–1250) poznat još kao Fibonacci (što dolazi od "filius Bonacci" – Bonaccijev sin) postavio je sljedeći **problem razmnožavanja zečeva**. Zečevi se razmnožavaju ovako. Svaki par zec–zečica, starih barem 2 mjeseca, dobiju tijekom svakog sljedećeg mjeseca par mladih: zeca i zečicu. Ako smo na početku godine počeli s jednim novorođenim parom, koliko će ukupno biti parova zec–zečica nakon godine dana, odnosno općenito nakon n mjeseci? (Naravno, pretpostavljamo da je ovo idealizirani model, tj. da zečevi ne ugibaju itd.)

Neka je F_n broj parova zec–zečica na početku n-tog mjeseca od početka praćenja tog procesa razmnožavanja. Početkom drugog mjeseca još imamo samo jedan par, pa je $F_1 = 1, F_2 = 1$. No, početkom idućeg mjeseca imamo već novi par, tako da su

sada dva para pa je $F_3 = 1+1 = 2$. Općenito, na početku $(n+1)$-og mjeseca imamo F_{n+1} parova, a na početku $(n+2)$-gog mjeseca imamo još uvijek tih F_{n+1} parova, ali dobivamo i F_n novorođenih parova (jer je F_n parova starih barem 2 mjeseca zrelo za oplodnju). Dakle, vrijedi rekurzija

$$F_{n+2} = F_{n+1} + F_n. \tag{1}$$

Obično se još definira i $F_0 = 0$, što zajedno s $F_1 = 1$ daje iz (1) sljedeću tablicu

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	...
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377	610	...

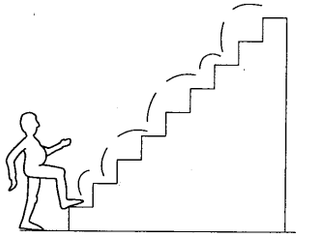
Vidimo, dakle, da je rješenje problem razmnožavanja $F_{13} = 233$. Niz brojeva $(F_n)_{n\geq 0}$ za koje je $F_0 = 0$ i $F_1 = 1$, te vrijedi (1) za sve $n \geq 0$, zove se Fibonaccijev niz, a F_n **n-ti Fibonaccijev broj**.

Već smo se susreli s tim brojevima (v. Primjer 42 u prethodnom poglavlju), a sada navodimo još neke kombinatorne probleme - kojima se kao rješenje javljaju Fibonaccijevi brojevi.

Primjer 6. Bakterije se razmnožavaju prema ovoj shemi: svaka živi dva sata i svaki sat daje jednu novu bakteriju (dakle, samo dvije tijekom života). Koliko je živo potomstvo jedne bakterije nakon 24 sata, nakon 48 sati i općenito nakon n sati od pojave prve bakterije?

Rješenje. Neka je b_n traženi broj. Očito je $b_0 = 1$, $b_1 = 2$, $b_2 = 3$. Za $n \geq 3$, $b_n - b_{n-2}$ je broj bakterija koje žive kao potomstvo bakterija živih nakon $n-1$ sati, a tih je b_{n-1}. Dakle, vrijedi $b_n = b_{n-2} + b_{n-1}$. To je ista rekurzija kao (1), ali su početne vrijednosti pomaknute za dva mjesta naprijed. Zato je $b_n = F_{n+2}$. U posebnom je slučaju, $b_{24} = F_{26} = 175\,683$. No, $b_{48} = F_{50} \approx 6$ bilijuna (poslije ćemo vidjeti zašto). □

Primjer 7. Koliko ima različitih načina da se čovječuljak sa slike popne n stuba, ako odjednom može zakoračiti ili na jednu ili na dvije stube? (Pritom dva uspinjanja smatramo istim ako je "čovo" kročio na točno iste stube.)



Rješenje. Označimo traženi broj sa s_n. Očito je $s_1 = 1$, $s_2 = 2$. "Čovo" može početi s jednom stubom ili dvije. U prvom slučaju može se nastaviti penjati na s_{n-1} načina, a u drugom slučaju na s_{n-2} načina. Dakle, ukupan broj uspona je $s_n = s_{n-1} + s_{n-2}$. Ovdje su početne vrijednosti pomaknute za jedan, pa je $s_n = F_{n+1}$.

Uočite da se isti odgovor dobiva na pitanje: koliki je broj načina da se broj n zapiše kao uređeni zbroj (tj. rastav) u jedinice i dvojke? □

Primjer 8. a) Koliko ima binarnih nizova duljine n bez susjednih nula?

b) Koliko ima podskupova od $[n]$ koji ne sadrže dva susjedna broja? (usp. primjer 42 iz poglavlja II.)

Rješenje. Postoji očita bijekcija

$$\left\{ \begin{array}{c} \text{binarni nizovi duljine } n \\ \text{bez susjednih nula} \end{array} \right\} \to \left\{ \begin{array}{c} \text{podskupovi iz } [n] \text{ bez} \\ \text{dvaju susjednih brojeva} \end{array} \right\}$$

Naime, takvom binarnom nizu pridružimo skup mjesta na kojima su nule. Npr. , za $n = 7$, $(1,0,1,1,0,1,0) \mapsto \{2,5,7\} \subseteq [7]$. Zato su odgovori na a) i b) jednaki.

Ako je a_n traženi broj iz a), onda je $a_1 = 2$, $a_2 = 3$. Za $n \geq 3$, svaki takav binarni niz počinje ili jedinicom, pa se može nastaviti na a_{n-1} načina, ili nulom (stoga na drugom mjestu ne smije biti nula) pa se može nastaviti na a_{n-2} načina. Dakle, opet $a_n = a_{n-1} + a_{n-2}$, i zbog pomaka početnih uvjeta slijedi $a_n = F_{n+2}$. □

Napomenimo još jedanput da usporedbom dvaju rješenja Primjera 8 b) i Primjera 41 iz poglavlja II dobivamo "eksplicitni" izraz za Fibonaccijeve brojeve kao sume binomnih koeficijenata

$$F_{n+2} = \sum_{k \geq 0} \binom{n-k+1}{k}. \tag{2}$$

Primjer 9. Koliko ima binarnih nizova $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n,)$, $\varepsilon_i \in \{0,1\}$, takvih da je $\varepsilon_1 \leq \varepsilon_2 \geq \varepsilon_3 \leq \varepsilon_4 \geq \varepsilon_5 \leq \ldots$?

Rješenje. Neka je A_n traženi broj. Tada je $A_1 = 2$, $A_2 = 3$ (jer su 00; 01; i 11 svi takvi nizovi duljine 2). Za $n \geq 3$, ako niz započinje s 0, možemo ga nastaviti na A_{n-1} načina, a ako započinje s 1, onda na drugom mjestu mora biti 1 pa ga možemo nastaviti na A_{n-2} načina. Dakle, $A_n = A_{n-1} + A_{n-2}$, pa je opet $A_n = F_{n+2}$. □

Primjer 10 (Kombinatorno značenje potencija Fibonaccijevih brojeva). Dokažite da nizova podskupova $(S_1, S_2, \ldots, S_n)$, $S_i \subseteq [r] = \{1, \ldots, r\}$, takvih da je $S_1 \subseteq S_2 \supseteq S_3 \subseteq S_4 \supseteq \ldots$ ima F_{n+2}^r.

Rješenje. Za svako $i \in [r]$, $j \in [n]$, definirajmo

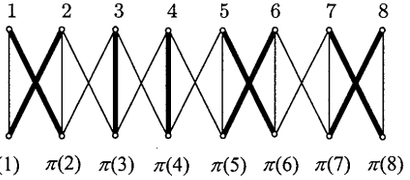
$$\varepsilon_{i_j} = \left\{ \begin{array}{ll} 1, & \text{ako } i \in S_j, \\ 0, & \text{ako } i \notin S_j. \end{array} \right.$$

Za čvrsto $i \in [r]$, niz $\varepsilon_i = (\varepsilon_{i_1}, \varepsilon_{i_2}, \ldots, \varepsilon_{i_n})$ potpuno određuje pripadnost broja i svakom članu S_j bilo kojeg promatranog niza $(S_1, S_2, \ldots, S_n)$, a zbog $S_1 \subseteq S_2 \supseteq S_3 \subseteq \ldots$ vrijedi $\varepsilon_{i_1} \leq \varepsilon_{i_2} \geq \varepsilon_{i_3} \leq \ldots$. Prema prethodnom primjeru takvih nizova $\varepsilon_i = (\varepsilon_{i_1}, \ldots, \varepsilon_{i_n})$ ima F_{n+2}. Skup svih promatranih nizova $(S_1, \ldots, S_n)$ je stoga u bijekciji sa skupom svih nizova $\varepsilon_i = (\varepsilon_{i_1}, \varepsilon_{i_2}, \ldots, \varepsilon_{i_r})$, pa iz pravila produkta slijedi da je odgovor doista F_{n+2}^r. □

Primjer 11. Dokažite da svih permutacija π skupa $[n]$ za koje je $|\pi(k) - k| \leq 1$, za svako $k \in [n]$, ima F_{n+1}.

Rješenje. Neka je p_n traženi broj. Iz pretpostavke slijedi da je $\pi(n) = n$ ili $\pi(n) = n-1$. U prvom slučaju ima p_{n-1}, takvih razmještaja, a u drugom p_{n-2}, jer je tada nužno $\pi(n-1) = n$ (jer zbog pretpostavke $\pi(i) \neq n$ za $i \leq n-2$). Zato je $p_n = p_{n-1} + p_{n-2}$, a zbog $p_1 = 1, p_2 = 2$ slijedi $p_n = F_{n+1}$.

Geometrijski to možemo ovako zamišljati. Nacrtajmo dva disjunktna skupa točaka (vrhova): $\{1, 2, \ldots, n\}$ i $\{\pi(1), \pi(2), \ldots, \pi(n)\}$. Spojimo bridom i s $\pi(j) \iff |i-j| \leq 1$. Tada ima F_{n+1} načina da odaberemo disjunktne bridove (masni) koji pokrivaju sve vrhove (tj. ovaj graf ima F_{n+1} savršenih sparivanja; to što se neki bridovi sijeku izvan vrhova nas ne zanima – o tome više u točki sparivanja u grafovima u pogl. VI o grafovima.)



□

Fibonaccijevi se brojevi ne javljaju samo u matematici, nego i drugdje: biologiji, računarstvu, arhitekturi, fizici itd. U biologiji (osim idealiziranog razmnožavanja zečeva), primijećeno je da se listovi nekih biljaka duž stabljike okreću za F_n/F_{n+1}-ti ili F_n/F_{n+2}-ti dio punog kuta s obzirom na prethodni donji list, jer tako dobivaju najviše izravne sunčeve svjetlosti. Ta je pojava poznata kao **filotaksa**.

Npr., brijest i lipa imaju 1/2 filotaksu, kruška i ruža 3/8-filotaksu, badem i vrba 5/13-filotaksu, suncokret 34/55-filotaksu itd. U računarstvu je odavno poznato (G. Lamé, 1844.) da u Euklidovu algoritmu za nalaženje najveće zajedničke mjere dvaju brojeva, najgori slučaj (tj. najveći broj dijeljenja) nastupa kod susjednih Fibonaccijevih brojeva (dokaz vidi u [56*]).

Objašnjenje za sve te i druge fenomene dolazi odatle što omjeri susjednih Fibonaccijevih brojeva

$$\frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34}, \cdots$$

predstavljaju najbolje racionalne aproksimacije iracionalnog broja

$$\alpha = \frac{1+\sqrt{5}}{2} \approx 1,61803\ldots \tag{3}$$

Taj se broj zove **omjer zlatnog reza** (ili **božanski omjer**), i to je ime uveo Leonardo da Vinci. Veza broja α i Fibonaccijevih brojeva je u sljedećem. Podijelimo osnovnu rekurziju $F_{n+1} = F_n + F_{n-1}$ s F_n i označimo $\alpha_n = F_{n+1}/F_n$. Tada dobivamo

$$\alpha_n = 1 + \frac{1}{\alpha_{n-1}}. \tag{4}$$

Ako ovu jednakost iteriramo, dobivamo

$$\frac{F_{n+1}}{F_n} = \alpha_n = 1 + \frac{1}{\alpha_{n-1}} = 1 + \frac{1}{1 + \dfrac{1}{\alpha_{n-2}}} = 1 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{\alpha_{n-3}}}} = \ldots$$

Dokažimo da niz $(\alpha_n)_{n\geq 1}$ konvergira. Prvo, jasno je $1 \leq \alpha_n \leq 2$, tj. (α_n) je omeđen. Nadalje, niz $(\alpha_{2n-1})_{n\geq 1}$ raste, a $(\alpha_{2n})_{n\geq 1}$ pada, pa su oba ova podniza konvergentna. To lako slijedi iz Cassinijevog identiteta (vidi iduću Propoziciju 1). Isto tako iz Cassinijevog identiteta slijedi $\alpha_n - \alpha_{n-1} = (-1)^n/F_nF_{n-1}$, pa zbog $F_n \geq n$, za $n \geq 5$, slijedi da je $|\alpha_n - \alpha_{n-1}|$ po volji malo za dovoljno veliki n. To sve zajedno povlači konvergenciju od (α_n). Na drugi se način konvergencija od (α_n) dobiva iz eksplicitne formule za F_n u Propoziciji 2.

Označimo li $\alpha = \lim_{n\to\infty} \alpha_n$, onda prelaskom na limes u (4) slijedi

$$\alpha = 1 + \frac{1}{\alpha}, \quad \text{tj. } \alpha^2 - \alpha - 1 = 0, \tag{5}$$

čije je jedino pozitivno rješenje dano s (3). Zato je i $\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \alpha = 1,61803\ldots$ i vrijedi ovaj razvoj u tzv. **neprekidne razlomke**:

$$\alpha = 1 + \frac{1}{\alpha} = 1 + \frac{1}{1+\frac{1}{\alpha}} = 1 + \frac{1}{1+\frac{1}{1+\frac{1}{\alpha}}} = \ldots = 1 + \cfrac{1}{1+\cfrac{1}{1+\cfrac{1}{1+\ldots}}}$$

U arhitekturi i umjetnosti (od starih Egipćana, preko starogrčkog, pa renesansnog doba i sve do danas) uočeno je da je ljudskom oku ugodno i estetično promatrati pravokutnike (npr. prozore, vrata, slike itd.) kod kojih je omjer visine a i širine b jednak $\alpha \approx 1,618$. To se postiže tako da je "omjer većeg prema manjem dijelu jednak omjeru cijele dužine prema većem dijelu":

$$a : b = (a + b) : a.$$

Označimo li $x := a/b$, odavde dobivamo

$$x = 1 + \frac{1}{x},$$

pa (zbog $x > 0$) dobivamo $x = \alpha$.

Dokažimo sada neke osnovne činjenice o Fibonaccijevim brojevima.

PROPOZICIJA 1. *Vrijedi sljedeće*

a) $\sum_{k=0}^{n} F_n = F_{n+2} - 1$; *b)* $\sum_{k=0}^{n} F_{2k-1} = F_{2n}$;

c) $\sum_{k=0}^{n} F_k^2 = F_nF_{n+1}$; *d)* $F_{m+n} = F_{m-1}F_n + F_mF_{n+1}$

e) $F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ (**Cassinijev**[3] **identitet**);

f) Svaki se prirodni broj n može jednoznačno zapisati kao $n = F_{n_1} + F_{n_2} + \cdots + F_{n_k}$, gdje je $n_1 > n_2 > \cdots > n_k > 0$ i $n_i \geq n_{i+1} + 2$ za sve i (**Zeckendorfov teorem**).

[3]Jean Dominique Cassini (1625–1712), francuski zvjezdoznanac i matematičar talijanskog podrijetla (pravim imenom Giovanni Domenico). Otkrio je 4 Saturnova satelita i vrijeme obrtanja Jupitera. Po njemu su nazvane ravninske krivulje, tzv. **Cassinijevi ovali**; to je skup točaka za koje je produkt udaljenost do dva fokusa stalan.

Dokaz. a) Napišemo (jedan ispod drugog) sve jednakosti $F_k = F_{k+1} - F_{k-1}$, za $k = 1, 2, \ldots, n$ i onda ih sve zbrojimo (teleskopiramo). Odatle odmah slijedi tvrdnja.

b) Ovaj put teleskopiramo sve jednakosti $F_{2k-1} = F_{2k} - F_{2k-2}$, $k = 1, 2, \ldots, n$ i opet tvrdnja slijedi neposredno.

c) Sada teleskopiramo jednakosti $F_k^2 = F_k(F_{k+1} - F_{k-1}) = F_kF_{k+1} - F_kF_{k-1}$, za $k = 1, 2, \ldots, n$ i opet tvrdnja odmah slijedi.

d) To se može jednostavno dokazati indukcijom po m za čvrsto n. Kombinatorno, to ide ovako. Lijeva strana F_{m+n} broji sve binarne nizove duljine $m+n-2$ bez susjednih nula (Primjer 8a). Pogledajmo poziciju na mjestu $m+1$. Ako je na tom mjestu 1, onda lijevo možemo popuniti niz na F_m načina, a desno na F_{n+1} načina, dakle ukupno na F_mF_{n+1}. Ako je pak na poziciji $m+1$ nula, onda na dva mjesta oko nje moraju biti jedinice, pa dobivamo $F_{m-1}F_n$ načina. Odatle slijedi tvrdnja.

e) Cassinijev se identitet lako dokazuje indukcijom po n. Međutim, ljepše je ovako. Indukcijom po n, lako se dokaže jednakost matrica

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

Uzmemo li determinante na obje strane (sjetimo se $\det(A \cdot B) = \det A \cdot \det B$-Cauchy-Binetov teorem), tvrdnja odmah slijedi. Treći je način da se za $n \geq 0$ definira $F_{-n} := (-1)^{n-1}F_n$ i uvrsti $m = -n + 1$ u d).

f) Za svako $n \in \mathbb{N}$, $\exists! n_1 \in \mathbb{N}$ tako da je $F_{n_1} \leq n < F_{n_1+1}$. Ako je $n = F_{n_1}$, dokaz je gotov. U protivnom je $0 < n - F_{n_1} < F_{n_1+1} - F_{n_1} = F_{n_1-1}$. Tada $\exists! n_2 \in \mathbb{N}$ tako da je $F_{n_2} \leq n - F_{n_1} < F_{n_2+1}$. Sada $F_{n_2} \leq n - F_{n_1} < F_{n_1-1}$ povlači $n_2 \leq n_1 - 2$. Ako je $n - F_{n_1} = F_{n_2}$, tj. $n = F_{n_1} + F_{n_2}$, dokaz je gotov, a u protivnome $\exists! n_3 \in \mathbb{N}$, $n_3 \leq n_2 - 2$ tako da je $F_{n_3} \leq n - F_{n_1} - F_{n_2} < F_{n_3+1}$ itd., na kraju dolazimo do parcijalne sume F_{n_k}, tako da je $n = F_{n_1} + F_{n_2} + \cdots + F_{n_k}$. Za jednoznačnost uporabite Primjer 8 b).

□

Izračunajmo sada eksplicitno F_n kao funkciju od n. Prvi su to učinili de Moivré i, neovisno, D. Bernoulli i J. P. M. Binet još u 18. stoljeću.

PROPOZICIJA 2. *n-ti Fibonaccijev broj je jednak*

$$F_n = \frac{1}{\sqrt{5}}\left[\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right], \quad \text{za } n = 0, 1, 2, \ldots \tag{6}$$

Dokaz. Ideja je dokaza da se rješenje rekurzije $F_n = F_{n-1} + F_{n-2}$, $n \geq 2$ (zanemarujući na trenutak početne vrijednosti F_0, F_1) potraži u obliku $F_n = x^n$. Uvrštavanjem dobivamo $x^n = x^{n-1} + x^{n-2}$, tj. $x^{n-2}(x^2 - x - 1) = 0$, pa zbog $x \neq 0$

imamo $x^2 - x - 1 = 0$. Dakle, $F_n = x^n$ je rješenje Fibonaccijeve rekurzije ako i samo ako je x rješenje ove kvadratne jednadžbe, tj. $x_{1,2} = (1 \pm \sqrt{5})/2$. Prema tome su $F_n^{(1)} = x_1^n$ i $F_n^{(2)} = x_2^n$ rješenja te rekurzije. No tada vrijedi $F_n^{(1)} = F_{n-1}^{(1)} + F_{n-2}^{(1)}$, $F_n^{(2)} = F_{n-1}^{(2)} + F_{n-2}^{(2)}$. Ako prvu jednakost pomnožimo s λ, a drugu s μ i to zbrojimo, dobivamo da je i njihova linearna kombinacija

$$G_n = \lambda F_n^{(1)} + \mu F_n^{(n)}, \quad \lambda, \mu \in \mathbb{R}$$

također rješenje, tj. $G_n = G_{n-1} + G_{n-2}$ (što zapravo znači da skup svih rješenja čini vektorski prostor). Prema tome je $F_n = \lambda x_1^n + \mu x_2^n$ također rješenje rekurzije. Sada iz početnih vrijednosti $F_0 = 0$, $F_1 = 1$ dobivamo $\lambda + \mu = 0$ i $\lambda x_1 + \mu x_2 = 1$. Rješenje ovog sustava linearnih jednadžbi je $\lambda = 1/\sqrt{5}$, $\mu = -1/\sqrt{5}$, pa tvrdnja slijedi. □

Formula (6) se obično u literaturi zove **Binetova formula**. Rješenja x_1, x_2 karakteristične jednadžbe $x^2 - x - 1 = 0$ označit ćemo s $x_1 = \alpha = (1+\sqrt{5})/2 \approx 1,61803\ldots$ (omjer zlatnog reza) i $x_2 = \beta = (1 - \sqrt{5})/2 \approx -0,61803\ldots$. ($\alpha + \beta = 1, \alpha\beta = -1$). Dakle,

$$F_n = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n). \tag{7}$$

KOROLAR 1. *Brojevi F_n rastu eksponencijalno, točnije*

$$F_n \sim \frac{1}{\sqrt{5}}\alpha^n. \tag{8}$$

Nadalje, F_n je jednak najbližem cijelom broju od $\alpha^n/\sqrt{5}$, točnije

$$F_n = \left\lfloor \frac{1}{\sqrt{5}}\alpha^n + \frac{1}{2} \right\rfloor. \tag{9}$$

Dokaz. Kako je $|\beta| < 1$, to je $\lim_{n\to\infty} \beta^n = 0$, pa ako (7) podijelimo s $\alpha^n/\sqrt{5}$, odmah dobivamo

$$\lim_{n\to\infty} \frac{F_n}{\alpha^n/\sqrt{5}} = 1,$$

što znači da vrijedi (8).
Formula (9) slijedi iz ovoga:

$$|F_n - \frac{1}{\sqrt{5}}\alpha^n| = \frac{1}{\sqrt{5}}|\alpha^n - \beta^n - \alpha^n| = \frac{1}{\sqrt{5}}|\beta|^n \le \frac{1}{\sqrt{5}}|\beta| \le \frac{1}{\sqrt{5}} < \frac{1}{2}.$$

□

Lucasovi[4] **brojevi** L_n se definiraju slično:

$$L_1 = 1,\ L_2 = 3, \quad L_{n+2} = L_{n+1} + L_n,\ n \ge 1 \tag{10}$$

Pokažimo neke veze između Fibonaccijevih i Lucasovih brojeva.

[4]Edouard Lucas (1842–1891), francuski matematičar. Ustvari je Lucas i uveo naziv Fibonaccijevi brojevi.

Primjer 12. Dokažite sljedeće formule:

a) $L_n = F_{n-1} + F_{n+1}$; b) $F_{2n} = F_n L_n$;
c) $L_{n-1} + L_{n+1} = 5F_n$; d) $L_n^2 - 5F_n^2 = 4(-1)^n$;

Rješenje. a) Za $n = 1$ i $n = 2$ formula se izravno provjeri. Pretpostavimo li da vrijedi za n i $n+1$, onda zbrajanjem tih jednakosti odmah vidimo da vrijedi i za $n+2$.

b) Iz Propozicije 1.d) za $m = n$ dobivamo $F_{2n} = F_n(F_{n-1} + F_{n+1}) = F_n L_n$.

c) Iz a) je $L_{n-1} + L_{n+1} = (F_{n-2} + F_n) + (F_n + F_{n+2}) =$
$= 2F_n + F_{n-2} + F_{n+2} = 2F_n + F_{n-2} + F_n + F_{n+1} = 3F_n + F_{n-2} + F_{n+1} =$
$3F_n + F_{n-2} + F_n + F_{n-1} = 4F_n + F_{n-2} + F_{n-1} = 4F_n + F_n = 5F_n$.

d) Prvo, u Cassinijev identitet (Propozicija 1.e)) uvrstimo $F_{n-1} = F_{n+1} - F_n$ da dobijemo

$$F_{n+1}^2 - F_{n+1}F_n - F_n^2 = (-1)^n.$$

Množenjem s 4 imamo

$$4(-1)^n = 4F_{n+1}^2 - 4F_{n+1}F_n - 4F_n^2 = (2F_{n+1} - F_n)^2 - 5F_n^2 =$$
$$= (F_{n+1} + F_{n-1})^2 - 5F_n^2 = L_n^2 - 5F_n^2.$$

□

Ustvari, formula d) iz ovog primjera se može uzeti za definiciju Fibonaccijevih i Lucasovih brojeva, tj. oni su sva rješenja diofantske jednadžbe $x^2 - 5y^2 = 4(-1)^n$. To i mnoga druga svojstva dokazana su u lijepoj knjižici [29*].

Na potpuno isti način kao za Fibonaccijeve brojeve, pokazuje se (učinite to) da za Lucasove brojeve vrijedi:

$$L_n = \alpha^n + \beta^n,$$
$$L_n \sim \alpha^n, L_n = \lfloor \alpha^n + 1/2 \rfloor,\ n \ge 2.$$

U idućem ćemo primjeru vidjeti jedno kombinatorno značenje Lucasovih brojeva.

Primjer 13. a) Koliko ima r-članih podskupova iz $[n]$ koji ne sadrže dva uzastopna broja ni 1 ni n?

b) Koliko ima svih podskupova iz $[n]$ koji ne sadrže dva uzastopna broja ni 1 ni n? (Drukčije rečeno, ako brojeve $1, 2, \ldots, n$ redom smjestimo kao točke na kružnici, koliko ima r-podskupova tih točaka koji ne sadrže dvije susjedne točke, odnosno svih takvih podskupova?)

Rješenje. a) Označimo s $f_2^*(n,r)$ traženi broj, a s $f_2(n,r)$ broj r-podskupova iz $[n]$ koji ne sadrže dva susjedna broja. Prema Primjeru 41 iz poglavlja II je

$$f_2(n,r) = \binom{n-r+1}{r}. \tag{*}$$

Ako r-podskup od n točaka na kružnici sadrži broj (točku) n, onda ne smije sadržavati ni 1 ni $n-1$, pa takvih ima $f_2(n-3, r-1)$, a ako ne sadrži broj (točku) n, onda takvih

ima $f_2(n-1,r)$. Dakle, imamo (rabeći (*)):

$$f_2^*(n,r) = f_2(n-3,r-1) + f_2(n-1,r) = \binom{n-r-1}{r-1} + \binom{n-r}{r} =$$

$$= (\frac{r}{n-r}+1)\binom{n-r}{r} = \frac{n}{n-r}\binom{n-r}{r}.$$

b) Označimo s K_n traženi broj. Ako "kružni podskup" sadrži broj (točku) n, onda ne smije sadržavati ni 1 ni $n-1$, pa ih ima K_{n-2}, a ako ne sadrži broj (točku) n, onda ih ima K_{n-1}. Dakle, $K_n = K_{n-2} + K_{n-1}$, za $n \geq 3$. No, izravnom provjerom se odmah vidi da je $K_1 = 1$ i $K_2 = 3$. Stoga K_n i L_n zadovoljavaju istu rekurziju i imaju iste početne vrijednosti (10), pa se podudaraju, tj. $K_n = L_n$. (Na drugi način, zbrojite sve $f_2^*(n,r)$ po $r \geq 0$ i uporabite (2).)

□

§ 2. Linearne rekurzije s konstantnim koeficijentima

Po uzoru na Fibonaccijevu rekurziju, sada ćemo dati "recept" kako se rješavaju i sve rekurzije tog tipa. **Linearna homogena rekurzija s konstantnim koeficijentima reda** r za niz $(a_n)_{n\geq 0}$ realnih ili kompleksnih brojeva je rekurzija oblika:

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \ldots + c_r a_{n-r}, \quad n \geq r, \tag{11}$$

gdje su $c_1, c_2 \ldots, c_r$ zadane konstante i $c_r \neq 0$. Naziv "linearna homogena" dolazi odatle što skup svih rješenja od (11) čini vektorski prostor (nad $\mathbb{R}$ ili $\mathbb{C}$). Naime, ako su (a'_n) i (a''_n) dva niza koji zadovoljavaju (11), onda uvrštavanjem a'_n u (11) i množenjem s λ, pa uvrštavanjem a''_n u (11) i množenjem s μ, te konačno zbrajanjem tih dviju jednakosti slijedi da i niz $(\lambda a'_n + \mu a''_n)$, $\lambda, \mu \in \mathbb{C}$ zadovoljava (11). Nadalje, imamo i "nul-rješenje" $a_n = 0$.

Rekurzija (11) se rješava tako da (kao u dokazu Propozicije 2) rješenja potražimo u obliku $a_n = x^n$, za neko $x \neq 0$ (jer nas "nul-rješenje" ili "trivijalno rješenje" ne zanima). Uvrštavanjem u (11), nakon skraćivanja s $x \neq 0$ dobivamo

$$x^r - c_1 x^{r-1} - c_2 x^{r-2} - \ldots - c_r = 0. \tag{12}$$

Ta se jednadžba zove **karakteristična jednadžba rekurzije** (11). Ona ima r (ne nužno različitih) rješenja $x_1, x_2, \ldots, x_r \in \mathbb{C}$ koja zovemo **karakteristični korijeni rekurzije** (11). Zbog $c_r \neq 0$, oni su svi $\neq 0$. Dakle, za $0 \neq x \in \mathbb{C}$, $a_n = x^n$ je rješenje od (11) ako i samo ako je x karakteristični korijen od (11).

PROPOZICIJA 3. *Pretpostavimo da su svi karakteristični korijeni $x_1, x_2, \ldots, x_r$ rekurzije* (11) *međusobno različiti brojevi. Tada je svako rješenje te rekurzije dano formulom*

$$a_n = \lambda_1 x_1^n + \lambda_2 x_2^n + \ldots + \lambda_r x_r^n, \quad n \geq r, \tag{13}$$

za neke brojeve $\lambda_1, \ldots, \lambda_r \in \mathbb{C}$.

Dokaz. Kako su $x_1^n, \ldots, x_r^n$ rješenja rekurzije (11), a skup svih rješenja čini vektorski prostor, onda je i njihova linearna kombinacija (13) rješenje te rekurzije.

Obratno, neka je a_n bilo koje rješenje rekurzije (11). Tada je a_n, za $n \geq r$, potpuno određen ako znamo početne uvjete. Neka su stoga npr., $a_0 = b_0, a_1 = b_1, \ldots, a_{r-1} = b_{r-1}$ početni uvjeti rekurzije (11). Tada treba pokazati da možemo odabrati konstante $\lambda_1, \ldots, \lambda_r$, tako da vrijedi

$$\begin{array}{ccccccccc} \lambda_1 & + & \lambda_2 & + & \ldots & + & \lambda_r & = & b_0 \\ \lambda_1 x_1 & + & \lambda_2 x_2 & + & \ldots & + & \lambda_r x_r & = & b_1 \\ & & \vdots & & & & & & \\ \lambda_1 x_1^{r-1} & + & \lambda_2 x_2^{r-1} & + & \ldots & + & \lambda_r x_r^{r-1} & = & b_{r-1}. \end{array}$$

Ovaj sustav od r linearnih jednadžbi s r nepoznanica $\lambda_1, \ldots, \lambda_r$ ima za matricu sustava matricu $V = (x_i^{j-1})$, čija je determinanta Vandermondeova determinanta[5]

$$\det V = \prod_{1 \leq i < j \leq r} (x_j - x_i).$$

Kako su prema pretpostavci svi karakteristični korijeni $x_1, \ldots, x_r$ međusobno različiti, slijedi da je $\det V \neq 0$, pa ovaj sustav ima jedinstveno rješenje po λ_1, λ_2, $\ldots$, λ_r. □

Rješenje (13) se zove **opće rješenje rekurzije** (11). Uočite da smo ustvari dokazali da nizovi $(x_1^n), \ldots, (x_r^n)$ čine bazu prostora $\mathcal{A}$ svih rješenja od (11), te da je dimenzija tog prostora $\dim \mathcal{A} = r$ (nad $\mathbb{C}$).

Primjer 14. Riješite rekurziju $a_n = 4a_{n-1} - a_{n-2} - 6a_{n-3}$, za $n \geq 3$, uz početne uvjete $a_0 = -1, a_1 = 2, a_3 = 4$.

Rješenje. Stavimo li $a_k = x^k$ u ovu rekurziju trećeg reda, dobivamo karakterističnu jednadžbu $x^3 - 4x^2 + x + 6 = 0$, čiji su korijeni $x_1 = -1, x_2 = 2, x_3 = 3$. Stoga je opće rješenje dano s $a_n = \lambda_1(-1)^n + \lambda_2 2^n + \lambda_3 3^n$. Treba još odrediti $\lambda_1, \lambda_2, \lambda_3$ iz početnih uvjeta: $a_0 = \lambda_1 + \lambda_2 + \lambda_3 = -1$, $a_1 = -\lambda_1 + 2\lambda_2 + 3\lambda_3 = 2$, $a_2 = \lambda_1 + 4\lambda_2 + 9\lambda_3 = 4$. Jedinstveno rješenje ovog sustava je $\lambda_1 = -1, \lambda_2 = -1, \lambda_3 = 1$, pa je traženo rješenje

$$a_n = 3^n - 2^n - (-1)^n.$$

□

Primjer 15. Komunikacijskim kanalima mogu se predati poruke koristeći se samo trima simbolima $a = \cdot$, $b = +$, $c = -$. Dopustive poruke su one kod kojih se na susjednim mjestima ne pojavljuje simbol a. Koliko ima dopustivih poruka duljine n?

Rješenje. Neka je d_n broj dopustivih poruka duljine n. Odmah se vidi da je $d_1 = 3, d_2 = 8$. Za $n \geq 3$, ako dopustiva poruka duljine n počinje s b ili c, onda se poruka može

[5] Sve činjenice iz linearne algebre mogu se naći u standardnim udžbenicima, npr. K. Horvatić, *Linearna Algebra I, II*, skripta Sveučilišta u Zagrebu, Zagreb, 1997, zatim npr. [132],[128],[129] itd.

dokrajčiti na $2d_{n-1}$ načina, a ako počinje s a, onda na drugom mjestu može biti ili b ili c pa se poruka može kompletirati na $2d_{n-2}$ načina. Stoga dobivamo za $n \geq 3$:

$$d_n = 2d_{n-1} + 2d_{n-2}.$$

Karakteristična jednadžba te rekurzije je $x^2 - 2x - 2 = 0$, čiji su korijeni $x_{1,2} = 1 \pm \sqrt{3}$, pa je opće rješenje za $n \geq 3$ dano s

$$d_n = \lambda(1+\sqrt{3})^n + \mu(1-\sqrt{3})^n.$$

Iz početnih se uvjeta lako odrede λ i μ, pa se kao konačno rješenje dobiva

$$d_n = \frac{2+\sqrt{3}}{2\sqrt{3}}(1+\sqrt{3})^n - \frac{2-\sqrt{3}}{2\sqrt{3}}(1-\sqrt{3})^n.$$

□

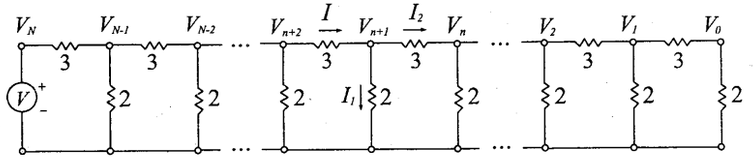
Evo jednog primjera iz elektrotehnike.

Primjer 16. Promotrimo električnu mrežu u kojoj imamo N otpornika od $2\,\Omega$ (ohma) i N otpornika od $3\,\Omega$ koji su spojeni žicama (kao na slici) s izvorom struje napona V. Nađite izraz za napon v_n, $0 \leq n \leq N$, u svakom čvoru (razgraništu) mreže kao funkciju od n. (To je također pad napona duž otpornika od $2\,\Omega$ ispod tog čvora; znamo da je $v_n = V$ napon koji daje izvor-generator.)

Rješenje. Da riješimo taj problem, podsjetimo na dva fundamentalna zakona.

Kirchhoffov zakon: U svakom čvoru mreže, suma ulaznih struja jednaka je sumi izlaznih struja iz tog čvora.

Ohmov zakon: Ako je pad napona duž otpornika od R ohma jednak $V_2 - V_1$, onda je jačina struje I u otporniku jednaka $I = (V_2 - V_1)/R$.



Promatrajmo jačinu struje u čvoru označenom s v_{n+1} (vidi sliku). Prema Kirchhoffovom zakonu je $I = I_1 + I_2$, a prema Ohmovom zakonu, $I = (v_{n+2} - v_{n+1})/3$, $I_1 = v_{n+1}/2$, $I_2 = (v_{n+1} - v_n)/3$ pa odavde slijedi za $0 \leq n \leq N-2$:

$$\frac{v_{n+2} - v_{n+1}}{3} = \frac{v_{n+1}}{2} + \frac{v_{n+1} - v_n}{3} \iff 2v_{n+2} - 7v_{n+1} + 2v_n = 0.$$

Pripadna karakteristična jednadžba je $2x^2 - 7x + 2 = 0$, čiji su korijeni $\alpha = (7+\sqrt{33})/4$, $\beta = (7-\sqrt{33})/4$. Stoga je $v_n = \lambda_1\alpha^n + \lambda_2\beta^n$. Nadalje imamo $(v_1 - v_0)/3 = v_0/2 \Rightarrow v_1 = 5v_0/2$, pa je $v_0 = \lambda_1 + \lambda_2$ i $5v_0/2 = v_1 = \lambda_1\alpha + \lambda_2\beta$, odakle dobivamo $\lambda_1 = v_0(5-2\beta)/2(\alpha-\beta)$, $\lambda_2 = v_0(2\alpha-5)/2(\alpha-\beta)$. Odavde je

$$v_n = \frac{v_0}{2(\alpha-\beta)}[(5-2\beta)\alpha^n + (2\alpha-5)\beta^n].$$

Zbog

$$V = v_N = \frac{v_0}{2(\alpha-\beta)}[(5-2\beta)\alpha^N + (2\alpha-5)\beta^N],$$

dobivamo $v_0 = 2(\alpha-\beta)V/[(5-2\beta)\alpha^N + (2\alpha-5)\beta^N]$, pa konačno

$$v_n = V\Big[\frac{(5-2\beta)\alpha^n + (2\alpha-5)\beta^n}{(5-2\beta)\alpha^N + (2\alpha-5)\beta^N}\Big].$$

□

Sada promotrimo opći slučaj kada korijeni karakteristične jednadžbe (12) rekurzije (11) nisu nužno međusobno različiti nego se ponavljaju.

PROPOZICIJA 4. *Pretpostavimo da je karakteristični polinom $P(x)$ rekurzije (11) dan s*

$$P(x) = (x-x_1)^{k_1}(x-x_2)^{k_2}\dots(x-x_t)^{k_t},$$

gdje su $x_1, x_2, \dots, x_t \in \mathbb{C}\setminus\{0\}$ svi međusobno različiti, a $k_1, \dots, k_t$ prirodni brojevi za koje je $k_1 + k_2 + \dots + k_t = r$. Tada je svako rješenje te rekurzije dano formulom

$$a_n = \sum_{i=1}^{t}\sum_{j_i=0}^{k_i-1} \lambda_{ij_i} n^{j_i} x_i^n\ , \tag{14}$$

za neki izbor konstanti $\lambda_{ij_i} \in \mathbb{C}$ $(i = 1,2,\dots,t,\ j_i = 0,1,\dots,k_i-1)$.

Dokaz. Dokaz je potpuno analogan dokazu Propozicije 3, samo što je tehnički malo zamršeniji, pa ga nećemo provesti u svim detaljima, već to prepuštamo čitatelju.

Osnovna je ideja (vidi dokaz i tekst iza Propozicije 3) da dokažemo da prostor $\mathcal{A} = \{(a_n)\}$ svih rješenja rekurzije (11) ima za bazu sve nizove (ukupno njih r):

$$n^{j_1}x_1^n (0 \leq j_1 \leq k_1-1), n^{j_2}x_2^n (0 \leq j_2 \leq k_2-1), \dots, n^{j_t}x_t^n (0 \leq j_t \leq k_t-1).$$

Da su ovo rješenja proizlazi odatle što je x_i k_i-struka nultočka od $P(x)$ ako i samo ako je x_i nultočka svih derivacija od $P(x)$ do uključivo reda $k_i - 1$.

Egzistencija brojeva λ_{ij_i} svodi se opet na $r \times r$ linearni sustav čija matrica ima opći član $(n^{j_i}x_i^n)$, $0 \leq n \leq r-1$, $0 \leq j_i \leq k_i - 1$, $i = 1,\dots,t$. Determinanta D te matrice je **poopćena Vandermondeova determinanta** (jer se za $k_1 = \dots = k_t$ svodi na Vandermondeovu) i iznosi

$$D = \prod_{i=1}^{t}(-x_i)^{\binom{k_i}{2}} \prod_{1\leq i<j\leq t}(x_j - x_i)^{k_i k_j}.$$

Kako su $x_1, \dots, x_t$ međusobno različiti ne-nul brojevi, slijedi da je $D \neq 0$, pa sustav ima jedinstveno rješenje po λ_{ij_i}. □

Rješenje (14) također se zove **opće rješenje rekurzije** (11).

Primjer 17. Riješite rekurziju $a_n = 5a_{n-1} - 6a_{n-2} - 4a_{n-3} + 8a_{n-4}$ za $n \geq 4$ uz početne uvjete $a_0 = 1, a_1 = 8, a_2 = 12, a_3 = 38$.

Rješenje. Uvrstimo li $a_n = x^n$, dobivamo karakterističnu jednadžbu $x^4 - 5x^3 + 6x^2 + 4x - 8 = 0$, tj. $(x-2)^3(x+1) = 0$, koja ima trostruki korijen $x_1 = 2$ i jednostruki korijen $x_2 = -1$. Rješenja pridružena korijenu $x_1 = 2$ su: $2^n, n2^n, n^2 2^n$, a rješenje pridruženo korijenu $x_2 = -1$ jest: $(-1)^n$. Stoga je opće rješenje te rekurzije

$$a_n = \lambda_1 2^n + \lambda_2 n 2^n + \lambda_3 n^2 2^n + \lambda_4 (-1)^n.$$

Iz početnih uvjeta dobivamo sustav od 4 linearne jednadžbe po $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ čije je rješenje (provjerite) $\lambda_1 = 3, \lambda_2 = -1/4$, $\lambda_3 = 1/4$, $\lambda_4 = -2$. Stoga je opće rješenje rekurzije uz dane početne vrijednosti:

$$a_n = 3 \cdot 2^n - n2^{n-2} + n^2 2^{n-2} - 2(-1)^n.$$

□

Linearna nehomogena rekurzija s konstantnim koeficijentima

To je rekurzija oblika

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_r a_{n-r} + f(n), \ n \geq r, \tag{15}$$

gdje je $f : \mathbb{N} \to \mathbb{C}$ zadana funkcija (zapravo, f je dovoljno zadati na $\{r, r+1, \ldots\}$). **Pripadna homogena rekurzija** od (15) je ona koja se dobiva izostavljanjem $f(n)$ (tj. ona za koju je $f(n) = 0$ za svako $n \geq r$). Bilo koje rješenje od (15) zove se **partikularno rješenje nehomogene rekurzije**.

PROPOZICIJA 5. *Svako rješenje rekurzije* (15) *je zbroj općeg rješenja pripadne homogene rekurzije i partikularnog rješenja nehomogene.*

Dokaz. Neka je a'_n neko (partikularno) rješenje od (15). Tada je $a_n - a'_n$ rješenje pripadne homogene, pa se zbog Propozicije 4 ono može napisati kao opće rješenje $a_n^{(0)}$ (za neki izbor konstanti λ_{ij}). Dakle, $a_n = a_n^{(0)} + a'_n$. To smo i tvrdili. □

Kako se nalaze partikularna rješenja od (15)? Općenito, ne postoji efikasni algoritam za to, jer funkcija f može biti vrlo neugodna. Međutim, u praksi je najčešći slučaj da je f polinomska ili eksponencijalna funkcija ili njihov zbroj ili produkt.

Ako je, primjerice, $f(n) = P_k(n)$ polinom k-tog stupnja, onda se i partikularno rješenje a'_n traži u obliku polinoma $Q_k(n)$ k-tog stupnja čije koeficijente određujemo "metodom neodređenih koeficijenata". Egzistencija i jedinstvenost rješenja tom metodom jamči nam oblik baze iz dokaza Propozicije 4.

Primjer 18. Riješite rekurziju $a_n = 4a_{n-1} - 4a_{n-2} - 2n + 5 \cdot 3^n$, uz početni uvjet $a_0 = 0, a_1 = 1$.

Rješenje. Opće rješenje pripadne homogene rekurzije $a_n = 4a_{n-1} - 4a_{n-2}$ dobije se iz pripadne karakteristične jednadžbe $(x-2)^2$, pa je ono dano s $a_n^{(0)} = \lambda 2^n + \mu n 2^n$. Da nađemo partikularno rješenje nehomogene rekurzije, uočimo da je nehomogeni dio $f(n) = -2n + 5 \cdot 3^n$ zbroj polinoma prvog stupnja (to je član $-2n$) i eksponencijalne funkcije $5 \cdot 3^n$. Zato i partikularno rješenje tražimo u tom obliku, tj. $a'_n = An + B + C \cdot 3^n$.

Uvrstimo li to u početnu rekurziju, onda izjednačavanjem koeficijenata uz n, slobodnih članova i onih uz 3^n (tj. uz 3^{n-2}), dobivamo $A = -2, B = -8, C = 45$. Stoga je svako rješenje naše rekurzije oblika

$$a_n = \lambda 2^n + \mu n 2^n - 2n - 8 + 45 \cdot 3^n.$$

Iz početnih uvjeta dobivamo $\lambda = -37, \mu = -25$, pa je traženo rješenje

$$a_n = 5 \cdot 3^{n+2} - 25n \cdot 2^n - 37 \cdot 2^n - 2n - 8. \ ^6$$

□

§ 3. Neke linearne rekurzije, svođenje na njih i neki sustavi rekurzija

Prvo, ako je zadana funkcija $f : \mathbb{N} \to \mathbb{C}$, onda se linearna rekurzija oblika $a_n = f(n)a_{n-1}$ rješava tako da se pomnože (teleskopiraju) sve jednakosti $a_n = f(n)a_{n-1}$, $a_{n-1} = f(n-1)a_{n-2}$, $a_{n-2} = f(n-2)a_{n-3}, \ldots$, $a_2 = f(2)a_1$, $a_1 = f(1)a_0$, odakle se dobiva

$$a_n = f(1)f(2)\ldots f(n)a_0.$$

Kao primjenu ovoga izračunajmo volumen n-dimenzionalne kugle.

Primjer 19. Neka je $V_n(1) = V_n = V(B^n)$ volumen jedinične n-dimenzionalne kugle B^n. Tada je

$$V_n = \left\{ \begin{array}{ll} \frac{2(2\pi)^{(n-1)/2}}{1 \cdot 3 \cdot 5 \cdot \cdots \cdot n} & , \text{ako je } n \text{ neparan,} \\ \pi^{n/2}/(n/2)! & , \text{ako je } n \text{ paran} \end{array} \right\} = \frac{\pi^{n/2}}{\Gamma(n/2+1)}.$$

Rješenje. Presijecimo B^n s hiperravninom $x_n = \cos\varphi$. Kao presjek dobivamo $(n-1)$-dimenzionalnu kuglu radijusa $r = \sin\varphi$. Kako je $V_n(r) = r^n V_n(1)$, lako se vidi da je (nacrtajte sliku):

$$V_n = 2\int_{\pi/2}^{0} V_{n-1}(\sin\varphi) d(\cos\varphi) = 2V_{n-1}\int_0^{\pi/2} \sin^n\varphi d\varphi = 2V_{n-1}I_n.$$

Parcijalnim integriranjem ($u = \sin^{n-1}\varphi$, $dv = \cos\varphi d\varphi$) dobivamo $I_n = [(n-1)/n]I_{n-2}$. Kako je $V_1 = 2$, $V_2 = \pi$ i $V_3 = 4\pi/3$, dobivamo

$$V_n = \frac{2\pi}{n} V_{n-2}, \quad n \geq 3.$$

Teleskopiranjem ove jednakosti dobivamo navedenu formulu. □

[6] Čitatelj koji je upoznat s rješavanjem linearnih diferencijalnih jednadžbi s konstantnim koeficijentima uočit će sličnost među tih dviju metoda. Razlog je taj što je diskretni analogon derivacije **operator diferencije** Δ za nizove $\Delta a_n = a_{n+1} - a_n$ i svaka rekurzija se može shvatiti kao **diferencijska jednadžba**. Npr. gornja rekurzija je $(\Delta^2 - 2\Delta + 1)a_{n-2} + 2n - 5 \cdot 3^n = 0$.

Nadalje, linearnu nehomogenu rekurziju prvog reda s varijabilnim koeficijentima

$$a_n = f(n)a_{n-1} + g(n), \quad n \geq 1 \tag{16}$$

rješavamo na sljedeći način. Označimo $F(n) := [f(1)f(2)\dots f(n)]^{-1}$, te $b_n := F(n)a_n$. Ako (16) pomnožimo s $F(n)$, onda dobivamo linearnu rekurziju

$$b_n = b_{n-1} + g(n)F(n),$$

koju možemo riješiti teleskopiranjem, pa dobivamo

$$a_n = \frac{1}{F(n)}(a_0F(0) + \sum_{k=1}^{n} g(k)F(k)). \tag{17}$$

Primjer 20. Riješite rekurzije uz dani početni uvjet a_0:
a) $(n+1)a_n = (n^2+n)a_{n-1} - n, a_0 = 1$; b) $a_n = a_{n-1}/n^2 + 1/(n-1)!^2, a_0 = 0$.

Rješenje. a) $a_n = na_{n-1} - n/(n+1)$, pa je $f(n) = n$, $g(n) = -n/(n+1)$. Odatle je $F(n) = 1/n!$, pa je prema (17)

$$a_n = n!(1 - \sum_{k=1}^{n} \frac{1}{k+1} \cdot \frac{1}{(k-1)!}).$$

No, zbog $\sum_{k=1}^{n} 1/(k+1)(k-1)! = \sum_{k=1}^{n}(1/k! - 1/(k+1)!) = 1 - 1/(n+1)!$, slijedi $a_n = 1/(n+1)$.

b) Tu je $f(n) = 1/n^2$, $g(n) = 1/(n-1)!^2$, pa je $F(n) = n!^2$ i stoga

$$a_n = n!^{-2} \sum_{k=1}^{n} \frac{1}{(k-1)!^2} k!^2 = n!^{-2} \sum_{k=1}^{n} k^2 = \frac{n(n+1)(2n+1)}{6n!^2}.$$

□

Još jedna primjena rekurzija tipa (16) povezat će nam Stirlingove cikličke brojeve i tzv. harmonijske brojeve. n-ti **harmonijski broj** H_n je definiran kao

$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \dots + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k},$$

tj. to je n-ta parcijalna suma (divergentnog) harmonijskog reda. Rekurzija (27) iz poglavlja II za $k = 2$ daje (s pomakom za 1):

$$c(n+1, 2) = nc(n, 2) + c(n, 1).$$

Označimo li $c(n, 2) =: a_n$, onda zbog $c(n, 1) = (n-1)!$ slijedi

$$a_{n+1} = na_n + (n-1)!,$$

a ovo je rekurzija tipa (16). Iz (17) se lako dobiva formula za broj permutacija na $[n+1]$ s točno 2 ciklusa:

$$c(n+1, 2) = n!H_n. \tag{18}$$

Poznato je da je $\lim_{n\to\infty}(H_n - \ln n) = \gamma = 0,57721566\dots$ **Eulerova konstanta**, te za velike n, $H_n \approx \ln n + \gamma + 1/2n$. I mnoge druge nelinearne rekurzije pogodnom supstitucijom ili pogodnom supstitucijom nakon nekih transformacija mogu se svesti na linearne rekurzije s konstantnim koeficijentima ili linearne rekurzije prvog reda s varijabilnim koeficijentima. Evo nekih primjera.

Primjer 21. Riješite rekurziju $a_{n+2} = a_{n+1}^3 \cdot a_n^{-2}$, uz početne uvjete $a_0 = 1, a_1 = 2$.

Rješenje. Odmah se vidi (indukcijom) da je $a_n > 0$. Stavimo $b_n := \log_2 a_n$. Tada dobivamo $b_{n+2} = 3b_{n+1} - 2b_n$, uz $b_0 = 0, b_1 = 1$. Ovu linearnu homogenu rekurziju drugog reda s konstantnim koeficijentima znamo riješiti i rješenje je $b_n = 2^n - 1$. Stoga je $a_n = 2^{2^n-1}$. □

Primjer 22. Riješite "kvadratne" rekurzije: a) $a_{n+1} = a_n(2 - ca_n)$, uz početni uvjet $a_0 = a$; b) $a_{n+1} = a_n^2 - 2$, $a_0 = 3$.

Rješenje. a) Za $c = 0$, rekurzija je oblika $a_{n+1} = 2a_n$, pa produktnim teleskopiranjem odmah dobivamo $a_n = a2^n$. Ako je $c \neq 0$, onda se naša rekurzija može ovako transformirati

$$ca_{n+1} = ca_n(2 - ca_n) = (1 - (1 - ca_n))(1 + (1 - ca_n)) = 1 - (1 - ca_n)^2,$$

tj., $1 - ca_{n+1} = (1 - ca_n)^2$. Supstitucijom $b_n := 1 - ca_n$ dobivamo $b_{n+1} = b_n^2$, $b_0 = 1 - ac$. Odavde slijedi (iteriranjem ili supstitucijom $c_n = \log_2 b_n$) da je $b_n = (1 - ac)^{2^n}$, pa stoga $a_n = \frac{1}{c}(1 - (1 - ac)^{2^n})$.

b) Neka je $c > 1$ rješenje jednadžbe $c + 1/c = 3$. Napišimo $a_n = c_n + 1/c_n$. Tada imamo $a_n = c_n + \frac{1}{c_n} = \left(c_{n-1} + \frac{1}{c_{n-1}}\right)^2 - 2 = c_{n-1}^2 + \frac{1}{c_{n-1}^2}$. Iz $c_n = c_{n-1}^2$, $c_0 = c$ slijedi $c_n = c^{2^n}$, pa je

$$a_n = \lceil c^{2^n} \rceil.$$

Uočite da je $c = \alpha^2$, gdje je α omjer zlatnog reza, tj. $c = (3 + \sqrt{5})/2 \approx 2.618$. □

Bilješka 1. Rekurzija iz Primjera 22 a) je poseban slučaj poznate rekurzije koja se zove **populacijska** (ili **logistička**) **jednadžba**, a glasi

$$a_{n+1} = \alpha a_n(1 - a_n), \tag{19}$$

gdje je a_n proporcionalan populaciji u trenutku n (sati, godina itd.) od početka promatranja rasta populacije (npr. bakterija, insekata pa i ljudi), a $0 < \alpha < 4$ parametar koji ovisi o brzini razmnožavanja. Za $\alpha = 2$ dobivamo gornji primjer za $c = 2$.

Ustvari, ta rekurzija je diskretizacija kontinuiranog modela rasta populacije $P = P(t)$ u vremenu t po kojemu je relativni rast populacije P linearna padajuća funkcija od P, tj.

$$\frac{1}{P}\frac{dP}{dt} = k - aP.$$

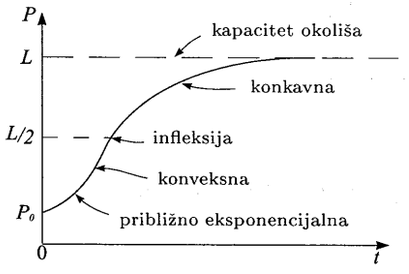
Za malu populaciju P dobivamo

$$\frac{1}{P}\frac{dP}{dt} \approx k,$$

tj. eksponencijalni rast. U logističkom modelu kada P raste, relativni rast pada prema 0 i dostiže nulu za $k - aP = 0$, tj. za $P = k/a$. Ova granična vrijednost $L = k/a$ se zove **kapacitet okoliša** i predstavlja najveću populaciju koju okoliš može podnijeti. Stavimo li $a = k/L$, logistička jednadžba postaje

$$\frac{dP}{dt} = kP(1 - \frac{P}{L}),$$

i to je neprekidni analogon od (19). Ovo je poznato pod nazivom **logistička diferencijalna jednadžba**, čije rješenje je (slikom i formulom):



$$P = \frac{L}{1 + Ae^{-kt}}, \quad A = \frac{L - P_0}{P_0},$$
$$P_0 = P(0).$$

Ovaj model potječe od belgijskog matematičara P. Verhulsta iz 1835. g.

Primjer 23. Riješite rekurziju $a_{n+1} = \frac{1}{2}(a_n + \frac{c}{a_n}), c > 0$, uz početni uvjet $a_0 = a$.

Rješenje. Transformirajmo ovu rekurziju ovako:

$$\frac{a_{n+1} - \sqrt{c}}{a_{n+1} + \sqrt{c}} = \frac{\frac{1}{2}(a_n + \frac{c}{a_n}) - \sqrt{c}}{\frac{1}{2}(a_n + \frac{c}{a_n}) + \sqrt{c}} = \frac{a_n^2 - 2a_n\sqrt{c} + c}{a_n^2 + 2a_n\sqrt{c} + c} = (\frac{a_n - \sqrt{c}}{a_n + \sqrt{c}})^2.$$

Označimo li $b_n := (a_n - \sqrt{c})/(a_n + \sqrt{c})$, dobivamo $b_{n+1} = b_n^2$, $b_0 = (a - \sqrt{c})/(a + \sqrt{c})$. Odatle (iteriranjem ili supstitucijom $c_n = \log_2 b_n$) lako dobivamo $b_n = b_0^{2^n}$, što konačno daje $a_n = \sqrt{c}(1 + b_0^{2^n})/(1 - b_0^{2^n})$. □

Bilješka 2. Ova rekurzija je tzv. **Heronov algoritam** za sukscesivne aproksimacije broja $\sqrt{c}$. Prelaskom na limes u rekurziji dobivamo $\lim_{n\to\infty} a_n = \sqrt{c}$.

Linearni homogeni sustavi rekurzivnih relacija često se eliminacijom svode na jednu linearnu homogenu rekurziju. Evo tipičnog primjera.

Primjer 24. Nizovi brojeva (a_n) i (b_n) zadovoljavaju sustav rekurzivnih relacija

$$a_{n+1} = 2a_n - b_n$$
$$b_{n+1} = a_n + 4b_n.$$

Ako je $a_0 = 2, b_0 = 1$, odredite a_n i b_n.

Rješenje. Iz prve jednadžbe je $b_n = 2a_n - a_{n+1}$. Stoga je $b_{n+1} = 2a_{n+1} - a_{n+2}$. Ako te izraze uvrstimo u drugu relaciju, nakon sređivanja dobivamo $a_{n+2} = 6a_{n+1} - 9a_n$. Opće rješenje te rekurzije je $a_n = \lambda 3^n + \mu n 3^n$, a zbog $a_0 = 2$ i $a_1 = 2a_0 - b_0 = 3$, dobivamo da je $\lambda = 2, \mu = -1$, pa je $a_n = (2 - n)3^n$. Odavde se dobiva $b_n = 2a_n - a_{n+1} = (n + 1)3^n$. □

Ako trebamo riješiti rekurzivnu relaciju oblika

$$a_{n+1} = \frac{pa_n + q}{ra_n + s}$$

uz početni uvjet $a_0 = a$, postupimo ovako. Neka su (b_n) i (c_n) nizovi koji zadovoljavaju sustav rekurzija

$$b_{n+1} = pb_n + qc_n$$
$$c_{n+1} = rb_n + sc_n,$$

s početnim uvjetima $b_0 = a$ i $c_0 = 1$. Taj sustav riješimo kao u gornjem primjeru. Tada, ako je $a_n = b_n/c_n$, onda je $a_0 = b_0/c_0 = a$ i imamo

$$a_{n+1} = \frac{b_{n+1}}{c_{n+1}} = \frac{pb_n + qc_n}{rb_n + sc_n} = \frac{pb_n/c_n + q}{rb_n/c_n + s} = \frac{pa_n + q}{ra_n + s},$$

pa je (a_n) traženi niz.

Primjer 25. Riješite rekurzivnu relaciju $a_{n+1} = \frac{2a_n - 3}{3a_n - 4}$, uz početni uvjet $a_0 = -1$.

Rješenje. Nađimo prvo rješenje sustava

$$b_{n+1} = 2b_n - 3c_n \tag{20}$$
$$c_{n+1} = 3b_n - 4c_n, \tag{21}$$

koji zadovoljava početne uvjete $b_0 = -1$, $c_0 = 1$. Eliminacijom c_n i c_{n+1} dobivamo rekurziju $b_{n+2} + 2b_{n+1} + b_n = 0$, čije je opće rješenje $b_n = (-1)^n[\lambda + \mu n]$. Iz $b_0 = -1$, $b_1 = 2b_0 - 3c_0 = -5$, dobivamo $\lambda = -1$, $\mu = 6$ pa je $b_n = (-1)^n(6n - 1)$. Odavde slijedi da je $c_n = \frac{1}{3}(2b_n - b_{n+1}) = (-1)^n(6n + 1)$. Stoga je rješenje naše rekurzije $a_n = b_n/c_n = (6n - 1)/(6n + 1)$. □

Jedna specijalna klasa rekurzivnih relacija koje se često javljaju u analizi nekih (rekurzivnih) algoritama zahtijeva pažnju. Takvi algoritmi tipa "**podijeli pa ovladaj**" rekurzivno reduciraju dani problem u nekoliko manjih potproblema istog tipa. Ukupan broj koraka a_n potrebnih da se takvim algoritmom procesira n ulaznih podataka (inputa), često zadovoljava rekurzivnu relaciju tipa

$$a_n = ca_{n/d} + f(n) \qquad (d \text{ je djelitelj od } n).$$

Sljedeća tablica daje oblik rješenja te rekurzije za neke vrijednosti $c, d, f(n)$.

c, d	$f(n)$	a_n
$c = 1$	a	$\lceil \log_d n \rceil$
$c = d$	a	$An + B$
$c < d$	an	An
$c = d$	an	$\sim n \log_d n$
$c > d$	an	$\sim n^{\log_d c}$

Pritom to treba shvatiti ovako: a_n je proporcionalan s navedenim izrazom za velike n. Da su to zaista rješenja gornje rekurzije, nije teško pokazati indukcijom.

Primjer 26. Nađite i riješite rekurziju za broj a_n usporedbi od po dva broja, potreban da se u skupu S od n različitih realnih brojeva nađu najmanji i najveći broj ako je n potencija od 2.

Rješenje. Ako je $|S| = 2$, onda je očito $a_2 = 1$. Neka su m_1 i M_1 najmanji i najveći brojevi redom u prvoj polovici od S (prvih $n/2$ brojeva), a m_2, M_2 najmanji i najveći brojevi u drugoj polovici skupa S. Tada ove dvije usporedbe: m_1 i m_2, te M_1 i M_2 određuju najmanji i najveći broj u čitavom S. Stoga je $a_n = 2a_{n/2} + 2$. Iz prethodne tablice dobivamo da je rješenje oblika $a_n = A_1 n + A_2$, pa uvrštavanjem u tu rekurziju i iz početnog uvjeta $a_2 = 1$ dobivamo da je $a_n = \frac{3}{2}n - 2$. Ta se metoda katkad zove i **binarno pretraživanje**. □

Primjer 27. Da se pomnože dva n-znamenkasta broja, treba normalno n^2 množenja tipa znamenka puta znamenka. Pokažite da se s "podijeli pa ovladaj" to množenje može učiniti mnogo efikasnijim.

Rješenje. Uzmimo prvo da je n potencija od 2. Neka su p i q n-znamenkasti brojevi. Svakoga od njih rastavimo na dva $n/2$-znamenkasta dijela: $p = p_1 10^{n/2} + p_2$, $q = q_1 10^{n/2} + q_2$. Tada je

$$p \cdot q = p_1 q_1 10^n + (p_1 q_2 + p_2 q_1) 10^{n/2} + p_2 q_2.$$

No, $p_1 q_2 + p_2 q_1 = (p_1 + p_2)(q_1 + q_2) - p_1 q_1 - p_2 q_2$, pa trebamo samo tri množenja $n/2$-znamenkastih brojeva $p_1 q_1$, $p_2 q_2$ i $(p_1 + q_1)(p_2 + q_2)$ da se odredi $p \cdot q$. (Uočite da $p_1 + p_2$ i $q_1 + q_2$ mogu biti i $((n/2) + 1)$-znamenkasti, ali to ne mijenja bitno red veličine rješenja.) Označimo s a_n broj množenja tipa znamenka puta znamenka da se pomnože dva n-znamenkasta broja na gornji način. Tada dobivamo rekurziju $a_n = 3a_{n/2}$. Iz prethodne tablice (ili množenjem tih relacija) dobivamo da je a_n proporcionalan s $n^{\log_2 3} \approx n^{1,6}$, što je bitno poboljšanje od n^2. Ta opća ocjena od a_n vrijedi i za sve brojeve, a ne samo potencije od 2. □

Primjer 28 (Strassenovo brzo množenje matrica). Za množenje dviju $(n \times n)$-matrica uobičajenim množenjem treba n^3 množenja broj × broj (i $n^2(n-1)$ zbrajanja). Pokažimo da se broj množenja može reducirati na $M(n) = O(n^{\log_2 7}) = O(n^{2.807\ldots})$, što je za velike n bitno bolje nego n^3. Tako je V. Strassen 1969. (na opće iznenađenje) pokazao da Gaussova metoda eliminacije za rješavanja sustava linearnih jednadžbi nije i najefikasnija metoda.

Rješenje. Neka su $A = [a_{ij}]$, $B = [b_{ij}]$ dvije $(n \times n)$-matrice i $C = AB = [c_{ij}]$. Neka je prvo $n = 2$. Za množenje dviju (2×2) matrica definirajmo sedam brojeva x_i ovako:

$$x_1 = (a_{11} + a_{22})(b_{11} + b_{22}),\ x_2 = (a_{12} - a_{22})(b_{21} + b_{22}),\ x_3 = (a_{11} - a_{21})(b_{11} + b_{12}),$$

$$x_4 = (a_{11} + a_{12})b_{22},\ x_5 = (a_{21} + a_{22})b_{11},\ x_6 = a_{11}(b_{12} - b_{22}),\ x_7 = a_{22}(b_{21} - b_{11}).$$

Tada se c_{ij} dobivaju samo zbrajanjem:

$$c_{11} = x_1 + x_2 - x_4 + x_7, \quad c_{12} = x_4 + x_6,$$
$$c_{21} = x_5 + x_7, \quad c_{22} = x_1 - x_3 - x_5 + x_6.$$

Za ovo računanje treba samo 7 umjesto 8 $(= 2^3)$ množenja (i 18 zbrajanja). Uzmimo sada $n = 2^k$, razdijelimo A i B na blok $(2^{k-1} \times 2^{k-1})$-podmatrice

$$A = \begin{bmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{bmatrix}, \qquad B = \begin{bmatrix} B_{11} & B_{12} \\ B_{21} & B_{22} \end{bmatrix},$$

i primijenimo gornje pravilo s A_{11} umjesto a_{11} itd. Tada za ukupni broj množenja očito vrijedi $M(2^k) = 7M(2^{k-1})$, što uz $M(2) = 7$ daje $M(2^k) = 7^k$. Za opći n, uklještimo $2^k \le n < 2^{k+1}$, pa dobivamo $M(n) = O(n^{\log_2 7})$. □

§ 4. Catalanovi brojevi

U primjerima 45 i 46 prethodnog poglavlja već smo se susreli s Catalanovim brojevima. Sada ćemo spoznati još neka kombinatorna značenja tih brojeva i to tako da ćemo naći rekurzije za te brojeve i (ili) naći bijekcije među objektima koje prebrojavaju.

Podsjetimo se, n-ti **Catalanov broj** C_n je

$$C_n = \frac{1}{n+1}\binom{2n}{n},$$

a prvih nekoliko su (uz konvenciju $C_0 = 1$):

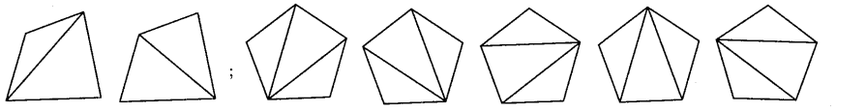
n	0	1	2	3	4	5	6	7	8	9	10	...
C_n	1	1	2	5	14	42	132	429	1430	4862	16796	...

Iz Stirlingove aproksimacije $n! \sim \sqrt{2\pi n}(n/e)^n$ nije teško izvesti asimptotiku za Catalanove brojeve:

$$C_n \sim \frac{4^n}{n\sqrt{\pi n}}.$$

Ustvari je Euler prvi razmatrao te brojeve, ali ih je Catalan ponovno otkrio riješivši neke probleme koje ćemo sad navesti.

Počnimo s **problemom triangulacije konveksnog poligona**. Problem je u tome da se izračuna broj T_{n+2} različitih načina da se konveksni $(n+2)$-terokut triangulira, tj. rastavi u n trokuta s $n-1$ dijagonala od kojih se nikoje dvije ne sijeku u unutrašnjosti. Za $n = 2$, četverokut možemo triangulirati na dva načina (sl. a), dakle $T_4 = 2$, a za $n = 3$, peterokut na pet načina (sl. b), dakle $T_5 = 5$:



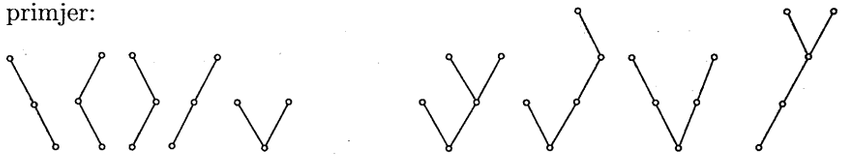
a) Triangulacije četverokuta b) Triangulacije peterokuta

Očito je $T_3 = 1$ jer je trokut već (jednoznačno) trianguliran, a dodatno još definiramo $T_2 := 1$. Drugi se problem zove **problem zagrada**. Problem je u tome da se izračuna broj Z_{n+1} različitih načina da se pomnoži $n+1$ brojeva $x_1, x_2, \ldots, x_{n+1}$ napisanih jedan do drugoga $x_1 x_2 x_3 \ldots x_{n+1}$ (u tome čvrstom poretku). Naime, mi znamo pomnožiti samo dva broja i prema zakonu asocijacije, dobivamo isti rezultat ako parom zagrada zagradimo svako od množenja. Problem je, dakle, naći ukupni broj takvih zagrađivanja. Za $n = 2$ imamo tri broja i $(x_1 x_2)x_3 = x_1(x_2 x_3)$ samo dva načina zagrađivanja, tj. $Z_3 = 2$. Za $n = 3$ imamo 4 broja i pet načina zagrađivanja (uočite da zadnje množenje ne zagrađujemo, jer je ono jednoznačno određeno):

$$(x_1 x_2)(x_3 x_4) = ((x_1 x_2)x_3)x_4 = (x_1(x_2 x_3))x_4 = x_1((x_2 x_3)x_4) = x_1(x_2(x_3 x_4)),$$

pa je $Z_4 = 5$. Očito je $Z_1 = Z_2 = 1$. Ovo je pitanje ekvivalentno tome koliko bi najviše rezultata dobili s neasocijativnim množenjem $n+1$ varijabli.

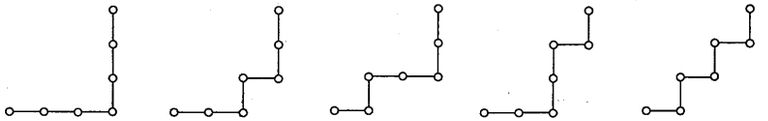
Treći je problem **problem binarnih stabala**. Stablo je, kao što znamo, povezani graf bez ciklusa. Binarna stabla (koja se često susreću u računarstvu, npr. u proučavanju strukture podataka, binarnim pretraživanjima i sortiranjima itd.) precizno se definiraju induktivno, tj. rekurzivno ovako. **Binarno stablo** je ili prazno (tj. nema bridova) ili se sastoji od jednog istaknutog vrha koji se zove **korijen** i uređenog para binarnih stabala koja se zovu **lijevo** i **desno podstablo**. Problem je da se izračuna broj B_n binarnih stabala s n vrhova (ovu privremenu oznaku B_n ne miješajte s oznakom za Bellove brojeve). Tako je $B_0 := 1, B_1 = 1, B_2 = 2, B_3 = 5$. Na primjer:



a) Binarna stabla s 3 vrha

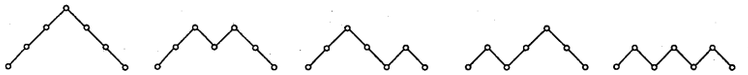
b) Neka binarna stabla s 5 vrhova

Četvrti je **problem putova u cjelobrojnoj mreži**. Naime, u cjelobrojnoj mreži u xy-ravnini treba naći broj P_n putova od $(0,0)$ do (n,n) s koracima $(1,0)$ i $(0,1)$ koji nikad ne prijeđu iznad pravca $y = x$. Očito $P_1 = 1$, $P = 2 = 2$. Za $n = 2$ nacrtamo sve te putove (ne crtamo cjelobrojnu mrežu), pa vidimo da je $P_3 = 5$.



$P_3 = 5$

(Taj smo problem riješili u Primjeru 45 c) u poglavlju II.) Peto, **problem Dyckovih[7] putova**. Ovaj se problem sastoji u tome da se izračuna broj D_n svih putova u cjelobrojnoj mreži u xy-ravnini od $(0,0)$ do $(2n,0)$ s koracima $(1,1)$ i $(1,-1)$ koji nikad ne padnu ispod osi x. Takvi se putovi zovu **Dyckovi putovi** (ili "planinski putovi"). Očito je $D_1 = 1, D_2 = 2$. Za $n = 3$ nacrtamo sve te putove (opet bez cjelobrojne mreže), pa vidimo da je $D_3 = 5$:



$D_3 = 5$

Konačno **Bertrandov[8] problem glasovanja**. Treba izračunati broj G_n nizova $(i_1, i_2, \ldots, i_{2n})$, $i_k \in \{-1, 1\}$, tako da je svaka parcijalna suma $i_1 + i_2 + \cdots + i_k \geq 0$, a ukupno $i_1 + i_2 + \cdots + i_{2n} = 0$. Interpretacija je ova. Na nekim predsjedničkim izborima, dva su kandidata A i B, a glasuje $2n$ ljudi. Svaki glas za A bilježimo s 1, a za B s -1. Na koliko načina možemo prebrojiti rezultate glasovanja, tako da B nikad nema više glasova od A, a konačni rezultat je ipak neriješen?

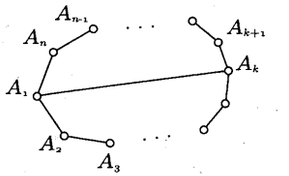
[7] Walther von Dyck (1856 – 1934), njemački matematičar

[8] Joseph Louis Francois Bertrand (1822–1900), francuski matematičar

PROPOZICIJA 6. *Vrijedi* $T_{n+2} = Z_{n+1} = B_n = P_n = D_n = G_n$. *Svi su ti brojevi jednaki* n*-tom Catalanovom broju* $C_n = \binom{2n}{n}/(n+1)$.

Dokaz. Plan dokaza je ovaj. Prvo ćemo pokazati da T_i-ovi, Z_i-ovi i B_i-ovi zadovoljavaju istu rekurziju i imaju iste početne uvjete (uz odgovarajuće pomake u indeksu), pa su jednaki. Zatim ćemo uspostaviti bijekciju među objektima koje prebrojavaju Z_{n+1} i G_n, G_n i D_n i konačno D_n i P_n. Na kraju ćemo izračunati jedan od tih brojeva.

Rekurzija za (triangulacije) T_{n+2}. Neka je $P = A_1A_2\ldots A_n$ konveksni n-terokut. U svakoj triangulaciji od P, stranica $\overline{A_1A_n}$ pripada nekom trokutu triangulacije. Taj trokut je uvijek oblika $A_1A_nA_k$, za neko $k = 2, 3, \ldots, n-1$. Za čvrsto k, dijagonalom $\overline{A_1A_k}$ poligon P je razbijen na "donji" k-terokut $A_1A_2\ldots A_k$ i "gornji" $(n-k+1)$-terokut $A_1A_k\ldots A_n$ (sl.).



Donji k-terokut možemo triangulirati na T_k načina, a gornji na T_{n-k+1} načina. Dakle, za čvrsto k, prema pravilu produkta čitav P na T_kT_{n-k+1} načina. Kada k varira, tj. za $k \in \{2, 3, \ldots, n-1\}$, prema pravilu sume dobivamo

$$T_n = T_2T_{n-1} + T_3T_{n-2} + \cdots + T_{n-1}T_2,$$

odnosno s pomakom indeksa za 2 dobivamo

$$T_{n+2} = T_2T_{n+1} + T_3T_n + \cdots + T_{n+1}T_2. \tag{22}$$

Rekurzija za Z_{n+1}. Promotrimo problem zagrada za n brojeva $x_1x_2\ldots x_n$. Da pomnožimo te brojeve uvijek imamo jedno završno množenje prvih k brojeva $x_1, x_2, \ldots, x_k$ i zadnjih $n-k$ brojeva $x_{k+1}, \ldots, x_n$ za neko $k = 1, 2, \ldots, n-1$. Na primjer, za $n = 7$ i $k = 4$, u zagrađivanju $(x_1(x_2(x_3x_4))) \cdot ((x_5x_6)x_7)$ završno je množenje prvih 4 i zadnja 3 broja. Prvih k brojeva možemo pomnožiti na Z_k načina, a zadnjih $n-k$ brojeva na Z_{n-k} načina, pa stoga za čvrsti k čitav produkt na Z_kZ_{n-k} načina. Prema pravilu sume, kad k ide od 1 do $n-1$ dobivamo

$$Z_n = Z_1Z_{n-1} + Z_2Z_{n-2} + \cdots + Z_{n-2}Z_2 + Z_{n-1}Z_1,$$

odnosno s pomakom indeksa za 1

$$Z_{n+1} = Z_1Z_n + Z_2Z_{n-1} + \cdots + Z_{n-1}Z_2 + Z_nZ_1. \tag{23}$$

Rekurzija za (binarna stabla) B_n. Iz definicije binarnog stabla slijedi da je za $n \geq 1$, broj B_n binarnih stabala s n vrhova jednak broju uređenih parova (B, B')

binarnih stabala s ukupno $n-1$ vrhova, od kojih B ima, recimo, k vrhova, a B' ostalih $n-k+1$ vrhova, $k=0,1,\ldots,n-1$. Opet iz pravila produkta i sume slijedi

$$B_n = B_0B_{n-1} + B_1B_{n-2} + \cdots + B_{n-2}B_1 + B_{n-1}B_0. \tag{24}$$

Rekurzije (22), (23), (24) su iste (do na pomak u indeksu), a početni uvjeti za T_{n+2}, Z_{n+1} i B_n su također isti. Zato je $T_{n+2} = Z_{n+1} = B_n$. (Rekurzije koje izražavaju član niza pomoću svih prethodnih kao što je slučaj s (22),(23),(24) katkad zovemo "duboke rekurzije" ili "rekurzije s čitavom prethistorijom".)

$\underline{G_n = D_n}$. To slijedi odmah iz toga što svakom nizu $(i_1, i_2, \ldots, i_{2n})$ iz definicije G_n pridružimo Dyckov put s koracima redom $(1,i_1),(1,i_2),\ldots,(1,i_{2n-1}),(1,i_{2n})$. To je bijekcija, jer mu je inverz ovo: svakom koraku uspona $\nearrow$ pridružimo 1, a koraku silaska $\searrow$ pridružimo -1.

$\underline{D_n = P_n}$. Da se to vidi, treba samo okrenuti sliku Dyckovog puta za 45° tako, da os x prijeđe u os $y=x$, čime se dobije odgovarajući put u cjelobrojnoj mreži (opišite tu linearnu transformaciju).

$\underline{Z_{n+1} = G_n}$. Svakom zagrađivanju produkta $x_1 \cdot x_2 \cdot \ldots \cdot x_{n+1}$ pridružimo niz $(i_1, i_2, \ldots, i_{2n})$ ovako. Prvo, s jednim ekstra parom zagrada zatvorimo završno množenje. Na taj način imamo n parova zagrada koje odgovaraju n sukcesivnim množenjima. Sada svako množenje (tj. svaki znak "$\cdot$") zamijenimo brojem 1, a svaku desnu zagradu (tj. svaki znak ")") zamijenimo brojem -1 i sve ostale izbrišemo. Na primjer, pođimo od produkta $((x_1 \cdot x_2) \cdot (x_3 \cdot x_4)) \cdot x_5$ (tu je $n=4$). Prvo ga "završno" zagradimo: $(((x_1 \cdot x_2) \cdot (x_3 \cdot x_4)) \cdot x_5)$. Sada svuda umjesto $\cdot$ pišemo 1, a umjesto) pišemo -1: $(((x_1 1 x_2 - 1 1 (x_3 1 x_4 - 1 - 1 1 x_5 - 1$, pa izbrišemo sve osim simbola 1 i -1, nakon čega ostaje: $1\ -1\ 1\ 1\ -1\ -1\ 1\ 1\ -1$, i konačno stavimo zareze između susjeda i sve stavimo u zagradu; dobivamo $(1,-1,1,1,-1,-1,1,-1)$. Ovaj se algoritam na očit način može obrnuti, čime smo dobili bijekciju.

Time smo dokazali sve jednakosti. Kako već otprije znamo iz "principa zrcaljenja" (Primjer 45 c) iz poglavlja II) da je $P_n = C_n$, tvrdnja Propozicije slijedi. □

Evo još jednog načina da izravno izračunamo Z_{n+1}.

Primjer 29. Neka je $Z(n+1)$ broj različitih načina da se izračuna produkt od $n+1$ brojeva $x_1, x_2, \ldots, x_{n+1}$ ali u bilo kojem poretku. Odredite $Z(n+1)$ i pomoću toga Z_{n+1}. (Određivanje $Z(n+1)$ je ekvivalentno tome da se nađe koliko najviše rezultata dobivamo s neasocijativnim i nekomutativnim množenjem varijabli $x_1, \ldots, x_{n+1}$.)

Rješenje. Naći ćemo jednu "plitku" rekurziju za brojeve $Z(n+1)$. Svakome od $Z(n)$ množenja varijabli $x_1, \ldots, x_n$ varijablu x_{n+1} možemo pridodati ili kao vanjski faktor na dva načina (kao prvi ili posljednji) ili pak svakome od $n-1$ unutrašnjih množenja, x_{n+1} možemo pridodati na 4 načina (kao prvi ili drugi faktor svakome od dva množitelja). Dakle, ukupno x_{n+1} možemo pridodati svakome od $Z(n)$ množenja na $4(n-1)+2 = 4n-2 = 2(2n-1)$ načina. Stoga dobivamo

$$Z(n+1) = 2(2n-1)Z(n).$$

Očito je $Z(1)=1$, pa teleskopiranjem ove rekurzije slijedi

$$Z(n+1) = 2(2n-1)\cdot 2(2n-3)\cdot\cdots\cdot 2(2\cdot 1-1) = 2^n(2n-1)!! =$$
$$= 2^n \cdot \frac{(2n)!}{2^n \cdot n!} = n!\binom{2n}{n}.$$

Kako $Z(n+1)$ broji množenja u bilo kojem poretku varijabli, Z_{n+1} se dobije tako da se ovaj rezultat podijeli s brojem premutacija $(n+1)!$ varijabli $x_1, \ldots, x_{n+1}$. Odatle slijedi

$$Z_{n+1} = \frac{1}{n+1}\binom{2n}{n} = C_n.$$

□

Primjer 30. a) Dokažite da je broj Dyckovih ("planinskih") putova od $(0,0)$ do $(2n,0)$ s točno k vrhunaca (sljemena) jednak tzv. **Narayaninom broju**

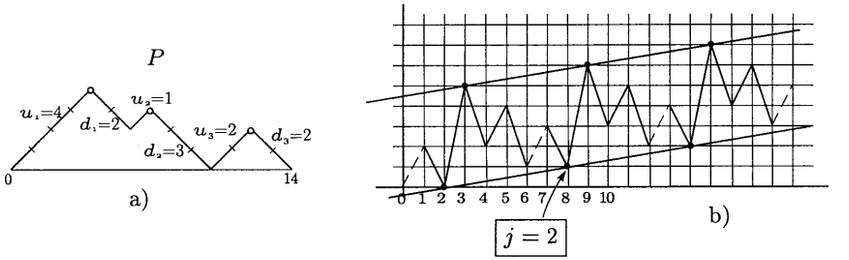
$$N(n,k) = \frac{1}{n}\binom{n}{k}\binom{n}{k-1} = \frac{1}{k}\binom{n}{k-1}\binom{n-1}{k-1}.$$

b) Dokažite da je suma Narayaninih brojeva jednaka Catalanovom broju. Točnije, dokažite

$$\sum_{k=1}^{n} N(n,k) = C_n = \frac{1}{n+1}\binom{2n}{n}.$$

Rješenje. a) Neka je $\mathcal{D}_{n,k}$ skup svih Dyckovih putova kao u a). Nadalje, označimo s $\mathcal{C}_{n,k}$ skup svih rastava (ili kompozicija) broja n u k dijelova. Prema Propoziciji 9 u poglavlju II imamo da je $\#\mathcal{C}_{n,k} = \binom{n-1}{k-1}$, $\#\mathcal{C}_{n+1,k} = \binom{n}{k-1}$. Da dokažemo formulu $kN(n,k) = \binom{n}{k-1}\binom{n-1}{k-1}$, konstruirat ćemo bijekciju $[k] \times \mathcal{D}_{n,k} \to \mathcal{C}_{n+1,k} \times \mathcal{C}_{n,k}$.

Prvo, svaki Dyckov put $P \in \mathcal{D}_{n,k}$ je potpuno određen nizom prirodnih brojeva $(u_1, d_1, u_2, d_2, \ldots, u_k, d_k)$, gdje je u_1 broj koraka prvog uspona od P, d_1 broj koraka prvog spusta, u_2 broj koraka drugog uspona itd. (možemo zamisliti da je svaki korak uspona $+1$, a korak spusta -1). Pri tome vrijedi (kao što svaki planinar znade): $u_1 \geq d_1$, $u_1 + u_2 \geq d_1 + d_2$, $\ldots, u_1 + \cdots + u_{k-1} \geq d_1 + \cdots + d_{k-1}$, a $u_1 + \cdots + u_k = d_1 + \ldots d_k = n$. Dakle, nizovi $u = (u_1, \ldots, u_k)$ i $d = (d_1, \ldots, d_k)$ su rastavi od n u k dijelova i sve parcijalne sume od u su $\geq$ od pripadnih parcijalnih suma od d. Kažemo da tada u **n-dominira** nad d i pišemo $u \succeq_n d$. Prema tome, svaki Dyckov put $P \in \mathcal{D}_{n,k}$ možemo poistovjetiti s uređenim parom $P = (u,d)$, gdje je $u \succeq_n d$ (simbole u i d čitaj "up's" i "down's"). Tako je npr. za $n=7$, $k=3$ put $P = ((4,1,2),(2,3,2))$ na sl. a).



Sada nam treba sljedeća činjenica poznata kao **Raneyeva lema**.

LEMA 1 (G. Raney, 1960.). *Neka je $(x_1, x_2, \ldots, x_m)$ bilo koji niz cijelih brojeva, takav da je suma svih članova 1. Tada među svim cikličkim pomacima toga niza*

$$(x_1, x_2, \ldots, x_m), (x_2, \ldots, x_m, x_1), \ldots, (x_m, x_1, \ldots, x_{m-1})$$

postoji točno jedan čije su sve parcijalne sume pozitivne. Drugim riječima, postoji jedinstveni j, $1 \leq j \leq m$, takav da su sve parcijalne sume niza $(x_j, x_{j+1}, \ldots, x_m, x_1, \ldots, x_{j-1})$ pozitivne.

Dokaz ove leme ćemo izvesti malo poslije. Sada želimo definirati preslikavanje $\varphi : \mathcal{C}_{n+1,k} \times \mathcal{C}_{n,k} \to [k] \times \mathcal{D}_{n,k}$. Neka je $(A, B) \in \mathcal{C}_{n+1,k} \times \mathcal{C}_{n,k}$, gdje je $A = (a_1, \ldots, a_k)$ rastav od $n+1$, a $B = (b_1, \ldots, b_k)$ rastav od n. Primijenimo Raneyevu lemu na niz $(a_1, -b_1, a_2, -b_2, \ldots, a_k, -b_k)$, jer mu je suma svih članova jednaka 1. Prema toj lemi postoji jedinstveni $j \in [k]$ takav da su sve parcijalne sume niza $(a_j, -b_j, a_{j+1}, -b_{j+1}, \ldots, a_{j-1}, -b_{j-1})$ pozitivne i $a_j \geq 2$, odnosno sve parcijalne sume niza $(a_j - 1, -b_j, a_{j+1}, -b_{j+1}, \ldots, a_{j-1}, -b_{j-1})$ su ≥ 0. Stavimo $u_1 = a_j - 1$, $u_2 = a_{j+1}$, $\ldots$, $u_k = a_{j-1}$, te $d_1 = b_j$, $d_2 = b_{j+1}$, $\ldots$, $d_k = b_{j-1}$, i $u = (u_1, \ldots, u_k)$, $d = (d_1, \ldots, d_k)$, čime smo dobili Dyckov put $P = (u, d) \in \mathcal{D}_{n,k}$. Definiramo $\varphi(A, B) = (j, P)$. Inverzno preslikavanje $\psi : [k] \times \mathcal{D}_{n,k} \to \mathcal{C}_{n+1,k} \times \mathcal{C}_{n,k}$ je ovo. Neka je $j \in [k]$ i $P = (u, d) \in \mathcal{D}_{n,k}$. Tada je $\psi(j, P) = (A, B)$, gdje su $A = (a_1, \ldots, a_k)$, $B = (b_1, \ldots, b_k)$ definirani ciklički s $a_j = u_1 + 1, a_{j+1} = u_2, \ldots, a_{j-1} = u_k$, te $b_j = d_1$, $b_{j+1} = d_2$, $\ldots, b_{j-1} = d_k$. Sada se lako vidi da je $\varphi\psi = \mathrm{id}$, $\psi\varphi = \mathrm{id}$, pa imamo bijekciju $[k] \times \mathcal{D}_{n,k} \longleftrightarrow \mathcal{C}_{n+1,k} \times \mathcal{C}_{n,k}$, čime je "planinarski" dokaz gotov. U primjeru na slici a), pridružujemo $\psi : (2, P) \mapsto (A, B)$, gdje je $A = (2, 5, 1)$, $B = (2, 2, 3)$.

Dokaz Raneyeve leme. Niz $(x_1, x_2, \ldots, x_m)$ produžimo periodički tako da dobijemo beskonačni niz $(x_1, x_2, \ldots, x_m, x_1, x_2, \ldots, x_m, x_1, x_2, \ldots)$, pri čemu je $x_{m+k} = x_k$ za sve $k \geq 0$. U koordinatnoj ravnini nacrtajmo sve parcijalne sume $s_n = x_1 + x_2 + \ldots x_n$ kao funkciju od n i tako dobivene susjedne točke (n, s_n) spojimo dužinama. Tada čitav "graf" te funkcije $n \mapsto s_n$ "titra" između dvaju paralelnih pravaca s koeficijentima smjera $1/m$, jer je $s_{m+n} = s_n + 1$. Na primjer, uzmimo $m = 6$ i niz $(2, -2, 5, -2, 1, -3)$ (to su brojevi iz gornjeg primjera $A = (2, 5, 1)$, $B = (2, 2, 3)$). Tada je na sl. b) prikazan "graf parcijalnih suma". Svaki od ovih dvaju pravaca dodiruje graf točno jedanput u svakom ciklusu od m točaka, jer pravac s nagibom $1/m$ prolazi cjelobrojnim točkama samo jedanput u m jedinica. Prva donja točka presjeka s pozitivnim koordinatama je točno ono mjesto u ciklusu od kojega su nadalje sve parcijalne sume pozitivne, jer ostale točke presjeka imaju samo veće koordinate. U našem je primjeru traženi broj $j = 2$ (vidi prethodnu sl. b). □

b) Prema Propoziciji 6 znamo da svih Dyckovih putova od $(0, 0)$ do $(2n, 0)$ ima C_n. Svaki Dyckov put ima k vrhunaca za neko k, $1 \leq k \leq n$, pa stoga slijedi tvrdnja b).

Uočite da smo (kombinatorno) dokazali i ovaj identitet

$$\sum_{k=0}^{n} N(n+1, k+1) = C_{n+1} = \sum_{k=0}^{n} C_k C_{n-k},$$

jer za Catalanove brojeve vrijedi rekurzija desne jednakosti. □

Lako je provjeriti da za Narayanine brojeve vrijedi

$$N(n+1, k+1) = \binom{n}{k}^2 - \binom{n}{k-1}\binom{n}{k+1},$$

pa kako je $N(n+1, k+1) \geq 0$ (jer ima kombinatorno značenje), slijedi (još jednom) log-konkavnost binomnih koeficijenata. Možemo stoga reći da Narayanini brojevi mjere log-konkavnost binomnih koeficijenata.

Za računanje Narayaninih brojeva najpogodnija je rekurzija

$$N(n+1, k+1) = \frac{n(n+1)}{k(k+1)} N(n, k) = \frac{\binom{n+1}{2}}{\binom{k+1}{2}} N(n, k)$$

uz početne uvjete $N(n, 1) = 1$, za sve $n \in \mathbb{N}$. To možemo tumačiti kao zakon apsorpcije za Narayanine brojeve.

Mi ćemo se još vratiti na Catalanove brojeve i uopće na rekurzije kad upoznamo funkcije izvodnice. Vidjet ćemo da funkcije izvodnice gotovo automatski rješavaju mnoge rekurzije.

Spomenimo da je u knjizi [65*] navedeno blizu 70 (naoko) različitih kombinatornih interpretacija Catalanovih brojeva i još 10-ak poopćenja. Primjerice,

$$r\text{-ti } \textbf{poopćeni Catalanov broj}: \quad C_n^{(r)} := \frac{1}{(r-1)n+1}\binom{rn}{n},$$

koji se za $r = 2$ podudara s običnim Catalanovim brojem C_n,

$$q\textbf{-analogon Catalanovog broja}: C_n^{(q)} = \frac{1}{(n+1)_q}\binom{2n}{n}_q \text{ itd.}$$

Dakle, prava pošast (koja ne dolazi iz Catalonije) nazvana "Catalomanija" (a što bi onda bila "Croatomanija"?).

§ 5. Dvoindeksne rekurzije i invertiranje polinomskih nizova i rekurzija

To su rekurzije za nizove $(a_{n,k})_{n,k \geq 0}$ koji ovise o dvama cijelim parametrima $n, k \geq 0$. Ne upuštajući se u detaljnu analizu, spomenimo neke takve jednostavne rekurzije i njihova rješenja koja znamo iz poglavlja II. Na primjer, rekurzije

$$a_{n,k} = a_{n-1,k-1} + a_{n-1,k} \quad ; \quad a_{n,k} = \frac{n}{k} a_{n-1,k-1},$$

$$a_{n+1,k+1} = \sum_{l=k}^{m} a_{l,k} \quad ; \quad a_{n-1,k} = \sum_{j=0}^{k} (-1)^{k-j} a_{n,j}$$

su zadovoljene za $a_{n,k} = \binom{n}{k}$, dok kombinacije s ponavljanjem $b_{n,k} = \binom{n+k-1}{k}$ zadovoljavaju rekurzije:

$b_{n,k} = b_{n,k-1} + b_{n-1,k}$; $\quad b_{n,k} = \frac{n}{k} b_{n+1,k-1}$; $b_{n+1,k} = \sum_{j=0}^{k} b_{n,j}$.

Stirlingovi brojevi II vrste zadovoljavaju rekurziju $s_{n,k} = s_{n-1,k-1} + k s_{n-1,k}$, a Stirlingovi brojevi I vrste rekurziju $c_{n,k} = c_{n-1,k-1} + (n-1)c_{n-1,k}$, dok Eulerovi brojevi zadovoljavaju $e_{n,k} = (k+1)e_{n-1,k} + (n-k)e_{n-1,k-1}$.

Sve ove rekurzije su bile algebarske posljedice izvjesnih polinomskih jednakosti (a mi smo ih dokazali i algebarski i kombinatorno). Na primjer, za brojeve $S(n,k)$ smo dokazali $x^n = \sum_{k=0}^{n} S(n,k)x^{\underline{k}}$, ((26) u pogl. II) što smo tumačili i kao prijelaz iz baze $\{1, x^{\underline{1}}, x^{\underline{2}}, \dots\}$ u bazu $\{1, x, x^2, \dots\}$ ∞-dimenzionalnog vektorskog prostora polinoma $\mathbb{R}[x]$ nad poljem $\mathbb{R}$. Iz te relacije (algebarski) možemo dobiti rekurziju (25) u pogl. II tako da $x^{\underline{k}}$ razvijemo po bazi $\{1, x, x^2, \dots\}$ i izjednačimo odgovarajuće koeficijente.

S druge strane, rekurziju (27') algebarski možemo izvesti iz (29) u poglavlju II, tako da bazu (x^k) razvijemo po bazi $(x^{\underline{k}})$. Iz tih dvaju postupaka zaključujemo (i to smo učinili, v. Korolar 6 pogl. II) da su matrice prijelaza jedna drugoj inverzne. Stoga su i odgovarajuće rekurzije jedna drugoj inverzne.

Sada to učinimo i općenito. Niz polinoma $(p_n(x))_{n\geq 0}$, $p_n(x) \in \mathbb{R}[x]$, takvih da je stupanj $\operatorname{st} p_n = n$, $\forall n \in \mathbb{N}_0$, očito čini bazu prostora $\mathbb{R}[x]$ (podsjetimo se da je stupanj polinoma p_0 jednak $0 \iff$ je $p_0(x) = a \neq 0$, a stupanj nul-polinoma jednak -1). Neka su $(p_n(x))_{n\geq 0}$ i $(q_n(x))_{n\geq 0}$ dva takva niza polinoma. Ako članove jedne baze napišemo u terminima druge baze, onda su matrice prijelaza jedna drugoj inverzne. Stoga vrijedi sljedeće.

PROPOZICIJA 7. *Neka su $(p_n(x))_{n\geq 0}$ i $(q_n(x))_{n\geq 0}$, dva niza polinoma koji čine bazu prostora polinoma $\mathbb{R}[x]$ i neka su koeficijenti prijelaza nizovi brojeva $(a_{n,k})$, odnosno $(b_{n,k})$, tj.*

$$q_n(x) = \sum_{k=0}^{n} a_{n,k}p_n(x), \qquad p_n(x) = \sum_{k=0}^{n} b_{n,k}q_k(x). \tag{25}$$

Tada za niz realnih brojeva $(u_n)_{n\geq 0}$ i $(v_n)_{n\geq 0}$ vrijedi $(\forall n \in \mathbb{N}_0)$:

$$v_n = \sum_{k=0}^{n} a_{n,k}u_k \iff u_n = \sum_{k=0}^{n} b_{n,k}v_k. \tag{26}$$

Dokaz. Stavimo li $a_{n,k} = b_{n,k} = 0$ za sve $n < k$, onda iz (25) slijedi da su matrice $A = [a_{n,k}]$ i $B = [b_{n,k}]$ prijelaza (tj. odgovarajući linearni operatori) međusobno inverzni. To onda znači da za sve vektore $u = (u_0, u_1, \dots)$, $v = (v_0, v_1, \dots)$ vrijedi

$$v = Au \iff u = Bv,$$

što je upravo (26) □

Odavde neposredno dobivamo

PROPOZICIJA 8. *Neka su $u = (u_n)_{n\geq 0}$ i $v = (v_n)_{n\geq 0}$ dva niza realnih brojeva. Tada vrijedi*

a) $v_n = \sum_{k=0}^{n} \binom{n}{k} u_k (\forall n \in \mathbb{N}_0) \iff u_n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} v_k (\forall n \in \mathbb{N}_0)$
(binomna inverzija);

b) $v_n = \sum_{k=0}^{n} s_{n,k}u_k \ (\forall n \in \mathbb{N}_0) \iff u_n = \sum_{k=0}^{n} S(n,k)v_k \ (\forall n \in \mathbb{N}_0)$
(Stirlingova inverzija);

c) $v_n = \sum_{k=0}^{n} \binom{n}{k}_q u_k (\forall n \in \mathbb{N}_0) \iff u_n = \sum_{k=0}^{n} (-1)^{n-k} q^{\binom{n-k}{2}} \binom{n}{k}_q v_k (\forall n \in \mathbb{N}_0)$
(Gaussova ili q-binomna inverzija).

Dokaz. a) Iz binomnog teorema imamo:

$$x^n = \sum_{k=0}^{n} \binom{n}{k} (x-1)^k, \qquad (x-1)^n = \sum_{k=0}^{n} (-1)^{n-k} \binom{n}{k} x^k.$$

Stoga su $a_{n,k} = \binom{n}{k}$ i $b_{n,k} = (-1)^{n-k}\binom{n}{k}$ koeficijenti prijelaza između dviju baza $x^n, n \geq 0$ i $(x-1)^n$, $n \geq 0$. Stoga tvrdnja slijedi iz Propozicije 7.

b) Slično kao a), tvrdnja slijedi iz formula (26) i (29) u poglavlju II.

c) Slijedi slično iz q-binomnog teorema (pronađite ga u poglavlju II. i izvedite to). □

Primjer 31. Dokažite da za Stirlingove brojeve II vrste vrijedi ova eksplicitna formula pomoću binomnih koeficijenata, faktorijela i potencija:

$$S(n,k) = \frac{1}{k!} \sum_{i=0}^{n} (-1)^{k-i} \binom{k}{i} i^n. \tag{27}$$

Rješenje. Iz formule (26) u poglavlju II. za $x = k$ i čvrsto n imamo

$$k^n = \sum_{i=0}^{n} \binom{k}{i} (i!S(n,i)).$$

Odavde iz Propozicije 8a) slijedi

$$k!S(n,k) = \sum_{i=0}^{n} (-1)^{k-i} \binom{k}{i} i^n,$$

a to je upravo (27). Na drugi ćemo način (27) dokazati pomoću formule uključivanja-isključivanja, usp. formula (6), pogl. IV. □

IV. Formula uključivanja-isključivanja i Möbiusova formula inverzije

§ 1. Formula uključivanja-isključivanja

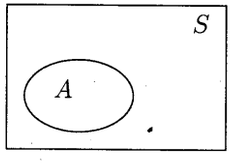
Nastavljamo s "umjetnošću prebrojavanja". Da odredimo broj elemenata $|A|$ nekog podskupa $A \subseteq S$ u konačnom skupu S, katkad je lakše izračunati $|\overline{A}|$, tj. veličinu komplementa $\overline{A} = S \setminus A$. Tada je $|A| = |S| - |\overline{A}|$. Ako imamo dva skupa $A, B \subseteq S$, onda iz de Morganove formule $\overline{A} \cap \overline{B} = \overline{A \cup B}$ slijedi $|\overline{A} \cap \overline{B}| = |S| - |A \cup B|$, a zbog $|A \cup B| = |A| + |B| - |A \cap B|$ slijedi $|\overline{A} \cap \overline{B}| = |\overline{A \cup B}| = |S| - |A| - |B| + |A \cap B|$. Slično je i s tri podskupa $A, B, C \subseteq S$ (izvedite to):

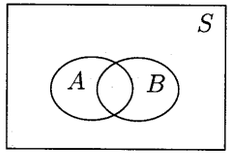
$$|\overline{A} \cap \overline{B} \cap \overline{C}| = |S| - (|A| + |B| + |C|) + (|A \cap B| + |B \cap C| + |C \cap A|) - |A \cap B \cap C|,$$

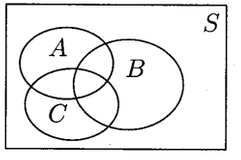
ili ekvivalentno (zbog de Morganove formule):

$$|A \cup B \cup C| = |A| + |B| + |C| - (|A \cap B| + |B \cap C| + |C \cap A|) + |A \cap B \cap C|.$$

Te formule možemo i grafički predočiti Vennovim dijagramima:







i izreći riječima: da odredimo veličinu unije triju skupova, prvo zbrojimo veličine tih skupova, pa oduzmemo veličine presjeka po dva od njih i na kraju dodamo veličinu presjeka svih triju.

Pokazat ćemo da slično vrijedi i za više skupova, ali prvo neki primjeri.

Primjer 1. U nekom razredu od 30 učenika, 10 ih voli matematiku[1], 14 fiziku, 13 kemiju, 5 učenika vole i matematiku i fiziku, 7 i fiziku i kemiju, 4 i matematiku i kemiju, a 3 vole sva tri predmeta. Koliko učenika ne voli ni jedan od tih triju predmeta?

Rješenje. Neka nam M, F, K znače skupove učenika u tom razredu koji redom vole matematiku, fiziku i kemiju, a $\overline{M}$, $\overline{F}$, $\overline{K}$ njihove komplemente. Mi tražimo broj $|\overline{M} \cap \overline{F} \cap \overline{K}|$. Iz gornje formule dobivamo $|\overline{M} \cap \overline{F} \cap \overline{K}| = 30 - (10 + 14 + 13) + (5 + 7 + 4) - 3 = 6$. □

[1] To je 30%. Odveć optimistično, hm?

Primjer 2. Koliko ima (prirodnih) brojeva do milijun koji nisu djeljivi ni s 2 ni s 3 ni s 5?

Rješenje. Neka je $S = [10^6]$, a $A_k \subseteq S$ skup svih brojeva iz S koji su djeljivi s k. Želimo izračunati $|\overline{A_2} \cap \overline{A_3} \cap \overline{A_5}|$. Prvo općenito, ako je $A_k \subseteq S$, gdje je $S = [n]$, skup brojeva djeljivih s k, onda su elementi iz A_k višekratnici broja k, tj. k, $2k$, $3k$,...,ak, gdje je a najveći broj takav da je $ak \leq n$. Stoga je $a = \lfloor n/k \rfloor$ i, dakle, $|A_k| = \lfloor n/k \rfloor$. Nadalje, ako su k i l relativno prosti, onda je očito $A_k \cap A_l = A_{kl}$. Stoga uvrštavanjem iz gornje formule dobivamo $|\overline{A_2} \cap \overline{A_3} \cap \overline{A_5}| = 166\,666$. □

Dakle, nakon što smo u Primjeru 2 uklonili sve višekratnike od 2, 3 i 5, ostalo nam je 166 666 brojeva. Ova se metoda naziva **Eratostenovo sito**, i po njoj se to katkad zove "**metoda sita**". Naime, da nađemo veličinu nekog skupa, mi najprije iz velikog skupa izbacimo sve "sumnjive" elemente, pa vratimo kandidate za "dobre" elemente, pa među njima opet izbacimo "sumnjive" itd. Dakle, elementi skupa su zaista prošli kroz "sito i rešeto".

Dokažimo sada i opći teorem.

TEOREM 1 (Formula uključivanja-isključivanja[2], ili kratko FUI). *Neka je S konačan skup, a $A_1, A_2, \ldots, A_n \subseteq S$. Tada vrijede formule:*

$$\begin{aligned} |\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}| = |S| - \sum |A_i| + \sum |A_i \cap A_j| - \\ - \sum |A_i \cap A_j \cap A_k| + \cdots + (-1)^n |A_1 \cap \cdots \cap A_n|, \end{aligned} \tag{1}$$

$$\begin{aligned} |A_1 \cup A_2 \cup \cdots \cup A_n| = \sum |A_i| - \sum |A_i \cap A_j| + \\ + \sum |A_i \cap A_j \cap A_k| - \cdots + (-1)^{n+1} |A_1 \cap \cdots \cap A_n|. \end{aligned} \tag{2}$$

Prije nego što dokažemo teorem, uočimo da su formule (1) i (2) ekvivalentne, što odmah slijedi iz de Morganovih formula: komplement unije je presjek komplementa, a komplement presjeka je unija komplemenata.

Nadalje, formule (1) i (2) se konciznije i preglednije mogu zapisati ovako. Za svaki podskup indeksa $I = \{i_1, i_2, \ldots, i_k\} \subseteq [n]$, neka je $A_I := A_{i_1} \cap A_{i_2} \cap \cdots \cap A_{i_k} = \bigcap_{i \in I} A_i$, $A_\emptyset = \bigcap_{i \in \emptyset} = S$, $\bigcup_{i \in \emptyset} A_i = \emptyset$. Tada se (1) i (2) mogu zapisati ovako:

$$\left| \bigcap_{i=1}^{n} \overline{A_i} \right| = \sum_{I \subseteq [n]} (-1)^{|I|} |A_I|, \tag{1'}$$

$$\left| \bigcup_{i=1}^{n} \overline{A_i} \right| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|-1} |A_I|. \tag{2'}$$

Dokazat ćemo formulu (2) (odnosno (2')) na dva načina i formulu (1') na jedan način.

[2] Prvi je tu formulu jasno formulirao i dokazao oko 1870. godine englesko-američki matematičar James J. Sylvester (1814 – 1897).

Dokaz I. Indukcijom po n. Za $n = 1$, formula (2) je trivijalna, a za $n = 2$ to je (za $A_1 = A$, $A_2 = B$) već poznata formula

$$|A \cup B| = |A| + |B| - |A \cap B|. \qquad (*)$$

Pretpostavimo da (2) vrijedi za n i dokažimo da vrijedi za $n+1$. Primijenimo $(*)$ za $A = \bigcup_{i=1}^{n} A_i$ i $B = A_{n+1}$, pa imamo

$$\Big|\bigcup_{i=1}^{n+1} A_i\Big| = \Big|\bigcup_{i=1}^{n} A_i\Big| + |A_{n+1}| - \Big|\Big(\bigcup_{i=1}^{n} A_i\Big) \cap A_{n+1}\Big| =$$

$$= |A_{n+1}| + \Big|\bigcup_{i=1}^{n} A_i\Big| - \Big|\bigcup_{i=1}^{n} (A_i \cap A_{n+1})\Big|.$$

Sada primijenimo pretpostavku indukcije na posljednja dva člana uz oznake $A_i' = A_i \cap A_{n+1}$, te $A_I' = A_I \cap A_{n+1}$. Tada je

$$\Big|\bigcup_{i=1}^{n} A_i\Big| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|-1} |A_I|,$$

$$\Big|\bigcup_{i=1}^{n} A_i'\Big| = \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|-1} |A_I'| = \sum_{\substack{n+1 \in J \subseteq [n+1] \\ |J| \geq 2}} (-1)^{|J|} |A_J|.$$

Stoga uvrštavanjem dobivamo

$$\Big|\bigcup_{i=1}^{n+1} A_i\Big| = |A_{n+1}| + \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|-1} |A_I| + \sum_{\substack{n+1 \in J \subseteq [n+1] \\ |J| \geq 2}} (-1)^{|J|-1} |A_J| =$$

$$= \sum_{\emptyset \neq I \subseteq [n]} (-1)^{|I|-1} |A_I| + \sum_{n+1 \in J \subseteq [n+1]} (-1)^{|J|-1} |A_J| =$$

$$= \sum_{\emptyset \neq K \subseteq [n+1]} (-1)^{|K|-1} |A_K|.$$

□

Dokaz II (kombinatorni). Promotrit ćemo broj pojava bilo kojeg elementa $x \in \bigcup_{i=1}^{n} A_i$. Na lijevoj strani u (2), element x koji se nalazi u nekom A_i broji se jedanput. Pokažimo da se i na desnoj strani broji samo jedanput. Ako se x pojavljuje u točno k A_i-ova, onda se on točno k puta pojavljuje u $\sum |A_i|$, točno $\binom{k}{2}$ puta u $\sum |A_i \cap A_j|$ i općenito točno $\binom{k}{t}$ puta u $\sum |A_{i_1} \cap \cdots \cap A_{i_t}|$, pri čemu t ide od 1 do k. Stoga se na desnoj strani od (2) element x pojavljuje točno

$$\binom{k}{1} - \binom{k}{2} + \cdots + (-1)^{t-1}\binom{k}{t} + \cdots + (-1)^{k-1}\binom{k}{k}$$

puta. No, ova suma je jednaka 1 (usp. pogl. II, formula (6)). □

Dokaz III (algebarski). Nakon svih množenja (tj. kad se "riješimo zagrada") vidimo da vrijedi sljedeći identitet (a dokaz ide lako indukcijom po n):

$$(1 + x_1)(1 + x_2) \cdot \cdots \cdot (1 + x_n) = \sum_{I \subseteq [n]} \Big(\prod_{i \in I} x_i\Big). \qquad (3)$$

Neka je $A = \bigcap_{i=1}^{n} \overline{A_i}$, $\chi_{A_i} : S \to \{0,1\}$ karakteristična funkcija podskupa A_i, a $\chi_A : A \to \{0,1\}$ karakteristična funkcija podskupa A. Uvrstimo li u (3) $x_i = -\chi_{A_i}$ dobivamo

$$\prod_{i=1}^{n} (1 - \chi_{A_i}) = \sum_{I \subseteq [n]} (-1)^{|I|} \prod_{i \in I} \chi_{A_i}.$$

S druge strane, očito je da je $\chi_{\overline{A_i}} = 1 - \chi_{A_i}$ i $\chi_{\bigcap_{i \in I} A_i} = \prod_{i \in I} \chi_{A_i}$. Prema tome je

$$\chi_A = \prod_{i=1}^{n} \chi_{\overline{A_i}} = \sum_{I \subseteq [n]} (-1)^{|I|} \chi_{\bigcap_{i \in I} A_i}.$$

Stoga su i vrijednosti u bilo kojoj točki $x \in S$ jednake. Zbrajanjem po svim $x \in S$ i rabeći očitu formulu $|B| = \sum_{x \in S} \chi_B(x)$, za svaki $B \subseteq S$, dobivamo formulu $(1')$. □

Iz dokaza III vidimo da je FUI zapravo poseban slučaj gotovo očiglednog algebarskog identiteta (3), pa bi mnogi algebričari mogli reći da je FUI zapravo trivijalna. U nekom smislu je to točno, ali je njezina važnost i ljepota ne u samoj formuli, nego u njezinoj širokoj primjenjivosti u kombinatorici, teoriji brojeva, algebri, geometriji i drugdje. Uostalom, kako može biti "lijepa" formula ako (za dano n) desna strana u (1) ima $1 + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$ sumanada? Ali i to za njezinu primjenjivost nije važno, kao što ćemo vidjeti u idućim primjenama.

PROPOZICIJA 1 (Eulerova funkcija). *Za $n \in \mathbb{N}$, Eulerova funkcija $\varphi(n)$ je broj prirodnih brojeva koji su $\leq n$, a relativno su prosti s n. Ako je $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$ kanonski rastav broja n, onda je*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \cdots \cdot \left(1 - \frac{1}{p_k}\right).$$

Dokaz. Neka je $A_i \subseteq [n]$ skup svih višekratnika od p_i, tj. $A_i = \{r \in [n] | r$ djeljivo s $p_i\}$, $i = 1, 2, \ldots, k$. Iz definicije od $\varphi(n)$ tada slijedi da je $\varphi(n) = |\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_k}|$. Stoga ćemo uporabiti (1). No prvo odredimo $|A_i|$, $|A_i \cap A_j|$ itd. Svi višekratnici od p_i u skupu $[n]$ su: $p_i, 2p_i, 3p_i, \ldots, \frac{n}{p_i} \cdot p_i = n$. Zato je $|A_i| = \frac{n}{p_i}$. Dalje, kako su p_i, p_j relativno prosti, onda na isti način slijedi da je $|A_i \cap A_j| = \frac{n}{p_i p_j}$ itd. Prema

tome, iz (1) imamo

$$\varphi(n) = n - \sum \frac{n}{p_i} + \sum \frac{n}{p_i p_j} - \cdots + (-1)^k \sum \frac{n}{p_1 p_2 \ldots p_k} =$$
$$= n\left(1 - \sum \frac{1}{p_i} + \sum \frac{1}{p_i p_j} - \cdots + (-1)^k \sum \frac{1}{p_1 p_2 \ldots p_k}\right) =$$
$$= n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

(Posljednja je jednakost zapravo identitet (3) za $x_i = -1/p_i$.) □

KOROLAR 1. *Eulerova funkcija φ je multiplikativna funkcija, tj. $\varphi(mn) = \varphi(m)\varphi(n)$ za relativno proste m i n.*

Dokaz. Naime, ako je $m = q_1^{\beta_1} \ldots q_l^{\beta_l}$ kanonski rastav od m, onda je zbog $M(m,n) = 1$, svaki p_i različit od svakog g_j, pa je kanonski rastav od $mn = p_1^{\alpha_1} \ldots p_k^{\alpha_k} q_1^{\beta_1} \ldots q_l^{\beta_l}$ i zato

$$\varphi(mn) = mn\left(1 - \frac{1}{p_1}\right) \ldots \left(1 - \frac{1}{p_k}\right)\left(1 - \frac{1}{q_1}\right) \ldots \left(1 - \frac{1}{q_l}\right) = \varphi(m)\varphi(n).$$

□

Sljedeći je problem u davna vremena (17. – 18. stoljeće) bio poznat po nazivu "**probléme des recontres**", a rješavali su ga onodobni najbolji matematičari. Kod nas je on poznat kao problem "totalne zbrke". Evo nekih zabavnih formulacija tog problema.

Na ulazu u cabaret stotinu je gospode predalo svoje šešire u garderobi do zahoda. Nakon predstave u sveopćoj navali stara rastresena i slabovidna "piš - frau" (koja je u međuvremenu i malo jače "potegnula" iz boce) vraćala im je šešire nasumce. Na koliko je načina to mogla učiniti tako da nitko ne dobije natrag svoj šešir? Priča za studente. Zamislite da ste diplomirali (možete?) i da ste s još stotinu kolega i kolegica došli na svečanu dodjelu diploma. Na koliko načina dekan (inače rastreseni profesor, kakvi već znaju biti profesori) može podijeliti diplome tako da nitko ne dobije svoju diplomu?

Ovo su posebni slučajevi problema da se nađe broj permutacija n-članog skupa (tj. bijekcija $\pi : [n] \to [n]$) bez fiksnih točaka. (Za preslikavanje $f : X \to X$, točka $x \in X$ je **fiksna** ako je $f(x) = x$.) Takve se permutacije još zovu i **deranžmani**. Broj deranžmana od $[n]$ označit ćemo s D_n. Definiramo $D_0 := 1$. Očito je $D_1 = 0$, a $D_2 = 1$ jer je jedina permutacija od $\{1,2\}$ bez fiksnih točaka 21. $D_3 = 2$, jer su 231 i 312 jedini deranžmani od $\{1,2,3\}$, $D_4 = 9$ itd.

PROPOZICIJA 2. *Broj deranžmana od n elemenata je jednak*

$$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \frac{1}{3!} + \cdots + (-1)^n \frac{1}{n!}\right). \qquad (4)$$

Dokaz. Nas zanima broj svih permutacija $\pi \in S_n$ za koje je $\pi(i) \neq i$ za sve $i \in [n]$. Neka je $S = S_n$. Za svako $i \in [n]$ neka je $A_i = \{\pi \in S_n | \pi(i) = i\}$. Tada je $D_n = |\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_n}|$. $|A_i|$ je broj permutacija od $[n]$ za koje je i fiksno, a ostalih $n-1$ elemenata slobodno permutiramo. Zato je $|A_i| = (n-1)!$. Tako je i općenito za $I = \{i_1, \ldots, i_k\} \subseteq [n]$, $|A_I| = |A_{i_1} \cap \cdots \cap A_{i_k}| = (n-k)!$. Broj k-podskupova iz $[n]$ je $\binom{n}{k}$, pa iz FUI (1′) slijedi

$$D_n = \sum_{I \subseteq [n]} (-1)^{|I|} |A_I| = \sum_{k=0}^{n} \sum_{|I|=k} (-1)^k |A_I| = \sum_{k=0}^{n} \binom{n}{k} (-1)^k (n-k)! =$$
$$= \sum_{k=0}^{n} (-1)^k \frac{n!}{k!} = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Katkad se desna strana od (4) označava simbolom $n¡$ i zove **subfaktorijel**. □

Kako je $e^{-1} = \sum_{k \geq 0} (-1)^k/k! = 0.3678794\ldots$, slijedi da je za velike n, broj deranžmana D_n približno jednak $n!e^{-1}$. Naime,

$$\left|D_n - \frac{n!}{e}\right| = n!\left|\sum_{k=0}^{n} \frac{(-1)^k}{k!} - \sum_{k=0}^{\infty} \frac{(-1)^k}{k!}\right| = n!\left|\sum_{k=n+1}^{\infty} \frac{(-1)^k}{k!}\right| =$$
$$= \frac{n!}{(n+1)!}\left|1 - \left(\frac{1}{n+2} - \frac{1}{(n+2)(n+3)} + \ldots\right)\right| < \frac{1}{n+1}.$$

Prema tome, možemo pisati

$$D_n = \left\lfloor \frac{n!}{e} + \frac{1}{2} \right\rfloor.$$

Broj $D_n/n!$ možemo interpretirati kao vjerojatnost da nasumce odabrana permutacija od $[n]$ nema fiksnih točaka. Zbog $\lim_{n\to\infty} D_n/n! = e^{-1}$, vjerojatnost da od 100 studenata na svečanoj podjeli diploma nitko ne dobije svoju diplomu (tj. da nastane totalna zbrka) je približno 0.36788. I za 500 ili 1000 studenata rezultat je približno isti.

Poopćeni "probléme de recontres" glasi ovako. Koliki je broj permutacija od n elemenata s točno k fiksnih točaka? Označimo s $D_n(k)$ taj broj, $0 \leq k \leq n$. Tada je $D_n(0) = D_n$ broj deranžmana od n elemenata. Da odredimo $D_n(k)$ uočimo da k-torku fiksnih točaka možemo izabrati na $\binom{n}{k}$ načina, a ostalih $n-k$ elemenata možemo "deranžirati" na D_{n-k} načina. Stoga je $D_n(k) = \binom{n}{k} D_{n-k}$. Iz (4) onda dobivamo

$$D_n(k) = \frac{n!}{k!} \sum_{j=}^{n-k} \frac{(-1)^j}{j!} \approx \frac{n!}{ek!}.$$

Zato je npr. vjerojatnost da od 100 studenata točno njih 10 dobije svoju diplomu jednaka $D_{100}(10)/100! \approx (10!e)^{-1}$ (vrlo mala), a da ih barem 10 dobije svoju diplomu jednaka $\sum_{k=10}^{100} D_{100}(k)/100! \approx \sum_{k=10}^{100} (ek!)^{-1}$ (malo veća).

PROPOZICIJA 3. *Broj surjekcija s n-članog na k-člani skup, $n \geq k$, dan je formulom*

$$\#\, Sur([n],[k]) = \sum_{j=0}^{k}(-1)^j \binom{k}{j}(k-j)^n. \tag{5}$$

Dokaz. Neka je S skup svih preslikavanja $[n] \to [k]$. Znamo da je $|S| = k^n$. Neka je $j \in [k]$ čvrst element iz kodomene i promotrimo skup A_j svih onih preslikavanja $f : [n] \to [k]$ koje "promaše" j, tj. kojima j nije u slici. Dakle, $A_j = \{f \in S | j \notin \operatorname{Im} f\}$, $j = 1, 2, \ldots, k$. Tada je $\overline{A_j} = \{f \in S | j \in \operatorname{Im} f\}$. Broj surjekcija je broj onih funkcija kojima su svi elementi iz kodomene u slici, pa je

$$\#\operatorname{Sur}([n],[k]) = |\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_k}|.$$

Za $J \subseteq [k]$, $|J| = j$, skup $A_J = \bigcap_{j \in J} A_j$ je skup svih funkcija $[n] \to [k] \setminus J$, a takvih je $(k-j)^n$, dok takav skup J možemo birati na $\binom{k}{j}$ načina. Iz FUI (1) tada slijedi

$$\#\operatorname{Sur}([n],[k]) = \sum_{j=0}^{k}(-1)^j \binom{k}{j}(k-j)^n.$$

□

Navedimo neke zanimljive posljedice koje potječu iz ove formule za broj surjekcija. Prvo, mi već znamo (Korolar 4 u poglavlju II) da je broj surjekcija $[n] \to [k]$ jednak $k!S(n,k)$, pa onda na još jedan način dobivamo (usp. Primjer 31 iz poglavlja III) eksplicitnu formulu za $S(n,k)$:

$$S(n,k) = \frac{1}{k!}\sum_{j=0}^{k}(-1)^j \binom{k}{j}(k-j)^n. \tag{6}$$

Dalje, kako je za $k = n$ svaka surjekcija $[n] \to [n]$ zapravo bijekcija, a za $k > n$ nema surjekcija $[n] \to [k]$, dobivamo sljedeće.

KOROLAR 2.

$$\sum_{j=0}^{k}(-1)^j \binom{k}{j}(k-j)^n = \begin{cases} k!S(n,k) & , za\ k < n, \\ n! & , za\ k = n, \\ 0 & , za\ k > n. \end{cases}$$

Nadalje, kako je svaka funkcija $[n] \to [k]$ zapravo surjekcija na neki t-člani podskup iz $[k]$, a taj možemo birati na $\binom{k}{t}$ načina, onda iz (5) slijedi

$$\sum_{t=0}^{k}\binom{k}{t}\sum_{j=0}^{t}(-1)^j \binom{t}{j}(t-j)^n = k^n.$$

I konačno, n-ti Bellov broj B_n je broj svih particija n-članog skupa, pa je $B_n = \sum_{k=0}^{n} S(n,k)$ (ili u jedan ili u dva ili, ..., ili u n blokova). Iz (6) stoga dobivamo i eksplicitnu formulu (u terminima binomnih koeficijenata) za n-ti Bellov broj:

KOROLAR 3.

$$B_n = \sum_{k=0}^{n}\frac{1}{k!}\sum_{j=}^{k}(-1)^j \binom{k}{j}(k-j)^n. \tag{7}$$

Ako u formuli (7) pišemo i umjesto $k-j$ te pustimo da k formalno ide do ∞ (što možemo, jer je $S(n,k) = 0$ za $k > n$), onda promjenom poretka sumacije dobivamo

$$B_n = \sum_{k=0}^{\infty}\frac{1}{k!}\sum_{i=0}^{k}(-1)^{k-i}\binom{k}{i}i^n = \sum_{i=0}^{\infty}\frac{i^n}{i!}\sum_{k=i}^{\infty}\frac{(-1)^{k-i}}{(k-i)!} = \frac{1}{e}\sum_{i=0}^{\infty}\frac{i^n}{i!},$$

tj. dokazali smo

KOROLAR 4. *Za n-ti Bellov broj vrijedi*

$$B_n = \frac{1}{e}\sum_{i=0}^{\infty}\frac{i^n}{i!}. \tag{8}$$

Evo i jednog sasvim konkretnog zadatka.

Primjer 3. Na koliko se načina 8 različitih predmeta može razmjestiti u 5 različitih kutija tako da nijedna kutija ne ostane prazna?

Rješenje. Traženi je broj očito jednak broju surjekcija $[8] \to [5]$, pa je odgovor $5!S(8,5)$, što bismo mogli izračunati iz tablice za $S(n,k)$-ove (vidi pogl. II) i to iznosi $5! \cdot 1050 = 126\,000$. No, iz formule (5), taj je broj također jednak

$$\sum_{j=0}^{5}(-1)^j \binom{5}{j}(5-j)^8 = 5^8 - \binom{5}{4}4^8 + \binom{5}{3}3^8 - \binom{5}{2}2^8 + \binom{5}{1} = 126\,000.$$

□

Formula uključivanja-isključivanja ima svoj prirodni analogon u teoriji vjerojatnosti. Naime, označimo s $p(x)$ vjerojatnost događaja X, s $X + Y$ događay "X ili Y (ili oba)", s $X \cdot Y$ događaj "X i Y", a $\overline{X}$ događaj "ne X". Ako su $A_1, A_2, \ldots, A_n$ događaji, onda su vjerojatnosni analogoni formula (1) i (2) ovi:

$$p(\overline{A_1} \cdot \overline{A_2} \cdot \cdots \cdot \overline{A_n}) = \sum_{j=0}^{n}(-1)^j P_j,\ p(A_1 + A_2 + \cdots + A_n) = \sum_{j=1}^{n}(-1)^{j-1}P_j,$$

gdje je $P_j = \sum_{|I|=j} p(\prod_{i \in I} A_i)$, $P_0 = 1$. Ako su događaji $A_1, A_2, \ldots, A_n$ nezavisni, onda je $p(\overline{A_1} \cdot \overline{A_2} \cdot \cdots \cdot \overline{A_n}) = \prod_{i=1}^{n}(1 - p(A_i))$.

Sada ćemo poopćiti FUI. Umjesto brojeva elemenata uzmimo bilo koju realnu funkciju na podskupovima.

TEOREM 2 (poopćeni FUI). *Neka je S konačni skup, a $f : 2^S \to \mathbb{R}$ realna funkcija definirana na podskupovima od S. Neka je $g : 2^S \to \mathbb{R}$ definirana s*

$$g(T) = \sum_{X \subseteq T} f(X),\ \forall T \subseteq S. \tag{9}$$

Tada je

$$f(T) = \sum_{X \subseteq T} (-1)^{|T-X|} g(X), \forall T \subseteq S. \tag{10}$$

(U obje formule sumira se po svim podskupovima $X \subseteq T$. Ovdje pišemo $T - X$ umjesto više uobičajenog $T \setminus X$.)

Dokaz. Skup svih funkcija $f : 2^S \to \mathbb{R}$ čini vektorski prostor V nad $\mathbb{R}$ (zbrajanje i množenje sa skalarima definirano je na očit način: $(f + f')(T) = f(T) + f'(T)$, $(\lambda f)(T) = \lambda f(T)$; $\dim V = 2^{|S|}$). Definirajmo linearni operator $\varphi : V \to V$ s

$$(\varphi f)(T) = \sum_{X \subseteq T} f(X).$$

Tvrdimo da je linearni operator $\psi : V \to V$ definiran s

$$(\psi f)(T) = \sum_{X \subseteq T} (-1)^{|T-X|} f(X),$$

inverz od φ. Pokažimo da je $\varphi\psi = 1_V$. Imamo

$$(\varphi\psi f)(T) = \sum_{X \subseteq T} (-1)^{|T-X|} \varphi f(X) = \sum_{X \subseteq T} (-1)^{|T-X|} \sum_{Z \subseteq X} f(Z) =$$

$$= \sum_{Z \subseteq T} \left(\sum_{Z \subseteq X \subseteq T} (-1)^{|T-X|} \right) f(Z).$$

Stavimo li $m = |T - Z|$, onda je za čvrste Z, T

$$\sum_{Z \subseteq X \subseteq T} (-1)^{|T-X|} = \sum_{i=0}^{m} (-1)^i \binom{m}{i} = \delta_{om},$$

pa je $\varphi\psi f(T) = f(T) \Rightarrow \varphi\psi f = f \Rightarrow \varphi\psi = 1_V$. □

Na potpuno isti način pokazuje se

$$g(T) = \sum_{X \supseteq T} f(X) \Rightarrow f(T) = \sum_{X \supseteq T} (-1)^{|X-T|} g(X). \tag{11}$$

Na S treba gledati kao na skup svojstava koje objekti (elementi) nekog konačnog skupa objekata U imaju ili nemaju. Za podskup $T \subseteq S$, označimo:

$f_=(T)$:= broj objekata iz U koji imaju točno svojstva iz T (dakle, nemaju svojstva iz $\overline{T} = S - T$);

$f_\geq(T)$:= broj objekata iz U koji imaju barem svojstva iz T (dakle, imaju sva svojstva iz T i možda još neka);

$f_\leq(T)$:= broj objekata iz U koji imaju najviše svojstva iz T (dakle, imaju samo neka svojstva iz T).

Tada očito vrijedi

$$f_\leq(T) = \sum_{X \subseteq T} f_=(X). \tag{12}$$

Iz Teorema 2 tada slijedi

$$f_=(T) = \sum_{X \subseteq T} (-1)^{|T-X|} f_\leq(X). \tag{13}$$

Isto je tako očito

$$f_\geq(T) = \sum_{X \supseteq T} f_=(X). \tag{14}$$

pa iz (11) slijedi

$$f_=(T) = \sum_{X \supseteq T} (-1)^{|T-X|} f_\geq(X). \tag{15}$$

Posebno, ako u (15) stavimo $T = \emptyset$, tj. brojimo sve objekte (iz U) koji nemaju nijedno svojstvo iz S, dobivamo

$$f_=(\emptyset) = \sum_X (-1)^{|X|} f_\geq(X) \tag{16}$$

(tu se sumira po svim podskupovima iz S), a ako u (13) stavimo $T = S$, dobivamo

$$f_=(S) = \sum_X (-1)^{|S-X|} f_\leq(X). \tag{17}$$

Važnost formula (16) i (17) je u tome što je $f_\leq(X)$ i $f_\geq(X)$ obično lakše izračunati. Formule (16) i (17) poopćuju obični FUI.

Naime, neka je U konačni skup, a $A_1, \ldots, A_n \subseteq U$, tako da je A_i skup svih elemenata iz U koji imaju neko svojstvo $i \in [n] = S$. Neka je $f_=(I)$ broj svih elemenata iz U koji imaju točno svojstva iz I, a $f_\geq(I)$ broj onih koji imaju barem svojstva iz $I \subseteq [n]$, onda (16) povlači $|\cap_{i=1}^n \overline{A_i}| = \sum_{I \subseteq [n]} (-1)^{|I|} |A_I|$, tj. (1′). Iz (16) i (17) neposredno slijedi i ovo.

KOROLAR 5. *Neka je S konačan skup, $A_1, \ldots, A_n \subseteq S$, a za $0 \leq k \leq n$, $S_k = \sum_{|I|=k} |A_I|$, $S_0 = |S|$, a $f_=(k)$ (odn. $f_\geq(k)$) broj elemenata iz S koji su u točno k (odn. barem k) podskupova A_i. Tada je:*

$$f_=(k) = \sum_{t=k}^{n} (-1)^{t-k} \binom{t}{k} S_t \tag{18}$$

$$f_\geq(k) = \sum_{t=k}^{n} (-1)^{t-k} \binom{t-1}{k-1} S_t \tag{19}$$

(za $k = 0$, (18) je (1), a za $k = 1$, (19) je (2)).

S običnom (ili poopćenom) FUI sada možemo izračunati i broj r-kombinacija konačnog multiskupa. Neka je $M = \{x_1^{n_1}, \ldots, x_k^{n_k}\}$ multiskup nad skupom $B = \{x_1, \ldots, x_k\}$, a kratnost od x_i jednaka n_i, $i = 1, \ldots, k$. Broj svih r-kombinacija od M označavamo s $\left(\!\binom{n_1,\ldots,n_k}{r}\!\right)$. Tada vrijedi sljedeće.

PROPOZICIJA 4 (MacMahon[3]).

$$\left(\!\binom{n_1, n_2, \ldots, n_k}{r}\!\right) = \sum_{t=0}^{k} (-1)^t \sum \binom{k + r - n_{i_1} - \cdots - n_{i_t} - t - 1}{k - 1}, \qquad (20)$$

gdje se unutrašnja sumacija vrši po svim $0 \leq i_1 < \cdots < i_t \leq k$.

Dokaz. Neka je S skup svih r-kombinacija s ponavljanjem skupa $B = \{x_1, \ldots, x_k\}$. Znamo da je $|S| = \binom{k+r-1}{k-1}$ (Propozicija 10 u poglavlju II), a za $i = 1, 2, \ldots, k$ neka je A_k skup svih onih r-kombinacija s ponavljanjem od B kod kojih se x_i javlja barem $n_i + 1$ puta. Ako od svake r-kombinacije u A_i odstranimo $n_i + 1$ x_i-ova ostaje nam $[r - (n_i + 1)]$-kombinacija s ponavljanjem skupa B. Obratno, ako svakoj $[r - (n_i + 1)]$-kombinaciji s ponavljanjem od B dodamo $n_i + 1$ x_i-ova, dobivamo r-kombinaciju s ponavljanjem u B u kojoj je barem $n_i + 1$ x_i-ova. Stoga je $|A_i| =$ broj $[r - (n_i + 1)]$-kombinacija s ponavljanjem od B, pa je $|A_i| = \binom{k+r-(n_i+1)-1}{k-1}$. Slično se izračunaju i svi $|A_{i_1} \cap \cdots \cap A_{i_t}|$, pa (20) slijedi iz FUI. (Pokušajte je izvesti iz poopćene FUI.) □

Stavimo li u (20) $n_1 = n_2 = \cdots = n_k = 1$, dobivamo r-kombinacije skupa $B = \{x_1, \ldots, x_k\}$, a njih ima $\binom{k}{r}$. Stoga kao posljedicu dobivamo identitet

$$\binom{k}{r} = \sum_{t=0}^{k} (-1)^t \binom{k}{t} \binom{k + r - 2t - 1}{k - 1}. \qquad (21)$$

Primjer 4. a) Koliko rješenja ima jednadžba $x_1 + x_2 + \cdots + x_k = r$ u skupu $\mathbb{N}_0^k$, tako da je $0 \leq x_i \leq n_i$, $i = 1, 2, \ldots, k$?

b) Koliko ima cjelobrojnih trojki (x, y, z), za koje je $x + y + z = 14$, a $0 \leq x \leq 8$, $0 \leq y \leq 7$, $0 \leq z \leq 6$?

Rješenje. a) Očito je odgovor dan formulom (20).

b) Tu je $r = 14$, $k = 3$, $n_1 = 8$, $n_2 = 7$, $n_3 = 6$, pa uvrštavanjem u (20) dobivamo da je traženi broj 35.

□

Primjer 5. a) Koliki je broj načina da se n_1 darova prve vrste, n_2 darova druge vrste, $\ldots, n_k$ darova k-te vrste razdijeli među r djece, tako da svako dijete dobije bar jedan dar?

b) Na koliko načina Djed Božićnjak može među četvero djece razdijeliti tri vrste darova: 7 autića, 8 lutaka i 10 čokolada ako svako dijete (svi su bili dobri!) mora dobiti bar jedan dar?

[3]Percy Alexander MacMahon (1854 – 1929), engleski matematičar; dugo je vremena proveo kao bojnik (major) u britanskoj okupacijskoj vojsci u Indiji.

Rješenje. a) Prema Primjeru 36 u poglavlju II, znamo da je broj načina da se svi darovi razdijele među t djece jednak $N_t = \prod_{j=1}^{k} \binom{n_j+t-1}{t-1}$. Neka je A_i skup svih razdioba među r-djece tako da i-to dijete ne dobije nijedan predmet. Traženi je broj jednak $|\overline{A_1} \cap \overline{A_2} \cap \cdots \cap \overline{A_r}|$. Očito je $|A_i| = N_{r-1}$, $A_i \cap A_j| = N_{r-2}$, itd., općenito $|A_I| = N_{r-t}$, gdje je $I \subseteq [r]$, $|I| = t$. Takvih podskupova I ima $\binom{r}{i}$, pa je traženi broj jednak

$$\sum_{t=0}^{r} (-1)^{r-t} \binom{r}{t} N_t.$$

(Uočite da je to isto kao i broj rješenja $(x_1, \ldots, x_k) \in \mathbb{N}^k$ jednadžbe $x_1 + \cdots + x_k = r$, tako da je $1 \leq x_i \leq n_i$, $i = 1, \ldots, k$.)

b) Tu je $r = 4$, $k = 3$, $n_1 = 7$, $n_2 = 8$, $n_3 = 10$, pa se dobije da je traženi broj (iznenađujuće velik) 5 239 868.

□

Kao daljnju primjenu poopćene FUI promotrit ćemo **problem permutacija sa zabranjenim pozicijama**. Naime, u problemu deranžmana (Propozicija 2) problem je bio izračunati broj permutacija $\pi \in S_n$ za koje je $\pi(i) \neq i$ za svako i, dakle gdje $\pi(i)$ ima neku zabranjenu poziciju. Sada ćemo to poopćiti.

Tu je zgodno (i vizualno) stvari opisati pomoću "šahovske ploče" ("šahovnice") veličine $n \times n$. Neka je $P \subseteq [n] \times [n]$ "krnja šahovska ploča", što ćemo kratko zvati **ploča**, i za svaku permutaciju $\pi \in S_n$ neka je **graf permutacije** π podskup $G(\pi) = \{(i, \pi(i)) | i \in [n]\} \subseteq [n] \times [n]$. Permutaciju $\pi \in S_n$ možemo zamišljati kao stavljanje n topova (kula) na šahovsku ploču $n \times n$ na pozicije $(i, \pi(i))$ tako da se nikoje dvije ne napadaju (tj. nikoje dvije nisu u istom retku ni u istom stupcu). Za zadanu ploču P ("zabrane") definirajmo za $0 \leq j, k \leq n$ brojeve

P_j = broj permutacija $\pi \in S_n$ za koje je $\#(P \cap G(\pi)) = j$;

t_k = broj k-podskupova od P čija svaka dva elementa imaju obje koordinate različite

= broj načina da se na P stavi k topova koji se ne napadaju.

Dakle, P_j je broj načina da se na čitavu ploču $[n] \times [n]$ stavi n topova koji se ne napadaju, ali da točno j topova bude u P. Nađimo vezu između brojeva P_j, a posebno P_0 i "topovskih brojeva" t_k. Prvo definiramo tzv. **topovski polinom** (engl. "rook polynomial"):

$$P_n(x) := \sum_{j=0}^{n} P_j x^j.$$

PROPOZICIJA 5.

$$P_n(x) = \sum_{k=0}^{n} t_k (n - k)! (x - 1)^k. \qquad (22)$$

Odavde je posebno

$$P_0 = P_n(0) = \sum_{k=0}^{n} (-1)^k t_k (n - k)!. \qquad (23)$$

Dokaz. Dovoljno je (22) dokazati za sve $x \in \mathbb{N}$. Lijeva strana broji načine da se n topova stavi na čitavu ploču $[n] \times [n]$ i svaki top koji je u P označi nekim brojem iz $[x]$ (to je u stvari funkcija $[j] \to [x]$).

S druge strane, takva se konfiguracija dobiva i tako da k topova koji se ne napadaju stavimo u P i svaki označimo nekim brojem iz $\{2, \ldots, x\}$, a ostalih $n-k$ topova stavimo na ploču $[n] \times [n]$ (u nenapadajuće položaje) na $(n-k)!$ načina i nove topove koji padnu u P označimo s 1. Tako dobijemo bijekciju. □

Primjer 6. (Jošte jednom o deranžmanima.) Uzmimo da je ploča jednaka dijagonali, tj. $P = \{(1,1), (2,2), \ldots, (n,n)\}$. Izračunajte $P_n(x)$ i $P_0 = D_n$.

Rješenje. Prvo je očito $t_k = \binom{n}{k}$, jer od dijagonalnih n biramo k pozicija. Stoga iz Propozicije 5 slijedi

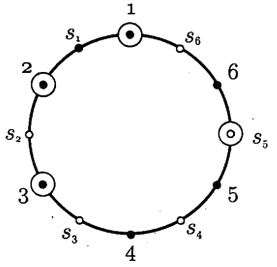
$$P_n(x) = \sum_{k=0}^{n} \binom{n}{k} (n-k)!(x-1)^k = \sum_{k=0}^{n} \frac{n!}{k!}(x-1)^k.$$

Odavde dobivamo $P_0 = P_n(0) = \sum_{k=0}^{n}(-1)^k n!/k!$, tj. još jedanput smo izračunali broj deranžmana D_n.

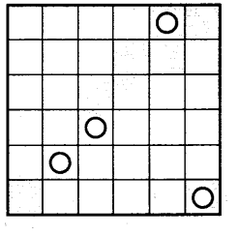
Slično se mogu (još jedanput) naći i brojevi $D_n(r)$ permutacija s točno r fiksnih točaka (učinite to). □

Sada ćemo riješiti također jedan pozanti stari kombinatorni problem koji potječe od E. Lucasa iz 1891. godine, a poznat je kao "problem bračnih parova" ili francuski "**probléme des ménages**": na koliko načina n bračnih parova (= "ménages") mogu posjesti oko okruglog stola tako da muškarci i žene alterniraju i tako da nijedna žena ne sjedi do svog muža (da ne dođe do svađe)?

Označimo s $M(n)$ traženi ("ménages") broj. Neka je $n \geq 2$. Prvo neka žene (njih n) zauzmu položaj oko okruglog stola. Broj takvih različitih mogućnosti je očito $2n!$. Fiksirajmo jedan takav položaj žena za okruglim stolom i označimo ih brojevima od 1 do n (počevši npr. od najstarije među njima). Ako je s_i prvo lijevo sjedište od žene označene s i, onda njezin muž ne smije sjesti na sjedišta s_i, s_{i+1} za $i \leq n-1$, a muž žene označene s n ne smije sjesti na sjedišta s_1 i s_n. Dakle, ono što još treba izračunati je broj $R(n)$ permutacija $\pi \in S_n$ za koje je $\pi(i) \neq i, i+1$ za $i \leq n-1$, a $\pi(n) \neq 1, n$ ili kraće $\pi(i) \not\equiv i, i+1 \pmod n$, za sve $i \in [n]$. Npr. za $n = 6$ vidi sl. a).



a)


b)

Tada je $M(n) = 2n!R(n)$. Da izračunamo $R(n)$ pogledajmo ploču $P = \{(1,1), (2,2), \ldots, (n,n), (1,2), (2,3), \ldots, (n-1,n), (n,1)\}$. Tada je $R(n)$ jednak broju P_0 za

tu ploču (vidi sl. b) za $n = 6$). Topovski broj t_k za tu ploču je jednak broju načina da se odabere k od $2n$ točaka na kružnici, tako da nikoje dvije nisu susjedne. Npr. za $k = 4$, $\{(2,2), (3,3), (5,6), (6,1)\}$ korespondira $\{2, 3, s_5, 1\}$ za $n = 6$ i na slikama a) i b) su označene kružićem. No, mi smo taj broj izračunali (vidi Primjer 13 u poglavlju 3) i on iznosi $\frac{2n}{2n-k}\binom{2n-k}{k}$. Stoga iz Propozicije 5 dobivamo

KOROLAR 6. *Topovski polinom za ploču* $P = \{(i,i), (i, i+1) \pmod n | i \in [n]\}$ *dan je formulom*

$$P_n(x) = \sum_{k=0}^{n} \frac{2n}{2n-k}\binom{2n-k}{k}(n-k)!(x-1)!.$$

Posebno je broj $R(n)$ *permutacija* $\pi \in S_n$ *za koje je* $\pi(i) \not\equiv i, i+1 \pmod n$ *za sve* $i \in [n]$ *jednak*[4]

$$R(n) = P_0 = P_n(0) = \sum_{k=0}^{n}(-1)^k \frac{2n}{2n-k}\binom{2n-k}{k}(n-k)!.$$

Dakle, $M(n) = 2n!R(n)$ i asimptotski je $M(n) \sim 2(n!/e)^2$.

I mnogi drugi kombinatorni problemi mogu se tako rješavati pogodnim izborom "zabranjene" (ili krnje) ploče P; zanimljive su tako k-neskladna ploča $\{(i,i), (i, i+1), \ldots, (i, i+k-1) \pmod n | i \in [n]\}$, Ferrerova ploča $\{(i,j) | i \in [m], 1 \leq j \leq b_i\}$ za $0 \leq b_1 \leq \cdots \leq b_m$ itd., ali se nećemo u to upuštati.

Vratimo se na (poopćenu) formulu uključivanja-isključivanja. Katkada ne možemo točno izračunati veličine svih presjeka skupova, nego samo neke. Tada nam sljedeće nejednakosti omogućuju da ipak dosta dobro procijenimo $|\overline{A_1} \cap \cdots \cap \overline{A_n}|$.

PROPOZICIJA 6 (Bonferronijeve nejednakosti; 1936.). *Neka su* $A_1, A_2, \ldots, A_n \subseteq U$ *podskupovi konačnog skupa* U, $A_I = \bigcap_{i \in I} A_i$, $A_\emptyset = U$ *za* $I \subseteq [n]$ *i neka je*

$$S_k = \sum_{|I|=k} |A_I|, \quad 0 \leq k \leq n.$$

Tada za svako k, $0 \leq k \leq n$, *vrijedi nejednakost*

$$S_k - S_{k+1} + \cdots + (-1)^{n-k} S_n \geq 0. \tag{24}$$

Dokaz I. Indukcijom po n, što prepuštamo čitatelju. □

Dokaz II. Kao i kod poopćene FUI na skup A_i gledamo kao na skup svih elemenata iz U koji imaju svojstvo i, $i = 1, 2, \ldots, n$. Tada je $|A_I| = f_{\geq}(I) = \sum_{J \supseteq I} f_{=}(J)$.

[4]Ovo se katkad zove **Touchardov teorem**, jer ga je 1933. godine dokazao francuski matematičar Jacques Touchard (1885 – 1968), rabeći običnu FUI.

Imamo sljedeće

$$S_k - S_{k+1} + \cdots + (-1)^{n-k} S_n = \sum_{|I|\geq k} (-1)^{|I|-k} f_{\geq}(I) =$$

$$= \sum_{|I|\geq k} \sum_{J\supseteq I} (-1)^{|I|-k} f_{=}(J) = \sum_{|J|\geq k} f_{=}(J) \sum_{\substack{I\supseteq J \\ |I|\geq k}} (-1)^{|I|-k} =$$

$$= \sum_{|J|\geq k} f_{=}(J) \sum_{i=k}^{|J|} (-1)^{i-k} \binom{|I|}{i}.$$

No zbog $\sum_{i=k}^{m} (-1)^{i-k} \binom{m}{i} = \binom{m-1}{k-1} \geq 0$ (vidi (19) u poglavlju II) i $f_{=}(J) \geq 0$, slijedi nejednakost (24). □

Označimo li $N := f_{=}(\emptyset) = |\overline{A_1} \cap \cdots \cap \overline{A_n}| = S_0 - S_1 + \cdots + (-1)^n S_n$, raspisane Bonferronijeve nejednakosti izgledaju ovako:

$$N \geq 0,\ N \leq S_0,\ N \geq S_0 - S_1,\ N \leq S_0 - S_1 + S_2, \ldots$$

Drugim riječima, parcijalne sume $S_0 - S_1 + \cdots + (-1)^k S_k$ redom premašuju i podbacuju vrijednost od N.

I FUI i razvoj determinante su alternirane sume. Može se očekivati da postoji neka veza. Pokazat ćemo da se neke determinante $\det(a_{ij})$, $0 \leq i, j \leq n$ za koje je $a_{ij} = 0$ za $j < i - 1$, mogu kombinatorno interpretirati pomoću FUI.

Sjetimo se da je skup svih padova $D(\pi)$ permutacije $\pi = i_1 i_2 \ldots i_n$ od $[n]$ definiran kao skup $D(\pi) = \{k \in [n] | i_k > i_{k+1}\}$. Očito je $D(\pi) \subseteq [n-1]$. Ako je $S \subseteq [n-1]$, označimo s $\alpha_n(S)$ odn. $\beta_n(S)$ brojeve permutacija $\pi \in S_n$ čiji je skup padova sadržan, odn. jednak skupu S. Formulom:

$$\alpha_n(S) = \#\{\pi \in S_n | D(\pi) \subseteq S\},\ \beta_n(S) = \#\{\pi \in S_n | D(\pi) = S\}.$$

Jasno je da vrijedi

$$\alpha_n(S) = \sum_{T\subseteq S} \beta_n(T).$$

Iz poopćene FUI tada slijedi

$$\beta_n(S) = \sum_{T\subseteq S} (-1)^{|S-T|} \alpha_n(T).$$

Primjer 7. Neka je $S = \{a_1, a_2, \ldots, a_k\} \subseteq [n-1]$, $a_1 < a_2 < \cdots < a_k$. Dokažite da je

$$\beta_n(S) = \det\left[\binom{n-a_i}{a_{j+1}-a_i}\right],$$

pri čemu je $0 \leq i, j \leq k$, $a_0 = 0$, $a_{k+1} = n$.

Rješenje. Prvo izračunajmo $\alpha_n(S)$. Svaku permutaciju $\pi = i_1 i_2 \ldots i_n$ za koju je $D(\pi) \subseteq S$ dobijemo tako da prvo odaberemo $i_1 < i_2 < \cdots < i_{a_1}$ na $\binom{n}{a_1}$ načina, pa onda $i_{a_1+1} < i_{a_1+2} < \cdots < i_{a_2}$ na $\binom{n-a_1}{a_2-a_1}$ načina i tako dalje. Stoga je $\alpha_n(S)$ multinomni koeficijent:

$$\alpha_n(S) = \binom{n}{a_1}\binom{n-a_1}{a_2-a_1}\binom{n-a_2}{a_3-a_3}\cdots\binom{n-a_k}{n-a_k} = \binom{n}{a_1, a_2-a_1, \ldots, n-a_k}.$$

Zato iz gornje formule, uzmemo li $T = \{a_{j_1}, \ldots, a_{j_t}\}$, $j_1 < \cdots < j_t \leq k$, dobivamo

$$\beta_n(S) = \sum (-1)^{k-t} \binom{n}{a_{j_1}, a_{j_2}-a_{j_1}, \ldots, n-a_{j_t}}, \qquad (*)$$

gdje se sumira po svim $1 \leq j_1 < j_2 < \cdots < j_t \leq k$. No, $(*)$ je oblika kao alternativna suma

$$D_k = \sum (-1)^{k-t} f(0, j_1) f(j_1, j_2) \ldots f(j_t, k+1),$$

gdje se sumira po svim $1 \leq j_1 < j_2 < \cdots < j_t \leq k$, a f je neka funkcija na $\{0, 1, \ldots, k+1\}^2$ za koju je $f(i,j) = 0$ za $i > j$. Članovi sume D_k su upravo ne-nul članovi razvoja $(k+1) \times (k+1)$ determinante čiji je (i,j)-ti član $f(i, j+1)$, za $i, j \in \{0, 1, \ldots, k\}$. Stavimo li $f(i,j) = 1/(a_j - a_i)!$ ($a_0 = 0$, $a_{k+1} = n$), dobivamo iz $(*)$

$$\beta_n(S) = n! \det\left[\frac{1}{(a_{j+1} - a_i)!}\right],$$

gdje su $i, j \in \{0, 1, \ldots, k\}$. Tako npr. za $n = 8$, $S = \{1, 5\}$ imamo da je (i,j)-ti član determinante $\beta_8(\{1,5\})$ tipa 3×3 jednak $f(i, j+1) = \binom{8-a_i}{a_{j+1}-a_i}$, gdje je $a_0 = 0$, $a_1 = 1$, $a_2 = 5$, $a_3 = 8$. Provjerite da se dobiva $\beta_8(\{1,5\}) = 217$. □

§ 2. Parcijalno uređeni skupovi i Möbiusova inverzija

U ovoj ćemo točki na apstraktnoj razini opisati jednu opću metodu koju je razvio Gian-Carlo Rota[5], a koja jako poopćava formulu uključivanja-isključivanja. No prvo ćemo detaljnije obraditi parcijalno uređene skupove, a oni su zanimljivi i sami po sebi s kombinatornog gledišta.

Parcijalno uređeni skupovi

Parcijalno (djelomično) uređen skup ili kraće **p.u. skup** je uređeni par $(P, \leq)$, gdje je $\leq$ **parcijalni uređaj** na P, tj. binarna relacija na P koja je refleksivna (tj. $x \leq x$, $\forall x \in P$), antisimetrična (tj. $x \leq y \ \&\ y \leq x \Rightarrow x = y$) i tranzitivna (tj. $x \leq y \ \&\ y \leq z \Rightarrow x \leq z$). Katkad pišemo $y \geq x$ umjesto $x \leq y$, te $x < y$ ako je $x \leq y$ i $x \neq y$. Ako ne vrijedi $x \leq y$, pišemo $x \not\leq y$. Ako je $x \not\leq y$ i $y \not\leq x$, onda x i y zovemo **neusporedivim elementima**, a inače **usporedivim**. Ako je P konačan skup, onda se i $(P, \leq)$ zove **konačan p.u. skup**. Element $\hat{0} \in P$ je **minimalan** ako je $x \not\leq \hat{0}$, $\forall x \in P$. Slično je $\hat{1} \in P$ **maksimalan** ako je $x \not\geq \hat{1}$, $\forall x \in P$. P može imati više minimalnih i maksimalnih elemenata. Za

[5] Gian-Carlo Rota (1932–1999), američki matematičar talijanskog podrijetla

$x, y \in P$, skup $[x,y] := \{z \in P | x \leq z \leq y\}$ se zove **segment** u P od x do y. Ako je svaki segment u P konačan skup, kažemo da je $(P, \leq)$ **lokalno konačan** p.u. skup. $(P, \leq)$ i $(P', \leq')$ su **izomorfni** ako postoji bijekcija f koja čuva uređaj, tj. $x \leq y$ u $P \iff f(x) \leq' f(y)$ u P'. Pišemo $P \cong P'$.

Ako su svaka dva elementa iz P usporediva, onda se $(P, \leq)$ zove **lanac** (ili **totalno uređen** ili **linearno uređen**), a ako su svaka dva različita elementa neusporediva, onda se zove **antilanac**. Kažemo da y **natkriva** x u $(P, \leq)$ i pišemo $x \lessdot y$ (ili $y \gtrdot x$) ako je $x < y$ i ne postoji $z \in P$ za koji je $x < z < y$. Dakle, $x \lessdot y \iff x < y$ i segment $[x,y] = \{x, y\}$. Lokalno konačni p.u. skup je potpuno određen relacijom natkrivanja.

Grafički se p.u. skupovi predočuju Hasseovim dijagramom. **Hasseov dijagram** p.u. skupa $(P, \leq)$ je graf čiji su vrhovi elementi iz P, a bridovi su parovi xy za koje je $x \lessdot y$, tj. x je natkriven s y i y se tada u ravnini crta "iznad" x.

Primjer 8. a) Ako je $P = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ ili $[n]$ s običnom nejednakošću $\leq$, onda je $(P, \leq)$ p.u. skup i to su sve lanci. $([n], \leq)$ je konačan lanac $1 < 2 < \cdots < n$ duljine n i označava se s $\underline{n}$.

b) Skup svih podskupova nekog (konačnog) skupa s parcijalnim uređajem kao inkluzijom. Tako se $(2^{[n]}, \subseteq)$ kao p.u. skup označava s B_n.

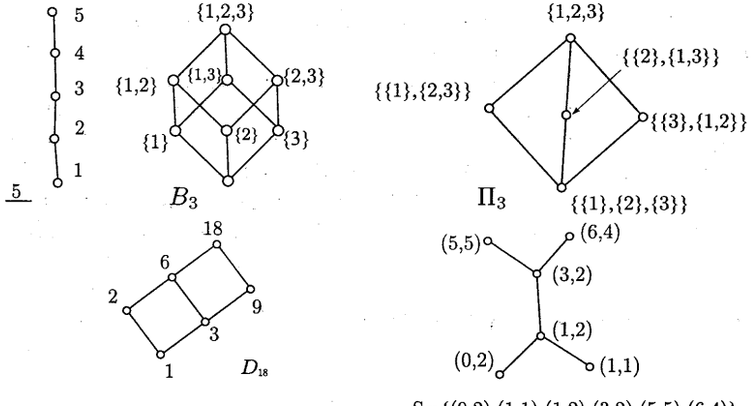
c) Skup svih djelitelja (divizora) prirodnog broja n je p.u. skup s $P = D_n = \{x \in \mathbb{N} | x \text{ dijeli } n\}$ i $x \leq y \iff x | y$.

d) $(\mathbb{R}^n, \leq)$, gdje je $(x_1, \ldots, x_n) \leq (y_1, \ldots, y_n) \iff x_i \leq y_i$ za $i = 1, \ldots, n$. Umjesto $\mathbb{R}^n$ možemo uzeti i bilo koji podskup $S \subseteq \mathbb{R}^n$.

e) Skup svih particija nekog (konačnog) skupa S s **profinjenjem** kao parcijalnim uređajem je p.u. skup. Pri tome za dvije particije π i σ skupa S pišemo $\pi \leq \sigma$ i kažemo da π **profinjuje** (ili **usitnjuje**) σ ako je svaki blok od π sadržan u nekom bloku od σ. Npr. za $S = [6]$, ako particija π od $[6]$ ima blokove $12, 3, 456$, a σ blokove $123, 456$, onda je $\pi \leq \sigma$. Sve particije od $[n]$ s tim parcijalnim uređajem označavamo s Π_n.

f) Skup svih potprostora n-dimenzionalnog vektorskog prostora $V_n(q)$ nad konačnim poljem $\mathbb{F}_q$ s inkluzijom kao parcijalnim uređajem je p.u. skup koji označavamo $L_n(q)$.

Evo i Hasseovih dijagrama nekih p.u. skupova na idućoj slici.



U ovim primjerima jedino je $\underline{5}$ lanac, a ostali nisu, ali u sebi imaju lanac, npr. u B_3 imamo lanac $\emptyset < \{3\} < \{2,3\} < \{1,2,3\}$ i to duljine 3. Tako i općenito **lanac** u $(P, \leq)$ je $C \subseteq D$ koji je kao p.u. skup $(C, \leq)$ lanac. **Duljina lanca** C je $|C| - 1$. **Rang** (ili **visina**) konačnog p.u. skupa je maksimalna duljina lanaca u P. Ako svi maksimalni lanci imaju istu duljinu n, onda je P **graduiran ranga** n. Tada imamo i **funkciju ranga** $r : P \to \{0, 1, \ldots, n\}$ i $r(x_0) = 0$ ako je x_0 minimalni element i $r(y) = r(x) + 1$ ako y natkriva x. Ako je $r(x) = i$, kažemo da je x **ranga** i. Odgovarajuća kombinatorna funkcija je tada **polinom ranga** od P

$$F(P, q) = \sum_{i=0}^{n} p_i q^i,$$

gdje je p_i broj elemenata u P ranga i. Tako su u gornjim primjerima svi p.u. skupovi $\underline{n}$, B_n, D_n, Π_n i $L_n(q)$ graduirani i npr. rang od $S \in B_n$ je $|S|$, a B_n je ranga n, rang od $\pi \in \Pi_n$ je $n-$ broj blokova od π, a Π_n je ranga $n-1$, dok je $W \in L_n(q)$ ranga jednakog $\dim W$, a $L_n(q)$ ima rang n.

Dualni pojam od lanca je **antilanac** (ili **Spernerova familija**) u P, tj. podskup $A \subseteq P$ koji je kao p.u. skup $(A, \leq)$ antilanac. **Širina** od P je veličina maksimalnog antilanca u P. Tako je npr. na gornjoj slici širina od B_3 jednaka 3, od Π_3 također 3, a širina zadnjeg primjera je 2.

Osnovni rezultati o p.u. skupovima su Dilworthov i Spernerov teorem.

TEOREM 3 (R. P. Dilworth, 1950.). *Neka je $(P, \leq)$ konačan p.u. skup širine k. Tada postoji particija od P u k lanaca $C_1, C_2, \ldots, C_k$. (Teorem vrijedi i za lokalno konačne p.u. skupove.)*

Dokaz. Indukcijom po $|P|$. Za $|P| = 1$ tvrdnja je trivijalna. Pretpostavimo da tvrdnja vrijedi za $|P| < n$ i neka je $(P \leq)$ p.u. skup i $|P| = n$. Možemo pretpostaviti da je širina k od $(P, \leq)$ veća od 1.

Uzmimo jedan minimalni element $x_0 \in P$ i jedan maksimalni element $y_0 \in P$, $x_0 \leq y_0$ i neka je $Q = P \setminus \{x_0, y_0\}$. Ako je širina od Q manja od k, onda se Q može particionirati u manje od k lanaca, što zajedno s $\{x_0, y_0\}$ daje particiju od P u najviše k lanaca. Zato pretpostavimo da Q ima širinu $k (> 1)$. Tada je $x_0 < y_0$ i neka je $A = \{a_1, a_2, \ldots, a_k\}$ antilanac u Q.

Promotrimo skupove $X = \{x \in P | x \leq a_i \text{ za neko } a_i \in A\}$ i $Y = \{y \in P | y \geq a_j \text{ za neko } a_j \in A\}$. Tada je očito $x_0 \in X \setminus Y$, $y_0 \in Y \setminus X$, pa je $|X|, |Y| < |P|$. Prema pretpostavci indukcije, postoje particije u lance $X = C_1' \cup C_2' \cup \cdots \cup C_k'$ i $Y = C_1'' \cup C_2'' \cup \cdots \cup C_k''$ Očito možemo preoznačiti te lance tako da je $a_i \in C_i' \cap C_i''$, $i = 1, 2, \ldots, k$. Tada je $C_i = C_i' \cup C_i''$ lanac za svako i, čime dobivamo particiju $P = C_1 \cup C_2 \cup \cdots \cup C_k$ od P u k lanaca. (Za drugi dokaz v. pogl VI, Korolar 16.) □

TEOREM 4 (E. Sperner, 1928.). *Širina p.u. skupa B_n je jednaka*

$$\binom{n}{\lfloor n/2 \rfloor}.$$

Drugim riječima, svaki antilanac podskupova iz $[n]$ *ima* $\leq \binom{n}{\lfloor n/2 \rfloor}$ *članova i postoji antilanac s točno toliko članova.*

Dokaz. Ključna je opaska činjenica da u bilo kojem p.u. skupu svaki lanac i antilanac imaju najviše jedan zajednički element. Stoga ako p.u. skup uspijemo particionirati u t lanaca, onda svaki antilanac ima $\leq t$ elemenata.

Sada promotrimo maksimalni lanac u B_n. On sadrži po jedan podskup svake veličine u $[n]$, pa je oblika:

$$\emptyset \subset \{i_1\} \subset \{i_1, i_2\} \subset \{i_1, i_2, i_3\} \subset \cdots \subset \{i_1, i_2, \ldots, i_n\}, \tag{25}$$

gdje je $i_1 i_2 \ldots i_n$ bilo koja permutacija (tj. linearni uređaj) od $[n]$. Prema tome, maksimalnih lanaca u B_n ima $n!$.

Neka je $\mathcal{A}$ bilo koji antilanac podskupova iz $[n]$ (tj. $A \not\subseteq B, B \not\subseteq A$, $\forall A, B \in \mathcal{A}$). Tvrdimo da je $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$. U tu svrhu promotrimo sve uređene parove $(A, \mathcal{C})$, gdje je $A \in \mathcal{A}$, a $\mathcal{C}$ maksimalni lanac koji sadrži A. Te parove ćemo izbrojiti na dva načina.

Prvo, kako smo već rekli, svaki lanac sadrži najviše jedan $A \in \mathcal{A}$, pa je broj parova $(A, \mathcal{C})$ najviše jednak broju maksimalnih lanaca, a to je $n!$.

S druge strane uzmimo jedan skup $A \in \mathcal{A}$ i pogledajmo koliko ga maksimalnih lanaca može sadržavati. Ako je $|A| = k$, onda lanac oblika (25) sadrži A ako i samo ako je $A = \{i_1, i_2, \ldots, i_k\}$ (jer A mora biti samo jedna točka tog lanca). No, linearnih uređaja od $[n]$ koji na prvih k mjesta imaju elemente iz A ima $k!$, dok ostatak $[n] \setminus A$ možemo linearno urediti na $(n-k)!$ načina. Stoga je A sadržan u $k!(n-k)!$ maksimalnih lanaca. Prema tome, promatranih uređenih parova $(A, \mathcal{C})$ ima $\sum_{A \in \mathcal{A}} |A|!(n - |A|)!$. Odatle zaključujemo da je

$$\sum_{A \in \mathcal{A}} |A|!(n - |A|)! \leq n!,$$

tj.

$$\sum_{A \in \mathcal{A}} \frac{1}{\binom{n}{|A|}} \leq 1. \tag{26}$$

Kako je $\binom{n}{k} \leq \binom{n}{\lfloor n/2 \rfloor}$ za sve $k = 0, 1, \ldots, n$ (Propozicija 14 u pogl. II), to iz (26) slijedi

$$1 \geq \sum_{A \in \mathcal{A}} \frac{1}{\binom{n}{|A|}} \geq |\mathcal{A}| \cdot \frac{1}{\binom{n}{\lfloor n/2 \rfloor}},$$

pa je $|\mathcal{A}| \leq \binom{n}{\lfloor n/2 \rfloor}$ kao što smo tvrdili. Uočimo još da svi k-člani podskupovi od $[n]$ čine antilanac u B_n, pa posebno i svi $\lfloor n/2 \rfloor$-člani podskupovi čine antilanac. Njegova je veličina $\binom{n}{\lfloor n/2 \rfloor}$. Stoga je širina od B_n doista kako se tvrdi. □

Nejednakost (26) u ovom dokazu je u literaturi poznata kao **LYM-nejednakost** prema autorima koji su je prvi (neovisno) dokazali Lubell, Yamamoto i Meshalkin (oko 1966/67. godine). Evo dviju primjena.

Primjer 9 (Littlewood-Offordov problem). Zadano je n realnih brojeva $a_1, a_2, \ldots a_n$ tako da su svi $a_i \geq 1$. Tada između svih 2^n sumâ oblika $\pm a_1 \pm a_2 \pm \cdots \pm a_n$, onih kojima je apsolutna vrijednost < 1 ima najviše $\binom{n}{\lfloor n/2 \rfloor}$.

Rješenje. Problem možemo reformulirati ovako: koliko najviše ima vektora $(\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_n)$, $\varepsilon_i = \pm 1$ tako da suma $\sum_{i=1}^n \varepsilon_i a_i$ padne u otvoreni interval $\langle -1, 1 \rangle$ (ili bilo koji otvoreni interval duljine 2)? Uzmimo da sume $a = \sum \varepsilon_i a_i$ i $a' = \sum \varepsilon_i' a_i$ leže u intervalu $\langle -1, 1 \rangle$ i neka je $a \neq a'$. Promotrimo skupove indeksa $J = \{i \in [n] | \varepsilon_i = 1\}$ i $J' = \{i \in [n] | \varepsilon_i' = 1\}$. Pretpostavimo da je $J \subseteq J'$. Tada je

$$a' - a = \sum \varepsilon_i' a_i - \sum \varepsilon_i a_i = 2 \sum_{i \in J' \setminus J} a_i \geq 2.$$

Stoga familija skupova J čini antilanac u p.u. skupu B_n, pa iz Spernerovog teorema slijedi tvrdnja. □

Primjer 10. Neka je prirodan broj $N = p_1 p_2 \ldots p_n$, gdje su p_i različiti prosti brojevi, tj. N nije djeljiv s kvadratom nijednog prostog broja. Tada je maksimalni broj djelitelja od N koji nisu djeljivi jedan s drugim najviše jednak $\binom{n}{\lfloor n/2 \rfloor}$

Rješenje. Svaki djelitelj d od N je oblika $d = p_{i_1} p_{i_2} \ldots p_{i_k}$. Njemu pridružimo skup $M_d = \{i_1, i_2, \ldots, i_k\} \subseteq \{1, 2, \ldots, n\}$. Tada je očito $d_1 | d_2 \iff M_{d_1} \subseteq M_{d_2}$. Prema tome, maksimalni skup djelitelja od N koji ne dijele jedan drugoga jednak je veličini maksimalnog antilanca od $[n]$. Tvrdnja tada slijedi iz Spernerovog teorema. □

Uređajni ideal I p.u. skupa P je podskup $I \subseteq P$ sa svojstvom da $x \in I$ i $y \leq x \Rightarrow y \in I$. Ako je $A \subseteq P$ neki skup (npr. antilanac), onda je skup $I = \{x \in P | x \leq a \text{ za neko } a \in A\}$ uređajni ideal u P; kažemo da A **generira** taj ideal. Ako je A jednočlan skup $A = \{a\}$, onda se taj ideal označava s $\langle a \rangle$ i zove **glavni uređajni ideal** u P. **Rešetka** (engl. lattice) je p.u. skup L u kojem svaka dva elementa imaju najveću donju i najmanju gornju među, ili kraće **infimum** i **supremum**. Pri tom za $x, y \in L$, **gornja međa** je svaki $z \in L$ takav da je $x, y \leq z$, a $\sup\{x, y\}$ (ili $x \vee y$) je gornja međa za x, y tako da za svaku gornju među w od x, y vrijedi $w \geq \sup\{x, y\}$. Slično se definira i $\inf\{x, y\}$ (ili $x \wedge y$). Konačna rešetka ima jedinstveni najmanji element 0 i jedinstveni najveći element 1. Svaki element koji natkriva 0 u konačnoj rešetki zove se **atom**. Konačna rešetka je **modularna** ako je graduirana i za funkciju ranga r vrijedi $r(x) + r(y) = r(x \vee y) + r(x \wedge y)$, $\forall x, y \in L$. Tako su npr., spomenuti primjeri $\underline{n}$, B_n, D_n i $L_n(q)$ modularne rešetke. S kombinatornog stajališta, važna klasa rešetaka su tzv. **distributivne rešetke**, tj. one za koje vrijedi $x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$ i $x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$, $x, y, z \in L$. Tako npr. $\underline{n}$, B_n i D_n jesu, a Π_n ($n \geq 3$) i $L_n(q)$ ($n \geq 2$) nisu distributivne. Osnovni je teorem da je konačna distributivna rešetka L kao p.u. skup izomorfna p.u. skupu $J(P)$ svih uređajnih ideala uređenih s inkluzijom nekog (do na izomorfizam jedinstvenog) p.u. skupa P.

Osnovne operacije s p.u. skupovima P i Q su sljedeće: **direktna suma** $P + Q$ je za disjunktne P i Q njihova unija s parcijalnim uređajem naslijeđenim iz P i Q; **uređajna suma** $P \oplus Q$ je $P \cup Q$ s uređajem $x \leq y$ u $P \oplus Q$ ako je a) $x \leq y$ u P ili b) $x \leq y$ u Q ili c) $x \in P$, $y \in Q$; **direktni produkt** $P \times Q$ s uređajem

$(x,y) \leq (x',y')$ ako je $x \leq x'$ u P i $y \leq y'$ u Q; **funkcijski p.u. skup** Q^P svih **funkcija** $f : P \to Q$ **koje čuvaju uređaj** (tj. $x \leq y \Rightarrow f(x) \leq f(y)$) s uređajem: $f \leq g \iff f(x) \leq g(x)$, $\forall x \in P$. Vrijede uobičajena pravila asocijativnosi, komutativnosti i distributivnosti za $+$ i $\times$ kao i eksponencijalni zakoni ($R^{P+Q} \cong R^P \times R^Q$, $(R^P)^Q \cong R^{P\times Q}$).

Ovdje završavamo s ovim kratkim potpurijem osnovnih pojmova i činjenica o p.u. skupovima. Zainteresiranog čitatelja upućujemo na knjigu [70*].

Möbiusova inverzija za p.u. skupove

Neka je $(P, \leq)$ lokalno konačni p.u. skup (tj. svi segmenti su konačni). Definirajmo **algebru incidencije** $A(P)$ od P koja će odražavati strukturu parcijalnog uređaja, a čiji se elementi zovu **funkcije incidencije** ovako:

$$A(P) = \{f : P \times P \to \mathbb{C} | x \not\leq y \Rightarrow f(x,y) = 0\}.$$

(Umjesto $\mathbb{C}$ možemo uzeti i bilo koje polje K karakteristike 0, npr. $\mathbb{R}$, $\mathbb{Q}$). Skup $A(P)$ zajedno s uobičajenim operacijama $f+g$ i λf ($\lambda \in \mathbb{C}$) tvori vektorski prostor (nad $\mathbb{C}$). Množenje $f * g$ funkcija $f, q \in A(P)$ zove se **konvolucija**, a definirano je formulom

$$(f * g)(x,y) := \sum_{x \leq z \leq y} f(x,z)g(z,y),$$

tj. sumira se po svim $z \in [x,y]$ i ta suma je konačna jer je $[x,y]$ konačan. Lako se vidi da je tada i $f * g \in A(P)$. Ako je $x \not\leq y$, onda je $(f * g)(x,y) = 0$.

Provjeru da je $A(P)$ asocijativna algebra (tj. $f*(g*h) = (f*g)*h$) s (dvostranim) jediničnim elementom δ (tj. $f * \delta = \delta * f = f$), gdje je

$$\delta(x,y) = \begin{cases} 1 & , \text{ako je } x = y \\ 0 & , \text{ako je } x \neq y, \end{cases}$$

prepuštamo čitatelju. Za konvoluciju $f * g$ nadalje ćemo pisati fg.

Za $f \in A(P)$ **lijevi** (odn. **desni**) **inverz** s obzirom na konvoluciju je element $g \in A(P)$ (ako postoji) sa svojstvom $gf = \delta$ (odnosno $fg = \delta$).

PROPOZICIJA 7. *Za $f \in A(P)$, sljedeće je ekvivalentno:*
a) f ima lijevi inverz; *b) f ima desni inverz;*
c) f ima dvostrani inverz f^{-1} (koji je nužno jedinstveni lijevi i desni inverz);
d) $f(x,x) \neq 0$, za sve $x \in P$.

Dokaz. Iz definicije konvolucije odmah slijedi da je postojanje $g \in A(P)$ za koji je $gf = \delta$ ekvivalentno s postojanjem $g \in A(P)$ za koji je $f(x,x)g(x,x) = 1$, $\forall x \in P$ i

$$g(x,y) = -\frac{1}{f(x,x)} \sum_{z < x \leq y} f(x,z)g(z,y), \ \forall x < y \text{ u } P. \tag{27}$$

Dakle, f ima lijevi inverz $g \iff f(x,x) \neq 0$, $\forall x \in P$. Slično f ima desni inverz $h \iff f(x,x) \neq 0$, $\forall x \in P$. Sada iz $gf = \delta$ i $fh = \delta$ slijedi $(gf)h = h \Rightarrow g(fh) = h \Rightarrow g\delta = h \Rightarrow g = h$. □

Definirajmo **zeta funkciju** $\zeta_P = \zeta \in A(P)$ formulom

$$\zeta(x,y) = \begin{cases} 1 & , \text{ako je } x \leq y, \\ 0 & , \text{inače.} \end{cases}$$

Prema Propoziciji 7, ζ ima inverz i označava se $\zeta^{-1} =: \mu = \mu_P$. Funkcija $\mu \in A(P)$ se zove **Möbiusova**[6] **funkcija p.u. skupa** $(P, \leq)$. Iz $\mu\zeta = \delta$, kao i (27), dobivamo (rekurzivni način računanja vrijednosti μ):

$$\mu(x,x) = 1, \ \mu(x,y) = -\sum_{x \leq z < y} \mu(x,z) \text{ za } x < y, \ \mu(x,y) = 0 \text{ za } x \not\leq y. \tag{28}$$

Möbiusova funkcija je od osnovne važnosti za dobivanje tzv. **formula inverzije**.

TEOREM 5 (Möbiusova formula inverzije). *Neka je $(P, \leq)$ lokalno konačan p.u. skup u kojem je svaki glavni uređajni ideal $\langle a \rangle = \{x \in P | x \leq a\}$ konačni i neka su $f, g : P \to \mathbb{C}$ dvije funkcije. Tada vrijedi:*

$$g(x) = \sum_{y \leq x} f(y) \iff f(x) = \sum_{y \leq x} g(y)\mu(y,x), \ \forall x \in P. \tag{29}$$

Dokaz. Dodajmo skupu P "umjetni" novi minimalni element $\hat{0}$ i označimo $\hat{P} := \{\hat{0}\} \cup P$. Na p.u. skupu $\hat{P}$ definirajmo funkcije incidencije $\hat{f}, \hat{g} \in A(\hat{P})$ ovako:

$$\hat{f}(\hat{0}, y) := f(y), \ \hat{g}(\hat{0}, y) := g(y), \text{ za sve } y \in P,$$

$$\hat{f}(x,y) = \hat{g}(x,y) = \hat{f}(x,\hat{0}) = \hat{g}(x,\hat{0}) = 0, \text{ za sve } x, y \in P.$$

Sada se lako provjeri (raspisivanjem) da je (29) ništa drugo doli invertiranje na segmentu $[\hat{0}, x]$ u $\hat{P}$:

$$\hat{g} = \hat{f}\zeta_{\hat{P}} \iff \hat{f} = \hat{g}\mu_{\hat{P}}.$$

□

Evo nekih primjera kako se računa Möbiusova funkcija μ i kako izgledaju formule inverzije.

Primjer 11. Neka je P lanac $\mathbb{N}_0 = \{0 < 1 < 2 < \dots\}$. Nađite μ i formulu inverzije.

Rješenje. Iz (28) redom nalazimo $\mu(i,i) = 1$, $\mu(0,1) = -\mu(1,1,) = -1$, $\mu(0,2) = -\mu(0,0) - \mu(0,1) = -1 + 1 = 0$ itd. općenito dobivamo

$$\mu(i,j) = \begin{cases} 1 & , \text{za } i = j, \\ -1 & , \text{za } i+1 = j, \\ 0 & , \text{inače.} \end{cases}$$

Möbiusova formula inverzije je oblika

$$g(n) = \sum_{i=0}^{n} f(i) \iff f(n) = g(n) - g(n-1), \text{ za sve } n \in \mathbb{N}.$$

[6] August Ferdinand Möbius (1790 – 1868), njemački matematičar

Drugim riječima, ova formula kaže da su operacije sume $\sum$ i diferencije Δ ($\Delta g(n) = g(n) - g(n-1)$) jedna drugoj inverzne. To možemo interpretirati kao diskretni (konačni) analogon osnovne Newton-Leibnizove formule u analizi

$$\int_a^b f(x)dx = F(b) - F(a) \iff f(x) = F'(x).$$

□

Primjer 12. Neka je $P = B_n$ rešetka ranga n svih podskupova n-članog skupa s inkluzijom kao uređajem. B_n se zove **Booleova algebra ranga** n. Odredite μ i formulu inverzije.

Rješenje. Formula (28) kaže da ako znamo sve vrijednosti $\mu(a,y)$, za $a \le y < b$, onda jednakosti $\mu(a,a) = 1$ i $\sum_{a \le y < b} \mu(a,y) = 0$ jednoznačno određuju $\mu(a,b)$.

Neka je X n-člani skup. B_n možemo poistovjetiti sa skupom svih podskupova iz X. Tvrdimo da je $\mu(S,T) = (-1)^{|T-S|}$ za $S \subseteq T \subseteq X$. Imamo:

$$\sum_{S \subseteq Y \subseteq T} (-1)^{|Y-S|} = \sum_{k=0}^{|T-S|} \binom{|T-S|}{k} (-1)^k = \begin{cases} 1 & , \text{ako } T = S, \\ 0 & , \text{ako } T \supset S. \end{cases}$$

Zbog gornje primjedbe to je zaista Möbiusova funkcija za B_n. Posebno je $\mu(\emptyset, [n]) = (-1)^n$.

Möbiusova formula inverzije za B_n tada izgleda ovako. Neka su $f, g : B_n \to \mathbb{C}$. Tada je

$$g(T) = \sum_{S \subseteq T} f(S) \iff f(T) = \sum_{S \subseteq T} (-1)^{|T-S|} g(S), \ \forall T \subseteq X.$$

Ovo su točno formule (9) i (10), tj. poopćena FUI. □

Za Möbiusovu funkciju vrijedi

PROPOZICIJA 8 (produktna formula). *Neka su P i Q lokalno konačni p.u. skupovi, a $P \times Q$ njihov direktni produkt. Ako je $(x,y) \le (x',y')$ u $P \times Q$, onda vrijedi*

$$\mu_{P \times Q}((x,y),(x',y')) = \mu_P(x,x')\mu_Q(y,y').$$

Dokaz. Opet prema (28), dovoljno je dokazati da za $a \le b$ vrijedi $\sum_{a \le z \le b} \mu(a,z) = \delta_{a,b}$. Neka je $(x,y) \le (x',y')$ u $P \times Q$. Imamo

$$\sum_{(x,y) \le (u,v) \le (x',y')} \mu_P(x,u)\mu_Q(y,v) = \left(\sum_{x \le u \le x'} \mu_P(x,u) \right) \left(\sum_{y \le v \le y'} \mu_Q(y,v) \right) =$$
$$= \delta_{x,x'} \cdot \delta_{y,y'} = \delta_{(x,y),(x',y')}.$$

Zbog jednoznačnosti od μ tvrdnja slijedi. □

Pomoću toga izračunajmo još jednom μ za B_n. B_n je očito izomorfan s $\underline{2}^n$. Möbiusova funkcija lanca $\underline{2} = \{1,2\}$ je $\mu(1,1) = \mu(2,2) = 1$, a $\mu(1,2) = -1$. Stoga ako B_n poistovjetimo sa skupom svih podskupova n-članog skupa X, onda iz produktne formule odmah slijedi da je za $S,T \subseteq X$ $\mu(S,T) = (-1)^{|T-S|}$.

Primjer 13 (Möbiusova funkcija u teoriji brojeva). Neka je $X = \mathbb{N}$, a uređaj u X neka je djeljivost, tj. $x \le y :\iff x \mid y$. Treba naći Möbiusovu funkciju i formulu inverzije.

Rješenje. Formula (28) daje u ovom slučaju $\mu(d,d) = 1$, $\mu(d,n) = 0$ za $d \nmid n$, te za $d \mid n$ $\mu(d,n) = -\sum \mu(d,x)$ (tj. sumacija je po svim $x \ne n$, za koje $d \mid x$ i $x \mid n$). Odatle slijedi da za proste brojeve p imamo $\mu(d,dp) = -1$, $\mu(d,dp^2) = 0$. Odavde induktivno (po r) slijedi da je za sve $r \ge 2$ $\mu(d,dp^r) = 0$. Nadalje, iz gornjih jednakosti slijedi da za različite proste brojeve p,q vijedi $\mu(d,dpq) = (-1)^2 = 1$, a odavde i gornje formule za $\mu(d,n)$, indukcijom po $k \in \mathbb{N}$ slijedi

$$\mu(d, dp_1p_2 \dots p_k) = (-1)^k,$$

gdje su $p_1, p_2, \dots, p_k$ različiti prosti brojevi. Tvrdimo da je općenito

$$\mu(d,n) = \begin{cases} 1 & , \text{za } n = d, \\ (-1)^k & , \text{za } n = dp_1p_2 \dots p_k, \text{ gdje su } p_1, \dots, p_k \\ & \text{različiti prosti brojevi,} \\ 0 & , \text{inače.} \end{cases}$$

Zaista, treba samo dokazati još posljednji redak. Ako $d \nmid n$, onda je prema definiciji $\mu(d,n) = 0$. Neka je $n = dp_1^{\alpha_1}p_2^{\alpha_2} \dots p_k^{\alpha_k}$, gdje je bar jedan $\alpha_i > 1$, $1 \le i \le k$. Tada imamo (rabeći (28)):

$$\mu(d, dp_1^{\alpha_1}p_2^{\alpha_2} \dots p_k^{\alpha_k}) = -\left[1 + \binom{k}{1}(-1)^1 + \binom{k}{2}(-1)^2 + \dots + \binom{k}{k}(-1)^k \right] = 0.$$

Neka je $f(n) = \sum_{d \mid n} g(d)$ (sumacija po svim djeliteljima $d \mid n$). Tada prema formuli inverzije slijedi da je $g(n) = \sum_{d \mid n} \mu(d,n) f(d)$. S druge strane, u teoriji brojeva definira se Möbiusova funkcija $\overline{\mu} : \mathbb{N} \to \{-1, 0, 1\}$ ovako. Neka je $n = p_1^{\alpha_1}p_2^{\alpha_2} \dots p_k^{\alpha_k}$ kanonski rastav prirodnog broja n. Tada definiramo

$$\overline{\mu}(n) := \begin{cases} 1 & , \text{za } n = 1, \\ (-1)^k & , \text{za } \alpha_1 = \alpha_2 = \dots = \alpha_k = 1, \\ 0 & , \text{inače.} \end{cases}$$

Iz gornjih jednakosti onda slijedi da je $\mu(d,n) = \overline{\mu}\left(\frac{n}{d}\right)$, za $d \mid n$, pa je formula inverzije u ovom slučaju

$$g(n) = \sum_{d \mid n} \overline{\mu}\left(\frac{n}{d}\right) f(d).$$

Tako npr., ako je φ Eulerova funkcija, onda se lako dokaže **Gaussova formula** $n = \sum_{d \mid n} \varphi(d)$. Tu je $f =$ identiteta, a $g = \varphi$, pa prethodnom inverzijom slijedi

$$\varphi(n) = \sum_{d \mid n} \overline{\mu}\left(\frac{n}{d}\right) d = n - \frac{n}{p_1} - \frac{n}{p_2} - \dots + \frac{n}{p_1p_2} + \dots,$$

što znamo i od prije. Naravno i obratno, iz ove jednakosti slijedi Gaussova formula. □

Primjer 14 (broj ogrlica ili broj cikličkih nizova). Pretpostavimo da imamo neograničenu količinu perli iz k različitih boja. Treba naći koliko ima ogrlica koje se sastoje od n perli. Pritom dvije ogrlice smatramo da su jednake ako jednu iz druge možemo dobiti nekim cikličkim pomakom (i-ta perla prelazi u $(i+1)$-vu).

Rješenje. Taj problem možemo i ovako formulirati: na skupu svih preslikavanja $f : [n] \to \{b_1, \ldots, b_k\}$ (i-toj perli ogrlice pridružimo $f(i) = b_j$ j-tu boju), definiramo relaciju ekvivalencije $f \sim f' :\iff f'(i) = f(i+d)$, $1 \le d \le n$, $i = 1, 2, \ldots, n$, zbrajanje modulo n. Jasno da se vektori $(f(1), \ldots, f(n))$ i $(f'(1), \ldots, f'(n))$ koji odgovaraju ekvivalentnim preslikavanjima razlikuju za neki ciklički pomak. Stoga ćemo skup vektora koji odgovara klasi ekvivalencije preslikavanja zvati **ciklički niz**. Broj tih cikličkih nizova $M_{n,k}$ je jednak traženom broju ogrlica.

Broj d je period cikličkog pomaka vektora $(f(1), \ldots, f(n))$ ako je $f(i+d) = f(i)$, $i = 1, 2, \ldots, n$. Svi vektori $(f(1), \ldots, f(n))$ koji dolaze od iste klase ekvivalencije preslikavanja imaju jedan te isti najmanji period d, pa neka je $M(d)$ broj klasa ekvivalencije f-ova za koje vektori $(f(1), \ldots, f(n))$ imaju najmanji period d. Broj elemenata svake klase očito je d. Stoga je ukupan broj preslikavanja f kod kojih vektori $(f(1), \ldots, f(n))$ imaju najmanji period d jednak $dM(d)$. Sumirajući po svim $d \mid n$, dobijemo broj svih preslikavanja, tj. $k^n = \sum_{d|n} dM(d)$. Odavde i iz formule inverzije u prethodnom primjeru dobivamo da je

$$M(n) = \frac{1}{n} \sum_{d|n} \overline{\mu}\left(\frac{n}{d}\right) k^d.$$

Kako su svi najmanji periodi djelitelji od n, to je traženi broj konačno jednak

$$M_{n,k} = \sum_{d|n} M(d) = \sum_{d|n} \frac{1}{d} \sum_{x|d} \overline{\mu}\left(\frac{d}{x}\right) k^x = \frac{1}{n} \sum_{d|n} \varphi\left(\frac{n}{d}\right) k^d.$$

(U posljednoj jednakosti koristili smo se posljednjom jednakošću iz prethodnog primjera. Uočite da se za $k = 1$ dobiva Gaussova formula). □

Primjer 15. Neka je D_N p.u. skup kao u Primjeru 8 c), i neka je $N = p_1^{n_1} \ldots p_k^{n_k}$ kanonski rastav prirodnog broja N. Odredite μ i formulu inverzije.

Rješenje. Svaki djelitelj od N je oblika $p_1^{a_1} \ldots p_k^{a_k}$, $0 \le a_i \le n_i$, $i = 1, \ldots, k$, pa je D_N kao p.u. skup izomorfan s $P = (\underline{n_1}+\underline{1}) \times \cdots \times (\underline{n_k}+\underline{1})$, s parcijalnim uređajem $(a_1, \ldots, a_n) \le (b_1, \ldots, b_n) :\iff a_i \le b_i$, $\forall i$. U tom je slučaju segment $[(a_1, \ldots, a_n), (b_1, \ldots, b_n)]$ u P izomorfan s produktom lanaca $(\underline{b_1} - \underline{a_1} + \underline{1}) \times \cdots \times (\underline{b_k} - \underline{a_k} + \underline{1})$, pa iz Primjera 11. i produktne formule slijedi

$$\mu((a_1, \ldots, a_k), (b_1, \ldots, b_k)) = \begin{cases} (-1)^{\sum(b_i - a_i)} & \text{, ako je svaki } b_i - a_i = 0 \text{ ili } 1, \\ 0 & \text{, inače.} \end{cases}$$

Stoga dobivamo da za $r \le s$ u D_N (tj. $r \mid s$) vrijedi

$$\mu(r, s) = \begin{cases} (-1)^t & \text{, ako je } s/r \text{ produkt } t \text{ različitih prostih brojeva,} \\ 0 & \text{, inače.} \end{cases}$$

pa je $\mu(r, s) = \overline{\mu}(s/r)$ (vidi Primjer 13.). Formula inverzije je

$$g(n) = \sum_{d|n} f(d) \iff f(n) = \sum_{d|n} g(d)\overline{\mu}(n/d), \ \forall n \mid N.$$

□

Izvedimo neka posebna svojstva Möbiusove funkcije za rešetke.

PROPOZICIJA 9. *Neka je L rešetka, $a \le b \in L$ i neka su 0 i 1 redom minimalni i maksimalni element u L. Tada vrijedi*

$$a) \sum_{x \vee a = b} \mu(0, x) = 0 \quad (a > 0); \qquad b) \sum_{x \wedge b = a} \mu(x, 1) = 0 \quad (b < 1).$$

Dokaz. a) Indukcijom po broju elemenata između a i b (tj. u segmentu $[a, b]$). Ako je $a = b$, ta suma je $\sum_{x \le b} \mu(0, x)$, a to je 0 zbog (28). Ako je $a < b$, onda imamo

$$\sum_{x \le b} \mu(0, x) = \sum_{a \le b_1 \le b} \left(\sum_{a \vee x = b_1} \mu(0, x) \right).$$

Lijeva strana je 0 (opet zbog (28)), a sve unutrašnje sume su 0 za $b_1 < b$ prema pretpostavci indukcije. Stoga je 0 i unutarnja suma za $b_1 = b$.
b) Slično kao a) ili pomoću a) tako da parcijalni uređaj okrenemo "naglavačke", tj. $x \le' y \iff y \le x$. Tada se lako vidi da je za $(L, \le')$ Möbiusova funkcija $\mu'(x, y) = \mu_L(y, x)$. □

Primjer 16. Neka je $\Pi(S)$ p.u. skup particija skupa S s profinjenjem kao uređajem, a $\Pi_n = \Pi([n])$. Odredite polinom ranga i Möbiusovu funkciju za tu rešetku.

Rješenje. Kako smo već rekli, Π_n je graduiran ranga $n-1$. Rang particije $\pi \in \Pi_n$ je $r(\pi) = n - (\text{broj blokova od } \pi) = n - |\pi|$. Stoga je polinom ranga te rešetke

$$F(\Pi_n, q) = \sum_{k=0}^{n-1} S(n, n-k) q^k, \tag{30}$$

gdje je $S(n, n-k)$ Stirlingov broj druge vrste.

U rešetki Π_n, minimalni element $\hat{0}$ je particija $\{\{1\}, \{2\}, \ldots, \{n\}\}$, a maksimalni element $\hat{1}$ je particija od jednog bloka – čitav skup $\{1, 2, \ldots, n\}$. Za bilo koje particije $\sigma, \pi \in \Pi_n$, $\sigma \le \pi$, neka je $\pi = \{B_1, B_2, \ldots, B_k\}$ i neka je B_i particioniran u λ_i blokova iz σ. Tada se lako pokaže da je kao p.u. skup segment $[\sigma, \pi] \cong \Pi_{\lambda_1} \times \Pi_{\lambda_2} \times \cdots \times \Pi_{\lambda_k}$. Posebno, ako je π particija tipa $t(\pi) = (t_1, t_2, \ldots)$, tj. ima t_i blokova veličine i, onda je $[\hat{0}, \pi] \equiv \Pi_1^{t_1} \times \cdots \times \Pi_n^{t_n}$.

Označimo $\mu_n = \mu(\hat{0}, \hat{1})$, gdje je μ Möbiusova funkcija od Π_n. Tada je zbog produktne formule $\mu(\sigma, \pi) = \mu_{\lambda_1} \mu_{\lambda_2} \ldots \mu_{\lambda_k}$. Prema tome, za potpuno određivanje μ, dovoljno je znati μ_n. Ako u Propoziciji 9 b) uzmemo da je $b \in \Pi_n$ particija $b = \{\{1\}, \{2, \ldots, n\}\}$, onda iz $\sum_{x \wedge b = \hat{0}} \mu(x, \hat{1}) = 0$ slijedi $\mu(\hat{0}, \hat{1}) = -\sum \mu(x, \hat{1})$, gdje se sumira po svim $x \ne \hat{0}$, $x \wedge b = \hat{0}$. Odredimo sve takve x. Neka je $x = \{A_1, \ldots, A_p\}$ takva particija od $[n]$. Ako je npr. $1 \in A_1$, onda zbog $x \wedge b = \hat{0}$ mora biti $A_i = A_i \cap \{2, \ldots, n\}$ za $i > 1$, pa je zato $|A_i| = 1$. Ali zbog $x \ne \hat{0}$ je $|A_1| \ge 2$. Opet zbog $x \wedge b = \hat{0}$, gledamo li $A_1 \cap \{2, \ldots, n\}$, vidimo da mora biti $|A_1| = 2$. Stoga je $x = \{\{1, i\}, \{2\}, \ldots, \{i-1\}, \{i+1\}, \ldots, \{n\}\}$, za neko $i \in \{2, \ldots, n\}$. Segment $[x, \hat{1}]$ u Π_n je očito izomorfan rešetki particija Π_{n-1} od $n-1$ elemenata ($\{1, i\}$ je jedan blok). Stoga dobivamo

$$\mu_n = \mu(\hat{0}, \hat{1}) = -\sum \mu(x, \hat{1}) = -(n-1)\mu_{n-1},$$

a odavde i iz $\mu_0 = 1$ zaključujemo

$$\mu_n = (-1)^{n-1}(n-1)!. \tag{31}$$

Na drugi se način ta važna formula dobije iz sljedećeg identiteta, izjednačavanjem koeficijenta uz q:

$$\sum_{\pi\in\Pi_n}\mu(\hat{0},\pi)q^{|\pi|}=q^{\underline{n}}=q(q-1)\dots(q-n+1).$$

□

Napomenimo da se i općenito za konačni graduirani p.u. skup P s $\hat{0}$ ranga n definira **karakteristični polinom p.u. skupa** P formulom

$$\chi(P,q)=\sum_{x\in P}\mu(\hat{0},x)q^{n-r(x)}=\sum_{k=0}^{n}w_kq^{n-k},$$

gdje je $w_k=\sum_{x\in P,r(x)=k}\mu(\hat{0},x)$ koeficijent uz x^{n-k} i zove se k-ti **Whitneyev broj prve vrste p.u. skupa** P. Broj elemenata iz P ranga k zove se k-ti **Whitneyjev broj druge vrste p.u. skupa** P i označava s W_k. Stoga je polinom ranga od P jednak

$$F(P,q)=\sum_{x\in P}q^{r(x)}=\sum_{k=0}^{n}W_kq^k.$$

Iz (30) slijedi da je $\chi(\Pi_n,q)=(q-1)(q-2)\dots(q-n+1)$, jer je Π_n ranga $n-1$, a $|\pi|=n-r(\pi)$. Stoga iz formule (29) u pogl. II. dobivamo $w_k=s(n,n-k)$ Stirlingov broj prve vrste, a iz (30) slijedi $W_k=S(n,n-k)$ za rešetku Π_n.

Prije idućeg primjera treba nam jedan pojam. **Geometrijska rešetka** je (konačna) rešetka L čiji je svaki element oblika $x_1\vee x_2\vee\dots\vee x_k$, gdje su $x_i\in L$ atomi (elementi koji natkrivaju 0) i ako x natkriva $x\wedge y$, onda $x\vee y$ natkriva y. Nije teško provjeriti da za takvu rešetku za rang vrijedi $r(x)+r(y)\geq r(x\vee y)+r(x\wedge y)$, $\forall x,y\in L$. Element koji je natkriven s 1 zove se **koatom**.

KOROLAR 7. *U konačnoj geometrijskoj rešetki L ranga n, za svaki atom $a\in L$ vrijedi*

$$\mu(0,1)=-\sum_{\substack{x\vee a=1\\ 1\neq x\not\geq a}}\mu(0,x). \tag{32}$$

Dokaz. Ako je $a\leq x$, onda je $x=1$. Stoga je ili $x\wedge a=0$ ili $x=1$. Iz $r(x)+r(a)\geq r(x\wedge a)+r(x\vee a)$ slijedi da je ili $x=1$ ili $r(x)+1\geq 0+n$, pa je ili $x=1$ ili $x\vee a=1$, tj. x koatom. Stoga iz Propozicije 9 a) iz $\sum_{a\vee x=1}\mu(0,x)=0$ tvrdnja neposredno slijedi. □

Primjer 17. Neka je $L_n=L_n(q)$ p.u. skup vektorskih potprostora n-dimenzionalnog prostora V_n nad poljem $\mathbb{F}_q$ od q elemenata uređenih inkluzijom. Odredite Möbiusovu funkciju i Möbiusovu inverziju primijenite na prebrojavanje linearnih injekcija $V_n\to X$, gdje je X vektorski prostor na $\mathbb{F}_q$ koji ima x vektora.

Rješenje. L_n je rešetka ranga n, pri čemu je rang potprostora $W\subseteq V_n$ jednak $r(W)=\dim W$. Nadalje, svaki potprostor je razapet svojim 1-dimenzionalnim potprostorima (to su atomi), a za potprostore $W,W'\subseteq V_n$ iz linearne algebre znamo da je $\dim W+\dim W'=\dim(W\cap W')+\dim(W+W')$. Stoga je L_n geometrijska (i modularna) rešetka. Svaki segment $[W,W']$ u L_n je kao p.u. skup izomorfan s rešetkom potprostora kvocijentnog prostora W'/W. Naime, ako pođemo od neke baze od W, onda je nadopunimo do baze (e_i) od W' i linearnim operatorom $A:W'\to W'$, $A(e_i)=0$ za $i\leq\dim W$, $A(e_i)=e_i$ inače, definiramo izomorfizam p.u. skupova $[W,W']\approx[0,W'/W]$, $U\mapsto A(U)/W$. Stoga je $[W,W']\cong L_m$, gdje je $m=\dim W'-\dim W$, pa $\mu(W,W')$ ovisi samo o broju m. Dakle, dovoljno je izračunati $\mu_n=\mu(L_n)$. U tu svrhu neka je a atom, tj. element iz L_n ranga 1. Elemenata $1\neq x\in L_n$ za koje je $x\vee a=1$ (tj. koatoma) ima $\binom{n}{n-1}_q=q^{n-1}+q^{n-1}+\dots+q+1$, a od tih njih iznad a ima $\binom{n-1}{n-2}_q=q^{n-2}+q^{n-3}+\dots+1$. Stoga koatoma x za koje je $x\not\geq a$ ima q^{n-1}. Sada iz (32) odmah dobivamo $\mu_n=-q^{n-1}\mu_{n-1}$, što zajedno s početnim uvjetom $\mu_0=1$ konačno daje

$$\mu_n=(-1)^nq^{\binom{n}{2}}. \tag{33}$$

Linearnih injektivnih operatora $V_n\to X$ s jedne strane ima (vidi pogl. II. Lema 1). $[n^{\underline{x}}]_q=\prod_{k=0}^{n-1}(x-q^k)$. S druge strane, za potprostor $U\subseteq V_n$, neka je $f_=(U)$ broj linearnih operatora $A:V_n\to X$ za koje je jezgra $\operatorname{Ker}A=U$, a $f_\geq(U)$ broj onih za koje je $\operatorname{Ker}A\supseteq U$. Tada vrijedi $f_\geq(U)=\sum_{W\supseteq U}f_=(W)$. Iz Möbiusove inverzije tada slijedi

$$[n^{\underline{x}}]_q=f_=(\{0\})=\sum_W f_\geq(W)\mu(0,W).$$

Ako je $\dim W=k$, onda je $f_\geq(W)=x^{n-k}$. Iz (33) je $\mu(0,W)=(-1)^kq^{\binom{k}{2}}$, a budući da ima $\binom{n}{k}_q$ potprostora dimenzije k, dobivamo

$$[n^{\underline{x}}]_q=\sum_{k=0}^{n}(-1)^kq^{\binom{k}{2}}\binom{n}{k}_q x^{n-k}.$$

Izjednačavanjem dvaju rezultata dobivamo

$$\prod_{k=0}^{n-1}(x-q^k)=\sum_{k=0}^{n}(-1)^kq^{\binom{k}{2}}\binom{n}{k}_q x^{n-k}.$$

Ovo vrijedi za beskonačno vrijednosti x, pa vrijedi i kao jednakost polinoma (u varijabli x).

Stavimo li ovdje $x=-y/z$, nakon množenja sa z^n dobivamo

$$\prod_{k=0}^{n-1}(y+zq^k)=\sum_{k=0}^{n}\binom{n}{k}_q q^{\binom{k}{2}}y^{n-k}z^k. \tag{34}$$

Ova se jednakost zove **q-binomna formula**, jer za $q=1$ prelazi u običnu. Ako u (34) stavimo $y=1$, uzmemo $|q|<1$ (što smijemo, jer (34) vrijedi za beskonačno mnogo q-ova, pa je to jednakost polinoma u q, pa vrijedi za svako q), te pustimo da $n\to\infty$, onda iz (34) dobivamo tzv. q-identitet

$$\prod_{k=0}^{\infty}(1+zq^k)=\sum_{k=0}^{\infty}(1-q)\dots(1-q^k)q^{\binom{k}{2}}z^k.$$

□

Sljedećom Propozicijom ćemo dati jedan važan način računanja Möbiusove funkcije naročito u geometriji i topologiji. No prije toga se vratimo zeta funkciji $\zeta \in A(P)$; $\zeta(x,y) = 1$ za $x \leq y$, $\zeta(x,y) = 0$ inače; $\zeta\mu = \delta$. ($\delta(x,y) = 1$ za $x = y$, a $\delta(x,y) = 0$ inače). Tada je

$$\mu = \zeta^{-1} = (\delta + (\zeta - \delta))^{-1},$$

a odavde "razvojem u geometrijski red" dobivamo

$$\mu = \sum_{k \geq 0} (-1)^k (\zeta - \delta)^k.$$

Ova je suma konačna ako je P konačan, a ima smisla i za lokalno konačne P. No, kako je očito

$$(\zeta - \delta)(x,y) = \begin{cases} 1 & , \text{za } x < y, \\ 0 & , \text{za } x = y, \\ 0 & , \text{inače.} \end{cases}$$

slijedi da je

$$(\zeta - \delta)^2(x,y) = (\zeta - \delta)(\zeta - \delta)(x,y) = \sum_{x<z<y} 1 = \begin{array}{l}\text{broj lanaca } x < z < y \\ \text{duljine 2 od } x \text{ do } y.\end{array}$$

Tako se indukcijom po k lako vidi da je i $(\zeta - \delta)^k(x,y)$ jednak broju lanaca $x = x_0 < x_1 < \cdots < x_k = y$ duljine k od x do y. Odavde slijedi:

PROPOZICIJA 10. *Neka je P lokalno konačni p.u. skup, $x, y \in P$, a C_k broj lanaca $x = x_0 < x_1 < \cdots < x_k = y$ duljine k od x do y. Tada je $\mu(x,y) = C_0 - C_1 + C_2 - C_3 + \ldots$*

Dokaz. Imamo

$$\begin{aligned} \mu(x,y) &= (\delta + (\zeta - \delta))^{-1}(x,y) = (\delta - (\zeta - \delta) + (\zeta - \delta)^2 - \ldots)(x,y) = \\ &= \delta(x,y) - (\zeta - \delta)(x,y) + (\zeta - \delta)^2(x,y) - \cdots = \\ &= C_0 - C_1 + C_2 - \ldots. \end{aligned}$$

□

Izlet u topologiju i geometriju

Prvo se podsjetimo nekih pojmova. d-dimenzionalni **simpleks** (kraće d-simpleks) Δ^k je konveksna ljuska od $d+1$ točaka $\{x_0, x_1, \ldots, x_d\} \subset \mathbb{R}^n$ ($n \geq d$) u općem položaju (tj. vektori $x_1 - x_0, \ldots, x_d - x_0$ su linearno nezavisni u $\mathbb{R}^n$). Tako su simpleksi dimenzije 0, 1, 2, 3 redom točka, dužina, trokut, tetraedar. Točke $x_0, x_1, \ldots, x_d$ se zovu **vrhovi**, dužine $x_i x_j$ **bridovi** i općenito skup $\{x_{i_1}, \ldots, x_{i_{k+1}}\}$ od $k+1$ vrhova se zove k-dimenzionalna **strana** (kratko k-**strana**) **simpleksa**. Uočite da je svaka strana simpleksa opet simpleks i da je broj k strana u d-simpleksu

Δ^d jednak $\binom{d+1}{k+1}$. **Rub** $\partial\Delta^d$ je unija svih strana od Δ^d. Općenitiji je pojam **simplicijalni kompleks**. To je familija (skup) simpleksa (u nekom $\mathbb{R}^n$) tako da se svaka dva simpleksa sijeku duž neke zajedničke strane.

Poučeni ovim, definiramo i (apstraktni) **simplicijalni kompleks** Δ na skupu **vrhova** V kao familiju podskupova od V s ova dva svojstva: a) $\{x\} \in \Delta$, $\forall x \in V$; b) ako je $S \in \Delta$, onda je i $T \in \Delta$, $\forall T \subseteq S$. Element $S \in \Delta$ se zove **strana** od Δ, a **dimenzija strane**S se definira kao $\dim S := |S| - 1$, posebno je prazan skup strana od Δ i $\dim \emptyset = -1$. **Dimenzija** od Δ je $\dim \Delta := \max_{S \in \Delta}(\dim S)$. Ako je Δ konačan, definiramo $f_k = f_k(\Delta)$ kao broj k-dimenzionalnih strana (kratko k-**strana**) od Δ, $k \geq 0$. Ako je $d = \dim \Delta$, onda se slog $f = (f_0, f_1, f_2, \ldots, f_d)$ zove f-**vektor** ("face-vector") od Δ. Alternirana suma

$$\chi(\Delta) := \sum_{k \geq 0} (-1)^k f_k = f_0 - f_1 + f_2 - \cdots + (-1)^d f_d, \tag{35}$$

se naziva **Eulerova karakteristika simplicijalnog kompleksa** Δ, a $\tilde{\chi}(\Delta) = \chi(\Delta) - 1$ **reducirana Eulerova karakteristika** od Δ.

Ako je $(P, \leq)$ neki p.u. skup, onda mu na prirodan način pridružimo (apstraktni) simplicijalni kompleks $\Delta = \Delta(P)$ ovako: vrhovi od $\Delta(P)$ su elementi od P, a strane od $\Delta(P)$ su lanci u P. $\Delta(P)$ se zove **uređajni kompleks** od $(P, \leq)$. Ako dodamo $\hat{0}$ i $\hat{1}$ (umjetne 0 i 1) i formiramo $\hat{P} = P \cup \{\hat{0}, \hat{1}\}$, onda iz Propozicije 10 i (35) zaključujemo

$$\mu_{\hat{P}}(\hat{0}, \hat{1}) = \tilde{\chi}(\Delta(P)).$$

Dakle, Möbiusova funkcija p.u. skupa je zapravo (reducirana) Eulerova karakteristika pridruženog uređajnog kompleksa.

S druge strane, svakom apstraktnom simplicijalnom kompleksu Δ pridružen je topološki prostor $X = |\Delta|$ koji se naziva **geometrijska realizacija** od Δ (a Δ **triangulacija** od X). To je naprosto unija odgovarajućih simpleksa u nekom $\mathbb{R}^N$ (ako je Δ konačan). Reducirana Eulerova karakteristika $\tilde{\chi}(X)$ topološkog prostora X u topologiji se definira kao

$$\tilde{\chi}(X) = \sum_{k \geq 0} (-1)^k \operatorname{rang} \tilde{H}_k(X; \mathbb{Z}),$$

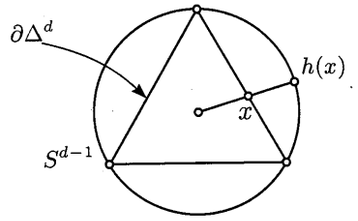
gdje je $\tilde{H}_k(X; \mathbb{Z})$ tzv. reducirana k-ta grupa homologije prostora X. Stoga je $\tilde{\chi}(X) = \tilde{\chi}(\Delta)$, pa Möbiusova funkcija $\mu_{\hat{P}}(\hat{0}, \hat{1})$ ovisi samo o geometrijskoj realizaciji $|\Delta(P)|$ od $\Delta(P)$, tj. o topološkoj strukturi. Ovo je jedna od vrlo važnih veza "diskretne" i "neprekidne" matematike. (O grupama homologije i sl. zainteresiranog čitatelja upućujemo na neki udžbenik iz algebarske topologije, npr. J. R. Munkres, Elements of Algebraic Topology, Addison-Wesley, Menlo Park CA, 1984.).

Primjer 18. Neka je B_{d+1} Booleova algebra podskupova $(d+1)$-članog skupa s inkluzijom kao uređajem. Odredite uređajni kompleks $\Delta(B_{d+1})$, geometrijsku realizaciju $|\Delta(B_{d+1})|$ i primijenite na to Möbiusovu funkciju.

Rješenje. Neka je $V = \{v_0, v_1, \ldots, v_d\}$. Tada je B_{d+1} izomorfan p.u. skupu svih podskupova od V. Stoga su vrhovi od $\Delta(B_{d+1})$ elementi od V, a strane simplicijalnog kom-

pleksa $\Delta(B_{d+1})$ su lanci u B_{d+1}. Maksimalan lanac u B_{d+1} je oblika $\emptyset \subset \{v_i\} \subset \{v_i, v_j\} \subset \cdots \subset V$, a svaki lanac u B_{d+1} je podlanac ovakvog maksimalnog.

Geometrijski, to je isto kao i rub $\partial\Delta^d$ d-simpleksa Δ^d sa skupom vrhova V, tj. $\Delta(B_{d+1})$ čine sve strane tog simpleksa osim samog simpleksa Δ^d (sve strane osim $\emptyset$ i Δ^d zovu se **prave strane**). Geometrijska realizacija $|\Delta(B_{d+1})|$ je dakle rub d-simpleksa $\partial\Delta^d$, a taj je homeomorfan $(d-1)$-dimenzionalnoj sferi $S^{d-1} = \{(x_1, x_2, \ldots, x_d) \in \mathbb{R}^d | x_1^2 + x_2^2 + \cdots + x_d^2 = 1\}$. Homeomorfizam (neprekidna bijekcija s neprekidnim inverzom) $h : \partial\Delta^d \to S^{d-1}$ ruba $\partial\Delta^d$ i sfere S^{d-1} je npr. radijalna projekcija; za $d = 2$ kao na slici:



Kako već znamo da je Möbiusova funkcija μ na B_{d+1} dana s $\mu(\emptyset, [d+1]) = (-1)^{d+1}$ (vidi Primjer 12), to iz prethodne diskusije lako dobivamo da je Eulerova karakteristika sfere

$$\chi(S^{d-1}) = 1 + (-1)^{d-1}. \tag{36}$$

(Ovo je u skladu s poznatom činjenicom iz topologije da su grupe homologije $\tilde{H}_k(S^{d-1}; \mathbb{Z}) \approx \mathbb{Z}$ ako je $k = d-1$ i 0 inače.) □

U geometriji se definira **konveksni d-dimenzionalni politop** P (kratko **d-politop** ili **d-poliedar**) kao omeđeni skup u $\mathbb{R}^d$ dobiven kao presjek konačno mnogo zatvorenih poluprostora određenih s hiperravninama (ili nadravninama) $H_1, H_2, \ldots, H_s$ u općem položaju. **Strane politopa** P su $P \cap H_i$, i to su $(d-1)$-dimenzionalne strane ili **facete** (ili **nadstrane**). Faceta od P je $(d-1)$-politop. Njezine facete su $(d-2)$-dimenzionalne strane od P i tako d **bridova** (1-strane) i **vrhova** (0-strane). Skup $\mathcal{F}(P)$ svih strana uređenih inkluzijom čini rešetku strana od P s najmanjim elementom praznom stranom $\emptyset$ dimenzije -1 i najvećom stranom P. **Rub** ∂P od P (tj. unija pravih strana) je također homeomorfan sferi S^{d-1}. **f-vektor** od P je $f = (f_0, f_1, \ldots, f_{d-1}) \in \mathbb{N}_0^d$, gdje je $f_k = f_k(P)$ broj k-strana od P. Pokazuje se (među ostalim rabeći i (36)) da za svaki d-politop P vrijedi **Euler-Poincaréova formula** (za dokaz vidi npr. [98]]):

$$\chi(P) = \sum_{k=0}^{d-1} (-1)^k f_k = 1 + (-1)^{d-1}. \tag{37}$$

Politop P je **simplicijalan** ako mu je svaka prava strana (tj. osim $\emptyset$ i P) simpleks. U dimenziji $d = 3$ su npr. tetraedar, oktaedar i ikozaedar simplicijalni.

Primjer 19. Möbiusova funkcija μ rešetke $\mathcal{F}(P)$ bilo kojeg d-politopa P ima vrijednost

$$\mu(0, 1) = (-1)^{d+1}.$$

Rješenje. Neka je $x \in \mathcal{F}(P)$ bilo koja prava strana od P. Tada je segment $[0, x]$ u $\mathcal{F}(P)$ kao p.u. skup izomorfan rešetki strana od x, tj $\mathcal{F}(x)$. Pretpostavimo induktivno da je

$\mu(0, x) = (-1)^{d-d(x)}$, gdje je $d(x) = \dim(x)$, za svaku stranu $x \neq 1$. Tada iz (28) i (37) slijedi

$$\mu(0, 1) = -\sum_{x \neq 1} \mu(0, x) = \sum_{x \neq 1} (-1)^{d(x)} = \sum_{k=-1}^{d-1} (-1)^k f_k = (-1)^{d+1}.$$

□

PROPOZICIJA 11 (Dehn[7]-Sommervilleove[8] jednakosti; 1927.). *Neka je P simplicijalni d-politop. Za svaku stranu x od P označimo s $f_k(x)$ broj k-strana od P koje sadrže x i $d(x) = \dim x$. Tada za svako $k \leq d-1$ vrijedi*

$$(-1)^{d-1} f_k(x) = \sum_{j=k}^{d-1} (-1)^j \binom{j - d(x)}{k - d(x)} f_j(x). \tag{38}$$

Posebno, za $x = \emptyset$, $d(\emptyset) := -1$, $f_k(\emptyset) = f_k =$ broj k-strana od P, dobivamo

$$(-1)^{d-1} f_k = \sum_{j=k}^{d-1} (-1)^j \binom{j+1}{k+1} f_j. \tag{39}$$

Za $k = -1$ i $f_{-1} := 1$, (39) se svodi na Euler-Poinaréovu formulu (37) za simplicijalne politope.

Dokaz. Promotrimo rešetku $\mathcal{F}(P)$ simplicijalnog d-politopa P. Kako je svaka strana od P simpleks i svaka strana od x također simpleks i kako svaki podskup vrhova simpleksa definira stranu simpleksa, zaključujemo da je svaki segment $[x, y]$ iz $\mathcal{F}(P)$ kao p.u. skup izomorfan p.u. skupu svih podskupova $(d(y) - d(x))$-članog skupa, tj. Booleovoj algebri ranga $d(y) - d(x)$. Zato je Möbiusova funkcija μ za rešetku $\mathcal{F}(P)$ dana s

$$\mu(x, y) = (-1)^{d(y)-d(x)}, \text{ za } x \leq y.$$

Posebno je $\mu(y, P) = (-1)^{d-d(y)}$, za svaku stranu y politopa P. Sada za čvrsto $x \in \mathcal{F}(P)$, $x \neq P$, $d(x) = k < d$ računajmo:

$$\begin{aligned}
(-1)^{d-k} f_k(x) &= \sum_{\substack{y \geq x \\ d(y)=k}} (-1)^{d-d(y)} = \sum_{\substack{y \geq x \\ d(y)=k}} \mu(y, P) = \\
&= \Big(\text{zbog (28): } \mu(y, P) = -\sum_{y \leq z < P} \mu(y, z)\Big) = \\
&= -\sum_{\substack{y \geq x \\ d(y)=k}} \sum_{y \leq z < P} \mu(y, z) = -\sum_{\substack{x \leq y \leq z \\ d(y)=k}} \mu(y, z) = \\
&= -\sum_{\substack{x \leq y \leq z \\ d(y)=k}} (-1)^{d(z)-d(y)} = -\sum_{j \geq k} \sum_{\substack{x \leq y \leq z \\ d(y)=k \\ d(z)=j}} (-1)^{j-k}.
\end{aligned}$$

[7]Max Dehn (1878 – 1952), njemački matematičar
[8]Duncan M. Y. Sommerville (1872 – 1934), engleski matematičar

Sada u unutrašnjoj sumi za čvrsto j, z možemo odabrati na $f_j(x)$ načina, a onda y na $\binom{j-d(x)}{k-d(x)}$ načina, pa dakle ukupno parova $y \le z$ na $\binom{j-d(x)}{k-d(x)} f_j(x)$ načina. Zato konačno dobivamo

$$(-1)^{d-k} f_k(x) = -\sum_{j \ge k} (-1)^{j-k} \binom{j-d(x)}{k-d(x)} f_j(x),$$

a odavde slijedi (38). □

Dehn-Sommervilleove jednakosti (39) se mogu i ljepše zapisati:

$$f_{k-1} = \sum_{j=k}^{d} (-1)^{d-j} \binom{j}{k} f_{j-1},$$

posebno, recimo, za $k = d-1$ dobivamo $2f_{d-2} = df_{d-1}$. No još elegantnije se one mogu zapisati pomoću tzv h-**vektora** $h = (h_0, h_1, \ldots, h_d) \in \mathbb{Z}^{d+1}$ simplicijalnog politopa P. Naime, prvo definiramo f-**polinom** d-**politopa** kao

$$f(x) = \sum_{i=0}^{d} f_{i-1} x^{d-i}.$$

Tada je h-**polinom** od P definiran s

$$h(x) = \sum_{i=0}^{d} h_i x^{d-i} := f(x-1).$$

Sada iz $f(x) = h(x+1)$ slijedi

$$\sum_{i=0}^{d} h_i (x+1)^{d-i} = \sum_{i=0}^{d} f_{i-1} x^{d-i},$$

pa nakon razvoja $(x+1)^{d-i}$ po binomnoj formuli i usporedbom koeficijenata uz x^{d-k} dobivamo

$$h_k = \sum_{i=0}^{k} (-1)^{k-i} \binom{d-i}{d-k} f_{i-1}, \qquad f_{k-1} = \sum_{i=0}^{k} \binom{d-i}{k-i} h_i.$$

Dakle, poznavanje f-vektora i h-vektora od P je ekvivalentno. Posebno dobivamo $h_0 = 1$, $h_1 = f_0 - d$, $h_d = f_{d-1} - f_{d-2} + f_{d-3} - \cdots + (-1)^{d-1} f_0 + (-1)^d$. Vidimo da je $h_0 = h_d$, jer je to Euler-Poincaréova formula (37). Indukcijom po k se može pokazati da su Dehn-Sommervilleove jednakosti ekvivalentne s:

$$h_k = h_{d-k}, \text{ za } k = 0, 1, \ldots, d, \tag{40}$$

a ovo je ekvivalentno s **formulom dualiteta za** h**-polinome**:

$$x^d h(1/x) = h(x). \tag{41}$$

Pokazuje se da ovakvi "dualiteti" vrijede i za tzv. **Eulerov p.u. skup** P, tj. konačni graduirani p.u. skup s 0 i 1, za koji je Möbiusova funkcija $\mu_P(x,y) = (-1)^{\ell(x,y)}$, gdje je $\ell(x,y)$ duljina segmenta $[x,y]$ za $x \le y$.

Povijesna bilješka. Prvu najavu Möbiusove inverzije nalazimo u Eulerovim radovima. On je pošao od dobro poznatog reda

$$\frac{\pi^2}{6} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \frac{1}{6^2} + \frac{1}{7^2} + \ldots.$$

Formalnim invertiranjem dobio je

$$\frac{6}{\pi^2} = 1 - \frac{1}{2^2} - \frac{1}{3^2} - \frac{1}{5^2} + \frac{1}{6^2} - \frac{1}{7^2} + \frac{1}{10^2} \pm \ldots,$$

što je (uz oznaku $\mu(n)$ = Möbiusova funkcija iz teorije brojeva):

$$\frac{6}{\pi^2} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^2}.$$

Möbius je 1832. otišao korak dalje i promatrao ovaj problem. Neka je zadana funkcija

$$f(x) = \sum_{j=1}^{\infty} a_j x^j.$$

Treba naći koeficijente b_k tako da je

$$x = \sum_{k=1}^{\infty} b_k f(x^k).$$

Iz $f(x^k) = \sum_{j=1}^{\infty} a_j x^{jk}$ onda slijedi

$$x = \sum_{k=1}^{\infty} b_k \sum_{j=1}^{\infty} a_j x^{jk} = \sum_{n=1}^{\infty} \left(\sum_{jk=n} a_j b_k \right) x^n,$$

pa je rješenje rekurzivno dano s

$$a_1 b_1 = 1$$

$$\sum_{jk=n} a_j b_k = 0, \ n > 1.$$

Tako npr. za $f(x) = x/(1-x) = x + x^2 + x^3 + \ldots$ je $a_j = 1$ za sve j, pa je $b_1 = 1$, a za $n > 1$ je $\sum_{d|n} b_d = 0$. Odavde slijedi da je $b_n = \mu(n)$. Slično, pođemo li od

$$f(x) = -\ln(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \ldots,$$

imamo da je $a_j = 1/j$. Tvrdimo da je $b_k = \mu(k)/k$. Naime, očito je $b_1 = 1$, a za $n > 1$ je

$$\sum_{jk=n} a_j b_k = \sum_{jk=n} \frac{1}{j}\frac{\mu(k)}{k} = \frac{1}{n}\sum_{k|n} \mu(k) = 0.$$

To daje

$$x = \sum_{k=1}^{\infty} \frac{\mu(k)}{k}(-\ln(1-x^k)),$$

a odavde formalnim eksponiranjem dobivamo lijepu formulu

$$e^x = \prod_{k=1}^{\infty} (1-x^k)^{-\mu(k)/k}.$$

U daljnjem razvoju te teorije treba spomenuti imena: R. Dedekind, L. Dirichlet, P. Hall, L. Weisner, G. C. Rota, R. P. Stanley i druge.

V. Funkcije izvodnice

§ 1. Osnovna ideja i jednostavni primjeri

Funkcija izvodnica je jedno od najmoćnijih računskih sredstava u kombinatorici. Grubo govoreći, nizu brojeva pridružimo red potencija čiji zbroj je neka (često neprekidna) funkcija koju zovemo pripadna funkcija izvodnica. Dakle, funkcija izvodnica kao jedan objekt zamjenjuje čitav niz brojeva, a svatko će se složiti da je lakše manipulirati s jednim objektom nego s beskonačno mnogo članova niza. Mnogi problemi s nizovima mogu se tada riješiti računanjem s funkcijama. Ideja funkcija izvodnica potječe od L. Eulera, J. Stirlinga i de Moivrea iz 18. stoljeća.

DEFINICIJA 1. *Neka je $a_0, a_1, a_2, \ldots, a_n, \ldots$ niz realnih (ili kompleksnih) brojeva. Pripadna obična* **funkcija izvodnica** *(kratko FI) je formalni red potencija*

$$A(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots = \sum_{n\geq 0} a_n x^n. \tag{1}$$

To ćemo često bilježiti oznakom $(a_n)_{n\geq 0} \overset{FI}{\longleftrightarrow} A(x)$. Također ćemo rabiti oznaku $\langle x^n\rangle A(x) = a_n$, koja znači da je **koeficijent** *od $A(x)$ uz x^n jednak a_n. Pripadna* **eksponencijalna funkcija izvodnica** *(kratko EFI) niza (a_n) je formalni red potencija*

$$E(x) = a_0 + \frac{a_1}{1!}x + \frac{a_2}{2!}x^2 + \cdots + \frac{a_n}{n!}x^n + \cdots = \sum_{n\geq 0} \frac{a_n}{n!}x^n. \tag{2}$$

To ćemo bilježiti oznakom $(a_n)_{n\geq 0} \overset{EFI}{\longleftrightarrow} E(x)$.

Slično imamo i funkcije izvodnice više varijabli, npr.

$$F(x,y,z) = \sum_{k\geq 0}\sum_{l\geq 0}\sum_{m\geq 0} x^k y^l z^m/m!$$

za niz $(a_{k,l,m})_{k,l,m\geq 0}$ (i možemo je smatrati "običnom" za indekse k i l, tj. u varijablama x i y, a "eksponencijalnom" za indeks m, tj. u varijabli z).

Ovi redovi potencija su "formalni" u smislu da nas ne zanima koje vrijednosti poprima varijabla x, te da ignoriramo pitanje njihove konvergencije. Stoga funkcije izvodnice ne smatramo običnim funkcijama, osim kad je varijabla u području konvergencije reda (a to ćemo prešutno pretpostavljati). Stoga ćemo uvijek (kad god je to moguće) nastojati funkciju izvodnicu prikazati eksplicitnim analitičkim izrazom

ili "zatvorenom formulom", tj. izračunati sumu reda. U tom slučaju koeficijente od (1) i (2) možemo računati kao u Taylorovoj formuli: $a_n = A^{(n)}(0)/n!$ i $a_n = E^n(0)$, pri čemu deriviramo formalno, tj. član po član.

S funkcijama izvodnicama možemo izvoditi razne prirodne operacije koje imaju kombinatorna značenja. Naime, osnovna pravila prebrojavanja prevodimo na jezik formalnih redova potencija ovako. Neka su $(a_n)_{n\geq 0}$, $(b_n)_{n\geq 0}$ dva niza (kompleksnih) brojeva s pridruženim funkcijama izvodnicama $A(x)$ i $B(x)$ redom, tj. $(a_n)_{n\geq 0} \leftarrow^{\text{FI}} A(x)$, $(b_n)_{n\geq 0} \overset{\text{FI}}{\longleftrightarrow} B(x)$. Tada imamo

1. **Pravilo jednakosti**: $A = B$ (tj. $A(x) = B(x)$, $\forall x$) $\iff$ $a_n = b_n$, $\forall n \geq 0$.
2. **Pravilo zbroja**: $A(x) + B(x) = (A + B)(x)$, tj.
$$(\sum_{n\geq 0} a_n x^n) + (\sum_{n\geq 0} b_n x^n) = \sum_{n\geq 0} (a_n + b_n) x^n.$$
3. **Pravilo množenja**: $A(x) \cdot B(x) = C(x)$, tj.
$$(\sum_{n\geq 0} a_n x^n) \cdot (\sum_{n\geq 0} b_n x^n) = \sum_{n\geq 0} c_n x^n,$$
gdje je $c_0 = a_0 b_0$, $c_1 = a_0 b_1 + a_1 b_0, \ldots$, $c_n = \sum_{i=0}^{n} a_i b_{n-i}$, $\ldots$

S ovim operacijama zbrajanja i množenja skup svih formalnih redova (nad $\mathbb{C}$) se označava s $\mathbb{C}[[x]]$ (a nad $\mathbb{R}$ s $\mathbb{R}[[x]]$) i nije teško provjeriti da čini integralnu domenu, tj. $\mathbb{C}[[x]]$ je komutativni prsten s jedinicom bez djelitelja nule. (S algebarskog stajališta, skup $\mathbb{C}[[x]]$ zapravo čini domenu glavnih ideala, pa stoga i domenu s jednoznačnom faktorizacijom; glavni ideali su oblika (x^n), za neko $n \geq 0$). Slično se definira i skup formalnih redova potencija u m varijabli $x_1, x_2, \ldots, x_m$ (m može biti i beskonačno) i označava s $\mathbb{C}[[x_1, \ldots x_m]]$ i čini domenu s jednoznačnom faktorizacijom (za $m \geq 2$ to nije i domena glavnih ideala).

Ako je $F(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{C}[[x]]$, a $\lambda \in \mathbb{C}$, onda je $\lambda F(x) = \sum_{n\geq 0} (\lambda a_n) x^n \in \mathbb{C}[[x]]$. Ako su $F(x)$ i $G(x)$ elementi od $\mathbb{C}[[x]]$ koji zadovoljavaju $F(x)G(x) = 1$, onda (na prirodan način) pišemo $G(x) = F(x)^{-1}$ (ovdje je 1 kraći zapis za formalni red $1 + 0 \cdot x + 0 \cdot x^2 + \ldots$). Lako se vidi da $F(x)^{-1}$ postoji (i jedinstven je) ako i samo ako je $a_0 \neq 0$, gdje je $F(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{C}[[x]]$. Često simbolički pišemo $a_0 = F(0)$ iako $F(x)$ nije funkcija od x.

Nadalje, ako je $F(x) = \sum_{n\geq 0} a_n x^n \in \mathbb{C}[[x]]$ formalni red potencija, tj. FI za niz $(a_n)_{n\geq 0}$, onda je **formalna derivacija** $F'(x)$ (ili dF/dx ili $DF(x)$) formalni red potencija $F'(x) = \sum_{n\geq 0} n a_n x^{n-1} = \sum_{n\geq 0} (n+1) a_{n+1} x^n$, tj. FI za niz $((n+1)a_{n+1})_{n\geq 0}$. Nije teško provjeriti da vrijede sva osnovna pravila za formalno deriviranje:

$$(F + G)' = F' + G', \qquad (FG)' = F'G + FG', \qquad F(G(x))' = G'(x)F'(G(x)).$$

Slično, **formalni integral** od $F(x) = \sum_{n\geq 0} a_n x^n$ je integral član po član:

$$\int_0^x F(t)dt = a_0 x + \frac{1}{2} a_1 x^2 + \cdots = \sum_{n\geq 1} \frac{1}{n} a_{n-1} x^n.$$

Primjer 1. Odredite FI za niz $(a_n)_{n\geq 0}$, ako je:
a) $a_n = 1$; b) $a_n = n$; c) $a_n = n^2$; d) $a_n = n^3$;
e) $a_n = \binom{\alpha}{n}$ (gdje je $\alpha \in \mathbb{C}$ zadani čvrsti broj); f) $a_n = 1/n (n \geq 1)$.

Rješenje. a) Pođimo od dobro poznatog geometrijskog reda (podsjetimo da on konvergira za $|x| < 1$, što prešutno pretpostavljamo):

$$1 + x + x^2 + \cdots + x^n + \cdots = \frac{1}{1-x}, \tag{3}$$

pa je očito $(1, 1, 1, \ldots) \overset{\text{FI}}{\longleftrightarrow} 1/(1-x)$.

b) Ako formalno deriviramo (3), dobivamo

$$1 + 2x + 3x^2 + \cdots + nx^{n-1} + \cdots = \frac{1}{(1-x)^2},$$

pa množenjem ove jednakosti s x dobivamo

$$x + 2x^2 + 3x^3 + \cdots + nx^n + \cdots = \frac{x}{(1-x)^2}. \tag{4}$$

c) Deriviranjem (4) i množenjem s x odmah se dobiva da je $(n^2) \overset{\text{FI}}{\longleftrightarrow} x(x+1)/(1-x)^3 = F_2(x)$.

d) Ako (formalno) deriviramo $F_2(x)$ i to pomnožimo s x, lako dobivamo $(n^3) \overset{\text{FI}}{\longleftrightarrow} (x^3 + 4x^2 + x)/(1-x)^4$.

e) Funkcija izvodnica za niz $a_n = \binom{\alpha}{n}$ je po definiciji jednaka $F_\alpha(x) = \sum_{n\geq 0} \binom{\alpha}{n} x^n$. No prema teoremu o binomnom redu, znamo da je $(1+x)^\alpha = \sum_{n\geq 0} \binom{\alpha}{n} x^n$ za $|x| < 1$ (što opet prešutno pretpostavljamo). Zato je funkcija izvodnica za niz $\binom{\alpha}{0}, \binom{\alpha}{1}, \binom{\alpha}{2}, \ldots$ jednaka $(1+x)^\alpha$.

f) Ako formalno integriramo geometrijski red $\sum_{n\geq 0} t^n = 1/(1-t)$, tj. "napadnemo" obje strane s $\int_0^x dt$, onda dobivamo

$$\sum_{n\geq 0} \frac{1}{n+1} x^{n+1} = \sum_{n\geq 1} \frac{1}{n} x^n = \ln \frac{1}{1-x}. \tag{5}$$

Stoga je $(1/n)_{n\geq 1} \overset{\text{FI}}{\longleftrightarrow} \ln 1/(1-x)$. □

Primjer 2. Neka je $N \geq 0$ zadan cijeli broj. Odredite FI za niz a_n, gdje je a_n broj n-kombinacija s ponavljanjem N-članog skupa.

Rješenje. Znamo da je broj n-kombinacija s ponavljanjem N-članog skupa (v. Propoziciju 10 u pogl. II) jednak

$$a_n = \binom{N+n-1}{n}.$$

Znamo također (zakon recipročnosti za binomne koeficijente) da je

$$\binom{N+n-1}{n} = (-1)^n \binom{-N}{n}.$$

Stoga je tražena funkcija izvodnica

$$F_N(x) = \sum_{n\geq 0}\binom{N+n-1}{n}x^n = \sum_{n\geq 0}(-1)^n\binom{-N}{n}x^n =$$
$$= \sum_{n\geq 0}\binom{-N}{n}(-x)^n = (1-x)^{-N} = \frac{1}{(1-x)^N}.$$

(Tu smo uporabili binomni red iz prethodnog primjera e) za $\alpha = -N$). □

U prethodnim smo primjerima imali zadane nizove brojeva i za njih našli FI u zatvorenoj formi, tj. analitičkim izrazom. No, prava korist funkcija izvodnica u kombinatorici je upravo u mogućnosti rješavanja obrnutog problema. Naime, ako tražimo broj a_n s nekim kombinatornim značenjem i ako uspijemo na neki način izračunati FI za taj niz, onda određivanjem koeficijenata uz x^n razvojem u red potencija (npr. Taylorovom formulom i sl.) te funkcije izvodnice dobijemo a_n. Pokažimo to nekim primjerima.

Primjer 3. Riješimo obrnuti problem iz prethodnog primjera. Dakle, za zadani $N \geq 0$, prvo odredite funkciju izvodnicu F_N za niz a_n brojeva n-kombinacija s ponavljanjem N-članog skupa i onda odredite a_n.

Rješenje. a_n je broj n-članih multiskupova od elemenata nekog N-članog skupa $S = \{x_1, x_2, \ldots, x_N\}$. U svakom takvom multiskupu, element x_1 se ili uopće ne pojavljuje ili se pojavljuje jedanput ili dvaput ili triput itd., pa to pišemo kao sumu $1 + x_1 + x_1^2 + x_1^3 + \ldots$, i slično za ostale x_i. Promotrimo produkt

$$(1 + x_1 + x_1^2 + \ldots)(1 + x_2 + x_2^2 + \ldots)\ldots(1 + x_N + x_N^2 + \ldots).$$

Svaki član tog produkta je oblika $x_1^{i_1}x_2^{i_2}\ldots x_N^{i_N}$. Nas zanima koliko ima takvih članova za koje je $i_1 + i_2 + \cdots + i_N = n$, i to s ne nužno različitim x-ovima, pa ih i ne želimo razlikovati. Stoga stavimo $x_1 = x_2 = \cdots = x_N = x$. Tada gornji produkt prelazi u traženu funkciju izvodnicu za kombinacije s ponavljanjem:

$$F_N(x) = (1 + x + x^2 + \ldots)^N = (\frac{1}{1-x})^N = (1-x)^{-N}.$$

Koeficijent a_n uz x^n je (iz binomnog reda):

$$a_n = \langle x^n\rangle(1-x)^{-N} = \binom{-N}{n}(-1)^n = \binom{N+n-1}{n}.$$

Time smo još jedanput (ovaj put s funkcijama izvodnicama) izveli formulu za broj kombinacija s ponavljanjem. □

Primjer 4. Na koliko se načina 24 (jednaka) bombona može razdijeliti među četvero djece tako da svako dijete dobije barem 3, ali ne više od 8 bombona?

Rješenje. Razdiobu bombona koje svako dijete može primiti prikažimo u obliku $x^3 + x^4 + \cdots + x^8$. Kako je riječ o četvero djece, to je pripadna funkcija izvodnica jednaka $f(x) = (x^3 + x^4 + \cdots + x^8)^4$. Traženi je broj jednak koeficijentu uz x^{24} od $f(x)$. Prvo je

$$f(x) = x^{12}(1 + x + x^2 + \cdots + x^5)^4 = x^{12}((1-x^6)/(1-x))^4,$$

pa je

$$\langle x^{24}\rangle f(x) = \langle x^{12}\rangle((1-x^6)/(1-x))^4 = \langle x^{12}\rangle(1-x^6)^4(1-x)^{-4} =$$
$$= \langle x^{12}\rangle\left[1 - \binom{4}{1}x^6 + \binom{4}{2}x^{12} - \ldots\right]\left[\binom{-4}{0} + \binom{-4}{1}(-x) + \binom{-4}{2}(-x)^2 + \ldots\right] =$$
$$\binom{-4}{12}(-1)^{12} - \binom{4}{1}\binom{-4}{6}(-1)^6 + \binom{4}{2}\binom{-4}{0} = \binom{15}{3} - 4\binom{9}{3} + \binom{4}{2} = 125.$$

□

Primjer 5. Na raspolaganju imamo 8 kovanica od jedne kune, 6 kovanica od dvije kune i 4 kovanice od pet kuna. Na koliko načina možemo isplatiti svotu od 14 kuna?

Rješenje. U svakoj isplati od 14 kuna sudjeluje neki broj (≥ 0) kovanica od jedne kune. Obilježimo jednu kunu s x. Tada kovanica od dvije kune ima vrijednost x^2, a kovanica od pet kuna x^5. Pripadna funkcija izvodnica isplate je jednaka

$$f(x) = (1 + x + x^2 + \cdots + x^8)(1 + x^2 + x^4 + x^6 + x^8 + x^{10} + x^{12})(1 + x^5 + x^{10} + x^{15} + x^{20}).$$

Traženi je broj jednak koeficijentu uz x^{14} od $f(x)$, tj. $\langle x^{14}\rangle f(x)$. Naime, nakon provedenih množenja, tipični član će biti oblika

$$x^{n_1+2n_2+5n_3},$$

pri čemu je $0 \leq n_1 \leq 8$, $0 \leq n_2 \leq 6$, $0 \leq n_3 \leq 4$. Svaki takav član daje jedan način isplate neke svote, a nas zanima isplata za koju je $n_1 + 2n_2 + 5n_3 = 14$.

Sada se traženi broj $\langle x^{14}\rangle f(x)$ lako izračunava (uz malo strpljiva računanja ili brže pogodnim kompjuterskim programom za množenje polinoma). Dobiva se $\langle x^{14}\rangle f(x) = 11$.

(Naravno, ovaj rezultat bismo mogli dobiti i listanjem svih mogućnosti, ali uvijek ostaje sumnja jesmo li neke izostavili. Ova metoda, međutim, daje sistematski način za takva računanja za mnogo složenija pitanja.) □

§ 2. Račun s funkcijama izvodnicama i neke primjene

Poopćenja prethodnog primjera upućuju na probleme oko particije broja. Podsjetimo (v. II §7.) da je **particija broja** $n \in \mathbb{N}$ prikaz broja n kao zbroja prirodnih brojeva (pri čemu je poredak nevažan). $p(n)$ je broj particija od n i po definiciji je $p(0) := 0$.

PROPOZICIJA 1. *Funkcija izvodnica za niz brojeva $p(0), p(1), \ldots, p(n), \ldots$ je (beskonačni) produkt*

$$P(x) = \prod_{k=1}^{\infty}\frac{1}{1-x^k}.$$

Ustvari, broj $p(n)$ je koeficijent uz x^n u produktu od konačno faktora:

$$p(n) = \langle x^n\rangle\prod_{k=1}^{m}\frac{1}{1-x^k}, \qquad m \geq n.$$

Dokaz. Znamo da je

$$\frac{1}{1-x^k} = 1 + x^k + x^{2k} + x^{3k} + \dots.$$

Stoga je koeficijent uz x^n u produktu

$$(1 + x + x^2 + \dots)(1 + x^2 + x^4 + \dots)(1 + x^3 + x^6 + \dots)(1 + x^4 + x^8 + \dots)\dots$$

jednak broju načina da se x^n prikaže kao $x^{k_1}x^{2k_2}\dots x^{nk_n} = x^{k_1+2k_2+\dots nk_n}$, tj. broju particija $p(n)$. Odatle slijedi tvrdnja. □

Pokažimo sada pomoću funkcija izvodnica Eulerov teorem (usp. Propozicija 16 d) u poglavlju II).

PROPOZICIJA 2 (Euler). *Broj particija $\bar{p}(n)$ od n u različite sumande jednak je broju particija $p_0(n)$ od n u neparne sumande.*

Dokaz. Neka je $\bar{P}(x) \overset{\text{FI}}{\longleftrightarrow} (\bar{p}(n))$, a $P_0(x) \overset{\text{FI}}{\longleftrightarrow} (p_0(n))$. Pokazat ćemo da su te funkcije izvodnice jednake, pa će stoga i koeficijenti uz x^n biti jednaki, tj. $\bar{p}(n) = p_0(n)$.

Za računanje broja $\bar{p}(n)$, svaki se prirodni broj k ili ne pojavljuje kao sumand od n ili se pojavljuje točno jedanput. To nam očito uračunava polinom $1 + x^k$. Stoga je

$$\bar{P}(x) = (1 + x)(1 + x^2)(1 + x^3)\cdots = \prod_{k=1}^{\infty}(1 + x^k).$$

S druge strane, očito je

$$P_0(x) = (1+x+x^2+x^3+\dots)(1+x^3+x^6+\dots)(1+x^5+x^{10}+\dots)(1+x^7+x^{14}+\dots)\cdots =$$

$$= \frac{1}{1-x}\cdot\frac{1}{1-x^3}\cdot\frac{1}{1-x^5}\cdot\frac{1}{1-x^7}\cdots.$$

Sada imamo (proširivanje, pa skraćivanje razlomaka u beskonačnom produktu)

$$\bar{P}(x) = (1 + x)(1 + x^2)(1 + x^3)(1 + x^4)\cdots = \frac{1-x^2}{1-x}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^6}{1-x^3}\cdot\frac{1-x^8}{1-x^4}\cdots =$$

$$= \frac{1}{1-x}\cdot\frac{1}{1-x^3}\cdot\frac{1}{1-x^5}\cdots = P_0(x).$$

Odatle slijedi tvrdnja. □

Nađimo još neke funkcije izvodnice i neke primjene.

Primjer 6. Neka je $H_n = 1 + 1/2 + \cdots + 1/n$ n-ti **harmonijski broj**.

a) Dokažite da je funkcija izvodnica za niz $(H_n)_{n\geq 1}$ dana s

$$H(x) = \sum_{n\geq 1} H_n x^n = \frac{1}{1-x}\ln\frac{1}{1-x}; \tag{6}$$

b) Dokažite da za harmonijske brojeve (osim očite rekurzije $H_{n+1} = H_n + 1/(n+1)$) vrijedi rekurzija s "potpunom prethistorijom":

$$\sum_{k=1}^{n} H_k = (n+1)(H_{n+1} - 1). \tag{7}$$

Rješenje. a) Znamo da je $1/(1-x) \overset{\text{FI}}{\longleftrightarrow} (1, 1, 1, \dots)$. Integriranjem dobivamo $\int_0^x (1-t)^{-1}dt = \ln(1-x)^{-1}$, tj. $\ln 1/(1-x) \overset{\text{FI}}{\longleftrightarrow} (0, 1, 1/2, \dots, 1/n, \dots)$. Množenjem s $1/(1-x)$ iz pravila produkta za funkcije izvodnice dobivamo odmah (6). Na drugi način, možemo postupiti i tako da očitu rekurziju $H_{n+1} = H_n + 1/(n+1)$ pomnožimo s x^{n+1}, sumiramo po $n \geq 1$ i uporabimo (5).

b) (7) možemo dobiti tako da "očitu" rekurziju $(k+1)H_{k+1} = (k+1)H_k + 1$ teleskopiramo od $k = 1$ do $k = n$. No, elegantnije je s funkcijama izvodnicama ovako. Prvo imamo

$$\frac{x}{1-x}H(x) = (x + x^2 + x^3 + \dots)(H_1 x + H_2 x^2 + H_3 x^3 + \dots) = \sum_{n\geq 1}(\sum_{k=1}^{n} H_k)x^{n+1}.$$

Deriviranjem $H(x)$ iz (6) dobivamo

$$H'(x) = \frac{1}{(1-x)^2}\ln\frac{1}{1-x} + \frac{1}{(1-x)^2},$$

pa je

$$xH'(x) = \frac{x}{1-x}H(x) + \frac{x}{(1-x)^2}.$$

Odavde, zbog (4), slijedi da je koeficijent uz x^{n+1} od $xH'(x)$ jednak

$$\langle x^{n+1}\rangle xH'(x) = \sum_{k=1}^{n} H_k + (n+1).$$

S druge strane, kako je

$$xH'(x) = \sum_{n\geq 1} nH_n x^n,$$

slijedi

$$\langle x^{n+1}\rangle xH'(x) = (n+1)H_{n+1}.$$

Izjednačavanjem ovih dvaju rezultata slijedi (7). □

Primjer 7. Dokažite da je FI za niz $a_n = \binom{2n}{n}$, $n \geq 0$, jednaka $(1-4x)^{-1/2}$.

Rješenje. Razvijemo po binomnom redu $(1-4x)^{-1/2}$. Imamo

$$\frac{1}{\sqrt{1-4x}} = (1-4x)^{-\frac{1}{2}} = \sum_{n\geq 0}\binom{-\frac{1}{2}}{n}(-4x)^n.$$

Kako je

$$\binom{-1/2}{n} = \frac{(-1/2)(-1/2-1)\dots(-1/2-n+1)}{n!} = (-1)^n\frac{1\cdot 3\cdot 5\cdot\dots\cdot(2n-1)}{2^n\cdot n!} =$$

$$= (-1)^n\frac{1\cdot 2\cdot 3\cdot 4\cdot\dots\cdot(2n-1)2n}{2^n\cdot n!\cdot 2\cdot 4\cdot\dots\cdot 2n} = (-1)^n\frac{(2n)!}{2^{2n}n!n!} = \frac{(-1)^n}{2^{2n}}\binom{2n}{n},$$

slijedi da je FI za niz $a_n = \binom{2n}{n}$ jednaka $(1-4x)^{-1/2}$. □

Primjer 8. Dokažite

$$\sum_{k=0}^{n} \frac{2k+1}{2^{2k}} \binom{2k}{k} = \frac{(2n+2)(2n+3)}{3 \cdot 4^{n+1}} \binom{2n+2}{n+1}.$$

Rješenje. Pođimo od $(1-4x)^{-1} \cdot (1-4x)^{-3/2} = (1-4x)^{-5/2}$. Tada razvojem u binomni red dobivamo

$$(\sum_{i\geq 0} 4^i x^i) \cdot (\sum_{j\geq 0} \binom{-3/2}{j} (-4x)^j) = \sum_{n\geq 0} \binom{-5/2}{n} (-4x)^n.$$

Odavde izjednačavanjem koeficijenata uz x^n i rabeći formule

$$\binom{-1/2}{n} = \frac{(-1)^n}{4^n}\binom{2n}{n}, \quad \binom{-3/2}{n} = \frac{(-1)^n(2n+1)}{4^n}\binom{2n}{n}$$
$$\binom{-5/2}{n} = \frac{(-1)^n(2n+2)(2n+3)}{3 \cdot 4^{n+1}}\binom{2n+2}{n+1},$$

slijedi tvrdnja. □

Primjer 9. Odredite FI za niz

$$a_n = \sum_{k=0}^{n} \binom{n+k}{2k} 2^{n-k}$$

i pomoću FI izračunajte a_n.

Rješenje. Neka je $(a_n)_{n\geq 0} \overset{\text{FI}}{\longleftrightarrow} A(x)$. Tada imamo

$$A(x) = \sum_{n\geq 0} a_n x^n = \sum_{k\geq 0} 2^{-k} \sum_{n\geq 0} \binom{n+k}{2k} 2^n x^n =$$
$$= \sum_{k\geq 0} 2^{-k}(2x)^{-k} \sum_{n\geq 0} \binom{n+k}{2k} (2x)^{n+k} = \sum_{k\geq 0} 2^{-k}(2x)^{-k} \frac{(2x)^{2k}}{(1-2x)^{2k+1}} =$$
$$= \frac{1}{1-2x} \sum_{k\geq 0} (\frac{x}{(1-2x)^2})^k = \frac{1}{1-2x} \cdot \frac{1}{1-x/(2x-1)^2} = \frac{1-2x}{(1-4x)(1-x)} =$$
$$= \frac{A}{1-4x} + \frac{B}{1-x} \Rightarrow A = \frac{2}{3}, B = \frac{1}{3}, \quad \text{pa je}$$
$$A(x) = \frac{2}{3(1-4x)} + \frac{1}{3(1-x)}.$$

Odavde slijedi da je
$a_n = \langle x^n \rangle A(x) = \frac{2}{3} \cdot 4^n + \frac{1}{3} = \frac{1}{3}(2^{2n+1}+1)$. □

Navedimo sada tablicu nekih važnih jednostavnih funkcija izvodnica:

Niz	Pripadni FI
$1, 1, \ldots, 1, \ldots$	$\sum_{n\geq 0} x^n = \frac{1}{1-x}$
$0, 1, \ldots, n, \ldots$	$\sum_{n\geq 0} nx^n = \frac{x}{(1-x)^2}$
$1, \binom{m}{1}, \ldots, \binom{m}{n}, \ldots, \binom{m}{m}$	$\sum_{n\geq 0} \binom{m}{n} x^n = (1+x)^m$
$1, \binom{\alpha}{1}, \binom{\alpha}{2}, \ldots, \binom{\alpha}{n}, \ldots$	$\sum_{n\geq 0} \binom{\alpha}{n} x^n = (1+x)^\alpha$
$1, 0, 1, 0, 1, 0, \ldots$	$\sum_{n\geq 0} x^{2n} = \frac{1}{1-x^2}$
$1, c, c^2, \ldots, c^n, \ldots$	$\sum_{n\geq 0} c^n x^n = \frac{1}{1-cx}$
$1, m+1, \binom{m+2}{2}, \binom{m+3}{3}, \ldots$	$\sum_{n\geq 0} \binom{m+n}{n} x^n = \frac{1}{(1-x)^{m+1}}$
$1, c, \binom{c+1}{2}, \binom{c+2}{3}, \ldots$	$\sum_{n\geq 0} \binom{c+n-1}{n} x^n = \frac{1}{(1-x)^c}$
$1, -1, 1, -1 \ldots$	$\sum_{n\geq 0} (-1)^n x^n = \frac{1}{1+x}$
$1, 0, \ldots, 0, 1, 0, \ldots, 1, 0, \ldots$	$\sum_{n\geq 0} x^{mn} = \frac{1}{1-x^m}$
$1, 2, 4, \ldots, 2^n, \ldots$	$\sum_{n\geq 0} 2^n x^n = \frac{1}{1-2x}$
$1, \binom{2}{1}, \binom{4}{2}, \ldots, \binom{2n}{n}, \ldots$	$\sum_{n\geq 0} \binom{2n}{n} x^n = \frac{1}{\sqrt{1-4x}}$
$1, 1, \frac{1}{2!}, \frac{1}{3!}, \ldots, \frac{1}{n!}, \ldots$	$\sum_{n\geq 0} \frac{x^n}{n!} = e^x$
$0, 1, \frac{1}{2}, \frac{1}{3}, \ldots, \frac{1}{n}, \ldots$	$\sum_{n\geq 1} \frac{x^n}{n} = \ln \frac{1}{1-x}$
$0, 1, -\frac{1}{2}, \frac{1}{3}, -\frac{1}{4} \ldots$	$\sum_{n\geq 1} \frac{(-1)^{n-1}}{n} x^n = \ln(1+x)$
$0, 1, 1+\frac{1}{2}, 1+\frac{1}{2}+\frac{1}{3}, \ldots$	$\sum_{n\geq 1} H_n x^n = \frac{1}{1-x} \ln \frac{1}{1-x}$

Isto tako, na temelju dosadašnjeg iskustva, čitatelj lako može provjeriti da za FI vrijede pravila sadržana u sljedećoj tablici:

$$A(x) = \sum_{n\geq 0} a_n x^n \overset{\text{FI}}{\longleftrightarrow} a_0, a_1, a_2, \ldots, a_n, \ldots$$
$$B(x) = \sum_{n\geq 0} b_n x^n \overset{\text{FI}}{\longleftrightarrow} b_0, b_1, b_2, \ldots, b_n, \ldots$$

lijevi pomak

$$xA(x) = \sum_{n\geq 1} a_{n-1} x^n, \quad 0, a_0, a_1, a_2, \ldots, a_{n-1}, \ldots$$

desni pomak

$$\frac{A(x) - a_0}{x} = \sum_{n\geq 0} a_{n+1} x^n, \quad a_1, a_2, a_3, \ldots, a_{n+1}, \ldots$$

desni m-ti pomak

$$\frac{A(x) - a_0 - a_1 x - \ldots - a_{m-1}x^{m-1}}{x^m} = \sum_{n\geq 0} a_{m+n} x^n, \; a_m, a_{m+1}, a_{m+2}, \ldots, a_{m+n}, \ldots$$

skaliranje

$$A(\lambda x) = \sum_{n\geq 0} \lambda^n a_n x^n, \quad a_0, \lambda a_1, \lambda^2 a_2, \ldots, \lambda^n a_n, \ldots$$

zbrajanje

$$A(x)+B(x)=\sum_{n\geq 0}(a_n+b_n)x^n, \quad a_0+b_0, a_1+b_1, \ldots, a_n+b_n, \ldots$$

deriviranje

$$A'(x)=\sum_{n\geq 0}(n+1)a_{n+1}x^n, \quad a_1, 2a_2, \ldots, (n+1)a_{n+1}, \ldots$$

integriranje

$$\int_0^x A(t)dt=\sum_{n\geq 1}\frac{1}{n}a_{n-1}x^n, \quad 0, a_0, \frac{a_1}{2}, \frac{a_2}{3}, \ldots, \frac{a_{n-1}}{n}, \ldots$$

konvolucija

$$A(x)B(x)=\sum_{n\geq 0}(\sum_{k=0}^{n}a_kb_{n-k})x^n, \quad a_0b_0, a_0b_1+a_1b_0, \ldots, \sum_{k=0}^{n}a_kb_{n-k}, \ldots$$

parcijalne sume

$$\frac{A(x)}{1-x}=\sum_{n\geq 0}(\sum_{k=0}^{n}a_k)x^n \quad a_0, a_0+a_1, \ldots, \sum_{k=0}^{n}a_k, \ldots$$

Uočimo da je EFI za niz $(a_n)_{n\geq 0}$ ništa drugo nego li FI za niz $(a_n/n!)_{n\geq 0}$. No, katkad je pogodnije raditi izravno s eksponencijalnom funkcijom izvodnicom.

Primjer 10. Odredite EFI za niz $(a_n)_{n\geq 0}$ ako je
a) $a_n=c$; b) $a_n=c^n$; c) $a_n=n$; d) $a_n=n!$; e) $a_n=1/(n+1)$ $(n\geq 1)$.

Rješenje. a) EFI za niz $c, c, c, \ldots$, po definiciji je jednak

$$\sum_{n\geq 0}c\frac{x^n}{n!}=c\sum_{n\geq 0}\frac{x^n}{n!}=c\cdot e^x.$$

b) EFI za niz $1, c, c^2, \ldots, c^n, \ldots$ je

$$\sum_{n\geq 0}c^n\frac{x^n}{n!}=\sum_{n\geq 0}\frac{(cx)^n}{n!}=e^{cx}.$$

c) Imamo $\sum_{n\geq 0}n\frac{x^n}{n!}=\sum_{n\geq 1}\frac{x^n}{(n-1)!}=x\sum_{n\geq 1}\frac{x^{n-1}}{(n-1)!}=xe^x$.
d) Ovaj put je EFI jednaka

$$\sum_{n\geq 0}n!\frac{x^n}{n!}=\sum_{n\geq 0}x^n=\frac{1}{1-x}.$$

e) Pođimo od

$$\sum_{n\geq 1}\frac{x^n}{n!}=e^x-1.$$

Ako obje strane podijelimo s x, dobivamo traženu EFI. Imamo:

$$\sum_{n\geq 0}\frac{1}{n+1}\frac{x^n}{n!}=\sum_{n\geq 1}\frac{1}{n}\cdot\frac{x^{n-1}}{(n-1)!}=\frac{e^x-1}{x}.$$

□

Kao i za obične FI, tako i za EFI imamo razna pravila, no izdvojimo za sada samo dva. Ako je $(a_n)_{n\geq 0}\overset{\text{EFI}}{\longleftrightarrow}A(x)$, $(b_n)_{n\geq 0}\overset{\text{EFI}}{\longleftrightarrow}B(x)$, onda je $A(x)B(x)\overset{\text{EFI}}{\longleftrightarrow}(c_n)_{n\geq 0}$, gdje je (*"binomna konvolucija"*)

$$c_n=\sum_{k=0}^{n}\binom{n}{k}a_kb_{n-k},$$

te $e^xA(x)\overset{\text{EFI}}{\longleftrightarrow}(d_n)_{n\geq 0}$, gdje je (*"binomna parcijalna suma"*)

$$d_n=\sum_{k=0}^{n}\binom{n}{k}a_k.$$

Ustvari, prijelaz od EFI na FI je sljedeći. Ako je $(a_n)_{n\geq 0}\overset{\text{EFI}}{\longleftrightarrow}A(x)$, onda je

$$(a_n)_{n\geq 0}\overset{\text{FI}}{\longleftrightarrow}\int_0^\infty A(xt)e^{-t}dt, \tag{8}$$

ako ovaj integral postoji. Ovo je **Laplaceova transformacija**. To odmah slijedi iz činjenice

$$\int_0^\infty t^ne^{-t}dt=\Gamma(n+1)=n!$$

§ 3. Rekurzije i funkcije izvodnice

Funkcije izvodnice su vrlo pogodne za rješavanje rekurzija. No, i obrnuto, često iz funkcija izvodnica možemo naći i novu rekurziju različitu od one od koje smo pošli. Počnimo s rekurzijom za Fibonaccijeve brojeve.

Primjer 11. Odredite FI za niz $(F_n)_{n\geq 0}$ Fibonaccijevih brojeva i pomoću toga izračunajte F_n.

Rješenje. Neka je $F(x)=\sum_{n\geq 0}F_nx^n$, tj. $F(x)\overset{\text{FI}}{\longleftrightarrow}(F_n)_{n\geq 0}$. Osnovnu rekurziju

$$F_{n+2}=F_{n+1}+F_n$$

pomnožimo s x^{n+2} i potom to sumirajmo po $n\geq 0$. Dobivamo

$$\sum_{n\geq 0}F_{n+2}x^{n+2}=\sum_{n\geq 0}F_{n+1}x^{n+2}+\sum_{n\geq 0}F_nx^{n+2}.$$

Lijeva je strana jednaka $F(x) - F_0 - F_1 x$, a desna $x(F(x) - F_0) + x^2 F(x)$. Odavde zbog početnih uvjeta $F_0 = 0$, $F_1 = 1$ slijedi

$$F(x) - x = xF(x) + x^2 F(x) \Rightarrow$$
$$F(x) = \frac{x}{1 - x - x^2}. \tag{9}$$

Sada ćemo ovu funkciju razviti u parcijalne razlomke. Prvo, $1-x-x^2 = 0$, za $x_{1,2} = (-1 \pm \sqrt{5})/2$. Označimo li $\alpha = (1+\sqrt{5})/2$, $\beta = (1-\sqrt{5})/2$, onda je $1-x-x^2 = (1-\alpha x)(1-\beta x)$, pa je

$$F(x) = \frac{x}{(1-\alpha x)(1-\beta x)}.$$

Metodom neodređenih koeficijenata odredimo A i B tako da je

$$\frac{x}{(1-\alpha x)(1-\beta x)} = \frac{A}{1-\alpha x} + \frac{B}{1-\beta x}.$$

Odavde nalazimo $A = -B = 1/\sqrt{5}$, pa je konačno

$$F(x) = \frac{1}{\sqrt{5}}\left(\frac{1}{1-\alpha x} - \frac{1}{1-\beta x}\right), \tag{10}$$

a odavde (zbog $1/(1-\alpha x) = 1 + \alpha x + \alpha^2 x^2 + \dots$) dobivamo poznatu formulu

$$F_n = \langle x^n \rangle F(x) = \frac{1}{\sqrt{5}}(\alpha^n - \beta^n).$$

□

Riješimo sada pomoću FI jednu tipičnu linearnu homogenu rekurziju (s konstatnim koeficijentima).

Primjer 12. Neka je $(a_n)_{n\geq 0}$ niz za koji je $a_0 = 0$, $a_1 = 1$, $a_2 = -1$, a za $n \geq 3$, $a_n + a_{n-1} - 16a_{n-2} + 20a_{n-3} = 0$. Odredite FI za $(a_n)_{n\geq 0}$ i opći član a_n.

Rješenje. Neka je $(a_n)_{n\geq 0} \overset{\text{FI}}{\longleftrightarrow} f(x)$. Zbrojimo sljedeće jednakosti

$$\left.\begin{array}{rcl} f(x) & = & a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n + \dots \\ xf(x) & = & a_0 x + a_1 x^2 + \dots + a_{n-1} x^n + \dots \\ -16x^2 f(x) & = & -16a_0 x^2 - 16a_1 x^3 - \dots - 16a_{n-2} x^n + \dots \\ 20x^3 f(x) & = & 20a_0 x^3 + \dots + 20a_{n-3} x^n + \dots \end{array}\right\} + \Rightarrow$$

$$(1 + x - 16x^2 + 20x^3) f(x) = a_0 + (a_0 + a_1)x + (a_2 + a_1 - 16a_0)x^2 +$$
$$+ (a_3 + a_2 - 16a_1 + 20a_0)x^3 + \dots + (a_n + a_{n-1} - 16a_{n-2} + 20a_{n-2})x^n + \dots$$

Kako je $a_n + a_{n-1} - 16a_{n-2} + 20a_{n-3} = 0$ za $n \geq 3$ i $a_0 = 0$, $a_1 = 1$, $a_2 = -1$, slijedi da je $(1 + x - 16x^2 + 20x^3) f(x) = x$, tj.:

$$f(x) = \frac{x}{1 + x - 16x^2 + 20x^3}.$$

Zbog $1 + x - 16x^2 + 20x^3 = (1-2x)^2(1+5x)$, postoje konstante A, B, C, tako da je

$$f(x) = \frac{A}{1-2x} + \frac{B}{(1-2x)^2} + \frac{C}{1+5x}.$$

Metodom neodređenih koeficijenata nalazimo $A = -2/49$, $B = 7/49$, $C = -5/49$, pa je

$$f(x) = \frac{1}{49}\left[\frac{-2}{1-2x} + \frac{7}{(1-2x)^2} - \frac{5}{1+5x}\right].$$

Odavde zbog

$$\frac{1}{(1-\alpha x)^m} = \sum_{k\geq 0} \binom{m+k-1}{k} \alpha^k x^k$$

razvojem $f(x)$ u red potencija konačno nalazimo

$$a_n = \langle x^n \rangle f(x) = \frac{1}{49}[7(n+1)2^n - 5(-5)^n - 2^{n+1}].$$

□

Sada ćemo funkcije izvodnice primijeniti na jedan važan problem računarstva, a to je **problem sortiranja** (razvrstavanja). Problem se općenito svodi na to da se nađe što efikasniji algoritam koji će danih n (različitih) realnih brojeva poredati ("sortirati") po veličini. Među najpoznatijima su tzv. "**mergesort**" (sortiranje stapanjem) i "**quicksort**" (brzo sortiranje).

Mergesort je algoritam tipa "podijeli pa ovladaj". Naime dana lista brojeva se rascijepi na dvije (približno jednake) podliste, pa se s tim podlistama učini isto itd. sve dok se ne dođe do podlista s jednim članom. Tada se postupno stapaju po dvije sortirane podliste u poretku u kojem se pojavljuju, sve dok se ne dobije uređaj (sortiranje) svih brojeva s liste.

Neka je c_n broj usporedbi koje mergesort algoritam treba za sortiranje n brojeva. Za sortiranje prve polovice brojeva $c_{\lfloor n/2 \rfloor}$, a druge polovice $c_{\lceil n/2 \rceil}$ usporedbi, te još n usporedbi za stapanje (po jedna za svako $k \in [n]$). Stoga je ukupni broj usporedbi s mergesortom dan rekurzijom i početnim uvjetima:

$$c_n = c_{\lfloor n/2 \rfloor} + c_{\lceil n/2 \rceil} + n \quad (n \geq 2),\ c_1 = 0. \tag{11}$$

Rekurzija (11) se najjednostavnije može riješiti pomoću diferencija. Ako je $d_n = \Delta c_n = c_{n+1} - c_n$, onda iz (11) slijedi $d_n = d_{\lfloor n/2 \rfloor} + 1$ za $n \geq 2$ i $d_1 = 0$, a odavde iteriranjem (dok ne dođemo do početnih uvjeta) slijedi $d_n = \lfloor \log_2 n \rfloor + 2$, pa konačno

$$c_n = n - 1 + \sum_{k=1}^{n-1} (\lfloor \log_2 k \rfloor + 1).$$

Nije teško pokazati da je

$$c_n = n\lfloor \log_2 n \rfloor + n + 1 - 2^{\lfloor \log_2 n \rfloor + 1}.$$

Do ovog se rezultata može doći i pomoću funkcija izvodnica, a mi ćemo tom metodom obraditi quicksort. Taj je algoritam također tipa "podijeli pa ovladaj".

Quicksort algoritam radi tako da polazeći od niza $x_1, x_2, \dots, x_n$, usporedi x_2, x_3, $\dots$, x_n s x_1 i podijeli ih u dvije grupe: one manje od x_1 i one veće od x_1. Poredak u obje grupe ostaje isti kao i onaj na početku. Tada se (rekurzivno) s

obje grupe napravi ista stvar itd. sve dok se ne dođe do najviše jednočlanih grupa. Ovaj se algoritam vrlo dobro ponaša "u prosjeku" (dok u "najgorem slučaju" kada je niz već sortiran treba oko n^2 usporedbi). Zato ovaj put rekurziju izražavamo u vjerojatnosnim terminima. Neka je q_n prosječni broj usporedbi (tj. očekivani broj usporedbi) da se s quicksortom sortira n brojeva u slučajnome poretku. Tada je $q_0 = 0$ i vrijedi:

$$q_n = n + 1 + \frac{1}{n}\sum_{j=1}^{n}(q_{j-1} + q_{n-j}),\ n \geq 1. \tag{12}$$

Naime, da dobijemo ukupni prosječni broj usporedbi, treba zbrojiti broj usporedbi za prvu podjelu (to je $n+1$) s brojem usporedbi u dvije grupe nakon prve podjele. Svaki se element s vjerojatnošću $1/n$ javlja kao "djelišni", a podgrupe na koje je preostalih $n-1$ elemenata podijeljeno imaju veličine $j-1$ i $n-j$ za neko $j \in [n]$.

Rekurziju (12) možemo lako razriješiti ovako. Prvo, j zamijenimo s $n-j+1$, pa dobivamo

$$q_n = n + 1 + \frac{2}{n}\sum_{j=1}^{n} q_{j-1}. \tag{13}$$

Pomnožimo li (13) s n i oduzmemo od toga istu formulu za $n-1$ (da uklonimo sumu), dobivamo $nq_n = (n+1)q_{n-1} + 2n$ (za $n > 1$). Dijeljenjem s $n(n+1)$ slijedi (za $n > 1$):

$$\frac{q_n}{n+1} = \frac{q_{n-1}}{n} + \frac{2}{n+1},$$

tj. uz oznaku $p_n = q_n/(n+1)$ dobivamo rekurziju $p_n = p_{n-1} + 2/(n+1)$, koju teleskopiramo i konačno (zbog $q_1 = 2$) dobivamo q_n izražen pomoću harmonijskog broja:

$$q_n = 2(n+1)(H_{n+1} - 1). \tag{14}$$

Napomenimo da ako je $n = N$ velik broj, onda je

$$H_n = \sum_{k=1}^{N}\frac{1}{k} \approx \int_1^N \frac{1}{x}dx = \ln N,$$

ili točnije $H_N = \ln N + \gamma + 1/(2N) + O(1/N^2)$, gdje je $\gamma = 0.57721\ldots$, pa je tada $q_N \approx 2N\ln N - 0.846N$.

No, izvedimo sada (14) pomoću funkcija izvodnica.

Primjer 13 (FI za quicksort). Odredite FI za niz $(q_n)_{n\geq 0}$ za koji je $q_0 = 0$ i za koji vrijedi rekurzija (13) i pomoću toga dokažite da za q_n vrijedi formula (14).

Rješenje. Prepišimo rekurziju (13) za niz q_n:

$$nq_n = n(n+1) + 2\sum_{k=1}^{n} q_{k-1},\ \text{za } n \geq 1,\ q_0 = 0. \tag{15}$$

Neka je $(q_n)_{n\geq 0} \overset{\text{FI}}{\longleftrightarrow} Q(x)$. Množenjem (15) s x^n i sumiranjem po n dobivamo

$$\sum_{n\geq 1} nq_n x^n = \sum_{n\geq 1} n(n+1)x^n + 2\sum_{n\geq 1}\sum_{k=1}^{n} q_{k-1}x^n.$$

Sada iz prethodnih primjera ili tablica dobivamo (uvjerite se detaljno) da je lijeva strana jednaka $xQ'(x)$, da je prvi član na desnoj strani $2x/(1-x)^3$, a drugi član (parcijalne sume!) jednak $2xQ(x)/(1-x)$. Stoga rekurzija (15) korespondira diferencijalnoj jednadžbi za pripadnu FI:

$$Q'(x) = \frac{2Q(x)}{1-x} + \frac{2}{(1-x)^3}. \tag{16}$$

Ova linearna (nehomogena) diferencijalna jednadžba prvog reda rješava se na standardan način. Prvo se riješi pripadna homogena jednadžba

$$R'(x) = \frac{2R(x)}{1-x}$$

tako da se integrira $R'(x)/R(x) = 2/(1-x)$, iz čega se dobije

$$R(x) = \frac{C}{(1-x)^2}.$$

Prijelazom $C \to C(x)$ ($C(x)$ se zove "integracioni faktor"), rješenje od (16) je oblika

$$Q(x) = \frac{C(x)}{(1-x)^2}.$$

Deriviranjem $((1-x)^2Q(x))' = C'(x)$ i rabeći (16) dobivamo

$$C'(x) = (1-x)^2Q'(x) - 2(1-x)Q(x) = (1-x)^2\left[\frac{2Q(x)}{1-x} + \frac{2}{(1-x)^3}\right] -$$
$$- 2(1-x)Q(x) = \frac{2}{1-x},$$

tj.

$$C'(x) = \frac{2}{1-x},$$

čiji je integral

$$C(x) = 2\ln\frac{1}{1-x}.$$

To konačno daje

$$Q(x) = \frac{2}{(1-x)^2}\ln\frac{1}{1-x}.$$

Odavde se $q_n = \langle x^n\rangle Q(x)$ dobije tako da se derivira FI za harmonijske brojeve (vidi tablicu), iz čega slijedi (14). □

Kao primjenu eksponencijalne funkcije izvodnice izvedimo formulu za broj deranžmana i Bellove brojeve.

Primjer 14 (EFI za broj deranžmana). Za $n \in \mathbb{N}$, neka je D_n broj deranžmana od $[n]$ (tj. permutacija bez fiksnih točaka), a $D_0 := 1$. Odredite EFI za niz $(D_n)_{n\geq 0}$ i pomoću toga D_n.

Rješenje. Neka je $(D_n)_{n\geq 0} \overset{\text{EFI}}{\longleftrightarrow} D(x)$. Broj permutacija od $[n]$ koje imaju neki čvrsti skup od $k \leq n$ elemenata kao skup fiksnih točaka jednak je očito D_{n-k}. Nadalje, na $\binom{n}{k}$ načina možemo odabrati k-člani skup kao skup fiksnih točaka, pa stoga imamo $\binom{n}{k}D_{n-k}$ permutacija od $[n]$ koje imaju točno k fiksnih točaka. Svaka permutacija od $[n]$ ima neki broj k $(0 \leq k \leq n)$ fiksnih točaka, pa dobivamo (rekurziju)

$$n! = \sum_{k=0}^{n} \binom{n}{k} D_{n-k}.$$

Sada uzmimo EFI obiju strana. EFI niza $(n!)$ je očito $1/(1-x)$, a na desnoj strani prepoznajemo "binomnu parcijalnu sumu", tj. pravilo $e^x D(x)$. Stoga dobivamo

$$\frac{1}{1-x} = e^x D(x),$$

tj.

$$D(x) = \frac{1}{1-x} e^{-x}.$$

Odavde slijedi

$$D(x) = \left(\sum_{i\geq 0} x^i\right)\left(\sum_{j\geq 0} (-1)^j \frac{x^j}{j!}\right) = \sum_{n\geq 0}\left(\sum_{k\geq 0} \frac{(-1)^k}{k!}\right) x^n,$$

pa odavde slijedi

$$D_n = n! \sum_{k=0}^{n} \frac{(-1)^k}{k!}.$$

Na drugi se način ovo može izvesti pomoću kratke rekurzije za D_n:

$$D_n = (n-1)D_{n-1} + (n-1)D_{n-2}. \qquad (*)$$

Naime, za svaki deranžman π od $[n]$ postoji jedinstveni k, $1 \leq k \leq n-1$, takav da je $\pi(k) = n$. Ako je $\pi(n) = k$, onda ostatak možemo deranžirati na D_{n-2} načina, a ako je $\pi(n) \neq k$, onda $[n] \setminus \{k\}$ ima D_{n-1} deranžmana. Pri tome k može biti $1, 2, \ldots, n-1$. Uočite da iz te rekurzije slijedi i još kraća rekurzija $D_n = nD_{n-1} + (-1)^n$. Sada prepišimo $(*)$ u obliku $D_{n+2} = (n+1)D_{n+1} + (n+1)D_n$, pomnožimo to s $x^{n+1}/(n+1)!$ i sumirajmo po $n \geq 0$. Dobivamo

$$\sum_{n\geq 0} D_{n+2} \frac{x^{n+1}}{(n+1)!} = \sum_{n\geq 0} D_{n+1} \frac{x^{n+1}}{n!} + \sum_{n\geq 0} D_n \frac{x^{n+1}}{n!},$$

što možemo pisati kao

$$\begin{gathered}\left(\textstyle\sum_{n\geq 0} D_{n+2} \frac{x^{n+2}}{(n+2)!}\right)' = x\left(\textstyle\sum_{n\geq 0} D_{n+1} \frac{x^{n+1}}{(n+1)!}\right)' + xD(x) \Rightarrow \\ (D(x) - D_0 - D_1 x)' = x(D(x) - D_0)' + xD(x) \Rightarrow \\ \frac{D'(x)}{D(x)} = \frac{x}{1-x} = \frac{1}{1-x} - 1,\end{gathered}$$

a odavde integriranjem slijedi $D(x) = -\ln(1-x) - x + C$, pa je $D(x) = e^{-x+C}/(1-x)$. Zbog $D(0) = 1$ dobivamo $C = 0$, pa opet $D(x) = e^{-x}/(1-x)$. □

Na sličan se način može izvesti i da je (obična) FI za niz $D_n(0)$, $D_n(1)$, $\ldots$, $D_n(m)$, $\ldots$, gdje je (za čvrsto n) broj $D_n(m)$ broj permutacija od $[n]$ s točno m fiksnih točaka jednaka

$$F_n(x) = n! \sum_{m=0}^{n} \frac{(x-1)^m}{m!}.$$

Primjer 15 (EFI za Bellove brojeve). Za $n \in \mathbb{N}_0$, Bellov broj B_n je broj particija n-članog skupa ($B_0 = 1$). Odredite EFI za niz $(B_n)_{n\geq 0}$ i odatle B_n.

Rješenje. Pođimo od rekurzije za Bellove brojeve (usp. Propozicija 20 u poglavlju II):

$$B_{n+1} = \sum_{k\geq 0} \binom{n}{k} B_k. \qquad (17)$$

Neka je $B(x) \overset{\text{EFI}}{\longleftrightarrow} (B_n)_{n\geq 0}$. Uočimo da općenito, ako je $A(x) \overset{\text{EFI}}{\longleftrightarrow} (a_n)_{n\geq 0}$ onda je $A'(x) \overset{\text{EFI}}{\longleftrightarrow} (a_{n+1})_{n\geq 0}$. Stoga uzmemo li EFI obiju strana te rekurzije (tj. pomnožimo ih s $x^n/n!$ i sumiramo po $n \geq 0$), na lijevoj strani dobivamo $B'(x)$, a na desnoj opet prepoznajemo "binomnu parcijalnu sumu", tj. produkt EFI za niz $(1, 1, 1, \ldots)$, a to je e^x i EFI za niz $(B_n)_{n\geq 0}$, a to je $B(x)$. Stoga desna strana daje $e^x B(x)$. Prema tome, dobivamo

$$B'(x) = e^x B(x).$$

Integriranjem $\int B'(x)/B(x)dx = \int e^x dx$ slijedi $\ln B(x) = Ce^x$, tj.

$$B(x) = C\exp(e^x).$$

Iz početnog uvjeta $B_0 = 1$ slijedi $B(0) = 1$, pa je $C = e^{-1}$, i konačno dobivamo

$$B(x) = \exp(e^x - 1) = e^{e^x - 1}. \qquad (18)$$

Pokažimo sada da vrijedi i obrnuto, tj. da iz (18) slijedi (17). U tu svrhu primijenimo na (18) operator $x(d/dx)\ln$, tj. prvo logaritmiramo, pa deriviramo i pomnožimo s x.

$$\begin{gathered}\ln B(x) = \ln\left(\textstyle\sum_{n\geq 0} B_n \frac{x^n}{n!}\right) = e^x - 1, \\ \textstyle\sum_{n\geq 0} nB_n \frac{x^n}{n!} / \sum_{n\geq 0} B_n \frac{x^n}{n!} = xe^x \Rightarrow \\ \textstyle\sum_{n\geq 0} nB_n \frac{x^n}{n!} = xe^x \sum_{n\geq 0} B_n \frac{x^n}{n!} = \left(\sum_{i\geq 0} \frac{x^{i+1}}{i!}\right)\left(\sum_{j\geq 0} B_j \frac{x^j}{j!}\right).\end{gathered}$$

Uzmemo li koeficijent uz x^{n+1} na obje strane, dobivamo (17).

Sada iz (18) nije teško izvesti formulu (koju već znamo, pogl IV. Korolar 4)

$$B_n = n!\langle x^n\rangle e^{e^x - 1} = \frac{1}{e}\sum_{k\geq 0} \frac{k^n}{n!}.$$

S druge strane, $B_n = \sum_{k=0}^{n} S(n,k)$, gdje je $S(n,k)$ Stirlingov particijski broj (ili druge vrste), a iz razvoja

$$\exp(e^x - 1) = \sum_{k\geq 0} \frac{(e^x - 1)^k}{k!}$$

slijedi

$$S(n,k) = \langle x^n/n! \rangle \frac{(e^x-1)^k}{k!}.$$

Odavde vidimo da je za čvrsto k, $(S(n,k))_{n\geq 0} \overset{\text{EFI}}{\longleftrightarrow} (e^x-1)^k/k!$. □

U sljedećem ćemo primjeru naći FI za Catalanove brojeve. Podsjetimo se da oni prebrojavaju triangulacije poligona, binarna stabla, Dyckove putove itd. (vidi poglavlje III). Njihova FI će zadovoljavati izvjesnu funkcionalnu jednadžbu.

Primjer 16 (FI za Catalanove brojeve). Neka je $b_0 = b_1 = 1$, a $b_n = b_0 b_{n-1} + b_1 b_{n-2} + \cdots + b_{n-1} b_0$ za $n \geq 1$. Odredite FI za niz $(b_n)_{n\geq 0}$ i pomoću toga pokažite da je $b_n = C_n = \binom{2n}{n}/(n+1)$ (n-ti Catalanov broj).

Rješenje. Neka je $(b_n)_{n\geq 0} \overset{\text{FI}}{\longleftrightarrow} f(x)$, tj. $f(x) = b_0 + b_1 x + b_2 x^2 + \ldots$. Ako ovu jednakost kvadriramo, dobivamo

$$\begin{aligned} f(x)^2 &= b_0^2 + (b_0 b_1 + b_1 b_0)x + (b_0 b_2 + b_1 b_1 + b_2 b_0)x^2 + (b_0 b_3 + b_1 b_2 + b_2 b_1 + b_3 b_0)x^3 + \ldots \\ &= 1 + b_2 x + b_3 x^2 + b_4 x^3 + \ldots. \end{aligned}$$

Množenje s x daje

$$x f(x)^2 = x + b_2 x^2 + b_3 x^3 + b_4 x^4 + \cdots = x + (f(x) - b_0 - b_1 x) = f(x) - 1.$$

Dakle,

$$x f(x)^2 - f(x) + 1 = 0. \tag{19}$$

Riješimo li ovu kvadratnu (funkcionalnu) jednadžbu po $f(x)$, dobivamo

$$f_{1,2}(x) = \frac{1 \pm \sqrt{1-4x}}{2x}.$$

Koji predznak valja uzeti? Treba pogledati limes kada $x \to 0$. Zbog $b_0 = 1$ slijedi da je $f(0) = 1$, no $\lim_{x\to 0} f_1(x) = \infty$, a $\lim_{x\to 0} f_2(x) = 1$ (uvjerite se u to rabeći L'Hospitalovo pravilo). Stoga je $f(x) = f_2(x)$, tj.

$$f(x) = \frac{1-\sqrt{1-4x}}{2x}.$$

Pomoću binarnog reda dobivamo (ili vidi tablicu za razvoj $\sqrt{1-4x}$):

$$b_n = \langle x^n \rangle f(x) = -\frac{1}{2}(-4)^{n+1}\binom{1/2}{n+1} = \frac{1}{n+1}\binom{2n}{n} = C_n \text{ (n-ti Catalanov broj).}$$

Pregledno, još jednom, imamo

$$\frac{1-\sqrt{1-4x}}{2x} = \sum_{n\geq 0} \frac{1}{n+1}\binom{2n}{n} x^n = 1 + x + 2x^2 + 5x^3 + 14x^4 + 42x^5 + 132x^6 + \ldots.$$

□

Sustavi rekurzija također se mogu rješavati s funkcijama izvodnicama.

Primjer 17 (iz nuklearne fizike). Opisat ćemo (približan) model za širenje neutrona visoke i niske energije nakon njihova sudara s jezgrama fisijske materije (npr. urana), poslije čega su apsorbirani. Ovdje je riječ o brzim reaktorima, gdje nema usporivača, kao npr. teške vode. (U stvarnosti, svi neutroni imaju dosta visoku energiju, i to ne samo u dvije razine, nego postoji cijeli kontinuirani spektar energetskih razina, a neutroni na najvišoj energetskoj razini zovu se visokoenergetski neutroni; neutroni više energetske razine nastoje proizvesti više novih neutrona nego oni nižih energija). Promatrajmo reaktor u trenutku 0 i pretpostavimo da je jedan visokoenergetski neutron ubačen u sustav. Nakon svakog vremenskog intervala od 1 mikrosekunde ($= 10^{-6}$ sekundi) događa se:

a) međudjelovanje visokoenergetskog neutrona s jezgrom (fisijske materije) nakon apsorpcije rezultira (nakon jedne mikrosekunde) stvaranjem dvaju visokoenergetskih i jednog niskoenergetskog neutrona;

b) međudjelovanje niskoenergetskog neutrona rezultira stvaranjem jednog neutrona svake od tih dviju razina.

Pretpostavimo li da svi slobodni neutroni djeluju s jezgrama jednu mikrosekundu nakon "rađanja", odredite a_n = broj visokoenergetskih neutrona, b_n = broj niskoenergetskih neutrona u reaktoru nakon n mikrosekundi.

Rješenje. Očito je $a_0 = 1$, $b_0 = 0$ i imamo sustav rekurzivnih relacija

$$\begin{aligned} a_{n+1} &= 2a_n + b_n \\ b_{n+1} &= a_n + b_n. \end{aligned}$$

Neka su $f(x)$ i $g(x)$ funkcije izvodnice za nizove (a_n) i (b_n) redom. Množeći rekurzije s x^{n+1} i tada sumirajući po $n \geq 0$, dobivamo $f(x) - a_0 = 2xf(x) + xg(x)$ i $g(x) - b_0 = xf(x) + xg(x)$, a iz tog sustava dobivamo

$$f(x) = \frac{1-x}{x^2-3x+1}, \qquad g(x) = \frac{x}{x^2-3x+1}.$$

Odavde se lako dobiva (učinite to sami)

$$a_n = \frac{5-\sqrt{5}}{10}\left(\frac{3+\sqrt{5}}{2}\right)^{n+1} + \frac{5+\sqrt{5}}{10}\left(\frac{3-\sqrt{5}}{2}\right)^{n+1},$$

$$b_n = \frac{3\sqrt{5}-5}{10}\left(\frac{3+\sqrt{5}}{2}\right)^{n+1} - \frac{3\sqrt{5}+5}{10}\left(\frac{3-\sqrt{5}}{2}\right)^{n+1}.$$

□

§ 4. Simbolička metoda

Sada ćemo ukratko obraditi jednu snažnu metodu suvremene kombinatorike kojom ćemo funkciju izvodnicu za prebrojavanje kombinatornih objekata izravno dobiti iz strukture tih objekata.

Funkcionalnu jednadžbu (19) iz Primjera 16 izveli smo iz rekurzije za brojeve b_n koji broje binarna stabla s n vrhova. Drukčije napisana, ta funkcionalna jednadžba je

$$f(x) = 1 + x f(x)^2,$$

i ona točno odražava kombinatornu strukturu binarnih stabala u sljedećem smislu: "binarno stablo je ili prazno ili se sastoji od vrha i dva binarna (pod)stabla".

Ovakvo poimanje funkcija izvodnica naziva se **simbolička metoda**.

Neka je $\mathcal{A}$ neka klasa (skup) nekih kombinatornih objekata. Svaki objekt iz te klase ima svoju "veličinu" (ili "težinu") i s a_n označimo broj članova iz $\mathcal{A}$ veličine n. Tada je pripadna **funkcija izvodnica koja prebrojava klasu** $\mathcal{A}$ definirana s

$$A(x) = \sum_{n\geq 0} a_n x^n = \sum_{\alpha\in\mathcal{A}} x^{|\alpha|}, \tag{20}$$

što zapisujemo kao $A(x) \overset{\text{FI}}{\longleftrightarrow} \mathcal{A}$. Ako su $\mathcal{A}$ i $\mathcal{B}$ dvije klase kombinatornih objekata, onda imamo i dvije prirodne operacije: disjunktna suma $\mathcal{A}+\mathcal{B}$ koja se sastoji od disjunktnih kopija članova iz $\mathcal{A}$ i $\mathcal{B}$ i Kartezijev produkt $\mathcal{A}\times\mathcal{B}$ koja se sastoji od uređenih parova objekata od kojih je prvi član iz $\mathcal{A}$, a drugi iz $\mathcal{B}$.

Navedimo osnovna pravila koja će nam omogućiti funkcionalne veze funkcija izvodnica izravno iz konstruktivnih opisa objekata.

PROPOZICIJA 3 (FI - simbolička metoda). *Neka su $\mathcal{A}$ i $\mathcal{B}$ dvije klase kombinatornih objekata i neka $A(x) \overset{FI}{\longleftrightarrow} \mathcal{A}$ i $B(x) \overset{FI}{\longleftrightarrow} \mathcal{B}$. Tada je*
a) $A(x)+B(x) \overset{FI}{\longleftrightarrow} \mathcal{A}+\mathcal{B}$; b) $A(x)B(x) \overset{FI}{\longleftrightarrow} \mathcal{A}\times\mathcal{B}$;
c) $\frac{1}{1-A(x)}$ je FI koja prebrojava nizove objekata iz $\mathcal{A}$.

Dokaz. a) To je naprosto pravilo sume: ako su a_n i b_n redom brojevi objekata u $\mathcal{A}$ i $\mathcal{B}$ veličine n, onda je a_n+b_n broj objekata veličine n u $\mathcal{A}+\mathcal{B}$.
b) Za svako $k\in\{0,1,\ldots,n\}$, možemo spariti svaki od a_k objekata veličine k iz $\mathcal{A}$ sa svakim od b_{n-k} objekata veličine $n-k$ iz $\mathcal{B}$ da dobijemo objekt veličine n u $\mathcal{A}\times\mathcal{B}$. Stoga je broj objekata veličine n u $\mathcal{A}\times\mathcal{B}$ jednak $\sum_{k=0}^{n} a_k b_{n-k}$ i ta konvolucija povlači tvrdnju. Drugi dokaz je još kraći:

$$\sum_{\gamma\in\mathcal{A}\times\mathcal{B}} x^{|\gamma|} = \sum_{\alpha\in\mathcal{A}}\sum_{\beta\in\mathcal{B}} x^{|\alpha|+|\beta|} = A(x)\times B(x).$$

c) Svi nizovi objekata iz $\mathcal{A}$ se mogu prikazati kao

$$\varepsilon + \mathcal{A} + \mathcal{A}^2 + \mathcal{A}^3 + \ldots,$$

pri čemu je ε prazan niz. Iz a) i b) slijedi da je FI koja prebrojava klasu svih nizova iz $\mathcal{A}$ jednaka

$$1 + A(x) + A(x)^2 + A(x)^3 + \cdots = \frac{1}{1-A(x)}.$$

□

Primjer 18. Neka je $\mathcal{F}$ klasa koja se sastoji od binarnih nizova bez susjednih nula. Odredite simboličkom metodom pripadnu funkciju izvodnicu i pomoću toga izračunajte broj takvih nizova veličine (tj. duljine) n.

Rješenje. Svaki takav niz je ili prazan, tj. ε ili je jedna 0, ili pak 1 ili 01 iza kojih slijedi niz bez susjednih 0. Simbolički to znači

$$\mathcal{F} = \varepsilon + \{0\} + \{1,01\}\times\mathcal{F}.$$

Ako je $F(x) \overset{\text{FI}}{\longleftrightarrow} \mathcal{F}$, onda Propozicija 3 odmah to prevodi u formulu (tj. funkcionalnu jednadžbu) za funkciju izvodnicu:

$$F(x) = 1 + x + (x+x^2)F(x).$$

Odavde slijedi da je $F(x) = (1+x)/(1-x-x^2)$. Odavde slijedi da je broj takvih nizova duljine n jednak $\langle x^n\rangle F(x) = F_{n+2}$, Fibonaccijev broj (što otprije znamo, npr. Primjer 8 u poglavlju III). □

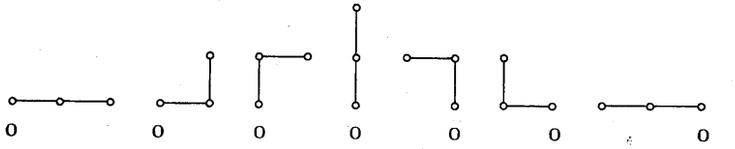
Ako je $\mathcal{B}$ klasa binarnih stabala, onda imamo simboličku formulu

$$\mathcal{B} = \varepsilon + \{\bullet\}\times\mathcal{B}\times\mathcal{B},$$

pa ako $\{\bullet\}$ prelazi u x, a $f(x) \overset{\text{FI}}{\longleftrightarrow} \mathcal{B}$, onda dobivamo $f(x) = 1 + xf(x)^2$

Evo još jednog poučnog primjera.

Primjer 19. U cjelobrojnoj mreži u ravnini promatrajmo sve šetnje (ustvari putove) u toj mreži koje počinju u ishodištu, a imaju korake $D=(1,0)$, $L=(-1,0)$ ili $G=(0,1)$ i nisu samopresječne, tj. nikad se ne pojavljuje DL ili LD kao dio šetnje. Odredite FI za niz $(w_n)_{n\geq 0}$, gdje je w_n broj takvih šetnji duljine n, pa onda i w_n. Npr. $w_0=1$, $w_1=3$, $w_2=7$ (vidi sliku).



Rješenje. Neka je $\mathcal{W}$ klasa svih takvih šetnji (engl. walks). Tada je svaka takva šetnja ili trivijalna ili počinje s G, D ili L. Ako počinje s G, može slobodno nastaviti s članom iz $\mathcal{W}$, a ako počne s D, mora nastaviti s članom iz $\mathcal{W}_L$, tj. s šetnjom koje ne počinju s L i konačno ako počinje s L, mora nastaviti s članom iz $\mathcal{W}_D$. Stoga vrijedi simbolička jednadžba

$$\mathcal{W} = \varepsilon + G\times\mathcal{W} + D\times\mathcal{W}_L + L\times\mathcal{W}_D. \tag{$*$}$$

Neka je $\mathcal{W} \overset{\text{FI}}{\longleftrightarrow} W(x)$, $\mathcal{W}_L \overset{\text{FI}}{\longleftrightarrow} W_L(x)$, $\mathcal{W}_D \overset{\text{FI}}{\longleftrightarrow} W_D(x)$. Iz sličnih je razloga $\mathcal{W}_L = \varepsilon + G\times\mathcal{W} + D\times\mathcal{W}_L$, pa odatle slijedi $W_L = 1 + xW + xW_L \Rightarrow W_L = (1+xW)/(1-x)$ i slično za W_D. Tada iz $(*)$ dobijemo da je tražena FI

$$W(x) = \frac{1+x}{1-2x-x^2} = \frac{A}{1-\alpha x} + \frac{B}{1-\beta x},$$

gdje su $\alpha = (1+\sqrt{2})/2$, $\beta = (1-\sqrt{2})/2$, a odatle (provjerite) da je

$$w_n = \frac{1}{2}\left[(1+\sqrt{2})^{n+1} + (1-\sqrt{2})^{n+1}\right].$$

Primijetite da bez ograničenja na samopresijecanje, ukupno ima 3^n putova s n koraka. No s tim ograničenjem taj se broj od 3^n reducira na približno $(1+\sqrt{2})^n \approx (2.414\ldots)^n$. □

U prethodnoj smo diskusiji radili s objektima koje ne razlikujemo, no ako pojedine objekte razlikujemo, tj. ako su *označeni*, onda je poredak u kojem ih skupljamo kad tvorimo nove kombinatorne objekte bitan. Označene objekte obično prebrojavamo s eksponencijalnom funkcijom izvodnicom i tada pišemo slično kao gore $A(x) \overset{\text{EFI}}{\longleftrightarrow} \mathcal{A}$, tj. ako je a_n broj objekata iz $\mathcal{A}$ veličine n, onda je

$$A(x) = \sum_{n\geq 0} a_n \frac{x^n}{n!} = \sum_{\alpha\in\mathcal{A}} \frac{x^{|\alpha|}}{|\alpha|!}. \tag{21}$$

Relevantne operacije su disjunktna suma $\mathcal{A}+\mathcal{B}$ kao i u slučaju neoznačenih objekata, ali umjesto Kartezijevog produkta, ovdje uvodimo operaciju produkta $\mathcal{A}*\mathcal{B}$ kao klasu svih uređenih parova $(\alpha,\beta)\in\mathcal{A}\times\mathcal{B}$ preoznačenih na sve konzistentne načine. Osim ovoga, ovdje je prirodno promatrati i skupove objekata. Broj skupova veličine n računa se tako da se broj nizova označenih objekata duljine n podijeli s $n!$.

PROPOZICIJA 4 (EFI - simbolička metoda). *Neka su $\mathcal{A}$ i $\mathcal{B}$ dvije klase označenih kombinatornih objekata i neka $A(x) \overset{EFI}{\longleftrightarrow} \mathcal{A}$, $B(x) \overset{EFI}{\longleftrightarrow} \mathcal{B}$. Tada je*
a) $A(x)+B(x) \overset{EFI}{\longleftrightarrow} \mathcal{A}+\mathcal{B}$; b) $A(x)B(x) \overset{EFI}{\longleftrightarrow} \mathcal{A}*\mathcal{B}$;
c) $\frac{1}{1-A(x)}$ je EFI koja prebrojava nizove objekata iz $\mathcal{A}$;
d) $e^{A(x)}$ je EFI koja prebrojava skupove objekata iz $\mathcal{A}$ (ovo je tzv. **eksponencijalna formula***).*

Dokaz. a) To je isto kao a) u Propoziciji 3.
b) Za svako $k\in\{0,1,\ldots,n\}$ možemo spariti svaki od a_k objekata veličine k iz $\mathcal{A}$ sa svakim od b_{n-k} objekata veličine $n-k$ iz $\mathcal{B}$ da dobijemo objekt veličine n u $\mathcal{A}*\mathcal{B}$. Međutim, njihovo preoznačavanje se može učiniti na $\binom{n}{k}$ načina jer ako je $|X|=n$, onda je očito broj uređenih parova (S,T), $S\cap T=\emptyset$, $S\cup T=X$, $|S|=k$, $|T|=n-k$ jednak $\binom{n}{k}$. Stoga je broj objekata veličine n u $\mathcal{A}*\mathcal{B}$ jednak ("binomna konvolucija"):

$$\sum_{k=0}^{n}\binom{n}{k}a_k b_{n-k}.$$

c) To slijedi isto kao c) u Propoziciji 3.
d) Ako je $\mathcal{A}^2=\mathcal{A}*\mathcal{A}$, $\mathcal{A}^3=\mathcal{A}*\mathcal{A}*\mathcal{A}$ itd., onda skupove objekata simbolički možemo reprezentirati s

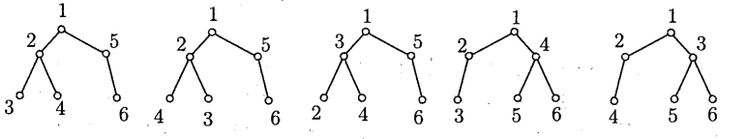
$$\varepsilon+\mathcal{A}+\frac{1}{2!}\mathcal{A}^2+\frac{1}{3!}\mathcal{A}^3+\ldots$$

Iz a) i b) slijedi tvrdnja. □

Primijenit ćemo to na stabla. Ponovimo (i precizirajmo), **stablo** T je konačni skup vrhova tako da vrijedi: a) posebno odabrani vrh zove se **korijen** od T i b) ostali vrhovi (osim korijena) su particionirani u $m\geq 0$ disjuntnih nepraznih skupova $T_1,\ldots,T_m$ koji su stabla i zovu se **podstabla** korijena.

Varijacija ove (rekurzivne) definicije je ova. **Ravninsko** (ili **uređeno**) **stablo** dobivamo ako umjesto b) vrijedi b′) ostali vrhovi (osim korijena) čine *uređenu* particiju $(T_1,\ldots,T_m)$ od $m\geq 0$ disjunktnih nepraznih skupova $T_1,\ldots,T_m$ od kojih je svaki ravninsko (ili uređeno) stablo.

Katkada se stablo još naziva i **neuređeno stablo** (da bismo jasno razlikovali uređena i neuređena). Na donjoj je slici nacrtano pet različitih uređenih stabala i to označenih (jer su im vrhovi označeni) s istim pripadnim (neuređenim) stablom.



Na prvoj je slici vrh 1 korijen, a vrhovi 2 i 5 su **sinovi** (**nasljednik vrha stabla**) od 1; 3 i 4 su sinovi od 2, a 6 sin od 5; isto se tako 1 zove **otac** (**prethodnik**) od 2 i 5. Svaki vrh osim korijena ima jedinstvenog oca. Svaki vrh bez sinova zove se **list** (ili **vanjski vrh**), a ostali **unutarnji vrhovi**. Na prvoj slici, 3, 4 i 6 su listovi.

Kažimo još da za $m\geq 2$ definiramo m-**arno stablo** T tako da a) i b) u gornjoj definiciji zamijenimo s: a″) T je ili prazno ili je jedan vrh (**korijen**) posebno odabran i b″) ostali vrhovi (osim korijena) čine uređenu particiju $(T_1,\ldots,T_m)$ u točno m disjunktnih (možda i praznih) skupova $T_1,\ldots,T_m$, a svako od njih je m-arno stablo.

Šuma je disjunktna unija stabala, tj. to je graf čije su komponente povezanosti stabla.

Primjer 20. Simboličkom metodom odredite EFI i prebrojite a) uređena označena stabla; b) neuređena označena stabla (tzv. **Cayleyeva stabla**).

Rješenje. a) Neka je $\mathcal{U}$ skup (klasa) uređenih označenih stabala, u_n broj takvih stabala s n vrhova, a $U(x) \overset{\text{EFI}}{\longleftrightarrow} (u_n)_{n\geq 0}$. Tada je

$$U(x)=\sum_{T\in\mathcal{U}}\frac{x^{|T|}}{|T|!}=\sum_{n\geq 0}u_n\frac{x^n}{n!}.$$

Uređena označena šuma je ili prazna ili je neuređeni niz uređenih označenih stabala, pa se simbolički može prikazati kao $\varepsilon+\mathcal{U}+\mathcal{U}^2+\mathcal{U}^3+\ldots$ (gdje je $\mathcal{U}^2=\mathcal{U}*\mathcal{U}$ itd.). Stoga je

$$\mathcal{U}=\{\bullet\}*(\varepsilon+\mathcal{U}+\mathcal{U}^2+\mathcal{U}^3+\ldots).$$

Odatle iz Propozicije 4 slijedi

$$U(x)=x(1+U(x)+U(x)^2+U(x)^3+\ldots)=x\frac{1}{1-U(x)}.$$

Iz ove (funkcionalne) jednadžbe po $U(x)$ dobivamo

$$U(x)=\frac{1-\sqrt{1-4x}}{2}.$$

Sada (razvojem u red) slijedi

$$u_n=n!\langle x^n\rangle U(x)=n!\frac{1}{n}\binom{2n-2}{n-1}=\frac{(2n-2)!}{(n-1)!}.$$

b) Neka je $\mathcal{C}$ skup (klasa) Cayleyevih stabala, c_n broj Cayleyevih stabala s n vrhova, a $C(x) \overset{\text{EFI}}{\longleftrightarrow} (c_n)_{n\geq 0}$. Tada je

$$C(x) = \sum_{T\in\mathcal{C}} \frac{x^{|T|}}{|T|!} = \sum_{n\geq 0} c_n \frac{x^n}{n!}.$$

Neuređena označena šuma (ili **Cayleyeva šuma**) je ili prazna ili je skup od k Cayleyevih stabala koji nose različite oznake, pa se simbolički može prikazati kao $\varepsilon + \mathcal{C} + \mathcal{C}^2/2! + \mathcal{C}^3/3! + \cdots + \mathcal{C}^k/k! + \ldots$ (gdje je $\mathcal{C}^2 = \mathcal{C} * \mathcal{C}$ itd.). Zato je

$$\mathcal{C} = \{\bullet\} * (\varepsilon + \mathcal{C} + \mathcal{C}/^2! + \mathcal{C}^3/3! + \ldots).$$

Iz Propozicije 4 odatle slijedi

$$C(x) = x(1 + C(x) + \frac{C(x)^2}{2!} + \frac{C(x)^3}{3!} + \ldots) = xe^{C(x)}.$$

Funkcionalnu jednadžbu $C(x) = xe^{C(x)}$ možemo razriješiti tzv. Lagrangeovom inverzijom (koju ćemo obraditi malo poslije) i kojom dobivamo

$$c_n = n!\langle x^n\rangle C(x) = n^{n-1}.$$

Ako označimo $y = C(x)$, onda iteriranjem jednakosti $y = xe^y$ dobivamo

$$y = xe^y = xe^{xe^y} = xe^{xe^{xe^y}} = \cdots = xe^{xe^{xe^{x\cdots}}}.$$

(Precizno, ako definiramo $y_0 = x$, a za $k \geq 0$, $y_{k+1} = xe^{y_k}$, onda je $y = \lim_{k\to\infty} y_k$.) □

Sada jedna primjena na permutacije.

Primjer 21. Neka je $k \in \mathbb{N}$ čvrst, a $e_k(n)$ broj permutacija π od $[n]$ za koje je $\pi^k = \mathrm{id}$; posebno, za $k = 2$, $e_2(n)$ je broj involutornih permutacija π na $[n]$, tj. $\pi^2 = \pi \circ \pi = \mathrm{id}$. Nađite EFI za $(e_k(n))_{n\geq 0}$ (uz $e_k(0) := 1$). Posebno, što se pobliže može reći o brojevima $e_2(n)$ involutornih permutacija na $[n]$?

Rješenje. Podrobnije ćemo razmotriti brojeve $e_2(n)$. Permutacija $\pi \in S_n$ je involucija, tj. $\pi^2 = \mathrm{id} \iff \pi(\pi(i)) = i,\ \forall i \iff \pi$ se sastoji samo od ciklusa duljine 1 ili 2. No, EFI za cikluse duljine k je očito $x^k/k!$, pa je EFI za cikluse duljine $\leq k$ jednaka

$$\frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^k}{k!}.$$

Permutacija je zapravo skup svojih ciklusa, pa iz Propozicije 4 d) slijedi da je EFI za niz $(e_k(n))_{n\geq 0}$ jednaka

$$E_k(x) = \exp\left(\frac{x}{1!} + \frac{x^2}{2!} + \cdots + \frac{x^k}{k!}\right).$$

Posebno, dakle,

$$E_2(x) = \sum_{n\geq 0} e_2(n)\frac{x^n}{n!} = \exp(x + \frac{x^2}{2}).$$

Ako ovo deriviramo, dobivamo

$$E_2'(x) = \sum_{n\geq 1} e_2(n)\frac{x^{n-1}}{(n-1)!} = (1+x)\exp(x + \frac{x^2}{2}) = (1+x)E_2(x) =$$
$$= (1+x)\sum_{n\geq 0} e_2(n)\frac{x^n}{n!}.$$

Izjednačavanjem koeficijenata uz $x^n/n!$ dobivamo rekurziju

$$e_2(n+1) = e_2(n) + ne_2(n-1),\ n \geq 1.$$

Rabeći $e^{x+x^2/2} = e^x e^{x^2/2}$ nađimo i eksplicitnu formulu za $e_2(n)$. Imamo

$$E_2(x) = \sum_{n\geq 0} e_2(n)\frac{x^n}{n!} = e^x \cdot e^{x^2/2} = \left(\sum_{i\geq 0}\frac{x^i}{i!}\right)\left(\sum_{j\geq 0}\frac{x^{2j}}{2^j j!}\right) =$$
$$= \left(\sum_{i\geq 0}\frac{x^i}{i!}\right)\left(\sum_{j\geq 0}\frac{(2j)!}{2^j j!}\frac{x^{2j}}{(2j)!}\right),$$

pa izjednačavanjem koeficijenata uz x^n slijedi

$$e_2(n) = \sum_{\substack{k=0\\ k \text{ paran}}}^{n} \binom{n}{k}\frac{k!}{2^{k/2}(k/2)!}.$$

Može se pokazati da je asimptotski

$$e_2(n) \sim \frac{1}{\sqrt{2}}\left(\frac{n}{e}\right)^{n/2} e^{\sqrt{n}-1/4}.$$

□

Naglasimo još jednom da eksponencijalna formula $B(x) = e^{A(x)}$ iz Propozicije 4 d) daje vezu među EFI za klase $\mathcal{A}$ i $\mathcal{B}$, pri čemu je $\mathcal{B}$ klasa koju čine skupovi objekata iz $\mathcal{A}$. Katkad je lakše "prebrojiti" $\mathcal{B}$ i tada s eksponencijalnom formulom možemo "odrediti" (ili "prebrojiti") $\mathcal{A}$. Tipični je sljedeći primjer.

Primjer 22. Označimo sa $c(n)$, $n \geq 1$, broj svih povezanih jednostavnih grafova (znači bez petlji i višestrukih bridova) s vrhovima iz n-članog skupa $[n]$. Odredite EFI za niz $(c(n))_{n\geq 1}$.

Rješenje. Neka je $\mathcal{G}$ klasa svih jednostavnih, a $\mathcal{C}$ klasa svih jednostavnih povezanih grafova, i u obje su klase vrhovi označeni. Neka je $g(n)$ broj jednostavnih grafova s vrhovima u skupu $[n]$. Neka je $\mathcal{G} \overset{\text{EFI}}{\longleftrightarrow} G(x) \overset{\text{EFI}}{\longleftrightarrow} (g(n))_{n\geq 0}$, a $\mathcal{C} \overset{\text{EFI}}{\longleftrightarrow} C(x) \overset{\text{EFI}}{\longleftrightarrow} (c(n))_{n\geq 1}$. Svaki objekt u $\mathcal{G}$, tj. (jednostavni) graf je skup svojih komponenti povezanosti; dakle, $\mathcal{G}$ čine skupovi objekata iz $\mathcal{C}$. Stoga iz eksponencijalne formule (Propozicija 4 d)) slijedi

$$G(x) = \exp C(x) = e^{C(x)}. \qquad (\heartsuit)$$

No klasu $\mathcal{G}$ je lako "prebrojiti". Naime, $g(n) = 2^{\binom{n}{2}}$. To je zato, što svaki od $\binom{n}{2}$ parova vrhova iz $[n]$ može biti spojen ili ne spojen bridom (tj. za svaki par vrhova imamo dvije mogućnosti). Stoga je EFI za $(g(n))_{n\geq 0}$ dana s:

$$G(x) = \sum_{n\geq 0} 2^{\binom{n}{2}} \frac{x^n}{n!}. \qquad (\heartsuit\heartsuit)$$

Uvrstimo li $(\heartsuit)$ u $(\heartsuit\heartsuit)$ i logaritmiramo, dobivamo traženu EFI

$$C(x) = \sum_{n\geq 1} c(n)\frac{x^n}{n!} = \ln \sum_{n\geq 0} 2^{\binom{n}{2}} \frac{x^n}{n!}.$$

(Uočite da oba reda $C(x)$ i $G(x)$ imaju radijus konvergencije nula; pa ipak oba imaju kombinatorna značenja. U tome još jednom vidimo snagu i punu vrijednost formalnih redova potencija. Pokušajte s djelovanjem operatora xd/dx dobiti rekurziju za $c(n)$-ove). □

Ovo su bili samo neki primjeri uporabe simboličke metode.

§ 5. Lagrangeova formula inverzije

Promotrimo formalni red potencija $f(x) = a_1x + a_2x^2 + \cdots \in \mathbb{C}[[x]]$ sa slobodnim članom jednakim nula. Formalni red potencija $g(x) \in \mathbb{C}[[x]]$ se zove **kompozicijski inverz** od f, ako je $f(g(x)) = g(f(x)) = x$. Tada pišemo $g(x) = f^{\langle -1\rangle}(x)$. Prvo ćemo objasniti kada $f(x)$ ima kompozicijski inverz.

PROPOZICIJA 5. *Formalni red potencija $f(x) = a_1x + a_2x^2 + \cdots \in \mathbb{C}[[x]]$ ima (jedinstveni) kompozicijski inverz $f^{\langle -1\rangle}(x)$ ako i samo ako je $a_1 \neq 0$.*

Dokaz. Neka je $g(x) = b_1x + b_2x^2 + \cdots \in \mathbb{C}[[x]]$ tako da je $(f(g(x)) = x$. Tada imamo

$$a_1(b_1x + b_2x^2 + \ldots) + a_2(b_1x + b_2x^2 + \ldots)^2 + a_3(b_1x + b_2x^2 + \ldots)^3 + \cdots = x.$$

Izjednačavanjem koeficijenata na obje strane dobivamo beskonačni sustav jednadžbi

$$\begin{aligned} a_1b_1 &= 1 \\ a_1b_2 + a_2b_1^2 &= 0 \\ a_1b_3 + 2a_2b_1b_2 + a_3b_1^3 &= 0 \\ &\vdots \end{aligned}$$

Prvu jednadžbu možemo (jednoznačno) riješiti po b_1 ako i samo ako je $a_1 \neq 0$. Tada možemo riješiti i drugu jednadžbu (jednoznačno) po b_2, pa treću po b_3 itd. Dakle, $g(x)$ postoji (i jedinstven je) ako i samo ako je $a_1 \neq 0$. □

Ponekad se jednadžba $y = f(x)$ može riješiti po x, što daje $x = f^{\langle -1\rangle}(y)$. Tako npr. vrijedi $(e^x - 1)^{\langle -1\rangle} = \ln(1 + x)$, $\left(\frac{a+bx}{c+dx}\right)^{\langle -1\rangle} = \frac{a+cx}{b-dx}$, ako je $ad - bc \neq 0$ itd.

No, u puno slučajeva nećemo moći jednostavno izraziti $f^{\langle -1\rangle}(x)$. Ipak, Lagrangeova formula inverzije će izraziti koeficijente od $f^{\langle -1\rangle}(x)$ pomoću koeficijenata izvjesnih drugih formalnih redova potencija. Lagrange je do te formule došao rješavajući problem lokalnog invertiranja holomorfnih funkcija u kompleksnoj analizi.

TEOREM 1 (Lagrangeova formula inverzije). *Neka je $F(x) = a_1x + a_2x^2 + \cdots \in \mathbb{C}[[x]]$, $a_1 \neq 0$, te $k, n \in \mathbb{Z}$ zadani brojevi. Tada vrijedi*

$$n\langle x^n\rangle F^{\langle -1\rangle}(x)^k = k\langle x^{n-k}\rangle \left(\frac{x}{F(x)}\right)^n = k\langle x^{-k}\rangle F(x)^{-n}. \qquad (22)$$

Ekvivalentna formulacija je ova. Neka je $G(x) \in \mathbb{C}[[x]]$, $G(0) \neq 0$, a $f(x)$ definirana s

$$f(x) = xG(f(x)). \qquad (23)$$

Tada je

$$n\langle x^n\rangle f(x)^k = k\langle x^{n-k}\rangle G(x)^n. \qquad (24)$$

Dokaz. Prvo, da su (22) i (24) ekvivalentne slijedi iz toga što je $f(x) = F^{\langle -1\rangle}(x)$ isto što i $f(x) = xG(f(x))$, gdje je $G(x) = x/F(x)$. Mi ćemo teorem dokazati analitički (iako postoje i kombinatorni dokazi).

Laurentov formalni red je formalni red koji dopušta i negativne eksponente, tj. to je red oblika $y = \sum_{n\in\mathbb{Z}} c_nx^n$. Ključna je opaska ovog dokaza sljedeća. Derivacija Laurentovog reda nema člana uz x^{-1}, tj.

$$\langle x^{-1}\rangle y' = 0. \qquad (25)$$

Neka je $k \in \mathbb{Z}$ zadan broj. Primijetimo da za $k < 0$, potencije $F^{\langle -1\rangle}(x)^k$ i $f(x)^k$ su Laurentovi redovi s negativnim eksponentima koji sežu samo do k-tog, tj. oblika su $\sum_{i\geq k} b_ix^i$. Isto tako i za $k \geq 0$, $F^{\langle -1\rangle}(x)^k$ počinje od k-tog eksponenta. Obje tvrdnje lako slijede indukcijom po $|k|$. Isto tako jasno je da su za $n < k$ objema stranama od (22) i (24) nule. Neka je, dakle,

$$F^{\langle -1\rangle}(x)^k = \sum_{i\geq k} b_ix^i,$$

odakle slijedi, stavimo li $y = F^{\langle -1\rangle}(x)$, tj. $x = F(y)$, da je

$$y^k = \sum_{i\geq k} b_iF(y)^i,$$

pa prelaskom natrag na x umjesto y dobivamo

$$x^k = \sum_{i\geq k} b_iF(x)^i.$$

Deriviramo li objema stranama ove jednakosti, slijedi

$$kx^{k-1} = \sum_{i\geq k} ib_iF(x)^{i-1}F'(x)$$

$$\Rightarrow \frac{kx^{k-1}}{F(x)^n} = \sum_{i\geq k} ib_iF(x)^{i-n-1}F'(x). \qquad (26)$$

Sada razvijmo obje strane od (26) kao Laurentove redove s konačno mnogo negativnih eksponenata. Na primjer,

$$\frac{kx^{k-1}}{F(x)^n} = \frac{kx^{k-1}}{(a_1x + a_2x^2 + \dots)^n} = kx^{k-n-1}(a_1 + a_2x + \dots)^{-n}.$$

Odredimo koeficijent uz x^{-1} na obje strane od (26). Prvo, očito je

$$F(x)^{i-n-1}F'(x) = \frac{1}{i-n}\frac{d}{dx}F(x)^{i-n},\ i \neq n.$$

Zato je koeficijent uz x^{-1} na obje strane od (26) zbog (25) jednak

$$\langle x^{-1}\rangle nb_nF(x)^{-1}F'(x) = \langle x^{-1}\rangle nb_n\frac{a_1 + 2a_2x + \dots}{a_1x + a_2x^2 + \dots} =$$
$$= \langle x^{-1}\rangle nb_n(\frac{1}{x} + \dots) = nb_n.$$

Odatle slijedi da je i za lijevu stranu od (26):

$$\langle x^{-1}\rangle\frac{kx^{k-1}}{F(x)^n} = nb_n = n\langle x^n\rangle F^{\langle -1\rangle}(x)^k,$$

a to je ekvivalentno s prvom jednakošću u (22). Druga jednakost u (22) je trivijalna. Time je formula (22), pa time i teorem dokazan. □

Sada pogledajmo neke primjene Lagrangeove inverzije.

Primjer 23. U Primjeru 20 b) imali smo za $y = C(x)$ funkcionalnu jednadžbu $y = xe^y$.

a) Odredite koeficijent uz x^n od $(xe^{-x})^{\langle -1\rangle}$;

b) Za $k \in \mathbb{Z}$ odredite koeficijent uz x^n k-te potencije $\left((xe^{-x})^{\langle -1\rangle}\right)^k$. Što je kombinatorna posljedica?

Rješenje. a) Tvrdimo (kao što smo iskazali u rješenju Primjera 20 b)) da je

$$(xe^{-x})^{\langle -1\rangle} = \sum_{n\geq 1} n^{n-1}\frac{x^n}{n!}.$$

Stavimo li u (22) da je $F(x) = xe^{-x}$ i $k = 1$, dobivamo

$$\langle x^n\rangle(xe^{-x})^{\langle -1\rangle} = \frac{1}{n}\langle x^{n-1}\rangle e^{nx} = \frac{1}{n}\frac{n^{n-1}}{(n-1)!} = \frac{n^{n-1}}{n!},$$

i odatle slijedi gornja formula.

b) Iz (22) također kao u a) slijedi

$$\langle x^n\rangle\left((xe^{-x})^{\langle -1\rangle}\right)^k = \frac{k}{n}\langle x^{n-k}\rangle e^{nk} = \frac{k}{n}\cdot\frac{n^{n-k}}{(n-k)!}.$$

Kombinatorna je posljedica da je za $k \geq 1$ broj $c_{n,k}$ neuređenih označenih šuma na n vrhova s k komponenti povezanosti jednak

$$c_{n,k} = n!\langle x^n\rangle\frac{C(x)^k}{k!} = \frac{n!}{k!}\cdot\frac{k}{n}\cdot\frac{n^{n-k}}{(n-k)!} = \binom{n-1}{k-1}n^{n-k}.$$

□

Primjer 24. Neka su $(a_n)_{n\geq 0}$ i $(b_n)_{n\geq 0}$ dva niza brojeva za koje vrijedi

$$b_n = \sum_{k\geq 0}\binom{k}{n-k}a_k,$$

za svako $n \geq 0$. Pomoću FI izrazite a_n pomoću b_k-ova (tj. invertirajte ovu formulu).

Rješenje. Neka je $A(x) \overset{\text{FI}}{\longleftrightarrow} (a_n)_{n\geq 0}$, $B(x) \overset{\text{FI}}{\longleftrightarrow} (b_n)_{n\geq 0}$. Pomnožimo gornju formulu za b_n s x^n, pa sumirajmo po $n \geq 0$ i promijenimo poredak sumacije po n i k; imamo:

$$B(x) = \sum_{n\geq 0}b_nx^n = \sum_{n\geq 0}\sum_{k\geq 0}\binom{k}{n-k}a_kx^n = \sum_k a_kx^k\sum_n\binom{k}{n-k}x^{n-k} =$$
$$= \sum_k a_kx^k(1+x)^k = \sum_k a_k(x+x^2)^k = A(x+x^2).$$

Stavimo li $x + x^2 = y$, dobivamo

$$A(y) = B(x) = B(x(y)), \qquad (*)$$

gdje je $x = x(y)$ rješenje jednadžbe $x + x^2 = y$ za koje je $x(0) = 0$. To znači da je $x(y) = (\sqrt{1+4y} - 1)/2$. Sada je $a_n = \langle y^n\rangle A(y) = \langle y^n\rangle B((\sqrt{1+4y} - 1)/2)$, pa bi trebalo izračunati $\langle y^n\rangle((\sqrt{1+4y} - 1)/2)^k$. No, umjesto toga poslužit ćemo se Lagrangeovom inverzijom. Neka je $y = F(x) = x + x^2$. Tada je $x(y) = y^{\langle -1\rangle} = F(x)^{\langle -1\rangle}$, pa (22) povlači

$$n\langle x^n\rangle\left(F(x)^{\langle -1\rangle}\right)^k = k\langle x^{n-k}\rangle\left(\frac{x}{x+x^2}\right)^n = k\langle x^{n-k}\rangle(1+x)^{-n} =$$
$$= k\langle x^{n-k}\rangle\sum_{j\geq 0}\binom{-n}{j}x^j = k\binom{-n}{n-k} =$$
$$= \left(\text{rabeći "reciprocitet" } \binom{-x}{r} = (-1)^r\binom{x+r-1}{r}\right) =$$
$$= (-1)^{n-k}k\binom{2n-k-1}{n-k}.$$

Iz $(*)$ stoga slijedi (za $n \geq 1$):

$$a_n = \langle y^n\rangle A(y) = \langle y^n\rangle B(x(y)) = \langle y^n\rangle B(y^{\langle -1\rangle}) =$$
$$= \langle y^n\rangle\sum_k b_k\left(y^{\langle -1\rangle}\right)^k = \sum_k b_k(-1)^{n-k}\frac{k}{n}\binom{2n-k-1}{n-k}.$$

Dakle,

$$a_n = \sum_{k\geq 0}(-1)^{n-k}\frac{k}{n}\binom{2n-k-1}{n-k}b_k,\ n \geq 1 \text{ i } a_0 = b_0.$$

□

Primjer 25 (t-arna stabla s obzirom na listove). Neka je $t \geq 2$ čvrst cijeli broj. Pomoću FI odredite broj $C_n^{(t)}$ svih t-arnih stabala s n unutrašnjih i $(t-1)n+1$ vanjskih vrhova (listova).

Rješenje. Neka je $\mathcal{T}$ klasa t-arnih stabala. Svaki vrh t-arnog stabla je ili vanjski ili ima t podstabala od kojih je svako t-arno. Stoga je (simbolički) $\mathcal{T} = \{\bullet\} + \mathcal{T} \times \mathcal{T} \times \cdots \times \mathcal{T}$ (t faktora). Neka je $\mathcal{T} \overset{\text{FI}}{\longleftrightarrow} T(x)$. Tada iz Propozicije 3 slijedi

$$T(x) = x + T(x)^t.$$

Stavimo li $y = T(x)$ i $F(y) = y - y^t = x$, onda je traženi broj $C_n^{(t)}$ jednak

$$C_n^{(t)} = \langle x^{(t-1)n+1} \rangle T(x) = \langle x^{(t-1)n+1} \rangle y = \langle x^{(t-1)n+1} \rangle F^{\langle -1 \rangle}(x).$$

Iz formule Lagrangeove inverzije (22) imamo

$$\begin{aligned}
((t-1)n+1)\langle x^{(t-1)n+1} \rangle F^{\langle -1 \rangle}(x) &= \langle x^{(t-1)n} \rangle \left(\frac{x}{F(x)} \right)^{(t-1)n+1} = \\
&= \langle x^{(t-1)n} \rangle \left(\frac{x}{x - x^t} \right)^{(t-1)n+1} = \langle x^{(t-1)n} \rangle \left(1 - x^{t-1}\right)^{-[(t-1)n+1]} = \\
&= \langle x^{(t-1)n} \rangle \sum_{k \geq 0} (-1)^k \binom{-[(t-1)n+1]}{k} x^{(t-1)k} = \\
&= (-1)^n \cdot (-1)^n \binom{(t-1)n+1+n-1}{n} = \frac{1}{(t-1)n+1} \binom{tn}{n}.
\end{aligned}$$

Dakle,

$$C_n^{(t)} = \frac{1}{(t-1)n+1} \binom{tn}{n} = \frac{1}{tn+1} \binom{tn+1}{n},$$

a to je **poopćeni Catalanov broj**, jer je za $t = 2$ to (obični) Catalanov broj. Dakle,

$$T(x) = \sum_{n \geq 0} \frac{1}{tn+1} \binom{tn+1}{n} x^{(t-1)n+1}.$$

□

§ 6. Poopćeni binomni i eksponencijalni redovi i hipergeometrijski redovi

U ovom ćemo se odjeljku prvo pozabaviti dvjema posebnim familijama funkcija izvodnica s kojima raznim manipulacijama dobivamo vrlo bogatu kolekciju raznih netrivijalnih kombinatornih identiteta. Nakon toga ćemo detaljnije promotriti hipergeometrijske redove.

Za (realni) parametar t definiramo **poopćeni binomni red** $\mathcal{B}_t(x)$ i **poopćeni eksponencijalni red** $\mathcal{E}_t(x)$ s formulama

$$\mathcal{B}_t(x) = \sum_{n \geq 0} (tn)^{\underline{n-1}} \frac{x^n}{n!}, \qquad \mathcal{E}_t(x) = \sum_{n \geq 0} (tn+1)^{n-1} \frac{x^n}{n!}. \tag{27}$$

Za $t = 0$ je (zbog $0^{\underline{-1}} = 0^{\underline{0}} = 1$) očito $\mathcal{B}_0(x) = 1 + x$, a $\mathcal{E}_0(x) = e^x$, pa odatle i nazivi "opći binomni i eksponencijalni redovi". Nadalje je očito $\mathcal{B}_1(x) = 1/(1-x)$, dok je za $t = 1$, $\mathcal{E}_1(x) = \mathcal{E}(x)$ red koji je proučavao G. Eisenstein

$$\mathcal{E}(x) = \sum_{n \geq 0} (n+1)^{n-1} \frac{x^n}{n!} = 1 + x + \frac{3}{2}x^2 + \frac{8}{3}x^3 + \frac{125}{24}x^4 + \frac{54}{5}x^5 + \ldots$$

Ako pogledamo $x\mathcal{E}(x)$ i usporedimo to s redom iz Primjera 20 b), vidimo da je $y = (xe^{-x})^{\langle -1 \rangle} = x\mathcal{E}(x)$, pa kako je $y = xe^y$, slijedi da vrijedi funkcionalna jednadžba $\mathcal{E}(x) = e^{x\mathcal{E}(x)}$. Uočite da je $\mathcal{E}(\ln x) = e^{\ln x \mathcal{E}(\ln x)} = x^{\mathcal{E}(\ln x)} = \cdots = x^{x^{x^{\cdots}}}$. Za $t = 2$ je

$$\mathcal{B}_2(x) = \sum_{n \geq 0} \frac{1}{n+1} \binom{2n}{n} x^n = \sum_{n \geq 0} \frac{1}{2n+1} \binom{2n+1}{n} x^n = \frac{1 - \sqrt{1-4x}}{2x},$$

kao što znamo iz Primjera 16. Za $t = -1$ (i malo računanja) imamo

$$\mathcal{B}_{-1}(x) = \sum_{n \geq 0} \binom{1-n}{n} \frac{x^n}{1-n} = \sum_{n \geq 0} \binom{2n-1}{n} \frac{(-x)^n}{1-2n} = \frac{1 + \sqrt{1+4x}}{2}.$$

Sada općenito, prvo napišimo $\mathcal{B}_t(x)$ drukčije:

$$\mathcal{B}_t(x) = \sum_{n \geq 0} \frac{1}{tn+1} \binom{tn+1}{n} x^n = \sum_{n \geq 0} \frac{1}{(t-1)n+1} \binom{tn}{n} x^n. \tag{28}$$

Dokažimo da ovaj red ima sljedeće važno svojstvo. Za svako $r \in \mathbb{R}$ vrijedi:

$$\mathcal{B}_t(x)^r = \sum_{n \geq 0} \frac{r}{tn+r} \binom{tn+r}{n} x^n. \tag{29}$$

Prvo, ako su $t, r \in \mathbb{N}$, onda iz Primjera 25 vidimo da je $\mathcal{B}_t(x)$ FI za niz $(C_n^{(t)})_{n \geq 0}$ poopćenih Catalanovih brojeva. Za klasu $\mathcal{T}$ t-arnih stabala vrijedi (zašto?) simbolička formula

$$\mathcal{T} = \varepsilon + \{\bullet\} \times \mathcal{T} \times \mathcal{T} \times \cdots \times \mathcal{T} \quad (t \text{ faktora } \mathcal{T}).$$

Zbog $C_n^{(t)} = \langle x^n \rangle \mathcal{B}_t(x)$ je $\mathcal{T} \overset{\text{FI}}{\longleftrightarrow} \mathcal{B}_t(x)$, pa iz Propozicije 3 slijedi

$$\mathcal{B}_t(x) = 1 + x\mathcal{B}_t(x)^t, \tag{30}$$

ili što je ekvivalentno, $\mathcal{B}_t(x)^{1-t} = x + \mathcal{B}_t(x)^{-t}$. Ustvari, za $T(x)$ iz Primjera 25 i $\mathcal{B}_t(x)$ vrijedi $T(x) = x\mathcal{B}_t(x^{t-1})$, pa $T(x) = x + T(x)^t$ povlači $x\mathcal{B}_t(x^{t-1}) = x + x^t\mathcal{B}_t(x^{t-1})^t$, što daje opet (30). Izjednačavanjem koeficijenata uz x^n u (30) dobivamo polinomski identitet u t za koji znamo da vrijedi za svako $t \in \mathbb{N} \setminus \{1\}$, pa stoga (30) vrijedi za svako $t \in \mathbb{R}$.

Označimo li $y = \mathcal{B}_t(x)$, onda (30) daje $y = 1 + xy^t$, tj. $(y-1)y^{-t} = x$. Stavimo li $F(y) = (y-1)y^{-t} = x$, tj. $y = F^{\langle -1\rangle}(x)$, onda za $r \in \mathbb{Z}$ iz Lagrangeove formule inverzije (22) uz malo računanja (učinite to) dobijemo da za $r, t \in \mathbb{Z}$ vrijedi

$$\langle x^n\rangle \mathcal{B}_t(x)^r = \frac{1}{tn+r}\binom{tn+r}{n}.$$

Kako je izraz na desnoj strani polinom u t i r, i ta jednakost vrijedi za sve $t, r \in \mathbb{Z}$, slijedi da vrijedi i za sve $t, r \in \mathbb{R}$. Time smo dokazali (29). Na sličan način se može dokazati (učinite to) da je za $r \in \mathbb{R}$:

$$\mathcal{E}_t(x)^r = \sum_{n\geq 0} r\frac{(tn+r)^{n-1}}{n!}x^n, \tag{31}$$

rabeći osnovni identitet (funkcionalnu jednadžbu)

$$\mathcal{E}_t(x) = e^{x\mathcal{E}_t(x)^t}, \quad \text{tj. } \ln \mathcal{E}_t(x) = x\mathcal{E}_t(x)^t, \tag{32}$$

koji slijedi "limesiranjem" formula za $\mathcal{B}_t(x)$, jer vrijedi

$$\mathcal{E}_t(x) = \lim_{y\to\infty} \mathcal{B}_{ty}(x/y)^y.$$

Primjer 26. Za čvrsto $r \in \mathbb{R}$ odredite FI za niz čiji je opći član

$$\text{a) } a_n = \frac{r}{r+2n}\binom{r+2n}{n}; \qquad \text{b) } b_n = \frac{r}{r-n}\binom{r-n}{n}.$$

Rješenje. a) Iz (29) za $t = 2$ dobivamo odmah $(a_n)_{n\geq 0} \overset{\text{FI}}{\longleftrightarrow} \mathcal{B}_2(x)^r$.
b) Iz (29) za $t = -1$ slijedi $(b_n)_{n\geq 0} \overset{\text{FI}}{\longleftrightarrow} \mathcal{B}_{-1}(x)^r$. □

Napomena 1. U svim ovim i sljedećim formulama malo pažnje treba posvetiti slučaju da je neki nazivnik nula; npr. ako je $tn + r = 0$, za neko n u (29) onda smatramo da je $tn + r$ skraćen s pripadnim $tn + r$ u brojniku.

Primjer 27. Dokažite da za čvrste brojeve $r, t \in \mathbb{R}$ vrijedi

$$\text{a) } \frac{\mathcal{B}_t(x)^r}{1-t+t\mathcal{B}_t(x)^{-1}} = \sum_{n\geq 0}\binom{tn+r}{n}x^n; \tag{33}$$

$$\text{b) } \frac{\mathcal{E}_t(x)^r}{1-x t\mathcal{E}_t(x)^t} = \sum_{n\geq 0}(tn+r)^n\frac{x^n}{n!}; \tag{34}$$

$$\text{c) } \mathcal{B}_t(-x)^{-1} = \mathcal{B}_{1-t}(x); \qquad \text{d) } \mathcal{E}_t(x)^t = \mathcal{E}_1(tx).$$

Rješenje. a) Deriviramo li (29) po x i pomnožimo s x, dobivamo

$$x\mathcal{B}_t(x)^{r-1}\mathcal{B}_t'(x) = \sum_{n\geq 0}\frac{n}{tn+r}\binom{tn+r}{n}x^n.$$

Stoga je

$$\langle x^n\rangle(xt\mathcal{B}_t(x)^{-1}\mathcal{B}_t'(x)+1)\mathcal{B}_t(x)^r = t\langle x^n\rangle x\mathcal{B}_t^{r-1}\mathcal{B}_t'(x) + \langle x^n\rangle\mathcal{B}_t(x)^r =$$
$$= \frac{tn}{tn+r}\binom{tn+r}{n} + \frac{r}{tn+r}\binom{tn+r}{n} = \binom{tn+r}{n},$$

pa je $(xt\mathcal{B}_t(x)^{-1}\mathcal{B}_t'(x)+1)\mathcal{B}_t(x)^r$ desna strana od (33). Zato još samo treba pokazati da je

$$xt\mathcal{B}_t(x)^{-1}\mathcal{B}_t'(x) + 1 = \frac{1}{1-t+t\mathcal{B}_t(x)^{-1}}.$$

No, ovo lako slijedi deriviranjem formule (30) po x.

b) Analogno kao a), prvo deriviramo (31), pa provjerimo da je $(xt\mathcal{E}_t^{-1}(x)\mathcal{E}_t'(x)+1)\mathcal{E}_t(x)^r$ desna strana od (34). Deriviranjem (32) po x lako se provjeri da je $xt\mathcal{E}_t^{-1}(x)\mathcal{E}_t'(x) + 1 = 1/(1 - xt\mathcal{E}_t(x)^t)$.

c) Ova "recipročnost" slijedi iz (29) za $r = -1$ i "recipročnosti" za binomne koeficijente.

d) A ovo slijedi iz (31) za $r = t$. □

Primjer 28. Dokažite da za sve realne brojeve r, s, t vrijede **Abelovi identiteti** (ili **poopćene binomne formule**):

$$\text{a) } \sum_{k=0}^{n}\binom{n}{k}(tk+r)^k(tn-tk+s)^{n-k}\frac{r}{tk+r} = (tn+r+s)^n;$$

$$\text{b) } \sum_{k=0}^{n}\binom{n}{k}(tk+r)^k(tn-tk+s)^{n-k}\frac{r}{tk+r}\cdot\frac{s}{tn-tk+s} = \frac{r+s}{tn+r+s}(tn+r+s)^n.$$

(Uočite da za $t = 0$ oni prelaze u binomnu formulu.)

Dokažite nadalje da vrijede **poopćene Vandermondeove konvolucije**:

$$\text{c) } \sum_{k\geq 0}\binom{tk+r}{k}\binom{tn-tk+s}{n-k}\frac{r}{tk+r}\cdot\frac{s}{tn-tk+s} = \frac{r+s}{tn+r+s}\binom{tn+r+s}{n};$$

$$\text{d) } \sum_{k\geq 0}\binom{tk+r}{k}\binom{tn-tk+s}{n-k}\frac{r}{tk+r} = \binom{tn+r+s}{n}.$$

(Uočite da za $t = 0$ oni prelaze u Vandermondeovu konvoluciju.)

Raznim specijalizacijama ovih formula, npr. $r = 0$, $r + s = 0$ itd. dobiju se zanimljivi identiteti.

Rješenje. a) Ovo slijedi odmah rabeći (31) i (34) određivanjem koeficijenata uz x^n na objema stranama jednakosti

$$\mathcal{E}_t(x)^r\cdot\frac{\mathcal{E}_t(x)^s}{1-x t\mathcal{E}_t(x)^t} = \frac{\mathcal{E}_t(x)^{r+s}}{1-x t\mathcal{E}_t(x)^t}.$$

b) Ovo slijedi odmah iz (31), pogledamo li koeficijente uz x^n na objema stranama jednakosti $\mathcal{E}_t(x)^r\cdot\mathcal{E}_t(x)^s = \mathcal{E}_t(x)^{r+s}$.

c) Rabeći (29), ovo slijedi iz $\langle x^n\rangle(\mathcal{B}_t(x)^r\cdot\mathcal{B}_t(x)^s) = \langle x^n\rangle\mathcal{B}_t(x)^{r+s}$.

d) A ovo slijedi iz (33) i

$$\mathcal{B}_t(x)^r\cdot\frac{\mathcal{B}_t(x)^s}{1-t+t\mathcal{B}_t(x)^{-1}} = \frac{\mathcal{B}_t(x)^{r+s}}{1-t+t\mathcal{B}_t(x)^{-1}}.$$

□

Definirajmo sada hipergeometrijske redove. Prvo, geometrijski red $\sum_{k\geq 0} t_k$ je takav da je kvocijent susjednih članova konstantan, tj. $t_{k+1}/t_k = x$ ne ovisi o k; ako je $t_0 = c$, onda je taj red $\sum_{k\geq 0} cx^k$. **Hipergeometrijski red** $\sum_{k\geq 0} t_k$ je red za koji je $t_0 = 1$, a kvocijent susjednih članova je racionalna funkcija indeksa sumacije, tj.

$$\frac{t_{k+1}}{t_k} = \frac{P(k)}{Q(k)},$$

gdje su P i Q polinomi u k. Ako (nad $\mathbb{C}$) potpuno faktoriziramo P i Q, onda možemo pisati

$$\frac{t_{k+1}}{t_k} = \frac{P(k)}{Q(k)} = \frac{(k+a_1)(k+a_2)\dots(k+a_m)}{(k+b_1)(k+b_2)\dots(k+b_n)(k+1)}x, \tag{35}$$

gdje je x konstanta. a_i-ovi su negativni korijeni od P, a b_j-ovi negativni korijeni od Q; ako Q ne sadrži faktor $k+1$, dodamo ga gore i dolje (jer su formule tada puno jednostavnije). Ako ovo teleskopiramo, dobivamo

$$t_k = \frac{a_1^{\overline{k}} a_2^{\overline{k}} \dots a_m^{\overline{k}}}{b_1^{\overline{k}} b_2^{\overline{k}} \dots b_n^{\overline{k}}} \frac{x^k}{k!}, \tag{36}$$

pa tako dolazimo do hipergeometrijskog reda definiranog kao u poglavlju II:

$$F\left(\begin{matrix} a_1,\dots,a_m \\ b_1,\dots,b_n \end{matrix}\middle| x\right) := \sum_{k\geq 0} t_k = \sum_{k\geq 0} \frac{a_1^{\overline{k}} \dots a_m^{\overline{k}}}{b_1^{\overline{k}} \dots b_n^{\overline{k}}} \frac{x^k}{k!}. \tag{37}$$

Da naglasimo broj parametara u brojniku i nazivniku, zapisujemo to i u obliku ${}_mF_n(a_1,\dots,a_m;b_1,\dots,b_n|x)$ ili ${}_mF_n\left(\begin{matrix} a_1,\dots,a_m \\ b_1,\dots,b_n \end{matrix}\middle| x\right)$. Dakle, hipergeometrijski red je naprosto EFI za ove kvocijente. Primjeri!

Primjer 29. Napišite red $\sum_{k\geq 0} t_k$, gdje je $t_k = (k+1)/(2k+1)!$, kao hipergeometrijski.

Rješenje. Očito je $t_0 = 1$, a kvocijent susjednih članova je

$$\frac{t_{k+1}}{t_k} = \frac{(k+2)(2k+1)!}{(k+1)(2k+3)!} = \frac{k+2}{(k+1)(2k+2)(2k+3)} = \frac{(k+2)}{(k+1)(k+3/2)(k+1)}\frac{1}{4}.$$

Stoga je taj red kao hipergeometrijski red

$$\sum_{k\geq 0} t_k = F\left(\begin{matrix} 2 \\ 1, 3/2 \end{matrix}\middle| \frac{1}{4}\right).$$

□

Primjer 30. Izrazite **Besselovu funkciju** J_p, $p \in \mathbb{N}_0$,

$$J_p(x) = \sum_{k\geq 0} \frac{(-1)^k (x/2)^{2k+p}}{k!(k+p)!}$$

kao hipergeometrijsku funkciju.

Rješenje. Prvo, član $t_0 = (x/2)^p/p! \neq 1$. Kvocijent susjeda je

$$\frac{t_{k+1}}{t_k} = \frac{(-1)^{k+1}(x/2)^{2k+2+p} k!(k+p)!}{(-1)^k (x/2)^{2k+p}(k+1)!(k+p+1)!} = \frac{1}{(k+p+1)(k+1)} \cdot \left(-\frac{x^2}{4}\right).$$

Stoga je Besselova funkcija oblika

$$J_p(x) = \frac{(x/2)^p}{p!} \cdot {}_0F_1\left(\begin{matrix} - \\ p+1 \end{matrix}\middle| -\frac{x^2}{4}\right).$$

□

Identifikacija raznih redova (ili redova potencija) kao neki hipergeometrijski red ${}_mF_n(\dots)$ može biti dosta glomazno i dosadno računanje. Srećom, postoje kompjuterski softverski paketi kao npr. `Mathematica`, `Maple` i drugi koji nam uvelike u tome mogu pomoći.

Za bilo koji kompleksni broj z, definiramo $z!$ formulom $\frac{1}{z!} = \lim_{n\to\infty} \frac{1}{n^z}\binom{z+n}{n}$, ili kao $z! = \Gamma(z+1) = \int_0^\infty t^z e^{-t} dt$ ($\Re z > -1$). Γ je **gama funkcija** i možemo je analitički produžiti na $\mathbb{C} \setminus \{-1,-2,-3,\dots\}$. Vrijede sljedeće formule:

$$0! = 1, \qquad z! = z(z-1)!, \qquad (-z)! = \frac{\pi}{(z-1)!\sin \pi z}. \tag{38}$$

Definiramo

$$z^{\underline{w}} = \frac{z!}{(z-w)!}, \qquad z^{\overline{w}} = \frac{\Gamma(z+w)}{\Gamma(z)}, \qquad \binom{z}{w} = \frac{z!}{w!(z-w)!}.$$

(Ako se pojavi ∞/∞ treba uzeti odgovarajući limes.)

Vrijede sljedeći identiteti za hipergeometrijske funkcije:

Gaussov ${}_2F_1$ identitet. Ako je $b \leq 0$ cijeli broj ili $\Re(c-a-b) > 0$, onda je

$${}_2F_1\left(\begin{matrix} a, b \\ c \end{matrix}\middle| 1\right) = \frac{\Gamma(c-a-b)\Gamma(c)}{\Gamma(c-a)\Gamma(c-b)}.$$

Kummerov ${}_2F_1$ identitet.

$${}_2F_1\left(\begin{matrix} a, b \\ 1+b-a \end{matrix}\middle| -1\right) = \frac{\Gamma(b/2+1)\Gamma(b-a+1)}{\Gamma(b+1)\Gamma(b/2-a+1)}.$$

Saalschűtzov ${}_3F_2$ identitet. Ako je $n \in \mathbb{N}$, onda je

$${}_3F_2\left(\begin{matrix} a, b, -n \\ c, a+b-c-n+1 \end{matrix}\middle| 1\right) = \frac{(c-a)^{\overline{n}}(c-b)^{\overline{n}}}{c^{\overline{n}}(c-a-b)^{\overline{n}}}.$$

Dixonov ${}_3F_2$ identitet. Najjednostavnije ga je napisati za $a, b, c \in \mathbb{N}_0$ kao

$$\sum_k (-1)^k \binom{a+b}{a+k}\binom{b+c}{b+k}\binom{c+a}{c+k} = \frac{(a+b+c)!}{a!b!c!}.$$

Prevedeno u hipergeometrijski jezik, vrijedi općenito za $a, b, c \in \mathbb{C}$, $\Re a + \Re b < 1 + \Re(c/2)$:

$$ {}_3F_2\left(\begin{matrix} a, b, c \\ 1+c-a, 1+c-b \end{matrix} \,\middle|\, 1 \right) = \frac{(c/2)!}{c!} \frac{(c-a)!(c-b)!(c/2-a-b)!}{(c/2-a)!(c/2-b)!(c-a-b)!}. $$

Clausenov ${}_4F_3$ identitet. Za $n \in \mathbb{N}_0$ je

$$ {}_4F_3\left(\begin{matrix} a, b, 1/2-a-b-n, n \\ 1/2+a+b, 1-a-n, 1-b-n \end{matrix} \,\middle|\, 1 \right) = \frac{(2a)^{\overline{n}}(a+b)^{\overline{n}}(2b)^{\overline{n}}}{(2a+2b)^{\overline{n}}a^{\overline{n}}b^{\overline{n}}}. $$

Vrijede i mnogi drugi identiteti, no tu ćemo s njima za sada stati. Umjesto toga, navedimo i neke opće transformacije za hipergeometrijske funkcije.

Pfaffov reciprocitet

$$ \frac{1}{(1-x)^a} F\left(\begin{matrix} a, b \\ c \end{matrix} \,\middle|\, \frac{-x}{1-x} \right) = F\left(\begin{matrix} a, c-b \\ c \end{matrix} \,\middle|\, x \right). $$

Deriviranje

$$ F'\left(\begin{matrix} a_1, \ldots, a_m \\ b_1, \ldots, b_n \end{matrix} \,\middle|\, x \right) = \frac{a_1 \ldots a_m}{b_1 \ldots b_n} F\left(\begin{matrix} a_1+1, \ldots, a_m+1 \\ b_1+1, \ldots, b_n+1 \end{matrix} \,\middle|\, x \right). $$

Diferencijalna jednadžba. Ako je $F = {}_mF_n(a_1, \ldots, a_m; b_1, \ldots, b_n|x)$, $D = \frac{d}{dx}$, a $\theta = x\frac{d}{dx}$, onda F zadovoljava (operatorski zapisanu) diferencijalnu jednadžbu

$$ D(\theta + b_1 - 1) \ldots (\theta + b_n - 1)F = (\theta + a_1) \ldots (\theta + a_m)F. $$

Npr., za $F = {}_2F_1(a, b; c|x)$, ta je diferencijalna jednadžba

$$ x(1-x)F''(x) + (c - x(a+b+1))F'(x) - abF(x) = 0. $$

Pogledajmo na primjerima kako nam ova "baza podataka" može poslužiti.

Primjer 31. Za $n \in \mathbb{N}$ izračunajte sume

a) $S_n = \sum_{k \geq 0} (-1)^k \binom{2n}{k}^2$;

b) $T_n = \sum_{k \geq 0} (-1)^k \binom{2n}{k}\binom{2k}{k}\binom{4n-2k}{2n-k}$.

Rješenje. a) Sumu S_n pokušajmo identificirati kao vrijednost nekog hipergeometrijskog reda. Stoga prvo pogledajmo vrijednost kvocijenta susjednih članova sume. Imamo

$$ \frac{t_{k+1}}{t_k} = \frac{(-1)^{k+1}\binom{2n}{k+1}^2}{(-1)^k\binom{2n}{k}^2} = -\frac{(k-2n)^2}{(k+1)^2}. $$

Početni je član $t_0 = 1$, pa iz (35) vidimo da je $a_1 = -2n$, $a_2 = -2n$, te $b_1 = 1$. Prema (36) vidimo da je

$$ S_n = {}_2F_1\left(\begin{matrix} -2n, -2n \\ 1 \end{matrix} \,\middle|\, -1 \right). $$

Sada iz "baze podataka" vidimo da se ovo može izračunati iz Kummerovog identiteta za $a = -2n$, $b = -2n$. Dakle,

$$ S_n = {}_2F_1\left(\begin{matrix} -2n, -2n \\ 1 \end{matrix} \,\middle|\, -1 \right) = \frac{\Gamma(-n+1)\Gamma(1)}{\Gamma(-2n+1)\Gamma(n+1)} = \frac{(-n)!}{(-2n)!} \cdot \frac{1}{n!}. $$

No, kako izračunati $(-n)!/(-2n)!$? Bukvalno uvrštavanje u formulu (38) daje da je ovo neodređeni oblik ∞/∞ (jer $(-n+\varepsilon)! \to \infty$ za $\varepsilon \to 0$). No, ako pogledamo kvocijent, imamo

$$ \frac{(-n)!}{(-2n)!} = \frac{\pi}{(n-1)!\sin n\pi} \cdot \frac{(2n-1)!\sin 2n\pi}{\pi} = \frac{(2n-1)!2\cos n\pi}{(n-1)!} = $$
$$ = (-1)^n \frac{2(2n-1)!}{(n-1)!} \cdot \frac{n}{n} = (-1)^n \frac{(2n)!}{n!}. $$

Tu se, dakle, dogodio "fenomen" da su se singulariteti pokratili i to je redovit slučaj pri uporabi "baze podataka" identiteta. Prema tome, dobivamo da je

$$ S_n = (-1)^n \frac{(2n)!}{n!} \cdot \frac{1}{n!} = (-1)^n \binom{2n}{n}. $$

b) Potpuno slično kao u a). Dakle, pogledamo kvocijent susjednih članova, pa dobivamo da je

$$ \frac{t_{k+1}}{t_k} = \frac{(k+\frac{1}{2})(k-2n)^2}{(k-2n+\frac{1}{2})(k+1)(k+1)}, $$

pa se radi o tipu hipergeometrijskog reda ${}_3F_2(\ldots)$. No, početni član t_0 nije 1, nego je $t_0 = \binom{4n}{2n}$. Dakle,

$$ T_n = \binom{4n}{2n} {}_3F_2\left(\begin{matrix} -2n, \frac{1}{2}, -2n \\ 1, -2n+\frac{1}{2} \end{matrix} \,\middle|\, 1 \right). $$

Iz "baze podataka" vidimo da možemo primijeniti Dixonov identitet za $a = -2n$, $b = 1/2$, $c = -2n$. Uvrštavanje daje

$$ T_n = \binom{4n}{2n} \frac{(-n)!(-2n-\frac{1}{2})!(n-\frac{1}{2})!}{(-2n)!n!(-n-\frac{1}{2})!(-\frac{1}{2})!}. $$

Ako pogledamo kvocijent kao u a), dobivamo (rabeći (38)):

$$ \frac{(-n)!}{(-2n)!} = (-1)^n \frac{(2n)!}{n!}, \qquad \frac{(-2n-\frac{1}{2})!}{(-n-\frac{1}{2})!} = \frac{(-1)^n(n-\frac{1}{2})!}{(2n-\frac{1}{2})!}. $$

Nadalje, za prirodni broj m imamo:

$$ \left(m-\frac{1}{2}\right)! = \left(m-\frac{1}{2}\right)\left(m-\frac{3}{2}\right) \cdot \cdots \cdot \frac{1}{2}\left(-\frac{1}{2}\right)! = $$
$$ = \frac{(2m-1)(2m-3)\ldots 1}{2^m}\left(-\frac{1}{2}\right)! = \frac{(2m)!}{4^m m!}\left(-\frac{1}{2}\right)!. $$

Konačno, uvrštavanjem svega ovoga slijedi $T_n = \binom{2n}{n}^2$. Prema tome, dokazali smo identitet

$$ \sum_{k \geq 0} (-1)^k \binom{2n}{k}\binom{2k}{k}\binom{4n-2k}{2n-k} = \binom{2n}{n}^2. $$

□

Dva su se bitna noviteta za teoriju i praksu u ovom području dogodila relativno nedavno. Prvi je Gosperov algoritam iz 1978. Ako je $(a_k)_{k\geq 1}$ niz za koji je a_k hipergeometrijski (tj. oblika (36)), onda Gosperov algoritam utvrđuje ima li niz parcijalnih suma

$$s_n = \sum_{k=1}^{n} a_k$$

svojstva da je s_{n+1}/s_n racionalna funkcija od n i ako jest, izračunava eksplicitno s_n. Primijetimo da ako je s_{n+1}/s_n racionalna funkcija od n, onda je i a_{n+1}/a_n racionalna, jer je

$$\frac{a_{n+1}}{a_n} = \frac{s_{n+1}/s_n - 1}{1 - s_{n-1}/s_n}.$$

(Uočite da obrat ne mora vrijediti: uzmite npr. $a_k = k!k$.)

Drugi nedavni prodor je tzv. **WZ - metoda**, Wilfa i Zeilbergera, kojom se algoritamski, takoreći kompjuterski dokazuju kombinatorni identiteti u klasi hipergeometrijskih funkcija — uistinu vrlo široke klase. To se dogodilo 1990.-92. (dakle, u doba agresije i Domovinskog rata u Hrvatskoj). To su algoritmi koji provjeravaju naslućene identitete. Ukratko i u bitnome, ta se metoda sastoji u sljedećem. Pretpostavimo da želimo dokazati identitet oblika

$$\sum_k U(n,k) = S(n),\ n \geq 0, \tag{39}$$

gdje je $S(n) \neq 0$, $U(n,k)$ hipergeometrijski. Neka je $F(n,k) = U(n,k)/S(n)$. WZ - metoda traži racionalnu funkciju $R(n,k)$ takvu da ako je $G(n,k) = R(n,k)\cdot F(n,k-1)$, onda za sve $n,k \in \mathbb{Z}$, $n \geq 0$ vrijedi

$$F(n+1,k) - F(n,k) = G(n,k+1) - G(n,k). \tag{40}$$

Pritom mora vrijediti sljedeće:

a) za sve $k \in \mathbb{Z}$, postoji $f_k = \lim_{n\to\infty} F(n,k)$ i konačan je;

b) za sve $n \in \mathbb{Z}$, $n \geq 0$, $\lim_{k\to\pm\infty} G(n,k) = 0$;

c) $\lim_{k\to-\infty} \sum_{n\geq 0} G(n,k) = 0$.

Ako vrijede svi ovi uvjeti i (39) vrijedi za $n = 0$, onda vrijedi i za sve $n \geq 0$.

Tako se npr. Dixonov identitet

$$\sum_k (-1)^k \binom{n+b}{n+k}\binom{b+c}{b+k}\binom{c+n}{c+k} = \frac{(n+b+c)!}{n!b!c!}$$

dokazuje WZ - metodom tako da se uzme

$$R(n,k) = \frac{(b+1-k)(c+1-k)}{2(n+k)(n+b+c+1)}$$

i provjeri da su tada svi navedeni zahtjevi ispunjeni. Taj $R(n,k)$ se sistematski nađe Gosperovom metodom ili novijim tzv. "**metodama kreativnog teleskopiranja**".

O ovim metodama i algoritmima čitatelj može više naučiti iz knjige [57*].

§ 7. Još neke funkcije izvodnice

Mnoge kombinatorne rezultate koje smo do sada našli "pješke" potvrdili smo pomoću FI. Nađimo još neke takve funkcije izvodnice.

Neka su $K_1, K_2, \ldots, K_n \subseteq \mathbb{N}_0$ zadani podskupovi nenegativnih cijelih brojeva, a $S = \{a_1, a_2, \ldots, a_n\}$ zadani n-člani skup **r-kombinacija od S s ponavljanjem tipa** $(K_1, \ldots, K_n)$ je r-kombinacija s ponavljanjem na skupu S u kojoj se element $a_i \in S$ pojavljuje k puta ako i samo ako je $k \in K_i$, $i = 1, 2, \ldots, n$.

PROPOZICIJA 6. *Funkcija izvodnica za r-kombinacije s ponavljanjem od S tipa $(K_1, \ldots, K_n)$ je jednaka*

$$f(x) = \prod_{i=1}^{n} \sum_{k\in K_i} x^k.$$

Dokaz. Elementu $a_i \in S$ pridružimo varijablu x_i. Tada pojavu elementa a_i bilo k_1 puta, bilo k_2 puta itd. u r-kombinaciji opisuje red $x_i^{k_1} + x_i^{k_2} + \ldots$. Stoga je tražena funkcija izvodnica očito jednaka

$$\prod_{i=1}^{n} \sum_{k\in K_i} x_i^k.$$

Budući da se radi o kombinacijama s ponavljanjem, možemo izjednačiti $x_1 = x_2 = \cdots = x_n = x$, čime dobivamo tvrdnju. □

Nakon svih izvršenih množenja vidimo da je broj r-kombinacija od S s ponavljanjem tipa $(K_1, \ldots, K_n)$ jednak broju rješenja jednadžbe $y_1 + y_2 + \cdots + y_n = r$ u skupu $K_1 \times \cdots \times K_n$.

Neki zanimljivi posebni slučajevi su sljedeći.

1. $K_i = \mathbb{N}_0$, $i = 1, .., n$. Tada dobivamo FI za r-kombinaciju s ponavljanjem n-članog skupa;

2. $K_i = \mathbb{N}$, $i = 1, .., n$. Tada je pripadna FI jednaka

$$f(x) = (x+x^2+\ldots)^n = x^n(1-x)^{-n} = x^n \sum_{r\geq 0} \binom{n+r-1}{r} x^r = \sum_{k=n}^{\infty} \binom{k-1}{n-1} x^k,$$

i to je FI za broj r-kombinacija s ponavljanjem od n elemenata u kojima sudjeluju svi elementi n-članog skupa.

3. $K_i = 2\mathbb{N}_0 = \{0, 2, 4, \ldots\}$, $i = 1, .., n$. Tada je FI jednaka

$$f(x) = (1 + x^2 + x^4 + \ldots)^n = (1-x^2)^{-n} = \sum_{r\geq 0} \binom{n+r-1}{r} x^{2r},$$

i to je FI za brojeve kombinacije s ponavljanjem n-članog skupa u kojima se svaki element pojavljuje paran broj puta.

Primjer 32. Nađite EFI za broj razmještaja elemenata n-članog skupa u k različitih kutija, k čvrst.

Rješenje. Neka nam simbol $x_1^{n_1}x_2^{n_2}\dots x_k^{n_k}$ znači da smo u i-tu kutiju stavili n_i elemenata, $i=1,\dots,k$, i jasno $n_1+\dots+n_k=n$. Simbol x_i znači da je element smješten u i-tu kutiju. Polinom $(x_1+x_2+\dots+x_k)^n$ indicira sve razmještaje n-članog skupa u k kutija. Stoga je tražena EFI

$$f(t)=\sum_{n=0}^{\infty}(x_1+x_2+\dots+x_k)\frac{t^n}{n!}=\exp(t\sum_{i=1}^{k}x_i)=\prod_{i=1}^{k}\exp(tx_i).$$

Za $x_1=\dots=x_k=1$, EFI za sve moguće razmještaje u k kutija je $f(t)=\exp(kt)$. Iz multinomnog teorema nalazimo da je broj razmještaja n-članog skupa u k kutija K_i, tako da u K_i dođe n_i elemenata jednak $n!/n_1!\dots n_k!$. □

Slično kao gore, ako su $K_1,\dots,K_n\subseteq\mathbb{N}_0$, a $S=\{a_1,\dots,a_n\}$, onda je **r-permutacija** od S **s ponavljanjem tipa** $(K_1,\dots,K_n)$ ona za koju se a_i pojavljuje u r-permutacija k puta ako i samo ako je $k\in K_i$. Kao i gore dobiva se da je EFI za te permutacije

$$f(x)=\prod_{i=1}^{n}(\sum_{k\in K_i}\frac{x^k}{k!}),$$

a odavde da je broj r-permutacija s ponavljanjem od n elemenata tipa $(K_1,\dots,K_n)$ jednak sumi $\sum r!/r_1!\dots r_n!$, gdje se sumira po svim $r_1\in K_1,\dots,r_n\in K_n$, tako da je $r_1+\dots+r_n=r$. Ako su K_i konačni, to daje broj r-permutacija konačnog multiskupa. A ako su npr. svi $K_i=\mathbb{N}$, onda je EFI za r-permutacije s ponavljanjem od n elemenata u kojima se svaki element pojavljuje bar jedanput jednaka

$$f(x)=\prod_{i=1}^{n}(\sum_{k\geq 1}\frac{x^k}{k!})=\prod_{i=1}^{n}(e^x-1)=(e^x-1)^n.$$

Odavde se lako dobiva (kako?) da je broj r-permutacija s ponavljanjem od n elemenata u kojima se svaki element pojavljuje bar jedanput jednak

$$\sum_{j=0}^{n}(-1)^j\binom{n}{j}(n-j)^r.$$

Primjer 33 (Bernoullijevi[1] brojevi). $B_n, n=0,1,\dots$ se dobivaju s eksponencijalnom funkcijom izvodnicom

$$\sum_{n=0}^{\infty}B_n\frac{x^n}{n!}=\frac{x}{e^x-1}.$$

Dokažite rekurzije za Bernoullijeve brojeve:

$$\sum_{r=0}^{n-1}\binom{n}{r}B_r=\begin{cases}1, & \text{za } n=1\\ 0, & \text{za } n=0,2,3,4,\dots,\end{cases}\qquad(41)$$

$$\sum_{r=0}^{n}\binom{n}{r}B_r=(-1)^nB_n\qquad(42)$$

Rješenje. Primijenit ćemo tzv. **Blissardov simbolični račun**, koji se sastoji u sljedećem. Nizu $a=(a_0,a_1,\dots)$ realnih brojeva pridružimo linearni funkcional $L_a:\mathbb{R}[a]\to\mathbb{R}$ tako da je $L_a(a^n)=a_n$ i koji se po linearnosti proširi do čitavog vektorskog prostora $\mathbb{R}[a]$ polinoma u varijabli a. Onda i njega proširimo do (označenog isto) linearnog operatora $L_a:(\mathbb{R}[a])^*[[t]]\to\mathbb{R}^*[[t]]$ tako da je $L_a\exp(at)=\exp_a t=\sum_{n\geq 0}a_nt^n/n!$, pri čemu je domena algebra eksponencijalnih formalnih redova s koeficijentima u algebri polinoma $\mathbb{R}[a]$ u varijabli a.

Neka je $B=(B_0,B_1,\dots)$ Bernoullijev niz, a $L_B(\exp(Bx))=\frac{x}{e^x-1}$.

Odavde slijedi

$$\begin{aligned}x &= (e^x-1)L_B(\exp(Bx))=L_B(\exp x\exp(Bx)-\exp(Bx))=\\ &= L_B(\exp((B+1)x)-\exp(Bx))=L_B(\sum_{n=0}^{\infty}((B+1)^n-B^n)\frac{x^n}{n!})=\\ &= L_B(\sum_{n=0}^{\infty}(\sum_{r=0}^{n-1}\binom{n}{r}B^r)\frac{x^n}{n!})=\sum_{n=0}^{\infty}(\sum_{r=0}^{n-1}\binom{n}{r}B_r)\frac{x^n}{n!}.\end{aligned}$$

Odavde odmah slijedi (41). Ako gore zamijenimo x s $-x$, dobivamo

$$L_B(\exp(-Bx))=\frac{-x}{e^{-x}-1}=\frac{xe^x}{e^x-1}=L_B(\exp((B+1)x)).$$

Izjednačavanjem koeficijenata uz x^n dobivamo $L_B(B+1)^n=L_B(-B)^n$, a odavde dobivamo (42).

Iz (41) i (42) dobivamo zbog $B_0=1$ da je $B_1=-1/2$, $B_n=(-1)^nB_n$, za $n\neq 1$, tj. $B_3=B_5=B_7=\dots 0$, $B_2=1/6$, $B_4=-1/30$, $B_6=1/42$, $B_8=-1/30$, $B_{10}=5/66$, $B_{12}=-691/2730$ itd. □

Spomenimo ovdje **Dirichletovu funkciju izvodnicu** niza brojeva $a=(a_1,a_2,\dots)$. To je formalni red oblika

$$f_a(s)=\sum_{n=1}^{\infty}\frac{a_n}{n^s}.$$

Taj je red od velikog značenja u multiplikativnoj teoriji brojeva, jer dobro odražava multiplikativnu strukturu cijelih brojeva. Ako je (a_n) multiplikativni niz (tj. $a_{mn}=a_ma_n$ za relativno proste brojeve m i n), onda se red f_a može zapisati u vidu Eulerove produktne formule:

$$f_a(s)=\prod_{p\in\mathbb{P}}(1+\frac{a_p}{p^2}+\frac{a_{p^2}}{p^{2s}}+\frac{a_{p^3}}{p^{3s}}+\dots),$$

što omogućava nalaženje mnogih svojstava od f_a, pa time i svojstava niza a. Za proučavanje aditivnih svojstava niza cijelih brojeva $0\leq a_1\leq a_2\leq\dots$ pogodnija je funkcija

$$f(s)=\sum_{k=1}^{\infty}s^{a_k},$$

[1] Jacob Bernoulli (1654 – 1705), brat Johanna I (1667 – 1748), a stric Daniela (1700 – 1782), švicarski matematičari

jer zbrajanje takva dva niza odgovara množenju ovakvih funkcija izvodnica.

Napomenimo da ako je niz $a = (1, 1, \ldots)$, onda je Dirichletova FI poznata **Riemannova**[2] **zeta funkcija** iz teorije brojeva

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Ona je dobro definirana za realne $s > 1$, a iz ocjene za harmonijski broj H_n lako se vidi da $\zeta(1)$ divergira, a za sve realne $s > 1$ konvergira. Zeta funkcija ima kanonsko proširenje na čitavu kompleksnu ravninu (s jednostavnim polom u $s = 1$). Za nju (i dalje) vrijedi Eulerova produktna formula

$$\zeta(s) = \prod_{p \in \mathbf{P}} \frac{1}{1 - p^{-s}}.$$

Nije teško pokazati da je $\zeta(-2n) = 0$, za $n \in \mathbb{N}$, dok je

$$\zeta(2n) = (-1)^{n-1} \frac{2^{2n-1}}{(2n)!} B_{2n} \pi^{2n},$$

pa je tako npr. $\zeta(2) = 1 + 1/2^2 + 1/3^2 + \cdots = \pi^2/6$, $\zeta(4) = 1 + 1/2^4 + 1/3^4 + \cdots = \pi^4/90$ itd. O brojevima $\zeta(2n+1)$ zasad se ne zna mnogo, zna se npr. da je $\zeta(3)$ iracionalan (R. Apéry, 1979). Jedna od najspektakularnijih slutnji u čitavoj matematici je **Riemannova hipoteza** (oko 1860.), koja kaže da sve netrivijalne nultočke zeta funkcije (tj. sve koje su različite od parnih negativnih brojeva) leže na pravcu

$$\Re(s) = \frac{1}{2}.$$

Među mnogobrojnim ekvivalentnim formulacijama Riemannove slutnje možda je najelementarniji oblik nejednakost zbroja svih djelitelja prirodnog broja n pomoću harmonijskog broja H_n:

$$\sum_{d|n} d \leq H_n + e^{H_n} \ln H_n, \ n \in \mathbb{N}.$$

Na kraju ovog odlomka kažimo još nešto o kompoziciji EFI. Neka su

$$A(x) = \sum_{k=0}^{\infty} a_k \frac{x^k}{k!}, \qquad B(x) = \sum_{l=0}^{\infty} b_l \frac{x^l}{l!}$$

EFI za nizove (a_k) i (b_l), $b_0 = 0$. Tada je formalna kompozicija $C = A \circ B$, $C(x) = A(B(x))$ dobro definirani formalni red

$$C(x) = \sum_{n=0}^{\infty} c_n \frac{x^n}{n!}.$$

[2]Bernhardt Riemann (1826 – 1866), njemački matematičar

PROPOZICIJA 7 (Faá di Bruno, 1857). *Uz gornje oznake vrijedi*

$$c_0 = 0, \quad c_n = \sum_{k=1}^{n} a_k B_{n,k}(b_1, b_2, \ldots, b_{n-k+1}), n \geq 1,$$

gdje su $B_{n,k}$ **eksponencijalni Bellovi polinomi** *definirani s*

$$\sum_{n,k=0}^{\infty} B_{n,k}(x_1, \ldots, x_{n-k+1}) \frac{t^n u^k}{n!} = \exp(u \sum_{n=1}^{\infty} x_m \frac{t^m}{m!}).$$

Ova formula Faá di Brune omogućava nam računanje uzastopnih derivacija funkcija, kao npr. $\log A(x)$, u terminima derivacija od $A(x)$. Dokaz te formule ide izravno uporabom multinomne formule i prepuštamo ga čitatelju (ne moramo baš sve ovdje dokazati; ako vam dokaz ne ide, pogledajte [51] ili [194]).

§ 8. Tri osnovne vrste funkcija izvodnica

Na temelju dosadašnjeg iskustva vidimo da se u kombinatorici najčešće pojavljuju (u teoriji i praksi) tri osnovne vrste funkcija izvodnica. To su: racionalne, algebarske i D-konačne (tj. diferencijabilno konačne). Algebarske su funkcije prirodno poopćenje racionalnih, a D-konačne prirodno poopćenje algebarskih funkcija. Stoga imamo hijerarhiju

D-konačne FI
|
algebarske FI
|
racionalne FI

U ovoj ćemo točki kratko opisati njihova osnovna strukturna svojstva. Počnimo od **racionalnih funkcija izvodnica** u jednoj varijabli. To su funkcije izvodnice oblika $F(x) = \sum_{n \geq 0} f(n) x^n$ koje su racionalne funkcije u prstenu $\mathbb{C}[[x]]$. To znači da postoje polinomi $P(x), Q(x) \in \mathbb{C}[x]$, tako da je $F(x) = P(x)Q(x)^{-1}$ u $\mathbb{C}[[x]]$. Pritom pretpostavljamo da je $Q(0) \neq 0$ pa stoga postoji $Q(x)^{-1}$ u $\mathbb{C}[[x]]$. Umjesto $\mathbb{C}$ možemo uzeti bilo koje polje K karakteristike 0, ali ćemo i dalje raditi sa $\mathbb{C}$. Osnovna svojstva racionalnih funkcija izvodnica dana su sljedećim teoremom.

TEOREM 2 (osnovna svojstva racionalne FI). *Neka je* $d \in \mathbb{N}$, *te* $a_1, a_2, \ldots, a_d$ *zadani kompleksni brojevi,* $a_d \neq 0$. *Za funkciju* $f : \mathbb{N}_0 \to \mathbb{C}$ *sljedeći su uvjeti ekvivalentni.*

(i)
$$\sum_{n \geq 0} f(n) x^n = \frac{P(x)}{Q(x)}, \tag{43}$$

gdje su $Q(x) = 1 + a_1 + a_2 x^2 + \cdots + a_d x^d$ *i* $P(x)$ *polinomi u varijabli* x, *a* P *je stupnja* $< d$;

(ii) Za svako $n \geq 0$ *vrijedi rekurzija reda* d

$$f(n+d) + a_1 f(n+d-1) + a_2 f(n+d-2) + \cdots + a_d f(n) = 0; \tag{44}$$

(iii) Za svako $n \geq 0$ imamo "eksplicitnu" formulu

$$f(n) = \sum_{i=1}^{k} P_i(n) c_i^n, \tag{45}$$

pri čemu je $1 + a_1 x + a_2 x^2 + \cdots + a_d x^d = \prod_{i=1}^{k} (1 - c_i x)^{d_i}$, gdje su c_i različiti a $P_i(n)$ polinom u n stupnja $< d_i$, $i = 1, .., k$.

Dokaz. Za čvrsti polinom $Q(x) = 1 + a_1 x + \cdots + a_d x^d$, definirajmo sljedeće (kompleksne) vektorske prostore.

$V_1 := \{f : \mathbb{N}_0 \to \mathbb{C} |$ vrijedi (i)$\}$, $V_2 := \{f : \mathbb{N}_0 \to \mathbb{C} |$ vrijedi (ii)$\}$,
$V_3 := \{f : \mathbb{N}_0 \to \mathbb{C} |$ vrijedi (iii)$\}$, te pomoćni prostor

$V_4 := \{f : \mathbb{N}_0 \to \mathbb{C} | \sum_{n \geq 0} f(n) x^n = \sum_{i=1}^{k} G_i(x)(1 - c_i x)^{-d_i}$, gdje su

$G_i(x)$ polinomi stupnja $< d_i$, a brojevi c_i, d_i imaju značenje kao u (iii).$\}$

Teorem će biti dokazan ako pokažemo da je $V_1 = V_2 = V_3$. Prvo pokažimo da je $\dim_{\mathbb{C}} V_i = d$, $i = 1, 2, 3, 4$. U (i) možemo slobodno odabrati d koeficijenata od $P(x)$. Zato je $\dim V_1 = d$.

U (ii) slobodno možemo odabrati vrijednosti od $f(0), f(1), \ldots, f(d-1)$, čime su ostale vrijednosti $f(n)$ jednoznačno određene. Zato je $\dim V_2 = d$. U (iii) slobodno možemo odabrati d koeficijenata polinoma $P_1(n), \ldots, P_k(n)$, pa je $\dim V_3 = d$. Za V_4 slobodno možemo odabrati d koeficijenata od $G_1(x), \ldots, G_k(x)$, pa je $\dim V_4 = d$.

Neka je sada $f \in V_1$. Izjednačavanjem koeficijenata uz x^n u identitetu $Q(x) \sum_{n \geq 0} f(n) x^n = P(x)$, dobivamo da je $f \in V_2$. Iz $\dim V_1 = \dim V_2$ tada slijedi $V_1 = V_2$.

Sada uzmimo $f \in V_4$. Stavimo li sumu $\sum_{i=1}^{k} G_i(x)(1 - c_i x)^{-di}$ nad zajednički nazivnik, odmah dobivamo da je $f \in V_1$. Zato je $V_4 \subseteq V_1$, a zbog $\dim V_4 = \dim V_1$ slijedi $V_1 = V_4$. Time smo do sada pokazali da je $V_1 = V_2 = V_4$.

Nadalje, suma $\sum_{i=1}^{k} G_i(x)(1 - c_i x)^{-d_i}$ je konačna linearna kombinacija članova oblika $x^j (1 - cx)^{-s}$, gdje je $j < s$. No, znamo da je

$$\frac{x^j}{(1-cx)^s} = x^j \sum_{n \geq 0} (-c)^n \binom{-s}{n} x^n = \sum_{m \geq 0} x^m c^m c^{-j} \binom{s+m-1-j}{s-1}.$$

Izraz $c^{-j}\binom{s+m-1-j}{s-1}$ je polinom od m stupnja $s-1$. Odatle slijedi da je $V_4 \subseteq V_3$. Iz $\dim V_3 = \dim V_4$ tada dobivamo da je $V_4 = V_3$. Konačno je stoga $V_1 = V_2 = V_3 (= V_4)$ i teorem je dokazan. □

Tako, na primjer, za Fibonaccijeve brojeve $F_n = f(n)$ znamo da je $f(n+2) - f(n+1) - f(n) = 0$, te $f(0) = 0$, $f(1) = 1$. Tu je $d = 2$, $a_1 = a_2 = -1$, pa iz Teorema 2 slijedi da postoje brojevi A i B tako da je $\sum_{n \geq 0} f(n) x^n = (Ax + B)/(1 - x - x^2)$.

Izjednačavanjem koeficijenata uz 1 i uz x dobivamo (kao i u Primjeru 11):

$$\sum_{n \geq 0} F_n x^n = \frac{x}{1 - x - x^2}.$$

Kako je $1 - x - x^2 = (1 - \alpha x)(1 - \beta x)$, $\alpha = (1 + \sqrt{5})/2$, $\beta = (1 - \sqrt{5})/2$, to opet iz Teorema 2 slijedi $f(n) = F_n = a\alpha^n + b\beta^n$, za neke brojeve a i b. Uzmemo li $n = 0$ i $n = 1$ dobivamo (opet) $a = 1/\sqrt{5} = -b$.

Primjer 34 (FI za Stirlingove brojeve $S(n,k), k \geq 0$, čvrst). Nađite FI za niz $(S(n,k))_{n \geq 0}$ Stirlingovih particijskih brojeva, pri čemu je $k \geq 0$ čvrst. Pomoću toga nađite eksplicitnu formulu za $S(n,k)$.

Rješenje. Osnovnu rekurziju $S(n,k) = S(n-1, k-1) + kS(n-1,k)$ (usp. Prop. 17, pogl. II) pomnožimo s x^n i sumirajmo po $n \geq 0$. Neka je $S_k \overset{\text{FI}}{\longleftrightarrow} (S(n,k))_{n \geq 0}$. Tada slijedi

$$S_k(x) = xS_{k-1}(x) + kxS_k(x), \quad k \geq 1 (S_0(x) = 1),$$

a odavde

$$S_k(x) = \frac{x}{1 - kx} S_{k-1}(x).$$

Množenjem (teleskopiranjem) ovih formula slijedi

$$S_k(x) = \sum_{n=0}^{\infty} S(n,k) x^n = \frac{x^k}{(1-x)(1-2x)\ldots(1-kx)}. \tag{+}$$

Iz razvoja u parcijalne razlomke

$$\frac{1}{(1-x)(1-2x)\ldots(1-kx)} = \sum_{j=1}^{k} \frac{\alpha_j}{1 - jx},$$

da nađemo α_j, pomnožimo obje strane s $1 - jx$ i stavimo $x = 1/j$. Dobivamo

$$\begin{aligned} \alpha_j &= \frac{1}{(1-1/j)(1-2/j)\ldots(1-(j-1)/j)(1-(j+1)/j)\ldots(1-k/j)} = \\ &= (-1)^{k-j} \frac{j^{k-1}}{(j-1)!(k-j)!}, \quad 1 \leq j \leq k. \end{aligned} \tag{++}$$

Zato je iz (+) i (++):

$$\begin{aligned} S(n,k) &= \langle x^n \rangle \frac{x^k}{(1-x)(1-2x)\ldots(1-kx)} = \langle x^{n-k} \rangle \frac{1}{(1-x)(1-2x)\ldots(1-kx)} \\ &= \langle x^{n-k} \rangle \sum_{j=1}^{k} \frac{\alpha_j}{1-jx} = \sum_{j=1}^{k} \alpha_j \langle x^{n-k} \rangle \frac{1}{1-jx} = \sum_{j=1}^{k} \alpha_j j^{n-k} = \\ &= \sum_{j=1}^{k} (-1)^{k-j} \frac{j^{k-1}}{(j-1)!(k-j)!} j^{n-k} = \sum_{j=1}^{k} (-1)^{k-j} \frac{j^{n-1}}{(j-1)!(k-j)!} = \\ &= \sum_{j=1}^{k} (-1)^{k-j} \binom{k-1}{j-1} j^{n-1} \quad \text{(usp. Primjer 31, pogl. III).} \end{aligned}$$

Na drugi način, interpretirajte osnovnu rekurziju kao rekurziju (44) i primijenite Teorem 2. □

Sada definirajmo algebarske FI. Kažemo da je formalni red potencija $u \in \mathbb{C}[[x]]$ **algebarski formalni red** (nad $\mathbb{C}$) ako postoje polinomi $P_0(x), \ldots, P_d(x) \in \mathbb{C}[x]$ koji nisu svi 0, tako da je

$$P_0(x) + P_1(x)u + \cdots + P_d(x)u^d = 0. \tag{46}$$

Najmanji prirodni broj d za koji vrijedi (46) zove se **stupanj** od u, i pišemo $\deg u = d$.

Uočimo da algebarski red u ima stupanj 1 ako i samo ako je u racionalna. Nije teško pokazati (učinite to sami) da je skup $\mathbb{C}_{\text{alg}}[[x]]$ svih algebarskih formalnih redova potprsten (ili čak podalgebra) od $\mathbb{C}[[x]]$ koji sadrži prsten $\mathbb{C}(x) \cap \mathbb{C}[[x]]$ svih racionalnih funkcija P/Q, gdje su $P, Q \in \mathbb{C}[x]$, $Q(0) \neq 0$.

Tako je, naprimjer, red $u = \sum_{n\geq 0} \binom{2n}{n} x^n$ algebarski. Zaista. Sjetimo se da je FI za niz $\binom{2n}{n}$ jednaka $u = 1/\sqrt{1-4x}$. Stoga je $(1-4x)u^2 - 1 = 0$, pa je u algebarska stupnja 1 ili 2 nad $\mathbb{C}$. Kada bi stupanj od u bio 1, tj. $\deg u = 1$, onda bi postojali polinomi $P(x), Q(x) \in \mathbb{C}[x]$ tako da je $u = P(x)/Q(x)$, pa bi bilo

$$(1-4x)P(x)^2 = Q(x)^2.$$

Stupanj polinoma na lijevoj strani je neparan, a na desnoj paran broj, što je kontradikcija. Dakle, u je algebarski red stupnja 2.

Općenitiji je sljedeći primjer.

Primjer 35. Neka je $k \in \mathbb{N}$ čvrst prirodni broj, a

$$u = u(x) = \sum_{n\geq 0} \binom{kn}{n} x^n.$$

Dokažite da je u algebarski red potencija.

Rješenje. Osnovni je trik ovdje da se pogleda red FI za poopćene Catalanove brojeve

$$T_k(x) = T(x) = \sum_{n\geq 0} \frac{1}{kn+1}\binom{kn+1}{n} x^{(k-1)n+1} = \sum_{n\geq 0} \frac{1}{(k-1)n+1}\binom{kn}{n} x^{(k-1)n+1}.$$

(vidi Primjer 25 i tekst iza formule (30)). Znamo da je $T(x) = x + T(x)^k$. Odmah se vidi da je $x^{k-1}u = T'$. Deriviranjem jednakosti $T(x) = x + T^k(x)$, dobivamo $T' = 1 + kT'T^{k-1}$, a množenje ovoga s T daje $T'T = T + kT'(T-x)$. Odavde je

$$T = \frac{kT'x}{1+(k-1)T'}.$$

Opet iz $T = x + T^k$ odatle dobivamo

$$\frac{kT'x}{1+(k-1)T'} = x + \left(\frac{kT'x}{1+(k-1)T'}\right)^k \Rightarrow$$

$$\frac{T'-1}{1+(k-1)T'} = x^{k-1}\left(\frac{kT'}{1+(k-1)T'}\right)^k.$$

Stoga je

$$\frac{u-1}{1+(k-1)u} = x\left(\frac{ku}{1+(k-1)u}\right)^k.$$

Odavde množenjem sa zajedničkim nazivnikom dobivamo jednakost tipa (46), pa je zato u algebarski red potencija. Slično se dobije čak i za $k \in \mathbb{Q}$. □

Primjer 36. Dokažite da e^x nije algebarska. Točnije, dokažite

$$\sum_{n\geq 0} \frac{x^n}{n!} \notin \mathbb{C}_{\text{alg}}[[x]].$$

Rješenje. Pretpostavimo da je e^x algebarska stupnja d. Po definiciji tada postoje polinomi $P_i(x) \in \mathbb{C}[x]$, $i = 0, 1, .., d$ tako da je

$$P_d(x)e^{dx} + P_{d-1}(x)e^{(d-1)x} + \cdots + P_0(x) = 0, \tag{$*$}$$

pri čemu je stupanj polinoma $P_d(x)$, tj. $\deg P_d(x)$ minimalan. Deriviramo li tu jednakost po x i oduzmemo od toga $(*)$ pomnoženu s d dobijemo:

$$(P_0' - dP_0) + [P_1' - (d-1)P_1]e^x + \cdots + (P_{d-1}' - P_{d-1})e^{(d-1)x} + P_d'e^{dx} = 0.$$

No, ova jednakost ima ili stupanj manji od d ili je inače u kontradikciji s minimalnošću od $\deg P_d(x)$.

Malo općenitije, može se pokazati (vidi [181], vol. II, pogl. 8) da ako je $F(x) \in \mathbb{Q}[[x]]$ algebarska, onda postoji $m \in \mathbb{N}$ tako da je $F(mx) \in \mathbb{Z}[[x]]$. Odatle također slijedi da $e^x \notin \mathbb{C}_{\text{alg}}[[x]]$ (kako?). □

Kako smo već napomenuli, skup $\mathbb{C}_{\text{alg}}[[x]]$ svih algebarskih redova potencija čini podalgebru od $\mathbb{C}[[x]]$. Prema tome, ako su $u, v \in \mathbb{C}_{\text{alg}}[[x]]$, a $\alpha, \beta \in \mathbb{C}$, onda su $\alpha u + \beta v$, $uv \in \mathbb{C}_{\text{alg}}[[x]]$. No još je jedna operacija s redovima potencija od interesa u kombinatorici. To je **Hadamardov produkt** $u * v$ dvaju redova potencija u, v. Ako je $u = \sum_{n\geq 0} f(n)x^n$, a $v = \sum_{n\geq 0} g(n)x^n$, onda je $u * v := \sum_{n\geq 0} f(n)g(n)x^n$. Ako su u, v algebarske, onda $u * v$ ne mora biti algebarska. Primjer za to je $u = v = (1-4x)^{-1/2} = \sum \binom{2n}{n} x^n$, jer se može pokazati da $\sum_{n\geq 0} \binom{2n}{n}^2 x^n$ nije algebarska.

(To slijedi iz teorema R. Jungena, vidi Comm. Math. Helv. 3 (1931), 266 – 306, koji kaže da ako je $y = \sum a_n x^n \in \mathbb{C}[[x]]$ algebarski i $a_n \sim cn^r\alpha^n$ za neke konstante $0 \neq c \in \mathbb{C}$, $0 > r \in \mathbb{R}$ i $0 \neq \alpha \in \mathbb{C}$, onda je $r = s + 1/2$, za neko $s \in \mathbb{Z}$. Iz Stirlingove asimptotske formule slijedi, međutim, da je $\binom{2n}{n}^2 \sim cn^{-1}\alpha^n$. Zato $\sum \binom{2n}{n}^2 x^n$ nije algebarski.) Mi ćemo sada dokazati da za Hadamardov produkt ipak vrijedi nešto slabije svojstvo.

PROPOZICIJA 8. *Neka je $u \in \mathbb{C}[[x]]$ algebarska, a $v \in \mathbb{C}[[x]]$ racionalna. Tada je Hadamardov produkt $u * v$ algebarska.*

Dokaz. Neka je $u = \sum f(n)x^n$, $v = \sum g(n)x^n$. Iz Teorema 2 slijedi da postoje brojevi $c_1, \ldots, c_r \in \mathbb{C}$ i polinomi $P_1, \ldots, P_r \in \mathbb{C}[x]$ tako da je

$$g(n) = \sum P_i(n)c_i^n, \tag{47}$$

za sve dovoljno velike n. No iz definicije algebraičnosti se lako vidi da promjena konačno mnogo koeficijenata od v ne utječe na to je li $u*v$ algebarska. Stoga možemo pretpostaviti da (47) vrijedi za sve $n \geq 0$. Kako je $\mathbb{C}_{\text{alg}} \subseteq \mathbb{C}[[x]]$ podalgebra, slijedi da je linearna kombinacija algebarskih opet algebarska funkcija. Zato je dovoljno dokazati da su za $0 \neq c \in \mathbb{C}$ redovi oblika $u_1 = \sum c^n f(n) x^n$ i $u_2 = \sum n f(n) x^n$ algebarski.

Neka je $P(x,y) \in \mathbb{C}[x,y]$ nenul polinom za koji je $P(x,u) = 0$. Tada je $P(cx,y) \neq 0$, a $P(cx,u_1) = 0$. Stoga je u_1 algebarska. Nadalje, pogledajmo derivaciju

$$0 = \frac{d}{dx} P(x,u) = \left.\frac{\partial P(x,y)}{\partial x}\right|_{y=u} + u' \left.\frac{\partial P(x,y)}{\partial y}\right|_{y=u}. \tag{48}$$

Pretpostavimo li da smo uzeli polinom $P(x,y)$ minimalnog stupnja u y, slijedi da je $\partial P(x,y)/\partial y$ nenul polinom u y manjeg stupnja nego P. Zato je $\partial P(x,y)/\partial y|_{y=u} \neq 0$. Iz (48) tada slijedi da je

$$u' = -\frac{\left.\frac{\partial P(x,y)}{\partial x}\right|_{y=u}}{\left.\frac{\partial P(x,y)}{\partial y}\right|_{y=u}}$$

racionalna funkcija od x i u. Stoga je u' algebarska. Zbog toga je $u_2 = xu'$ algebarska, čime je dokaz gotov. □

Tako primjerice (bez računanja) iz ove Propozicije slijedi da su $\sum n\binom{2n}{n} x^n$, $\sum nC_n x^n$, $\sum F_n C_n x^n$ isto algebarske.

Važno svojstvo racionalnih funkcija izvodnica je da njezini koeficijenti zadovoljavaju linearnu rekurziju s konstantnim koeficijentima. Koeficijenti algebarske funkcije izvodnice također zadovoljavaju rekurzije, ali s polinomskim koeficijentima. Takve će rekurzije zadovoljavati i općenitiji redovi, o čemu ćemo sada reći nešto više.

PROPOZICIJA 9. *$\mathbb{C}(x)$ neka je polje racionalnih funkcija s koeficijentima iz $\mathbb{C}$. Neka je $u \in \mathbb{C}[[x]]$. Tada su sljedeća svojstva ekvivalentna:*

(i) Vektorski prostor nad $\mathbb{C}(x)$ razapet s u i svim derivacijama $u', u'', \ldots$ je konačno dimenzionalan, tj.

$$\dim_{\mathbb{C}(x)} [\mathbb{C}(x)u + \mathbb{C}(x)u' + \mathbb{C}(x)u'' + \ldots] < \infty.$$

(ii) Postoje polinomi $p_0(x), p_1(x), \ldots, p_d(x) \in \mathbb{C}[x]$, $p_d(x) \neq 0$, tako da je (uz oznaku $u^{(j)} = d^j u/dx^j$)

$$p_d(x)u^{(d)} + p_{d-1}u^{(d-1)} + \cdots + p_1(x)u' + p_0(x)u = 0. \tag{49}$$

(iii) Postoje polinomi $q_0(x), \ldots, q_m(x)$, $q(x) \in \mathbb{C}[x]$, $q_m(x) \neq 0$, tako da je

$$q_m(x)u^{(m)} + q_{m-1}u^{(m-1)} + \cdots + q_1(x)u' + q_0(x)u = q(x). \tag{50}$$

Ako u zadovoljava bilo koje (stoga i svako) od ovih triju svojstava, onda se u naziva **D-konačan** (ili **diferencijabilno konačan**) **red potencija**.

Dokaz. *(i)* $\Rightarrow$ *(ii)*. Pretpostavimo da je $\dim[\mathbb{C}(x)u + \mathbb{C}(x)u' + \ldots] = d$. Tada su $u, u', \ldots, u^{(d)}$ linearno zavisni nad $\mathbb{C}(x)$. Napišemo li tu linearnu zavisnost s koeficijentima iz $\mathbb{C}(x)$ i "počistimo" li sve nazivnike tako da koeficijenti postanu polinomi, dobijemo (49).
(ii) $\Rightarrow$ *(iii)*. Ovo je trivijalno.
(iii) $\Rightarrow$ *(i)*. Pretpostavimo da vrijedi (50) i neka je stupanj polinoma $q(x) = s$. Deriviramo li (50) $s+1$ puta, dobivamo jednakost (49), pri čemu je $d = m+s+1$, a $p_d(x) = q_m(x) \neq 0$. Riješimo li tu jednakost po $u^{(d)}$, dobivamo da je

$$u^{(d)} \in \mathbb{C}(x)u + \cdots + \mathbb{C}(x)u^{(d-1)}. \tag{51}$$

Deriviramo li jednakost koja $u^{(d)}$ izražava kao $\mathbb{C}(x)$-linearnu kombinaciju od u, u', $\ldots$, $u^{(d-1)}$, dobivamo da je

$$u^{(d+1)} \in \mathbb{C}(x)u + \mathbb{C}(x)u' + \cdots + \mathbb{C}(x)u^{(d)}.$$

No, zbog (51) je $\mathbb{C}(x)u + \mathbb{C}(x)u' + \cdots + \mathbb{C}(x)u^{(d)} = \mathbb{C}(x)u + \mathbb{C}(x)u' + \cdots + \mathbb{C}(x)u^{(d-1)}$. Nastavimo li tako, dobivamo induktivno da je za svako $k \in \mathbb{N}_0$

$$u^{(d+k)} \in \mathbb{C}(x)u + \mathbb{C}(x)u' + \cdots + \mathbb{C}(x)u^{(d-1)}.$$

Zbog toga vrijedi (i). □

Tako je, primjerice, $u = e^x$ D-konačan, jer je $u' = u$. I općenitije, svaka linearna kombinacija redova oblika $x^m e^{ax}$ $(m \in \mathbb{N}_0, a \in \mathbb{C})$ je D-konačna, jer takvi redovi zadovoljavaju linearnu homogenu diferencijalnu jednadžbu s konstantnim koeficijentima. Nadalje, red $u = \sum_{n\geq 0} n! x^n$ je D-konačan jer je $(xu)' = \sum_{n\geq 0}(n+1)! x^n$, pa je $x(xu)' = u - 1$, tj. u zadovoljava $x^2u' + (x-1)u + 1 = 0$.

Kažemo da je funkcija $f : \mathbb{N}_0 \to \mathbb{C}$ **P-rekurzivna** (ili **polinomski rekurzivna**) ako postoje polinomi $P_0, \ldots, P_l \in \mathbb{C}[n]$, $P_l \neq 0$, tako da je

$$P_l(n)f(n+l) + P_{l-1}(n)f(n+l-1) + \cdots + P_0(n)f(n) = 0, \tag{52}$$

za sve $n \in \mathbb{N}_0$. Riječima, f je P-rekurzivna ako zadovoljava homogenu linearnu rekurziju s polinomskim koeficijentima.

PROPOZICIJA 10. *Neka je $u = \sum_{n\geq 0} f(n)x^n \in \mathbb{C}[[x]]$. Tada je u D-konačan ako i samo ako je f P-rekurzivna.*

Dokaz. Pretpostavimo prvo da je u D-konačan. Tada vrijedi (49) (uz $p_d(x) \neq 0$). Ako u deriviramo i puta, pa pomnožimo s x^j, dobivamo

$$x^j u^{(i)} = \sum_{n\geq 0} (n+i-j)^{\underline{i}} f(n+i-j) x^n.$$

Ako takve izraze uvrstimo u (49) te izjednačimo koeficijente uz x^{n+k} za čvrst dovoljno velik k, dobit ćemo rekurziju tipa (52) za f (uz $P_l(n) \neq 0$). Ta rekurzija neće kolabirat na $0 = 0$, jer ako je $\langle x^j \rangle p_d(x) \neq 0$, onda je $\langle n^d \rangle P_{d-j+k}(n) \neq 0$.

Obrnuto, neka f zadovoljava (52) (uz $P_l(n) \neq 0$). Za čvrsto $i \in \mathbb{N}_0$, polinomi $(n+i)^{\underline{j}}$, $j \geq 0$, čine $\mathbb{C}$-bazu prostora polinoma $\mathbb{C}[n]$, jer je $\deg(n+i)^{\underline{j}} = j$. Stoga je $P_i(n)$ $\mathbb{C}$-linearna kombinacija polinoma $(n+i)^{\underline{j}}$, pa je $\sum_{n\geq 0} P_i(n) f(n+i) x^n$ $\mathbb{C}$-linearna kombinacija redova oblika $\sum_{n\geq 0}(n+i)^{\underline{j}} f(n+i)x^n$. No svaki takav red je oblika

$$\sum_{n\geq 0}(n+i)^{\underline{j}} f(n+i)x^n = R_i(x) + x^{j-1}u^{(j)},$$

gdje je $R_i(x) \in x^{-1}\mathbb{C}[x^{-1}]$ (tj. $R_i(x)$ je Laurentov red čiji su svi eksponenti negativni). Na primjer, iz $u' = \sum_{n\geq 0} n f(n) x^{n-1}$ slijedi da je

$$\begin{aligned} x^{-1}u' &= \sum_{n\geq -1}(n+2)f(n+2)x^n \\ &= f(1)x^{-1} + \sum_{n\geq 0}(n+2)f(n+2)x^n. \end{aligned}$$

Stoga, ako (52) pomnožimo s x^n i sumiramo po $n \geq 0$, dobivamo

$$0 = \sum a_{ij} x^{j-i} u^{(j)} + R(x),$$

pri čemu je ova suma konačna, $a_{ij} \in \mathbb{C}$, a $R(x) \in x^{-1}\mathbb{C}[x^{-1}]$. Lako se vidi da nisu svi $a_{ij} = 0$. Ako ovu jednakost pomnožimo s dovoljno velikom potencijom x^N, dobit ćemo jednakost tipa (50), pa je u D-konačan. □

Tako je, primjerice, $f(n) = n!$ P-rekurzivna funkcija jer je $f(n+1)-(n+1)f(n) = 0$. Stoga je red $\sum_{n\geq 0} n! x^n$ D-konačan. I funkcija $f(n) = \binom{2n}{n}$ je P-rekurzivna, jer je lako provjeriti da vrijedi $(n+1)f(n+1) - 2(2n+1)f(n) = 0$. Zato je red $u = \sum_{n\geq 0}\binom{2n}{n}x^n = 1/\sqrt{1-4x}$ D-konačan.

Ovi primjeri ukazuju na to da su algebarski radovi i D-konačni. To je i sadržaji našeg sljedećeg teorema.

TEOREM 3. *Neka je $u \in \mathbb{C}[[x]]$ algebarski stupnja d. Tada je u D-konačan. Točnije, u zadovoljava jednadžbu* (49) *reda d ili jednadžbu* (50) *reda $m = d-1$.*

Dokaz. Iz formule (48) (u dokazu Propozicije 8) vidimo da je $u' \in \mathbb{C}(x,u)$, tj. u' je racionalna funkcija reda od x i u. Ako dalje deriviramo (48) s obzirom na x, onda indukcijom po k zaključujemo da je $u^{(k)} \in \mathbb{C}(x,u)$, za sve $k \geq 0$. Kako je stupanj od u jednak d, slijedi da je $\dim_{\mathbb{C}(x)} \mathbb{C}(x,u) = d$. Stoga su $u, u', \ldots, u^{(d)}$ linearno zavisni nad $\mathbb{C}(x)$. To daje jednadžbu oblika (49). Slično, $1, u, u', \ldots, u^{(d-1)}$ su linearno zavisni nad $\mathbb{C}(x)$, što daje (50), pri čemu je $m \leq d-1$. □

Primjer 37. Neka je $F(x) = A(x)/B(x)$ racionalna funkcija $F(0) = 1$. Tada je dobro definiran d-ti korijen $u = F(x)^{1/d}$, $d \in \mathbb{N}$, $u(0) = 1$. Pokažite da je u D-konačna i nađite pripadne rekurzije za koeficijente od u ako je a) $B(x) = 1$; b) $A(x) = 1$.

Rješenje. Prvo imamo da je $u^d = F(x)$. Deriviranje daje $du^{d-1}u' = F'(x)$, pa množenjem s u dobivamo $dF(x)u' = F'(x)u$. Iz $F(x) = A(x)/B(x)$ odavde dobivamo

$$dABu' = (A'B - AB')u. \tag{53}$$

Odavde slijedi da je u D-konačna.

Ako je $B(x) = 1$, a $F(x) = A(x) = a_0 + a_1 x + \cdots + a_r x^r$, te $u = \sum f(n)x^n$, onda izjednačavanjem koeficijenata uz x^{n+r-1} u (53) dobivamo

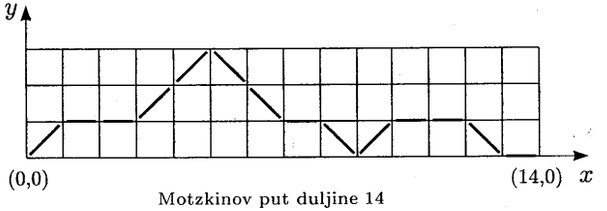
$$\sum_{j=0}^{r} a_{r-j}(dn + dj - r + j)f(n+j) = 0. \tag{54}$$

Slično, ako je $A(x) = 1$, $B(x) = b_0 + b_1 x + \cdots + b_r x^r$, $u = \sum f(n)x^n$, dobivamo

$$\sum_{j=0}^{r} b_{r-j}(dn + dj + r - j)f(n+j) = 0. \tag{55}$$

□

Sada ćemo kao primjenu gornje teorije riješiti dva vrlo važna enumerativna problema. Prvo definirajmo **Motzkinov put**[3] kao put u cjelobrojnoj mreži u ravnini od $(0,0)$ do $(n,0)$ s koracima $(1,0), (1,1)$ i $(1,-1)$ koji nikad ne padne ispod osi x. **Motzinov broj** M_n je broj Motzkinovih puteva od $(0,0)$ do $(n,0)$. Uočite da ako na Motzkinovu putu nema koraka $(1,0)$, onda se radi o Dyckovu putu (pa je n nužno paran broj). Npr. na slici je Motzkinov put ($n = 14$).



Motzkinov put duljine 14

Ako Motzkinov put projiciramo na os y, vidimo da Motzkinov broj M_n možemo interpretirati i kao broj zatvorenih šetnji na $\mathbb{N}_0$ s n koraka -1, 0 ili 1 koje počinju i završavaju u ishodištu.

Uočimo da, brojimo li koliko na Motzkinovu putu ima koraka $(1,0)$, odmah dobivamo da su Catalanovi i Motzkinovi brojevi vezani formulama

$$M_n = \sum_{k\geq 0}\binom{n}{2k}C_k, \qquad C_{n+1} = \sum_{k\geq 0}\binom{n}{k}M_k.$$

Primjer 38. Dokažite da za Motzkinove brojeve M_n, uz $M_0 := 1$, vrijedi:

a) $M_{n+1} = M_n + \sum_{k=0}^{n-1} M_k M_{n-k-1}$
(duga konvolucijska rekurzija)

[3]Theodore S. Motzkin (1908 – 1970), izraelski matematičar

b) Funkcija izvodnica za $(M_n)_{n\geq 0}$ je dana s

$$M = M(x) = \sum_{n\geq 0} M_n x^n = \frac{1 - x - \sqrt{1 - 2x - 3x^2}}{2x^2}$$
$$= 1 + x + 2x^2 + 4x^3 + 9x^4 + 21x^5 + 51x^6 + 127x^7 + 323x^8 + \cdots$$

$M(x)$ je algebarska (stoga i D-konačna).

c) $(n+2)M_n = (2n+1)M_{n-1} + 3(n-1)M_{n-2}$
(kratka polinomska rekurzija).

d) Niz $(M_n)_{n\geq 0}$ je log-konveksan, tj. $M_n^2 \leq M_{n-1}M_{n+1}$, za sve $n \geq 1$.

e) Postoji $\lim_{n\to\infty} M_n/M_{n-1}$ i jednak je 3.

f) $M_n \sim \sqrt{\frac{3}{4\pi}} 3^{n+1} n^{-3/2}$.
(Time možemo smatrati da smo s kombinatornog stajališta dokazali sve važne aspekte Motzkinovog niza (M_n): i dugu i kratku rekurziju, FI, ponašanje niza i asimptotiku.)

Rješenje. a) Za $n = 0$ je $M_0 := 1$, a i za $n = 1$ je $M_n = 1$ jer tada imamo samo jedan (trivijalan) Motzkinov put. Za $n \geq 1$, Motzkinov put s $n+1$ koraka ili počinje ravno (tj. s korakom $(1,0)$), pa ga možemo nastaviti na M_n načina ili počinje s korakom $(1,1)$ i prvi se puta vraća na os x nakon $k+1$ koraka (tj. dolazi u vrh $k+2$). Takvih putova ima koliko i uređenih parova (P_1, P_2), gdje je P_1 Motzkinov put od $(1,1)$ do $(k+1,1)$ koji nisu ispod pravca $y = 1$, a P_2 Motzkinov put od $(k+2,0)$ do $(n+1,0)$. Putova P_1 ima M_k, a putova P_2 ima koliko i Motzkinovih putova s $n+1-(k+2) = n-k-1$ koraka, a to je M_{n-k-1}. Odatle slijedi a).

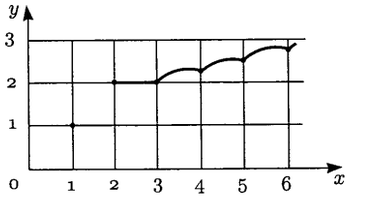
b) To slijedi tako da rekurziju iz a) pomnožimo s x^{n+1} i sumiramo po $n \geq 0$. Zbog $M_0 = 1$ lako dobivamo $x^2M^2 + (x-1)M + 1 = 0$. Odavde zbog $M(0) = M_0 = 1$ slijedi b). (Pokušajte za vježbu ovu jednadžbu za M izvesti simboličkom metodom, bez poziva na a)). Po definiciji je M zbog prethodne jednadžbe algebarska, pa zbog Teorema 3 D-konačna.

c) Iz formule (54), za polinom $A(x) = 1 - 2x - 3x^2$ imamo $r = 2$, $a_0 = 1$, $a_1 = -2$, $a_2 = -3$, $d = 2$, pa iz $2x^2M(x) + x - 1 = \sqrt{1 - 2x - 3x^2}$ uzimanjem koeficijenta uz x^{n+2} na objema stranama dobivamo tvrdnju c).

d) Podijelimo li kratku rekurziju iz c) s M_{n-1} i označimo $x_n = M_n/M_{n-1}$, dobivamo

$$(n+2)x_n = 2n + 1 + \frac{3(n-1)}{x_{n-1}}, \quad n \geq 2. \tag{56}$$

Početni je uvjet ove rekurzije $x_1 = M_1/M_0 = 1$. Log-konveksnost $M_n^2 \leq M_{n-1}M_{n+1}$ je ekvivalentna s $x_n \leq x_{n+1}$. Dakle, treba dokazati da (x_n) raste. U tu svrhu promotrimo funkciju $f : [2,\infty\rangle \to \mathbb{R}$ definiranu ovako: $f(x) = 2$ za $x \in [2,3]$, te $(x+2)f(x-1)f(x) = (2x+1)f(x-1) + 3(x-1)$, za $x \geq 3$. Uočite da je $f(n) = x_n$, $n \geq 2$. Tako definirana funkcija (tzv. *dinamički sistem*) je neprekidna, a na svakom intervalu $\langle n, n+1\rangle$, $n \geq 2$, f je racionalna s nenul nazivnikom, pa stoga i glatka na svakom takvom intervalu. Dakle, dovoljno je dokazati da je f rastuća funkcija.



Uočite da je $f(x) = 2$, za $x \in [2,3]$,
$f(x) = \frac{7x-1}{2(x+2)}$, za $x \in [3,4]$,
$f(x) = \frac{20x^2-9x-14}{7x^2+6x-16}$, za $x \in [4,5]$,
$f(x) = \frac{61x^3-123x^2-40x+60}{20x^3-9x^2-83x+30}$, za $x \in [5,6]$ itd.

Lako je provjeriti da je $f(x) \geq 2$, za svako $x \geq 2$. Pretpostavimo induktivno da je f rastuća na segmentu $[3,n]$. Za $n = 4$ to se lako provjeri. Za $x \in \langle n, n+1\rangle$, deriviranjem dinamičkog sistema dobivamo

$$f'(x) = \frac{3}{((x+2)f(x-1))^2}\left[f^2(x-1) + 3f(x-1) - (x-1)(x+2)f'(x-1)\right] =$$
$$= \frac{3}{((x+2)f(x-1))^2}\left[f^2(x-1) + 3f(x-1) + \frac{3(x^2-1)(x^2-4)f'(x-2)}{(x+1)^2 f(x-2)} - \right.$$
$$\left. - \frac{3(x-1)(x+2)}{(x+1)^2 f(x-2)} \cdot (f(x-2)+3)\right].$$

Po pretpostavci indukcije f raste na $[3,n]$, pa je $f(x-1) \geq f(x-2) \geq 2$, i $f'(x-2) \geq 0$. Zato je dovoljno dokazati da je $f'(x) \geq 0$, a to slijedi iz toga što je

$$f^2(x-1) + 3f(x-1) \geq \frac{3(x-1)(x+2)}{(x+1)^2} \cdot \frac{f(x-2)+3}{f(x-2)} \quad \Longleftrightarrow$$

$$\frac{[f^2(x-1) + 3f(x-1)]f(x-2)}{f(x-2)+3} \geq \frac{3(x-1)(x+2)}{(x+1)^2}, \tag{57}$$

a ova posljednja jednakost je točna, jer je zbog pretpostavke indukcije $f(x-1) \geq f(x-2) \geq 2$, pa je lijeva strana od (57) veća ili jednaka $f^2(x-2) \geq 4$, a maksimum desne strane iz (57) je jednak 3. Time smo dokazali da je $f'(x) \geq 0$, $\forall x \in \langle n, n+1\rangle$, pa i na intervalu $\langle n, n+1\rangle$ funkcija f raste. Zbog neprekidnosti f raste i na $[3, n+1]$. Prema tome, f raste. Posebno je stoga $x_{n+1} \geq x_n$.

Još jedan kratki dokaz da niz (x_n) raste jest sljedeći. Uklještimo x_n između susjednih članova rastućeg niza $a_n = 6n/(2n+3)$. Točnije, vrijedi $a_n \leq x_n \leq a_{n+1}$, za svako $n \geq 3$, što se lako provjeri indukcijom po $n \geq 3$.

e) Nije se teško uvjeriti da je funkcija f iz d) omeđena, jer vrijedi $2 \leq f(x) \leq 7/2$, $\forall x \geq 2$. Zato je niz (x_n) omeđen i rastući, pa stoga konvergentan. Prelaskom na limes kada $n \to \infty$ u (56) odmah dobivamo da je $\lim_{n\to\infty} x_n = 3$. (Ove dokaze d) i e) dali su T. Došlić, D. Svrtan i D. Veljan 2000. g.)

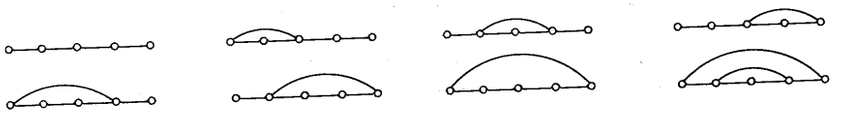
f) To slijedi iz jednog Darbouxovog teorema (vidi [42*]) koji u našoj situaciji kaže

$$M_n \sim \frac{1}{4\sqrt{\pi n^3}}[-r\Delta'(r)]^{1/2} r^{-n-2},$$

gdje je r najmanji pozitivni korijen diskriminante Δ jednadžbe $x^2M^2 + (x-1)M + 1 = 0$. □

Primjer 39. Sekundarna struktura[4] je jednostavni graf sa skupom vrhova $[n]$ i dvije vrste bridova: segmentima $i, i+1$, za $1 \leq i \leq n-1$ i lukovima u gornjoj poluravnini koji spajaju neke i, j, $j - i > l$ (l čvrst), s time da su lukovi disjunktni. Takva se struktura

zove ranga l. Neka je $S^{(l)}(n)$ broj svih sekundarnih struktura ranga l sa skupom vrhova $[n]$. Npr., za $l = 1$, $n = 5$ imamo $S^{(1)}(5) = 8$ (tu lukovi "preskaču" barem $l = 1$ vrh):



a) Vrijedi $S^{(l)}(n+1) = S^{(l)}(n) + \sum_{k=l}^{n-1} S^{(l)}(k)S^{(l)}(n-k-1)$, za $n \geq l+1$, uz početne uvjete $S^{(l)}(0) = S^{(l)}(1) = \cdots = S^{(l)}(l+1) = 1$;

b) Funkcija izvodnica $S_l(x)$ niza $S^{(l)}(n)$, $n = 0, 1, 2, \ldots$ dana je s

$$S_l(x) = \frac{-\omega_l(x) - \sqrt{\omega_l^2(x) - 4x^2}}{2x^2},$$

gdje je $\omega_l(x) = 2x - (1 + x + \cdots + x^{l+1})$;

c) Za $l = 1$ vrijedi kratka rekurzija (za $n \geq 4$):

$$\begin{aligned}(n+2)S^{(1)}(n) =& (2n+1)S^{(1)}(n-1) + (n-1)S^{(1)}(n-2) + \\ &+ (2n-5)S^{(1)}(n-3) - (n-4)S^{(1)}(n-4)\end{aligned}$$

s početnim uvjetima $S^{(1)}(0) = S^{(1)}(1) = S^{(1)}(2) = 1$, $S^{(1)}(3) = 2$ (i slično za sve l);

d) U graničnom slučaju $l = 0$ imamo $S^{(0)}(n) = M_n$ (Motzkinov broj), a "degenerirani" je slučaj $l = -1$ (u kojem dopuštamo petlje) i tada je $S^{(-1)}(n) = C_{n+1}$ (Catalanov broj);

e) Niz $(S^{(1)}(n))_{n\geq 0}$ je log-lonveksan;

f) Vrijedi asimptotika

$$S^{(1)}(n) \sim \sqrt{\frac{15+7\sqrt{5}}{8\pi}} \left(\frac{3+\sqrt{5}}{2}\right)^n n^{-3/2}$$

(i slično za sve l).

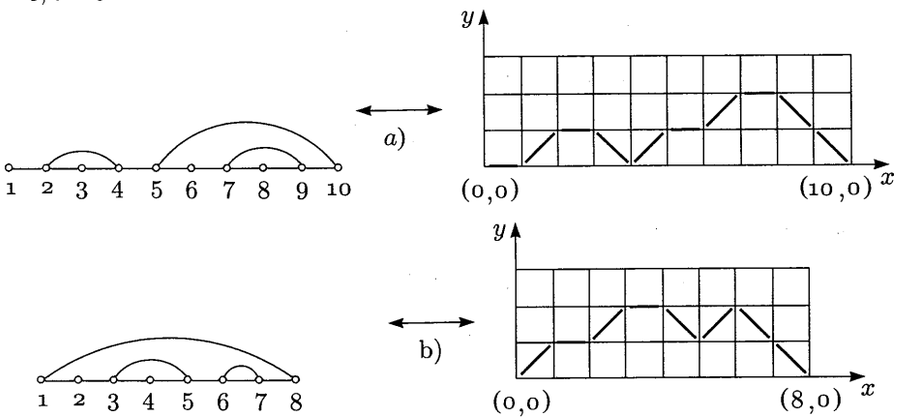
Rješenje. a) Za $n \leq l$ imamo očito samo jednu (trivijalnu) sekundarnu strukturu ranga l na n vrhova, pa zato vrijede početni uvjeti. Neka je $n \geq l+1$. Tada, sekundarna struktura ili nema luk koji počinje u 1, pa tada imamo $S^{(l)}(n)$ takvih struktura ili pak ima luk od 1 do nekog vrha $k+2$ koji je barem l vrhova daleko, a u tom slučaju imamo $S^{(l)}(k)S^{(l)}(n-k-1)$ takvih struktura. Odatle slijedi navedena rekurzija.

[4]U biologiji su ove strukture važne za razumijevanje uloge RNK u staničnom metabolizmu i dekodiranju nasljednih informacija koje su sadržane u DNK. Biolozi nazivaju vrhove sekundarne strukture bazama, segmente p-vezama, a lukove h-vezama (p dolazi od *phosphorous*, a h od *hydrogen*).

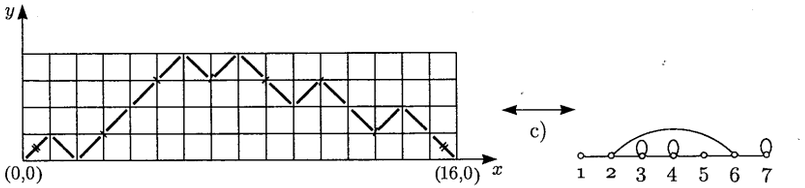
b) Rekurziju iz a) pomnožimo s x^{n+1} i sumiramo po $n \geq 0$. Tada uzmemo li u obzir početne uvjete, dobivamo $x^2 S_l^2(x) + \omega_l(x)S_l(x) + 1 = 0$, a odavde navedenu formulu.

c) Ovo slijedi iz formule (54) i b) slično kao tvrdnja c) u prethodnom primjeru, jer je $S^{(l)}(x)$ algebarska FI; ovdje je za $l = 1$, $\omega_1(x) = x - 1 - x^2$.

d) Neka je $\mathcal{S}^{(l)}$ skup svih sekundarnih struktura ranga l na n vrhova, a $\mathcal{M}^{(l)}(n)$ skup svih Motzkinovih putova duljine n, čiji je svaki plato (ili visoravan) duljine $\geq l$. Pokušajte sami opisati bijekciju $\mathcal{S}^{(l)}(n) \leftrightarrow \mathcal{M}^{(l)}(n)$, $l \geq 0$, iz ovih dvaju crteža: a) $n = 10, l = 1$ i b) $n = 8$, $l = 0$



U "degeneriranom" slučaju $l = -1$ imamo bijekciju $\mathcal{S}^{(-1)}(n) \leftrightarrow \mathcal{D}_{n+1}$, s Dyckovim putovima duljine $2(n+1)$. Dyckov put nužno počinje korakom $(1,1)$, a završava korakom $(1,-1)$, pa njih odbacimo, dok ostatak Dyckova puta (duljine $2n$) podijelimo u grupe od po dva koraka. Pokušajte sami objasniti tu bijekciju s donjim crtežom c) za $n = 7$:



e) To slijedi indukcijom iz ovoga: $a_n \leq x_n \leq a_{n+1}$, $n \geq 6$, gdje je $x_n = S^{(1)}(n)/S^{(1)}(n-1)$, $a_n = 2n\varphi^2/(2n+3)$, gdje je $\varphi = (1+\sqrt{5})/2$ omjer zlatnog reza.

f) Ovo izlazi slično kao i f) u prethodnom primjeru.

(Dokaze tvrdnji a)–f) dali su T. Došlić, D. Svrtan i D. Veljan 2000.g.) □

Završno u ovoj točki navodimo bez dokaza sljedeći teorem.

TEOREM 4. *Neka je $\mathcal{D}$ skup svih D-konačnih redova potencija iz $\mathbb{C}[[x]]$. Tada vrijedi:*

(i) $\mathcal{D}$ je podalgebra od $\mathbb{C}[[x]]$ (tj. $u, v \in \mathcal{D} \Rightarrow \alpha u + \beta v \in \mathcal{D}$, $uv \in \mathcal{D}$);

(ii) Ako je $u \in \mathcal{D}$, a $v \in \mathbb{C}_{alg}[[x]]$, $v(0) = 0$, onda je $u(v(x)) \in \mathcal{D}$;

(iii) Ako su $u, v \in \mathcal{D}$, onda je Hadamardov produkt $u * v \in \mathcal{D}$.

Zato su npr. funkcije $e^{x/\sqrt{1-4x}}$, $e^{3x}\sqrt{1-4x}$, $e^x + \sum_{n\geq 0} n!x^n$ D-konačne, ali npr. $\sqrt{\cos x}$, $1/\sin x$, e^{e^x-1} nisu D-konačne.

Sljedeći korak u teoriji funkcija izvodnica jest proučavanje nekomutativnih funkcija izvodnica u više varijabli nad nekim poljem K. Ukratko, ako je X skup, koji se zove **alfabet**, neka je X^* slobodni monoid generiran s X, tj. X^* je skup konačnih slogova $w = w_1 \dots w_n$ sastavljenih od slova $w_i \in X$ (uključivo praznu riječ 1). w se zove **riječ** nad alfabetom X, a n **duljina** riječi $w = w_1 \dots w_n$. **Formalni red potencija** u X (nad poljem K) je funkcija $S : X^* \to K$ koju poistovjećujemo sa

$$S = \sum_{w \in X^*} S(w)w.$$

Skup $K\langle\langle X\rangle\rangle$ svih takvih formalnih redova na očit način ima strukturu prstena (štoviše K-algebre) s jedinicom 1 (zbrajanje je po komponentama, a množenje je uobičajeno množenje redova, uzimajući u obzir nekomutativnost varijabli). Formalni red $S \in K\langle\langle X\rangle\rangle$ je **nekomutativni polinom** ako je suma $\sum S(w)w$ konačna. Skup svih polinoma $S \in K\langle\langle X\rangle\rangle$ čini podalgebru $K\langle X\rangle$ od $K\langle\langle X\rangle\rangle$.

Ako je $S \in K\langle\langle X\rangle\rangle$ tako da je $S(1) = \alpha \neq 0$, definiramo

$$T = \frac{1}{\alpha} \sum_{n\geq 0} \left(1 - \frac{S}{\alpha}\right)^n \in K\langle\langle X\rangle\rangle.$$

Tada je $ST = TS = 1$, pa je $T = S^{-1}$ u $K\langle\langle x\rangle\rangle$.

Tako je, naprimjer,

$$\left(1 - \sum_{x \in X} x\right)^{-1} = \sum_{w \in X^*} w.$$

Formalni red S je **nekomutativni racionalni red** ako je element najmanje podalgebre $K_{\text{rat}}\langle\langle X\rangle\rangle \subseteq K\langle\langle X\rangle\rangle$ koja sadrži $K\langle X\rangle$ tako da ako S^{-1} postoji, onda je i $S^{-1} \in K_{\text{rat}}\langle\langle X\rangle\rangle$.

Ako je npr. $K = \mathbb{Q}$, a $X = \{x, y, z\}$, onda je $xy + 3xyx - (1/2)xzxy^2x^3z$ polinom, a $S = [(1+x)^{-1} + y]^{-1}[x^2 + y^2xy(1 - xyz)^{-1} + xyz]$ je racionalni red.

Neka je $M_{n,n}(K)$ monoid svih $n \times n$ matrica nad K s uobičajenim množenjem matrica.

Osnovni teorem o racionalnim formalnim redovima kaže da je formalni red $S \in K\langle\langle X\rangle\rangle$ racionalan ako i samo ako postoji $n \in \mathbb{N}$, homomorfizam monoida $\mu : X^* \to M_{n,n}(K)$ i matrice $a \in M_{1,n}(K)$, $b \in M_{n,1}(K)$ (redak - i stupac - vektori) tako da je

$$S(w) = a \cdot \mu(w) \cdot b,$$

za sve $w \in X^* \setminus \{1\} (= X^+)$.

Ako je $Y = \{y_1, \dots, y_n\}$ alfabet disjunktan s X, onda se skup jednadžbi $y_i = p_i$, $1 \leq i \leq n$ zove **pravi algebarski sustav jednadžbi**, ako je

(i) $p_i \in K\langle X, Y\rangle$ (tj. p_i je polinom nad alfabetom $X \cup Y$);

(ii) $p_i(1) = 0$ i $p_i(y_j) = 0$ (tj. p_i nema konstantnog člana ni članova oblika $c_j y_j$, $0 \neq c_j \in K$).

Rješenje pravog algebarskog sustava $y_i = p_i$, $i = 1, \dots, n$ je uređena n-torka $(R_1, \dots, R_n) \in K\langle\langle X\rangle\rangle^n$ formalnih redova na X s konstatnim članom 0 za koji je

$$R_i = p_i(X, Y)_{y_i = R_i}.$$

Svaki R_i se zove **komponenta** sustava $y_1 = p_1, \dots, y_n = p_n$.

Tako je, na primjer, za $X = \{x, y\}$, $Y = \{z\}$, $z = xy + xzy$, pravi algebarski sustav s rješenjem

$$R = \sum_{n\geq 1} x^n y^n$$

koje nije racionalno, dok npr. sustav $z = xy + zxy$ ima racionalno rješenje $R = \sum_{n\geq 1}(xy)^n = (1 - xy)^{-1} - 1$. Svaki pravi algebarski sustav jednadžbi ima jedinstveno rješenje.

Formalni red $S \in K\langle\langle X\rangle\rangle$ je **algebarski** ako je $S - S(1)$ komponenta pravog algebarskog sustava jednadžbi.

Nosač (*engl. support*) **formalnog reda** $S \in K\langle\langle X\rangle\rangle$ je skup

$$\text{supp}(S) = \{w \in X^* \mid S(w) \neq 0\}.$$

Formalni jezik (ili kratko **jezik**) je podskup $L \subseteq X^*$. Jezik L je **racionalan** (odn. **algebarski**) ako je on nosač racionalnog (odn. algebarskog) formalnog reda. U uporabi su često još i nazivi **regularni jezik** za racionalni jezik i **kontekstnoslobodan jezik** za algebarski jezik.

Redovi $\sum x^n y^n$ i $\sum (xy)^n$ su algebarski. Svaki racionalni red je i algebarski red.

Dobar dio ove teorije ćemo sada protumačiti na jednom od najvažnijih algebarskih jezika u kombinatornoj teoriji. To je Dyckov jezik.

Primjer 40. Dyckov jezik D je podskup od $\{x, y\}^*$ tako da ako x zamijenimo lijevom zagradom, a y desnom zagradom, onda dobivamo niz pravilno ugniježđenih zagrada. Ekvivalentno, riječ $w = w_1 w_2 \dots w_m$ je u D (pri čemu je $w_i = x$ ili y) ako je za sve j, $1 \leq j \leq m$, broj x-ova u $w_1 w_2 \dots w_j$ veći ili jednak broju y-ova, a ukupni broj x-ova jednak ukupnom broju y-ova u w (pa je stoga m paran broj). Element $w \in D$ se zove **Dyckova riječ**. Dyckove riječi duljine ≤ 6 su:

$$1, xy, x^2y^2, xyxy, x^3y^3, x^2yxy^2, x^2y^2xy, xyx^2y^2, xyxyxy.$$

Prema Propoziciji 6 iz pogl. III znamo da je broj riječi duljine $2n$ u D jednak Catalanovom broju C_n. Ključno rekurzivno svojstvo Dyckove riječi w je sljedeće. Ako je w neprazna riječ, onda počinje s x nakon čega dolazi Dyckova riječ, pa nakon toga y (desna zagrada koja zatvara početnu x), te konačno opet Dyckova riječ. Prema tome, D je rješenje sustava

$$z = 1 + xzyz.$$

Zato je $D^+ = D - 1$ rješenje pravog algebarskog sustava (pišemo $z' = z - 1$)

$$\begin{aligned} z' &= x(z'+1)y(z'+1) = \\ &= xy + xyz' + xz'y + xz'yz'. \end{aligned}$$

Odavde slijedi (po definiciji) da je Dyckov jezik D algebarski. □

Već i na ovom jednostavnom (ali važnom) primjeru čitatelj može uvidjeti da se mnoga računanja mogu bitno pojednostaviti kad se neki kombinatorni problem prevede na odgovarajući jezik.

Teorija algebarskih funkcija, Abelovih integrala i srodne relativno dobro izgrađene teorije 19. i 20. stoljeća tek trebaju naći prave primjene u kombinatornoj teoriji.

Izrecimo na kraju ovog poglavlja još jednom osnovnu "apstraktnu" ideju funkcija izvodnica. Svakom elementu α skupa S (koji može biti i beskonačan) pridružimo težinu $w(\alpha)$ iz neke Abelove grupe. Funkcija izvodnica od S s obzirom na težinsku funkciju w je formalna suma $\sum_{\alpha\in S} w(\alpha)$. Ako su sve težine jednake 1, dobijemo kardinalnost od S. Prema tome, pojam funkcije izvodnice je poopćenje pojma kardinalnosti skupa. U tipičnoj je situaciji svakom $\alpha \in S$ pridružena "duljina" $\ell(\alpha)$, a "težina" od α je monom $x^{\ell(\alpha)}$, pa je prirodna funkcija $F_S(x) = \sum_{\alpha\in S} x^{\ell(\alpha)}$. Njezino je poznavanje ekvivalentno poznavanju broja elemenata iz S sa svakom unaprijed zadanom duljinom.

Mnogi nizovi cijelih brojeva (navedeni npr. u knjizi N. J. A. Sloane, S. Plouffe, *Encyclopedia of Integer Sequences*, Academic Press, N. Y., 1996) još očekuju potpuna kombinatorna objašnjenja, naročito sa stanovišta teorije funkcija izvodnica.

VI. Uvod u teoriju grafova

§ 1. Osnovni pojmovi teorije grafova

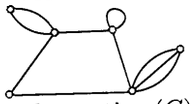
Grafovi su jedna od osnovnih matematičkih struktura. Stoga se i pojavljuju u raznim oblicima i raznim situacijama. Mnoge se pojave modeliraju grafovima (dijagramima) koji se sastoje od točaka i njihovih spojnica. Na primjer, točke (vrhovi ili čvorovi) mogu predstavljati ljude iz neke skupine, a spojnice (bridovi) parove prijatelja, ili točke mogu predstavljati komunikacijske centre, a spojnice komunikacijske veze. Graf može predstavljati električnu mrežu, čiji su vrhovi električke komponente, a spojnice električne veze. Cestovne, željezničke, zrakoplovne veze itd. daljnji su primjeri modela s grafovima. U računarstvu se često dijagram toka nekog algoritma prikazuje grafom kojem su čvorovi naredbe (instrukcije), a lukovi iz jedne u drugu naredbu su bridovi. Isto se tako grafovima prezentiraju i razne kompjuterske strukture podataka, umrežavanje i paralelizam računala i njihov sekvencijalni rad, evolucijska ili porodična stabla u biologiji, kemijske veze među atomima ili molekulama, raspored poslova u velikim gospodarskim projektima itd.

Ponovimo ukratko osnovne pojmove. **Graf** je uređeni par $G = (V, E)$, gdje je $\emptyset \neq V = V(G)$ skup **vrhova** (*engl. vertex*), $E = E(G)$ skup **bridova** (*engl. edge*) disjunktni s V, a svaki brid $e \in E$ spaja dva vrha $u, v \in V$ koji se zovu **krajevi** od e[1]. Kažemo još da su tada vrhovi u i v **incidentni** s e, a vrhovi u i v **susjedni** i pišemo $u \sim v$ ili $e = uv$ (ili pravilno $e = \{u, v\}$). Bridove s bar jednim zajedničkim krajem također zovemo incidentnim. Graf G je **konačan** ako su V i E konačni skupovi, a inače je **beskonačan**. Grafovi G i H su **izomorfni**, i pišemo $G \approx H$ ako postoje bijekcije $\theta : V(G) \to V(H)$ i $\varphi : E(G) \to E(H)$ tako da je vrh v incidentan s bridom e u G ako i samo ako je $\theta(v)$ incidentan s $\varphi(e)$ u H. Uređeni par $f = (\theta, \varphi) : G \to H$ se tada zove **izomorfizam** iz G u H. Izomorfizam, dakle, čuva incidenciju i susjednost. Brid čiji se krajevi podudaraju zove se **petlja**, a ako su krajevi različiti – **pravi brid** ili **karika**. Dva brida ili više njih s istim parom krajeva zovu se **višestruki bridovi**. Graf G je **jednostavan** ako nema ni petlja ni višestrukih bridova. Graf sa samo jednim vrhom zove se **trivijalan**, a inače **netrivijalan**. G je **prazan graf** ako je $E(G) = \emptyset$. Ako ne kažemo drukčije, mi ćemo isključivo proučavati konačne grafove. Dva osnovna parametra vezana uz konačni graf su

[1] Preciznije, graf je uređena trojka $G = (V, E, \varphi)$, gdje je $\varphi : E \to \binom{V}{2}$ funkcija koja svakom bridu e pridružuje 2-člani multiskup vrhova $\varphi(e) = \{u, v\}$ koji se zovu krajevi od e.

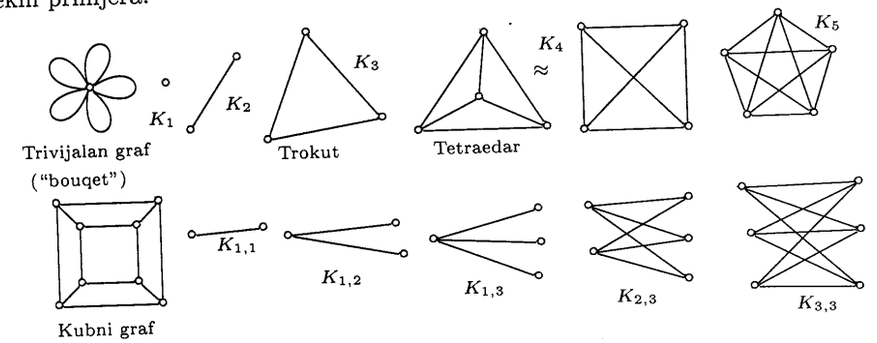
$v(G) = |V(G)|$ = **red** od G = broj vrhova od G,

$e(G) = |E(G)|$ = **veličina od** G = broj bridova od G.

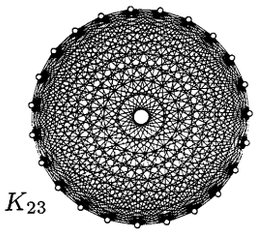
G: 

Graf G na ovoj slici ima 6 vrhova, tj. $v(G) = 6$, 10 bridova, tj. $e(G) = 10$, ima jednu petlju, jedan dvostruki i jedan trostruki brid. Mi ćemo prilikom crtanja grafa uglavnom izostavljati oznake vrhova i bridova i crtežom stoga reprezentirati klasu ekvivalencije izomorfnih grafova.

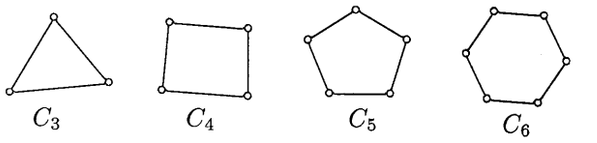
Opišimo neke specijalne grafove koje ćemo često rabiti. Jednostavan graf u kojem je svaki par vrhova spojem bridom zove se **potpun graf**. Do na izomorfizam postoji jedinstveni potpun graf s n vrhova (i $\binom{n}{2}$ bridova) koji označavamo s K_n. Ustvari, ako je $V(K_n) = \{1, 2, \ldots, n\} = [n]$, onda je $E(K_n) = \binom{[n]}{2}$. Graf G je **bipartitan** (ili **dvodijelni**) ako mu se skup vrhova može particionirati u dva skupa X i Y tako da svaki brid ima jedan kraj u X, a drugi u Y. Particija (X, Y) zove se tada **bipartricija** grafa. Bipartitni graf s biparticijom (X, Y) označavamo s $G(X, Y)$. **Potpun bipartitni graf** jednostavan je bipartitni graf s biparticijom (X, Y) u kojem je svaki vrh iz X spojen sa svakim vrhom u Y. Ako je $|X| = m$ i $|Y| = n$, takav je graf jedinstven do na izomorfizam i označava se s $K_{m,n}$; $v(K_{m,n}) = m + n$, $e(K_{m,n}) = mn$. Graf određen vrhovima i bridovima kocke zove se **kubni graf**. Evo nekih primjera:



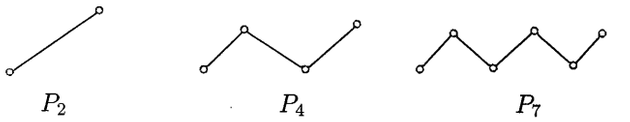
Estetski je vrlo lijep (ornament, pleter, čipka) crtež grafa K_{23} s 253 brida:



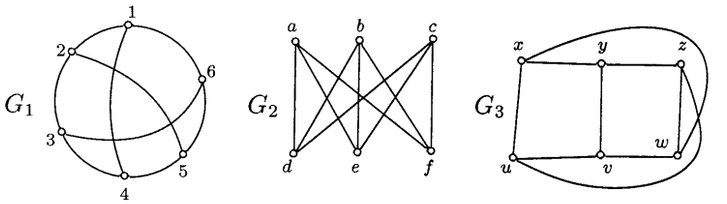
Daljnji važni primjeri (jednostavnih) grafova su ciklusi i putovi. **Ciklus** C_n na n vrhova možemo definirati skupom vrhova $V = \{1, 2, \ldots, n\}$ i skupom bridova $E = \{\{i, i+1\} \mid i < n\} \cup \{1, n\}$:



Put P_n na n vrhova: $V = \{1, 2, \ldots, n\}$, $E = \{\{i, i+1\} \mid i < n\}$:



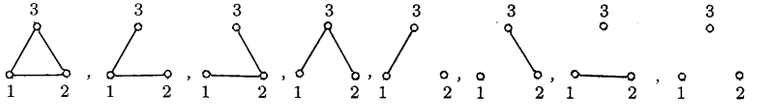
Primjer 1. Jesu li grafovi na donjoj slici izomorfni? Ako jesu, nađite neki izomorfizam.



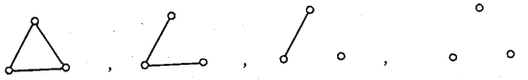
Rješenje. Sva tri grafa su izomorfna s $K_{3,3}$. Jedan izomorfizam $G_1 \to G_2$ se na vrhovima može ovako zadati: $1 \mapsto a$, $2 \mapsto d$, $3 \mapsto b$, $4 \mapsto e$, $5 \mapsto c$, $6 \mapsto f$. Zato se brid 12 iz G_1 preslika u brid ad iz G_2 itd. Jedan izomorfizam $G_2 \to G_3$ je dan s $a \mapsto x$, $b \mapsto z$, $c \mapsto v$, $d \mapsto u$, $e \mapsto y$, $f \mapsto w$, pa stoga brid $ad \mapsto xu$, $ae \mapsto xy$, $af \mapsto xw$ itd. □

Bilješka 1. a) Jedan od velikih otvorenih problema u teoriji grafova pita da li postoji neki efikasni postupak (algoritam) kojim bi se moglo odlučiti jesu li dva dana grafa izomorfna ili ne. Postoje opravdane sumnje da takav algoritam ne postoji. Poteškoća je u tome da se provjeri jesu li dva grafa s n vrhova neizomorfna, mi bismo prema definiciji trebali provjeriti da ni jedna od $n!$ bijekcija na skupovima vrhova ne daje izomorfizam grafova. Često te provjere možemo izbjeći. Npr., ako su brojevi bridova grafa različiti, onda je jasno da su takvi grafovi neizomorfni. Poslije ćemo promatrati i razne druge parametre koji će razlikovati neizomorfne grafove. No, općenito nije poznata neka efikasna metoda koja će *uvijek* razlikovati neizomorfne grafove.

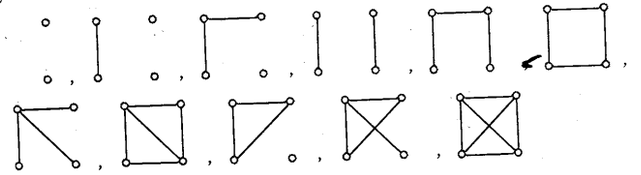
b) Ako je $V = \{1, 2, \ldots, n\}$ skup vrhova, onda izbor jednostavnog grafa sa skupom vrhova V znači da treba odabrati podskup $E \subseteq \binom{V}{2}$. Kako je $\#\binom{V}{2} = \binom{n}{2}$, slijedi da svih grafova na V ima $2^{\binom{n}{2}}$. No, među njima je znatno manje međusobno neizomorfnih grafova. Npr., za $n = 3$, imamo $2^{\binom{3}{2}} = 8$ grafova čiji je skup vrhova $V = \{1, 2, 3\}$. To su



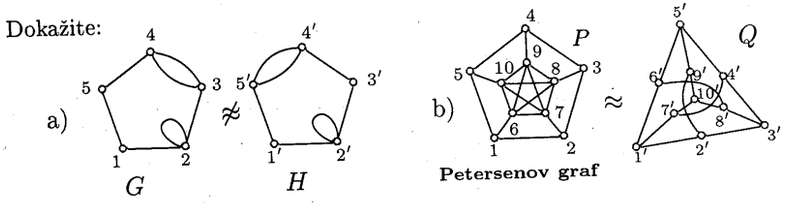
Među njima možemo naći samo 4 klase međusobno neizomorfnih. To su:



Slično, do na izomorfizam postoji 11 jednostavnih grafova s 4 vrha:



Primjer 2. Dokažite:

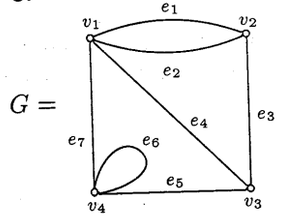


Rješenje. a) G i H imaju po jednu petlju u 2 i $2'$, pa bi svaki izomorfizam $G \to H$ morao preslikati $2 \mapsto 2'$. No tada bi moralo biti $1 \mapsto 1'$ ili $1 \mapsto 3'$. Ako $1 \mapsto 1'$, onda mora $5 \mapsto 5'$, pa vidimo da nikako ne možemo dvostruke bridove 34 preslikati u dvostruke bridove $4'5'$. Slično se vidi da otpada mogućnost $1 \mapsto 3'$. Zato je $G \not\approx H$.

b) Graf Q možemo zamišljati tako da za vrhove ima vrhove tetraedra i polovišta bridova tetraedra. Jedan tetraedra te da smo još dodatno spojili polovišta nasuprotnih bridova tetraedra. Jedan izomorfizam $P \to Q$ je (na vrhovima) ovaj: $1 \mapsto 1'$, $2 \mapsto 2'$, $3 \mapsto 3'$, $4 \mapsto 8'$, $5 \mapsto 6'$, $6 \mapsto 7'$, $7 \mapsto 9'$, $8 \mapsto 4'$, $9 \mapsto 10'$, $10 \mapsto 5'$. □

Često je vrlo korisno relacije incidencije i susjedstva u grafu prikazati matricama. Neka je G graf s vrhovima $v_1, v_2, \ldots, v_n$ u nekom poretku i bridovima $e_1, \ldots, e_m$ u nekom poretku. **Matrica incidencije** grafa G je (pravokutna) $n \times m$-matrica $M = M(G) = [m_{ij}]$, gdje je m_{ij} = broj (0, 1 ili 2) koliko su puta v_i i e_j incidentni. Matrica incidencije potpuno određuje graf. **Matrica susjedstva** (engl. *adjacency matrix*) grafa G je (kvadratna) $n \times n$-matrica $A = A(G) = [a_{ij}]$, gdje je a_{ij} = broj bridova koji spajaju v_i i v_j. A je, dakle, simetrična matrica (tj. $a_{ij} = a_{ji}$) čiji su članovi nenegativni cijeli brojevi. Ako je graf jednostavan, onda je A $(0,1)$-matrica, tj. $a_{ij} = 0$ ili 1, $\forall i, j$, a na glavnoj dijagonali su nule. I obrnuto, svaka takva matrica reprezentira neki graf. A je simetrična matrica, pa ima n realnih svojstvenih vrijednosti $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ čija je suma $\mathrm{Tr}A = 0$ (ako je G jednostavan.)

Primjer 3.



$$M(G) = \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array} \begin{array}{c} \begin{array}{ccccccc} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 & e_7 \end{array} \\ \begin{bmatrix} 1 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 2 & 0 \end{bmatrix} \end{array}$$

$$A(G) = \begin{array}{c} \begin{array}{cccc} v_1 & v_2 & v_3 & v_4 \end{array} \\ \begin{bmatrix} 0 & 2 & 1 & 1 \\ 2 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix} \end{array} \begin{array}{c} \\ v_1 \\ v_2 \\ v_3 \\ v_4 \end{array}$$

Matrica susjedstva je u pravilu mnogo manja negoli matrica incidencije. Napomenimo da obje ovise o odabranim poretcima, odnosno označavanju (labeliranju) vrhova i bridova grafa. Često se graf implementira u računalo upravo s matricom susjedstva. Budući da $A(G)$ ima dosta nula, to i nije najefikasniji način pohrane grafa u računalu. Efikasnije je s listom stvarnih susjedstava ili još bolje s listama susjedstava za svaki vrh posebno (bez ponavljanja već navedenih susjedstava).

Primjer 4. Neka su M i A matrice incidencije i susjedstva grafa G. Tada je a) zbroj članova svakog stupca od M jednak 2; b) zbroj članova j-tog stupca od A jednak broju bridova s jednim krajem v_j.

Rješenje. a) Svaki brid ima dva kraja (u slučaju petlje oni se podudaraju), pa tvrdnja očito slijedi. Tvrdnja b) je također očita. □

Primjer 5. Automorfizam grafa $G = (V, E)$ je izomorfizam od G na samog sebe, tj. to je bijekcija $f : V \to V$ za koju je $uv \in E \iff f(u)f(v) \in E$. Skup svih takvih automorfizama se označava s $\mathrm{Aut}(G)$.

a) Dokažite da je $\mathrm{Aut}(G)$ grupa s operacijom kompozicije;

b) Odredite $\mathrm{Aut}(K_n)$, $\mathrm{Aut}(K_{n,n})$, $\mathrm{Aut}(P_n)$ i $\mathrm{Aut}(C_n)$;

c) **Komplementarni graf** G^c grafa G je graf s istim skupom vrhova kao i G, a dva vrha u G^c su susjedna ako i samo ako nisu susjedna u G. Ako je G jednostavan graf, dokažite $\mathrm{Aut}(G) \approx \mathrm{Aut}(G^c)$.

d) Nađite graf G s barem dva vrha za koji je Aut$G$ trivijalna grupa i dokažite da ne postoji takav jednostavni graf s $2 \leq |V(G)| \leq 5$ (takvi grafovi se još zovu **asimetrični grafovi**);

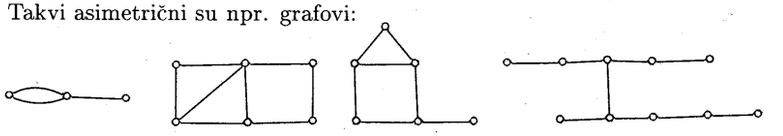
e) Neka je $\Lambda = \{\, \mathrm{id}\,, (123), (132)\} \leq S_3$ podgrupa simetrične grupe S_3. Dokažite da ne postoji jednostavni graf G s $V(G) = \{1, 2, 3\}$ tako da je $\mathrm{Aut}(G) \approx \Lambda$, ali postoji jednostavan graf H tako da je $\mathrm{Aut}(H) \approx \Lambda$. (**Fruchtov teorem** iz 1939. godine kaže da za svaku konačnu grupu Λ postoji graf G za koji je $\mathrm{Aut}(G) \approx \Lambda$.)

Rješenje. a) Ako su $f, g \in \mathrm{Aut}(G)$, onda iz definicije odmah slijedi da je i $f \circ g \in \mathrm{Aut}(G)$. Identiteta 1_G je očito automorfizam od G, a iz definicije automorfizma je jasno da je i $f^{-1} \in \mathrm{Aut}(G)$.

b) $\mathrm{Aut}(K_n) \approx S_n$ jer permutaciji $\sigma \in S_n$ pridružimo $f_\sigma \in \mathrm{Aut}(K_n)$, $f_\sigma(i) = \sigma(i)$. Preslikavanje $\sigma \mapsto f_\sigma$ je izomorfizam grupa $S_n \to \mathrm{Aut}(K_n)$.
$\mathrm{Aut}(K_{n,n}) \approx S_n \times S_n$; konstruirajte sami izomorfizam ovih grupa.
$\mathrm{Aut}(P_n) \approx \mathbb{Z}_2$. Ako je $P_n = v_1 v_2 \ldots v_n$ put, onda je jedan automorfizam identiteta, a drugi $v_i \mapsto v_{n-i+1}$, $i = 1, \ldots, n$ (zašto drugih nema?).
$\mathrm{Aut}(C_n) \approx D_n$ = **diedarska grupa** reda $2n$. D_n je grupa izometrija pravilnog n-terokuta, a sastoji se od zrcaljenja s_i oko osi simetrija poligona, $s_i^2 = 1$, te svih rotacija $r, r^2, \ldots, r^n = 1$ poligona oko središta. D_n ima prezentaciju $\langle x, y | x^2 = y^2 = (xy)^n = 1 \rangle$.

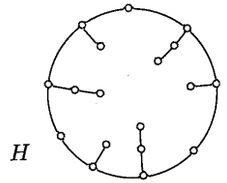
c) Identiteta $f \mapsto f$ daje izomorfizam $\mathrm{Aut}(G) \to \mathrm{Aut}(G^c)$. Tako npr. potpun graf K_n i njegov komplement K_n^c (tj. prazan graf na n vrhova) imaju za grupu automorfizama S_n.

d) Takvi asimetrični su npr. grafovi:



Izravnom provjerom ("malih grafova") nije teško provjeriti drugu tvrdnju d).

e) Provjerom svih grafova sa slike iz prethodne bilješke b) vidimo da nijedan nema grupu automorfizama $\approx \Lambda \approx \mathbb{Z}_3$ (ciklička grupa reda 3). Primjer grafa H za koji je $\mathrm{Aut}(H) \approx \Lambda \approx \mathbb{Z}_3$ je na idućoj slici.



I uopće, takvi grafovi imaju grupu automorfizama cikličku grupu $\mathbb{Z}_n$, jer su jedini automorfizmi rotacije. Lako se vidi da je i za orijentirani ciklus $\vec{C}_n$, $\mathrm{Aut}(\vec{C}_n) \approx \mathbb{Z}_n$. □

Neka su G i H grafovi. Ako je $V(H) \subseteq V(G)$ i $E(H) \subseteq E(G)$, a svaki brid iz H ima iste krajeve u H kao što ih ima u G, onda kažemo da je H **podgraf** od G i pišemo $H \subseteq G$ (ili $G \supseteq H$), a G zovemo **nadgraf** od H. Ako je $H \subseteq G$ i $H \neq G$, pišemo $H \subset G$ i zovemo **pravi podgraf** od G. Podgraf $H \subseteq G$ za koji je $V(H) = V(G)$ zovemo **razapinjući podgraf** od G. Podgraf $H \subseteq G$ koji je potpun zove se **klika** u G.

Unija dvaju podgrafova $G_1, G_2 \subseteq G$ je podgraf $G_1 \cup G_2$ čiji je skup vrhova $V(G_1) \cup V(G_2)$, a skup bridova $E(G_1) \cup E(G_2)$. Slično je **presjek** $G_1 \cap G_2$ podgraf sa skupom vrhova $V(G_1) \cap V(G_2)$ i skupom bridova $E(G_1) \cap E(G_2)$.

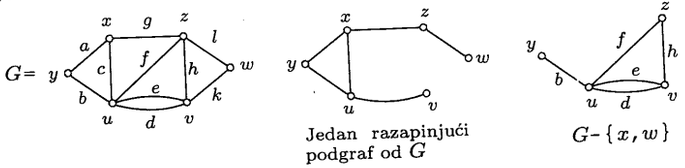
Neka je $G = (V, E)$, a $V' \subseteq V$. Podgraf od G čiji je skup vrhova $V \setminus V'$, a skup bridova se sastoji od bridova iz G čija su oba kraja u $V \setminus V'$ označavamo s $G - V'$. To je podgraf od G dobiven tako da "iščupamo" V' zajedno sa svim bridovima koji su incidentni s nekim vrhom iz V'. Ako je $V' = \{v\}$, pišemo $G - v$ umjesto $G - \{v\}$.

Slično za $E' \subseteq E$, podgraf od G čiji je skup vrhova V, a skup bridova $E \setminus E'$, označavamo s $G - E$, a ako je $E = \{e\}$, s $G - e$.

U oba prethodna slučaja kažemo da smo **odstranili** (uklonili, izbacili) V', odnosno E'.

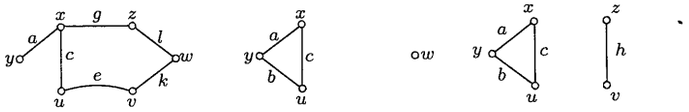
Ako je $\emptyset \neq V' \subseteq V$, onda se podgraf od G čiji je skup vrhova V', a skup bridova je podskup od E čija su oba kraja u V' zove **podgraf induciran** s V' i označava s $G[V']$. Uočite da je $G - V' = G[V \setminus V']$. Za $\emptyset \neq E' \subseteq E$, podgraf od G čiji je skup vrhova skup krajeva bridova od E', a skup bridova E', zove se **podgraf induciran bridovima** E' i označava s $G[E']$. Graf dobiven iz G **dodavanjem** skupa bridova E' zapisujemo kao $G + E'$. Ako je $E' = \{e\}$, pišemo $G + e$ umjesto $G + \{e\}$.

Primjer 6.



Jedan razapinjući podgraf od G

$G - \{x, w\}$



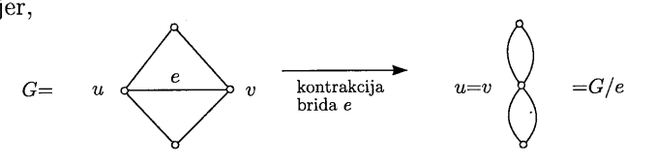
$G - \{b, d, f, h\}$

Inducirani podgraf $G[\{x, y, u, w\}]$

Bridovima inducirani podgraf $G[\{a, b, c, h\}]$

Bilješka 2. Jedan od također nerješenih velikih problema u teoriji grafova je tzv. **problem rekonstrukcije**, a potječe od S. Ulama[2], pa se i iskazuje kao **Ulamova slutnja** (iz 1942.). Ako su G i H grafovi s $n(\geq 3)$ vrhova $u_1, u_2, \ldots, u_n$ i $v_1, v_2, \ldots, v_n$ redom i ako su za svako i podgrafovi $G_i = G - u_i$ i $H_i = H - v_i$ izomorfni, onda su G i H izomorfni.

Još jedna operacija na bridovima (osim odstranjivanja i dodavanja) igra značajnu ulogu. To je kontrakcija brida. Kažemo da je brid $e \in E(G)$ **kontraktiran** ako je odstranjen, a njegovi vrhovi identificirani. Tako dobiveni graf označavamo s G/e. Na primjer,



Ako je $E' \subseteq E(G)$, onda je G/E' graf dobiven iz G kontrakcijom svakog brida iz E', a ako je $H \subseteq G$ podgraf, onda je G/H graf $G/E(H)$.

Minora grafa G je bilo koji graf dobiven iz G nizom elementarnih operacija: odstranjivanja vrhova, odstranjivanja bridova i kontrakcije bridova. Minore grafova igraju vrlo važnu ulogu u "strukturalnoj teoriji grafova". Često je od presudne važnosti da se neki graf ne može dobiti kao minora nekog grafa. Poslije ćemo vidjeti neke efekte ove "strukturalne teorije grafova".

Skup susjeda vrha $v \in V(G)$ u grafu G označavamo s $N_G(v)$. Ako je G jednostavan graf, onda definiramo **stupanj vrha** v, $d_G(v)$ kao broj susjeda od v. Općenito, u bilo kojem grafu G je **stupanj** od v broj $d_G(v)$ bridova od G incidentnih s v, pri čemu se svaka petlja računa kao dva brida. Intuitivno stupanj vrha je broj sjecišta male kružnice oko vrha s linijama koje izlaze iz tog vrha. Ako je jasno o kojem se grafu radi, pišemo $d(v)$ umjesto $d_G(v)$. Rabit ćemo sljedeće oznake za minimalni i maksimalni stupanj grafa:

$$\delta := \delta(G) := \min_{v \in V(G)} d_G(v), \quad \Delta := \Delta(G) := \max_{v \in V(G)} d_G(v).$$

Graf G je **d-regularan** ako je $d(v) = d$, $\forall v \in V(G)$, a **regularan** ako je d-regularan za neko $d \geq 0$. Vrh v je **izoliran** ako je $d(v) = 0$, a **list** ako je $d(v) = 1$.

Tako primjerice, potpun graf K_n je $(n-1)$-regularan, a potpun bipartitni graf $K_{n,n}$ je n-regularan. Očito da izomorfni grafovi u odgovarajućim vrhovima imaju jednake stupnjeve.

Ponovimo (iz Uvoda) osnovnu činjenicu o stupnjevima grafa koju je prvi formulirao Euler 1736. i dokažimo je (još jedanput) formalno.

[2]Stanislav Ulam (1909 – 1984), američki matematičar poljskog podrijetla. Napisao poznatu knjigu "Adventures of a Mathematician".

PROPOZICIJA 1. *U svakom je grafu $G = (V, E)$ zbroj svih stupnjeva dvostruki broj bridova:*

$$\sum_{v \in V} d(v) = 2e(G).$$

Dokaz. (Prebrojavanjem na dva načina.) Neka je M matrica incidencije grafa G i izračunajmo sumu njezinih članova na dva načina: tako da zbrojimo retke i stupce. Suma članova retka od M koji odgovara vrhu v je $d(v)$, a suma svakog stupca je očito 2. Zapišemo li $M = [m_{ve}], v \in V, e \in E$, tada imamo:

$$\sum_{v \in V} d(v) = \sum_{v \in V} \sum_{e \in E} m_{ve} = \sum_{e \in E} \sum_{v \in V} m_{ve} = \sum_{e \in E} 2 = 2e(G).$$

□

KOROLAR 1 (Lema o rukovanju ili "Handshaking Lemma"). *U svakom je grafu broj vrhova neparnog stupnja paran broj.*

Za dokaz vidi Uvod.

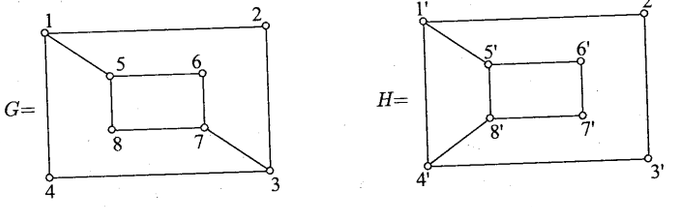
Primjer 7. ***n*-kubni graf** (ili ***n*-kocka**) Q_n je jednostavni graf čiji je skup vrhova $V = \{0,1\}^n$, a dva su vrha $(a_1, \ldots, a_n)$ i $(b_1, \ldots, b_n)$ spojena bridom ako i samo ako se razlikuju u točno jednoj koordinati. Dokažite a) Q_n je n-regularan i bipartitan; b) $v(Q_n) = 2^n$, $e(Q_n) = n2^{n-1}$; c) broj k-dimenzionalnih strana od Q_n (shvaćenih kao potpoliedri) je $f_k(Q_n) = \binom{n}{k} 2^{n-k}$.

Rješenje. a) Uzmimo npr. vrh $(0, 0, \ldots, 0)$. On je spojen s točno n ostalih: $(1, 0, \ldots, 0)$, $\ldots$, $(0, 0, \ldots, 1)$. Tako je (zbog simetrije) i za svaki vrh kocke. Dakle, $d_{Q_n}(v) = n$, $\forall v \in V(Q_n)$. Najjednostavnija biparticija od Q_n je ova: $X =$ sve n-torke iz $\{0,1\}^n$ s parnim brojem jedinica, $Y =$ sve n-torke s neparnim brojem jedinica.

b) Očito $v(Q_n) = 2^n$. Iz Propozicije 1 i a) imamo da je $2^n \cdot n = 2e(Q_n)$, odakle slijedi $(Q_n) = n2^{n-1}$.

c) k-strana u Q_n potpuno je određena izborom k fiksnih koordinata od njih n, a njih je $\binom{n}{k}$, dok preostalih $n-k$ mogu biti proizvoljne, a njih je 2^{n-k}. □

Primjer 8. Odredite stupnjeve svih vrhova na slici i ustanovite jesu li ti grafovi izomorfni.



Rješenje. Oba grafa imaju 8 vrhova i 10 bridova. Vrhovi $2, 4, 6, 8$ u G imaju stupanj 2, a ostali vrhovi stupanj 3, dok su u H vrhovi $2'$, $3'$, $6'$, $7'$ stupnja 2, a ostali stupnja 3. Dakle, ti grafovi imaju jednak broj vrhova stupnja 2 i jednak broj vrhova stupnja 3. Kad bi G i H bili izomorfni, onda bi podgrafovi inducirani s 4 vrha stupnja 2 (tj. $G[\{2, 4, 6, 8\}]$ i $H[\{2', 3', 6', 7'\}]$) bili izomorfni. Međutim, među vrhovima $2, 4, 6, 8$ nema uopće bridova, dok $H[\{2', 3', 6', 7'\}]$ ima dva brida $2'3'$ i $6'7'$. Prema tome, ti podgrafovi nisu izomorfni, pa stoga G i H nisu izomorfni. □

Primjer 9. Neka je G jednostavan graf, a $k \in \mathbb{N}$, $2 \leq k \leq n-2$ čvrst broj. Ako je $n \geq 4$ i ako svi inducirani podgrafovi od G sa k vrhova imaju isti broj m bridova, onda je $G \approx K_n$ ili $G \approx K_n^c$. Dokažite.

Rješenje. Neka je $V(G) = \{v_1, \ldots, v_n\}$. Izračunajmo $e(G) - d(v_i) = e(G - v_i)$. Od preostalih $n-1$ vrhova može se odabrati $\binom{n-1}{k}$ k-članih podskupova, a svaki tako inducirani podgraf ima m bridova, pa ukupno ima $m\binom{n-1}{k}$ bridova. Tu je svaki brid uračunat toliko puta koliko se od preostalih $n-3$ vrhova može odabrati $k-2$ vrha. Stoga dobivamo

$$e(G) - d(v_i) = e(G - v_i) = m\binom{n-1}{k} \Big/ \binom{n-3}{k-2},$$

i očito je G regularan. Sličnim se zaključivanjem za vrhove v_i, v_j dobiva

$$e(G) - d(v_i) - d(v_j) + a_{ij} = e(G - v_i - v_j) = m\binom{n-2}{k} \Big/ \binom{n-4}{k-2},$$

gdje je $a_{ij} = 1$ ako su v_i, v_j susjedni, a 0 inače. Odavde oduzimanjem slijedi da a_{ij} ne ovisi o indeksima i, j. U slučaju da je $a_{ij} = 1$ za svako i, j, iz gornjih formula i Propozicije 1 slijedi da je $m = \binom{k}{2}$ i $d(v_i) = n-1$, $\forall i$, pa je $G \approx K_n$. Slično, za $a_{ij} = 0$, $\forall i, j$, dobivamo $d(v_i) = 0$, $\forall i$, pa je $G \approx K_n^c$. □

Primjer 10. Jednostavni graf $G = (V, E)$ je **vršno-tranzitivan** ako grupa $\mathrm{Aut}(G)$ djeluje tranzitivno na vrhovima, tj. ako $\forall u, v \in V$, $\exists g \in \mathrm{Aut}(G)$, tako da je $g(u) = v$. Slično, G je **bridno-tranzitivan** ako grupa $\mathrm{Aut}(G)$ djeluje tranzitivno na bridovima.

a) Dokažite da ako je G vršno-tranzitivan, onda je regularan. Obrat ne vrijedi.

b) Nađite graf koji je vršno-tranzitivan, a nije bridno-tranzitivan.

c) Nađite graf koji je bridno-tranzitivan, a nije vršno-tranzitivan i dokažite da je svaki takav graf bez izoliranih vrhova bipartitan.

Rješenje. a) Neka su $u, v \in V$, a $g \in \mathrm{Aut}(G)$ tako da je $g(u) = v$. Tada g bijektivno preslikava skup susjeda $N_G(u)$ na skup susjeda $N_G(v)$. Zato je $d_G(u) = d_G(v)$. Protuprimjer za obrat je disjunktna unija 3-ciklusa i 4-ciklusa (objasnite zašto).

b) Graf trostrane prizme, tj. dva trokuta 123 i $1'2'3'$ s dodatnim bridovima $11'$, $22'$, $33'$. Svi vrhovi su očito "ravnopravni", dok bridovi nisu.

c) Očit primjer je $K_{1,2}$ (i općenito $K_{m,n}$, $m \neq n$; zašto?). Ostatak prepuštamo čitatelju. □

Niz stupnjeva grafa G je niz stupnjeva $(d(v_1), \ldots, d(v_n))$ svih vrhova $v_1, \ldots, v_n$ uzetih u rastućem poretku, tj. $d(v_1) \leq d(v_2) \leq \cdots \leq d(v_n)$. Gotovo je očito da izomorfni grafovi imaju iste nizove stupnjeva, pa su stoga dva grafa s različitim nizovima stupnjeva neizomorfni. Obrnuto, grafovi s istim nizovima stupnjeva ne moraju biti izomorfni. Na primjer, disjunktna unija dvaju 3-ciklusa $C_3 \cup C_3$ i C_6 ima niz stupnjeva $(2, 2, 2, 2, 2, 2)$, a očito nisu izomorfni (jer je $C_3 \cup C_3$ nepovezan, a C_6 povezan - vidi iduću točku).

Drugi je primjer Petersenov graf i graf peterostrane prizme; oba imaju niz stupnjeva $(3, 3, \ldots, 3)$, a oni nisu izomorfni jer Petersenov graf nema ciklusa duljine 4, a peterostrana prizma ima pet ciklusa duljine 4 (nacrtajte sliku).

Niz brojeva $d = (d_1, d_2, \ldots, d_n) \in \mathbb{N}_0^n$, $d_1 \leq d_2 \leq \cdots \leq d_n$ je **grafički** ako postoji jednostavni graf čiji je niz stupnjeva d. Nije svaki niz d grafički.

Primjer 11. Dokažite da niz $(1,1,3,3,3,3,5,6,8,9)$ nije grafički.

Rješenje. Kad bi taj niz bio grafički, onda bi vrh sa stupnjem $d_{10} = 9$ bio susjedan sa svim ostalim vrhovima, pa stoga i s oba vrha stupnja 1. Stoga vrh stupnja 8 ne može biti susjedan ni s jednim vrhom stupnja 1. No tada je preostalo još 7 vrhova, pa nijedan ne može imati stupanj 8. Zato taj niz nije grafički. □

Sljedećom propozicijom ćemo dati karakterizaciju grafičkih nizova i time efikasan algoritam kojim se lako može ustanoviti je li neki niz grafički.

PROPOZICIJA 2. *Niz* $d = (d_1, d_2, \ldots, d_n) \in \mathbb{N}_0^n$, $d_1 \leq d_2 \leq \cdots \leq d_n$, $n \geq 2$ *je grafički ako i samo ako je niz* $d' = (d'_1, d'_2, \ldots, d'_{n-1})$ *grafički, gdje je*

$$d'_i = \begin{cases} d_i & , za\ i < n - d_n, \\ d_i - 1 & , za\ i \geq n - d_n \end{cases}.$$

Dokaz. Pretpostavimo prvo da je d' grafički niz nekog grafa $G' = (V', E')$, gdje je $V' = \{v_1, v_2, \ldots, v_{n-1}\}$, a $d_{G'}(v_i) = d_i$, za $i = 1, \ldots, n-1$. Neka je v_n novi vrh različit od svih $v_1, \ldots, v_{n-1}$. Definirajmo graf $G = (V, E)$, gdje je $V = V' \cup \{v_n\}$, a $E = E' \cup \{v_i v_n | i = n - d_n, n - d_n + 1, \ldots, n-1\}$. Drugim riječima, v_n spojimo sa d_n zadnjih vrhova od G'. Tada je d niz stupnjeva od G.

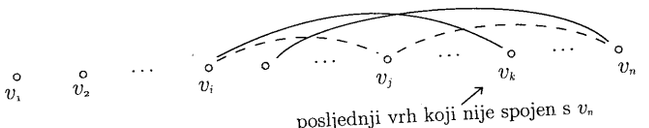
Dokažimo sada obrat, tj. ako je d grafički, da je onda i d' grafički. Promotrimo skup $\mathcal{G}$ svih grafova na skupu vrhova $\{v_1, \ldots, v_n\}$ takvih da je $d(v_i) = d_i$, $i = 1, \ldots, n$.

Tvrdnja. Skup $\mathcal{G}$ sadrži graf G_0 u kojem je vrh v_n susjedan točno s vrhovima $v_{n-d_n}, v_{n-d_n+1}, \ldots, v_{n-1}$, tj. sa zadnjih d_n vrhova.

Ako je G_0 graf kao u tvrdnji, onda graf $G' = (\{v_1, \ldots, v_{n-1}\}, E')$ gdje je $E' = \{e \in E(G_0) | v_n \notin e\})$ ima niz vrhova d' (tj. odstranimo vrh v_n iz G_0). Dakle, treba još dokazati tvrdnju.

Ako je $d_n = n - 1$, tj. ako je v_n susjedan sa svim ostalim vrhovima, onda svaki graf iz $\mathcal{G}$ zadovoljava tvrdnju. Pretpostavimo stoga da je $d_n < n - 1$. Za svaki graf $G \in \mathcal{G}$, definirajmo $k(G)$ kao najveći indeks $k \in [n-1]$ tako da je $v_k v_n \notin E(G)$. Neka je $G_0 \in \mathcal{G}$ s najmanjim $k(G)$. Dokažimo da je $k(G_0) = n - d_n - 1$. Odatle očito slijedi tvrdnja.

Pretpostavimo suprotno, tj. $k = k(G_0) > n - d_n - 1$. Vrh v_n mora biti susjedan s d_n vrhova i najviše $d_n - 1$ od njih može imati veći indeks nego v_k. Stoga postoji indeks $j < k$ tako da je v_j susjedan s v_n, pa je $v_k v_n \notin E(G_0)$, a $v_j v_n \in E(G_0)$.



Kako je $d_{G_0}(v_j) \leq d_{G_0}(v_k)$, slijedi da postoji vrh v_i susjedan s v_k, ali nesusjedan s v_j. U tom slučaju promotrimo novi graf $G' = (V, E')$, gdje je $E' = (E(G_0) \setminus \{v_i v_k, v_j v_n\}) \cup \{v_i v_j, v_k v_n\}$ (v. sliku). Tada se lako provjeri da je niz stupnjeva od G' također jednak d, ali je $k(G') \leq k(G_0) - 1$, što je u kontradikciji s izborom od G_0. Time je tvrdnja dokazana, a time i Propozicija. □

Primjer 12. Je li niz $(1,1,1,2,2,3,4,4,5,5)$ grafički?

Rješenje. Višestruko ćemo primijeniti Propoziciju 2. Prva primjena daje $(n = 10, d_n = 5)$: $(1,1,1,2,2,3,4,4,5,5) \to (1,1,1,2,1,2,3,3,4)$. Sada ovaj niz uredimo rastuće: $(1,1,1,1,2,2,3,3,4)$ i opet primijenimo Propoziciju itd. Nakon 6 takvih primjena doći ćemo do niza $(0,0,0,0)$, a ovaj niz je niz stupnjeva praznog grafa s 4 vrha, pa je stoga i polazni niz grafički. (Pokušajte naći primjer takvog grafa.) □

Izlet u topologiju - Spernerova lema i Browerov teorem o fiksnoj točki

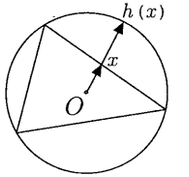
Jedna lijepa primjena dosada urađene teorije grafova skrenut će nas malo u topologiju. Zamislimo, npr. neku rotaciju kugle oko njezina središta ili sažimanje kugle prema središtu. Tada je središte kugle fiksna točka te rotacije ili sažimanja. Ili, ako smo "promućkali" punu zatvorenu šalicu kave, tada nakon "mućkanja" bar jedna točka ostane u istom položaju.

Brouwerov[3] teorem o fiksnoj točki. *Neka je* $D^n = \{x \in \mathbb{R}^n | \|x\| \leq 1\}$ *zatvorena jedinična kugla u* $\mathbb{R}^n$, *a* $f : D^n \to D^n$ *neprekidno[4] preslikavanje. Tada* f *ima fiksnu točku. (Kratko se još kaže da* D^n *ima* **svojstvo fiksne točke**.*)*

Taj vrlo važan rezultat u matematici slijedi iz jednog kombinatornog rezultata poznatog kao Spernerova lema, a ta lema je lagana posljedica Korolara 1 (tj. leme o rukovanju). Uočimo prvo da Brouwerov teorem u dimenziji 1 glasi ovako: *Za svako neprekidno preslikavanje* $f : [0,1] \to [0,1]$ *postoji točka* $x_0 \in [0,1]$ *tako da je* $f(x_0) = x_0$.

To se obično dokazuje tako da se pogleda neprekidna funkcija $g : [0,1] \to \mathbb{R}$, $g(x) = f(x) - x$. Tada je $g(0) \geq 0$, a $g(1) \leq 0$, pa g u nekoj točki $x_0 \in [0,1]$ mora poprimiti vrijednost 0 (zbog Rolleovog teorema iz analize). Intuitivno, to znači da graf funkcije $y = f(x)$ mora prijeći pravac $y = x$. Sada krenimo u više dimenzije.

Uočimo prvo da je n-kugla D^n topološki ekvivalentna n-simpleksu. Npr., za $n = 2$ postoji homeomorfizam h trokuta na krug, dobiven radijalnim rastezanjem svake dužine Ox linearno na dužinu $Oh(x)$ (sl.). Stoga je dovoljno dokazati da simpleks ima svojstvo fiksne točke. Mi ćemo radi jednostavnosti razmatranja provesti u dimenziji 2.

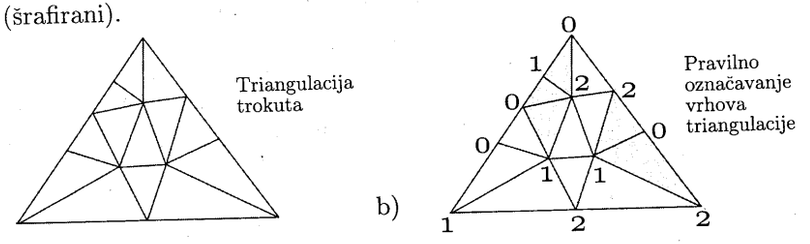


Neka je, dakle, T 2-dimenzionalni simpleks, tj. trokut u ravnini. **Simplicijalna subdivizija** (ili **triangulacija**)od T je rastav od T na konačno mnogo manjih trokutića, tako da se svaka dva trokutića ili ne sijeku ili im je presjek zajednički vrh ili zajednička stranica (v. sliku). Sada uvedimo sljedeće **pravilno označavanje**

[3] Luitzen Egbertus Jan Brouwer (1881 – 1966), nizozemski matematičar

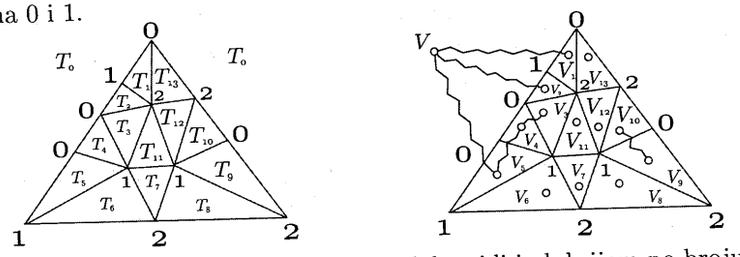
[4] Sve relevantne pojmove i činjenice iz topologije, čitatelj može naći u [153].

vrhova. Neka su vrhovi trokuta označeni trima simbolima, npr. 0, 1, 2, a vrhove trokutova subdivizije također označimo s 0, 1 ili 2, ali tako da vrhovi koji su na stranici 01 budu označeni s 0 ili 1, oni koji su na stranici 02 s 0 ili 2, a oni koji su na 12 s 1 ili 2. Trokut subdivizije čiji vrhovi imaju sve tri oznake $0, 1, 2$ zvat ćemo **istaknut**. Npr. (na slici b)) pravilno označavanje vrhova ima pet istaknutih trokutića (šrafirani).



Spernerova lema. *Svako pravilno označavanje simplicijalne subdivizije trokuta ima neparan broj istaknutih trokutića.*

Dokaz. Označimo s T_0 područje ravnine van trokuta T, a s $T_1, T_2, \ldots, T_m$ trokutiće subdivizije. Konstruiramo graf G ovako. $V(G) = \{v_0, v_1, \ldots, v_m\}$, gdje je $v_i \in \text{int}T_i$ (nutrina od T_i). Dva vrha v_i, v_j spojimo bridom $\iff$ T_i, T_j imaju zajednički brid s oznakama 0 i 1.



Očito je stupanj $d(v_0)$ neparan broj (to se lako vidi indukcijom po broju točaka na stranici 01). Korolar 1 tada povlači da među vrhovima $v_1, v_2, \ldots, v_m$ ima neparan broj njih s neparnim stupnjem. No svaki vrh $v_i, i = 1, 2, \ldots, m$ ima očito stupanj $d(v_i) \leq 2$, pa stoga među njima ima neparan broj njih stupnja 1. Međutim, jasno je vrh v_i $(i = 1, 2, \ldots, m)$ stupnja 1 ako i samo ako je T_i istaknut trokut. Prema tome, sigurno i postoji istaknut trokut. □

Spernerova lema se u višim dimenzijama dokazuje indukcijom po dimenziji n.

Dokaz Brouwerovog teorema o fiksnoj točki. Dokaz ćemo provesti opet za dimenziju 2, tj. za trokut T. Neka je $f : T \to T$ neprekidno preslikavanje. Neka su vrhovi od T točke a_0, a_1, a_2 u ravnini. Tada se svaka točka $x \in T$ može prikazati kao $x = x_0a_0 + x_1a_1 + x_2a_2$, gdje su $x_i \geq 0$, $\sum x_i = 1$. Prema tome, x se može jedinstveno reprezentirati vektorom (x_0, x_1, x_2). Realni brojevi x_i još se zovu **baricentričke koordinate** od x. Preslikavanje f tada se može zapisati kao $f(x_0, x_1, x_2) = (x_0', x_1', x_2')$. Definirajmo skupove $F_i := \{x \in T | x_i' \leq x_i\}$, $i = 0, 1, 2$. Dovoljno je dokazati da je $F_0 \cap F_1 \cap F_2 \neq \emptyset$. Tada, naime, postoji

točka $x \in F_0 \cap F_1 \cap F_2$, pa zbog $x_i' \leq x_i$, $i = 0, 1, 2$, te $\sum x_i = \sum x_i' = 1$ slijedi $(x_0', x_1', x_2') = (x_0, x_1, x_2)$, tj. $f(x) = x$.

Stoga prvo uočimo da za svaku triangulaciju od T postoji pravilno označavanje vrhova, tako da svaki vrh označen sa i leži u skupu F_i, $i = 0, 1, 2$. Zaista, to se može postići pravilnim označavanjem (u skladu s f) ovako. Neka je v vrh triangulacije, a $f(v) = v'$. Tada označimo v s $i := \min\{j | v_j' \leq v_j \neq 0\}$. Ako je $v' = v$, teorem je dokazan, a ako je $v' \neq v$, onda zbog $\sum v_j' = \sum v_j = 1$ postoji indeks i tako da je $v_i' \leq v_i \neq 0$, pa je to označavanje dobro definirano. Provjerimo da je i pravilno. Prvo, ako je $a_i' = a_i$, teorem je dokazan, a ako je $a_i' \neq a_i$, onda je a_i označen s i. Ako je v na bridu nasuprot a_i, onda je v_i=0, pa iz $v' \neq v$ slijedi da v nije označen s i. Prema Spernerovoj lemi, postoji trokut uvw te triangulacije, tako da je $u \in F_0$, $v \in F_1$, $w \in F_2$.

Kako to vrijedi za svaku triangulaciju od T, jasno je da možemo odabrati po volji finu triangulaciju, naime takvu da duljina maksimalne stranice svih trokutića (tzv. **očica**) triangulacije bude po volji malen broj. Uzmimo sada niz triangulacija čije očice teže nuli (npr. takav niz da je očica n-te triangulacije manja od $1/n$). Tada, prema spomenutom, dobivamo niz trokutića $u^{(n)}v^{(n)}w^{(n)}$, tako da je $u^{(n)} \in F_0$, $v^{(n)} \in F_1$, $w^{(n)} \in F_2$, za sve $n \in \mathbb{N}$.

Budući da je f neprekidno preslikavanje, a baricentričke koordinate neprekidno ovise o točki, to se lako vidi da je F_i zatvoren (pa zbog omeđenosti i kompaktan) skup. Stoga postoje konvergentni podnizovi nizova $u^{(n)}, v^{(n)}, w^{(n)}$ čije udaljenosti postaju po volji male. Zbog toga ti podnizovi konvergiraju nekoj točki $x \in F_0 \cap F_1 \cap F_2$, čime je dokaz završen. Dokaz je sasvim analogan u bilo kojoj dimenziji. □

Zanimljivo je da Brouwerov teorem povlači Spernerovu lemu. Njihova poopćenja, razne primjene (npr. u optimizaciji i napose u ekonomiji), kao i algoritme za nalaženje fiksnih točaka, čitatelj može naći u [217].

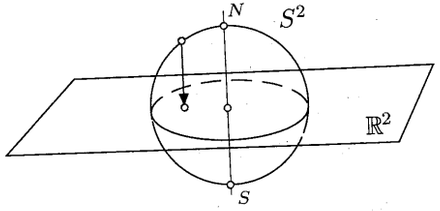
Bilješka 3. a) Postoje i mnogo općenitiji teoremi o fiksnoj točki nego što je Brouwerov teorem. Oni općenito govore o tome da pod izvjesnim uvjetima neka funkcija f ima fiksnu točku. Takvi su zaključci od osnovne važnosti u mnogim područjima u matematici, jer često tako dokazujemo egzistenciju rješenja raznih jednadžbi (npr. diferencijalnih i integralnih jednadžbi, dinamičkih sistema itd.). Važnost takvih teorema ogleda se čak i u teoriji kompjuterskih programa, napose u tzv. *programskoj semantici.*

b) I mnogi drugi teoremi iz tzv. *algebarske topologije* mogu se dokazati kombinatorno. Takav je i sljedeći rezultat (v. [19*].)

Borsuk[5]-Ulamov teorem (1933). *Za svako neprekidno preslikavanje $f : S^n \to \mathbb{R}^n$ postoje dvije antipodalne točke x, $-x \in S^n$, takve da je $f(x) = f(-x)$. ($S^n = \{x \in \mathbb{R}^{n+1} | \|x\| = 1\}$ je* **n-dimenzionalna (jedinična) sfera**).

Tako primjerice, ako (neprekidno) projiciramo sferu S^2 na ekvatorijalnu ravninu (tj. "spljoštimo" je), onda "sjeverni pol" N i "južni pol" S padnu u istu točku.

[5]Karol Borsuk (1905 – 1982), poljski matematičar.



Slikovito možemo i ovako izreći ovaj teorem. Na Zemlji u svakom trenutku postoje dvije antipodalne točke u kojima su temperature jednake i tlak zraka jednak (uz pretpostavku da se one neprekidno mijenjaju). Evo i još nekih "konkretnih" primjena Brouerowog teorema o fiksnoj točki i Borsuk-Ulamovog teorema o antipodima.

Primjer 13. Dokažite **Frobeniusov**[6]**teorem**. Neka je $A = [a_{ij}]$ realna $n \times n$ matrica, $a_{ij} \geq 0$, $\forall i, j$. Tada A ima realnu svojstvenu vrijednost $\lambda \geq 0$.

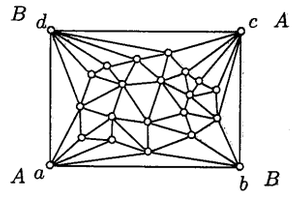
Rješenje. Možemo pretpostaviti da je A regularna matrica, jer inače možemo uzeti da je $\lambda = 0$. Neka je $A : \mathbb{R}^n \to \mathbb{R}^n$ pripadni linearni operator matrice A, a $S^{n-1} \subset \mathbb{R}^n$ jedinična sfera iz $\mathbb{R}^n$. Definirajmo neprekidno preslikavanje $B|_{S^{n-1}} : S^{n-1} \to S^{n-1}$, $B(x) = Ax/\|Ax\|$. Tada B preslikava prvi "oktant" $Q = \{(x_1, \ldots, x_n) \in S^{n-1} | x_i \geq 0, \forall i\}$ u sama sebe, a Q je homeomorfan s $(n-1)$-kuglom D^{n-1}. Sada se primijeni Brouwerov teorem na $B|_Q$ i tvrdnja slijedi. □

Primjer 14. Dokažite da je Brouwerov teorem o fiksnoj točki ekvivalentan sljedećem. Ne postoji neprekidno preslikavanje $f : D^n \to D^n$ čija je restrikcija na rubnu sferu S^{n-1} identiteta. Kaže se još da ne postoji retrakcija kugle D^n na sferu S^{n-1}. (**Retrakcija** topološkog prostora X na potprostor $A \subset X$ je neprekidno preslikavanje $r : X \to X$, tako da je $r|_A = \mathrm{id}_A$.)

Rješenje. Kad bi postojala retrakcija $g : D^n \to D^n$ na sferu S^{n-1}, onda neprekidno preslikavanje $x \mapsto -g(x)$ sa D^n u D^n ne bi imalo fiksnu točku. Obratno, ako $f : D^n \to D^n$ nema fiksne točke, promotrite neprekidno preslikavanje koje točki $x \in D^n$ pridružuje presjek zrake kroz $f(x)$ i x sa sferom S^{n-1}. □

Evo i jedne "konkretne" primjene Spernerove leme (a zapravo leme o rukovanju) na inačicu igre HEX. Dva igrača, recimo Ante A i Branka B igraju sljedeću igru na kvadratnoj ploči $abcd$ koja je na bilo koji način triangulirana (kao na donjoj slici). Igrači igraju naizmjence i to tako da npr. Ante počinje s vrhovima a i c i obilježi ih s A, a Branka počinje s vrhovima b i d i obilježi ih s B. Pri svakom potezu, svaki igrač obilježava jedan vrh triangulacije svojim simbolom i cilj mu je da svojim simbolima poveže svoju dijagonalu (Ante dijagonalu ac ili Branka dijagonalu bd preko vrhova triangulacije). Pobjednik je onaj igrač koji prvi poveže svoju dijagonalu. Ako igrač koji je na potezu nema mogućnost da označi vrh, igra se smatra neriješenom ili pat pozicijom.

[6]Ferdinand Frobenius (1849 – 1917), njemački matematičar



Primjer 15. Dokažite da gornja igra HEX ne može završiti neriješeno.

Rješenje. Pretpostavimo suprotno, tj. da je nastupila pat pozicija. Neka je $\mathcal{A}$ skup vrhova koje je označio Ante, a $\mathcal{B}$ skup vrhova koje je označila Branka. Pridružimo vrhovima oznake $1, 2, 3$ prema sljedećem pravilu. Vrh iz $\mathcal{A}$ je označen s 1 ako se može povezati putem iz a preko vrhova iz $\mathcal{A}$. Slično, vrhovi iz $\mathcal{B}$ koji se mogu povezati putem preko vrhova iz $\mathcal{B}$ označeni su s 2. Ostale vrhove označimo s 3. Po pretpostavci su c i d označeni s 3, jer bi inače jedan od igrača pobijedio.

Pokažimo da postoji unutarnji trokut T čiji su vrhovi označeni s $1, 2$ i 3. To vodi na kontradikciju, jer vrh označen s 3 (neka je to x) ne može pripadati ni skupu $\mathcal{A}$ ni skupu $\mathcal{B}$. Naime, kada bi $x \in \mathcal{A}$, pogledamo vrh y od T označenog s 1. Po definiciji, postoji put od a do y označenih samo s elementima iz $\mathcal{A}$ i taj bi se put tada mogao produžiti do x, jer je y susjedan s x. Iz sličnih razloga $x \in \mathcal{B}$. To je kontradikcija.

Egzistenciju takvog trokuta T dokazujemo isto kao i Spernerovu lemu. Detalje ostavljamo čitatelju. □

S matematičkog su stajališta mnoge igre razmatrane u knjizi [13*]. A sada jedna "konkretna" primjena Borsuk-Ulamovog teorema.

Primjer 16 ("Teorem o sendviču sa šunkom"). Dokažite da se sendvič sa šunkom jednim potezom noža može raspoloviti. Točnije, ako su u prostoru $\mathbb{R}^3$ dana tri omeđena izmjeriva skupa, onda postoji ravnina koja (po volumenu) istovremeno raspolavlja sva tri skupa. Analogna tvrdnja vrijedi i u bilo kojem prostoru $\mathbb{R}^n$ u kojem imamo n skupova.

Dokaz. Mi ćemo dokaz provesti u dimenziji $n = 2$. U višim dimenzijama dokaz je potpuno analogan. Neka su, dakle, $A_1, A_2 \subseteq \mathbb{R}^2$ dva omeđena izmjeriva skupa. Tu ravninu $\mathbb{R}^2$ ćemo identificirati s afinom ravninom $\alpha = \{(x, y, 1) \,|\, x, y \in \mathbb{R}\}$ u $\mathbb{R}^3$. Za svaki vektor $x \in S^2$, neka je $f_i(x)$ mjera (ovdje površina) onog dijela od A_i koji je na istoj strani kao x s obzirom na ravninu H_x kroz ishodište koja je okomita na x, $i = 1, 2$. Borsuk-Ulamov teorem primijenjen na (očito neprekidnu) funkciju $f : S^2 \to \mathbb{R}^2$, $f(x) = (f_1(x), f_2(x))$ povlači da postoji $x \in S^2$ tako da je $f_1(x) = f_1(-x)$ i $f_2(x) = f_2(-x)$. To znači da pravac $\alpha \cap H_x$ raspolavlja oba skupa A_1 i A_2. □

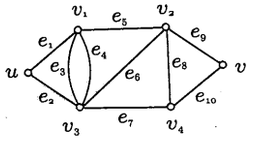
Već na temelju ovih primjera jasno je da između "diskretne" i "neprekidne" matematike postoji velika međuovisnost. S time ćemo se još sresti (posebice u §6 Planarni grafovi).

Šetnje, putovi i povezanost grafova

Šetnja u grafu G je niz $W := v_0 e_1 v_1 e_2 \ldots e_k v_k$, čiji članovi su naizmjence vrhovi v_i i bridovi e_i, tako da su krajevi od e_i vrhovi v_{i-1} i v_i, $1 \leq i \leq k$. U jednostavnom je grafu šetnja potpuno određena samo nizom svojih vrhova $v_0 v_1 \ldots v_k$. Kažemo da je v_0 **početak**, a v_k **kraj** šetnje W ili da je W **šetnja od** v_0 **do** v_k ili (v_0, v_k)**-šetnja**.

Vrhovi $v_1, v_2, \ldots, v_{k-1}$ su **unutarnji vrhovi šetnje**, a broj k se zove **duljina šetnje** W. Ako su $W = v_0e_1v_1 \ldots e_kv_k$ i $W' = v_ke_{k+1}v_{k+1} \ldots e_lv_l$ dvije šetnje, onda se šetnja $v_0e_1 \ldots e_kv_ke_{k+1} \ldots e_lv_l$ dobivena **nadovezivanjem** W i W' kod vrha v_k obilježava s WW', a šetnja $v_ke_kv_{k-1} \ldots e_1v_0$ dobivena obrnutim redoslijedom obilaska od W zove se **inverzna šetnja** od W i obilježava s W^{-1}. Dio šetnje $W = v_0e_1v_1e_2 \ldots e_kv_k$ je podniz $v_ie_{i+1}v_{i+1} \ldots e_jv_j$ susjednih članova od W. To se još zove i (v_i, v_j)-**dio** od W. Šetnja W je **zatvorena** ako je $v_0 = v_k$. Kažemo da v_i **prethodi** vrhu v_j u W ako je $i < j$ i katkad pišemo $v_i \prec v_j$. Ako su svi bridovi $e_1, e_2, \ldots, e_k$ šetnje W međusobno različiti, onda se W zove **staza**, a ako su na stazi i svi vrhovi $v_0, \ldots, v_k$ međusobno različiti, ona se zove **put**. Uočite da je (v_0, v_k)-šetnja minimalne duljine nužno (v_0, v_k)-put. Zatvorena staza pozitivne duljine čiji su vrhovi (osim krajeva) međusobno različiti zove se **ciklus**. Dva vrha u, v grafa G su **povezana** ako postoji (u, v)-put u G. Smatramo da uvijek imamo trivijalni (u, u)-put. **Udaljenost** $d_G(u, v)$ dvaju vrhova u i v u grafu G je duljina najkraćeg (u, v)-puta u G. Ako nema puta u G koji spaja u i v, stavljamo $d_G(u, v) = \infty$. Kad je iz konteksta jasno o kojem je grafu riječ, pišemo samo $d(u, v)$. Katkad ćemo jednostavno reći "put" kao sinonim za podgraf čiji su vrohovi i bridovi članovi puta. **Dijametar** grafa G, diam G je maksimalna udaljenost među njegovim bridovima, tj. to je duljina puta maksimalne duljine u G. **Struk** (engl. *girth*) je duljina najkraćeg ciklusa u grafu (ako uopće ima ciklusa), a inače ga definiramo kao nulu. Ciklus je **paran** ako je parne duljine, a inače je **neparan**.

Primjer 17.



(u, v)-šetnja: $ue_1v_1e_3v_3e_7v_4e_7v_3e_6v_2e_9v$
(u, v)-staza: $ue_2v_3e_3v_1e_4v_3e_7v_4e_{10}v$
(u, v)-put: $ue_2v_3e_4v_1e_5v_2e_9v$
$d(u, v) = 3 = \text{diam } G$, struk $G = 2$. □

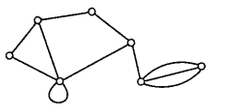
PROPOZICIJA 3. *Neka je G jednostavni graf minimalnog stupnja δ. Tada*

(i) G sadrži put P duljine $\geq \delta$;

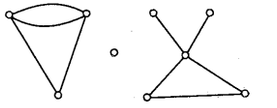
(ii) ako je $\delta \geq 2$, G sadrži ciklus C duljine $\geq \delta + 1$.

Dokaz. (Odabirom maksimalnog puta.) Neka je $P := v_0v_1 \ldots v_k$ maksimalni put u G, tj. onaj koji se ne može dalje produljiti ni na jednom kraju. Tada su svi susjedi od v_0 u P. Neka je $k := \max\{i \mid v_0v_i \in E\}$. Tada je $k \geq d(v_0) \geq \delta$. Stoga je P duljine $\geq \delta$, a ako je $\delta \geq 2$, onda je $C := v_0v_1 \ldots v_kv_0$ ciklus duljine $\geq \delta + 1$. □

Graf je **povezan** ako su svaka dva njegova vrha povezana nekim putom. **Komponenta povezanosti** grafa G je maksimalni povezan podgraf od G (tj. povezani podgraf koji nije sadržan ni u jednom većem povezanom podgrafu). Ekvivalentno se povezanost može definirati ovako. Povezanost među vrhovima je relacija ekvivalencije, pa stoga postoji particija skupa vrhova V na klase ekvivalencije i to su komponente povezanosti. Ako graf ima samo jednu komponentu povezanosti, onda je povezan (a inače **nepovezan**). **Broj komponenti povezanosti** od G označavamo s $c(G)$.



povezan graf



nepovezan graf s 3 komponente

Primjer 18. Dokažite da je $c(G) + e(G) \geq v(G)$.

Dokaz. Indukcijom po $e(G)$. Ako je $e(G) = 0$, onda se G sastoji od izoliranih vrhova, pa je $c(G) = v(G)$. Ako je $e \in E(G)$, onda je $e(G) \geq c(G - e) - 1$ jer e spaja ili dva vrha iz iste komponente od $G - e$, pa je $c(G) = c(G - e)$, ili iz različitih komponenata, pa je $c(G - e) = c(G) - 1$. Indukcijom slijedi $c(G - e) + e(G - e) \geq v(G - e) = v(G) \Rightarrow c(G) + e(G) \geq c(G - e) + 1 + e(G - e) - 1 = c(G - e) + e(G - e) \geq v(G)$. □

Veza između šetnji u grafu i matrice susjedstva dana je sljedećom Propozicijom.

PROPOZICIJA 4. *Neka je $A = A(G) = [a_{ij}]$ matrica susjedstva grafa G. Tada je (i, j)-ti član l-te potencije A^l jednak broju (v_i, v_j)-šetnji u G duljine l. Stoga je broj svih šetnji na G duljine l jednak sumi svih članova od A^l.*

Dokaz. Indukcijom po l. Šetnja duljine 1 između dvaju vrhova znači da su dva vrha povezana bridom, pa za $l = 1$ tvrdnja Propozicije slijedi iz definicije matrice susjedstva. Pretpostavimo da tvrdnja vrijedi za $k - 1$ i dokažimo je za k. Neka je $a_{ij}^{(k)}$ (i, j)-ti član matrice A^k. Tada je $(n = v(G))$:

$$a_{ij}^{(k)} = \sum_{r=1}^{n} a_{ir}^{(k-1)} a_{rj}.$$

Svaka (v_i, v_j) šetnja duljine k sastoji se od (v_i, v_r) šetnje duljine $k - 1$, gdje je v_r neki susjed od v_j i brida v_rv_j



Po pretpostavci indukcije, broj (v_i, v_r)-šetnji duljine $k - 1$ je jednak $a_{ir}^{(k-1)}$, pa je (prema pravilima umnoška i zbroja) broj (v_i, v_j)-šetnji duljine k jednak

$$\sum_{v_rv_j \in E} a_{ir}^{(k-1)} = \sum_{r=1}^{n} a_{ir}^{(k-1)} a_{rj} = a_{ij}^{(k)},$$

čime je induktivni dokaz završen. □

KOROLAR 2. *Udaljenost između dvaju vrhova v_i, v_j je jednaka*

$$d_G(v_i, v_j) = \min\{k \in \mathbb{N} \mid a_{ij}^{(k)} \neq 0\}.$$

Dakle, da se što brže izračunaju udaljenosti svih parova vrhova grafa, treba primijeniti brze algoritme za množenje matrica. Takav je, npr. **Strassenov algoritam** reda $O(n^{\log_2 7})$ iz Primjera 28 u pogl. III.

Eksplicitne formule za broj šetnji i putova dane duljine vrlo je teško naći općenito. Međutim, broj šetnji na danom putu može se eksplicitno izračunati.

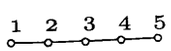
Definirajmo **matričnu funkciju izvodnicu za broj šetnji** na grafu G kao (I je jedinična matrica)

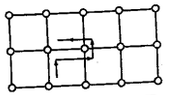
$$W(G,t) := (I - tA)^{-1} = I + tA + t^2A^2 + \cdots = \sum_{l\geq 0} W^l(G)t^l = \frac{\operatorname{adj}(I-tA)}{\det(I-tA)}$$

i **karakteristični polinom grafa** $\varphi(G,t) := \det(I - tA)$. Pritom je $W^l(G)$ matrica čiji je (i,j)-ti član $(W^l(G)_{i,j}) =: W^l_G(v_i,v_j)$ jednak broju (v_i,v_j)-šetnji duljine l u G, a adj označava adjunktu matrice. **Funkcija izvodnica za broj šetnji** u G je definirana s

$$W_G(t) := \sum_{l\geq 0} W_G(l)t^l.$$

Neka je sad $G = P_n$ put (ili **linearni graf**) s n vrhova $1,2,\ldots,n$. Tada je njegova matrica susjedstva $A_n := A(P_n) = (\delta_{|i-j|,1})$. Ako je $G = P_m \times P_n =: P_{m,n}$ produkt dvaju putova, onda je matrica susjedstva $A(P_{m,n}) = A_m \otimes I_n + A_n \otimes I_m$, gdje je $\otimes$ Kroneckerov produkt matrica, a I_k jedinična $(k\times k)$-matrica. (Uočite da ti sumandi komutiraju s obzirom na množenje matrica!)

a) 

b) 

šetnja duljine 3 na $P_{5,3}$

Označimo nadalje s $W_n(i;j;t) := \sum_{l\geq 0} W^l_n(i,j)t^l$, $W_n(t) := \sum_{l\geq 0} W^l_n t^l$ odgovarajuće funkcije izvodnice za brojeve šetnji, tj. $W_n(i;j;t) := W(P_n,t)_{i,j}$, $W_n(t) := W_{P_n}(t)$, a analogno $W_{m,n} := W_{P_{m,n}}(t)$ itd. Metodama "spektralne teorije grafova" dokazuje se tada da vrijedi ova formula (vidi [61]):

$$W^l_n = \frac{2^l}{n+1}\sum_{j=1}^{n+1} \cot^2\frac{2j-1}{n+1}\frac{\pi}{2}\cos^l\frac{2j-1}{n+1}\pi.$$

No udruženim kombinatornim i analitičkim metodama može se dokazati sljedeće (usp. [135]).

TEOREM (D. Svrtan, D. Veljan 1987.).

a) $W_n(i;j;t) = \frac{U_{i-1}(1/2t)U_{n-j}(1/2t)}{tU_n(1/2t)}$ *za* $i \leq j$;

b) $W_n(t) = \frac{1}{1-2t}\left[n - \frac{2t}{1-2t}\left(1 - \frac{1+U_{n-1}(1/2t)}{U_n(1/2t)}\right)\right]$;

c) $W^l_n = (n+1)2^l - \binom{l}{l/2} - 4l\binom{l-1}{\lfloor (l-1)/2\rfloor}$ *za* $l \leq n$ *i općenito*

$$W^l_n = n2^l - \sum_{k\in\mathbb{Z}}(-1)^k \sum_{j=0}^{l-1} 2^{-j}\binom{j}{\lfloor \frac{j+k(n+1)}{2}\rfloor};$$

d) Asimptotsko ponašanje od W^l_n *(tj. za dovoljno velike* $l \leq n$*) je*

$$\frac{W^l_n}{n2^l} \sim 1 + \frac{1}{n} - \frac{4}{\pi}\sqrt{\lfloor\frac{l}{2}\rfloor/\pi} - \frac{3-(-1)^l}{2\pi}/\sqrt{\pi\lfloor l/2\rfloor};$$

e) $W^l_{m,n} = (m+1)(n+1)4^l - (m+n+2)(2l+1)\binom{2l}{l} - \binom{l}{l/2}^2 - 8l\left(2\lfloor\frac{l}{2}\rfloor+1\right)\binom{l-1}{\lfloor l/2\rfloor}^2$, $l \leq m,n$;

f) Asimptotsko ponašanje od $W^l_{m,n}$ *(*$l \leq m,n$ *dovoljno velik) je*

$$\frac{W^l_{m,n}}{mn4^l} \sim \left(1-\frac{a_l}{m}\right)\left(1-\frac{a_l}{n}\right) + \frac{2-(-1)^l}{\pi mnl} - \frac{(-1)^l}{\pi mnl(l-1)},\ \textit{gdje je}\ a_l = \frac{2l+1}{\sqrt{\pi l}} - 1.$$

Pritom je $U_n(x)$ **Čebiševljev polinom druge vrste** definiran s $U_n(x) = \sin(n+1)\theta/\sin\theta$, gdje je $x = \cos\theta$. $U_0(x) = 1$, $U_1(x) = 2x$, $U_2(x) = 4x^2 - 1$ itd. Vrijedi rekurzija $U_{n+1} = 2xU_n(x) - U_{n-1}(x)$. Nadalje, u svim gornjim formulama podrazumijeva se standardna konvencija

$$\binom{p}{q/2} = \begin{cases} \text{obični binomni koeficijent za } p \geq q/2 \geq 0,\ q \text{ paran broj} \\ 0, \text{ inače} \end{cases}$$

Uočite nadalje da šetnje u P_n odgovaraju dijagonalnim putovima u kvadratnoj mreži ravnine. Npr. ako je P_5 smješten na osi y kao segment $[0,5]$, onda šetnji 3454 u P_5 odgovara put $(0,3)(1,4)(2,5)(3,4)$ u kvadratnoj mreži. Taj se put projicira na kvadratnu mrežu.

§ 2. Ciklusi i stabla

Ciklusi i stabla (posebno putovi) su najjednostavniji, ali su i među najvažnijim grafovima, jer su u nekom smislu od njih sagrađeni svi grafovi. Zato ćemo njihovu proučavanju posvetiti punu pažnju. Započnimo jednim primjerom o njihovim karakterističnim polinomima i spektrima.

Primjer 19. a) Odredite svojstvene vrijednosti (spektar) n-ciklusa C_n i među njima najmanju i dokažite da je karakteristični polinom od C_n dan formulom $\varphi(C_n,t) = 2(T_n(t/2)-1)$, gdje je T_n **Čebiševljev polinom prve vrste**. $T_n(x) = \cos(n\arccos x)$ ili rekurzivno (zbog adicijske formule) dan s $T_0(x) = 1$, $T_1(x) = x$ i $T_{n+1}(x) = 2xT_n(x) - T_{n-1}(x)$.

b) Neka je G graf s n vrhova $x_1, \ldots, x_n$, a $G_i = G - x_i$, $i = 1, \ldots, n$. Dokažite da za karakteristični polinom $\varphi(G,t)$ vrijedi

$$\varphi'(G,t) = \sum_{i=1}^{n} \varphi(G_i,t).$$

c) Odredite karakteristični polinom i spektar puta P_n.

Rješenje. a) Matrica susjedstva $A_n = A(C_n) = [a_{ij}]$ od C_n dana je s $a_{i,i\pm1} = 1$, $i = 1, \ldots, n$, a ostali $a_{ij} = 0$ (tu se $i \pm 1$ računa mod n). Svi n-ti korijeni iz jedinice su $1, \ldots, n$, a ostali $a_{ij} = 0$ (tu se $i \pm 1$ računa mod n). Svi n-ti korijeni iz jedinice su $1, \xi, \xi^2, \ldots, \xi^{n-1}$, gdje je $\xi = e^{\frac{2\pi i}{n}}$. Neka je $\lambda = \xi^k$ bilo koji od tih korijena. Tvrdimo da je $(1, \lambda, \ldots, \lambda^{n-1})^T$ svojstveni vektor od A_n sa svojstvenom vrijednosti $\lambda + \lambda^{-1}$. Naime, iz oblika matrica A_n (raspišite je npr. za $n = 5$) vidimo da je

$$A_n \begin{bmatrix} 1 \\ \lambda \\ \vdots \\ \lambda^{n-1} \end{bmatrix} = \begin{bmatrix} \lambda + \lambda^{n-1} \\ \lambda^2 + 1 \\ \vdots \\ 1 + \lambda^{n-2} \end{bmatrix} = (\lambda + \lambda^{-1}) \begin{bmatrix} 1 \\ \lambda \\ \vdots \\ \lambda^{n-1} \end{bmatrix}.$$

Vektori $(1, \lambda, \ldots, \lambda^{n-1})^T$ su nezavisni (Vandermondeova determinanta je $\neq 0$), pa su $\lambda + \lambda^{-1} = \xi^k + \xi^{-k} = 2\cos\frac{2\pi}{n}$, $0 \le k \le n-1$ sve svojstvene vrijednosti od C_n. Kako je cos padajuća, najmanja među njima je $2\cos(n-1)\pi/n = -2\cos\pi/n$. (Uočimo usput da je i za svaki neprazan jednostavan graf G, najmanja svojstvena vrijednost od $A = A(G)$ negativna, jer ako su $\lambda_1 \ge \lambda_2 \ge \cdots \ge \lambda_n$ sve svojstvene vrijednosti, onda im je suma jednaka tragu Tr A, a Tr $A = 0$, jer su svi $a_{ii} = 0$.)

Sada se lako provjeri da polinom $Q_n(t) = \frac{1}{2}\varphi(C_n,t) + 1\frac{1}{2}\prod_{k=0}^{n-1}(t - 2\cos\frac{2k\pi}{n} + 1)$ zadovoljava $Q_n(t) = T_n(t/2)$. Zato je $\varphi(C_n,t) = 2(T_n(t/2) - 1)$. Eksplicitna formula za T_n je (pokušajte je izvesti):

$$T_n(t) = \frac{n}{2} \sum_{k=0}^{\lfloor n/2 \rfloor} \frac{(-1)^k}{n-k} \binom{n-k}{k} (2t)^{n-2k}.$$

b) Kako je derivacija determinante (čiji su članovi funkcije od t) jednaka sumi determinanata u kojima deriviramo sve članove jednog retka, slijedi da deriviranjem $\varphi(G,t) = \det(tI_n - A)$ dobivamo

$$\varphi'(G,t) = \sum_{i=1}^{n} \det(tI_n - A)_i = \sum_{i=1}^{n} \det(tI_{n-1} - A_i) = \sum_{i=1}^{n} \varphi(G_i,t).$$

c) Primijenimo b) na $G = C_n$ i uočimo da za $v \in V(C_n)$ imamo $C_n - v \approx P_{n-1}$ dobivamo da je $\varphi(P_{n-1},t) = \frac{1}{n}\varphi'(C_n,t)$.

Sada u igru ulaze **Čebiševljevi polinomi druge vrste** U_n, definirani s $U_n(x) = \sin(n+1)\theta/\sin\theta$, $\theta = \arccos x$, ili rekurzivno (isto kao i T_n) s $U_{n+1} = 2xU_n(x) - U_{n-1}(x)$, ali s početnim uvjetima $U_0(x) = 1$, $U_1(x) = 2x$. Tada (slično kao u a)) dobivamo

$$\varphi(P_n,t) = U_n(t/2) = \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k \binom{n-k}{k} t^{n-2k}.$$

Lako se vidi da se spektar od P_n sastoji od brojeva $2\cos k\pi/(n+1)$, $k = 1, \ldots, n$. □

Karakterizirajmo sada bipartitne grafove pomoću ciklusa.

PROPOZICIJA 5 (D. König, 1916.). *Graf $G = (V,E)$ je bipartitan ako i samo ako ne sadrži neparne cikluse.*

Dokaz. $\Rightarrow$: Neka je G bipartitan s biparticijom (X,Y), a $C = v_0v_1 \ldots v_kv_0$ bilo koji ciklus u G. Uzmimo da je $v_0 \in X$. Tada zbog $v_0v_1 \in E$ i bipartitnosti od G slijedi $v_1 \in Y$. Tada je opet $v_2 \in X$ itd., općenito $v_{2i} \in X$ i $v_{2i+1} \in Y$. Zbog $v_0 \in X$ je $v_k \in Y$ (jer je v_kv_0 brid), pa je $k = 2i+1$ za neko i. To znači da je C paran ciklus.

$\Leftarrow$: Dokažimo prvo tvrdnju za povezan graf. Neka je G povezan graf bez neparnih ciklusa i neka je $u_0 \in V$ bilo koji čvrst vrh od G. Definirajmo skupove

$$X = \{x \in V \mid d(u_0,x) \text{ paran}\}, \quad Y = \{y \in V \mid d(u_0,y) \text{ neparan}\}.$$

Tvrdimo da je (X,Y) biparticija od G. Prvo, očito je da je $X \cup Y = V$ i $X \cap Y = \emptyset$. Neka su $v, w \in X$ bilo koja dva vrha i dokažimo da vw ne može biti brid u G. Neka je P najkraći put (u_0,v)-put, Q najkraći (u_0,w)-put, a u_1 posljednji zajednički vrh od P i Q. Kako su P i Q najkraći putovi, slijedi da su i (u_0,u_1)-dijelovi najkraći (u_0,u_1) putovi, pa imaju istu duljinu. Kako su $v, w \in X$ slijedi da su P i Q parne duljine, pa su iste parnosti i zato su duljine od $P_1 = (u_1,v)$-dio od P i $Q_1 = (u_1,w)$-dio od Q iste parnosti. Stoga je (v,w)-put $P_1^{-1}Q_1$ parne duljine. Kad bi vw bio brid, onda bi $P_1^{-1}Qwv$ bio ciklus neparne duljine. To je u suprotnosti s pretpostavkom. Stoga nikoja dva vrha u X nisu spojena bridom. Slično, nikoja dva vrha u Y nisu spojena bridom. □

A sada jedan "društveni" problem koji ćemo riješiti s pomoću ciklusa (i putova).

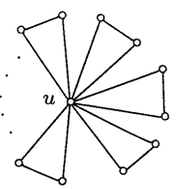
Primjer 20. U nekom društvu od barem troje ljudi, svake dvije osobe imaju točno jednog zajedničkog prijatelja. Tada u tom društvu postoji osoba ("političar") koji je svakome iz tog društva prijatelj.

Rješenje. Ovu situaciju ćemo modelirati grafom $G = (V,E)$, $|V| = n \ge 3$, u kojem skup vrhova V predstavlja članove tog društva, a dva vrha spojimo bridom ako (i samo ako) su pripadni članovi prijatelji.

S tim modelom tvrdnja se svodi na sljedeći teorem: □

TEOREM 1 (o prijateljstvu). *Neka je G jednostavni graf s $n \ge 3$ vrhova u kojem svaka dva vrha imaju točno jedan zajednički susjedan vrh. Tada postoji vrh koji je susjedan svim vrhovima grafa G.*

Dokaz. Mi ustvari tvrdimo da je jedini graf tog tipa – graf "vjetrenjače":



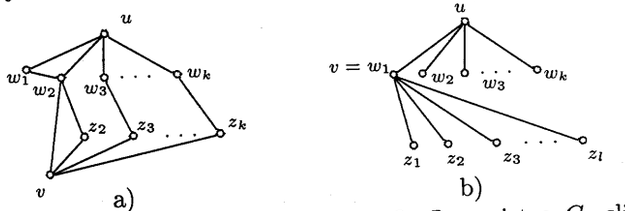
Pretpostavimo suprotno i neka je G graf u kojem nijedan vrh nije susjedan svim ostalima. Da dobijemo kontradikciju, dokazat ćemo dvije tvrdnje. Prva je kombinatorne prirode, a druga rabi linearnu algebru.

Tvrdnja 1. $n = k^2 - k + 1$, za neko $k \geq 2$;

Tvrdnja 2. $k = 2$.

Zajedno tvrdnja 1. i 2. daju kontradikciju, jer za $k = 2$, $n = 3$ što daje $G = K_3$, a to je "vjetrenjača", a pretpostavili smo da G to nije.

Dokaz tvrdnje 1. Pokažimo prvo da je G regularan, tj. $d(u) = d(v)$, za svako $u, v \in V$. Iz uvjeta teorema odmah slijedi da G ne sadrži ciklus C_4 kao podgraf. Nazovimo to *svojstvo* C_4. Neka su prvo u i v nesusjedni vrhovi i neka je $d(u) = k$, a $w_1, \ldots, w_k$ svi susjedi od u. Tada je točno jedan od vrhova w_i susjedan s v, recimo $w_1, \ldots, w_k$ svi susjedi od u. Tada je točno jedan od vrhova w_i susjedan s v, recimo $w_2 \sim v$, a w_2 je susjedan s točno jednim od ostalih w_i, recimo $w_2 \sim w_1$. Tada imamo situaciju kao na sl. a). Vrh v ima s w_1 zajedničkog susjeda w_2,



a)

b)

a s w_i, $i \geq 2$, zajedničkog susjeda z_i, $i \geq 2$. Iz svojstva C_4 slijedi da su svi z_i međusobno različiti. Stoga dobivamo da je $d(v) \geq k = d(u)$, pa zbog simetrije slijedi $d(u) = d(v)$.

Neka su sada u i v susjedni vrhovi, a $v = w_1, w_2, \ldots, w_k$ svi susjedi od u. Ako je z neki nesusjed od u (a takav po pretpostavci postoji) ujedno i nesusjed od v, onda prema prvom dijelu dokaza dobivamo da je $d(u) = d(z) = d(v)$. Stoga možemo pretpostaviti da je v susjedan sa svim vrhovima $z_j \notin \{w_2, \ldots, w_k\}$. Na sl. b) je prikazana situacija sa svih $(1 + k + l)$ vrhova grafa.

Kako po pretpostavci G nije "vjetrenjača", slijedi $d(v) < n - 1$, pa stoga postoji w_i, recimo w_2, koji nije susjedan s v. No, z_1 i w_2 moraju imati zajedničkog susjeda. To ne može biti u jer u i z_1 nisu susjedi, a ne može to biti ni $v = w_1$, jer v i w_2 nisu susjedni. Taj susjed ne mogu biti ni ostali w_j zbog svojstva C_4, a iz istog razloga ne može biti ni jedan od vrhova z_j, $j \geq 2$.

Time smo iscrpili sve mogućnosti za zajedničkog susjeda od z_1 i w_2, pa taj slučaj ne može nastupiti i zato zaključujemo da je doista $d(u) = k$, za sve $u \in V$, gdje je $2 \leq k \leq n - 1$.

Pogledamo li opet sliku b), vidimo da svaki w_i ima točno $k - 2$ susjeda izvan $\{w_1, \ldots, w_k\}$ i svi su ti vrhovi zbog svojstva C_4 međusobno različiti. To su i svi preostali vrhovi, jer svaki vrh z koji je izvan $\{u, w_1, \ldots, w_k\}$ ima zajedničkog susjeda s u. Stoga dobivamo $n = 1 + k + k(k-2) = k^2 - k + 1$ čime je tvrdnja 1. dokazana.

Dokaz tvrdnje 2. Ovdje ćemo rabiti neke standardne rezultate iz linearne algebre. Neka je $A = [a_{ij}]$ matrica susjedstva od G. Kako je iz dokaza Tvrdnje 1, $d(u) = k$, $\forall u$, slijedi da svaki redak iz A ima točno k jedinica, a iz uvjeta teorema, za svaka dva retka postoji točno jedan stupac gdje oni imaju obje jedinice. Na glavnoj dijagonali su same nule, i A je simetrična.

Neka je $A^2 = [a_{ij}^{(2)}]$ kvadrat matrice A. Tada je

$$a_{ii}^{(2)} = \sum_{r=1}^{n} a_{ir} a_{ri} = \text{ (zbog simetrije) } = \sum_{r=1}^{n} a_{ir}^2 = k,$$

jer u svakom retku od A imamo točno k jedinica. Ako je $i \neq j$, onda je

$$a_{ij}^{(2)} = \sum_{r=1}^{n} a_{ir} a_{rj} = \sum_{r=1}^{n} a_{ir} a_{jr} = 1,$$

jer u ovoj sumi "preživi" samo jedan sumand $1 \cdot 1$, zbog toga što za svaka dva retka postoji točno jedan stupac na kojem su obje jedinice. Dakle,

$$A^2 = \begin{bmatrix} k & 1 & \cdots & 1 \\ 1 & k & & 1 \\ \vdots & & \ddots & 1 \\ 1 & \cdots & 1 & k \end{bmatrix} = (k-1)I + J,$$

gdje je I jedinična matrica, a J se sastoji od samih jedinica. Lako je provjeriti da J ima svojstvene vrijednosti n (višestrukosti 1) i 0 (višestrukosti $n - 1$). Stoga A^2 ima svojstvene vrijednosti $k - 1 + n = k^2$ (višestrukosti 1) i $k - 1$ (višestrukosti $n - 1$). Kako je A simetrična, pa se stoga može dijagonalizirati, slijedi da A ima svojstvene vrijednosti k (višestrukosti 1) i $\pm\sqrt{k-1}$.

Neka je r svojstvenih vrijednosti jednako $\sqrt{k-1}$, a s svojstvenih vrijednosti $-\sqrt{k-1}$, pri čemu je $r + s = n - 1$. Suma svih svojstvenih vrijednosti od A je jednaka tragu $\mathrm{Tr}\, A = 0$, pa je

$$k + r\sqrt{k-1} - s\sqrt{k-1} = 0,$$

pa je posebno $r \neq s$ i

$$\sqrt{k-1} = \frac{k}{s-r}.$$

Stoga je $\sqrt{k-1}$ cijeli broj t (jer ako je za $m \in \mathbb{N}$, $\sqrt{m}$ racionalan, onda je i cijeli - dokažite to!), pa dobivamo

$$t(s-r) = k = t^2 + 1.$$

Odatle slijedi da t dijeli $t^2 + 1$ i budući da t dijeli t^2, slijedi da dijeli dva uzastopna broja, pa mora biti $t = 1$. Stoga je $k = 2$. Time je dokazana tvrdnja 2 i time teorem. □

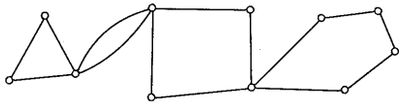
Ovaj lijep dokaz dali su P. Erdös, A. Rényi i V. Sós, 1966. godine. Teorem o prijateljstvu se može i ovako reformulirati.

Ako je G jednostavan graf ($n \geq 3$) tako da svaka dva vrha povezuje točno jedan put duljine 2, onda je jedini takav graf "vjetrenjača". No, ako putove duljine 2 zamijenimo putovima duljine $l > 2$, odgovor se općenito ne zna.

Kotzigova slutnja (1983.). *Neka je $l > 2$. Tada ne postoji graf sa svojstvom da se svaka dva vrha mogu povezati s točno jednim putom duljine l.*

Ako neki graf uopće ima ciklus, prirodno se nameće pitanje može li se na neki način i rastaviti na cikluse (i na dijelove bez ciklusa, tj. stabla).

Ciklički rastav grafa G je particija skupa bridova $E(G)$ na cikluse.



Očito, ako uopće imamo ciklički rastav grafa, onda svaki vrh mora biti parnog stupnja. Vrijedi i obratno.

PROPOZICIJA 6 (O. Veblen[7], 1912). *Graf dopušta rastav na cikluse ako i samo ako su mu svi vrhovi parnog stupnja.*

Dokaz. Ako, dakle, graf ima ciklički rastav, onda je svaki vrh incidentan s nula ili dva brida svakog od ciklusa, pa mu je stupanj paran.

Obratno, neprazan graf kojemu je svaki vrh parnog stupnja ima prema Propoziciji 3 (ii) bar jedan ciklus. Stoga podgraf dobiven odstranjivanjem bridova tog ciklusa također ima sve vrhove parnog stupnja. Sada dovoljnost lako slijedi indukcijom po $e(G)$. □

Graf koji nema ciklusa zove se **aciklički graf** ili **šuma**, a povezani aciklički graf **stablo** (ili **drvo**). Komponente povezanosti šume su stabla.

TEOREM 2 (karaterizacije stabla). *Neka je $G = (V, E)$ jednostavni graf. Tada su sljedeće tvrdnje ekvivalentne.*

(a) G je stablo;

(b) Jedinstvenost putova: za svaka dva vrha $x, y \in V$ postoji jedinstveni (x, y)-put u G;

(c) G je povezan, a za svako $e \in E(G)$, $G - e$ je nepovezan;

(d) G nema ciklusa, a dodavanjem bilo kojeg brida $e \in \binom{V}{2} \setminus E$, graf $G + e$ sadrži ciklus (tj. stablo je maksimalni graf bez ciklusa);

(e) $v(G) = e(G)+1$, odnosno **Eulerova karakteristika** $\chi(G) := v(G)-e(G)+1 = 2$.

Za dokaz teorema trebaju nam prvo dvije leme. Prva je o listovima (vrhovima stupnja 1), a druga o "rastu stabla".

LEMA 1 (o listovima). *Netrivijalno stablo T ima bar 2 lista.*

[7] Oswald Veblen (1880 – 1960), američki matematičar

Dokaz I. Neka je $P = v_0e_1v_1 \dots e_lv_l$ put u stablu T maksimalne duljine. Njegova je duljina barem 1, pa je $v_0 \neq v_l$. Tvrdimo da su v_0 i v_l listovi. Pretpostavimo npr. da v_0 nije list. Tada postoji brid $e = v_0v \neq e_1$. Ako $v \notin \{v_0, \dots, v_l\}$, onda se put P može produžiti bridom e, a ako je $v = v_i$, za neko $i \geq 2$, onda $[(v_0, v_i)$-dio od $P] + e$ čini ciklus. U oba slučaja dobivamo kontradikciju i lema je dokazana. □

Dokaz II leme o listovima. Neka je p_i broj vrhova od T stupnja $i \geq 1$. Znamo da je $e(T) = v(T) - 1$ (neovisno o Teoremu 2, vidi idući Primjer 21). Ako je $n = v(T)$, onda iz $2n-2 = \sum d(v) = \sum_{i=1}^{n-1} ip_i$ slijedi $p_1 - p_3 - 2p_4 - \dots - (n-3)p_{n-1} = 2$, a odatle $p_1 \geq 2$.

□

LEMA 2 (rast stabla). *Neka je G jednostavan graf, a $v \in V$ list. Tada su sljedeće dvije tvrdnje ekvivalentne:*

(i) G je stablo;

(ii) $G - v$ je stablo.

Dokaz. $(i) \Rightarrow (ii)$. Treba pokazati da $G - v$ nema ciklusa i da je povezan. Kako G nema ciklusa, očito je da ni $G-v$ nema ciklusa. Neka su x, y dva vrha iz $G-v$. Kako je G povezan, to postoji (x, y)-put u G. Taj put ne može sadržavati vrh stupnja 1 različit od x i y, pa ne sadrži v. Zato je sadržan u $G - v$, pa je $G - v$ povezan.

$(ii) \Rightarrow (i)$. Neka je $G - v$ stablo. Vraćanjem lista v natrag ne možemo stvoriti ciklus, jer inače v ne bi bio list. Da je G povezan, također je skoro očito. Ako su $x, y \in V(G)$ oba različita od v, onda su oni povezani putom već u $G-v$, a ako je npr. $y = v$, onda (x, v)-put dobijemo tako da do (jedinog) susjeda v' od v konstruiramo (x, v')-put u $G - v$ i tome dodamo brid $v'v$. □

Ovo nam omogućava da dano stablo reduciramo na sve manje i manje stablo otkidajući redom listove. I obrnuto, počevši od jednog vrha, dodavajući brid po brid tako da je drugi kraj list, dobivamo stabla, tj. tako "raste stablo".

Dokaz Teorema 2. Dokazat ćemo da je $(a) \iff (b), (c), (d), (e)$. Dokaz ćemo provesti indukcijom po broju vrhova $v(G)$. Ako je $v(G) = 1$, sve tvrdnje su očito točne, pa u tom slučaju teorem vrijedi. Dokažimo prvo da (a) povlači ostale tvrdnje $(b), (c), (d), (e)$. Neka je G stablo s bar dva vrha i neka je v jedan od listova (koji postoji po Lemi 1), a v' njegov jedini susjed. Pretpostavimo da $G - v$ zadovoljava $(b), (c), (d), (e)$. Tada je po Lemi 2 $G - v$ stablo i gotovo je očito da zadovoljava $(b), (c), (e)$ (detalje prepuštamo čitatelju). Pokažimo samo da $(a) \Rightarrow (d)$. Kako je G povezan, svaka dva vrha $x, y \in V(G)$ mogu se povezati putom P. Ako $xy \notin E(G)$, onda je $P + e$ ciklus.

Sada dokažimo da $(b), (c), (d), (e) \Rightarrow (a)$. U (b) i (c) već pretpostavljamo povezanost. Pokažimo da grafovi iz (b) i (c) ne sadrže ciklus. Graf iz (b) nema ciklusa, jer su dva vrha iz ciklusa povezana dvama različitim putovima, a onaj iz (c) nema ciklusa, jer bi inače odstranjivanjem brida iz ciklusa dobili povezan graf. Tako smo već dokazali ekvivalenciju $(a), (b)$ i (c).

Dokažimo sad $(d) \Rightarrow (a)$. Dovoljno je dokazati da je G povezan. Samo ćemo obrnuti zaključivanje iz dokaza $(a) \Rightarrow (d)$. Neka su $x, y \in V(G)$ dva vrha. Tada su oni ili povezani bridom $e = xy$, a ako nisu, onda graf $G+e$ sadrži ciklus. Uklanjanje brida e iz tog ciklusa daje (x,y)-put u G.

Konačno dokažimo da $(e) \Rightarrow (a)$. To ćemo dokazati indukcijom po $v(G)$. Neka je G povezani graf za koji je $v(G) = e(G) + 1 \geq 2$. Tada iz Propozicije 1 slijedi da je zbroj stupnjeva svih vrhova od G jednak $2v(G) - 2$. Vrhova ima $v(G)$, pa slijedi da ne mogu svi stupnjevi biti ≥ 2. Kako je G povezan, bar jedan od stupnjeva mora biti 1, tj. G ima list v. Graf $G' = G - v$ je opet povezan i zadovoljava $v(G') = e(G') + 1$. Po pretpostavci indukcije, G' je stablo, pa je po Lemi 2 i G stablo. □

Primjer 21. Dokažite bijektivno tvrdnju (e) iz Teorema 2, tj. da za stabla T vrijedi

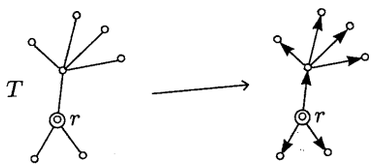
$$|E(T)| = |V(T)| - 1.$$

Rješenje. Prvo se podsjetimo da je **korijen stabla** bilo koji čvrsto odabrani vrh. Dalje, **orijentacija brida** je "stavljanje strelica" na svaki brid. Točnije, ako je $e = \{u, v\}$ neki brid, onda on izborom uređenog para (u, v) postaje orijentirani brid $\vec{e} = (u, v)$ s početkom u i krajem v (vidi Usmjereni grafovi ili digrafovi u §2.).

Sada je ideja sljedeća. Neka je T stablo, a $r \in V(T)$ korijen. Orijentirajmo svaki brid iz T tako da "ne gleda korijen" (tj. tako da mu kraj bude dalje od korijena nego početak). To onda daje očitu bijekciju (dokažite je i formalno):

$$\{\text{bridovi od } T\} \longrightarrow \{\text{ne korijeni od } T\}$$

Na primjer:



Ovako orijentirano stablo katkad se zove **stabljika** (engl. *arborescence*). □

KOROLAR 3. *Za svaku je šumu G*

$$e(G) - v(G) + c(G) = 0.$$

Dokaz. Šuma je disjunktna unija od konačno mnogo stabala. Ako je $c(G) = 1$, onda je G stablo, pa se ta formula svodi na $v(G) = e(G) + 1$, koja za stablo vrijedi zbog Teorema 2 (e). Još jedanput uporabom te činjenice induktivno po $c(G)$ zaključujemo da ona vrijedi općenito. □

KOROLAR 4. *Ako za graf G vrijedi $e(G) \geq v(G)$, onda G sadrži ciklus.*

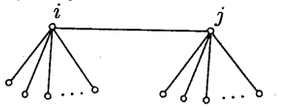
Dokaz. Kad bi G bio acikličan, onda bi iz Korolara 3, $e(G) \geq v(G)$ i činjenice $c(G) \geq 1$ slijedilo $0 \leq e(G) - v(G) = -c(G) \leq -1$, kontradikcija. □

Korolar 4 je vrlo jednostavan primjer rezultata koji pripada u tzv. *ekstremalnu teoriju grafova*. Korolar 4, naime, tvrdi da svaki graf na n vrhova i dovoljno mnogo bridova (barem n) sadrži ciklus. Donja granica za broj bridova je i najbolja moguća, jer postoje grafovi s n vrhova i $n-1$ bridova koji nemaju ciklusa (to su stabla). U tom su smislu stabla *ekstremalni grafovi* za svojstvo sadržavanja ciklusa. Na ekstremalnu teoriju grafova ćemo se vratiti u §8.

Grafovi s n vrhova i barem n bridova, prema tome, uvijek sadrže ciklus. Duljina tog ciklusa može biti bilo koji broj između 1 i n. Sljedeći teorem, međutim, pokazuje koliko najmanje bridova treba imati (jednostavni) graf da bi sigurno sadržavao trokut $C_3 (= K_3)$.

TEOREM 3 (W. Mantel, 1907.). *Neka je $G = (V, E)$ jednostavni graf s n vrhova i m bridova. Ako je $m > n^2/4$, G sadrži trokut. Jednakost vrijedi samo za n paran i $G = K_{n/2,n/2}$ (to je ovdje "ekstremalni graf").*

Dokaz. Dokažimo da ako G nema trokuta da je $m \leq n^2/4$. Uzmimo (jednostavnosti radi) da je $V = \{1, \ldots, n\}$, i neka je $d_i = d_G(i)$. Tada je $\sum_{i=1}^{n} d_i = 2m$. Neka je $ij \in E$ bilo koji brid. Kako G nema trokuta, slijedi da je $d_i + d_j \leq n$, jer su skupovi susjeda vrhova i, j disjunktni.



Zbrajanjem tih nejednakosti dobivamo

$$\sum_{ij \in E} (d_i + d_j) \leq n \cdot m.$$

U ovoj se sumi d_i pojavljuje točno d_i puta, pa dobivamo da je

$$n \cdot m \geq \sum_{ij \in E} (d_i + d_j) = \sum_{i \in V} d_i^2 .$$

Sada za brojeve $d_1, \ldots, d_n$ uporabimo kvadratno-aritmetičku nejednakost

$$\frac{1}{n} \sum_{i=1}^{n} d_i^2 \geq \left(\frac{1}{n} \sum_{i=1}^{n} d_i \right)^2 ,$$

pa slijedi

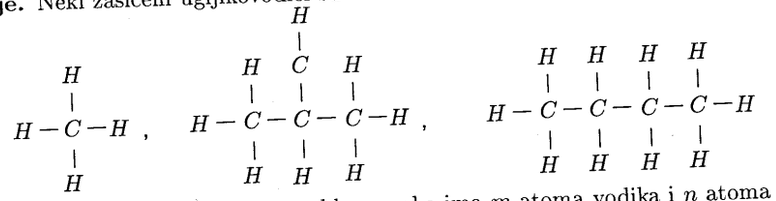
$$mn \geq \sum_{i \in V} d_i^2 \geq \frac{1}{n} \left(\sum_{i \in V} d_i \right)^2 = \frac{1}{n} 4m^2,$$

odakle dobivamo $m \leq n^2/4$. U slučaju jednakosti je $d_i = d_j$, za sve i, j, pa je $d_i = n/2$ (zbog $d_i + d_j = n$), a odavde, jer nema trokuta, da je $G = K_{n/2,n/2}$. □

Ovaj je teorem poseban slučaj Turanovog teorema (v. Teorem 28. u §8).

Primjer 22 (iz kemije). Zasićeni ugljikovodik je molekula oblika C_mH_n, a svaki atom ugljika C ima 4 kemijske veze (ili valenciju 4), a svaki atom vodika H jednu vezu. Te veze ne tvore cikluse. Dokažite da zasićeni ugljikovodik C_mH_n može postojati samo u slučaju $n = 2m + 2$.

Rješenje. Neki zasićeni ugljikovodici su

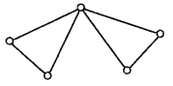


Graf zasićenih ugljikovodika je stablo, pa ako ima m atoma vodika i n atoma ugljika, onda prema Teoremu 2 (e) ima $m + n - 1$ bridova. Iz Propozicije 1 slijedi da je $4m + n = 2(m + n - 1) \Rightarrow n = 2m + 2$. □

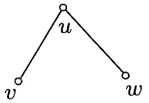
Primjer 23. Neka je G jednostavan graf $G = (V, E)$ s n vrhova bez 4-ciklusa $C_4 (\approx K_{2,2})$. Dokažite da je tada

$$|E| \leq \frac{n}{4}(1 + \sqrt{4n - 3}).$$

Rješenje. Kao primjer grafa s $n = 5$ vrhova bez C_4 je "vjetrenjača"



i to je jedini graf s 5 vrhova i 6 bridova bez C_4. Neka je G s n vrhova i m bridova bez C_4. Promotrimo skup S svih parova oblika $(u, \{v, w\}) \in V \times \binom{V}{2}$, takvih da je $v \sim u \sim w$, $v \neq w$. Drugim riječima, S je skup svih podgrafova oblika



Sumiranjem po svim u nalazimo da je $|S| = \sum_{u \in V} \binom{d(u)}{2}$. S druge strane, svaki par $\{v, w\}$ ima zbog uvjeta na C_4 najviše jednog zajedničkog susjeda. Zato je $|S| \leq \binom{n}{2}$. Stoga je

$$\sum_{u \in V} \binom{d(u)}{2} \leq \binom{n}{2},$$

odnosno

$$\sum_{u \in V} d(u)^2 \leq n(n-1) + \sum_{u \in V} d(u).$$

Opet iz aritmetičko-kvadratne nejednakosti (ili Cauchy-Schwarzove nejednakosti za brojeve $(d(u_1), \ldots, d(u_n))$ i $(1, 1, \ldots, 1)$) je

$$\left(\sum_{u \in V} d(u)\right)^2 \leq n \sum_{u \in V} d(u)^2,$$

pa slijedi

$$\left(\sum_{u \in V} d(u)\right)^2 \leq n^2(n-1) + n \sum_{u \in V} d(u),$$

odnosno

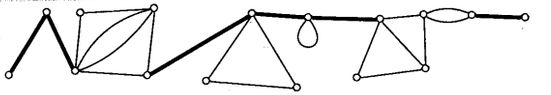
$$4|E|^2 - 2n|E| - n^2(n-1) \leq 0.$$

Rješavanjem ove kvadratne nejednadžbe slijedi tvrdnja.

Ako je X 3-dimenzionalni vektorski prostor nad poljem $\mathbb{Z}_p$ (p prost broj), neka je $0 \neq x \in X$, a $[x]$ 1-potprostor od X određen vektorom x. Graf G neka ima vrhove $[x]$, a $[x] \sim [y]$ u $G \iff x \cdot y = 0$ (tj. $x_1y_1 + x_2y_2 + x_3y_3 = 0$, gdje je $x = (x_1, x_2, x_3)$, $y = (y_1, y_2, y_3)$). Pokazuje se da je $v(G) = n = p^2 + p + 1$, $e(G) = (n-1)(1 + \sqrt{4n-3})/4$, dakle, tu se (zamalo) postiže jednakost. □

Rezni bridovi i vrhovi

Rezni brid grafa G je brid $e \in E(G)$ za koji je $c(G - e) > c(G)$, tj. čijim se izbacivanjem graf raspada na više komponenti povezanosti. Na primjer, na donjoj su slici debelo izvučeni rezni bridovi.



PROPOZICIJA 7. *Brid $e \in E(G)$ je rezni ako i samo ako nije brid ciklusa iz G.*

Dokaz. $\Rightarrow$: Ako je e rezni brid, onda je $c(G-e) > c(G)$, pa postoje vrhovi $u, v \in V$ koji su povezani putom u G, ali ne u $G - e$. Stoga postoji (u, v)-put P u G koji prolazi bridom e. Neka su x, y krajevi od e tako da x prethodi vrhu y na putu P. Vrh u je u $G - e$ povezan s x dijelom puta P, a y je u $G - e$ povezan s v dijelom od P. Kad bi e bilo u ciklusu C, onda bi x i y bili povezani u $G - e$ putom $C - e$, pa bi u i v bili povezani u $G - e$, što je kontradikcija.

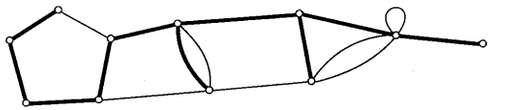
$\Leftarrow$: Neka e nije u ciklusu i pretpostavimo da $e = xy$ nije rezni brid u G. Tada je $c(G - e) = c(G)$. x i y su u istoj komponenti jer su povezani bridom $e = xy$. Stoga su x i y u istoj komponenti od $G - e$, pa postoji (x, y)-put P u $G - e$. No, tada je e u ciklusu $P + e$ od G, što je kontradikcija. □

KOROLAR 5. *Povezani graf G je stablo ako i samo ako je svaki brid u G rezni.*

Dokaz. $\Rightarrow$: Ako je G stablo i $e \in E(G)$, onda zbog acikličnosti od G, e nije sadržan u ciklusu, pa je prema Propoziciji 7, e rezni brid u G.

$\Leftarrow$: Pretpostavimo da je G povezan, ali da nije stablo. Tada G sadrži ciklus C. Prema Propoziciji 7, nijedan brid od C ne može biti rezni brid od G, što je kontradikcija s pretpostavkom. □

Razapinjuće stablo (ili **kičma**) grafa G je razapinjući podgraf (tj. sadrži sve vrhove) koji je stablo. Na donjoj slici je debelo izvučeno razapinjuće stablo (kičma):



KOROLAR 6. *Svaki povezani graf ima razapinjuće stablo. Stoga svaki graf ima razapinjuću šumu.*

Dokaz. Neka je G povezan graf. Promotrimo skup svih povezanih razapinjućih podgrafova od G. Taj je skup neprazan jer npr. sadrži G. Neka je T minimalni element tog skupa s obzirom na inkluziju. Tada je $c(T) = 1$, a $c(T - e) > 1$, $\forall e \in E(T)$. Stoga je svaki brid od T rezni brid od T, pa kako je T povezan, iz Korolara 5 slijedi da je T stablo. □

KOROLAR 7. *Ako je G povezan graf, onda je $e(G) \geq v(G) - 1$.*

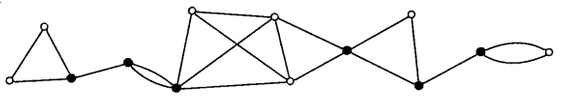
Dokaz. Ako je G povezan, onda zbog Korolara 6 sadrži razapinjuće stablo T, pa iz Teorema 2 (e) slijedi $e(G) \geq e(T) = v(T) - 1 = v(G) - 1$. □

PROPOZICIJA 8. *Neka je T razapinjuće stablo povezanog grafa G, a $e \in E(G) \setminus E(T)$. Tada $T + e$ sadrži jedinstveni ciklus.*

Dokaz. Kako je T aciklički, svaki ciklus od $T + e$ sadrži e. Nadalje, C je ciklus od $T + e$ ako i samo ako je $C - e$ put u T koji spaja krajeve od e. Prema Teoremu 2 (b), T ima jedinstveni takav put. Stoga $T + e$ sadrži jedinstveni ciklus. □

Za podskupove $S, S' \subseteq V(G)$ označimo sa $[S, S']$ skup svih bridova od G s jednim krajem u S, a drugim u S'. **Bridni rez** od G je podskup od $E(G)$ koji je oblika $[S, \bar{S}]$, gdje je $\emptyset \neq S \subseteq V$, $\bar{S} = V \setminus S$. Minimalni neprazni bridni rez od G zove se **vez** (engl. *bond*). Svaki rezni brid e daje rez $\{e\}$. Ako je G povezan, onda je rez B od G minimalni podskup od $E(G)$ tako da je $G - B$ nepovezan.

Analogno reznom bridu, definiramo da je vrh v **rezni vrh** grafa ako se skup bridova E može particionirati u dva skupa E_1 i E_2 tako da je $G[E_1] \cap G[E_2] = \{v\}$. Ako je G bez petlji i netrivijalan (tj. $v(G) \geq 2$), onda je v vezni vrh od G ako i samo ako je $c(G - v) > c(G)$. Na primjer, na donjoj su slici rezni vrhovi podebljani



PROPOZICIJA 9. *Vrh v stabla G je rezni ako i samo ako je $d(v) > 1$.*

Dokaz. Ako je $d(v) = 0$, G je točka, pa v nije rezni vrh. Ako je $d(v) = 1$, $G - v$ je aciklički graf s $v(G - v) - 1$ bridova, pa je prema Teoremu 2 (e) $G - v$ stablo. Stoga je $c(G - v) = 1 = c(G)$, pa v nije rezni vrh od G.

Ako je $d(v) > 1$, onda postoje susjedni vrhovi $u \neq w$ od v i zbog Teorema 2 (b) put uvw je jedinstven (u, w)-put. Stoga ne postoji (u, w)-put u $G - v$, pa je $c(G - v) > 1 = c(G)$. Stoga je v rezni vrh u G. □

KOROLAR 8. *Povezan (netrivijalan) graf G bez petlji ima bar dva vrha koji nisu rezni.*

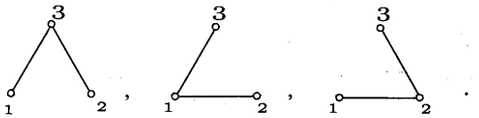
Dokaz. Prema Korolaru 6, G ima razapinjuće stablo T. Prema Lemi 1 i Propoziciji 9, T ima bar dva vrha u, v koji nisu rezni vrhovi od T. Dokažimo da oni nisu rezni vrhovi od G. T je razapinjući podgraf od G, pa je $T - u$ razapinjući podgraf od $G - u$ i $c(G - u) \leq c(T - u) = 1$ povlači $c(G - u) = 1$. Zato u nije rezni vrh od G. Slično i v. □

Općenitiji pojam je **vršni rez**, tj. podskup $S \subseteq V(G)$, tako da je $G - S$ nepovezan. Na taj ćemo se pojam vratiti poslije.

Broj razapinjućih stabala

Neka je $T(G)$ broj svih razapinjućih stabala povezanog grafa G. Određivanje broja razapinjućih stabala grafa (i pripadna teorija) ima raznih teorijskih i praktičnih primjena, a takvi su problemi prvo razmatrani u elektrotehnici. Ako je graf G električno kolo, pri čemu su bridovi žice (jediničnog otpora) koje se sastaju u vrhovima, onda je otpor između vrhova x, y koji su spojeni bridom jednak omjeru broja razapinjućih stabala koji sadrže brid xy i ukupnog broja $T(G)$ razapinjućih stabala od G. Ovo nije od prevelike važnosti u elektrotehnici, jer rijetko su svi otpori jednaki, no određene modifikacije s težinama na bridovima za praksu su važnije.

Pogledajmo neke primjere. Broj $T(K_3) = 3$, jer su sva razapinjuća stabla grafa K_3 sa skupom vrhova $\{1, 2, 3\}$:



Dakle, $T(G)$ broji sva moguća razapinjuća stabla, a ne samo neizomorfna. Npr. K_6 ima samo 6 neizomorfnih razapinjućih stabala, a kao što ćemo pokazati $6^4 = 1296$ različitih razapinjućih stabala od K_6.

Opća rekurzija za $T(G)$ dana je sljedećom Propozicijom.

PROPOZICIJA 10. *Neka je e karika (tj. nije petlja) u grafu G. Tada je*

$$T(G) = T(G - e) + T(G/e).$$

(Pritom je, podsjetimo, G/e graf dobiven iz G kontrakcijom brida e.)

Dokaz. Prvo je očito da je $v(G/e) = v(G) - 1$, $e(G/e) = e(G) - 1$ i $c(G/e) = c(G)$. Stoga, ako je T stablo, onda je $|V(T/e)| = |E(T/e)| + 1$, pa je (Teorem 2 (e)) i T/e stablo.

Neka je T razapinjuće stablo povezanog grafa G. Ako $e \notin E(T)$, onda je T razapinjuće stablo od $G - e$. Obratno, svako razapinjuće stablo od $G - e$ očito je i razapinjuće stablo od G koje ne sadrži e. Stoga je $T(G - e)$ broj razapinjućih stabala od G koja ne sadrže e. Ako je T razapinjuće stablo od G koje sadrži e, onda njemu odgovara razapinjuće stablo T/e od G/e. Lako je provjeriti da je to pridruživanje bijekcija (uvjerite se u to i popratite dokaz konkretnim primjerom, npr. $G = K_4$). □

Ova je rekurzija prilično nezgrapna za velike grafove, no osnovno pitanje koliko je $T(K_n)$ davno je razriješeno i jedan je od najljepših i najjednostavnijih netrivijalnih rezultata u kombinatorici.

TEOREM 4 (A. Cayley, 1889.). *Broj $T(K_n)$ razapinjućih stabala od K_n, tj. broj stabala na skupu vrhova $\{1, 2, \ldots, n\}$ jednak je n^{n-2}.*

nogo dokaza ovog teorema, ali nijedan nije doslovce izravan. tvari, već i izveli pomoću funkcija izvodnica (pokušajte to ati nekoliko dokaza ilustrirajući pritom razne nove tehnike tata.

stupnjeva.) Prvo dokažimo sljedeću Lemu.

MA 3. *Ako je* $d = (d_1, d_2, \ldots, d_n) \in \mathbb{N}^n$, *tako da je* $\sum_{i=1}^n d_i = 2n-2$, *onda je broj razapinjućih stabala od* K_n *u kojima vrh* i *ima stupanj* d_i, $i = 1, \ldots, n$ *jednak*

$$\frac{(n-2)!}{(d_1-1)!\ldots(d_n-1)!}.$$

Dokaz Leme. Indukcijom po n. Za $n = 1, 2$ Lema je trivijalna. Kako je $\sum_{i=1}^n =$ $2n-2 < 2n$, postoji $i \in [n]$ tako da je $d_i = 1$. Možemo pretpostaviti da je $d_n = 1$ i neka je vrh j jedini susjed od n, za neko $j \in [n-1]$. Otkidanje lista n rezultira novim stablom na vrhovima $1, 2, \ldots, n-1$ s nizom stupnjeva (redom) $d' = (d_1, \ldots, d_{j-1}, d_j - 1, d_{j+1}, \ldots d_{n-1})$. Obratno, ako imamo stablo na vrhovima $1, 2, \ldots, n-1$ s nizom stupnjeva d', onda spajanjem vrha j s vrhom n dobijemo stablo na vrhovima $1, 2, \ldots, n$ s nizom stupnjeva d. Prema pretpostavci indukcije, broj stabala na $1, 2, \ldots, n-1$ s nizom stupnjeva (redom) d' jednak je

$$\frac{(n-3)!}{(d_1-1)!\ldots(d_{j-1})!(d_j-2)!(d_{j+1}-1)!\ldots(d_{n-1}-1)!} = \frac{(d_j-1)(n-3)!}{(d_1-1)!\ldots(d_n-1)!},$$

jer smo uzeli da je $d_n = 1$.

Primijetimo da je to točno i za $d_j = 1$, jer je tada to 0. Stoga je ukupni broj stabala na $1, \ldots, n$ sa stupnjevima $d_1, \ldots, d_n$ jednak (jer j može biti $1, \ldots, n-1$):

$$\sum_{j=1}^{n} \frac{(d_j-1)(n-3)!}{(d_1-1)!\ldots(d_n-1)!} = \left(\sum_{j=1}^{n-1}(d_j-1)\right) \frac{(n-3)!}{(d_1-1)!\ldots(d_n-1)!} =$$

$$(n-2) \cdot \frac{(n-3)!}{(d_1-1)!\ldots(d_n-1)!} = \frac{(n-2)!}{(d_1-1)!\ldots(d_n-1)!}.$$

□

Ukupni broj $T(K_n)$ razapinjućih stabala jednak je (rabeći multinomni teorem):

$$\sum_{\substack{d_1,\ldots,d_n \geq 1 \\ d_1+\ldots+d_n = 2n-2}} \frac{(n-2)!}{(d_1-1)!\ldots(d_n-1)!} = \sum_{\substack{k_1,\ldots,k_n \geq 0 \\ k_1+\ldots+k_n = n-2}} \frac{(n-2)!}{k_1!\ldots k_n!} =$$

$$= \underbrace{(1+1+\cdots+1)}_{n}{}^{n-2} = n^{n-2}.$$

□

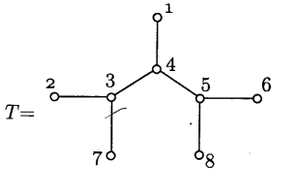
Dokaz 2. (Bijekcija - Prüferov kôd.) Uspostavit ćemo sljedeću bijekciju

$$\left\{ \begin{array}{c} \text{stabla sa skupom} \\ \text{vrhova } [n] \end{array} \right\} \longrightarrow \left\{ \begin{array}{c} \text{nizovi iz } [n] \\ \text{duljine } n-2 \end{array} \right\}$$

$$T \mapsto t = (t_1, t_2, \ldots, t_{n-2}).$$

Kako desni skup očito ima n^{n-2} elemenata, slijedit će da je $T(K_n) = n^{n-2}$. Pokazat ćemo, dakle, da svako stablo s vrhovima $1, 2, \ldots, n$ možemo kodirati ili dekodirati s nizom od $n-2$ broja iz $[n] = \{1, 2, \ldots, n\}$, kako je to učinio H. Prüfer 1918. godine.

Dakle, neka je T neko stablo sa skupom vrhova $[n]$ (koji smatramo uređenim na prirodani način). Prema Lemi 1, svako stablo (osim trivijalnog) ima bar dva lista. Osnovna ideja ovog dokaza je da na sustavan način "otkidamo" listove sve dok ne otkinemo sve osim posljednjeg lista i promotrimo učinak tog vandalizma. Neka je s_1 prvi list (u prirodnom poretku od $[n]$) stabla T, a t_1 oznaka jedinog susjeda od s_1. Otkinimo s_1, promotrimo stablo $T - s_1$ i na njemu ponovimo isto, tj. neka je s_2 prvi list u $T - s_1$, a t_2 oznaka njegova jedinog susjeda itd. sve do t_{n-2}. Evo primjera za $n = 8$.



$\mapsto (4, 3, 5, 3, 4, 5)$

Očito je da su različitim stablima pridruženi različiti nizovi. Sada rekonstruirajmo (dekodirajmo) stablo T iz zadanog niza $t = (t_1, \ldots, t_{n-2})$. Prvo uočimo da se u gornjoj konstrukciji vrh $i \in V(T)$ u nizu $t = (t_1, \ldots, t_{n-2})$ pojavljuje točno $d_T(i) - 1$ puta[8]. Stoga su listovi u T točno oni koji se ne pojavljuju u nizu t.

Neka je $t = (t_1, \ldots, t_{n-2})$ niz brojeva iz $[n]$. Neka je s_1 prvi vrh iz $[n]$ koji nije u $(t_1, \ldots, t_{n-2})$. Spojimo bridom s_1 i t_1. Dalje, neka je s_2 prvi vrh iz $[n] \setminus \{s_1\}$ koji nije u $(t_2, \ldots, t_{n-2})$. Spojimo s_2 i t_2 itd., sve dok ne konstruiramo $n-2$ bridova $s_1t_1, s_2, t_2, \ldots, s_{n-2}t_{n-2}$. Konačno, T dobivamo spajanjem dvaju preostalih vrhova iz $[n] \setminus \{s_1, \ldots, s_{n-2}\}$. □

Dokaz 3. (Bijekcija - A. Joyal, 1981.) Promatrat ćemo ne samo stabla T iz $[n]$, nego stabla zajedno s dvama uočenim vrhovima koja ćemo nazvati *lijevi kraj* ○ i *desni kraj* □ (koji se mogu i podudarati). Neka je $\mathcal{T}_n = \{(T, ○, □) | T$ stablo na $[n]$, ○, □ vrhovi od $T\}$.

Jasno je da je $|\mathcal{T}_n| = n^2 T(K_n)$. Treba, dakle, samo dokazati da je $|\mathcal{T}_n| = n^n$. To ćemo dokazati konstrukcijom bijekcije sa skupa svih funkcija $[n]^{[n]}$ na $\mathcal{T}_n$.

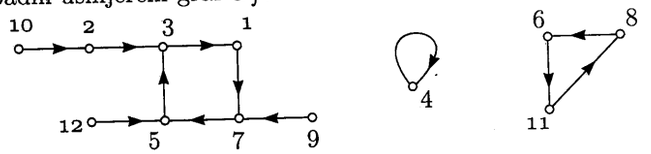
Neka je $f : [n] \to [n]$ bilo koja funkcija. Funkciju f ćemo reprezentirati usmjerenim grafom $\vec{G}_f$ čiji su vrhovi $1, 2, \ldots n$, a lukovi od i prema $f(i)$, $i \in [n]$.

[8] Naime, ako je m_i broj pojavljivanja vrha i u nizu t, onda je jasno $d_T(i) \geq m_i + 1$, a zbog $\sum_i m_i = n-2$ i $\sum_i (d_T(i) - 1) = 2(n-1) - n = n-2$ slijedi da mora vrijediti jednakost, za svaki i.

Kao primjer, neka je $n = 12$, a funkcija

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 7 & 3 & 1 & 4 & 3 & 11 & 5 & 6 & 7 & 2 & 8 & 5 \end{pmatrix}.$$

Tada je pripadni usmjereni graf $\vec{G}_f$:



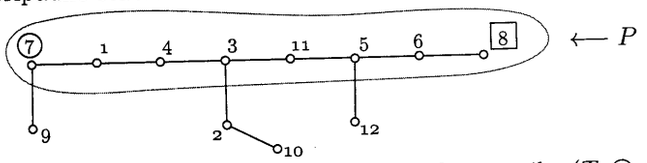
Pogledajmo komponente od $\vec{G}_f$. Kako iz svakog vrha izlazi točno jedna "strelica", slijedi da svaka komponenta ima jednako mnogo vrhova i bridova, pa zato svaka komponenta sadrži točno jedan usmjereni ciklus. Neka je $C \subseteq [n]$ unija vrhova tih ciklusa. Ako malo razmislimo, vidimo da je C jedinstveno određeni maksimalni podskup od $[n]$ takav da restrikcija $f|_C$ djeluje kao bijekcija $C \to C$. Pišimo $f|_C = \begin{pmatrix} a & b & \dots & z \\ f(a) & f(b) & \dots & f(z) \end{pmatrix}$ tako da su brojevi $a, b, \dots, z$ napisani u prirodnom poretku, čime dobivamo poredak $f(a), f(b), \dots, f(z)$ u drugom retku, tj. poredak elemenata od C. $f(a)$ će biti lijevi, a $f(z)$ desni kraj.

Stablo T koje odgovara funkciji f konstruiramo ovako. Nacrtamo $f(a), f(b), \dots, f(z)$ u tom poretku kao put P od $f(a)$ do $f(z)$, a ostatak ispunimo kao u $\vec{G}_f$ (izostavljajući strelice).

U našem primjeru $C = \{1, 3, 4, 5, 6, 7, 8, 11\}$, a

$$f|_C = \begin{pmatrix} 1 & 3 & 4 & 5 & 6 & 7 & 8 & 11 \\ 7 & 1 & 4 & 3 & 11 & 5 & 6 & 8 \end{pmatrix},$$

pa stoga pripadno stablo T:



Ovo se pridruživanje lako i obrne. Ako je zadana trojka $(T, \bigcirc, \square)$, prvo pogledamo jedinstveni put P od $\bigcirc$ do $\square$. To daje skup C i bijekciju $f|_C : C \to C$, tako da u donji red napišemo vrhove kako se pojavljuju u P, a onda iznad njih te iste vrhove u prirodnom poretku. Ostale vrijednosti $i \mapsto f(i)$ odredimo po jedinstvenim putovima od i do P. □

Dokaz 4. (Matrični teorem o stablima.) Dokazat ćemo poznati

Matrični teorem o stablima (Kirchoff). *Neka je G povezani graf bez petlji s n vrhova i m bridova, a M matrica incidencije od G. U svakom stupcu od M zamijenimo na bilo koji način jednu od dviju jedinica s -1 (to daje orijentaciju od G). Tako dobijemo matricu N i neka je $Q = NN^T$. (Q je simetrična matrica sa stupnjevima $d_i = d_G(i)$ na glavnoj dijagonali.) Tada je $T(G) = \det Q_{ii}$, za sve $i = 1, \dots, n$, gdje je Q_{ii} dobivena iz Q izbacivanjem i-tog retka i i-tog stupca.*

Ako je $G = K_n$, dobivamo

$$Q_{ii} = \begin{bmatrix} n-1 & -1 & \cdots & -1 \\ -1 & n-1 & \cdots & -1 \\ & & \ddots & \\ -1 & -1 & \cdots & n-1 \end{bmatrix}$$

i nije teško izračunati da je $\det Q_{ii} = n^{n-2}$.

Dokaz matričnog teorema o stablima. Podsjetimo se iz linearne algebre da Binet-Cauchyjev teorem kaže da ako je A $(r \times s)$-matrica, a B $(s \times r)$-matrica, $r \leq s$, onda je $\det(AB)$ jednako sumi produkata determinanata odgovarajućih $(r \times r)$-matrica, pri čemu "odgovarajući" znači da uzimamo iste indekse za r stupaca u A i r redaka u B (vidi Bilješku 4). Za našu matricu Q_{ii} to znači

$$\det Q_{ii} = \sum_C \det C \cdot \det C^T = \sum_C (\det C)^2,$$

gdje C ide po svim $(n-1) \times (n-1)$ podmatricama od $N \setminus \{i\text{-ti redak}\}$. $n-1$ stupaca od C odgovara podgrafu od G s $n-1$ bridova na n vrhova. Stoga samo treba dokazati da je

$$\det C = \begin{cases} \pm 1, & \text{ako ti bridovi čine stablo,} \\ 0, & \text{inače.} \end{cases}$$

Uzmimo prvo da $n-1$ bridova ne razapinju stablo. Tada postoji komponenta koja ne sadrži i. Odgovarajući retci tih komponenata u sumi daju 0, pa su oni linearno zavisni i stoga je $\det C = 0$.

Sada pretpostavimo da stupci od C razapinju stablo. Tada postoji vrh $j_1 \neq i$ stupnja 1 i neka je e_1 (jedini) incidentni brid s j_1. Uklonimo li j_1, e_1, dobivamo stablo s $n-2$ bridova. Opet postoji vrh $j_2 \neq i$ stupnja 1 incidentan samo s bridom e_2. Nastavimo tako sve do $j_1, j_2, \dots, j_{n-1}$ i $e_1, e_2, \dots, e_{n-1}$ s $j_i \in e_i$. Sada ispermutiramo retke i stupce tako da dovedemo j_k u k-ti redak, a e_k u k-ti stupac. Prema konstrukciji $j_k \notin e_l$ za $k < l$, pa je tako dobivena matrica C' donja trokutasta s elementima na glavnoj dijagonali ± 1. Stoga je $\det C = \pm \det C' = \pm 1$ i dokaz je gotov. □

Bilješka 4. Binet-Cauchyjeva formula za $(r \times s)$-matricu A i $B = A^T$, $r \leq s$, glasi:

$$\det(AA^T) = \sum_I (\det A_I)^2,$$

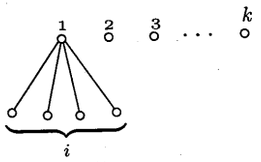
gdje se sumira po svim $I \in \binom{[s]}{r}$, a A_I je dobivena iz A izbacivanjem svih stupaca čiji indeks nije iz I.

Geometrijski to znači sljedeće. Ako retke iz A smatramo kao r vektore $\underline{a}_1, \ldots, \underline{a}_r$ u $\mathbb{R}^s$, onda oni razapinju paralelepiped P dimenzije r u $\mathbb{R}^s$, a $\det(AA^T)$ je kvadrat volumena od P. Odabir $(r \times r)$-podmatrice C od A je zapravo projekcija vektora $\underline{a}_1, \ldots, \underline{a}_r$ na neki r-dimenzionalni koordinatni potprostor od $\mathbb{R}^s$, a $\det(CC^T)$ je kvadrat volumena odgovarajuće projekcije od P.

Tako za $r = 2$, $s = 3$ dobivamo da za površinu $p(P)$ paralelograma P i njegove projekcije P_{xy}, P_{yz}, P_{zx} na koordinatne ravnine vrijedi $p(P)^2 = p(P_{xy})^2 + p(P_{yz})^2 + p(P_{zx})^2$, što je poopćeni **Pitagorin poučak**. Za $r = 1$, $s = 2$ dobivamo običan Pitagorin poučak.

□

Dokaz 5. (Rekurzija, J. Riordan, 1968.) Označimo s $T_n = T(K_n)$, a s $T_{n,k}$ broj (označenih) šuma na $[n]$ koje se sastoje od k stabala, tako da su vrhovi $1, 2, \ldots, k$ u različitim stablima. Očito je $T_{n,1} = T_n$. Neka je vrh 1 susjedan s i vrhova kao na slici.



Uklonimo li vrh 1, onda tih i vrhova zajedno s $2, 3, \ldots, k$ daju ukupno $T_{n-1,k-1+i}$ šuma. No ovih i vrhova možemo slobodno birati među $n - k$ vrhova različitih od $1, \ldots, k$. Stoga za $n \geq k \geq 1$ dobivamo

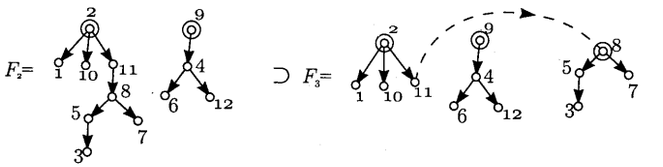
$$T_{n,k} = \sum_{i=0}^{n-k} \binom{n-k}{i} T_{n-1,k-1+i},$$

pri čemu je $T_{0,0} := 1$, $T_{n,0} = 0$, za $n > 0$. Odavde nije teško indukcijom i binomnom formulom dobiti (učinite to) da je

$$T_{n,k} = kn^{n-k-1}.$$

Posebno, $T_{n,1} = T_n = n^{n-2}$. □

Dokaz 6. (Dvostruko prebrojavanje, J. Pitman, 1999.) **Korijenska šuma** na $[n]$ je šuma s izborom korijena u svakom stablu. Neka je $\mathcal{F}_{n,k}$ skup svih korijenskih šuma na $[n]$ s točno k korijenskih stabala. Stoga je $\mathcal{F}_{n,1}$ skup svih korijenskih stabala i $|\mathcal{F}_{n,1}| = nT_n$, jer korijen može biti bilo koji od n vrhova. Orijentirajmo svaku šumu $F_{n,k} \in \mathcal{F}_{n,k}$ "od korijena", tj. tako da bridovi "ne gledaju svoj korijen" (usp. Primjer 21). Reći ćemo da šuma F *sadrži* šumu F' ako F sadrži F' kao usmjereni graf ($F \supseteq F'$). Očito, ako je $F \supset F'$, onda F ima manje komponenti nego F'. Na primjer, za $n = 12$ na slici $F_2 \supset F_3$ (crtkani luk zasad ignorirajte):



Sada dolazi ključna ideja. Reći ćemo da je niz $F_1, \ldots, F_k$ šuma *profinjujući niz* ako je $F_i \in \mathcal{F}_{n,i}$, te $F_i \supset F_{i+1}$, $\forall i$. Neka je $F_k \in \mathcal{F}_{n,k}$ čvrsta (zadana) šuma. Promotrimo sljedeće brojeve:

$$N(F_k) := \#\{ \text{ korijenskih stabala } \supseteq F_k\}$$
$$N^*(F_k) := \#\{ \text{ profinjujućih nizova koji završavaju s } F_k\}.$$

Prebrojit ćemo $N^*(F_k)$ na dva načina, prvo da počnemo sa stablom, a drugo da počnemo s F_k. Uzmimo prvo da $F_1 \in \mathcal{F}_{n,1}$ sadrži F_k. Budući da slobodno možemo otkidati $k-1$ bridova od $F_1 \setminus F_k$ na sve moguće načine da dobijemo profinjujući niz od F_1 do F_k, slijedi

$$N^*(F_k) = N(F_k)(k-1)! \tag{1}$$

S druge strane, da iz F_k dobijemo F_{k-1} treba dodati po jedan orijentirani brid iz svakog vrha v do svakog od $k-1$ korijena stabala koji ne sadrže v. Na gornjoj smo slici da dobijemo $F_3 \to F_2$ dodali brid $11 \to 8$ crtkano. Takvih izbora imamo $n(k-1)$. Slično, za F_{k-1} trebamo dodati usmjereni brid iz svakog vrha v do svakog od $k-2$ korijena koji ne sadrži v. Takvih izbora ima $n(k-2)$. Nastavimo li tako, dobijemo

$$N^*(F_k) = n^{k-1}(k-1)! \,. \tag{2}$$

Iz (1) i (2) slijedi

$$N(F_k) = n^{k-1}, \text{ za svako } F_k \in \mathcal{F}_{n,k} \,.$$

Posebno za $k = n$, F_n se sastoji od n izoliranih vrhova, pa je $N(F_n)$ broj svih korijenskih stabala i stoga $|\mathcal{F}_{n,1}| = n^{n-1}$, odakle slijedi Cayleyeva formula.

Iz ovog dokaza možemo dobiti i više. Formula (2) za $k = n$ daje

$$\#\{ \text{ profinjujućih nizova } (F_1, F_2, \ldots, F_n)\} = n^{n-1}(n-1)! \,. \tag{3}$$

Za $F_k \in \mathcal{F}_{n,k}$, neka je $N^{**}(F_k)$ broj onih profinjujućih nizova $F_1, \ldots, F_n$ čiji je k-ti član F_k. Taj je broj jednak $N^*(F_k)$ puta broj izbora $(F_{k+1}, \ldots, F_n)$. Ali taj potonji broj je $(n-k)!$, jer slobodno možemo ukloniti $(n-k)$ bridova od F_k na sve moguće načine, pa je

$$N^{**}(F_k) = N^*(F_k)(n-k)! = n^{k-1}(k-1)!(n-k)! \,. \tag{4}$$

Kako ovaj broj ne ovisi o izboru F_k, dijeljenje (3) s (4) daje broj korijenskih šuma na $[n]$ s k stabala:

$$|\mathcal{F}_{n,k}| = \frac{n^{n-1}(n-1)!}{n^{k-1}(k-1)!(n-k)!} = \binom{n-1}{k-1} n^{n-k} = \binom{n}{k} kn^{n-k-1} \,.$$

Budući da k korijena možemo odabrati na $\binom{n}{k}$ načina, odavde dobivamo da je broj $T_{n,k}$ iz dokaza 5 jednak $T_{n,k} = kn^{n-k-1}$. To smo dobili bez rekurzije i bez indukcije, nego samo inteligentnim prebrojavanjem. □

Potraga za stablima

Mnoge činjenice koje smo do sada dokazali (kao npr. Propozicija 3, Korolar 4, Teorem 3) samo tvrde da pod izvjesnim uvjetima postoje izvjesna stabla ili ciklusi. No, ono što je za praksu važno je kako naći te podgrafove. Jasno je da ćemo, barem u teoriji, iscrpnom potragom u konačnom grafu i konačnom vremenu, biti u stanju pronaći te podgrafove, ali za praksu to nije dovoljno, jer je tu bitno vrijeme. Za praksu su potrebni brzi, dobri ili efikasni algoritmi. Vrijeme izvršenja algoritma mjeri se ukupnim brojem osnovnih računskih operacija (aritmetičkih operacija, usporedbi itd.) potrebnih za njegovu provedbu i ovisi o veličini i prirodi ulaznih podataka. **Složenost algoritma u teoriji grafova** je vrijeme njegove provedbe u najgorem slučaju na grafovima dane veličine, a pod time se obično misli na broj vrhova i/ili broj bridova. **Polinomski algoritam** je onaj čija je složenost odozgo omeđena polinomom u veličini ulaznog grafa, a **eksponencijalni algoritam** onaj čija je složenost odozdo omeđena eksponencijalnom funkcijom u veličini ulaznog grafa. Polinomske algoritme smatramo efikasnima, jer vrijeme njihove provedbe raste relativno sporo s rastom ulaznih podataka (npr. grafovi s nekoliko tisuća vrhova mogu se efektivno procesuirati), dok eksponencijalni rade jako dugo već s malim grafovima (od nekoliko desetaka vrhova).

Potraga za razapinjućim stablima je posebno zanimljiv slučaj u pretraživanjima grafova i izvor mnogih polinomskih algoritama.

Traženo stablo (*engl. search tree*) u povezanom grafu s n vrhova je razapinjuće stablo čiji su skupovi vrhova $\{v_0, v_1, \ldots, v_{n-1}\}$ i bridova $\{e_1, e_2, \ldots, e_{n-1}\}$ uređeni tako da je v_0 korijen, a za svako j, $1 \leq j \leq n-1$, podgraf sa skupom vrhova $\{v_0, v_1, \ldots, v_j\}$ i skupom bridova $\{e_1, e_2, \ldots, e_j\}$ čini stablo. Drugim riječima, traženo stablo je proces rasta razapinjućeg stabla, a ne samo završno stablo. Počinjemo s korijenom v_0, a stablo raste tako da u svakom koraku dodamo vrh v_j i brid $e_j = v_i v_j$. Pri tome se v_j zove **sin** od v_i, a v_i **otac** od v_j. Općenito postoji sloboda u izboru od v_j i e_j, ali ako ih pažljivo odaberemo, na kraju nam traženo stablo može dati važne strukturne informacije o samom grafu. Takav je prvi dokumentirani algoritam dao Dijkstra 1959. Dijkstrina se metoda danas zove **breadth-first search tree**. To je traženo stablo s vrhovima $\{v_0, v_1, \ldots, v_{n-1}\}$ i bridovima $\{e_1, e_2, \ldots, e_{n-1}\}$, tako da su za svako j, $1 \leq j \leq n-1$, v_j i e_j odabrani tako da je otac od v_j vrh v_i s najmanjim mogućim indeksom i. Takvo stablo raste linearno s vremenom. Osnovno je svojstvo te metode da je udaljenost između korijena i svakog vrha u tome stablu ista kao i njihova udaljenost u samom grafu. Stoga se prilikom rasta tog stabla može naći i najkraći put među svim parovima vrhova u grafu, pa se tako npr. može odrediti i dijametar grafa. Također, tom se metodom lako pokazuje je li graf bipartitan ili nije i to uporabom Propozicije 5. On ili daje biparticiju (sve udaljenosti od korijena parne ili neparne) ili daje najkraći neparni ciklus.

Druga vrlo efikasna metoda se zove **depth-first search tree** koju je dao Tarjan 1972. To je traženo stablo s vrhovima $\{v_0, v_1, \ldots, v_{n-1}\}$ i bridovima $\{e_1, e_2, \ldots, e_{n-1}\}$, tako da su za svako j, $1 \leq j \leq n-1$, v_j i e_j odabrani tako da je otac od v_j vrh v_i s najvećim mogućim indeksom i. I ta metoda radi u linearnom vremenu, a ima mnogo važnih primjena, npr. u nalaženju reznih vrhova grafa itd.

U raznim nam primjenama često trebaju i dodatne strukture na grafu. Jedna od najprirodnijih je da se svakom bridu $e \in E(G)$ pridruži njegova **težina** $w(e)$. U primjenama to je često cijena konstrukcije, stvarna udaljenost među krajevima itd., ali i skup boja, prsten $\mathbb{Z}_m$ ili $\mathbb{Z}$ itd. Dakle, w je funkcija $w : E(G) \to A$, gdje je $A = \mathbb{R}$ ili $\mathbb{R}_+$ ili $\mathbb{Z}_m$ itd. Uređeni par (G, w) grafa G i težinske funkcije w zove se **težinski graf**.

Ako je $H \subseteq G$ podgraf, onda je **težina podgrafa** H definirana kao $w(H) := \sum_{e \in E(H)} w(e)$ (ako ta suma ima smisla). Obični graf G smatramo težinskim s težinom $w(e) = 1$, $\forall e \in E(G)$. Mnogi problemi optimizacije svode se na to da se u težinskom grafu nađe podgraf određenog tipa s najmanjom ili najvećom težinom. Tako npr. Dijkstrin algoritam pronalazi u težinskom grafu s težinama iz $\mathbb{R}_+$ putove najmanje težine (tj. u običnom grafu najkraće putove).

Mnogi se problemi mogu riješiti polinomskim algoritmima, no ima i mnogo osnovnih problema za koje se ne zna postoji li polinomski algoritam. Jedna od najvažnijih zadaća teorijskog računarstva upravo je u tome da se odredi koji su problemi rješivi u polinomskom vremenu (tj. s polinomskim algoritmom). S time su u vezi sljedeći pojmovi.

Problem odluke je pitanje koje ima samo odgovore "da" ili "ne". Svaki objekt na koje je upućeno pitanje zove se **instanca problema**. Problem odluke pripada **klasi P** (polinomska) ako postoji polinomski algoritam koji rješava svaku instanciju problema u polinomskom vremenu. Problem odluke pripada **klasi NP** (nedeterministički polinomski) ako za svaku danu instanciju problema čiji je odgovor "da" postoji certifikat koji to provjerava u polinomskom vrmenu i čija je duljina odozgo omeđena polinomom u veličini ulaza. Takav se certifikat zove **sažetak**. Odavde se dobiva da je $\mathbf{P} \subseteq \mathbf{NP}$, jer je polinomski algoritam sam po sebi sažeti certifikat. Tako, primjerice, problem je li graf bipartitan pripada u klasu **P**, pa stoga i **NP**. No, s druge strane, za problem ima li neki graf razapinjući ciklus, ne zna se postoji li polinomski algoritam ili taj problem pripada klasi **NP**, jer je pripadni certifikat sam razapinjući ciklus. Provjera da graf ne sadrži razapinjući ciklus je puno teži problem. Na zna se pripada li taj problem klasi **NP**.

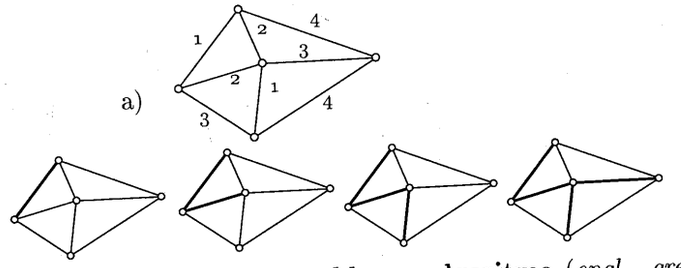
Kako smo rekli, $\mathbf{P} \subseteq \mathbf{NP}$. A je li $\mathbf{P} = \mathbf{NP}$ jedan je od temeljnih otvorenih problema teorijskog računarstva. Jedna potklasa od **NP** zove se **NP-potpuni** problemi. To su algoritamski najteži problemi u **NP** u smislu da ako se ijedan od njih može razriješiti u polinomskom vremenu, onda se i svaki problem iz **NP** može tako riješiti (pa je $\mathbf{P} = \mathbf{NP}$). Ima li graf razapinjući ciklus jedan je takav **NP**-potpun problem. Postoji i još šira klasa tzv. **NP-teških** problema, koji se u tom smislu čine gotovo beznadni. Svi ti pojmovi su formalno i precizno opisani u knjizi [77].

Ne upuštajući se u sve detalje, spomenimo jednostavni algoritam kojim se u danom povezanom težinskom grafu (G, w) nalazi minimalno razapinjuće stablo, tj. razapinjuće stablo T za koje je težina minimalna. Neka je $v(G) = n$.

Primov algoritam. Odaberi brid e minimalne težine u G i neka je $T := \{e\}$. Ponovi sljedeći korak sve dok T ima manje od $n-1$ bridova. Dodaj stablu T brid minimalne težine s jednim krajem u T, a drugim izvan T.

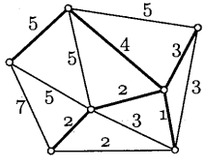
Nije teško vidjeti da taj algoritam završava s minimalnim razapinjućim stablom.

Evo malog primjera za težinski graf na slici a). Na slici b) je prikazan "rast stabla" primjenom Primovog algoritma.



Primov algoritam pripada u tzv. **pohlepne algoritme** (*engl. greedy algorithm*), jer pohlepnost "ne vidi dalje od nosa", pa u svakom koraku bira ono što je lokalno najbolje što može. Nije teško pokazati da je složenost Primovog algoritma reda $O(n^2)$. Sličan je i **Kruskalov algoritam** (iz 1956.). Prvo uredimo bridove $(e_1, \ldots, e_m)$ tako da je $w(e_1) \leq w(e_2) \leq \cdots \leq w(e_m)$. Tada redom konstruiramo skupove bridova $\emptyset = E_0 \subseteq E_1 \subseteq E_2 \subseteq \cdots \subseteq E$ pri čemu je $E_i = E_{i-1} \cup \{e_i\}$, ako u $E_{i-1} \cup \{e_i\}$ nema ciklusa, a $E_i = E_{i-1}$ inače. Algoritam završava ako je $|E_i| = n - 1$ ili je $i = m$. Ako je E_t mjesto gdje algoritam završava, onda je $T = (V, E_t)$ traženo minimalno razapinjuće stablo (pokušajte sami dokazati korektnost tog algoritma i njegovu složenost $O(n^2)$). Kruskalov (ili Primov) algoritam efikasno rješava "konkretan" **problem spajanja**: neke gradove treba povezati mrežom autocesta tako da ukupna gradnja bude najjeftinija, ako znamo cijene c_{ij} izgradnje između gradova i, j.

Kao primjer, uvjerite se (Kruskalovim ili Primovim algoritmom) da je podebljano stablo na donjoj slici optimalno (tj. minimalno razapinjuće) stablo:



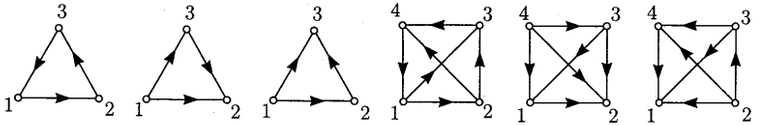
Usmjereni grafovi ili digrafovi

U ovoj ćemo točki i formalno definirati još jednu dodatnu strukturu koju smo već rabili. To su usmjereni grafovi. Potreba za njima javlja se i u praksi. Npr. kad želimo opisati regulaciju prometa u nekom gradu, potrebni su nam podaci o jednosmjernosti te o smjeru prometovanja u pojedinim ulicama. Intuitivno, usmjereni graf ima orijentirane bridove ("strelice").

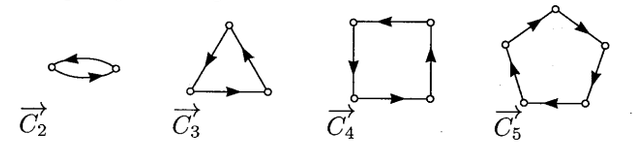
Usmjereni graf ili **digraf** (*engl. directed graph*, kratko *digraph*) D je graf G u kojem svaki brid ima smjer od **početka** prema **kraju**. D se još zove **orijentacija** od G i pišemo $D = \vec{G}$. Brid s početkom u, a krajem v je uređeni par (u, v) i katkad pišemo $u \to v$. Na crtežu stavljamo strelicu koja pokazuje od u prema v. Kaže se još da je $a = uv$ **lûk** od u prema v. Dva ili više luka s istim početkom i krajem

zovu se **višestruki lukovi**. **Striktni digraf** je onaj bez višestrukih lukova i petlji. (Preciznije, digraf D je uređena trojka $D = (V, A, \varphi)$, gdje je $\varphi : A \to V \times V$ funkcija koja svakom luku a pridružuje *uređeni par* vrhova (u, v) (moguće i jednakih) koji se zovu početak i kraj od a.)

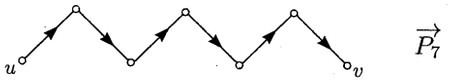
Pridruženi digraf $D(G)$ grafa G je digraf dobiven iz G zamjenom svakog brida dvama suprotno orijentiranim lukovima s istim krajevima. **Pripadni graf** $G(D)$ digrafa D je graf dobiven iz D brisanjem svih strelica (tj. orijentacije). **Turnir** je digraf čiji je pripadni graf jednostavan i potpun. Evo nekih turnira s 3 i 4 vrha:



Mnogi pojmovi koje smo imali kod grafova takoreći automatski se prenose na digrafove. Na primjer, **usmjereni ciklus** ili **diciklus**:



(u, v)-**usmjereni put** ili (u, v)-**diput**:



Digraf D je **slabo povezan** (ili kraće **povezan**) ako je pripadni graf povezan, a **jako povezan** ako za svaka dva vrha $u, v \in V(D)$ postoji (u, v)- i (v, u)-diput. **Komponenta** digrafa je komponenta (povezanosti) pripadnog grafa od D, a **jaka komponenta** digrafa D je maksimalni jako povezan poddigraf od D.

Za razliku od grafova, ovdje imamo dvije vrste stupnjeva vrha. Neka je v vrh digrafa D. Definiramo **instupanj** (ulazni stupanj) $d_D^-(v)$ i **outstupanj** (izlazni stupanj) $d_D^+(v)$ kao broj lukova s krajem, odnosno početkom v.

Analogon Propozicije 1 je sljedeća činjenica.

PROPOZICIJA 11. *Neka je D digraf sa skupom vrhova $V = V(D)$ i skupom lukova $A = A(D)$, tj. $D = (V, A)$, a $e(D) = |A(D)|$. Tada je*

$$\sum_{v \in V} d^-(v) = e(D) = \sum_{v \in V} d^+(v) \quad .$$

Dokaz je analogan dokazu Propozicije 1 i prepuštamo ga čitatelju.

Matrica susjedstva digrafa D na skupu vrhova $V(D) = \{v_1, v_2, \ldots, v_n\}$ je $(n \times n)$-matrica $A(D) = [a_{ij}]$, gdje je a_{ij} broj lukova u D s početkom u v_i i krajem u v_j. Digraf je **acikličan** ako ne sadrži diciklus. **Stabljika** je orijentacija stabla u kojem jedan vrh (korijen) ima instupanj 0, a svi drugi instupanj 1.

Primjer 24. Dokažite da digraf ima neparni diciklus (tj. diciklus neparne duljine) ako i samo ako neka jaka komponenta nije bipartitna. (To je usmjereni analogon Propozicije 5.)

Rješenje. Ako je D jako povezan digraf, uzmimo neki vrh $u_0 \in V(D)$ i promotrimo skup vrhova X čije su udaljenosti od u_0 parne, te skup Y vrhova čije su udaljenosti od u_0 neparne. Kad bi neki luk $a = xy$ spajao dva vrha u istom skupu, onda bi u_0 bio spojen s y s diputima iste parnosti. Nadovezivanje jednog od tih diputeva s (y, u_0)-putom daje usmjerenu zatvorenu šetnju neparne duljine koja očito sadrži neparni diciklus. Obrnuto, ako svaki luk iz D ima jedan kraj u X, a drugi u Y, onda je digraf bipartitan, a takav može imati samo parne dicikluse. Odatle slijedi tvrdnja. □

Kod igara na (di)-grafovima važan je pojam jezgre, tj. skupa pobjedničkih pozicija. Točnije, **jezgra digrafa** D je skup $S \subseteq V$ međusobno nesusjednih vrhova koji dominiraju nad komplementom $V \setminus S$. Pritom S **dominira** nad T ako $\forall v \in T$, $\exists u \in S$ tako da je $(u, v) \in A(D)$. Mnogi digrafovi nemaju jezgre; npr. neparni diciklusi.

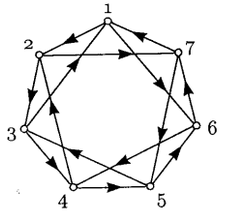
Primjer 25 (M. Richardson, 1953). Dokažite, ako digraf D nema neparnih diciklusa, onda D ima jezgru.

Rješenje. Indukcijom po broju n vrhova od D. Za $n = 1, 2, 3$ tvrdnja je jasna. Neka je D jako povezan digraf s n vrhova. Prema prethodnom primjeru, D je bipartitan s biparticijom (X, Y). Tada X ili Y čini jezgru. Ako D nije jako povezan, neka je D_1 maksimalna jaka komponenta od D i neka je $V_1 = V(D_1)$. Po pretpostavci indukcije, D_1 ima jezgru S_1. Neka je V_2 skup vrhova od D koji su dominirani s vrhovima iz S_1, a $D_2 := D \setminus (V_1 \cup V_2)$. Opet induktivno, D_2 ima jezgru S_2. Tada se lako provjeri da je $S_1 \cup S_2$ jezgra od D. □

Nalaženje neparnih diciklusa (ako ih uopće ima) može se izvesti polinomskim algoritmom tako da pogledamo neparne potencije matrice susjedstva sve dok se na dijagonali pojavi nenul član. Nalaženje parnih diciklusa je puno teže i ne zna se postoji li polinomski algoritam za njihovo nalaženje. Jedan jednostavan uvjet za egzistenciju parnih diciklusa u terminima minimalnih instupnjeva i outstupnjeva je sljedeći teorem.

TEOREM (C. Thomassen, 1992). *Neka je D striktan jako povezan digraf s minimalnim instupnjem $\delta^- \geq 3$ i minimalnim outstupnjem $\delta^+ \geq 3$. Tada D sadži parni diciklus.*

Da su uvjeti ovog Teorema oštri, vidi se na primjeru tzv. **Kohovog digrafa** na slici. To je jako povezan 2-diregularan digraf sa 7 vrhova bez parnih diciklusa.



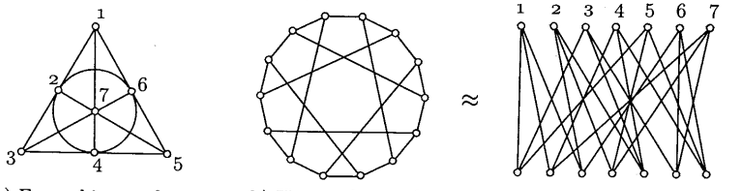
Kohov digraf

Opišimo ovdje ukratko još jednu zanimljivu vezu s naizgled puno općenitijim strukturama nego što su grafovi.

Hipergraf H se sastoji od skupa $V(H)$ čiji se elementi zovu **vrhovi** i familije podskupova $E(H)$ skupa vrhova $V(H)$ koji se zovu **hiperbridovi** (ili kraće **bridovi**, ako nema dvojbe o čemu se radi). Vrh v i brid e su **incidentni** ako je $v \in e$. **Graf incidencije hipergrafa** H je bipartitan graf s biparticijom $(V(H), E(H))$ u kojem je $v \in V(H)$ susjedan s $e \in E(H)$ ako i samo ako su oni incidentni u H. Dakle, svakom hipergrafu je na prirodni način pridružen jedan bipartitni graf. No i obrnuto, svakom bipartitnom grafu G s biparticijom (X, Y) odgovara hipergraf H čiji je skup vrhova X, a čiji su hiperbridovi skupovi susjeda vrhova iz Y. Tako možemo hipergraf rekonstruirati iz njegova grafa incidencije. Stoga su te dvije strukture zapravo jedno te isto.

Primjer 26. Hipergraf koji je konstruirao Fano[9] ima skup vrhova $V = \{1, 2, 3, 4, 5, 6, 7\}$, a skup hiperbridova $E = \{1\,2\,3, 3\,4\,5, 1\,5\,6, 1\,4\,7, 2\,5\,7, 3\,6\,7, 2\,4\,6\}$ i zove se **Fanov hipergraf** F. To je zapravo primjer konačne projektivne ravnine (vidi VII, §1) sa 7 vrhova i 7 pravaca. Konstruirajte F i njegov graf incidencije. Ima li neka "tajna veza" Fanovog hipergrafa i Kohovog digrafa?

Rješenje. Na slici a) je Fanov hipergraf, a na slici b) njegov graf incidencije koji se zove **Heawoodov graf**. To je 3-regularan graf s 14 vrhova.



a) Fanov hipergraf b) Heawoodov graf

"Tajna veza" je da sedam 3-članih podskupova vrhova Kohovog digrafa i njihovih "outsusjeda", čine bridove Fanovog hipergrafa. Postoji i opća veza između jako povezanih digrafova bez parnih diciklusa i izvjesne klase hipergrafova kakav je Fanov. □

§ 3. Obilasci grafova i digrafova

Eulerovi grafovi i digrafovi

Problem crtanja grafa bez podizanja olovke s papira, problem 7 mostova u Königsbergu i slično među najstarijim su problemima u teoriji grafova. **Eulerova tura** na grafu je zatvorena staza koja sadrži svaki brid. Dakle, to je zatvorena staza koja prolazi svakim bridom točno jedanput. Graf je **Eulerov** ako dopušta Eulerovu turu.

Već je Euler 1736. znao karakterizaciju takvih grafova u "lokalnim" terminima pomoću stupnjeva, ali je prvi korektan dokaz nađen tek 1873.

TEOREM 5. *Povezani graf G je Eulerov ako i samo ako mu je svaki vrh parnog stupnja.*

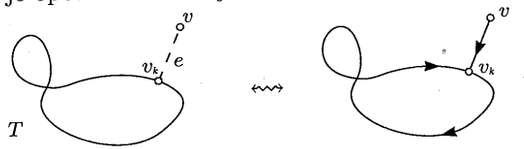
Dokaz. $\Rightarrow$: Neka je C Eulerova tura na G. Svaki put kada C "uđe" u vrh v, mora i izaći iz v. Točnije, ako fiksiramo jednu orijentaciju obilaska Eulerovom turom C, onda se skup bridova incidentnih s v može particionirati u dva skupa: ulazeći i

[9] Gino Fano (1871 – 1952), talijanski matematičar.

izlazeći iz v i među njima postoji očita bijekcija.
$\Leftarrow$: Glavni trik je (kao što smo već vidjeli) da pogledamo najdužu moguću stazu u G i dokažemo da je to Eulerova tura. Neka je, dakle, $T = (v_0, e_1, v_1, \ldots, e_m, v_m)$ najduža staza duljine m. Dovoljno je dokazati da je
(i) $v_0 = v_m$; (ii) $E(G) = \{e_1, e_2, \ldots, e_m\}$.
Pretpostavimo da je $v_m \neq v_0$. Tada je v_0 incidentan s neparnim brojem bridova iz T. No, kako je $d_G(v_0)$ paran, postoji brid $e \in E(G) \setminus E(T)$ incidentan s v_0, pa bi T mogli produžiti tim bridom, što je u kontradikciji s izborom T. Time smo dokazali (i).
Dokažimo (ii). Uzmimo prvo da je $V(T) \neq V(G)$ i neka je $u \in V(G) \setminus V(T)$. Kako je G povezan, odmah slijedi da postoji brid $e = vv_k$, $v \notin V(T)$, $v_k \in V(T)$. Tada imamo stazu

$$(v, e, v_k, e_{k+1}, v_{k+1}, \ldots, v_{m-1}, v_0, e_1, v_1, \ldots, e_k, v_k)$$

duljine $m+1$, što je opet kontradikcija s izborom T. Sličica:



Ako je $V(T) = V(G)$, a $E(T) \neq E(G)$, neka je $e \in E(G) \setminus E(T)$. Tada je e oblika $e = v_k v_l$ za neke k, l. Slično prethodnom slučaju sada imamo stazu

$$(v_k, e_{k+1}, v_{k+1}, \ldots, v_{m-1}, e_m, v_0, e_1, v_1, \ldots, e_k, v_k, e, v_l)$$

duljine $m+1$ i opet kontradikciju. Sličica:



□

Eulreova staza je staza koja prolazi svakim bridom grafa točno jedanput (a ne mora biti zatvorena).

KOROLAR 9. *Povezan graf G ima Eulerovu stazu, ako i samo ako ima najviše dva vrha neparnog stupnja.*

Dokaz. Ako G ima Eulerovu stazu onda kao u dokazu Teorema 5, svaki vrh koji nije početak ni kraj te staze ima parni stupanj. Ako G ima najviše dva vrha neparnog stupnja, onda ih ima 0, 1 ili 2. Ako ih ima 0, tj. svi su parnog stupnja, onda prema Teoremu 5 G ima zatvorenu Eulerovu stazu. Kako je $\sum d(v) = 2e(G)$, ne može biti samo jedan vrh neparnog stupnja, pa ako ih uopće ima, mora ih biti točno dva, recimo u i v. Neka je $e = uv$ novi (artificijelni) brid i promotrimo graf $G + e$. U tom su grafu svi vrhovi parnog stupnja, pa prema Teoremu 5 ima Eulerovu turu T. Tada je $T - e$ Eulerova staza u G. □

Ovaj Korolar povlači da graf mostova u Königsbergu nema Eulerovu stazu. Na digrafu D, **usmjerena Eulerova tura** je usmjerena zatvorena staza koja svakim lukom prođe točno jedanput. Analogon prethodnog teorema za digrafove je sljedeći.

PROPOZICIJA 12. *a) Povezani digraf D sadrži usmjerenu Eulerovu turu ako i samo ako je $d_D^+(v) = d_D^-(v)$, za svako $v \in V(D)$;*

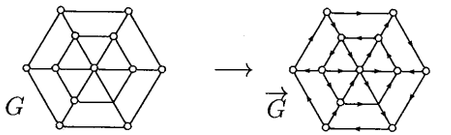
b) Neka su u, v dva vrha u povezanom digrafu D za koje je $d^+(u) - d^-(u) = k = d^+(v) - d^-(v)$, a za sve ostale vrhove x neka je $d^+(x) = d^-(x)$. Tada u D postoji k lučno-disjunktnih (u, v)-diputova.

Dokaz od a) je potpuno analogan dokazu Teorema 5, a iz a) se lako dobije tvrdnja b); to prepuštamo čitatelju.

Primjer 27. Neka je G povezan graf koji ima $2k$ ($k \geq 1$) vrhova neparnog stupnja. Dokažite da je G unija od k bridno disjunktnih staza (tj. nikoje dvije nemaju zajednički brid).

Rješenje. Dodavanjem novog vrha v i spajanjem bridom v s vrhovima $v_1, v_2, \ldots, v_{2k}$ neparnog stupnja dobivamo povezan graf G' u kojem su svi vrhovi parnog stupnja. Prema Teoremu 5 je G' Eulerov graf, pa ima Eulerovu turu T. Ako sada natrag oduzmemo v, dobivamo $G = G' - v$, čime se T raspada na k bridno disjunktnih staza i one sadrže sve bridove od G. (Kao što znamo, svaki graf ima parni broj vrhova neparnog stupnja.) □

Evo jedne "konkretne" primjene digrafova. Zamislimo da je graf na sl. a) plan nekog grada s centrom i dvije glavne obilaznice. Tada se taj graf može orijentirati tako da ulice budu jednosmjerne i da se iz svakog punkta može doći u svaki drugi punkt poštujući sustav jednosmjernog prometovanja, kao na sl. b).



a) b)

Primjer 28. (Jednosmjerni promet, H. Robbins, 1939.) Neka je G povezan graf. Tada G dopušta jako povezanu orijentaciju $\vec{G}$ ako i samo ako G nema reznog brida. Dokažite.

Rješenje. Neka je $\vec{G}$ jako povezana orijentacija od G, a $e \in E(G)$ orijentiran u $\vec{G}$ kao (u, v). Zbog jake povezanosti postoji (v, u)-diput $\vec{P}$ u $\vec{G}$, pa je e brid ciklusa $P + e$, pa prema Propoziciji 7, e nije rezni brid u G.

Obrnuto, pretpostavimo da G nema reznih bridova. Tada postoji ciklus $C = G_1$ u G. Definirajmo induktivno niz povezanih podgrafova $G_1 \subseteq G_2 \subseteq \cdots \subseteq G$ ovako. Ako G_i $(i = 1, 2, \ldots)$ nije razapinjući podgraf od G, neka je $v_i \in V(G - G_i)$. Tada se može pokazati da postoje bridno-disjunktni putovi P_i, Q_i od v_i do G_i. (Pokušajte to sami dokazati, a ako baš ne ide, pogledajte Korolar 30 Mengerovog teorema o k-bridno povezanim grafovima). Definiramo $G_{i+1} := G_i \cup P_i \cup Q_i$. Broj vrhova $v(G_1)$, $v(G_2)$,... strogo raste, pa niz $G_1, G_2, \ldots$ mora završiti s razapinjućim podgrafom G_n od G. Sada G_n orijentiramo tako da prvo orijentiramo G_1 kao diciklus, put P_i orijentiramo kao put s početkom v_i, a Q_i s krajem u v_i. Svaki G_i, pa tako i G_n tada je očito orijentiran tako da je jako povezan. Kako je G_n razapinjući podgraf, slijedi da je G tako orijentiran da je jako povezan. □

Jednu "konkretnu" primjenu Eulerovih grafova nalazimo u **problemu kineskog poštara**, koji je prvi razmatrao kineski matematičar Kuan 1962., pa odatle i naziv. Problem je ovaj. Poštar u poštanskom uredu pokupi poštu, odlazi je razdijeliti i potom se vraća u ured. Pritom on mora barem jedanput proći svakom ulicom svoje četvrti, a želi odabrati rutu kojom će što manje hodati. Prevedeno na jezik teorije grafova problem je ekvivalentan s time da se u povezanom težinskom grafu (G, w) s težinama $w(e) \geq 0$, $\forall e$ (to su duljine ulica) nađe Eulerova tura najmanje težine, tzv. **optimalna tura**.

Ako je G Eulerov graf, onda je svaka Eulerova tura na G optimalna, jer se njome svaki brid prijeđe točno jedanput. U tom se slučaju problem kineskog poštara lako rješava sljedećim **Fleuryjevim algoritmom** koji konstruira Eulerovu turu tako da počne u nekom vrhu i u svakom koraku bira rezni brid neprijeđenog podgrafa samo ako nema (druge) alternative.

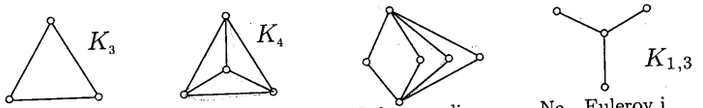
Lako se vidi da ovaj algoritam efikasno pronalazi Eulerovu turu u Eulerovom grafu. Za graf koji nije Eulerov, Edmonds i Johnson su 1974. našli također algoritam za problem kineskog poštara, no u to se nećemo upuštati (vidi usp. [137], [173]).

Hamiltonovi putovi i ciklusi

Za razliku od obilaska svih bridova, sada ćemo razmatrati probleme obilaska svih vrhova grafa. Prvi je te pojmove razmatrao Hamilton[10], pa su ti pojmovi po njemu dobili ime.

Hamiltonov put na grafu je razapinjući put, tj. put koji sadrži sve vrhove grafa, a **Hamiltonov ciklus** je razapinjući ciklus grafa. Graf je **Hamiltonov** ako ima Hamiltonov ciklus.

Problem egzistencije i nalaženja Hamiltonovih ciklusa je mnogo teži nego analogan problem za Eulerove staze. Uostalom, da Eulerovi i Hamiltonovi grafovi nemaju izravne veze, pokazuju ovi jednostavni primjeri:

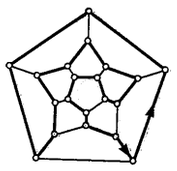


Eulerov i Hamiltonov | Ne - Eulerov, ali Hamiltonov | Eulerov, ali ne - Hamiltonov | Ne - Eulerov i ne - Hamiltonov

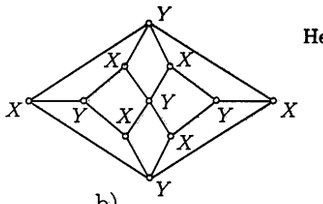
Hamilton je 1856. godine postavio sljedeći problem. Trgovački putnik treba obići neke gradove i vratiti se na mjesto polaska tako da svaki grad posjeti točno jedanput (i svakom cestom najviše jedanput). On je imao u vidu konkretnu igru "put oko svijeta" na **grafu dodekaedra**, a ceste između gradova bridovi dodekaedra. Dodekaedar je pravilni poliedar u čijem se svakom vrhu sastaju tri pravilna peterokuta. Dodekaedar ima 20 vrhova, 30 bridova i 12 peterokuta. Na sl. a) je debelo izvučen Hamiltonov ciklus, pa je graf dodekaedra Hamiltonov graf.

[10] William R. Hamilton (1805 – 1865), irski matematičar.

Graf dodekaedra



a)

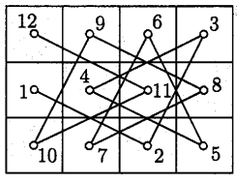


b)

Herschelov graf

Isto su tako i grafovi svih pravilnih poliedara Hamiltonovi (uvjerite se u to). Za razliku od grafa dodekaedra, na sl. b) je **Herschelov graf**. To je također graf poliedra koji je omeđen s 9 četverokuta (zamislite da ste središnji vrh malo izdigli iznad ravnine crteža). Taj graf nije Hamiltonov jer je bipartitan (biparticija (X, Y) je na slici), pa nema neparnih ciklusa (Propozicija 5), a ima 11 vrhova, pa bi Hamiltonov ciklus bio C_{11}.

Još jedna igra je bila izvorištem zanimanja za slične probleme, a to je **problem konjićevog skoka** na šahovskoj ploči $m \times n$ $(m, n \geq 3)$: mogu li se skakačem (konjem) obići sva polja ploče tako da na svako polje dođe samo jedanput? Drugim riječima, postoji li na pridruženom grafu "konjićev" Hamiltonov put? Odgovor je pozitivan, osim za ploče 3×3, 3×5, 3×6 i 4×4. Jedan "konjićev" Hamiltonov put na ploči 3×4 je prikazan kao put $1\,2\,3 \ldots 1\,2$ na slici:



Konjićev Hamiltonov put na ploči 3×4

Jedan od najvećih neriješenih problema teorije grafova je dati netrivijalan i zadovoljavajući nužan i dovoljan uvjet da graf bude Hamiltonov. Ustvari, problem određivanja je li graf Hamiltonov je **NP**-potpun. Općenitiji je poznati **problem trgovačkog putnika** (u literaturi poznat pod engleskim nazivom *Travelling Salesman Problem*). Taj problem glasi ovako. Na potpunom grafu sa zadanim težinama bridova treba naći Hamiltonov ciklus najmanje težine. I to je **NP**-potpun problem. Uočite da K_n ima $(n-1)!/2$ Hamiltonovih ciklusa, pa bi naivno uspoređivanje težina svih Hamiltonovih ciklusa zahtijevalo $O(n!)$ operacija, što je vrlo neefikasno.

Jedan od najjednostavnijih nužnih uvjeta za hamiltonijalnost grafa je sljedeće.

PROPOZICIJA 13. *Ako je G Hamiltonov graf, onda svaki pravi podskup $S \subset V(G)$ ima svojstvo da za broj komponenti $c(G - S)$ vrijedi*

$$c(G - S) \leq |S|.$$

Dokaz. Neka je C Hamiltonov ciklus od G, a $\emptyset \neq S \subset V(G)$. Tada očito $C \setminus S$ ima najviše $|S|$ komponenti, pa je $c(G - S) \leq |S|$. Kako je $C - S$ razapinjući podgraf od $G - S$, slijedi da je $c(G - S) \leq c(C - S)$, pa tvrdnja slijedi. □

Primjer 29. a) Dokažite da $K_{n,n+1}$ nije Hamiltonov i općenitije $K_{m,n}$, $m \neq n$, pa i općenito bipartitan graf s biparticijom (X,Y), za koju je $|X| \neq |Y|$ nije Hamiltonov graf.

b) Graf $K_{n,n}$ ima $(n-1)!n!/2$ Hamiltonovih ciklusa.

Rješenje. a) Ako je $G = K_{n,n+1}$, s biparticijom (X,Y), $|X| = n$, $|Y| = n+1$, uzmimo $S = X$. Tada je $c(G-S) = n+1$, a $|S| = n$, pa prema Propoziciji 13, G nije Hamiltonov. Slično je i za ostale tvrdnje iz a).

b) Ako $X = \{1,2,\ldots,n\}$, $Y = \{1',2',\ldots,n'\}$ čine biparticiju od $K_{n,n}$, onda svaki Hamiltonov ciklus od $K_{n,n}$ prolazi kroz 1. Iz 1 ima n bridova do Y, a iz svakog vrha iz Y se na $(n-1)$ načina možemo vratiti u $X \setminus \{1\}$. Nastavimo li na taj način, dobivamo da je broj takvih ciklusa

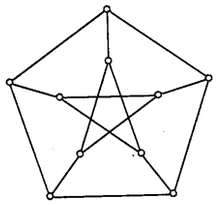
$$[n(n-1)][(n-1)(n-2)]\ldots[1\cdot 1] = (n-1)!n! \,.$$

Taj rezultat moramo podijeliti s 2 jer se svaki takav ciklus može obići u dva smjera. □

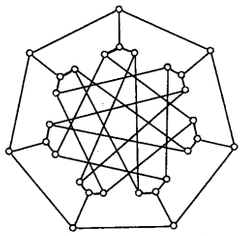
Primjer 30. Pokažimo da **Petersenov graf** P (sl. a)) nije Hamiltonov, ali je $P - v$ Hamiltonov, za svaki vrh $v \in V(P)$. Isto tako, dodavanjem bilo kojeg novog brida e, graf $P + e$ postaje Hamiltonov. Slično vrijedi i za **Coxeterov**[11] **graf** na sl. b).

Rješenje. Petersenov graf (otkriven 1898., iako ga je već poznavao A. Kempe 1886.) je graf s mnogim lijepim svojstvima i često služi kao protuprimjer raznim svojstvima ili je izuzetak za mnoge teoreme. To je 3-regularan graf s 10 vrhova i 15 bridova. Nije teško pokazati da P nije 3-bridno obojiv (naime, bridovi se ne mogu pravilno obojiti s 3 boje, tj. tako da susjedni budu različito obojeni) i to je najmanji jednostavni 3-regularni graf s tim svojstvom.

Zato P nije Hamiltonov, jer bi inače Hamiltonov ciklus mogli pravilno obojiti dvjema bojama, a ostale bridove trećom bojom, što bi dalo 3-bridnu obojivost od P. Da je $P - v$ Hamiltonov, a isto tako $P + e$ dobije se lako konstrukcijom Hamiltonovog ciklusa (učinite to!). Slična svojstva vrijede za 3-regularan Coxeterov graf, ali je to malo teže provjeriti. □



a) Petersonov graf P



b) Coxeterov graf

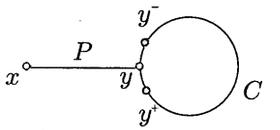
Sada prelazimo na neke dovoljne uvjete za hamiltonijalnost. Intuitivno je jasno da ako su stupnjevi svih vrhova dovoljno veliki, tj. ako je minimalni stupanj δ grafa što veći (kao funkcija od $n = v(G)$), onda je veća šansa da graf G sadrži izvjesne podgrafove. Tako npr., Propozicija 3 kaže da ako je $\delta \geq 2$, onda G sadrži ciklus duljine $\geq \delta + 1$, a Propozicija 1 i Teorem 3 povlače da za $\delta > n/2$, G sadrži trokut.

Osnovni je rezultat u tome smislu sljedeći teorem.

[11] Harold S. M. Coxeter, r.1907, kanadski matematičar.

TEOREM 6 (Dirac[12], 1952). *Neka je G jednostavan graf s $n \geq 3$ vrhova i minimalnim stupnjem $\delta \geq n/2$. Tada je G Hamiltonov graf.*

Dokaz. Kako je $n \geq 3$, a $\delta \geq n/2$, slijedi da je $\delta \geq 2$, pa prema Propoziciji 3 G ima ciklus. Neka je C najdulji ciklus u G. Ako je G Hamiltonov, dokaz je gotov, pa pretpostavimo da je $G \setminus C \neq \emptyset$. Uzmimo da je obilazak od C u pozitivnom smjeru s početkom (i krajem) u vrhu y i neka su y^+ i y^- susjedni vrhovi od y u C. Zbog $G \setminus C \neq \emptyset$, postoji netrivijalni (x,y)-put P u G. Stoga u G imamo "laso" $C \cup P$ (ili (x,y)-laso):



i putove $P \cup yy^+\ldots y^-$, $P \cup yy^-\ldots y^+$. Posebno, ako je C najdulji ciklus, a P netrivijalan put, onda x nije susjedan s oba vrha y^+ i y^-. Stavimo

$$V_1 := V(C), \quad V_2 := V(P) \setminus \{y\}, \quad V_3 := V(G) \setminus V(C \cup P),$$

te $d_i(x)$, $d_i(y^+)$ redom brojevi susjeda od x i y^+ u V_i, $i = 1,2,3$. Kako je C najdulji ciklus u G, a P netrivijalni put, zaključujemo da vrijedi sljedeće:

(*i*) x i y^+ ne mogu biti susjedni redom s dva susjedna vrha v i v^+ na ciklusu C. Zato je $d_1(x) + d_1(y^+) \leq |V_1|$.

(*ii*) y^+ nije susjedan ni s jednim vrhom iz V_2. Zato je $d_2(y^+) = 0$.

(*iii*) x i y^+ ne mogu biti susjedni nekom vrhu iz V_3. Zato je $d_3(x) + d_3(y^+) \leq |V_3|$.

Nadalje, očito je $d_2(x) \leq |V_2| - 1$. Stoga imamo

$$2\delta \leq d(x) + d(y^+) = \sum_{i=1}^{3}(d_i(x) + d_i(y^+)) \leq |V_1| + |V_2| - 1 + |V_3| = n - 1 \,,$$

a to je kontradikcija s pretpostavkom $2\delta \geq n$. Prema tome, C mora biti Hamiltonov ciklus u G. (Ovaj je dokaz dao J. Bondy, 1981.) □

Napomena. Uvjet $\delta \geq n/2$ se ne može zamijeniti s $\delta \geq \lfloor n/2 \rfloor$, što pokazuje $G = K_{\lfloor n/2 \rfloor, \lceil n/2 \rceil}$.

KOROLAR 10. *Ako je G jednostavan graf s n vrhova i $\delta \geq (n-1)/2$, onda G ima Hamiltonov put.*

Dokaz. Za $n = 1$, tvrdnja je trivijalna. Za $n \geq 2$, dodajmo vrh v. Graf $H = G + v$ ima $n+1$ vrh i minimalni stupanj $\geq (n+1)/2$. Iz Diracovog teorema 6 slijedi da H ima Hamiltonov ciklus C. Tada je $C - v$ Hamiltonov put u G. □

[12] Guy A. Dirac (1925 – 1984), danski matematičar.

Postoje brojna poopćenja Diracovog teorema i to u raznim smjerovima. Jedno takvo elegantno poopćenje je sljedeće.

TEOREM 7 (B. Bollobás i dr. 1993). *Neka je G jednostavni graf s n vrhova, a S skup svih vrhova iz G stupnja barem $n/2$. Ako je $|S| \geq 3$, onda G ima ciklus koji sadrži sve vrhove iz S. (Za $S = V(G)$ dobivamo Diracov teorem.)*

Dokaz. Zaključivanje je slično dokazu Diracovog teorema, pa nećemo iznijeti sve detalje. Neka je C ciklus koji ima najveći mogući broj vrhova iz S. Pretpostavimo da je $S \setminus V(C) \neq \emptyset$ i neka je $C \cup P$ jedan (x,y)-laso, gdje je $x \in S$. Ciklus C ima bar dva vrha iz S, jer svaka dva nesusjedna vrha iz S leže na 4-ciklusu u G. Neka je z prvi vrh iz S poslije y na C. Tada kao u dokazu Diracovog teorema, izbor ciklusa C povlači da je $d(x) + d(z) \leq n - 1$, što je kontradikcija. □

Ako malo analiziramo dokaz Diracovog teorema, vidimo da smo zapravo rabili samo ovo: postoje nesusjedni vrhovi x, y za koje je $d(x)+d(y) \geq n$. Stoga više-manje isti dokaz daje sljedeće.

TEOREM 8 (O. Ore, 1968). *Neka je G jednostavni graf s $n \geq 3$ vrhova, takav da je za svaka dva nesusjedna vrha, zbroj njihovih stupnjeva barem n. Tada je G Hamiltonov graf.*

Ustvari, dokaz Oreovog teorema počiva na ovoj lemi.

LEMA 4. *Neka je G jednostavni graf s $n \geq 3$ vrhova, a x i y nesusjedni vrhovi za koje je $d(x)+d(y) \geq n$. Tada je G Hamiltonov ako i samo ako je $G+xy$ Hamiltonov.*

Dokaz. Jasno, ako je G Hamiltonov, onda je i $G + xy$ Hamiltonov. Obratno, ako je $G+xy$ Hamiltonov, a pretpostavimo li da G nije Hamiltonov, onda kao u dokazu Diracovog teorema, dobivamo $d(x) + d(y) \leq n - 1$, suprotno pretpostavci. □

Ovom lemom prirodno dolazimo do definicije zatvarača grafa. **Zatvarač grafa** G na n vrhova je graf dobiven iz G rekurzivnim spajanjem parova nesusjednih vrhova čija je suma stupnjeva $\geq n$. Višestrukom primjenom Leme 4 dobivamo

TEOREM 9 (V. Chvatál, 1972). *Neka je G jednostavan graf na $n \geq 3$ vrhova i nizom stupnjeva $d_1 \leq d_2 \leq \cdots \leq d_n$. Pretpostavimo da vrijedi*

$$d_k \leq k < n/2 \Rightarrow d_{n-k} \geq n - k \,. \qquad (*)$$

Tada je G Hamiltonov graf.

Dokaz. Pokazat ćemo da je zatvarač od G potpun, pa će tvrdnja slijediti iz Leme 4. Pretpostavimo da G nije Hamiltonov i neka je H zatvarač od G. Tada je suma stupnjeva svaka dva nesusjedna vrha iz H najviše $n-1$. Neka su x i y dva takva vrha s najvećom sumom stupnjeva. Uzmimo da je $d_H(x) \leq d_H(y)$ i neka je $d_H(x) = k$.

Tada je $k \leq (n-1)/2$, a $d_H(y) \leq n - k - 1$. Promotrimo sljedeće skupove:

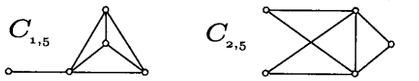
$$X := \{v \in V(G) \,|\, v \not\sim y \text{ u } H\}, \quad Y := \{w \in V(G) \,|\, w \not\sim x \text{ u } H\}.$$

Tada je $|X| = n - 1 - d_H(y) \geq k$, a zbog izbora x i y slijedi $d_G(v) \leq d_H(v) \leq k$, $\forall v \in X$. Slično je $|Y| = n - k - 1$ i $d_G(w) \leq d_H(w) \leq n - k - 1$, $\forall w \in Y$. Prema tome, G ima barem k vrhova stupnja barem k (to su vrhovi iz X)i barem $n - k$ vrhova stupnja barem $n-k-1$ (to su vrhovi iz $Y \cup \{x\}$). To proturječi pretpostavci $(*)$. Stoga je zatvarač od G potpun i tvrdnja slijedi. □

KOROLAR 11. *Neka je G jednostavan graf na $n \geq 3$ vrhova s nizom stupnjeva $d_1 \leq d_2 \leq \ldots d_n$. Ako vrijedi* (a) *ili* (b), *onda je G Hamiltonov. Pritom je*
(a) **(Pósa)** *$d_k \geq k+1$, za $k < n/2$;* (b) **(Bondy)** *$d_k \leq k, d_l \leq l \Rightarrow d_k + d_l \geq n$ $(k \neq l)$.*

Dokaz. Ako vrijedi (a), onda vrijedi $(*)$ iz Chvatálovog teorema. Ako vrijedi (b), neka je $d_k < k \leq n/2$ i $l = n - k$. Tada je ili $d_l \geq l$ ili $d_k + d_l \geq l + k = n$, pa stoga $d_l > l$, pa stoga opet vrijedi $(*)$ i zato je G Hamiltonov. □

Kažemo da je niz realnih brojeva $(p_1, p_2, \ldots, p_n)$ **majoriziran** nizom $(q_1, q_2, \ldots, q_n)$, ako je $p_i \leq q_i$, za sve i. Ako su G i G' grafovi s $v(G) = v(G') = n$ i nizovima stupnjeva $d_1 \leq d_2 \leq \cdots \leq d_n$, $d'_1 \leq d'_2 \leq \cdots \leq d'_n$ redom, onda kažemo da je G **stupnjevima majoriziran** s G', ako je $d_i \leq d'_i$, za svako i. **Spoj** $G * H$ disjunktnih grafova G i H dobije se tako da se svaki vrh iz G spoji jednim bridom sa svakim vrhom iz H. Za $1 \leq m < n/2$, neka je $C_{m,n} := K_m * (K_m^c \cup K_{n-2m})$. Na primjer,



LEMA 5. *$C_{m,n}$ nije Hamiltonov, a niz stupnjeva mu je*

$$(\underbrace{m, \ldots, m}_{m}, \underbrace{n-m-1, \ldots, n-m-1}_{n-2m}, \underbrace{n-1, \ldots, n-1}_{m}). \qquad (**)$$

Dokaz. Neka je S skup svih vrhova iz $C_{m,n}$ stupnja $n-1$. Tada je $\emptyset \neq S \subset V(C_{m,n})$ i $c(C_{m,n} - S) = m + 1 > |S|$, pa Propozicija 13 povlači da $C_{m,n}$ nije Hamiltonov. Druga tvrdnja je lagana provjera. □

KOROLAR 12. *Ako je G ne-Hamiltonov jednostavan graf s $n \geq 3$ vrhova, onda je G stupnjevima majoriziran s nekim $C_{m,n}$.*

Dokaz. Neka je $d_1 \leq d_2 \leq \cdots \leq d_n$ niz stupnjeva od G. Iz Teorema 9 slijedi da postoji $m < n/2$, tako da je $d_n \leq m$, a $d_{n-m} < n - m$. Odatle odmah slijedi da je $(d_1, d_2, \ldots, d_n)$ majoriziran nizom $(**)$. □

KOROLAR 13. *Neka je G jednostavan graf s $n \geq 3$ vrhova i brojem bridova $e(G) > \binom{n-1}{2} + 1$. Tada je G Hamiltonov graf. Jedini jednostavan ne-Hamiltonov graf s n vrhova i $\binom{n-1}{2} + 1$ bridova je $C_{1,n}$ i za $n = 5$, $C_{2,5}$.*

Dokaz. Iz Korolara 12 slijedi da je G stupnjevno majoriziran s nekim $C_{m,n}$, gdje je $0 < m < n/2$. Zato imamo (rabeći Propoziciju 1):

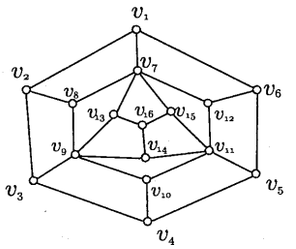
$$e(G) = e(C_{m,n}) = \frac{1}{2}[m^2 + (n-2m)(n-m-1) + m(n-1)] =$$
$$= \binom{n-1}{2} + 1 - \frac{1}{2}(m-1)(m-2) - (m-1)(n-2m-1) \leq \binom{n-1}{2} + 1,$$

odakle slijedi prva tvrdnja.

Nadalje, u prvoj nejednakosti može nastupiti jednakost samo ako G ima isti niz stupnjeva kao $C_{m,n}$, a u drugoj nejednakosti nastupa jednakost ako i samo ako je $m = 1$ ili $m = 2, n = 5$. Stoga je $e(G) = \binom{n-1}{2} + 1$ ako i samo ako G ima isti niz stupnjeva kao $C_{1,n}$ ili $C_{2,5}$, a odavde se lako vidi da mora biti $G \approx C_{1,n}$ ili $G \approx C_{2,5}$. □

Da se ustanovi ima li neki graf ili nema Hamiltonov put ili ciklus, često treba primijeniti neku ad hoc metodu. Evo jednog primjera.

Primjer 31. Graf G na donjoj slici nema Hamiltonov put. Dokažite.



Dokaz. Svaki Hamiltonov put sadrži najviše dva brida incidentna nekom vrhu. Vrh v_7 grafa G ima stupanj 5, pa stoga barem tri brida incidentna s v_7 nisu u Hamiltonovom putu. To isto vrijedi i za vrhove v_9 i v_{11}. Stupnjevi vrhova v_2, v_4, v_6, v_{16} jednaki su 3 pa barem jedan brid incidentan svakom tom vrhu nije u Hamiltonovom putu. Prema tome, ako G sadrži Hamiltonov put, onda na tom putu ne smije biti barem 13 od ukupno 27 bridova od G. Budući da G ima 16 vrhova, na Hamiltonovom bi putu od G trebalo biti barem 15 bridova. Dakle, G nema Hamiltonov put. □

Usmjereni Hamiltonovi putovi i ciklusi

Usmjereni Hamiltonov put u digrafu D je usmjereni put (tj. diput) koji sadrži sve vrhove iz D. Osnovni rezultat ovdje je (kao što je Diracov teorem za obične grafove) teorem o turnirima (potpunim usmjerenim grafovima).

TEOREM 10 (L. Rédei, 1934). *Svaki turnir ima usmjereni Hamiltonov put.*

Za dokaz nam treba sljedeća lema.

LEMA 6. *Neka je D striktni digraf, P (x,y)-diput u D duljine l, $v \in V(D) \setminus V(P)$, a $d_P(v)$ broj lukova iz D s jednim krajem v, a drugim iz P. Tada*

(i) Ako je postoji (x,y)-diput P', tako da je $V(P') = V(P) \cup \{v\}$, onda je $d_P(v) \leq l+2$;

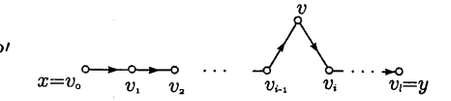
(ii) Ako je P najdulji diput u D, onda je $d_P(v) \leq l$.

Dokaz. *(i)* Neka je $P = (v_0, v_1, \ldots, v_l)$, $v_0 = x$, $v_l = y$. Promotrimo skupove $X := \{v_i \in V(P) \setminus \{v_0\} \mid (v, v_i) \in A(D)\}$, $Y := \{v_i \in V(P) \setminus \{v_0\} \mid (v_{i-1}, v) \in A(D))\}$.

Tada je $X \cup Y \subseteq \{v_1, v_2, \ldots, v_l\}$. Tvrdimo da je $X \cap Y = \emptyset$. Naime, kad bi postojao $v_i \in X \cap Y$, onda bi postojao (x,y)-diput (v. sliku)

$$P' = (v_0, v_1, \ldots, v_{i-1}, v, v_i, \ldots, v_l),$$

suprotno pretpostavci.



No, tada imamo

$$d_P(v) \leq |X| + |Y| + 2 = |X \cup Y| + |X \cap Y| + 2 \leq l + 2.$$

(ii) Ako je P najdulji put u D, onda ni (v, v_0) ni (v_l, v) ne mogu biti lukovi od D, jer bi u protivnom imali još dulje dipute. Stoga kao gore zaključujemo $d_P(v) \leq |X| + |Y| \leq l$. □

Dokaz Teorema 10. Neka je T turnir, a P najdulji diput u T duljine l. Kad P ne bi bio Hamiltonov, onda bi postojao vrh $v \in V(T) \setminus V(P)$. Kako je T turnir, imamo $d_P(v) = l + 1$, a iz Leme 6 (ii) znamo da je $d_P(v) \leq l$. To je kontradikcija, pa je P Hamiltonov diput na T. (Drugi dokaz će biti neposredna posljedica Gallai-Royovog teorema 16.) □

Poopćenje Rédeiovog teorema je sljedeći teorem.

TEOREM 11 (P. Camion, 1959). *Turnir je jako povezan ako i samo ako ima usmjereni Hamiltonov ciklus.*

Dokaz. Ako turnir ima Hamiltonov ciklus, onda je očito jako povezan. Neka je T jako povezan turnir, a $C = (v_0, v_1, \ldots, v_l)$ diciklus maksimalne duljine u T. Takav postoji, jer aciklički turnir nije jako povezan. Pretpostavimo da C nije Hamiltonov i neka je $v \in V(T) \setminus V(C)$. Neka je $(v_0, v) \in A(T)$. Ako je $(v, v_1) \in A(T)$, onda je $(v_0, v, v_1, \ldots, v_l)$ dulji diciklus od C. Zato je $(v_1, v) \in A(T)$ i slično $(v_i, v) \in A(T)$, $i = 1, \ldots, l$. Neka je $X = \{x \in V(T) \mid (v_0, x) \in A(T)\}$. Tada je $(v_i, x) \in A(T)$, $\forall x \in X$ (sličnim zaključivanjem kao gore). Neka je $(x,y) \in A(T)$ lûk za koji je $x \in X$, $y \notin X$ (takav postoji jer ima lukove u $A(T \setminus X)$). Tada $y \notin C$, pa stoga $y \notin X$ povlači $(y, v_0) \in A(T)$. No tada je $(x, y, v_0, \ldots, v_l)$ diciklus dulji od C. □

Teorem 10 slijedi sada tako da se na svaku jaku komponentu turnira primijeni Teorem 11, čime se u svakoj dobiva usmjereni Hamiltonov put i onda ti putovi zajedno daju usmjereni Hamiltonov put u čitavom turniru.

Drugo poopćenje Rédeiovog teorema je sljedeće.

TEOREM 12. *Na svakom turniru ima neparan broj Hamiltonovih putova.*

Za dokaz nam treba sljedeće. Neka je $D = (V, A)$ striktan digraf na skupu vrhova $V = \{1, 2, \ldots, n\}$, a π permutacija od V. Definirajmo skup $A_\pi \subseteq A$ ovako:

$$A_\pi := A \cap \{(\pi(i), \pi(i+1)) \mid i = 1, 2, \ldots, n-1\}.$$

Tada A_π inducira digraf čije su komponente diputovi i zove se **sistem diputova**

LEMA 7. *Neka je S_n skup svih permutacija od V, a $\mathcal{H}$ skup svih Hamiltonovih diputova na D. Za podskup $X \subseteq A$ definirajmo*

$$f(X) := \#\{\pi \in S_n \mid X = A_\pi\}, \quad h(X) := \{H \in \mathcal{H} \mid X \subseteq A(H)\}.$$

Tada je $f(X) \equiv h(X) \bmod 2$.

Dokaz Leme. Definirajmo $g(X) := \#\{\pi \in S_n \mid X \subseteq A_\pi\}$. Tada je $g(X) = \sum_{X \subseteq Y \subseteq A} f(Y)$. Iz formule uključivanja-isključivanja slijedi da je

$$f(X) = \sum_{X \subseteq Y \subseteq A} (-1)^{|Y|-|X|} g(Y).$$

Primijetimo da je $g(Y) = r!$ ako i samo ako je razapinjući poddigraf od D sa skupom lukova Y sistem diputova s r komponenti. Stoga je $g(Y)$ neparan ako i samo ako Y inducira neki Hamiltonov diput H od D. Stoga je

$$f(X) \equiv \sum_{\substack{H \in \mathcal{H} \\ X \subseteq A(H)}} (-1)^{n-1-|X|} \equiv h(X) \pmod 2.$$

□

Dokaz Teorema 12. Teorem očito vrijedi za acikličke turnire, jer svaki takav ima očito točno jedan Hamiltonov diput. No, svaki se turnir može iz acikličkog dobiti preorijentacijom nekih lukova. Stoga je dovoljno dokazati da se broj $h(T)$ Hamiltonovih diputa na turniru T ne mijenja, ako mu preorijentiramo neki luk a. Uzmimo u Lemi 7 da je $X = \{a\}$. Tada je $f(a) \equiv h(a) \pmod 2$. Ako je turnir T' dobiven iz turnira T preorijentacijom luka a, onda iz definicije f i h slijedi

$$h(T') = h(T) + f(a) - h(a) \equiv h(T) \pmod 2.$$

□

Na kraju, navedimo bez dokaza sljedeći teorem.

TEOREM (Meyniel, 1973). *Neka je D striktan jako povezan digraf na $n \geq 2$ vrhova, tako da je suma stupnjeva svaka dva nesusjedna vrha barem $2n - 1$. Tada D ima Hamiltonov diciklus.*

Ovaj teorem povlači sljedeće.

KOROLAR. *Neka je D striktni digraf na n vrhova, tako da za minimalni instupanj δ^- i minimalni outstupanj δ^+ vrijedi $\min\{\delta^-, \delta^+\} \geq n/2$. Tada D ima Hamiltonov diciklus.*

Ako ovaj Korolar primijenimo na pridruženi digraf $D(G)$ jednostavnog grafa G s $n \geq 3$ vrhova u kojem je $\delta \geq n/2$, dobivamo Diracov teorem 6.

Na ovu važnu temu hamiltonijalnosti još ćemo se povremeno vraćati.

§ 4. Povezanost grafova

Vršna i bridna povezanost grafova su dva parametra grafa koji mjere "jačinu povezanosti" grafa. Podsjetimo da je graf povezan ako se svaka dva vrha mogu povezati putom u grafu. Ekvivalentno, graf je povezan ako se skup vrhova ne može particionirati u dva prava podskupa, pri čemu su vrhovi u različitim podskupovima nesusjedni. Intuitivno, graf je "jako povezan", ako njegovu povezanost ne možemo uništiti uklanjanjem malog dijela grafa, odnosno ako među svaka dva vrha ima puno disjunktnih putova. Ove ideje ćemo sada formalizirati.

Familija (x, y)-putova u grafu je **bridno disjunktna** ako nikoja dva puta nemaju zajednički brid, a **unutarnje disjunktna** ako nikoja dva nemaju unutarnji zajednički vrh. Graf G s barem dva vrha je **k-bridno povezan** ako se svaka dva vrha mogu povezati s barem k bridno disjunktnih putova, a **k-povezan**, ako se svaka dva vrha mogu povezati s barem k unutarnje disjunktnih putova. Graf s jednim vrhom je po definiciji i k-bridno i k-povezan za $k = 0, 1$ (a ne za $k \geq 2$). Dakle, svaki graf je 0-povezan, a 1-povezan ako i samo ako je povezan. Graf G bez petlji i s bar dva brida je 2-povezan ako i samo ako se ne može razdvojiti na dva podgrafa G_1, G_2 tako da je $G_1 \cup G_2 = G$, $G_1 \cap G_2 = \{v\}$ i $G_1, G_2 \neq \{v\}$. Kako su unutarnje disjunktni putovi i bridno disjunktni, slijedi da je k-povezan ujedno i k-bridno povezan graf.

Slične su definicije i za digrafove. Digraf D je **jako k-lučno povezan** ako su svaka dva vrha x,y povezana s barem k lučno disjunktnih (x, y)-diputova, a **jako k-povezan** ako su svaka dva vrha x, y povezana s barem k unutarnje disjunktnih (x, y) diputova.

Bridna povezanost $\kappa'(G)$ grafa G je najveći cijeli broj k, za koji je G k-bridno povezan, a **povezanost** $\kappa(G)$ je najveći cijeli broj k za koji je G k-povezan. Slično, **jaka povezanost** digrafa D, $\kappa(D)$ je najveći cijeli broj k, za koji je D jako k-povezan i slično se definira **jaka lučna povezanost** $\kappa'(D)$ od D. Ovi se parametri mogu izračunati u polinomijalnom vremenu.

Vršni rez u G je podskup $S \subseteq V(G)$ tako da je $G - S$ nepovezan. Ako je $|S| = k$, kažemo da je to **k-vršni rez**. Ako je $x \in S$, a $y \notin S$, kažemo da ih S **separira**. **Bridni rez** u G je podskup $[S, \bar{S}] \subseteq E(G)$, gdje je $S \subseteq V(G)$ (a $\bar{S} = V(G) \setminus S$); pritom simbol $[X, Y]$, za $X, Y \subseteq V(G)$ znači skup svih bridova iz G s jednim krajem u X, a drugim u Y. Bridni rez $[S, \bar{S}]$ se još zove i **korub** od S (ili od $\bar{S}$), a ako je $x \in S$, $y \in \bar{S}$, kažemo da ih S **separira**. Minimalni neprazni bridni rez je **vez** (engl. *bond*). Svaki neprazni bridni rez je disjunktna unija vezova. Osnovni i bitni teorem kaže da se dva opisana pristupa podudaraju. Točnije, vrijedi ovaj teorem.

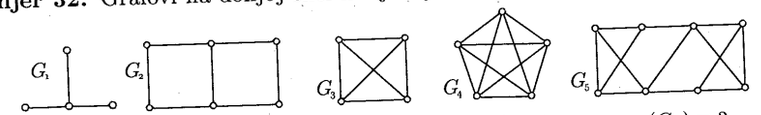
TEOREM 13 (K. Menger[13], 1927). *(i) Neka je G graf, a x i y dva vrha. Tada je maksimalni broj bridno disjunktnih (x, y)-putova u G jednak minimalnom broju bridova bridnog reza koji separira x i y.*

(ii) Neka su x, y nesusjedni vrhovi grafa G. Tada je maksimalni broj unutarnje disjunktnih (x, y)-putova u G jednak minimalnom broju vrhova u vršnom rezu od G koji separira x i y.

Prema tome, možemo reći da je povezanost (odn. bridna povezanost) grafa najmanji

broj vrhova (odn. bridova) čijim izbacivanjem preostali graf postaje nepovezan (ili trivijalan).

Primjer 32. Grafovi na donjoj slici imaju sljedeće povezanosti i bridne povezanosti.



$\kappa(G_1) = 1$, $\kappa'(G_1) = 1$ | $\kappa(G_2) = 2$, $\kappa'(G_2) = 2$ | $\kappa(G_3) = 3$, $\kappa'(G_3) = 3$ | $\kappa(G_4) = 4$, $\kappa'(G_4) = 4$ | $\kappa(G_5) = 2$, $\kappa'(G_5) = 3$

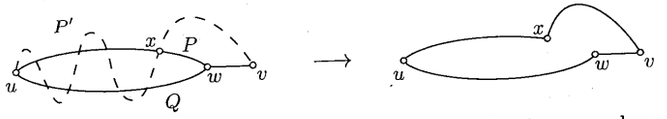
Kako smo već rekli, $\kappa(G) \leq \kappa'(G)$, a očito je i $\kappa'(G) \leq \delta(G)$.

Dokaz Mengerova teorema (kao i analogona za digrafove) provest ćemo poslije i dobiti kao posljedicu razmatranja u vezi sa sparivanjima (§7) ili protocima u mrežama (§10). Ipak, sada ćemo dati jednostavan dokaz vršne 2-povezanosti koji je dao Whitney[14] 1932.

Primjer 33 (Whitneyev teorem). Neka je G graf s barem tri vrha. Tada najmanji vršni rez u G ima bar dva elementa ako i samo ako su svaka dva (različita) vrha u G povezana s barem dva unutarnje disjunktna puta.

Dokaz. Ako su svaka dva vrha povezana s dva unutarnje disjunktna puta, onda je očito G povezan i nema 1-vršni rez, pa svaki vršni rez ima bar dva vrha.

Obrnuto, neka je najmanji vršni rez u G dvočlan i neka su $u, v \in V$. Dokažimo indukcijom po $d(u,v)$ da se u, v mogu povezati s dva unutarnje disjunktna puta. Ako je $d(u,v) = 1$, onda zbog pretpostavke slijedi da uv nije rezni, pa je uv brid nekog ciklusa C i zato su u i v spojeni s dva unutarnje disjunktna puta e i $C - e$. Pretpostavimo da tvrdnja vrijedi za svaka dva vrha na udaljenosti $< k$, i neka je $d(u,v) = k \geq 2$. Tada postoji (u,v)-put duljine k i neka je w neposredni prethodnik od v na tom putu. Tada je $d(u,w) = k - 1$ i neka su P, Q unutarnje disjunktni (u,w)-putovi. $G - w$ je povezan pa postoji (u,v)-put P' u $G - w$. Neka je x posljednji vrh od $P' \cap (P \cup Q)$ (takav x postoji jer je $u \in P' \cap (P \cup Q)$). Uzmimo da je $x \in P$. Tada su dva tražena unutarnje disjunktna (u,v)-puta ova: $[(u,x)$-dio od $P] \cup [(x,v)$-dio od $P']$ i $Q \cup wv$ (v. sl.)

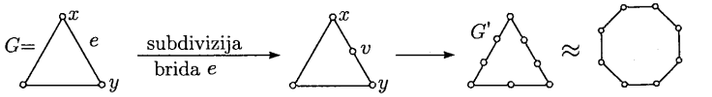


Iz ovoga je dokaza također jasno da je G 2-povezan ako i samo ako su svaka dva vrha na zajedničkom ciklusu. □

Povezan graf bez reznih vrhova još se naziva **blok**. Blok s barem tri vrha je 2-povezan, i obrnuto. **Blok grafa** je podgraf koji je blok i maksimalan je s obzirom na to svojstvo. Očito je svaki graf disjunktna unija svojih blokova.

[13] Karl Menger (1902 – 1985), austrijski matematičar.
[14] Hassler Whitney (1907 – 1986), američki matematičar.

Uvedimo sada operaciju subdivizije brida i grafa. **Subdivizija brida** $e = xy$ grafa je zamjena brida e s putom $P = xvy$, gdje je v novi vrh. Drugim riječima, subdivizija brida je umetanje novog vrha (stupnja 2) na tom bridu. **Subdivizija grafa** G je graf G' dobiven iz G rekurzivnim subdivizijama bridova. Na primjer,



G' je jedna subdivizija od G.

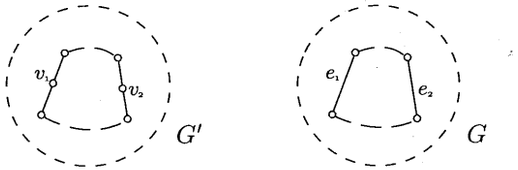
LEMA 8. *Graf G je 2-povezan ako i samo ako je bilo koja subdivizija G' 2-povezana. Drugim riječima, klasa blokova s barem tri vrha je zatvorena s obzirom na operaciju subdivizije.*

Dokaz. Neka je G'_e graf dobiven iz G subdivizijom brida $e = xy$. Dovoljno je dokazati da je G'_e 2-povezan ako i samo ako je G 2-povezan. No, očito je da je $G - v$ povezan ako i samo ako je $G'_e - v$ 2-povezan, za svako $v \in V(G)$. Dakle, ako je G'_e 2-povezan, onda je to i G. Obrnuto, ako je G 2-povezan, a G'_e dobivan umetanjem vrha v na e, onda je $G - e$ povezan, pa je $G'_e - v$ povezan. □

Sada kao posljedicu Whitneyevog teorema imamo sljedeće.

KOROLAR 14. *Svaka dva brida u 2-povezanom grafu s barem tri vrha (tj. u bloku) su na zajedničkom ciklusu.*

Dokaz. Neka su $e_1, e_2 \in E(G)$ subdividirani s novim vrhovima v_1 i v_2 redom. Tako dobiveni graf G' je prema Lemi 8 blok s barem 5 vrhova, pa je 2-povezan. Iza primjedbe nakon dokaza Whitneyevog teorema slijedi da su v_1 i v_2 na zajedničkom ciklusu (v. sl.).



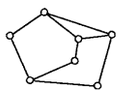
□

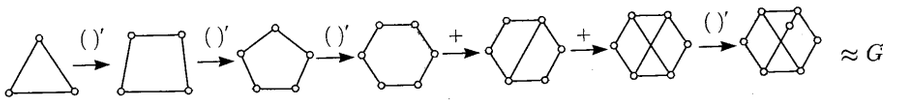
Pokažimo sada da se svaki 2-povezani graf (s ≥ 3 vrha, tj. blok) može izgraditi iz trokuta redom dodajući bridove na postojeće vrhove (ne i petlje) i subdividirajući bridove. Točnije, vrijedi

PROPOZICIJA 14. *Graf G bez petlji s barem 3 vrha je 2-povezan ako i samo ako se G može dobiti nizom dodavanja i subdividiranja bridova (u bilo kojem redoslijedu), počevši s trokutom (ili ciklusom).*

Prije dokaza, evo jednog vizualnog primjera. Operaciju dodavanja brida ćemo označiti s $+$, a subdividiranje brida sa $(\ )'$.

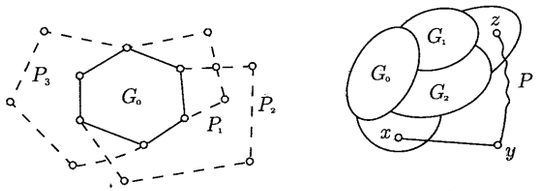
Primjer 34.





Dokaz. Očito je svaki graf dobiven na ovaj način iz trokuta C_3 2 povezan zbog Leme 8. Treba još dokazati da se svaki 2-povezani graf (bez petlji i barem tri vrha) može dobiti na taj način.

Prvo, očito da svaki ciklus (s barem tri vrha) možemo dobiti subdividiranjem trokuta. Zato ćemo odmah početi s nekim ciklusom. Neka je, dakle, G graf kao u Propoziciji, a $G_0 \subseteq G$ neki ciklus s barem 3 vrha (zašto postoji?). Pretpostavimo da je G_{i-1} već konstruiran. Neka je G_i dobiven iz G_{i-1} dodavanjem puta P_i koji spaja dva vrha iz G_{i-1}, i koji je unutarnje disjunktan s G_{i-1}. Na taj rekurzivni način mi dodajemo "uha" postojećem grafu G_{i-1} (stoga se katkad ovdje govori o "**ušnom rastavu**" - engl. *ear decomposition*):



Uočimo da se dodavanje takvih putova može izvesti nizom dodavanja i subdividiranja bridova (uvjerite se u to). Stoga treba još samo pokazati da se svaki 2-povezani graf G može dobiti dodavanjem "ušiju".

U tu svrhu, počnimo s bilo koji ciklusom $G_0 \subseteq G$. Pretpostavimo da su $G_0, G_1, \ldots, G_i$ već konstruirani. Ako je $G_i = G$, dokaz je gotov, pa pretpostavimo da je $E(G_i) \neq E(G)$. Kako je G povezan, postoji $e \in E(G) \setminus E(G_i)$, tako da je $e \cap V(G_i) \neq \emptyset$. Ako oba vrha od e leže u $V(G_i) =: V_i$, stavimo $G_{i+1} = G_i + e$. U protivnome, neka je $e = xy$, $x \in V_i$, $y \notin V_i$, te promotrimo povezani graf $G - x$ (taj je povezan, jer je G 2-povezan). Tada postoji (y,z)-put P za neko $z \in V_i$, tako da je P unutarnje disjunktan s G_i (P možemo uzeti da je najkraći put od y do $V_i(G)$ u $G - x$). Tada definiramo G_{i+1} dodavanjem brida e i puta P na G_i, tj. $G_{i+1} = G_i \cup e \cup P$. □

Slični "ušni rastav" može se provesti i za 2-bridno povezane grafove (i digrafove).

Primjer 35. Neka je G jednostavan povezan graf s n vrhova.

a) Dokažite da je $\kappa(G) \leq \delta(G) \leq \lfloor 2e(G)/n \rfloor$;

b) Ako je $\delta(G) \geq \lfloor n/2 \rfloor$, dokažite da je $\kappa'(G) = \delta(G)$.

Rješenje. a) Znamo već da je $\kappa \leq \kappa'$, a $\kappa' \leq \delta$, jer svi bridovi incidentni s vrhom stupnja δ čine δ-bridni rez od G. Iz $\delta n \leq \sum_{v \in V(G)} d(v) = 2e(G)$ slijedi i zadnja nejednakost.

b) G je povezan, pa je $\kappa' > 0$ i zbog a) je $\kappa' \leq \delta$. Pretpostavimo da je $\kappa' < \delta$. Tada postoji bridni rez $R = [S, \bar{S}]$, $\kappa' = |R| < \delta$. Neka su bridovi iz R incidentni s ukupno p vrhova iz S i q vrhova iz $\bar{S}$. Kad bi bilo $|S| \leq p$ (tj. $|S| = p$), onda bi svaki vrh iz S bio kraj bar jednog brida od R. Neka je $G_1 := G[S]$. Tada je

$$e(G_1) \geq (p\delta - \kappa')/2 > (p\delta - \delta)/2 = \delta(p-1)/2 > p(p-1)/2,$$

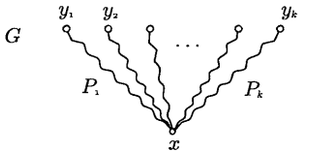
zbog $\delta > \kappa' \geq p$. To je kontradikcija jer jednostavni graf s p vrhova ima $\leq p(p-1)/2$ bridova. Zato je $|S| > p$. Analogno je $|\bar{S}| > q$. Stoga u S i $\bar{S}$ postoje vrhovi susjedni samo vrhovima iz S i $\bar{S}$ redom. No, iz $|S|, |\bar{S}| \geq \delta + 1$, slijedi $n \geq 2\delta + 2 \geq 2\lfloor n/2 \rfloor + 2 > n$, kontradikcija. Dakle je $\kappa' = \delta$. □

Nije teško pokazati (učinite to sami) da se Mengerov teorem može iskazati u sljedećem obliku, poznatom kao "lema o lepezi".

LEMA (o lepezi). *Neka je G k-povezan graf, $k \geq 1$, $x \in V(G)$, a $Y \subseteq V(G)$, $|Y| \geq k$, $x \notin Y$. Tada postoje (različiti) vrhovi $y_1, y_2, \ldots, y_k \in Y$ i unutarnje disjunktni putovi $P_1, P_2, \ldots, P_k$, tako da vrijedi*

(i) P_i je (x, y_i)-put, za $1 \leq i \leq k$;

(ii) $V(P_i) \cap Y = \{y_i\}$, za $1 \leq i \leq k$.



Primjer 36. Neka je G k-povezan graf, $k \geq 2$, a $S \subseteq V(G)$ skup od k vrhova. Tada G sadrži ciklus C koji sadrži sve vrhove iz S. Dokažite.

Rješenje. Indukcijom po k. Za $k = 2$ to slijedi iz Whitneyevog teorema. Pretpostavimo da tvrdnja vrijedi za sve $k < n$, gdje je $n \geq 3$. Neka je G n-povezan graf, a $S \subseteq V(G)$ n-člani skup i neka je $x \in S$. Promotrimo skup $S' = S \setminus \{x\}$. To je $(n-1)$-člani skup vrhova u n-povezanom grafu, pa po pretpostavci indukcije postoji ciklus C' u G koji sadrži sve točke iz S'. Ako je $x \in V(C')$, nemamo više što dokazivati (naime $C := C'$), pa uzmimo da $x \notin V(C')$. Vrhovi iz S' particioniraju C' u $n-1$ segmenata. Razlikujemo dva slučaja. Ako je duljina od C' barem n, primijenimo lemu o lepezi s $k := n$ i $Y := V(C')$. Po Dirichletovom principu dva od putova dobivanih iz leme, recimo P_i, P_j, moraju imati kraj u vrhovima y_i, y_j, koji leže u istom segmentu od C'. Sada ciklus C dobijemo iz C' tako da (y_i, y_j)-segment iz C' zamijenimo s (y_i, y_j)-putom $P_i P_j^{-1}$. Ako je pak C' duljine $n-1$, onda primijenimo lemu o lepezi za $k := n-1$ i $Y := V(C')$ i postupimo na isti način kao u prethodnom slučaju. □

Još jedan važan parametar grafa je stabilnost ili nezavisnost. Skup vrhova S grafa G je **stabilan** ili **nezavisan** ako nikoja dva vrha iz S nisu susjedna. Maksimalni kardinalni broj nekog nezavisnog skupa u G zove se **stabilnost** (ili **nezavisnost**) grafa G i obilježava se s $\alpha(G)$. Određivanje tog broja je **NP**-potpun problem. Razmatranje s povezanošću grafova završimo s jednim važnim teoremom koji veže povezanost, stabilnost i hamiltonijalnost. Dokaz (metodom najduljeg ciklusa) nije odveć težak, ali ga izostavljamo.

TEOREM (Chvátal-Erdös, 1972). *Neka je G graf s bar tri vrha, tako da njegova stabilnost α nije veća od njegove povezanosti κ, tj. $\alpha \leq \kappa$. Tada je G Hamiltonov graf.*

Dvije jednostavne posljedice ovog teorema su:

KOROLAR. *a) Ako je $\alpha \leq \kappa + 1$, onda G ima Hamiltonov put.*
b) Ako je G jednostavan d-regularan na $2d+1$ vrhova ($d \geq 2$), onda je G Hamiltonov.

Na kraju evo i jedne "konkretne" primjene povezanosti. Zamislimo da graf prikazuje komunikacijsku mrežu kojom su spojeni neki komunikacijski centri (čvorovi). Povezanost (ili bridna povezanost) te mreže je najmanji broj čvorova (ili njihovih veza, tj. bridova) čiji je kvar opasnost za daljnju komunikaciju u cijelome sustavu. Što je veća povezanost (ili bridna povezanost), veća je i pouzdanost mreže. S tog gledišta, stablo je vrlo nepouzdano, a potpun graf vrlo pouzdana mreža. No, spojiti izravno svaka dva centra je skupo i neefikasno. Stoga se nameće sljedeći problem.

Problem konstrukcije pouzdane komunikacijske mreže. Zadan je težinski graf G na n vrhova i prirodni broj k. Treba odrediti neki k-povezani razapinjući podgraf od G minimalne težine. Drugim riječima, kako treba najjeftinije umrežiti zadane komunikacijske centre ako znamo cijene izravnih veza i želimo imati unaprijed zadanu pouzdanost mreže?

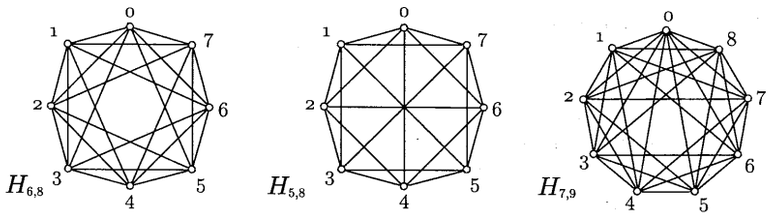
Općenito, ovaj teški problem još nije riješen za $k > 1$, ali ćemo ga mi riješiti u posebnom slučaju kada su težine svih bridova jednake (možemo uzeti da su jednake 1). Neka je, dakle, G graf na n vrhova. Tada je k-povezani razapinjući podgraf od G minimalne težine onaj razapinjući k-povezani podgraf koji ima minimalni broj bridova. Označimo s $f(n,k)$ najmanji broj bridova koje mora imati k-povezani graf s n vrhova (jasno $k < n$). Očito mora biti $2f(n,k) = \sum_{v \in V} d(v) \geq \delta n \geq kn$ (zbog $\kappa \leq \delta$), pa je

$$f(k,n) \geq \left\lceil \frac{kn}{2} \right\rceil . \qquad (*)$$

Sada ćemo konstruirati jedan k-povezani graf s n vrhova i točno $\lceil kn/2 \rceil$ bridova i time pokazati da u $(*)$ vrijedi jednakost.

Primjer 37 (F. Harary, 1962.). Postoji k-povezan graf $H_{k,n}$ s n vrhova i $\lceil kn/2 \rceil$ bridova.

Dokaz. Konstrukcija grafa $H_{k,n}$ ovisi o parnosti od k i n. Neka je prvo k paran, recimo $k = 2r$. Vrhovi od $H_{2r,n}$ su $0, 1, \ldots, n-1$, a dva vrha su spojena bridom ovako: $i \sim j \iff |i-j| \leq r \iff i - r \leq j \leq i + r$ (tu je zbrajanje mod n). Na sl. a) je prikazan $H_{6,8}$. Ako je k neparan, $k = 2r+1$, a n paran, onda se $H_{2r+1,n}$ konstruira tako da se prvo nacrta $H_{2r,n}$, i još dodaju bridovi koji spajaju vrh i s $i + n/2 \pmod n$, $0 \leq i \leq n/2$. Na sl. b) je $H_{5,8}$. Ako su k i n neparni, $k = 2r+1$, onda se $H_{2r+1,n}$ dobije iz $H_{2r,n}$ tako da se još spoje vrh 0 s $(n-1)/2$ i $(n+1)/2$, a vrh i s vrhom $i + (n+1)/2$, za $1 \leq i \leq (n-1)/2$. Na sl. c) je $H_{7,9}$. Lako je provjeriti da je doista $e(H_{k,n}) = \lceil kn/2 \rceil$.



Dokažimo da je $H_{k,n}$ k-povezan, tj. $\kappa(H_k, n) = k$. Razmotrimo prvo slučaj $k = 2r$ i pokažimo da $H_{2r,n}$ nema vršni rez s manje od $2r$ članova. Zbog simetričnosti od $H_{2r,n}$, dosta je pokazati da ako izbacimo manje od $2r$ vrhova, još uvijek možemo putom spojiti vrhove 0 i p za $p = 0, 1, \ldots, n-1$. Uzmimo da smo izbacili $2r-1$ vrhova, tj. neka je $S = \{i_1, i_2, \ldots, i_{2r-1}\}$ $(2r-1)$-vršni rez tako da su 0 i p u različitim komponentama od $H_{2r,n} - S$. Jedan od segmenata $[0,p]$ ili $[p,n]$ sadrži najviše $r-1$ vrhova iz S. Neka je to $[0,p]$. Tada očito postoji niz različitih vrhova iz $[0,p] \setminus S$ koji počinje s 0 i završava s p, tako da je razlika susjednih članova $\leq r$. No takav je niz jedan $(0,p)$-put u $H_{2r,n} - S$, što je suprotno tome da su 0 i p birani u raznim komponentama. Dakle, $H_{2r,n}$ je $2r$-povezan. Drugi se slučajevi dokazuju slično. Prema tome je $\kappa(H_{k,n}) = k$. Zbog $\kappa \leq \kappa'$ slijedi da je $H_{k,n}$ i bridno k-povezan.

Zaključno, ako je izgradnja izravne veze između svakih dvaju od n komunikacijska centra jednake cijene, i ako želimo imati zadanu pouzdanost k mreže, onda je najjeftinije izgraditi mrežu $H_{k,n}$. □

§ 5. Bojenje grafova i kromatski broj

Neka je G graf, a $k \in \mathbb{N}$ zadan broj. Tada je **k-bojenje vrhova** od G funkcija $c : V(G) \to \{1, 2, \ldots, k\}$ (ili $c : V(G) \to C$, $|C| = k$) koja svakom vrhu pridruži jednu od k boja. Ako je $c(v) = i$, kažemo da je vrh v **obojen** bojom i. Bojenje c je **pravilno** ako su susjedni vrhovi različito obojeni, tj. $u \sim v \Rightarrow c(u) \neq c(v)$. Pravilno k-bojenje grafa bez petlji je rastav $(C_1, C_2, \ldots, C_k)$ od $V(G)$ na k disjunktnih skupova $C_i = \{v \in V(G) \mid c(v) = i\}$ (mogu biti i prazni) i koji su nezavisni (sjetimo se, $S \subseteq V(G)$ je nezavisan ako nema susjednih vrhova u S). Uočimo da samo grafovi bez petlji dopuštaju pravilno bojenje. Zato ćemo ovdje razmatrati samo grafove bez petlji. Graf je **k-obojiv** ako dopušta pravilno k-bojenje. Jasno je da je G k-obojiv ako i samo ako je pripadni jednostavni graf k-obojiv, pa ćemo se nadalje ograničiti samo na jednostavne grafove.

Graf je 1-obojiv ako i samo ako je prazan (tj. $E(G) = \emptyset$), a 2-obojiv ako i samo ako je bipartitan. Stoga se 2-obojivost može ustanoviti u polinomskom vremenu. Je li graf k-obojiv za $k \geq 3$ je **NP**-potpun problem.

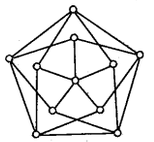
Kromatski broj $\gamma(G)$ grafa G je najmanji broj $k \in \mathbb{N}$, tako da je G k-obojiv. G je **k-kromatski** ako je $\gamma(G) = k$, a **k-kritičan** ako je k-kromatski, a $\gamma(G - v) < k$, $\forall v \in V(G)$. **Kromatski broj digrafa** D je kromatski broj pripadnog grafa $G(D)$.

Analogno se definira i bridno bojenje grafa (bez petlji). **Bridno k-bojenje** grafa G je pridruživanje $c : E(G) \to \{1, 2, \ldots, k\}$, a **pravilno bridno k-bojenje** je

takvo kod kojeg su incidentni bridovi različito obojeni. **Bridno kromatski broj** $\gamma'(G)$ grafa G (bez petlji) je najmanji broj $k \in \mathbb{N}$, za koji postoji pravilno bridno k-bojenje od G. Graf je 1-bridno obojiv ako i samo ako su mu svaka dva brida disjunktna, a ako je G bipartitan, onda je jasno da je $\gamma'(G) \geq \Delta(G)$ (maksimalni stupanj), zapravo je $\gamma'(G) = \Delta(G)$ i stoga se to može ustanoviti u polinomskom vremenu. Za $k \geq 3$, problem je li graf k-bridno obojiv je **NP**-potpun problem.

Izračunajmo kromatski i bridno-kromatski broj nekih grafova.

Primjer 38. Izračunajte γ i γ' sljedećih grafova
a) puta P_n; b) ciklusa C_n; c) K_n; d)$K_{m,n}$; e) Petersonov graf P
f) **Grötzschov graf** G na slici.



Rješenje. Svatko se lako može uvjeriti, pazeći da "uštedi" što više boja, da vrijedi sljedeće:

a) $\gamma(P_n) = \gamma'(P_n) = 2$, $n > 1$.

b) $\gamma(C_n) = \gamma'(C_n) = 2$ za n paran, a $\gamma(C_n) = \gamma'(C_n) = 3$ za n neparan.

c) $\gamma(K_n) = n$, a $\gamma'(K_n) = n - 1$, za n paran, $\gamma'(K_n) = n$, za n neparan.

d) $\gamma(K_{m,n}) = 2$, a $\gamma'(K_{m,n}) = \max\{m, n\}$.

e) $\gamma(P) = 3$, $\gamma'(P) = 4$.

f) $\gamma(G) = 4$. Ustvari je Grötzschov graf 4-kritičan; $\gamma'(G) = 5$.

□

Neke osnovne činjenice smo skupili u sljedećoj Propoziciji.

PROPOZICIJA 15. *a) Ako je G k-kritičan graf, onda je minimalni stupanj $\delta \geq k + 1$;*

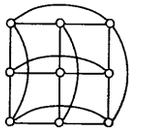
b) Ako je G k-kromatski graf, onda barem k vrhova od G ima stupanj $\geq k - 1$;

c) Za svaki graf je $\gamma \leq \Delta + 1$ (Δ je maksimalni stupanj).

Dokaz. a) Pretpostavimo da je $\delta < k - 1$ i neka je v vrh s minimalnim stupnjem, tj. $d(v) = \delta$. Kako je G k-kritičan, slijedi da je $G - v$ $(k-1)$-obojiv, pa neka je $(C_1, \ldots, C_{k-1})$ jedno $(k-1)$-bojenje od $G - v$. Tada je v susjedan s $\delta < k - 1$ vrhova u G, pa prema Dirichletovom principu v mora biti susjedan sa svim vrhovima nekog C_j. No tada je $(C_1, C_2, \ldots, C_j \cup \{v\}, \ldots, C_{k-1})$ jedno $(k-1)$-bojenje od G, što je kontradikcija s tim da je $\gamma(G) = k$. Stoga je $\delta \geq k - 1$.
b) Neka je G k-kromatski, a $H \subseteq G$ k-kritični podgraf od G. Iz a) slijedi da je svaki vrh u H stupnja $\geq k - 1$ u H, pa stoga i u G. Kako je H k-kromatski, slijedi da je $v(H) \geq k$, pa tvrdnja slijedi.
c) Iz b) imamo da ako je $\gamma(G) = k$, onda postoji barem k vrhova $v_1, \ldots, v_k$ tako da je $\Delta \geq d(v_1), \ldots, d(v_k) \geq k - 1$, pa je $\gamma \leq \Delta + 1$. Možemo i ovako zaključivati. Ako

redom bojimo vrhove grafa (u nekom poretku) pazeći da "uštedimo" što više boja, tj. tako da svaki vrh obojimo s što manjom od boja $1, 2, 3, \ldots$, dobivamo bojenje s $\leq \Delta + 1$ boja, pa je $\gamma \leq \Delta + 1$. □

Mnoga vršna i bridna svojstva grafa su dualna u sljedećem smislu. Ako je G graf, onda je **linijski graf** $L(G)$ od G definiran ovako. Vrhovi od $L(G)$ su bridovi od G, tj. $V(L(G)) = E(G)$, a dva vrha u $L(G)$ su spojena ako i samo ako su odgovarajući bridovi u G incidentni. Tako je npr. $L(C_n) \approx C_n$, $L(K_4) \approx$ graf oktaedra, a graf $L(K_{m,n})$ ima za vrhove kvadratnu rešetku $n \times n$, a dva su vrha susjedna ako i samo ako su u istom retku ili istom stupcu, npr.:

$L(K_{3,3}) \approx$ 

PROPOZICIJA 16. *Vrijede sljedeća svojstva linijskog grafa $L(G)$ jednostavnog grafa G.*

a) $L(G)$ ima $e(G)$ vrhova i $\sum_{v \in V(G)} \binom{d_G(v)}{2}$ bridova;

b) Ako je G Eulerov, onda je $L(G)$ i Eulerov i Hamiltonov, a ako je G Hamiltonov, onda je i $L(G)$ Hamiltonov (obrati ne vrijede);

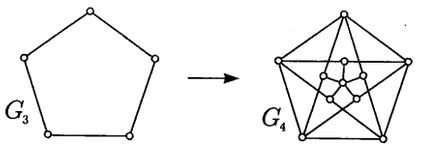
c) $\kappa'(G) = \kappa(L(G))$;

d) $\gamma'(G) = \gamma(L(G))$.

Dokaz je jednostavan i prepuštamo ga čitatelju. Evo jednog primjera konstrukcije k-kromatskog grafa bez trokuta.

Primjer 39. Dokažite da za svako k postoji graf G_k takav da je $\gamma(G_k) = k$, a $G_k \not\supseteq K_3$.

Rješenje. Za $k = 1, k = 2$ tvrdnja je trivijalna. Pretpostavimo induktivno da smo konstruirali $G_1, G_2, \ldots, G_{k-1}$ i uzmimo njihove disjunktne kopije. Neka je V skup od $|V(G_1)| \cdot |V(G_2)| \ldots |V(G_{k-1})|$ novih vrhova dobivenih odabirom po jednog vrha iz svakog $G_1, \ldots, G_{k-1}$. Tada se G_k dobiva iz $G_1, \ldots, G_{k-1}$ i V tako da se svaki vrh iz V spoji s odgovarajućim skupom od $k - 1$ vrhova, po jedan iz svakog G_i. Očito je G_k k-obojiv. Pretpostavimo da je G_k $(k-1)$-obojiv. Tada bi u G_1 postojao vrh x_1 boje i_1, u G_2 vrh x_2 boje $i_2 \neq i_1$, u G_3 vrh x_3 boje $i_3 \neq i_1, i_2$ itd. Vrh $v \in V$ koji je spojen s $x_1, x_2, \ldots, x_{k-1}$ tada bi bio spojen s vrhovima svih boja $(k-1)$-bojenja, što je kontradikcija. Dakle, $\gamma(G_k) = k$. Također je očito da $G_k \not\supseteq K_3$. Tako npr. za $k = 4$, ako je $G_3 = C_5$ ($\gamma(G_3) = 3$), onda se za G_4 dobiva jedan od **grafova Mycielskog** (ovdje je to Grötzschov graf):



□

A sada, dvije "konkretne" primjene kromatskog broja.

Primjer 40. a) *Problem rasporeda ispita.* Na kraju semestra studenti polažu ispite. Za svaki je ispit samo jedan termin u ispitnom roku. Koji je najmanji broj termina tako da ne bude kolizije? (Kolizija nastaje kada neki student mora istodobno polagati dva različita ispita u nekom terminu.)
b) *Problem skladištenja kemikalija.* Treba uskladištiti n različitih kemikalija $K_1, K_2, \ldots, K_n$. Pritom parovi inkompatibilnih kemikalija u neposrednoj blizini mogu izazvati eksploziju. Stoga kemikalije treba uskladištiti u odjeljke tako da inkompatibilne kemikalije budu u različitim odjeljcima. Koji je najmanji broj odjeljaka potreban da (zbog ovih razloga) ne dođe do eksplozije?

Rješenje. a) Neka je S skup svih studenata, a I skup svih ispita. Za svaki ispit $x \in I$, neka je S_x skup svih studenata koji polažu ispit x. Dva se ispita x i y moraju održati u različitim terminima $\iff S_x \cap S_y \neq \emptyset$. Sada konstruirajmo graf G čiji je skup vrhova $V(G) = I$, a dva vrha $x, y \in I$ spojimo bridom ako i samo ako se pripadni podskupovi S_x, S_y sijeku, tj. $x \sim y \iff S_x \cap S_y \neq \emptyset$ (to je tzv. **presječni graf** familije podskupova $(S_x)_{x \in I}$ od S). Očito je da bojenje grafa G s k boja odgovara rasporedu ispita u k-termina bez kolizije, jer se svi ispiti obojeni istom bojom mogu održati u istom terminu. Stoga je najmanji broj termina bez kolizija jednak kromatskom broju $\gamma(G)$ grafa G.
b) Slično postupimo i ovdje. Konstruiramo "graf inkompatibilnosti" G, čiji je skup vrhova $V(G) = \{K_1, K_2, \ldots, K_n\}$, a K_i, K_j spojimo bridom ako i samo ako su K_i, K_j inkompatibilne. Tada je najmanji broj odjeljaka u koje treba uskladištiti kemikalije a da se time ne izazove ekspozija jednak kromatskom broju $\gamma(G)$ grafa G. □

Kako smo već rekli, točno računanje kromatskog broja je teško. No, postoje relativno dobro gornje i donje međe. Gornja međa $\gamma \leq \Delta + 1$ katkad je jako loša, kao npr. za bipartitan graf je $\gamma = 2$, a Δ može biti po bolji velik. S druge strane, znamo da je za potpun graf i neparni ciklus $\gamma = \Delta + 1$. Brooksov teorem kaže da su to i jedini takvi grafovi.

TEOREM 14 (R. Brooks, 1941.). *Za svaki graf G je $\gamma(G) \leq \Delta(G) + 1$. Ako je $\Delta(G) = 2$, onda vrijedi jednakost ako i samo ako je neka komponenta od G neparni ciklus. Ako je $\Delta(G) \neq 2$, onda jednakost vrijedi ako i samo ako je neka komponenta od G potpun graf na $\Delta(G) + 1$ vrhova.*

Ekvivalentno: za jednostavni povezan graf G koji nije potpun niti je neparni ciklus vrijedi $\gamma(G) \leq \Delta(G)$.

Dokaz. Ako je $\Delta(G) = 1$, teorem je očit, a za $\Delta(G) = 2$ slijedi iz Propozicije 5. Stoga treba samo dokazati da ako je $\Delta(G) \leq k$ i $G \not\supseteq K_{k+1}$, za neko $k \geq 3$, da je onda G k-obojiv. To ćemo dokazati indukcijom po $v(G)$. Za $v(G) \leq 4$ tvrdnja je očita.

Ako je G nepovezan ili ima rezni vrh, onda je svaki blok od G k-obojiv, pa je zato i G k-obojiv. Ako je G 2-povezan s vršnim rezom $\{x, y\}$, onda je $G = G_1 \cup G_2$, $V(G_1 \cap G_2) = \{x, y\}$, pri čemu G_1, G_2 imaju manje vrhova od G, pa su po pretpostavci indukcije G_1 i G_2 k-obojivi. Ako je $xy \in E(G)$, onda ako su boje od x i y različite, gotovi smo, a ako su iste, onda ova dva k-bojenja preimenovanjem daju k-bojenje od G. Ako $xy \notin E(G)$, onda je po indukciji $G_i' = G_i \cup xy$ k-obojiv ili jednak K_{k+1}, za $i = 1, 2$. Tada je jasno opet, G k-obojiv, osim možda ako je barem jedan od G_i', recimo $G_i' = K_{k+1}$. No, u tom slučaju oba x i y su stupnja

1 u G_2, jer je $\Delta(G) \leq k$. Tada G_2 dopušta k-bojenje u kojem su x i y iste boje, zbog $k \geq 3$. Kako je $G_1 = K_{k+1} - xy$, slijedi da se to k-bojenje može proširiti do k-bojenja od G. Stoga možemo pretpostaviti da je G 3-povezan.

Bojenjem vrhova od G u nekom poretku tako da svaki vrh obojimo najmanjom od boja $1, 2, 3, \ldots$, dobit ćemo jedno $(k+1)$-bojenje od G. Ako pritom vrh x obojimo bojom $k + 1$, onda je $d(x) = k$, pa k susjeda od x imaju boje $1, 2, \ldots, k$. U tom slučaju možemo x prebojiti nekom bojom i, te prebojiti jedinog susjeda od x boje i jednom od boja $1, 2, \ldots, k + 1$. Na taj način možemo "pogurati" neželjenu boju $k+1$ od x nekom susjedu ili pak ona nestaje. Ako tako "poguramo" boju $k+1$ duž bilo kojeg puta $x_1 x_2 \ldots x_n$, počevši s x_1, dobivamo $(k + 1)$-bojenje od G, u kojem možda x_n ima boju $k+1$. Budući da imamo putove iz bilo kojeg vrha do x_n, slijedi da boju $k+1$ možemo "pogurati" tako da je prisutna samo u x_n. Ako je $d(x_n) < k$, onda vrh x_n možemo prebojiti tako da dobijemo k-bojenje od G. Stoga možemo pretpostaviti da su svi vrhovi od G stupnja k.

Neka su u i v nesusjedni vrhovi. Duž bilo kojeg puta do vrha v, "poguramo" boju $k + 1$ tako da je u čitavom G prisutna možda jedino kod v. U tom bojenju vrh u ima dva susjeda x i y iste boje. Kako je G 3-povezan, postoji (v, u)-put P u $G - x - y$. "Pogurnimo" boju $k + 1$ iz v duž P. Tada boja $k + 1$ ili nestaje ili završava kod vrha u. U posljednjem slučaju zbog $d(u) = k$ i zbog toga što su x i y isto obojeni, slijedi da postoji boja $i \in \{1, 2, \ldots, k\}$ kojom se može obojiti u. Na taj način dobivamo k-bojenje od G. □

Ako je x vrh za koji je $\gamma(G - x) < \gamma(G)$, onda je $d(x) \geq \gamma(G) - 1$, pa je zbog Propozicije 1, Brooksov teorem ekvivalentan sljedećem teoremu.

TEOREM 14'. *Neka je G k-kritičan graf. Tada je $\delta(G) \geq k - 1$ i $2e(G) \geq (k-1)v(G)$, s jednakošću ako i samo ako je G potpun ili neparni ciklus.*

Postoje i razne druge ograde kromatskog broja. Spomenimo

TEOREM (Hoffman-Wilf, 1970.). *Ako su $\lambda_{\min}$ i $\lambda_{\max}$ najmanja i najveća svojstvena vrijednost matrice susjedstva $A(G)$, onda je*

$$1 - (\lambda_{\max}/\lambda_{\min}) \leq \gamma(G) \leq 1 + \lambda_{\max}.$$

Mnogo je otvorenih, naizgled jednostavnih problema u vezi s bojanjima grafova, a mnogi kombinatorni problemi svode se na problem određivanja kromatskog broja. Najpoznatiji takav je bio "problem četiri boje" (sada "Teorem o 4 boje" o kojem ćemo više reći u idućoj točki), a sada ćemo ukratko opisati neke druge.

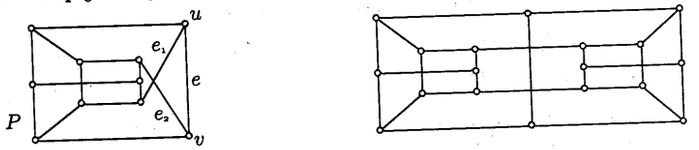
Erdös-Faber-Lovászova slutnja (1980). *Neka je G unija od najviše n potpunih grafova K_n, tako da svaka dva imaju najviše jedan zajednički vrh. Tada je G n-obojiv.*

(Erdös je svojedobno nudio 500 američkih dolara za dokaz ili obaranje ove slutnje.)

Hadwigerova[15] slutnja (1943). *Ako je G k-kromatski graf, onda se G može kontraktirati na graf koji sadrži K_k (tj. K_k je minora od G).*

Za $k = 4$, to je dokazao Dirac 1952., a 1994. su Robertson i Seymour "takoreći" dokazali tu slutnju pokazavši da u G nema izvjesnih minora, ali je općenito slutnja i dalje otvorena. Za $k = 5$, ona je ekvivalentna s teoremom o 4 boje.

Kako već znamo, Petersen je 1898. dokazao da je Petersenov graf P (najmanji) 3-bridno povezan 3-regularan graf koji nije 3-bridno obojiv ($\gamma'(P) = 4$). No, tek 1946. godine hrvatski je matematičar Blanuša[16] prvi konstruirao novi takav graf, tzv. **Blanušin graf**, ovako. Uzmimo dvije kopije od P. U prvoj se kopiji razrežu dva nesusjedna brida (npr. e_1, e_2), a u drugoj se za neki brid $e = uv$ razrežu druga dva brida ($\neq e$) incidentna s u odnosno v, te se odbace u, v i e. Sada se slobodni krajevi iz prve kopije stope na bilo koji način s onima iz druge kopije.



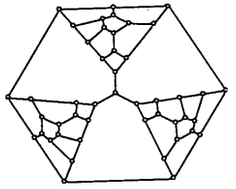
Jedan od Blanušinih grafova

(Posve asimetričan crtež Blanušinog grafa je logotip Hrvatskog matematičkog društva HMD-a.) U vezi s Blanušinim grafovima je i sljedeća čuvena slutnja.

Tutteova[17] slutnja (1966). *3-regularan 2-povezan jednostavan graf G za koji je $\gamma'(G) = \Delta(G) + 1$ sadrži subdiviziju Petersenovog grafa.*

Takvi grafovi bez bridnog reza s ≤ 3 brida osim tri brida kod istog vrha i bez ciklusa duljine ≤ 4 zovu se (engl.) "**snarks**". Petersenov graf je najmanji "snark", a Blanušin graf sljedeći. R. Isaacs je 1975. pronašao beskonačnu familiju "snarkova" (v. Amer. Math. Monthly **82**(1975), 221 – 239), a potraga za njima traje već cijelo stoljeće i nastavlja se dalje.

Tutteova slutnja povlači teorem o četiri boje. U pokušaju da dokaže tadašnju slutnju o četiri boje, Tait je još 1880. godine uzeo kao "očito" da je svaki 3-regularan, 3-povezan planaran graf Hamiltonov. No Tutte je 1946. (imajući u vidu upravo Blanušin graf) konstruirao kontraprimjer poznat kao **Tutteov graf** (v. sl.).



Spomenimo na kraju i jednu poznatu kombinatornu slutnju M. Knesera iz 1955. koju je topološkim sredstvima riješio L. Lovász 1978. Promotrimo familiju n-podskupova skupa $[n+2k] = \{1, 2, \ldots, 2n+k\}$ i definirajmo **Kneserov graf** $KG_{n,k}$ sa

[15] Hugo Hadwiger (1908 – 1981), švicarski matematičar.

[16] Danilo Blanuša (1903 – 1987), profesor na ETF-u (današnjem FER-u) i PMF-u Sveučilišta u Zagrebu. Inače se bavio specijalnim funkcijama i diferencijalno - geometrijskim aspektima smještavanja hiperboličkih u euklidske prostore.

[17] William Tutte, (r. 1917), britansko-kanadski matematičar, u vrijeme Drugog svj. rata dekodirao vojne njemačke šifre.

skupom vrhova $V(KG_{n,k})$ = svi n-člani podskupovi od $[2n+k]$, a bridom spojimo dva n-člana skupa ako i samo ako im je presjek prazan. Označimo li s C_i skup vrhova kojima je najmanji element i, onda $C_1, C_2, \ldots, C_{k+1}$, $V(KG_{n,k}) \setminus (C_1 \cup \cdots \cup C_{k+1})$ definira jedno $(k+2)$-bojenje od $KG_{n,k}$. Dakle, $\gamma(KG_{n,k}) \leq k+2$. Kneserova je slutnja bila da je $\gamma(KG_{n,k}) = k+2$. Kao primjer je $KG_{2,1}$ = Petersenov graf P. Lovász je grafu $G = (V, E)$ pridružio tzv. **kompleks susjedstva** $\mathcal{N}(G)$. To je simplicijalni kompleks čiji je skup vrhova V, a simpleksi su skupovi vrhova sa zajedničkim susjedom (tj. $A \in \mathcal{N}(G) \iff \exists v \in V$, tako da je $av \in E$, $\forall a \in A$). Rabeći Borsuk-Ulamov teorem o antipodima, Lovász je dokazao, prvo, da ako je $\mathcal{N}(G)$ $(k-1)$-povezan (kao topološki prostor), onda G nije $(k+1)$-obojiv i, drugo, da je $\mathcal{N}(KG_{n,k})$ $(k-1)$-povezan. Tako se konačno dobiva:

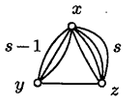
TEOREM (L. Lovász, 1978). *Ako su n-podskupovi $(2n+k)$-članog skupa particionirani u $k+1$ klasa, onda jedna klasa sadrži par disjunktnih n-skupova.*

Sličnim su tehnikama N. Alon, P. Frankl i L. Lovász 1986. to poopćili i dokazali da ako se n-podskupovi od $(tn + (t-1)k)$-članog skupa particioniraju u $k+1$ klasa, onda će jedna klasa sadržavati t međusobno disjunktnih n-podskupova.

Vratimo se na bojenje bridova grafova. Očito je uvijek $\gamma'(G) \geq \Delta(G)$, jer jednostavno obojimo sve bridove incidentne s vrhom v za koji je $d(v) = \Delta$ s Δ različitih boja. Osnovni rezultat ovdje je Vizingov teorem. Prvo nam trebaju neki pojmovi. Neka je G graf bez petlji. **Multiplicitet** $\mu = \mu(G)$ od G je maksimalni broj bridova koji spaja isti par vrhova u G.

Ako je φ neko bojenje vrhova (ili bridova) grafa G bojama $1, 2, \ldots, k$, onda se komponenta u podgrafu induciranom s vrhovima (ili bridovima) obojenim bojama i, j zove (i,j)-**Kempeov lanac**. Njegova je važnost u tome da zamjena tih dviju boja u Kempeovom lancu daje novo k-bojenje od G. Tu je zamjenu rabio Kempe već 1879. u pokušaju da riješi problem 4 boje.

s- trokut u grafu ćemo zvati trokut s vrhovima x, y, z koji ima s xz-bridova, $s-1$ xy-bridova i jedan yz-brid.



TEOREM 15 (V.G. Vizing, 1964). *Za svaki graf G s multiplicitetom $\mu(G) \geq 1$ vrijedi*

$$\Delta(G) \leq \gamma'(G) \leq \Delta(G) + \mu(G).$$

Ako je na desnoj strani jednakost, onda G sadrži $\mu(G)$-trokut (za $\mu(G) \geq 2$). Posebno, za jednostavni graf $\gamma' = \Delta$ ili $\gamma' = \Delta + 1$.

Dokaz. Lijeva nejednakost je očita. Pretpostavimo da teorem ne vrijedi. Tada postoji $s \geq 2$, tako da je $\mu(G) \leq s$, G ne sadrži s-trokut i $\gamma'(G) \geq \Delta(G) + s = \Delta + s$.

Tada G sadrži $(\Delta + s)$-bridno kritični podgraf G'. Neka je $e_0 = x_0x_1$ brid u G', a φ jedno $(\Delta + s - 1)$-bridno bojenje od $G' - e_0$. Označimo s $\overline{\varphi}(x)$ skup onih od $(\Delta + s - 1)$ boja koje nisu prisutne kod vrha x. Neka je P put u G, $P = x_0x_1 \ldots x_n$ s

bridovima $e_0 = x_0x_1$, $e_1 = x_1x_2, \ldots, e_{n-1} = x_{n-1}x_n$. Reći ćemo da je P *prihvatljiv* ako je prvi brid e_0 neobojen brid u G', a $\varphi(e_i) \in \bigcup_{j<i} \overline{\varphi}(x_j)$, za sve $i \geq 1$.

Ako je P prihvatiljiv u G' s obzirom na $(\Delta+s-1)$-bridno bojenje φ od $G'-e_0$, te ako postoje i, j, te boja β tako da je $0 \leq i < j \leq n$, a $\beta \in \overline{\varphi}(x_i) \cap \overline{\varphi}(x_j)$, onda se G' može $(\Delta+s-1)$-bridno obojiti. To ćemo dokazati dvostrukom indukcijom po j i po $j-i$. Kako je $\gamma'(G) = \Delta + s$, zaključak je da $\overline{\varphi}(x_i) \cap \overline{\varphi}(x_j)$ mora biti prazan za svaka dva vrha na prihvatljivom putu.

Ako je $j = 1$, onda je $i = 0$, pa se e_0 može obojiti bojom β i stoga φ proširiti do $(\Delta+s-1)$-bojenja od G'.

Ako je $j \geq 2$, a $j-i = 1$, onda boje β nema kod x_i i x_{i+1}. Neka je $\varphi(e_i) \in \overline{\varphi}(x_m)$ za neko $m < i$. Tada prebojimo e_i s β, čime dobivamo bojenje φ'. (x_0, x_i)-dio od P je prihvatljiv put s obzirom na φ', a $\overline{\varphi'}(x_m) \cap \overline{\varphi'}(x_i)$ sadrži boju $\varphi(e_i)$. Zbog $m < i < j$, onda tvrdnja slijedi indukcijom po j.

Promotrimo sada opći slučaj $j - i \geq 2$. Neka je $\delta \in \overline{\varphi}(x_{i+1})$. Ako je $\beta = \delta$, onda se j može zamijeniti s $i+1$, pa dokaz slijedi indukcijom po j. Ako je $\beta \neq \delta$, onda je boja β prisutna kod x_{i+1} i postoji (β, δ)-Kempeov lanac C koji počinje s x_{i+1}. Indukcijom po j možemo pretpostaviti da je boja δ prisutna kod svih vrhova $x_0, x_1, \ldots, x_i$, a β prisutna kod svih vrhova $x_0, x_1, \ldots, x_{i-1}, x_{i+1}$. Stoga nijedan od bridova $e_1, e_2, \ldots, e_i$ nije obojen s β ni δ (po definiciji prihvatljivog puta). Lanac C može, ali i ne mora završiti u x_i. U svakom od slučajeva zamijenimo boje β i δ na C čime dobivamo φ'.

Ako C ne završava u x_i, onda je put $P' = (x_0, x_{i+1})$-dio od P prihvatljiv s obzirom na φ' i $\beta \in \overline{\varphi'}(x_i) \cap \overline{\varphi'}(x_{i+1})$. Tada dokaz slijedi indukcijom po j. Ako pak C završava u x_i, onda je P prihvatljiv obzirom na φ' i $\beta \in \overline{\varphi'}(x_{i+1}) \cap \overline{\varphi'}(x_j)$. Tada dokaz slijedi indukcijom po $j-i$.

Kako smo već rekli, zaključak je da je $\overline{\varphi}(x_i) \cap \overline{\varphi}(x_j) = \emptyset$, za svaka dva vrha na svakom prihvatljivom putu. No, dokazat ćemo da to nije tako na najdužem prihvatljivom putu P. Ta kontradikcija će konačno dokazati teorem.

Ako je $\overline{\varphi}(x_i) \cap \overline{\varphi}(x_j) = \emptyset$ za $i \neq j$, onda $\sum_{0 \leq i \leq n} |\overline{\varphi}(x_i)| \geq \sum(\Delta+s-1-\Delta)+2 \geq n(s-1)+2$ različitih boja nema kod vrhova puta $P - x_n$ (dodatna dvojka se pojavljuje zato jer su x_0 i x_1 incidentni s najviše $\Delta - 1$ obojenih bridova). No svih tih $n(s-1)+2$ nedostajućih boja moraju biti prisutne kod x_n, jer bi inače $\overline{\varphi}(x_j) \cap \overline{\varphi}(x_n) \neq \emptyset$ za neko j. Kako P ima maksimalnu duljinu, slijedi da je x_n spojen s $P - x_n$ s barem $n(s-1)+2$ različita brida. No, zbog $\mu(G) \leq s$, a G nema s-trukuta, slijedi da je x_n spojen s x_0 i x_1 s najviše $2s-2$ bridova, s x_2 i x_3 s najviše $2s-2$ bridova itd. To daje $\leq n(s-1)+1$ bridova od x_n do $P - x_n$, što je kontradikcija. (Ovo je Kiersteadov dokaz iz 1984.) □

KOROLAR 15 (C. Shannon, 1949.). $\gamma'(G) \leq \frac{3}{2}\Delta(G)$.

Dokaz. Pretpostavimo da je $k = \gamma'(G) \geq \frac{3}{2}\Delta(G)$ i neka je G' k-bridno kritični podgraf od G. Iz Teorema 15 je $k \leq \Delta(G) + \mu(G)$, pa postoje dva vrha x, y spojena s $\geq \Delta(G)/2$ brida. Neka je φ jedno $(k-1)$-bridno bojenje od $G' - e$, gdje je $e = xy$. Broj boja u tom bojenju φ koje nisu prisutne kod x je $\geq (k-1) - (\Delta(G)-1) =$

$k - \Delta(G)$, i isto za y. Ali nijedna boja ne nedostaje kod oba x, y, pa je

$$2(k - \Delta(G)) + \frac{1}{2}\Delta(G) - 1 \leq k - 1 \;\Rightarrow\; k \leq \frac{3}{2}\Delta(G).$$

□

PROPOZICIJA 17. *Ako je G bipartitan graf, onda je $\gamma'(G) = \Delta(G)$.*

Dokaz. Očito je $\gamma'(G) \geq \Delta(G)$. Pretpostavimo da je $\gamma'(G) > \Delta(G)$ i neka je G' jedan $(\Delta(G)+1)$-bridno kritični podgraf od G. Neka je $e = xy \in E(G')$ i bridno obojimo $G' - e$ s $\Delta(G)$ boja. Vrh x je susjedan s $\leq \Delta(G) - 1$ obojenih bridova, pa postoji barem jedna boja α od $\Delta(G)$ boja koje nema kod x i slično postoji boja β koje nema kod y. Kad bi α i β bile iste boje, onda bi se istom bojom mogao obojiti e, što bi dalo $\Delta(G)$-bridno bojenje od G', suprotno pretpostavci. Dakle, $\alpha \neq \beta$. Stoga je boja β prisutna kod x i postoji (α, β)-Kempeov lanac C u G' koji počinje u x. Kako je G' bipartitan, a β nedostaje kod y, slijedi da y nije u C. No tada bi G' mogli $\Delta(G)$-bridno obojiti tako da zamijenimo boje α i β na bridovima iz C, a $e = xy$ obojimo bojom β. To je kontradikcija s izborom G'. □

Pomalo iznenađuje jednostavna veza kromatskog broja digrafa i duljine najduljeg diputa u digrafu.

TEOREM 16 (T. Gallai - B. Roy, 1968.). *Neka je D digraf, $\gamma = \gamma(G(D))$ kromatski broj pripadnog grafa $G(D)$, a $\lambda = \lambda(D)$ broj vrhova najduljeg diputa u D. Tada D sadrži diput duljine barem $\gamma - 1$, tj. vrijedi*

$$\gamma \leq \lambda.$$

Dokaz. Neka je D' maksimalni aciklički poddigraf od D, a λ' broj vrhova najduljeg diputa u D', te $\lambda'(v)$ broj vrhova najduljeg v-diputa u D'. Zbog $V(D) = V(D')$, slijedi da postoji λ'-bojenje c od D, definirano s $c(v) := \lambda'(v)$, za $v \in V(D')$. Pokažimo da je to pravilno bojenje od D (tj. od $G(D)$). Naime, ako je P neki (x, y)-diput u D', onda je $c(x) > c(y)$, jer ako je Q neki y-diput u D', onda je PQ neki x-diput u D' zbog acikličnosti od D'. Odavde slijedi da ako je $xy \in A(D')$, onda je $c(x) \neq c(y)$. Ako je pak $(x, y) \in A(D) \setminus A(D')$, onda zbog izbora od D' slijedi da postoji (y, x)-diput u D', pa je opet $c(x) \neq c(y)$. Prema tome, c je (pravilno) bojenje od D, pa je $\gamma \leq \lambda$. □

Neposredna posljedica ovoga je Rédeiov teorem 10, jer ako je D turnir na n vrhova, onda je $\gamma = n$.

Napomena. Gallai-Royov teorem može se reformulirati i kao formula za kromatski broj grafa pomoću duljina najduljih diputa po svim orijentacijama grafa G:

$$\gamma(G) = \min\{\lambda(\overrightarrow{G}) | \overrightarrow{G} \text{ je orijentacija od } G\}.$$

Naime, iz Gallai-Royovog teorema slijedi $\gamma(G) \leq \lambda(\overrightarrow{G})$, za svaku orijentaciju $\overrightarrow{G}$ od G, a ako je $c : V(G) \to \{1, 2, \ldots, \gamma\}$ neko γ-bojenje od G, onda orijentirajmo G tako da je $(u, v) \in A(\overrightarrow{G})$, ako je $c(u) < c(v)$.

U neku je ruku "dualni" teorem Gallai-Royovog sljedeći

TEOREM 17 (Gallai-Milgram, 1960.). *Neka je D digraf, a $\alpha = \alpha(D)$ stabilnost (ili nezavisnost) pripadnog grafa $G(D)$. Tada se D može particionirati u najviše α diputa.*

Dokaz ovog teorema neposredno slijedi iz sljedeće leme. No, prvo neke oznake. Neka je $\mathcal{D}$ particija od D u diputove, a $\alpha(\mathcal{D})$ broj vrhova u maksimalnom nezavisnom skupu od $G(D)$ čiji elementi pripadaju različitim putovima iz $\mathcal{D}$. Dalje, $p(\mathcal{D})$ neka je skup početaka diputova iz $\mathcal{D}$, a $k(\mathcal{D})$ skup krajeva diputova iz $\mathcal{D}$.

LEMA 9 (J. Bondy, 1995). *Neka je D digraf, a $\mathcal{D}$ particija od D na diputove, tako da je $|\mathcal{D}| > \alpha(\mathcal{D})$. Tada postoji particija $\mathcal{P}$ na diputove digrafa D, tako da je $|\mathcal{P}| = |\mathcal{D}| - 1$, a $k(\mathcal{P}) \subset k(\mathcal{D})$ i $p(\mathcal{P}) \subset p(\mathcal{D})$.*

Dokaz leme. Indukcijom po $v(D)$. Za $v(D) = 1$, tvrdnja je trivijalna. Neka je $\mathcal{D}$ particija od D na dipute, tako da je $|\mathcal{D}| > \alpha(\mathcal{D})$. Tada očito $k(\mathcal{D})$ nije nezavisan skup, postoje $y, z \in k(\mathcal{D})$ tako da je $(y, z) \in A(D)$. Ako je (z) (trivijalan) diput u $\mathcal{D}$, definirajmo $\mathcal{P}$ kao particiju na diputove iz D dobivenu iz $\mathcal{D}$ tako da uklonimo (z) i produljimo diputove od $\mathcal{D}$ s krajem y s lukom (y, z). Stoga možemo pretpostaviti da (z) nije diput iz $\mathcal{D}$. Neka je x neposredni prethodnik od z na diputu iz $\mathcal{D}$ s krajem u z. Neka je $D' = D - z$, a $\mathcal{D}'$ restrikcija od $\mathcal{D}$ na D'. Tada očito vrijedi $|\mathcal{D}'| = |\mathcal{D}| > \alpha(\mathcal{D}) \geq \alpha(\mathcal{D}')$, te $k(\mathcal{D}') = (k(\mathcal{D}) \setminus \{z\}) \cup \{x\}$ i $p(\mathcal{D}') = p(\mathcal{D})$. Po pretpostavci indukcije, postoji particija $\mathcal{P}'$ u diputove od D', tako da je $|\mathcal{P}'| = |\mathcal{D}'| - 1$, $k(\mathcal{P}') \subset k(\mathcal{D}')$ i $p(\mathcal{P}') \subset p(\mathcal{D}')$.

Ako je $x \in k(\mathcal{P}')$, definirajmo $\mathcal{P}$ kao particiju od D u diputove tako da svaki diput iz $\mathcal{P}'$ s krajem x produljimo lukom (x, z). Ako pak $x \notin k(\mathcal{P}')$, onda je $y \in k(\mathcal{P}')$, pa $\mathcal{P}$ definiramo kao particiju na diputove od D dobivenu iz $\mathcal{P}'$ tako da produljimo svaki diput iz $\mathcal{P}'$ s krajem u y lukom (y, z). U oba je slučaja $|\mathcal{P}| = |\mathcal{D}| - 1$, $k(\mathcal{P}) \subset k(\mathcal{D})$ i $p(\mathcal{P}) \subset p(\mathcal{D})$. □

Napomena. Gallai-Milgramov teorem se može reformulirati i kao formula za nezavisnost grafa G pomoću minimalnih brojeva diputova $\pi(\vec{G})$ u koje se orijentacija $\vec{G}$ od G može particionirati u diputove

$$\alpha(G) = \max\{\pi(\vec{G}) \mid \vec{G} \text{ je orijentacija od } \vec{G}\}.$$

Naime iz Gallai-Milgramovog teorema je $\alpha(G) \geq \pi(\vec{G})$, za svaku orijentaciju $\vec{G}$ od G, a ako G orijentiramo tako da iz svakog vrha nekog maksimalnog nezavisnog skupa u G strelice idu samo prema van, dobijemo obrnutu nejednakost.

Posljedica Gallai-Milgramovog teorema je poznati Dilworthov teorem (usp. pogl. IV, Teorem 3)

KOROLAR 16 (Dilworthov teorem, 1950.). *Neka je $(P, \leq)$ konačan parcijalno uređen skup. Tada je minimalni broj lanaca na koje se P može particionirati jednak maksimalnom broju elemenata nekog antilanca u P.*

Dokaz. Neka je $D(P)$ digraf čiji je skup vrhova P, a lukovi uređeni parovi (u, v), tako da je $u \leq v$ u P. Tada očito lanci i antilanci u P odgovaraju diputovima i

nezavisnim skupovima u $D(P)$. Gallai-Milgramov teorem povlači da postoji particija od P u lance, kojih je $\leq$ maksimalnog broja elemenata u antilancu. Obrnuta nejednakost slijedi iz toga što nikoja dva elementa antilanca ne mogu biti u nekom lancu. □

Kromatski polinomi

U proučavanju bojenja bolji uvid može se dobiti razmatrajući ne samo egzistenciju bojenja grafa sa zadanim brojem t boja, nego i broj svih t-bojenja grafa. Taj je pristup uveo Birkhoff[18] 1912., a nastavio Whitney 1932. u nastojanjima da riješe problem 4 boje.

Označimo s $P(G, t)$ broj svih različitih t-bojenja grafa G. (Jasno, dva bojenja smatramo različitim ako je neki vrh u ta dva bojenja različito obojen.) Dakle, $P(G, t) > 0$ ako i samo ako je G t-obojiv. Odnosno, $P(G, t) > 0$ za $t \geq \gamma(G)$, a $P(G, t) = 0$ za $t < \gamma(G)$. Očito je $P(K_n, t) = t(t-1)\dots(t-n+1) = t^{\underline{n}}$, a ako je $G = K_n^c$ = prazan graf na n vrhova, onda je $P(K_n^c, t) = t^n$.

Osnovna rekurzija za računanje brojeva $P(G, t)$ jest sljedeća.

PROPOZICIJA 18. *Za jednostavni graf G i svako $e \in E(G)$ vrijedi*

$$P(G, t) = P(G - e, t) - P(G/e, t).$$

Dokaz. Neka je $e = xy$. Svako t-bojenje od $G - e$ ili ima kod x i y iste boje ili različite boje. Zato bojenju od $G - e$ kod kojeg su x i y različito obojeni, pridružimo bojenje od G, a ako su isto obojeni pridružimo mu bojenje od G/e. Ovo pridruživanje je bijekcija, pa slijedi $P(G - e, t) = P(G, t) + P(G/e, t)$. □

KOROLAR 17. *Funkcija $t \mapsto P(G, t)$ grafa G s n vrhova je polinom u varijabli t stupnja n s cijelim koeficijentima. Vodeći član je t^n, konstantni član je 0, a koeficijenti alterniraju po predznaku.*

Dokaz. Indukcijom po $e(G)$. Ako je $e(G) = 0$, znamo da je tada $P(G, t) = t^n$ i tvrdnja je točna. Pretpostavimo da je tvrdnja točna za grafove s manje od m bridova i neka je G graf s n vrhova i $m \geq 1$ bridova, a $e \in E(G)$. Tada je $|E(G - e)| = |E(G/e)| = m - 1$, pa po pretpostavci indukcije postoje $a_1, a_2, \dots, a_{n-1}$, $b_2, \dots, b_{n-1} \in \mathbb{N}_0$, tako da je

$$P(G - e, t) = \sum_{i=1}^{n-1} (-1)^{n-i} a_i t^i + t^n, \quad P(G/e, t) = \sum_{i=1}^{n-2} (-1)^{n-i-1} b_i t^i + t^{n-1}.$$

Tada iz Propozicije 18 imamo

$$P(G, t) = P(G - e, t) - P(G/e, t) = \sum_{i=1}^{n-2} (-1)^{n-i} (a_i + b_i) t^i - (a_{n-1} + 1) t^{n-1} + t^n,$$

a odatle slijedi tvrdnja. □

[18] George D. Birkhoff (1884 – 1944), američki matematičar

Zbog svega ovoga se $P(G,t)$ zove **kromatski polinom grafa** G. Na isti se način kao gore pokazuje da je koeficijent uz t^{n-1} jednak $-e(G)$, a najmanji broj r tako da je koeficijent uz t^r različit od nule je broj $c(G)$ komponenti od G i, kako smo već rekli, $\gamma(G)$ je najmanji cijeli broj $t \geq 0$, za koji je $P(G,t) \neq 0$. Stoga kromatski polinom sadržava mnoge važne podatke o grafu, a gornja rekurzija ne daje polinomski algoritam za njegovo računanje. Ustvari, ne zna se neka korisna karakterizacija polinoma koji su kromatski polinomi.

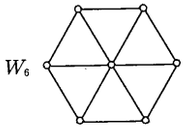
Primjer 41. a) Izračunajte kromatski polinom stabla T_n i ciklusa C_n na n vrhova, te **kotača** W_n s n žbica; $W_n = K_1 * C_n$;

b) Dokažite da kromatski polinom nema nultočaka u intervalu $\langle 0,1\rangle$.

Rješenje. a) Rabeći indukciju po n i osnovnu rekurziju iz Propozicije 18, nije se teško uvjeriti (učinite to sami) u to da je

$$P(T_n,t) = t(t-1)^{n-1}, \quad P(C_n,t) = (t-1)^n + (-1)^n(t-1).$$

Nadalje, iz definicije odmah slijedi da za spoj grafa G s K_1 (tj. jednim vrhom) vrijedi $P(G * K_1, t) = tP(G, t-1)$. Stoga dobivamo da je $P(W_n,t) = t(t-2)^n + (-1)^n t(t-2)$.



b) Ako graf G ima c komponenti povezanosti $G_1, G_2, \ldots, G_c$, jasno je da je $P(G,t) = P(G_1,t)P(G_2,t)\ldots P(G_c,t)$. Stoga je dovoljno dokazati sljedeće. Ako je G povezan graf na n vrhova, onda je $(-1)^{n-1}P(G,t) > 0$, za $t \in \langle 0,1\rangle$. Dokažimo to indukcijom po $e(G) = m$. Najmanji takav $e(G)$ je kada je $e(G) = n-1$, tj. kada je G stablo, a iz a) je $P(T_n,t) = t(t-1)^{n-1}$, pa je za stablo tvrdnja točna. Pretpostavimo da je tvrdnja točna za neko $m \geq n-1$ i neka je G povezan graf na n vrhova i $m+1$ bridova. Tada postoji brid $e \in E(G)$ tako da je $G-e$ povezan (zašto?). No, tada je G/e također povezan i ima m bridova. Stoga je po pretpostavci indukcije $(-1)^{n-1}P(G-e,t) > 0$ i $(-1)^{n-2}P(G/e,t) > 0$. Iz osnovne rekurzije tada slijedi da je i $(-1)^{n-1}P(G,t) > 0$. □

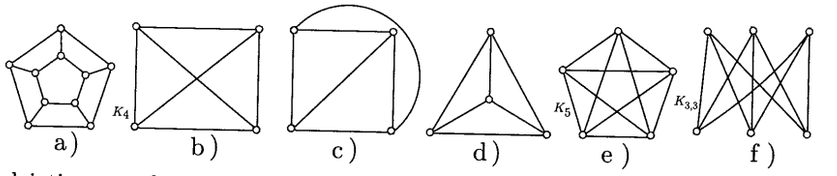
Na probleme bojenja ćemo se također još povremeno vraćati. Zainteresiranog čitatelja upućujemo na monografiju [46*].

§ 6. Planarni grafovi

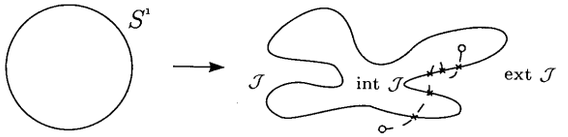
Smještavanje grafova u ravninu i druge plohe

Graf je **planaran** ako se može nacrtati (smjestiti) u ravnini $\mathbb{R}^2$ tako da mu se bridovi sijeku samo u vrhovima. Ili, kraće, graf G je planaran, ako dopušta **smještavanje u ravninu**. To znači da postoji funkcija f koja svakom vrhu od G pridružuje točku u ravnini $\mathbb{R}^2$, a svakom bridu e jednostavnu krivulju $f(e) \subset \mathbb{R}^2$ tako da se $f(e_1)$ i $f(e_2)$ sijeku u točki T ako i samo ako je $T = f(v)$, za neki vrh incidentan s e_1 i e_2 u G. Graf koji je već tako smješten u ravninu zove se **ravninski**, tj. to je uređeni par (G,f), gdje je G planarni graf, a f smještavanje od G u ravninu. Graf koji nije planaran zove se, naravno, **neplanaran**.

Tako su npr. grafovi svih pet pravilnih poliedara (tzv. Platonovih tijela) planarni; graf prizme sl. a) je ravninski; K_4 (tj. graf tetraedra) je planaran, iako na sl. b) ne izgleda tako, ali su na sl. c) i d) njegove izomorfne ravninske realizacije (smještenja), a na sl. e) i f) su K_5 i $K_{3,3}$ koji su neplanarni, što ćemo dokazati poslije.



Podsjetimo se da je **jednostavna krivulja** u ravnini slika $\alpha([0,1])$, gdje je $\alpha : [0,1] \to \mathbb{R}^2$ neprekidna, i $\alpha|_{[0,1\rangle}$ injekcija. Ako je $\alpha(0) = \alpha(1)$, onda se radi o **zatvorenoj jednostavnoj krivulji** ili **Jordanovoj** [19] **krivulji**. Ekvivalentno rečeno, Jordanova krivulja je homeomorfna slika kružnice S^1. Homeomorfizam je neprekidna bijekcija čiji je inverz također neprekidan. **Jordanov teorem o krivulji** kaže da je za svaku Jordanovu krivulju $\mathcal{J} \subset \mathbb{R}^2$, komplement $\mathbb{R}^2 \setminus \mathcal{J}$ jednak disjunktnoj uniji točno dvaju otvorenih (lukovima) povezanih skupova int $\mathcal{J}$ (unutrašnjost) i ext $\mathcal{J}$ (vanjština), pri čemu je int $\mathcal{J}$ omeđen, a ext $\mathcal{J}$ neomeđen, presjek zatvarača im je $\mathcal{J}$, tj. $\overline{\text{int}\,\mathcal{J}} \cap \overline{\text{ext}\,\mathcal{J}} = \mathcal{J}$, a svaka neprekidna krivulja s jednim krajem u int $\mathcal{J}$, a drugim u ext $\mathcal{J}$ siječe $\mathcal{J}$.



Premda je ovaj teorem intuitivno vrlo jasan, dokaz je prilično mukotrpan (za noviji dokaz vidi C. Thomassen, The Jordan - Schoenflies theorem and the classification of surfaces, Amer. Math. Monthly 99 (1992), 116 – 130).

Planarni grafovi (ili općenitije, grafovi nacrtani u ravnini s izvjesnim ograničenjima o tome kako se bridovi mogu sjeći) važni su u matematici, ali i u praksi i likovnoj umjetnosti. Na prijmer, u pitanjima egzistencije i klasifikacije popločavanja ravnine (vidi [39*]), zatim u pitanjima konstrukcije i dizajna integriranih krugova i "čipova"; tu treba znati može li se čip posve realizirati u ravnini ili, ako se ne može, da ga se realizira sa što manje presjeka bridova (spojnica), odnosno da se graf rastavi u što manje planarnih grafova (slojeva). S time su u vezi i dvije nove invarijante: grafa **presječni broj** i **debljina grafa**. Brzina rada mnogih algoritama na grafovima također u praksi jako ovisi o tome kako je graf realiziran u ravnini.

No, nije samo ravnina zanimljiv ambijentni prostor u koji se graf smještava. Analogna je definicija **smještavanja grafa** G u bilo koji **topološki prostor** X. Pišemo $G \hookrightarrow X$. S tog su gledišta mnogi prostori nezanimljivi, kao npr. $X = \mathbb{R}^3$. Naime, svaki se jednostavni graf može smjestiti u $\mathbb{R}^3$, tako da mu se bridovi sijeku samo u vrhovima i štoviše, bridovi su mu ravni segmenti. To se može postići npr. tako da vrhove smjestimo na tzv. "moment-krivulju" $\{(t,t^2,t^3) \mid t \in \mathbb{R}\}$ (dovršite

[19] Camile Jordan (1838 – 1922), francuski matematičar.

dokaz sami). Isto se tako svaki graf može smjestiti u tzv. 3-knjigu. Pritom je po definiciji, k-**knjiga** topološki prostor dobiven iz k disjunktnih kopija jediničnog kvadrata, pri čemu identificiramo po jednu stranicu iz svakog kvadrata u jednu zajedničku stranicu koja se zove hrbat k-knjige. Smještenje grafa G u 3-knjigu se može postići tako da prvo na stranici 1 naše 3-knjige nacrtamo sve vrhove od G pa potom spojimo svaki vrh v s $d_G(v)$ dužina s hrptom knjige i onda produljimo te dužine s poligonalnim crtama na stranice 2 i 3 (možemo ih smatrati pravokutnicima) i tako dobiti smještenje čitavog grafa G u 3-knjigu (detalje ostavljamo čitatelju).

Ono što jest zanimljivo jest smještavanje grafova u plohe kao što su sfera, torus, dvostruki torus, Möbiusova traka, Kleinova boca, projektivna ravnina, sfera s ručkama itd. (k-knjiga nije ploha za $k \geq 3$):

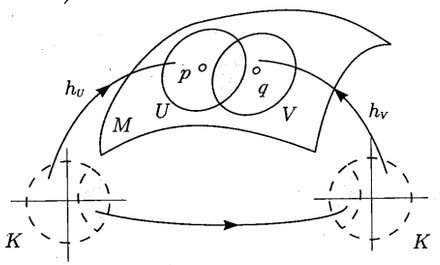


sfera torus dvostruki torus Möbiusova traka



Kleinova boca sfera s tri ručke

Kratka i precizna definicija plohe jest da je ploha (bez ruba) M 2-dimenzionalna mnogostrukost (engl. *manifold*). To znači da za svaku točku $p \in M$ postoji okolina $U \ni p$ u M i homeomorfizam h_U iz otvorenog jediničnog kruga $K \subset \mathbb{R}^2$ na U, $h_U(0) = p$. Nadalje, ako su $U \ni p$ i $V \ni q$ dva takva para, onda se na presjeku oni mogu "izravnati" ili "ispeglati" homeomorfizmom, tj. ako su $h_U : K \to U$ i $h_V : K \to V$ homeomorfizmi, onda je i kompozicija kao na slici homeomorfizam $h_U^{-1}(U \cap V) \to h_V^{-1}(U \cap V)$:



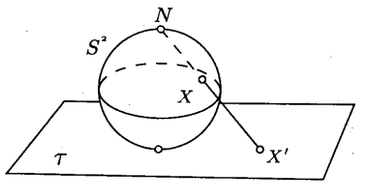
Sfera s ručkom dobije se iz sfere tako da se na sferi izbuše dvije (disjunktne kružne) rupe i na rubove kružnice onda "nalijepimo " ručku. Sfera s jednom ručkom je homeomorfna torusu, s dvije ručke dvostrukom torusu itd. S druge strane, ako na sferi izbušimo rupu i na rubnoj kružnici identificiramo antipodalne točke (ili što je isto na rubnu kružnicu "nalijepimo" Möbiusovu traku duž njezina ruba koji je kružnica), dobili smo sferu s nalijepljenom Möbiusovom trakom M. Sfera s jednom M je projektivna ravnina, s dvije Kleinova boca itd.

Teorem o klasifikaciji ploha kaže da je svaka zatvorena povezana ploha (tj.

kompaktna povezana 2-mnogostrukost bez ruba) homeomorfna ili sa sferom na koju je nalijepljeno nekoliko ručki ili sa sferom na koju je nalijepljeno nekoliko Möbiusovih traka. Kažemo da je (zatvorena) **ploha orijentabilna roda** (ili **genusa**) g ako je homeomorfna sferi s g ručki, a **neorijentabilna roda** g ako je homeomorfna sferi s g Möbiusovih traka. Sfera je ploha roda 0. Veza između planarnosti i smještavanja u sferu je sljedeća jednostavna činjenica.

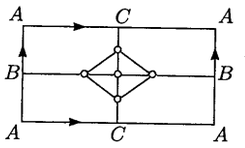
PROPOZICIJA 19. *Graf G je planaran ako i samo ako se može smjestiti na sferu S^2 (tj. plohu roda 0).*

Dokaz. Promotrimo sferu S^2, njezinu tangencijalnu ravninu τ u "južnom polu" i stereografsku projekciju sfere bez "sjevernog pola" N na ravninu τ, tj. preslikavanje $\pi_N : S^2 \setminus \{N\} \to \tau$, koje točki $X \in S^2 \setminus \{N\}$, pridružuje presjek X' pravca NX s ravninom τ. π_N je homeomorfizam.

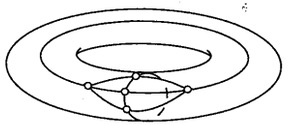


Stoga, ako je $G \hookrightarrow S^2$, onda s odgovarajućom stereografskom projekcijom dobivamo $G \hookrightarrow \mathbb{R}^2$, a s inverznim preslikavanjem dobijemo i obrat. □

Pokažimo sada i slikovno smještavanja grafova u neke plohe. Prvo, torus T se može dobiti tako da se nasuprotne stranice pravokutnika identificiraju kao na sljedećoj sl. a);



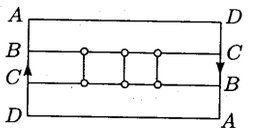
a)



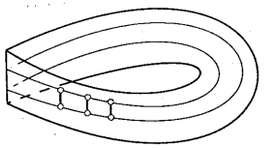
$K_5 \hookrightarrow T$

$K_5 \hookrightarrow M$ b)

točke s istim slovom su identificirane, a strelice označavaju kako su nasuprotne stranice identificirane. Na istoj je slici smješten i graf K_5. Na sl. b) je prikazana prostorna realizacija $K_5 \hookrightarrow T$. Slično je na idućoj slici prikazano smještenje $K_{3,3} \hookrightarrow M$ (Möbiusova traka):

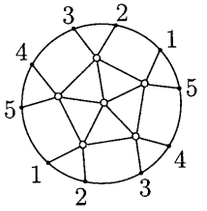


a)



$K_{3,3} \hookrightarrow M$ b)

Na realnu projektivnu ravninu $\mathbb{R}P^2$ može se gledati kao na plohu koja je homeomorfna zatvorenom krugu kojem su antipodalne (dijametralno suprotne točke) na rubnoj kružnici identificirane. Sljedeća slika pokazuje $K_6 \hookrightarrow \mathbb{R}P^2$.



Ustvari, općenito vrijedi sljedeće.

PROPOZICIJA 20. *Svaki se graf može smjestiti u neku orijentabilnu plohu, tj. u sferu s dovoljno mnogo ručki.*

Skica dokaza. Prvo nacrtamo graf G na sferi. Neka su $e_1, e_2, \ldots, e_n$ svi bridovi koji sijeku neki drugi brid. Tada umjesto svakog brida e_i dodamo (tj. nalijepimo) ručku kojom kao mostom premostimo brid s kojim se e_i siječe. Te ručke treba pažljivo konstruirati (samo blizu presjeka e_i, e_j bridova koji se sijeku) tako da budu disjunktne. Na taj način nestanu svi samopresjeci grafa, ali zato nastaje više ručki i na taj je način graf smješten na sferu s puno ručki, tako da se bridovi sijeku samo u vrhovima. □

Ako se graf G može smjestiti u (orijentabilnu) plohu roda g, a ne može se smjestiti u plohu roda $g-1$, onda kažemo da je g **rod** (ili **genus**) **grafa** G. Tako je npr. rod planarnog grafa 0, rod od K_5 jednak 1 itd.

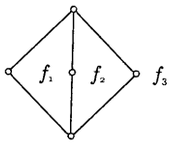
O pitanjima smještavanja grafova u plohe i topološku teoriju grafova zainteresiranog čitatelja upućujemo na knjige [96], [66*],[19*] i napose na [53*].

Eulerova formula

Vratimo se planarnim grafovima. Neka je G ravninski graf (dakle, planarni graf već smješten u ravninu $\mathbb{R}^2$). **Strana** od G je (topološki) zatvarač komponente +povezanosti komplementa $\mathbb{R}^2 \setminus G$. Brid (ili vrh) od G je **incidentan** sa stranom, ako je sadržan u toj strani. **Rub strane** čine oni bridovi koji su incidentni s tom stranom i još nekom drugom stranom. Dvije su strane **susjedne** ako imaju zajednički incidentan brid, a strana incidentna reznom bridu, susjedna je samoj sebi. Svi bridovi (i njihovi krajevi) incidentni sa stranom f čini zatvorenu šetnju u kojoj su rezni bridovi prijeđeni dvaput. Duljina te šetnje se zove **stupanj strane** f i označava s $d_G(f)$ (ili kratko $d(f)$). Ako je ta šetnja ciklus, strana je **ciklička**.

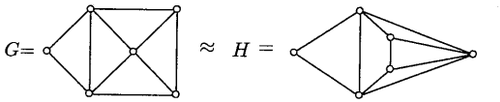
Pojam strane se slično definira i za smještavanje grafa u druge plohe. Iz Jordanovog teorema odmah vidimo da svaka ciklička strana definira svoju unutrašnjost i vanjštinu, a isto tako da svaki ravninski graf definira točno jednu neomeđenu stranu, koju još zovemo **vanjska strana**. Tako npr. ravninski graf $K_{2,3}$ nacrtan

kao na donjoj slici ima točno tri (cikličke) strane f_1, f_2, f_3 svaka stupnja 4, a njihovi rubovi su tri ciklusa. Vanjska strana je f_3.

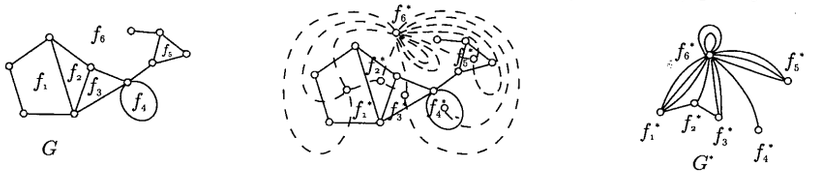


Skup svih strana ravninskog grafa G označavamo s $F(G)$, a njihov broj $f(G) := |F(G)|$.

Ravninskom grafu G na prirodni je način pridružen njegov (ravninski) **dualni graf** G^*. Vrhovi od G^* su strane od G, tj. $V(G^*) = F(G)$, a dva vrha iz G^* su spojena bridom e^* ako i samo ako su pripadne strane iz G incidentne sa zajedničkim bridom e. Time je definirana bijekcija $\varphi : E(G) \to E(G^*)$. Iz definicije je jasno da je e petlja u G ako i samo ako je e^* rezni brid u G^*. Stoga bijekcija φ ima svojstvo da je podskup $C \subseteq E(G)$ ciklus u G ako i samo ako je $\varphi(C)$ minimalni bridni rez u G^*. Nije teško pokazati da ako je G ravninski povezan graf, da je onda $(G^*)^* \approx G$. No, uočimo da ako su G i H izomorfni ravninski grafovi, onda njihovi duali G^* i H^* ne moraju biti izomorfni. Takvi su na donjoj slici.



$G^* \not\approx H^*$, jer G^* ima stranu f^* s $d(f^*) = 5$, dok H^* takvu stranu nema. Uočimo da općenito vrijedi sljedeće: $v(G^*) = f(G)$, $e(G^*) = e(G)$, i $d_{G^*}(f^*) = d_G(f)$, $\forall f \in F(G)$. Ilustrirajmo sve navedene pojmove jednim (slikovnim) primjerom.



Stupnjevi strana u G su $d(f_1) = 4$, $d(f_2) = 3$, $d(f_3) = 3$, $d(f_4) = 1$, $d(f_5) = 3$, $d(f_6) = 14$. Uzmemo li točku f_i^* u unutrašnjosti svakog područja f_i, spajanjem vrhova f_i^* prema gornjim pravilima dobivamo dualni graf G^*.

Primjer 42. Dokažite da za svaki ravninski graf G vrijedi $\sum_{f \in F(G)} d(f) = 2e(G)$.

Rješenje. To slijedi odmah primjenom Propozicije 1 na dualni graf G^*:

$$\sum_{f \in F(G)} d(f) = \sum_{f^* \in V(G^*)} d_{G^*}(f^*) = 2e(G^*) = 2e(G)..$$

□

Eulerova formula koju ćemo sada izvesti veže broj vrhova, bridova i strana ravninskog grafa i kao takva je u biti jedina formula te vrste, a i najstarija. To je klica iz koje se razvila algebarska topologija i prvi put ju je Euler spomenuo u

pismu Goldbachu 1752., a odnosila se na konveksne poliedre. Prvi je dokaz te formule dao Cauchy 1813., a znatno je poopćio Poincaré[20] 1899. (usp. pogl IV, Izlet u topologiju i geometriju)

TEOREM 18 (Eulerova formula). *Neka je G povezan ravninski graf. Tada je* **Eulerova karakteristika** *od G*

$$\chi(G) := v(G) - e(G) + f(G) = 2.$$

Dokaz I. Indukcijom po $e(G)$. Ako je $e(G) = 0$, onda je $v = 1$ i $f = 1$, pa formula vrijedi. Neka je $e(G) \geq 1$. Pretpostavimo prvo da G nema ciklusa. Tada je G stablo, pa je $v = e + 1$ (Teorem 2) i $f = 1$, jer tada imamo samo jednu neomeđenu stranu, pa formula opet vrijedi. Sada uzmimo da imamo ciklus i neka je $e \in E(G)$ brid nekog ciklusa. Tada je $G - e$ povezan (Propozicija 7), pa je po pretpostavci indukcije $\chi(G-e) = 2$. Očito je $v(G-e) = v(G)$ i $e(G-e) = e(G)-1$. No, iz Jordanovog teorema slijedi da je e incidentan s točno dvjema stranama f i f', pa nakon uklanjanja e, te se dvije strane stope u jednu stranu i stoga je $f(G-e) = f(G) - 1$. Zato imamo

$$\chi(G) = v(G)-e(G)+f(G) = v(G-e)-(v(G-e)+1)+f(G-e)+1 = \chi(G-e) = 2.$$

□

Dokaz II. Neka je $T \subseteq G$ razapinjuće stablo od G (ono postoji zbog Korolara 5). Neka je G^* dualni graf od G. Tada je i G^* povezan (i ravninski) i neka mu je T^* razapinjuće stablo. Tada je $v(G) = v(T)$, a jer je T stablo, slijedi (opet po Teoremu 2) $v(T) = e(T) + 1$, pa je $v(G) = e(T) + 1$. Sada $f(G) = v(G^*) = v(T^*) = e(T^*) + 1$. Zbrajanjem dobivamo

$$v(G) + f(G) = e(T) + 1 + e(T^*) + 1 = e(G) + 2,$$

jer imamo bijekciju $E(T^*) \to E(G) \setminus E(T)$, koja postoji jer T i T^* nemaju ciklusa, a $E(T) \cap E(T^*) = \emptyset$. (Gdje smo se u ovom dokazu prešutno pozvali na Jordanov teorem?) □

Izvedimo sada neke važne posljedice Eulerove formule. Prvo ćemo izvesti neka opća svojstva planarnih grafova.

PROPOZICIJA 21. *a) Sva ravninska smještenja danog povezanog planarnog grafa imaju isti broj strana.*

b) Jednostavni planaran graf G s $n \geq 3$ vrhova ima najviše $3n - 6$ bridova.

c) Jednostavni planaran graf G ima vrh stupnja najviše 5, tj. $\delta \leq 5$.

d) Za ravninski graf G je $\chi(G) := v(G) - e(G) + f(G) = 1 + c(G)$.

[20] Henri Poincaré (1854 – 1912), francuski matematičar

Dokaz. a) Neka su G i H dva ravninska smještenja nekog povezanog grafa. Tada je $G \approx H$, pa je $v(G) = v(H)$, $e(G) = e(H)$ pa iz Eulerove formule slijedi

$$f(G) = e(G) - v(G) + 2 = e(H) - v(H) + 2 = f(H).$$

b) Neka je prvo G povezan i neka je već smješten u ravninu, tj. neka je ravninski. Kako je G jednostavan, to je $d(f) \geq 3$, $\forall f \in F(G)$. Tada iz Primjera 42 i Eulerove formule imamo sljedeći niz zaključaka

$$2e(G) = \sum_{f \in F(G)} d(f) \Rightarrow 2e(G) \geq 3f(G) \Rightarrow 2 = v(G) - e(G) + f(G) \leq$$

$$\leq v(G) - e(G) + \frac{2}{3}e(G) = v(G) - \frac{1}{3}e(G) \Rightarrow e(G) \leq 3v(G) - 6.$$

Ako G ima k komponenti, onda zbrajanjem odgovarajućih nejednakosti za svaku komponentu tvrdnja slijedi i općenito.

Naglasimo još jednom da takav graf ima linearno mnogo bridova (tj. reda veličine $O(n)$).

c) Neka je $n = V(G)$. Ako je $n \geq 2$, to je trivijalno, a za $n \geq 3$, iz b) slijedi

$$\delta n \leq \sum_{v \in V(G)} d(v) = 2e(G) \leq 6n - 12 \;\Rightarrow\; \delta \leq 6 - \frac{12}{n} \;\Rightarrow\; \delta \leq 5.$$

d) To lako slijedi iz Eulerove formule indukcijom po broju komponenata $c(G)$. □

PROPOZICIJA 22. *Grafovi K_5 i $K_{3,3}$ su neplanarni.*

Dokaz. Kad bi K_5 bio planaran, onda bi za njegovo ravninsko smještavanje iz tvrdnje b) Propozicije 21 dobili sljedeću kontradikciju

$$10 = e(K_5) \leq 3v(K_5) - 6 = 3 \cdot 5 - 6 = 9.$$

Pretpostavimo sada da je $K_{3,3}$ planaran i neka je G pripadni ravninski graf. Kako je $K_{3,3}$ bipartitan, onda (zbog Propozicije 5) G ima samo cikluse duljine ≥ 4, pa svaka strana od G ima stupanj ≥ 4. Stoga iz Primjera 42 slijedi

$$4f(G) \leq \sum_{f \in F(G)} d_G(f) = 2e(G) = 2e(K_{3,3}) = 18 \;\Rightarrow\; f(G) \leq 4.$$

No, iz Eulerove formule tada dobivamo sljedeći apsurd

$$2 = v(G) - e(G) + f(G) \leq 6 - 9 + 4 = 1.$$

Neplanarnost od $K_{3,3}$ se na drugi način može dokazati i tako da se slično Propoziciji 21 b) prvo dokaže da jednostavni planarni graf bez trokuta ima $\leq 2n - 4$ bridova. Izvedite to sami. □

Primjer 43. Neka je G jednostavni 2-povezani planarni graf s $n \geq 3$ vrhova, a neka je n_i broj vrhova od G stupnja i, te f_i broj strana stupnja i (u nekom ravninskom smještenju od G). Tada vrijedi

$$\sum_{i\geq 1}(6-i)n_i = 12 + 2\sum_{j\geq 3}(j-3)f_j,$$

ili raspisano

$$5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 - n_7 - 2n_8 - \cdots = 12 + 2f_4 + 4f_5 + 6f_6 + \cdots.$$

Stoga je $5n_1 + 4n_2 + 3n_3 + 2n_4 + n_5 \geq 12$, pa svaki takav graf ima bar tri vrha stupnja ≤ 5 (što je poboljšanje Propozicije 21 c)).

Dokaz. Neka su n, e i f redom brojevi vrhova, bridova i strana od G. Tada je $\sum_i n_i = n$, a $\sum_j f_j = f$. Iz Eulerove formule tada slijedi

$$2e = 2(n + f - 2) = \sum_i 2n_i + \sum_j 2f_j - 4. \qquad (*)$$

Sada iz Propozicije 1 slijedi $\sum_{i\geq 1} in_i = 2e$, a zbog jednostavnosti i 2-povezanosti, svaka je strana od G neki j-ciklus, $j \geq 3$, pa iz Primjera 42 slijedi $\sum_{j\geq 3} jf_j = 2e$. Uvrštavanjem ovih izraza u $(*)$ dobivamo dvije jednakosti

$$\sum_j (j-2)f_j + 4 = \sum_i 2n_i, \qquad \sum_j 2f_j = \sum_i (i-2)n_i + 4.$$

Ako prvu pomnožimo s 2 i oduzmemo drugu, dobivamo

$$\sum_i (6-i)n_i - 4 = 2\sum_j (j-3)f_j + 8,$$

a odatle slijedi tvrdnja. □

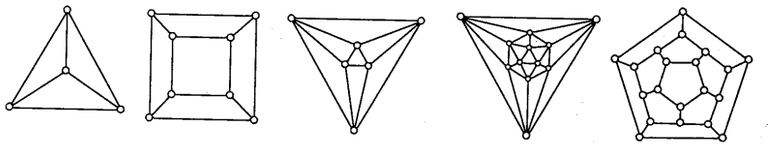
Najstarija i najpoznatija primjena Eulerove formule odnosi se na klasifikaciju pravilnih (konveksnih) poliedara. Upravo je promatrajući poliedre Euler oko 1752. došao do svoje formule i za grafove uveo pojmove "vrh", "brid" i "strana" za ravninske grafove.

Svakom je konveksnom poliedru P na prirodan način pridružen graf $G(P)$ čiji vrhovi su vrhovi poliedra, a bridovi su bridovi poliedra. $G(P)$ se zove **graf poliedra** P. Pravilni (3-dimenzionalni) poliedar P omeđen je sa sukladnim pravilnim poligonima, recimo p-terokutima, a svaki je vrh poliedra incidentan s istim brojem bridova, recimo q. Ako oko poliedra opišemo kuglu sa središtem unutar poliedra, onda ćemo radijalnom projekcijom rub poliedra, tj. graf $G(P)$, smjestiti na rubnu sferu. Na taj način dobivamo iz Propozicije 19 da je $G(P)$ planaran, pa neka je G pripadni ravninski graf. Tada je p stupanj svake strane od G, a q stupanj svakog vrha od G. Očito su $p, q \geq 3$. Ako poliedar ima n vrhova, e bridova i f strana, onda su to i odgovarajući parametri ravninskog grafa G. Iz Propozicije 1 slijedi tada da

je $qn = 2e$, a iz Primjera 42 da je $pf = 2e$. Uvrstimo li to u Eulerovu formulu, dobivamo

$$2 = n - e + f = \frac{2}{q}e - e + \frac{2}{p}e = \frac{2p + 2q - pq}{pq}e.$$

Stoga je $2p + 2q - pq > 0$, a to je ekvivalentno s $(p-2)(q-2) < 4$. Zbog $p, q \geq 3$ slijedi da su jedini parovi $(p, q) = (3,3),(3,4),(4,3)$, $(3,5)$ i $(5,3)$ i redom su to poliedri, tj. njihovi grafovi, kao na slici.



tetraedar kocka oktaedar ikozaedar dodekaedar

Dakle, do na izomorfizam (tj. izomorfizam pripadnih grafova) postoji najviše pet pravilnih poliedara, a za njihovu se egzistenciju geometrijskim konstrukcijama znalo već u starogrčkoj matematici, otkada se i zovu **Platonova tijela**. Prema tome, dokazali smo sljedeće

PROPOZICIJA 23. *Postoji točno pet pravilnih poliedara, tj. Platonovih tijela.*

Kažimo da teorije planarnih grafova i konveksnih poliedara imaju vrlo duboke veze. Općenito se i svakom d-dimenzionalnom konveksnom politopu P (tj. konveksnoj ljusci od konačno mnogo točaka u $\mathbb{R}^d$) na isti način kao za $d = 3$ pridruži **graf politopa** $G(P)$, tj. gledamo samo vrhove i bridove od P (tzv. "1-skelet"); npr. graf 4-dimenzionalnog simpleksa je K_5. Prirodno je pitanje karakterizacije grafova koji su izomorfni grafu nekog d-dimenzionalnog politopa. U dimenziji $d = 2$ to je trivijalno, jer su to ciklusi duljine ≥ 3. U dimenziji ≥ 3, odgovor je sljedeći

TEOREM (Steinitz[21], 1922). *Jednostavni graf G je graf 3-politopa ako i samo ako je G planaran i 3-povezan.*

Da je graf 3-politopa planaran i 3-povezan prilično je evidentno (projicirajte poliedar na zgodno odabranu ravninu), ali obratno, kako iz G izgraditi 3-politop P za koji je $G(P) \approx G$ prilično je mukotrpna konstrukcija vidi u [75*].

Grafovi d-politopa u svakoj dimenziji d jesu d-povezani (to je **Teorem Balinskog** iz 1961.), ali je pitanje karakterizacije grafova d-politopa za $d \geq 4$ i dalje otvoreno. Spominjemo tu i **Teorem Grünbauma i Motzkina** (1963) da graf d-politopa sadrži subdiviziju od K_{d+1}. Pravilni d-politopi su poznati u svakoj dimenziji d, ali ako samo malo oslabimo uvjete pravilnosti politopa (npr. ako ne zahtjevamo konveksnost ili akó dopustimo više vrsta strana itd.), vrlo brzo upadamo u teške kombinatorne i geometrijske probleme.

Mnogi kombinatorni ili geometrijski problemi s politopima važni su i u praksi, jer je poznato da svaki problem linearnog programiranja ima (optimalno) rješenje u vrhu pripadnog politopa. Tako je, na primjer, još otvoreno pitanje je li dijametar d-politopa (tj. dijametar pripadnog grafa) s n faceta (tj. $(d-1)$-dimenzionalnih

[21] Ernst Steinitz (1871 – 1928), njemački matematičar.

strana) najviše jednak $n - d$? Ocjena dijametra je u uskoj vezi s brojem iteracija po bridovima simpleks algoritma.

O tim i drugim pitanjima o politopima, grafovima i optimizaciji upućujemo na klasičnu knjigu Branka Grünbauma [98], te [67] i [48], a naročito na knjigu G. Zieglera [75*].

No, vratimo se primjenama Eulerove formule. Pomalo neočekivano, njezina je posljedica i Erdös-Gallai-Sylvesterov teorem (vidi pogl. I). Dokaz koji slijedi dao je N. Steenrod[22] 1944.

Primjer 44 (Erdös-Gallai-Sylvesterov teorem). Zadano je $n \geq 3$ točaka u ravnini, od kojih nisu sve na jednom pravcu. Tada postoji pravac koji sadrži točno dvije od tih točaka.

Dokaz. Prislonimo na ravninu $\mathbb{R}^2$ naše konfiguracije jediničnu sferu S^2 i stereografskom projekcijom (kao u dokazu Propozicije 19) preslikajmo našu konfiguraciju točaka iz $\mathbb{R}^2$ na S^2. Točka iz $\mathbb{R}^2$ prelazi u točku iz sfere S^2 koja je određena jediničnim vektorom v, čime je određen i par antipodalnih točaka $\pm v \in S^2$. Pritom pravci prelaze u velike kružnice na sferi. Tako taj teorem postaje ekvivalentan sljedećoj tvrdnji:

(A) *Neka je na sferi dano $n \geq 3$ parova antipodalnih točaka, koji nisu svi na jednoj velikoj kružnici. Tada postoji velika kružnica koja sadrži točno dva od danih n antipodalnih parova točaka.*

Da to dokažemo, dualizirajmo ovu sliku tako da svaki par antipodalnih točaka zamijenimo jednom velikom "ekvatorijalnom" kružnicom, tj. zamijenimo par $\pm v \in S^2$ velikom kružnicom $C_v := \{x \in S^2 \mid x \cdot v = 0\}$ ($x \cdot v$ je skalarni produkt vektora x i v).

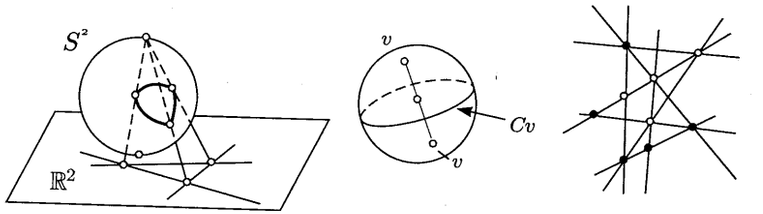
Na taj način tvrdnja (A) očito prelazi u sljedeću ekvivalentnu tvrdnju:

(B) *Neka je na sferi S^2 dano $n \geq 3$ velikih kružnica tako da ne prolaze sve istom točkom sfere. Tada postoji točka sfere u kojoj se sijeku točno dvije od tih velikih kružnica.*

Tu ćemo tvrdnju dokazati tako da konfiguraciji tih velikih kružnica pridružimo jednostavni ravninski graf G na S^2 (tj. u $\mathbb{R}^2$). Vrhovi od G su svi presjeci od po dvije velike kružnice te konfiguracije i oni dijele velike kružnice na bridove grafa G. Stupanj svakog vrha od G je očito paran broj i barem 4 (zbog konstrukcije od G). Prema Propoziciji 21 c) (a to je posljedica Eulerove formule) slijedi da postoji vrh stupnja točno 4. To dokazuje tvrdnju (B). Time smo dali i kombinatorni dokaz tog teorema (za razliku od geometrijskog dokaza iz pogl. I).

Manjom modifikacijom ovog dokaza može se dokazati i sljedeća "2-obojena" verzija tog teorema (D. Chakerian, 1970): Neka je u ravnini zadano $n \geq 3$ točaka koje su obojene bilo crvenom bilo plavom bojom, a sve točke nisu na jednom pravcu. Tada postoji "jednobojni" (ili "monokromatski") pravac, tj. pravac koji sadrži barem dvije od n točaka i koje su sve iste boje. Sličice za "vizualce":

[22] Norman Steenrod (1909 – 1970), američki matematičar.



□

Kao posljedicu Erdös-Gallai-Sylvesterovog teorema izvest ćemo još jedan važan rezultat iz geometrije incidencije i njegovo "apstraktno poopćenje".

Primjer 45. a) **(Erdös-de Bruijnov teorem, 1948.)** Neka je $\mathcal{T}$ skup od $n \geq 3$ točaka u ravnini, od kojih nisu sve na jednom pravcu. Tada skup $\mathcal{P}$ svih pravaca određenih s točkama iz $\mathcal{T}$ ima barem n pravaca.

b) Neka je X skup od $n \geq 3$ elemenata, a $A_1, A_2, \ldots, A_m$ pravi podskupovi od X, tako da je svaki par elemenata iz X sadržan u točno jednom od skupova A_i. Tada je $m \geq n$.

Rješenje. a) Indukcijom po n. Za $n = 3$ tvrdnja je trivijalna. Neka je $|\mathcal{T}| = n + 1$. Iz Erdös-Gallai-Sylvesterovog teorema slijedi da postoji pravac $p_0 \in \mathcal{P}$ koji ima samo dvije točke $P, Q \in \mathcal{T}$. Neka je $\mathcal{T}' = \mathcal{T} \setminus \{Q\}$, a $\mathcal{P}'$ skup svih pravaca određenih s točkama iz $\mathcal{T}'$. Ako točke iz $\mathcal{T}'$ nisu sve na jednom pravcu, iz induktivne pretpostavke slijedi $|\mathcal{P}'| \geq n$, pa zbog $\mathcal{P}' \cup \{p_0\} \subseteq \mathcal{P}$ slijedi $|\mathcal{P}| \geq n + 1$. Ako pak sve točke iz $\mathcal{T}'$ leže na jednom pravcu p, onda p i pravci QP, $P \in \mathcal{T}'$ definiraju točno $n + 1$ pravaca.

b) Za $x \in X$, neka je $r_x := \#\{i \in [m] \mid x \in A_i\}$, tj. r_x je broj skupova A_i koji sadrže x. Po pretpostavci je $2 \leq r_x < m$. Ako $x \notin A_i$, onda je $r_x \geq |A_i|$. Naime, $|A_i|$ skupova koji sadrže x zajedno s elementom iz A_i su različiti. Pretpostavimo suprotno, tj. $m < n$. Tada je $m|A_i| < nr_x$, pa je $m(n - |A_i|) > n(m - r_x)$ za $x \notin A_i$. Stoga imamo:

$$1 = \sum_{x \in X} \frac{1}{n} = \sum_{x \in X} \sum_{i, x \notin A_i} \frac{1}{n(m - r_x)} > \sum_{i} \sum_{x, x \notin A_i} \frac{1}{m(n - |A_i|)} = \sum_{i} \frac{1}{m} = 1,$$

što je kontradikcija. Ovaj su dokaz neovisno dali T. Motzkin i J. Conway. O konfiguracijama točaka i pravaca (učeno "aranžmanima") u ravnini i njihovoj kompleksnosti (tj. maksimalnom broju incidencija) bit će riječi poslije, usp. Szemerédi-Trotterov teorem 33.

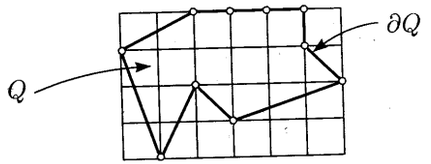
□

I sljedeća primjena Eulerove formule u geometriji je lijepa.

Primjer 46 (Pickova formula, 1899). Neka je Q jednostavni poligon u koordinatnoj ravnini s vrhovima u cjelobrojnoj rešetki. Tada je njegova površina $p(Q)$ dana formulom

$$p(Q) = N(\text{Int } Q) + \frac{1}{2} N(\partial Q) - 1,$$

gdje je $N(A)$ = broj cjelobrojnih točaka u skupu A, Int Q unutrašnjost od Q, a ∂Q rub od Q. Npr.,



$N(\text{Int } Q) = 9$
$N(\partial Q) = 10$
$p(Q) = 9 + 5 - 1 = 13.$

Dokaz. Triangulirajmo Q rabeći svih $N(\text{Int })$ i $N(\partial)$ vrhova. Ova triangulacija daje ravninski graf koji ravninu razbija na jedan neomeđeni dio i $f-1$ trokutića i neka ima $n = N(\text{Int }) + N(\partial)$ vrhova i $e = e(\text{Int }) + e(\partial)$ bridova. Lako se vidi (učinite to sami) da svaki trokutić te triangulacije (uočite da ne sadrži cjelobrojnih točaka) ima površinu $1/2$. Zato je površina $p(Q)$ jednaka

$$P(Q)\frac{1}{2}(f-1).$$

S druge strane, svaki trokutić ima tri stranice i svaka od $e(\text{Int })$ stranica graniči s dva trokutića, dok svaka od $e(\partial)$ stranica leži u točno jednom trokutiću. Stoga je

$$3(f-1) = 2e(\text{Int }) + e(\partial) \;\Rightarrow\; f = 2(e-f) - e(\partial) + 3.$$

Očito rubnih stranica ima isto koliko i vrhova, tj. $e(\partial) = N(\partial)$. Uzmemo li u obzir sve ove relacije i Eulerovu formulu, slijedi

$$f = 2(e-f) - e(\partial) + 3 = 2(n-2) - N(\partial) + 3 = 2N(\text{Int }) + N(\partial) - 1,$$

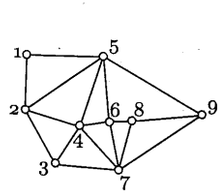
pa je konačno

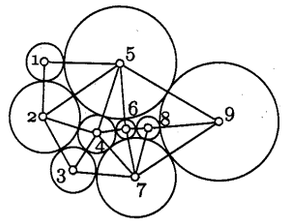
$$p(Q) = \frac{1}{2}(f-1) = N(\text{Int }) + \frac{1}{2}N(\partial) - 1.$$

I. Macdonald je 1963. poopćio tu formulu na d-politope, a 1971. i na simplicijalne komplekse rabeći njihovu Eulerovu karakteristiku. □

Zanimljiv je i važan problem diskretne geometrije (a Eulerova formula u rješenjima posebnih slučajeva igra važnu ulogu) jest sljedeći **problem pakiranja**. Neka je $\mathcal{C}$ konačna familija konveksnih tijela (npr. u $\mathbb{R}^3$) čije su unutrašnjosti disjunktne. Neka je $G(\mathcal{C})$ **kontaktni graf** familije $\mathcal{C}$, čiji vrhovi odgovaraju članovima od $\mathcal{C}$, a dva su vrha susjedna ako i samo ako se pripadni članovi od $\mathcal{C}$ dodiruju. Osnovni je problem karakterizacija klase grafova koji su kontaktni grafovi pakiranja sukladnih (ili sličnih itd.) kopija nekog čvrstog konveksnog tijela K.

Povijesno je posebno poznat slučaj kada je $K = D^3$ (kugla), a potječe iz pitanja koliko najviše jediničnih kugli može dodirivati zadanu jediničnu kuglu? Još tamo 1694. je I. Newton tvrdio da ih je 12, a D. Gregory da ih je 13. Tek su 1953. Schütte i van der Waerden dokazali da je Newton bio u pravu (a dokaz iz "KNJIGE" dao je J. Leech 1956., vidi [2*]). Prvi netrivijalni teorem za problem pakiranja sukladnih krugova (ili novčića) u ravnini je **Koebeov teorem** iz 1936. koji kaže da je jednostavni graf G kontaktni graf pakiranja krugova u ravnini ako i samo ako je G planaran. Koebe je to dokazao rabeći kompleksnu analizu, ali su W. Thurston i drugi oko 1985. našli kombinatorni dokaz (v. [55*]), bitno rabeći Eulerovu formulu.





Opći problem pakiranja je još uvijek neriješen, a nejasna je i **Keplerova slutnja** da je 12 jednakih dodirnih kugala koje diraju jednako veliku danu kuglu, a koje su postavljene u vrhovima pravilnog ikozaedra, "najgušće" pakiranje kugala (iako je dokaz te 300-godišnje slutnje najavljen oko 1997.).

Za teoriju su grafova dvije posljedice Koebovog teorema važne. Prva je očita posljedica.

TEOREM (I. Fáry, 1948). *Jednostavni planarni graf može se nacrtati u ravnini tako da su mu svi bridovi dužine.*

Druga je posljedica važna za algoritamske aspekte planarnih grafova, a ugrubo kaže da se planarni graf može rastaviti u dvije puno manje komponente uklanjanjem relativno malo vrhova. Preciznije, vrijedi sljedeće.

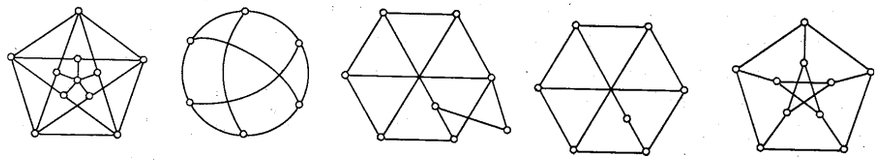
TEOREM (Lipton-Tarjan, 1979). *Neka je G jednostavni planarni graf s n vrhova. Tada postoji particija $A \cup B \cup C$ skupa vrhova od G, tako da je $|A|, |B| \leq \frac{3}{4}n$, $|C| < 2\sqrt{n}$, a nijedan vrh iz A nije susjedan nijednom vrhu iz B.*

Karakterizacije planarnih grafova

Zbog važnosti planarnosti grafova odavno se ukazala potreba za dobrom kombinatornom karakterizacijom planarnih grafova. No, prvo uočimo da planarnost grafa očito ne ovisi o tome je li neki brid subdividiran (tj. višeput umetnut vrh stupnja 2) ili je izvršen obratni postupak uklanjanja takvih vrhova. Dva grafa koji se jedan iz drugog dobiva s nekoliko takvih umetanja ili uklanjanja vrhova stupnja 2 (a shvaćenih kao podskupovi ravnine ili prostora) su homeomorfni. Osnovna karakterizacija planarnih grafova je sljedeći teorem.

TEOREM 19 (Kuratowski[23], 1930). *Graf G je planaran ako i samo ako ne sadrži subdiviziju od K_5 ni subdiviziju od $K_{3,3}$.*

Prema tome, možemo reći da je graf planaran ako i samo ako ne sadrži podgraf homeomorfan s K_5 ili $K_{3,3}$. Tako npr. grafovi na sljedećoj slici nisu planarni:



[23]Kasimir Kuratowski (1896 – 1980), poljski matematičar. Ovaj teorem se katkad zove i **Kuratowski-Pontrjaginov teorem**; Lav S. Pontrjagin (1908 – 1988), ruski matematičar

Graf Mycielskog na sl. a) sadrži subdiviziju od K_5, graf na sl. b) je izomorfan s $K_{3,3}$, graf na sl. c) sadrži podgraf na sl. d), a taj je subdivizija od $K_{3,3}$, Petersenov graf P na sl. e) sadrži subdiviziju od $K_{3,3}$ na sl. b); protumačite to geometrijski krenuvši od toga da je P tetraedar zajedno sa tri spojnice polovišta nasuprotnih bridova tetraedra (vidi Primjer 2 b)).

Jedan smjer teorema Kuratowskog je lagan. Ako je G planaran, onda očito ne može sadržavati subdivizije neplanarnih grafova K_5 i $K_{3,3}$ (Propozicija 22). No, obrat je puno teže dokazati, tj. da su K_5 i $K_{3,3}$ jedine "zapreke" za planarnost.

Podsjetimo da je **minora** grafa G graf dobiven nizom uklanjanja i kontraktiranja bridova (operacije $G-e$ i G/e) i uklanjanja vrhova ($G-v$). Uočimo da ako je G planaran, onda su $G-e$, G/e i $G-v$ planarni.

LEMA 10. *Graf sadrži subdiviziju od $K_{3,3}$ ako i samo ako sadrži $K_{3,3}$ kao minoru.*
Graf sadrži K_5 kao minoru ako i samo ako sadrži subdiviziju od K_5 ili sadrži $K_{3,3}$ s dva dodatna nesusjedna brida kao minoru.

Dokaz ove Leme nije težak, a svodi se na nekoliko crteža, pa ga prepuštamo čitatelju.

Iz Leme 10 odmah slijedi da je Teorem Kuratowskog ekvivalentan sljedećem teoremu.

TEOREM 19' (Wagner, 1937). *Graf G je planaran ako mu ni K_5 ni $K_{3,3}$ nisu minore.*

Zato je npr. Petersenov graf na prethodnoj slici e) neplanaran, jer mu kontrakcijom pet bridova (kojih?), K_5 postaje minora.

Kratko možemo reći da za smještavanje grafa na sferu (tj. u ravninu) imamo dvije **zabranjene minore** (K_5 i $K_{3,3}$).

D. König je 1936. postavio pitanje postoji li slična karakterizacija Kuratowskijevom teoremu za smještavanje grafova u bilo koju plohu. Sljedeći teorem daje (pozitivan) odgovor na to pitanje.

TEOREM (N. Robertson, P. Seymour, 1992). *Neka je M bilo koja ploha. Tada postoji konačna familija grafova $G_1, G_2, \ldots, G_n$ ("zabranjene minore") sa svojstvom da se graf G može smjestiti u plohu M ako i samo ako nijedan od grafova $G_1, \ldots, G_n$ nije minora od G. Nadalje, postoji polinomski algoritam kojim se to može provjeriti. Za projektivnu ravninu $\mathbb{R}P^2$ postoji lista od 35 zabranjenih minora.*

Kulminacija ove *"strukturalne teorije grafova"* je sljedeći vrlo općenit teorem istih autora.

TEOREM (N. Robertson, P. Seymour, 1996). *Neka je p neko svojstvo grafova tako da za svaki graf G sa svojstvom p i svaka minora od G ima svojstvo p. Tada postoji konačna familija $\mathcal{F}_p$ grafova tako da graf G ima svojstvo p ako i samo ako G nema minore iz $\mathcal{F}_p$.*

Bilješka. Teorem Kuratowskog je zapravo topološke prirode i tvrdi da je graf shvaćen kao konačni 1-dimenzionalni simplicijalni kompleks neplanaran ako i samo ako njegova geometrijska realizacija sadrži skup homeomorfan 1-skeletu tetraedra

zajedno sa spojnicama polovišta nasuprotnih bridova (to je $K_{3,3}$) ili 1-skeletu 4-dimenzionalnog simpleksa (to je K_5). Inače, opći je topološki rezultat da se svaki konačan n-dimenzionalni simplicijalni kompleks (topološki) može smjestiti u euklidski prostor $\mathbb{R}^{2n+1}$, a to je i najbolji rezultat, jer se n-skelet $(2n+2)$-dimenzionalnog simpleksa ne može smjestiti u $\mathbb{R}^{2n}$ (dokaz je npr. u [98]).

Svaki jednostavni graf (čak i beskonačni) može se shvatiti i kao višedimenzionalni simplicijalni kompleks čija je dimenzija jednaka dimenziji maksimalne klike (tj. potpunog podgrafa), jer je K_n graf $(n-1)$-dimenzionalnog simpleksa. Opći graf se može shvatiti kao tzv. **ćelijski kompleks**. Za takve se komplekse također definira **Eulerova karakteristika** $\chi(K) := \sum_{i\geq 0}(-1)^i f_i$, gdje je f_i broj i-dimenzionalnih simpleksa (odn. ćelija), a i razne druge kombinatorne i topološke invarijante (npr. prsten kohomologije). Stoga se mnogi rezultati o grafovima mogu dobiti iz odgovarajućih topoloških rezultata. Spomenimo samo poznatu, dugo vremena otvorenu tzv. glavnu slutnju (poznatiju po njemačkom nazivu **Hauptvermutung**). Naime, ako su dva grafa, odnosno pripadni kompleksi kombinatorno ekvivalentni (tj. jedan iz drugog dobiveni nizom subdivizija), onda su njihove geometrijske realizacije (tj. shvaćeni kao topološki prostori) homeomorfni. Hauptvermutung pita vrijedi li obrat, tj. povlači li homeomorfizam kombinatornu ekvivalenciju? U dimenzijama 1 i 2 slutnja se pokazala točnom (radovima Papakiryakopoulusa i drugih 1940 – 1950). No 1961. je Milnor[24] oborio Hauptvermutung, konstruirajući dva 6-dimenzionalna homeomorfna kompleksa koji kombinatorno nisu ekvivalentni. Tako je Hauptvermutung oboren u dimenzijama ≥ 6 (kasnije i u dimenziji 5), ali je i danas otvoren u dimenzijama 3 i 4.

Drugi primjer (djelomice) uspješne primjene metoda algebarske topologije i algebarske geometrije (koja proučava skupove rješenja algebarskih jednadžbi) bio je rješenje problema karakterizacije f-vektora simplicijalnih politopa. Taj je problem uspješno riješio Stanley[25] 1981. uporabom tzv. teškog Lefschetzovog teorema, ali je problem za bilo koje politope i dalje otvoren.

Skica dokaza Teorema Kuratowskog i Wagnera

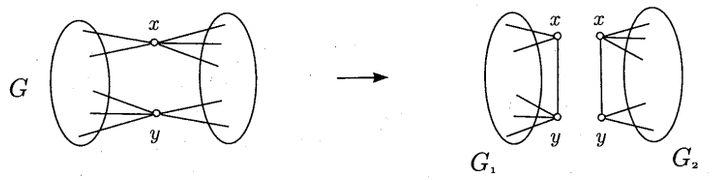
Sada ćemo bez nekih detalja, koje prepuštamo čitatelju, dati dokaz Teorema 19 (i istovremeno ekvialentnog teorema 19'). Taj je dokaz dao C. Thomassen 1984. Počnimo s sljedećom posljedicom Jordanovog teorema.

LEMA 11. *a) Graf (izomorfan s) $K_{2,3}$ ima ravninsko smještenje s točno tri strane, a njihovi rubovi su strane triju ciklusa od $K_{2,3}$;*
b) Rub svake strane 2-povezanog ravninskog grafa G je ciklus od G.

Dokaz. a) To odmah slijedi iz Jordanovog teorema o krivulji.
b) To slijedi iz a) opetovanim dodavanjima putova između dvaju vrhova, a počinjući s ciklusom (usp. Propoziciju 14). □

[24] John Milnor (r. 1931), američki matematičar.
[25] Richard Stanley (r. 1944), američki matematičar.

Prvo pogledajmo 2-povezan graf G. Lako se vidi da su tada $G-e$ i G/e opet 2-povezani. Naime, neka su x, y rezni vrhovi i neka su grafovi G_1 i G_2 dobiveni iz G operacijom razdvajanja kao na donjoj slici.



x i y nisu nužno susjedni u G, ali u G_1 i G_2 su susjedni. Očito da ako je G planaran, onda su oba G_1 i G_2 planarna. Nadalje, nije teško pokazati da je graf planaran ako i samo ako mu je svaki blok planaran. Stoga je planarnost zapravo zanimljiva tek za 3-povezane grafove.

Ako je bar jedan od G_1, G_2 2-povezan, onda gornji postupak razdvajanja možemo nastaviti sve dok ne dođemo do familije 3-povezanih grafova (pokazuje se neovisno o poretku u kojem smo to obavili).

Stoga pogledajmo 3-povezane grafove.

LEMA 12. *Neka je G 3-povezan graf s bar 4 vrha, a $e \in E(G)$ brid. Tada je ili G/e 3-povezan ili je $G-e$ subdivizija 3-povezanog grafa.*

Dokaz. Neka je $e = xy$ i neka je G/e nije 3-povezan. Tada postoji vrh z tako da $G' = G - \{x, y, z\}$ nije povezan. Treba pokazati da za svaka dva vrha x', y' različita od x, y postoje tri unutarnje disjunktna (x', y')-puta u $G-e$. Iz 3-povezanosti od G slijedi da takva tri puta postoje u G. Ako jedan od njih sadrži e, onda su x' i y' u istoj komponenti od G' ili je jedan x', y' jednak z. No, u tom slučaju postoji komponenta C od G' koja ne sadrži x' i y' i postoji put u $(C + xy) - e$ koji spaja x i y. No zamijenimo li e putom P, dobivamo tri unutarnje disjunktna (x', y')-puta u $G-e$. □

LEMA 13. *Neka je G 3-povezan graf s bar 5 vrhova. Tada postoji brid e iz G tako da je G/e 3-povezan.*

Dokaz. Pretpostavimo da brid $e_1 = xy$ nije dobar. Tada postoji vrh z tako da je $\{x, y, z\}$ vršni rez od G. Taj z postoji zbog Leme 12. Sada odaberimo xy tako da najveća komponenta C od $G - \{x, y, z\}$ bude najveća moguća. Neka je C' druga komponenta od $G - \{x, y, z\}$, a $u \in V(C')$ tako da je $uz \in E(G)$. Neka je $e_2 = uz$. Tada nije teško provjeriti da je G/e_2 3-povezan graf. □

Dokažimo sada sljedeću reformulaciju Leme 13.

PROPOZICIJA 24 (W. Tutte, 1961). *Neka je G 3-povezan graf. Tada vrijedi samo jedna od mogućnosti a), b) ili c). Pritom je*

a) G je kotač (tj. ciklus čiji je svaki vrh spojen s centrom);

b) Postoji $e \in E(G)$, tako da je $G-e$ 3-povezan;

c) Postoji $e \in E(G)$ koji nije iz nekog trokuta i G/e je 3-povezan.

Dokaz. Pretpostavimo da ne vrijedi ni b) ni c). Po Lemi 13, tada imamo u G trokut T s vrhovima x, y, z. Tvrdimo da bar dva vrha od T imaju stupanj 3. Pretpostavimo suprotno, i neka su $x_1, x_2 \notin V(T)$ susjedi od x, a $y_1, y_2 \notin V(T)$ susjedi od y. Kako $G - xy$ nije 3-povezan, postoji vrh z' tako da $G' := G - \{z, z'\} - xy$ nije povezan. Neka su G_x i G_y komponente od G' koje sadrže redom x i y. Kako je $G-y$ 2-povezan, postoje disjunktni putovi P_1, P_2 iz skupa $\{y_1, y_2\}$ u skup $\{z', z\}$. Jedan od x_1, x_2, recimo x_1 je različit od z'. U $G-x$ imamo unutarnje disjunktne putove Q_1, Q_2, iz x_1 do $\{z', z\}$. Kako su P_1, P_2 u $G_x + \{z, z'\}$, a Q_1, Q_2 u $G_y + \{z', z\}$, slijedi da je $P_1' := P_1 + Q_1 + Q_2$ jedan (y, z)-put. Putovi P_1', P_2 i $P_3 = yx + xz$ su tri unutarnje disjunktna (y, z)-puta, pa stoga brid yz zadovoljava b), kontradikcija.

Prema tome, T ima bar dva vrha stupnja 3. Neka su to x i y i neka je x' $(\neq y, z)$ susjed od x. Tada se lako vidi da je G/xx' 3-povezan. Zato xx' mora biti u nekom trokutu. Treći vrh tog trokuta mora biti z, osim ako je $G = K_4$. Tada opet zaključujemo da x' ima stupanj 3. Sada pogledamo susjeda x'' od x' različitog od x i z i nastavimo na isti način, pa vidimo da je G kotač s centrom z. □

Kao posljedica svega ovoga, očito vrijedi sljedeće.

KOROLAR 18. *Svaki jednostavni 3-povezani graf različit od K_4 ima brid čijom kontrakcijom dobivamo 3-povezan graf.*

Na temelju ovog Korolara pokažimo algoritam za planarnost. Neka je G bilo koji jednostavan 3-povezan graf. Uporabom Korolara 18 konstruirajmo niz grafova $H_1, H_2, \ldots, H_m$, gdje je $H_1 = G$, $H_m = K_4$, a H_{i+1} dobivamo iz H_i kontrakcijom jednog brida (ako se pojave višestruki bridovi, ostavljamo samo jedan), $i = 1, \ldots, m-1$.

Svakako H_m možemo nacrtati kao ravninski graf. Ako je H_{i+1} ravninski, onda ga, ako je to moguće, modificiramo u ravninski crtež od H_i tako da razdvojimo jedan vrh z u dva susjedna vrha x i y, a sve bridove koji nisu incidentni sa z zadržimo istima. Stoga modifikacija od H_{i+1} ima efekta jedino na bridove unutar (ili izvan) ciklusa C iz $H_{i+1} - z$ koji je rub strane od $H_{i+1} - z$ koja sadrži z. Dakle, ako se H_i ne može nacrtati kao ravninski graf, onda je jedini razlog za to taj da je C zajedno s x, y i bridovima incidentnim s x i y neplanaran. No tada u podgrafu H_i nije teško prepoznati subdiviziju od K_5 ili $K_{3,3}$. U tom slučaju H_i (pa stoga i G) sadrži K_5 ili $K_{3,3}$ kao minoru. □

Napomena 1. Brid xy zadovoljava zaključak Korolara 18 ako i samo ako je graf dobiven uklanjanjem vrhova x i y 2-povezan. To se može provjeriti u vremenu $O(q)$, gdje je q broj bridova grafa. Stoga se brid koji zadovoljava zaključak tog Korolara može naći u vremenu $O(q^2)$. Prema tome se niz $H_1, H_2, \ldots, H_m$ iz gornjeg algoritma može naći u vremenu $O(q^3)$ (obrnuti proces, iz H_m do H_1 zahtijeva i manje koraka). Dakle, navedeni algoritam za planarnost je složenosti $O(q^3)$. Ako je G jednostavan graf s n vrhova, onda je $q \leq n^2/2$, pa je tada ta složenost $O(n^6)$. Hopcroft i Tarjan su 1974. našli $O(n)$-algoritam za planarnost.

Navedimo još dvije karakterizacije planarnosti. Prvo nam treba jedna Lema o dualnim grafovima (kratko ćemo reći dual).

LEMA 14. *Ako G ima dual G^*, i ako je e brid iz G, a e^* odgovarajući brid iz G^*, onda je $G^* - e^*$ dual od G/e, a G^*/e^* dual od $G - e$. Posebno, ako G ima dual, onda i svaka minora od G ima dual.*

Dokaz je lagan i prepuštamo ga čitatelju. Lako se vidi da K_5 i $K_{3,3}$ nemaju dual. Stoga Kuratowskijev teorem povlači sljedeće.

TEOREM 20 (Whitney, 1932). *Graf je planaran ako i samo ako ima dual.*

Za sljedeću karakterizaciju nam treba pojam prostora ciklusa grafa. Neka je $\mathbb{Z}_2$ (ili $\mathbf{F}_2$ ili $GF(2)$) polje od 2 elementa $\{0,1\}$. Za podskup $S \subseteq E(G)$, neka je $\chi_S : E(G) \to \mathbb{Z}_2$ karakteristična funkcija podskupa S. Skup svih funkcija χ_S čini vektorski prostor nad $\mathbb{Z}_2$ (i zove se katkad **prostor bridova** od G), s operacijom $\chi_S + \chi_T := \chi_{S \triangle T}$ ($S \triangle T$ je simetrična razlika, $S \triangle T = (S \setminus T) \cup (T \setminus S)$). Parni podgrafovi (tj. podgrafovi kojima je svaki vrh parnog stupnja) čine potprostor prostora bridova koji se zove **prostor ciklusa** $\mathcal{C}(G)$.

TEOREM 21 (MacLane[26], 1937). *Graf je planaran ako i samo ako prostor ciklusa tog grafa ima bazu koja se sastoji od ciklusa, tako da je svaki brid u najviše dva od tih ciklusa.*

Planarnost i bojenje grafova

Možda je najveći poticaj razvoju teorije grafova dao **problem četiriju boja**, kojeg je 1852. postavio Francis Guthrie, nastojeći obojiti u što manje boja grofovije Engleske tako da one koje imaju zajedničku granicu budu različito obojene. Vidio je da su 4 boje dovoljne i postavio je opće pitanje može li se svaka planarna karta obojiti s četirima bojama. Bavili su se tim problemom de Morgan, Hamilton, Cayley i drugi. Kempe je 1879. objavio "dokaz", ali je Heawood 1890. našao grešku i "spasio što se spasiti može" dokazavši teorem o 5 boja.

Prelaskom na dualni graf, problem četiriju boja pita da li je jednostavni planarni graf 4-obojiv? Više od 120 godina bezuspješnih pokušaja mnogih da riješe taj problem, to je tek 1976. uspjelo Appelu i Hakenu dokazom na preko 100 strana i rabeći računalo. 1997. su Robertson, Sanders, Seymour i Thomas objavili jednostavniji dokaz od oko 40 stranica, ali također rabeći računalo (vidi J. Comb. Theory, Ser. B70 (1997), 2 – 44 kao i R. Thomas, An update on 4-color theorem, Notices AMS 45, (1998), 848 – 859).

TEOREM (o četirima bojama). *Svaki je planarni graf 4-obojiv.*

Mi ćemo dokazati na dva načina teorem o 5 boja.

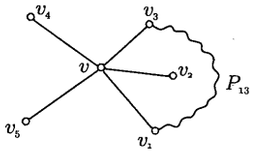
TEOREM 22 (Heawood[27], 1890). *Svaki je planaran graf 5-obojiv.*

Dokaz I. Uzmimo da teorem ne vrijedi. Tada postoji 6-kritični ravninski graf G. Iz Propozicije 15 slijedi da je $\delta \geq 5$, a iz Propozicije 21 c) da je $\delta \leq 5$, pa je $\delta = 5$ i neka je vrh $v \in V(G)$ takav da je $d(v) = 5$. Tada postoji 5-bojenje od $G - v$ i neka je

[26] Saunders Maclane (r. 1909), američki matematičar
[27] Percy Heawood (1861 – 1955), engleski matematičar

V_i skup svih vrhova boje $i, i = 1, \ldots, 5$. Kako G nije 5-obojiv, v mora biti susjedan vrhu svake od 5 boja. Stoga možemo uzeti da su susjedi od v takvi da je $v_i \in V_i$, $i = 1, \ldots, 5$. Označimo s $G(i,j) := G[V_i \cup V_j]$ graf induciran s $V_i \cup V_j$. Tvrdimo da v_i, v_j pripadaju istoj komponenti od $G(i,j)$. Kad ne bi bilo tako, pogledamo komponentu od $G(i,j)$ koja sadrži v_i. Zamijenimo li boje i, j u toj komponenti, dobivamo novo 5-bojenje od $G - v$ u kojemu sudjeluju samo 4 boje (sve osim boje i) kojima su obojeni svi susjedi od v. No, već smo vidjeli da je to nemoguće. Stoga su v_i, v_j u istoj komponenti od $G(i,j)$.

Neka je P_{ij} (v_i, v_j)-put u $G(i,j)$, a neka je C ciklus $vv_1P_{13}v_3v$. Budući da C separira $v_2 \in \text{Int } C$ i $v_4 \in \text{ext } C$ kao na donjoj slici, onda prema Jordanovom teoremu slijedi da put P_{24} mora sjeći C u nekoj točki. Jer je G ravninski, ta točka mora biti vrh u G. No, to je nemoguće, jer su vrhovi od P_{24} obojeni bojama 2 i 4, a vrhovi od C nisu obojeni tim bojama. Time smo dobili kontradikciju i teorem je dokazan. □



Za drugi dokaz nam treba sljedeći pojam. Neka je $G = (V, E)$ graf i neka je za svaki vrh $v \in V$ zadana lista boja $L(v)$ kojom možemo obojiti vrh v. **Bojenje po listama** od G je svako pravilno bojenje $c : V \to \bigcup_{v \in V} L(v)$, tako da je $c(v) \in L(v)$, $\forall v \in V$.

Listno kromatski broj $\gamma_l(G)$ od G je najmanji broj $k \in \mathbb{N}$, tako da G ima bojenje po listama za svaku skupinu listi $\{L(v) | v \in V\}$ takvu da je $|L(v)| = k$, $\forall v \in V$.

Naravno, $\gamma_l(G) \leq |V|$ jer nikada ne ostanemo bez neke boje, a s druge strane, $\gamma(G) \leq \gamma_l(G)$, jer je obično (pravilno) bojenje posebni slučaj bojenja po listama, kada su sve liste $L(v)$ jednaki skupovi boja. No, γ i γ_l se razlikuju, npr. za $G = K_{2,4}$, jer je $\gamma(K_{2,4}) = 2$, a $\gamma_l(K_{2,4}) = 3$ i slično grafovi s $\gamma = 2$, a γ_l po volji velik.

Kao i u prvom dokazu Heawoodovog teorema lako se vidi da je za svaki planarni graf G, $\gamma_l(G) \leq 6$. No, C. Thomassen je 1994. dokazao jaču tvrdnju (i to bez Eulerove formule!) da je $\gamma_l(G) \leq 5$, čime dobivamo i drugi dokaz (iz "KNJIGE") Heawoodovog teorema.

TEOREM 23 (C. Thomassen, 1994). *Za svaki planaran graf G vrijedi $\gamma_l(G) \leq 5$.*

Dokaz. Prvo je jasno da ako je $H \subseteq G$, onda je $\gamma_l(H) \leq \gamma_l(G)$, jer dodavanje bridova samo povećava kromatski broj. Stoga možemo pretpostaviti da je G povezan i da su sve omeđene strane ravninskog smještenja od G trokuti. Takav ćemo graf zvati **skoro trianguliran**. Ako teorem dokažemo za skoro triangulirane ravninske grafove, onda to povlači da teorem vrijedi i za sve ravninske grafove. Indukcijom ćemo dokazati sljedeću tvrdnju.

Tvrdnja. Neka je G skoro trianguliran graf, a C vanjski ciklus (tj. onaj koji je rub vanjskog područja). Pretpostavimo da za liste $L(v)$, $v \in V$, vrijedi:

(i) Dva susjedna vrha x, y iz C već su obojena redom bojama a i b;

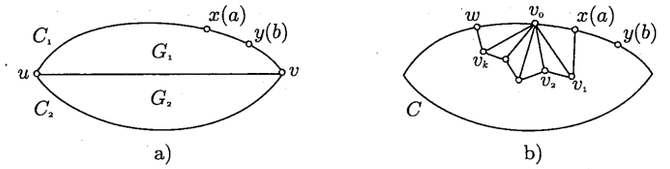
(ii) $|L(v)| \geq 3$, za sve ostale vrhove $v \in C$;

(iii) $|L(v)| \geq 5$, za sve vrhove iz unutrašnjosti od C.

Tada se bojenje od x, y može proširiti do bojenja po listama od G. Posebno je $\gamma_l(G) \leq 5$.

Za $|V| = 3$ to je očito, jer za jedini neobojeni vrh v vrijedi $|L(v)| \geq 3$, pa imamo boju po izboru. Za korak indukcije razlikujemo dva slučaja.

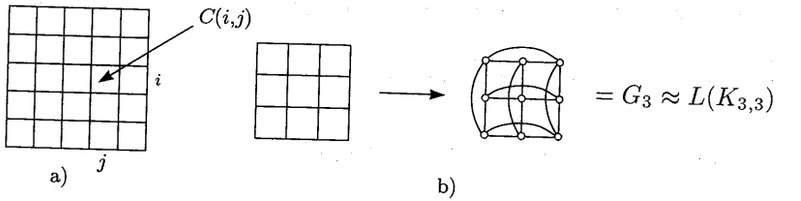
Slučaj 1. Pretpostavimo da C ima tetivu, tj. brid koji nije iz C, a spaja dva vrha u, v iz C. Tada je podgraf G_1 omeđen bridom uv i dijelom C_1 ciklusa C na kojem leže vrhovi x i y skoro trianguliran, pa po pretpostavci indukcije G_1 ima bojenje po listama s 5 boja. Neka su u tom bojenju vrhovi u i v obojeni redom bojama c i d. Preostali dio ("donji" dio) G_2 omeđen s C_2 i tetivom uv ima već obojene vrhove u i v, pa i taj podgraf po pretpostavci indukcije možemo bojiti po listama s 5 boja. Tako dobijemo bojenje po listama od G s 5 boja (v. sl. a)).



Slučaj 2. Pretpostavimo da C nema tetive. Neka je v_0 drugi susjedni vrh od x na C i neka su $x, v_1, \ldots, v_k, w$ svi susjedi od v_0. Kako je G skoro trianguliran, slijedi da je i $G' = G - v_0$ skoro trianguliran (v. sl. b)), a vanjski mu je ciklus $C' = (C - v_0) \cup P$, gdje je P put $xv_1 \ldots v_k w$. Zbog (ii) je $|L(v_0)| \geq 3$, pa u $L(v_0)$ postoje dvije boje c i d različite od a. Sada zamijenimo svaku listu boja $L(v_i)$ s $L(v_i) \setminus \{c, d\}$, a zadržimo sve ostale liste vrhova iz G'. Tada očito G' ima i dalje sva svojstva (i), (ii), (iii), pa po pretpostavci indukcije ima bojenje po listama s 5 boja. Obojimo li v_0 jednom od boja c ili d, proširili smo bojenje po listama od G' na čitav G. Time je dokaz gotov. □

Slutnja da je za planarni graf $\gamma_l(G) \leq \gamma(G) + 1$ pokazala se općenito netočnom. Naime, po teoremu o 4 boje je $\gamma(G) \leq 4$. Za $\gamma(G) = 2$ vrijedi $\gamma_l(G) \leq 3$, isto tako $\gamma(G) = 4 \Rightarrow \gamma_l(G) \leq 5$, ali postoje primjeri s $\gamma(G) = 3$ i $\gamma_l(G) = 5$.

U svezi s listno kromatskim brojem spomenimo ovdje sljedeći problem poznat kao **Dinitzov problem** iz 1978. Promotrimo $n \times n$ (šahovsku) ploču i pretpostavimo da za svaku ćeliju (ili polje) (i, j) imamo skup $C(i, j)$ od n boja, tako da polje (i, j) možemo obojiti jednom od boja iz $C(i, j)$. Može li se tada cijela ploča obojiti tako da u svakom retku i svakom stupcu imamo različite boje (sl. a))?



Dinitzov je problem elegantno riješio F. Galvin 1995 (v. [2*]) pridruživši $n \times n$ ploči graf G_n kojem su vrhovi polja na ploči, a dva vrha susjedna ako i samo ako su pripadna polja u istom retku ili u istom stupcu. Ustvari je G_n izomorfan linijskom grafu $L(K_{n,n})$ grafa $K_{n,n}$ (sl. b)). Galvin je dokazao da je listno kromatski broj $\gamma_l(G_n) = n$ i tako potvrdno riješio Dinitzov problem. Još uvijek je otvoren problem vrijedi li za svaki linijski graf G $\gamma(G) = \gamma_l(G)$?

Što se može reći o kromatskom broju grafova koji se mogu smjestiti u druge plohe? Za grafove koji se mogu smjestiti u orijentabilnu plohu M_g roda g (sfera s g ručaka) definira se **kromatski broj plohe** $\gamma(M_g)$

$$\gamma(M_g) := \max\{\gamma(G) \mid G \hookrightarrow M_g\}.$$

Podsjetimo se da je rod od G najmanji $g \geq 0$, tako da $G \hookrightarrow M_g$. Indukcijom po g nije teško dokazati da vrijedi analogon Eulerove formule za povezani graf G roda g smješten u M_g s $f(G)$ strana:

$$\chi(G) := v(G) - e(G) + f(G) = 2 - 2g. \qquad (*)$$

Ako je G jednostavan povezan graf roda g s $n = v(G) \geq 3$ vrhova, onda je svaka strana omeđena s barem tri brida, pa je $3f(G) \leq 2e(G)$, pa iz $(*)$ slijedi $e(G) \leq 3n - 6 + 6g$ (analogon Propoziciji 21 b)). Ako je G k-kritičan, $k \geq 7$, onda odatle zbog $\delta(G) \geq k - 1$ slijedi $(k-1) \cdot n \leq 2e(G) \leq 6n + 12(g-1)$, pa zbog $n \geq k \geq 7$ slijedi da je $(k-7)k - 12(g-1) \leq 0$, pa dobivamo da za takav graf vrijedi

$$\gamma(G) \leq k \leq \left\lfloor \frac{7 + \sqrt{1 + 48g}}{2} \right\rfloor.$$

Međutim, vrijedi i puno jača tvrdnja.

TEOREM (Ringel-Youngs, 1968). *Za $g > 0$ vrijedi*

$$\gamma(M_g) = \left\lfloor \frac{7 + \sqrt{1 + 48g}}{2} \right\rfloor.$$

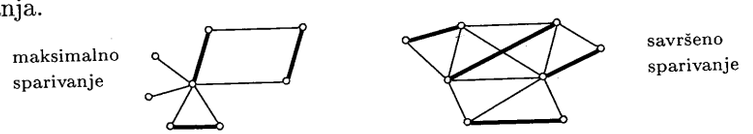
Teorem o četirima bojama povlači da je ta formula točna i za $g = 0$. Za $g = 1$ dobivamo da je kromatski broj torusa jednak 7; jer se npr. 7-kromatski graf K_7 može smjestiti na torus. O tim pitanjima vidi u [96],[192], [231] i [53*].

§ 7. Sparivanje u grafovima

Sparivanje (engl. *matching*) u grafu $G = (V, E)$ je podskup $M \subseteq E$ bridova koji su karike, a nikoja dva nisu susjedna. Kažemo da su dva kraja brida u M **sparena**

u M. Sparivanje od M **zasićuje** vrh v, ili se kaže da je v M-**zasićen** ako je neki brid iz M incidentan s v, a inače je v M-**nezasićen**.

Jedan od osnovnih problema teorije sparivanja jest pokazati da postoji ili konstruirati sparivanje s dovoljno mnogo bridova. Ako je svaki vrh iz G M-zasićen, kažemo da je M **savršeno sparivanje**[28] (engl. *perfect matching*). M je **maksimalno sparivanje** u G, ako ne postoji sparivanje M', za koje je $|M'| > |M|$. Savršeno je očito i maksimalno sparivanje. Na primjer, na slici su debelo izvučena sparivanja.



Katkad se o sparivanju govori i kao o **pakiranju bridova**, a slično govorimo i o **pakiranju vrhova**, tj. o nezavisnim (ili stabilnim) skupovima vrhova. **Pokrivač** (ili **vršni pokrivač**) je skup vrhova $K \subseteq V$, tako da svaki brid iz G ima bar jedan kraj u K, a **bridni pokrivač** L je skup bridova tako da je svaki vrh incidentan s bar jednim bridom iz tog skupa L. Sljedeći su parametri grafa G ovdje od interesa:

$\nu(G) :=$ veličina maksimalnog sparivanja (tj. pakiranja bridova) u G;

$\alpha(G) :=$ veličina maksimalnog stabilnog skupa (tj. pakiranja vrhova) u G;

$\tau(G) :=$ veličina minimalnog pokrivača od G;

$\rho(G) :=$ veličina minimalnog bridnog pokrivača od G.

Pokazuje se da računanje $\nu(G)$ polinomski ovisi o veličini od G, dok je računanje $\alpha(G)$ **NP**-težak problem.

Pogledajmo sada neke veze među ovim parametrima za opće grafove. Kao prvo, budući da je skup $S \subseteq V$ stabilan ako i samo ako je $V \setminus S$ pokrivač od G, odmah dobivamo

$$\alpha(G) + \tau(G) = |V(G)| = n. \tag{1}$$

Iako komplement sparivanja ne mora biti bridni pokrivač, niti komplement bridnog pokrivača mora biti sparivanje, ipak su parametri $\nu(G)$ i $\rho(G)$ za bridove u istoj vezi kao (1). Naime, vrijedi

PROPOZICIJA 25 (T. Gallai, 1959). *Ako je $\delta > 0$ (tj. G nema izoliranih vrhova), onda je $\nu(G) + \rho(G) = |V(G)| = n$.*

Dokaz. Neka je M maksimalno sparivnje u G, a U skup svih M-nezasićenih vrhova. Kako je $\delta > 0$, za svaki $u \in U$, odaberimo brid $e(u)$ incidentan s u i neka je $E' \subseteq E(G) \setminus M$ skup svih takvih bridova. Tada je $M \cup E'$ bridni pokrivač od G, pa je $|M|+|M \cup E'| = 2|M|+|E'| \leq (|V|-|U|)+|U| = |V| = n$, pa je $\nu(G)+\rho(G) \leq n$. Obrnuto, neka je L minimalni bridni pokrivač od G, $|L| = \rho(G)$. Minimalnost od L povlači da je L skup bridova šume. Neka je k broj komponenata povezanosti te šume. Tada je $k = n - \rho(G)$. Svaka komponenta sadrži brid (jer G nema izoliranih vrhova), pa odabir po jednog brida iz svake komponente daje jedno sparivanje u G veličine k. Stoga je $\nu(G) \geq k = n - \rho(G)$, tj. $\nu(G) + \rho(G) \geq n$. □

[28] U kemijskoj (ili fizikalnoj) literaturi, to se često zove **Kekuléova struktura**, prema njemačkom kemičaru Augustu Kekuléu (1829 – 1896).

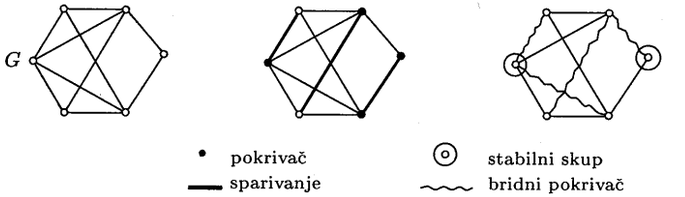
S druge strane, ako je K pokrivač od G, a M sparivanje u G, onda K sadrži barem jedan kraj svakog brida od M, pa je $|M| \leq |K|$. Posebno, ako je M^* maksimalno sparivanje, a $\overline{K}$ minimalni pokrivač, onda je $|M^*| \leq |\overline{K}|$, pa je

$$\nu(G) \leq \tau(G). \tag{2}$$

Uočite da ako je još $|M| = |K|$, onda zbog $|M| \leq |M^*| \leq |\overline{K}| \leq |K|$ slijedi da je M maksimalno sparivanje, a K minimalni pokrivač. Slično, ako je L bridni pokrivač od G, a S stabilan skup vrhova, onda je $|S| \leq |L|$, pa je

$$\alpha(G) \leq \rho(G). \tag{3}$$

Sličica za (2), (3):



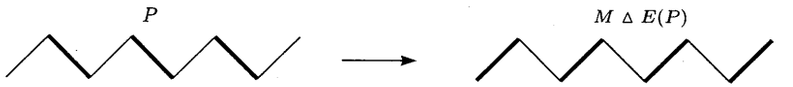
Jednakosti u (2) i (3) ne vrijede općenito, npr. $\nu(K_3) = \alpha(K_3) = 1$, a $\tau(K_3) = \rho(K_3) = 2$. Pokazat ćemo poslije da jednakosti u (2) i (3) vrijede za bipartitne grafove, pa je za bipartitne grafove teorija sparivanja puno lakša.

Spomenimo još ovdje da je $M \subseteq E(G)$ sparivanje ako i samo ako je M stabilni skup u linijskom grafu $L(G)$ od G.

Jedna od osnovnih ideja teorije sparivanja je pojam uvećanog puta. Neka je M sparivanje u G. M-**alternirajući put** u G je put čiji bridovi alterniraju u M i $E \setminus M$. M-alternirajući put P je M-**uvećani put** ako su mu početak i kraj M-nezasićeni vrhovi.

TEOREM 24 (C. Berge, 1957). *Sparivanje M u G je maksimalno sparivanje ako i samo ako G ne sadrži M-uvećani put.*

Dokaz. Pretpostavimo da G sadrži M-uvećani put P. Tada zamjenom debelitanki bridovi na P dobivamo sparivanje $M' = M \triangle E(P)$ u G s $|M'| = |M| + 1$ bridova, pa M ne može biti maksimalno sparivanje:



Obrnuto, pretpostavimo da M nije maksimalno sparivanje, i neka je M' maksimalno sparivanje s $|M'| > |M|$. Promotrimo inducirani podgraf $H = G[M \triangle M'] \subseteq G$. Svaki vrh $v \in V(H)$ je incidentan s najviše jednim bridom iz M i najviše jednim iz M', pa je $1 \leq d_H(v) \leq 2$. Stoga je svaka komponenta od H ili parni ciklus ili put i u oba slučaja bridovi alterniraju u M i M'. Kako je $|M'| > |M|$, slijedi da H ima

više bridova iz M' nego iz M, pa je zato neka komponenta od H put P iz H koji mora početi i završiti s bridovima iz M'. Početak i kraj od P su M'-zasićeni u H, pa su M-nezasićeni u G. Stoga je P jedan M-uvećani put u G. □

Ovaj teorem omogućuje da se efikasno (polinomijalno) izračuna $\nu(G)$.

Sparivanje u bipartitnim grafovima

Dokažimo prvo već najavljeni osnovni teorem da je za bipartitni graf G $\nu(G) = \tau(G)$, što omogućuje da se u tom slučaju svi parametri ν, α, τ, ρ mogu efikasno izračunati.

TEOREM 25 (König-Egerváry, 1931). *Za bipartitni graf G je $\nu(G) = \tau(G)$, tj. broj bridova maksimalnog sparivanja jednak je broju vrhova minimalnog pokrivača.*

Dokaz. Indukcijom po broju bridova $e(G)$. Ako je $e(G) = 0$, onda je $\nu(G) = \tau(G) = 0$. Za korak indukcije treba nam sljedeća tvrdnja.

Tvrdnja. Ako G ima bridova, a M bilo koje maksimalno sparivanje od G, onda je bar jedan kraj svakog brida od G M-zasićen.

Dovršimo prvo dokaz Teorema. Ako je $e(G) > 0$, onda iz Tvrdnje slijedi da postoji vrh $v \in V(G)$ koji zasićuju sva maksimalna sparivanja od G. Tada je $\nu(G-v) = \nu(G)-1$. Neka je K bilo koji pokrivač od $G-v$. Tada je $K \setminus \{v\}$ pokrivač od G, slijedi $\tau(G) \leq \tau(G-v)+1$. Po pretpostavci indukcije je $\nu(G-v) = \tau(G-v)$, pa je $\tau(G) \leq \nu(G)$, što zajedno s (2) daje $\nu(G) = \tau(G)$. Preostaje dokazati tvrdnju.

Dokaz Tvrdnje. Pretpostavimo da Tvrdnja nije istinita i neka je $e = uv \in E(G)$ za koji postoje maksimalna sparivanja M_u, M_v, tako da je u M_u-nezasićen, a v M_v-nezasićen. Tada postoje putovi P_u s krajem u i P_v s krajem v tako da $E(P_u), E(P_v) \subseteq M_u \triangle M_v$. Kako su M_u i M_v maksimalna sparivanja, slijedi $|M_u| = |M_v|$, pa su duljine od P_u i P_v parne. Pretpostavimo da su P_u i P_v različiti. Tada je $P = P_u + P_v + e$ put neparne duljine koji spaja jedan M_u-nezasićen i jedan M_v-nezasićen vrh. Zamijenimo li bridove iz $E(P) \cap M_u$ s neparno numeriranim bridovima puta P, dobivamo sparivanje koje je veće od M_u, što je kontradikcija. Stoga je $P_u = P_v$. No tada je $P+e$ neparni ciklus, a to je nemoguće zbog Propozicije 5. □

Iz Propozicije 25 i Teorema 25, odmah dobivamo:

PROPOZICIJA 26. *Za bipartitni graf G bez izoliranih vrhova je $\alpha(G) = \rho(G)$, tj. broj vrhova maksimalnog nezavisnog skupa jednak je broju bridova minimalnog bridnog pokrivača od G.*

U mnogim primjenama često želimo naći sparivanje bipartitnog grafa G s bipartricijom (X, Y) koje zasićuje sve vrhove iz X. Sljedeći teorem daje nužni i dovoljni uvjet za to. Za skup $S \subseteq V(G)$, **skup susjeda** $N_G(S)$, ili kraće $N(S)$, je skup svih vrhova susjednih nekom vrhu iz S.

TEOREM 26 (P. Hall[29], 1935). *Bipartitni graf G s bipartricijom (X, Y) ima sparivanje koje zasićuje sve vrhove iz X ako i samo ako vrijedi ("* Hallov uvjet*"):*

$$|N(S)| \geq |S|, \quad \forall S \subseteq X.$$

Dokaz. Nužnost je gotovo očita. Ako je M sparivanje u G koje zasićuje sve vrhove iz X, a $S \subseteq X$, onda su vrhovi iz S spareni bridovima iz M s različitim vrhovima iz $N(S)$, pa je očito $|N(S)| \geq |S|$.

Da dokažemo dovoljnost, pretpostavimo da ne postoji sparivanje koje zasićuje X. Tada je $\nu(G) < |X|$. Prema Teoremu 25, $\nu(G) = \tau(G)$, pa postoji pokrivač K od G, $|K| = \nu(G) < |X|$. Neka je $S = X \setminus K$. Tada je skup susjeda $N(S) \subseteq Y \cap K$. Stoga je $|S| = |X| - |K \cap X| = |X| - |K| + |Y \cap K| > |N(S)|$, suprotno Hallovom uvjetu. □

Iako za provjeru Hallovog uvjeta treba eksponencijalna provjera ($2^{|X|}$), ipak je ovaj teorem podloga za jedan dobar algoritam za nalaženje maksimalnog sparivanja u bipartitnom grafu. No, prvo neke primjene. Počnimo s "konkretnom" primjenom.

Primjer 47 (Problem zapošljavanja). Poduzeće želi zaposliti nove djelatnike za obavljanje poslova P_1, P_2, P_3, P_4 i P_5. Među kandidatima K_1, K_2, K_3, K_4, K_5 koji su se prijavili, K_1 je kvalificiran za poslove P_3 i P_4, K_2 za P_3, K_3 za P_1, P_2 i P_5, K_4 za P_3 i P_4, a K_5 za P_2 i P_5. Mogu li se ti kandidati rasporediti na poslove tako da svaki obavlja (različit) posao za koji je kvalificiran i da se svi poslovi obavljaju?

Rješenje. Prirodni model za taj problem je bipartitan graf s biparticijom koju čine $\{K_1, \ldots, K_5\}$ i $\{P_1, \ldots, P_5\}$, te $K_i \sim P_j$ ako i samo ako je K_i kvalificiran za posao P_j. Pitanje u problemu je ekvivalentno tomu postoji li sparivanje u tom grafu koje zasićuje sve vrhove iz $\{K_1, \ldots, K_5\}$. Odgovor je ne, jer je za skup $S = \{K_1, K_2, K_4\}$, $|N(S)| < |S|$, pa iz Hallovog teorema slijedi da takvo sparivanje ne postoji.

Naravno, problem je kako (i je li moguće) provesti takvo zapošljavanje ako je poslova više, a kandidata još puno više. Takve probleme rješavaju efikasni algoritmi bazirani na teoriji sparivanja. □

KOROLAR 19. *Bipartitni graf G s biparticijom (X, Y) ima savršeno sparivanje ako i samo ako je $|X| = |Y|$ i $|N(S)| \geq |S|$, $\forall S \subseteq X$. Posebno, k-regularni bipartitni graf ima savršeno sparivanje za $k > 0$.*

Dokaz. Prvi dio odmah izlazi primjenom Hallovog teorema na X i Y i činjenice $|X| = |Y|$. Drugi dio slijedi iz toga što je tada $k|X| = |E| = k|Y|$ i zato $|X| = |Y|$. Ako je $S \subseteq X$, onda je svaki brid incidentan vrhu iz S incidentan vrhu iz $N(S)$, pa je $k|N(S)| \geq k|S|$ i tvrdnja slijedi iz prvog dijela. □

Korolar 19 ima slikovitu interpretaciju poznatu kao teorem o ženidbi ili udaji, ili kratko, **teorem o braku**. U nekom selu svaka djevojka pozna točno k mladića, a svaki mladić pozna točno k djevojaka. Tada se djevojke i mladići mogu savršeno spariti, tj. svaki se mladić oženiti djevojkom koju pozna, a svaka se djevojka udati za mladića kojeg pozna.

Za sljedeću primjenu, neka su $A_1, A_2, \ldots, A_n$ bilo kakvi podskupovi skupa S. **Sistem različitih predstavnika** (ili **transverzala** ili **priječnica**) familije skupova $(A_i, 1 \leq i \leq n)$ je podskup $\{a_1, a_2, \ldots, a_n\} \subseteq S$, tako da je za svako i, $a_i \in A_i$, te $a_i \neq a_j$, za sve $i \neq j$.

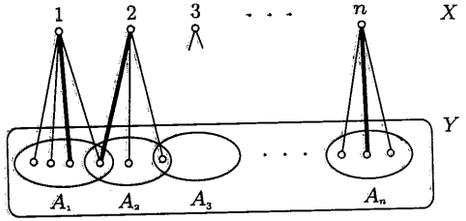
Ekvivalentno, to je injekcija $f : [n] \to S$, tako da je $f(i) \in A_i$, za svako $i \in [n]$.

[29] Philip Hall (1904 – 1982), engleski matematičar.

Uočite da npr. $A_1 = \{1,2\}$, $A_2 = \{1,2,3,4,5\}$, $A_3 = \{4\}$, $A_4 = \{1,4\}$ nema priječnicu.

KOROLAR 20 (o priječnici). *Skupovi $A_1, A_2, \ldots, A_n$ imaju priječnicu ako i samo ako je $|\bigcup_{i\in I} A_i| \geq |I|$, $\forall I \subseteq [n]$.*

Dokaz. Neka je G bipartitan graf s biparticijom (X,Y), gdje je $X = [n]$, $Y = \bigcup_{i=1}^{n} A_i$ (ili bilo koji veći skup), a vrh $i \in X$ spojen s vrhom $y \in Y$, ako i samo ako je $y \in A_i$. Tada $(A_i, 1 \leq i \leq n)$ imaju priječnicu ako i samo ako G ima sparivanje koje zasićuje X, a to je prema Hallovom teoremu ekvivalentno s $|\bigcup_{i\in I} A_i| \geq |I|$, $\forall I \subseteq [n]$. □



Primjer 48. a) Ako je G bipartitan graf s biparticijom (X,Y), koji je k-regularan na X (tj. $d(x) = k$, $\forall x \in X$), a l-regularan na Y, onda G ima sparivanje koje zasićuje X ili Y $(k, l > 0)$;

b) Ako su $A_1, \ldots, A_n \subseteq S$, i za svako j je $|A_j| = k$, a svaki $x \in S$ leži u točno l podskupova A_j, gdje je $l \leq k$, onda $(A_i, 1 \leq i \leq n)$ ima priječnicu;

c) **Latinski pravokutnik** tipa $r \times n$, $r \leq n$ je $(r \times n)$-matrica s članovima iz $[n]$, tako da su u svakom retku i svakom stupcu različiti članovi. **Latinski kvadrat** reda n je latinski pravokutnik tipa $n \times n$. Svaki se latinski pravokutnik L tipa $r \times n$ može proširiti do latinskog kvadrata reda n dodavanjem $n - r$ redaka. Dokažite.

Rješenje. a) Kao i u dokazu Korolara 19, ako je $l \leq k$, a $S \subseteq X$, onda slijedi da je $k|S| \leq l|N(S)| \leq k|N(S)|$, pa kao tamo slijedi tvrdnja.

b) To slijedi iz a) kao što je iz Korolara 19 slijedio Korolar 20.

c) Za $j \in [n]$, neka je A_j skup brojeva kojih nema u j-tom stupcu od L. Očito je $|A_j| = n - r$. Nadalje, svaki broj $i \in [n]$ je u točno $n - r$ skupova A_j. Stoga iz b) slijedi da familija $A_1, A_2, \ldots, A_n$ ima priječnicu, koju možemo dodati kao $(r+1)$-vi redak latinskom pravokutniku L. Nastavimo li taj postupak $n - r$ puta, dolazimo do latinskog kvadrata reda n. □

Primjer 49. Krnja (šahovska) ploča je dio pravokutne $m \times n$ ploče, čiji su kvadratići naizmjence obojeni bijelo (b) i crno (c), pri čemu su oni sa zajedničkom stranicom obojeni različito. **Savršeno pokrivanje dominima** takve ploče znači da svaki domino pokriva točno dva susjedna kvadratića, a svaki je kvadratić pokriven s točno jednim dominom. Nađite nužan i dovoljan uvjet da se krnja ploča P može savršeno pokriti dominima.

Rješenje. Označimo s B i C redom skupove bijelih, odnosno crnih, kvadratića na ploči P. Neka je G bipartitan graf s biparticijom (B,C), a bijeli kvadratić spojimo (bridom u G) s crnim kvadratićem ako i samo ako su susjedni (tj. sa zajedničkom stranicom). Dakle,

brid u G odgovara dominu koje pokriva ta dva kvadratića na P. Tada P ima savršeno pokrivanje dominima ako i samo ako G ima sparivanje koje zasićuje B.

Za svaki $S \subseteq B$ označimo sa $C(S)$ skup svih crnih kvadratića koji imaju zajedničku stranicu s bar jednim kvadratićem iz S. Tada iz Teorema 26 odmah slijedi da je traženi uvjet

$$|B| = |C| \text{ i } |C(S)| \geq |S|, \ \forall S \subseteq B.$$

Ovakva domina se u kemiji i fizici još zovu **dimeri** (dvoatomne molekule). Problem dimera je izračunati broj savršenih pokrivanja dimerima, ponašanje tih brojeva, asimptotika, funkcija izvodnica itd. □

Za egzistenciju i konstrukciju maksimalnog sparivanja bipartitnog grafa G s biparticijom (X,Y) važan je pojam defekta od G. Ako je $S \subseteq X$, onda se broj $\sigma(S) := |S| - |N(S)|$ zove **defekt** od S, a **defekt grafa** G je $\sigma(G) := \max\{\sigma(S) \mid S \subseteq X\}$. Očito je $\sigma(\emptyset) = 0$, pa je $\sigma(G) \geq 0$. Ako je $\sigma(G) > 0$, onda postoji $S \subseteq X$ za koji je $|S| > |N(S)|$, pa ne postoji sparivanje koje zasićuje X. Stoga je prirodno pitanje: koji je maksimalni broj vrhova iz X koji se mogu spariti s vrhovima iz Y.

PROPOZICIJA 27. *Neka je (X,Y) biparticija bipartitnog grafa G. Maksimalni broj vrhova iz X koji se mogu spariti s vrhovima iz Y jednak je $|X| - \sigma(G)$.*

Dokaz. Zbog Teorema 25 dovoljno je dokazati da je $\tau(G) = |X| - \sigma(G)$. Neka je $S \subseteq X$ skup za koji se postiže $\sigma(G)$, tj. $\sigma(G) = |S| - |N(S)|$, a $K = N(S) \cup (X \setminus S)$. K je pokrivač od G, pa je $\tau(G) \leq |K| = |N(S)| + |X| - |S| = |X| - \sigma(G)$. Za obrnutu nejednakost, neka je $\overline{K}$ minimalni pokrivač od G, a $K' = X \setminus \overline{K}$. Tada je $N(K') \subseteq \overline{K} \cap Y$, pa imamo $|N(K')| \leq |\overline{K} \cap Y| = |\overline{K}| - |\overline{K} - X| = |\overline{K}| - |X| + |X \setminus \overline{K}| = \tau(G) - |X| + |K'|$, pa je $\sigma(G) \geq |K'| - |N(K')| \geq |X| - \tau(G) \Rightarrow \tau(G) \geq |X| - \sigma(G)$. □

Kao posljedicu odavde dobivamo sljedeće.

KOROLAR 21. *Neka je $A_1, A_2, \ldots, A_n$ familija konačnih skupova. Tada je najveći broj skupova te familije koji imaju priječnicu jednak*

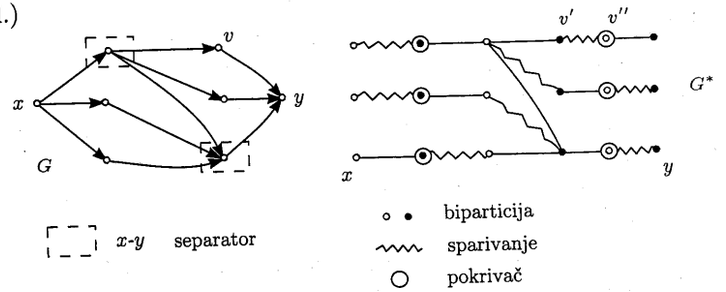
$$n - \max_{I \subseteq [n]} (|I| - |\bigcup_{i \in I} A_i|).$$

Sada ćemo pokazati da je Mengerov teorem 13, koji je također tipa "minimaks", zapravo ekvivalentan König-Egervaryjevom teoremu 25. Dokazat ćemo vršnu verziju (Teorem 13 (ii)) i to čak za digrafove. Podsjetimo da ako su $x \neq y$ vrhovi grafa G, onda se podskup $S \subseteq V \setminus \{x,y\}$ za koji x i y leže u različitim komponentama od $G - S$ zove x-y **separator**.

TEOREM 13' (Menger). *Neka je G graf (ili digraf), a $x \neq y$ nesusjedni vrhovi (xy nije luk) od G. Tada je maksimalni broj unutarnje disjunktnih (x,y)-putova (diputova) u G jednak minimalnom broju vrhova u x-y separatoru u G.*

Dokaz. Dokazat ćemo usmjerenu verziju. Odatle neusmjerena verzija lako slijedi ako svaki brid uv zamijenimo dvama suprotno orijentiranim lukovima (u,v) i (v,u).

Pridružit ćemo digrafu G bipartitni graf G^* ovako. Svaki vrh $v \neq x, y$ ćemo rascijepiti u dva nova vrha v', v'', vrh x ćemo zamijeniti (rascijepiti) s $d^+(x)$ novih vrhova, a y s $d^-(y)$ novih vrhova. Svakom luku (x, u) iz G pridružimo brid koji spaja u' s jednim od novih (različitih) vrhova pridruženih vrhu x, a svakom luku (u, y) iz G pridružimo brid koji spaja u'' s jednim od novih (različitih) vrhova pridruženih vrhu y. Vrhovi u' i v'' od G^* su susjedni ako i samo ako je $u = v$ ili je (u, v) luk u G. (v. sl.)



Neka je M maksimalno sparivanje u G^*. Tada je za svaki vrh $u \in V \setminus \{x, y\}$, bar jedan od vrhova u', u'' M-zasićen. Ustvari, ako je samo jedan od njih M-zasićen, onda ako zamijenimo taj jedini incidentni brid iz M s bridom $u'u''$, dobivamo drugo maksimalno sparivanje koje zasićuje oba vrha. Tada se lukovi od G za koje su pripadni bridovi iz G^* u sparivanju M mogu rastaviti u unutarnje disjunktne cikluse i (x, y)-putove u G, a broj (x, y)-putova među njima je $|M| - |V \setminus \{x, y\}|$. Prema König-Egervaryjevom teoremu 25, postoji pokrivač K od G^* takav da je $|K| = |M|$ i možemo uzeti da su jedino u' ili u'' iz K. Neka je S skup vrhova u iz G za koje su oba u' i u'' iz K. Kad bi svaki (x, y)-diput u G zaobišao sve vrhove iz S, onda bi postojao brid iz G^* koji nije pokriven s K, što je kontradikcija. Stoga je S jedan x-y separator veličine $|M| - |V \setminus \{x, y\}|$ i teorem je dokazan. □

Sljedeća primjena König-Egervaryjevog teorema je iz teorije matrica. Prvo neki pojmovi. $0-1$ matrica je $m \times n$ matrica A čiji su svi članovi 0 ili 1. **Rang** od A je veličina najvećeg podskupa R članova od A koji su jednaki 1, a nikoja dva člana od R nisu u istom retku ni u istom stupcu. (Ovaj rang se podudara s običnim rangom matrice u kojoj sve jedinice iz A zamijenimo s različitim varijablama.) Kvadratna $n \times n$ matrica $A = [a_{ij}]$ je **dvostruko stohastička matrica** ako je $a_{ij} \geq 0$, $\forall i, j$, a suma članova svakog retka i suma članova svakog stupca jednaka 1. **Dijagonalu** takve matrice čini n članova tako da nikoja dva nisu u istom retku ili istom stupcu. $n \times n$ 0-1 matrica A je **permutacijska matrica** ako sve jedinice leže na nekoj dijagonali. Matrica A je **konveksna kombinacija matrica** $A_1, A_2, \ldots, A_k$ ako postoje realni brojevi $\lambda_1, \lambda_2, \ldots, \lambda_k \geq 0$, $\sum_{i=1}^k \lambda_i = 1$, tako da je $A = \sum_{i=1}^k \lambda_i A_i$.

Primjer 50. a) Rang 0-1 matrice A jednak je veličini najmanjeg skupa redaka i stupaca od A koje sadrže sve jedinice iz A;

b) Dvostruko stohastička matrica A ima dijagonalu koja je sadržana u njezinim nenul članovima;

c) (**Birkhoff**[30] **- von Neumannov**[31] **teorem, 1953.**) Svaka dvostruko stohastička matrica je konveksna kombinacija permutacijskih matrica.

Dokaz. a) Neka su I i J skupovi redaka i stupaca od A, a G bipartitni graf s biparticijom (I, J), pri čemu je $i \in I$ spojen s $j \in J$ ako i samo ako je $a_{ij} = 1$. Tada je $\nu(G)$ jednak rangu od A, a $\tau(G)$ veličini najmanjeg skupa redaka i stupaca koje sadrže sve jedinice. Iz Teorema 25 slijedi tvrdnja.

b) Neka je $\tilde{A}$ dobivena iz A zamjenom svakog pozitivnog člana od A s 1. Tada zbog a) matrica A ima dijagonalu sadržanu u njezinim nenul članovima ako i samo ako $\tilde{A}$ ima rang n. Neka s R i S redom podskupovi skupa redaka i skupa stupaca od A koji se sastoje od samih nenul članova. Kako je suma svakog retka i svakog stupca od A jednaka 1, slijedi da je suma svih članova od A jednaka n, a to je manje ili jednako zbroju svih članova iz redaka od R i svih članova iz stupaca od S. Zato je $|R| + |S| \geq n$, pa $\tilde{A}$ ima rang n.

c) Dovoljno je dokazati da je svaka nenegativna kvadratna matrica A čija je suma svakog retka i suma svakog stupca pozitivna konstanta jednaka nenegativnoj linearnoj kombinaciji permutacijskih matrica. To dokazujemo indukcijom po broju pozitivnih članova. Neka je A takva $n \times n$ matrica. Kako je suma svakog retka i svakog stupca pozitivna, slijedi da pozitivnih članova ima barem n. Ako ih je točno n, onda je A jednaka permutacijskoj matrici pomnoženoj s pozitivnim brojem. Neka je broj pozitivnih članova veći od n. Prema b) postoji dijagonala sadržana u nenul članovima iz A. Neka je λ_1 najmanji član te dijagonale, a A_1 odgovarajuća permutacijska matrica. Neka je $A' = A - \lambda_1 A_1$. Tada je i A' matrica kao A, ali s manje nenul članova. Po pretpostavci indukcije postoje $\lambda_2, \ldots, \lambda_k > 0$ i permutacijske matrice $A_2, \ldots, A_k$ tako da je $A' = \sum_{i=1}^k \lambda_i A_i$, pa je $A = \sum_{i=1}^k \lambda_i A_i$, što smo i htjeli. □

Savršena sparivanja

Sada ćemo karakterizirati grafove koji dopuštaju savršena sparivanja. **Komponenta grafa** je **neparna** ili **parna** ako ima neparan ili paran broj vrhova. Za graf G, označimo s $c_o(G)$ broj neparnih komponenti od G.

TEOREM 27 (W. Tutte, 1947.). *Graf $G = (V, E)$ ima savršeno sparivanje ako i samo ako vrijedi* ("Tutteov uvjet"):

$$c_o(G - S) \leq |S|, \quad \forall S \subseteq V. \tag{$*$}$$

Prije dokaza izvedimo sljedeću posljedicu.

KOROLAR 22 (Petersen, 1891.). *3-regularni graf G bez reznih bridova ima savršeno sparivanje.*

Dokaz. Neka je $S \subseteq V$, a $G_1, G_2, \ldots, G_k$ sve neparne komponente od $G - S$, te m_i broj bridova s jednim krajem u S, a drugim u G_i, $1 \leq i \leq k$. G nema reznih

[30] Garrett Birkhoff (1911 – 1996), američki matematičar

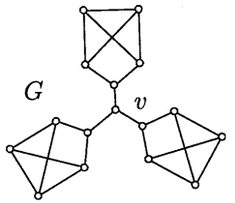
[31] John von Neumann (1903 – 1957), američki matematičar mađarskog podrijetla.

bridova pa je $m_i \neq 1$. Zbog 3-regularnosti od G, slijedi da je $\sum_{v\in V_i} d(v) = 3|V_i|$, te $\sum_{v\in S} d(v) = 3|S|$, gdje je $V_i = V(G_i)$, $1 \leq i \leq k$. Iz prve jednakosti slijedi da je $m_i = \sum_{v\in V_i} d(v) - 2e(G_i)$ neparan broj, pa je $m_i \geq 3$, za svako i. Odavde i iz druge jednakosti slijedi

$$c_o(G-S) = k \leq \frac{1}{3}\sum_{i=1}^{k} m_i \leq \frac{1}{3}\sum_{v\in S} d(v) = |S|.$$

Stoga, Tutteov Teorem 27 povlači da G ima savršeno sparivanje. □

Napomenimo da 3-regularan graf s reznim bridovima (i to barem tri njih) ne mora imati savršeno sparivanje. Primjer za to je graf G na donjoj slici (uzmite $S = \{v\}$):



Dokaz Teorema 27. Nužnost je gotovo očita. Neka je M savršeno sparivanje u G. Tada za svaku neparnu komponentu od $G-S$ postoji brid iz M koji je spaja sa S. Ako je B skup svih takvih bridova, onda je $c_o(G-S) \leq |B| \leq |S|$. Dovoljnost ćemo dokazati indukcijom po veličini od G. Uzmemo li u $(*)$ da je $S = \emptyset$, dobivamo da je svaka komponenta od G parna i stoga $|V|$ paran. Stoga su $|S|$ i $c_o(G-S)$ iste parnosti, za sve $S \subseteq V$. Zbog toga, ako je $c_o(G-S) < |S|$, za sve neprazne $S \subseteq V$, možemo ukloniti bilo koji par susjednih vrhova u, v iz G. Tada će $(*)$ i dalje vrijediti, pa po pretpostavci indukcije, postoji savršeno sparivanje M' od $G-\{u,v\}$. Tada je $M' \cup \{uv\}$ savršeno sparivanje od G.

Uzmimo stoga da postoji $\emptyset \neq S \subseteq V$ tako da je $c_o(G-S) = |S|$ i neka je S odabran tako da je maksimalan skup s tim svojstvom. Označimo s X skup svih vrhova iz $V \setminus S$ iz parnih komponenti od $G-S$.

Prvo, inducirani podgraf $G[X]$ ima savršeno sparivanje, jer kad ga ne bi imao, onda bi po indukciji postojao $S' \subseteq X$ tako da $G[X]-S'$ ima više od $|S'|$ neparnih komponenti. No tada se odmah vidi da za skup $S \cup S'$ ne vrijedi $(*)$ za G.

Drugo, neka je K skup svih vrhova neke neparne komponente od $G-S$, a $v \in K$ bilo koji vrh. Tvrdimo da i $G[K \setminus \{v\}]$ ima savršeno sparivanje. Kad ne bi bilo tako, onda bi po indukciji postojao skup $\overline{S} \subseteq K \setminus \{v\}$ tako da $G[K \setminus (\overline{S} \cup \{v\})]$ ima barem $|\overline{S}|+2$ neparnih komponenti. Stoga $G-(S \cup \overline{S} \cup \{v\})$ ima barem $|S \cup \overline{S} \cup \{v\}|$ neparnih komponenti, što je u kontradikciji s maksimalnošću od S.

Konačno, neka je $\overline{G}$ bipartitni graf dobiven iz $G-X$ tako da uklonimo sve bridove s vrhovima iz S, a svaku neparnu komponentu od $G-S$ kontraktiramo u jedan pseudovrh. Neka je W skup svih tih pseudovrhova (neki od njih mogu biti i obični vrhovi od G). Ako $\overline{G}$ ima savršeno sparivanje, onda smo gotovi, jer tada savršeno sparivanje od $\overline{G}$ zajedno sa savršenim sparivanjem od $G[X]$ i savršenim

sparivanjem od $G'-v$, za svaku neparnu komponentu G' od $G-S$ i pogodnim vrhom v iz G', daju savršeno sparivanje od G.

Kad $\overline{G}$ ne bi imao savršeno sparivanje, onda bi prema Hallovom teoremu 26 postojao $W' \subseteq W$, tako da je $|N_{\overline{G}}(W')| < |W'|$. No tada skup $S^* = N_{\overline{G}}(W') \subseteq S$ ne zadovoljava $(*)$, što je kontradikcija. □

Kao i Hallov teorem, i Tutteov teorem je osnova za polinomski algoritam (složenosti $O(n^3)$) koji za dani graf G ili nalazi savršeno sparivanje ili nalazi $S \subseteq V$ takav da je $c_o(G-S) > |S|$, a izvjesnim modifikacijama i algoritam koji za dani težinski graf nalazi sparivanje ili savršeno sparivanje maksimalne težine.

Neki primjeri i algoritmi sparivanja

U proučavanjima sparivanja od koristi je i polinom sparivanja. Označimo s $m(G,k)$ broj sparivanja u G s točno k bridova. ($m(G,0) := 1$). Ako graf G ima n vrhova, onda se **polinom sparivanja** od G definira kao

$$M(G,x) := \sum_{k=0}^{\lfloor n/2 \rfloor} (-1)^k m(G,k) x^{n-2k}.$$

Primjer 51. a) Odredite $m(G,k)$ i polinom sparivanja, ako je graf G:
1) put P_n s n vrhova; 2) ciklus C_n s n vrhova; 3) K_n; 4) $K_{n,n}$; 5) bipartitan graf $T(n)$ s biparticijom (X,Y), gdje je $X = \{1,2,\ldots,n\}$, $Y = \{1',2',\ldots,n'\}$, a $i \sim j' \iff i > j$; 6) $G = L_n$ ljestve s n prečaka, a $k = n$.

b) Dokažite da za $M(G,x)$ vrijedi rekurzija $M(G,x) = M(G-e,x) - M(G-u-v,x)$, gdje je $e = uv \in E(G)$.

Rješenje. a) 1) Među $n-1$ segmenata $12, 23, \ldots, (n-1)n$ treba izabrati njih k tako da nema susjednih. Iz Primjera 41 u poglavlju II slijedi da je traženi broj $m(P_n,k) = \binom{n-1-k+1}{k} = \binom{n-k}{k}$.
Polinom sparivanja je $M(P_n,x) = \sum_{k\geq 0}(-1)^k\binom{n-k}{k}x^{n-2k} = x^n\sum_{k\geq 0}\binom{n-k}{k}(-\frac{1}{x^2})^k$. Sumu $a_n = \sum_{k\geq 0}\binom{n-k}{k}z^k$ izračunamo tako da rabeći Pascalovu formulu dobivamo rekurziju $a_n = a_{n-1} + za_{n-2}$ s početnim vrijednostima $a_0 = a_1 = 1$ i onda poznatim metodama rješavanja takve rekurzije dobivamo za $z \neq -1/4$:

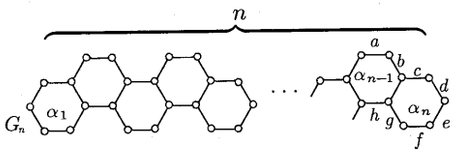
$$a_n = \frac{1}{\sqrt{1+4z}}\left[\left(\frac{1+\sqrt{1+4z}}{2}\right)^{n+1} - \left(\frac{1+\sqrt{1+4z}}{2}\right)^{n+1}\right],$$

te $a_n = (n+1)/2^n$ za $z = -1/4$. Uvrstimo li $z = -1/x^2$ dobivamo $M(P_n,x)$. Za ostale rezultate navest ćemo samo $m(G,k)$; uvjerite se u te rezultate s "umjetnošću prebrojavanja": 2) $m(C_n,k) = \frac{n}{n-k}\binom{n-k}{k}$; 3) $m(K_n,k) = \frac{n!}{k!(n-2k)!2^k}$; 4) $m(K_{n,n};k) = \binom{n}{k}^2 k!$; 5) $m(T(n),k) = S(n,n-k)$ (Stirlingov broj 2. vrste); 6) $m(L_n,n) = F_{n+1}$.

b) Tvrdnja slijedi lako iz $m(G,k) = m(G-e,k) + m(G-u-v,k-1)$, a ovo slijedi iz toga što sparivanje ili sadrži brid e ili ga ne sadrži. □

Evo jednog primjera iz fizikalne kemije.

Primjer 52. Koliko savršenih sparivanja ima graf G_n koji se sastoji od n šesterokuta $\alpha_1, \alpha_2, \ldots, \alpha_n$ pozicioniranih u cik-cak poziciji kao na sl.



Broj vrhova $v(G_n) = 4n + 2$, a bridova $e(G_n) = 5n + 1$. To je molekularni graf izvjesnih benzenoidnih policikličkih ugljikovodika: $C_{4n+2}H_{2n+4}$. Za kemičare taj problem glasi: koliko Kekuléovih struktura ima ova molekula?

Rješenje. Označimo traženi broj s $K(n)$. Označimo segmente na zadnja dva šesterokuta s α_{n-1} i α_n s $a, b, \ldots, h$ kao na slici. Skup M svih savršenih sparivanja od G_n se može particionirati kao $M = M_c \cup M_d$, gdje su $M_c, M_d \subseteq M$ skupovi sparivanja od G_n koje sadrži segment c, odnosno d. Savršeno sparivanje od G_n koje sadrži segment c mora sadržavati i segmente a, e i g, pa je očito $\#M_c = K(n-2)$, tj. to je broj savršenih sparivanja od $G_n - \alpha_{n-1} - \alpha_n$. Savršeno sparivanje od G_n koje sadrži segment d, mora sadržavati i segment f, pa je $\#M_d = K(n-1)$, tj. to je broj savršenih sparivanja od $G_n - \alpha_n$. Zato je $K(n) = K(n-2) + K(n-1)$. Lako se vidi da je $K(1) = 2$, $K(2) = 3$. Stoga je $K(n) = F_{n+1}$ (Fibonaccijev broj). □

Sada ćemo dati opću formulu za broj savršenih sparivanja uravnoteženog bipartitnog grafa. Za to nam treba pojam permanente matrice. **Permanenta** $n \times n$ **matrice** $A = [a_{ij}]$ je broj per A definiran (kao i determinanta, samo bez predznaka) s:

$$\text{per } A = \sum_{\pi \in S_n} a_{1\pi(1)} a_{2\pi(2)} \cdots a_{n\pi(n)} \cdot$$

Primjer 53. Neka su $X = \{x_1, x_2, \ldots, x_n\}$, $Y = \{y_1, y_2, \ldots, y_n\}$ dva n-skupa, a G bipartitni graf s biparticijom (X, Y), te $P(G) = [p_{ij}]$ $n \times n$ matrica, $p_{ij} = 1$, ako je $x_i y_j \in E(G)$, $p_{ij} = 0$, ako $x_i y_j \notin E(G)$. Tada je per $P(G)$ jednak broju savršenih sparivanja od G.

Rješenje. Svaki član sumacije u per $P(G)$ je jednak 1 ako su svi članovi $p_{ij} = 1$, a 0 inače. Stoga je član jednak 1 ako i samo ako odgovarajući bridovi čine savršeno sparivanje u G. Dakle, per $P(G) \neq 0$ ako i samo ako G ima savršeno sparivanje, a njihov broj je očito jednak per $P(G)$. □

Bilješka. Van der Waerdenova slutnja iz 1927. kaže da za dvostruko stohastičku $n \times n$ matricu vrijedi per $A \geq n!/n^n$ s jednakošću ako i samo ako su svi članovi $1/n$. Ta je slutnja dokazana 1981. (Falikman i Egoričev). To onda povlači da r-regularan bipartitan graf s dva n-člana skupa biparticije ima barem $n!(r/n)^n$ savršenih sparivanja.

Opišimo ukratko algoritam kojim se rješava (posebni slučaj) **problema zapošljavanja**: svatko od n ljudi $x_1, \ldots, x_n$ može obavljati jedan ili više od n poslova $y_1, \ldots, y_n$. Mogu li se oni zaposliti tako da svatko radi posao koji može obavljati?

Konstruiramo li bipartitan graf G s biparticijom (X, Y), $X = \{x_1, x_2, \ldots, x_n\}$, $Y = \{y_1, y_2, \ldots, y_n\}$, pri čemu je $x_i \sim y_j$ ako i samo ako x_i može obavljati posao y_j, onda taj problem ekvivalentan s problemom ima li G savršeno sparivanje.

Sljedeći algoritam ili konstruira savršeno sparivanje u G ili stane kada nađe podskup $S \subset X$ za koji je $|N(S)| < |S|$, pa prema Hallovom teoremu G nema savršeno sparivanje. Ideja je da započnemo s nekim sparivanjem M na G (M može biti i prazan, ako ne znamo ništa bolje). Ako M zasićuje X, onda je ono i savršeno. Ako pak postoji M-nezasićen vrh $u \in X$, onda algoritam sustavno traži M-uvećani put P s početkom u. Tada se dobiva veće sparivanje $M' = M \triangle E(P)$ s kojim je zasićeno više vrhova u X nego s M i tada ponovimo postupak s M' umjesto s M. Ako takav put P ne postoji, nađemo skup R svih vrhova koji su s vrhom u povezani M-alternirajućim putom. Tada za skup $S = R \cap X$ vrijedi $|N(S)| < |S|$. Taj je algoritam dao J. Edmonds 1965., a zove se **mađarska metoda** (jer se zasniva na idejama Mađara Königa i Egervaryja).

Algoritam mađarske metode

Ulaz. Bipartitni graf G s biparticijom (X, Y), $|X| = |Y|$.

Izlaz. Savršeno sparivanje u G ili skup $S \subseteq X$, za koji je $|N(S)| < |S|$.

Korak 1. Neka je M bilo koje sparivanje od G, npr. $M = \emptyset$.

Korak 2. Ako je X M-zasićen, stop. (M je savršeno sparivanje od G.) U protivnome, neka je $u \in X$ M-nezasićen. Stavimo $S = \{u\}$, $T = \emptyset$.

Korak 3. Ako je $N(S) = T$, stop. ($|N(S)| < |S|$, pa G nema savršeno sparivanje.) U protivnome, neka je $y \in N(S) \setminus T$.

Korak 4. Ako je y M-zasićen, neka je $yz \in M$. Zamijenimo S sa $S \cup \{z\}$, a T sa $T \cup \{y\}$ i vratimo se na korak 3. Ako je y M-nezasićen, neka je P M-uvećani (u, y)-put. Zamijenimo M s $M' = M \triangle E(P)$ i vratimo se na korak 2.

Nije teško pokazati da je složenost ovog algoritma $O(n^3)$, gdje je $n = |V(G)|$. Modifikacijama ovog algoritma može se dobiti algoritam koji za bilo koji graf G ili nalazi savršeno sparivanje od G ili skup $S \subseteq V(G)$ za koji je $c_o(G - S) > |S|$, pa prema Tutteovom teoremu 27, G nema savršeno sparivanje, i onda nalazi maksimalno sparivanje (rabeći Bergov teorem 24). Isto se tako mogu dobiti i težinske verzije, što je za praksu najvažnije. Na primjer, **problem optimalnog zapošljavanja** može se ovako formulirati. Zadan je potpun bipartitan graf G s biparticijom (X, Y), $|X| = |Y| = n$ (dakle, $G \approx K_{n,n}$) i zadane su težine (ili cijene) $c_{ij} = w(x_i y_j) \geq 0$ bridova ($x_i \in X, y_j \in Y$). Treba naći savršeno sparivanje u težinskom grafu (G, w) koje je maksimalne težine, tj. suma težina bridova u tom sparivanju je maksimalna (ili dualno, minimalne težine).

Mi se ovdje nećemo upuštati u konstrukcije i analize ovog i drugih kombinatornih algoritama, i probleme kombinatorne optimizacije, te analize pripadnih algoritama, nego zainteresiranog čitatelja upućujemo na odgovarajuću literaturu, npr. knjige [2], [70], [83], [97], [137], [173], te [148], te [7*], [42*], [45*], [64*] i neke članke u [35*].

§ 8. Ekstremalna teorija grafova

Tipični problem ekstremalne teorije grafova jest sljedeći. Neka je G jednostavni graf s n vrhova, a $\mathcal{P}$ neko svojstvo grafova. Koliko najviše bridova može imati G, tako da ima svojstvo $\mathcal{P}$? Posebno je zanimljiv slučaj kad svojstvo $\mathcal{P}$ glasi: "G ne sadrži podgraf izomorfan nekom čvrstom grafu H". Graf H se zove **zabranjeni podgraf**. Dakle, koliko najviše bridova može imati G, ako nema neki čvrsti H kao podgraf , (tj. $G \not\supseteq H$). Neke posebne slučajeve, npr. kad je $H = K_3$ (trokut) već smo razriješili (usp. Teorem 3) ili $H = C_4$ (usp. Primjer 23).

Počnimo sada s najjednostavnijim zabranjenim podgrafovima: putovima i ciklusima. I to smo zapravo razriješili. Naime, ne upuštajući se u detalje, nije teško pokazati da Diracov teorem 6 (i diskusiju iza) možemo ovako preformulirati.

TEOREM 6' (Dirac). *Neka je G jednostavan povezan graf s $n \geq 3$ vrhova tako da je $d(x) + d(y) \geq r$ za svaki par nesusjednih vrhova $x, y \in V(G)$. Tada vrijedi sljedeće.*

(i) Ako je $r = n$, onda G sadrži Hamiltonov ciklus;

(ii) Ako je $r < n$, onda $G \supseteq P_r$ (put) i $G \supseteq C_{\lceil (r+1)/2 \rceil}$ (ciklus).

Posljedica je sljedeća.

KOROLAR 23. *a) Neka je G graf s n vrhova. Ako G ne sadrži put duljine r, onda je*

$$|E(G)| \leq \frac{r-1}{2} n,$$

s jednakošću ako i samo ako je svaka komponenta od G izomorfna s K_r.
b) Slično, ako G ne sadrži ciklus duljine $\geq r$, onda G ima $\leq (r-1)(n-1)/2$ bridova.

Dokaz. a) Indukcijom po n. Ako je $n \leq r$, tvrdnja je trivijalna. Neka je $n > r$. Ako je G nepovezan, onda primjenom pretpostavke indukcije na svaku komponentu tvrdnja lako slijedi.

Neka je G povezan. Tada prema Teoremu 6' (ii), G ima vrh x, tako da je $d(x) < r/2$, jer bi inače $G \supseteq P_r$. Tada graf $G - x$ nije disjunktna unija grafova izomorfnih s K_r. Po pretpostavci indukcije, imamo da je $|E(G-x)| < (r-1)(n-1)/2$, pa je

$$|E(G)| = |E(G-x)| + d(x) < \frac{(r-1)(n-1)}{2} + \frac{r-1}{2} = \frac{r-1}{2} n.$$

Dokaz za cikluse je sličan. □

Sada promotrimo najzanimljiviji slučaj kada je zabranjeni podgraf potpun graf K_r. Podgraf koji je izomorfan grafu K_r zove se r-**klika** u grafu. Dakle, pitamo se koliko najviše bridova ima jednostavni graf G koji ne sadrži r-kliku kao podgraf (dakle, $G \not\supseteq K_r$)?

Prije nego što se upustimo u to pitanje, evo jednog "konkretnog" primjera kojim ćemo dati dovoljan uvjet da $G \supseteq K_r$, tj. da G sadrži r-kliku.

Primjer 54. Na nekom je kongresu sudjelovalo 360 matematičara. Svaki od njih ne pozna najviše 60 ostalih. Dokažite da postoji barem deset njih koji se svi međusobno poznaju.

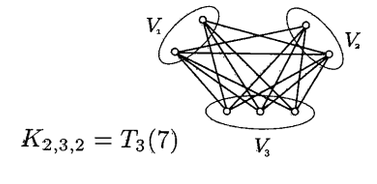
Rješenje. Neka je G graf čiji su vrhovi svi sudionici kongresa, a dva vrha spojena bridom ako i samo se odgovarajući matematičari poznaju.

Tada se tvrdnja svodi na sljedeće. Neka je G jednostavni graf s n vrhova, a $1 \neq r \in \mathbb{N}$ takav da je minimalni stupanj $\delta > \left\lfloor n \cdot \frac{r-2}{r-1} \right\rfloor$. Tada G sadrži r-kliku, tj. $G \supseteq K_r$.

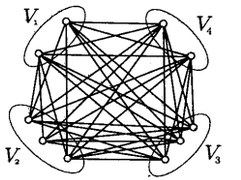
Ovu tvrdnju dokažimo kontradikcijom. Pretpostavimo suprotno, tj. $G \not\supseteq K_r$. Tada G može najviše sadržavati kliku K_{r-1} s vrhovima $v_1, v_2, \ldots, v_{r-1}$. Neka je $V_i = \{v \in V(G) \mid v \not\sim v_i\}$, $i = 1, \ldots, r-1$. Tada je $\bigcup_{i=1}^{r-1} V_i = V$, pa je $n = |\bigcup_{i=1}^{r-1} V_i| \leq \sum_{i=1}^{r-1} |V_i| \leq (r-1)(n-\delta)$, a to je u proturječju s pretpostavkom. U našem je slučaju $n = 360$, $r = 10$, pa tvrdnja slijedi. □

Ako nas zanima kada $G \not\supseteq K_r$, onda je prirodno promotriti $(r-1)$-**partitni graf**, tj. onaj kojem je skup vrhova particioniran u $r-1$ podskupova $V_1, V_2, \ldots, V_{r-1}$ s tim da nikoja dva vrha iz iste klase V_i nisu spojena bridom. Ali, želimo li u nekom smislu takve optimalne grafove, onda je osnovna ideja da se skup vrhova od G particionira u $r-1$ podjednakih klasa, a bridom spoje svaka dva vrha iz različitih klasa. Formalno, neka su $n_1, n_2, \ldots, n_{r-1} \in \mathbb{N}$, $n_1 + n_2 + \cdots + n_{r-1} = n = |V(G)|$ i neka je $V(G) = V = V_1 \cup V_2 \cup \cdots \cup V_{r-1}$ particija s $|V_i| = n_i$, $i = 1, \ldots, r-1$. Bridom spojimo dva vrha ako i samo ako su u različitim klasama V_i. To je **potpun** $(r-1)$-**partitni graf** i označava se s $K_{n_1, n_2, \ldots, n_{r-1}}$; on ima $n_1 + \cdots + n_{r-1} = n$ vrhova i $\sum_{i \neq j} n_i n_j$ bridova. Među takvim grafovima najviše bridova ima onaj kod kojeg je ukupni broj vrhova n podijeljen u gotovo jednake dijelove n_i, tj. $n_i = \lfloor \frac{n}{r-1} \rfloor$ ili $\lceil \frac{n}{r-1} \rceil$, za sve i, $1 \leq i \leq r-1$. To je ekvivalentno s time da je $|n_i - n_j| \leq 1$, za sve i, j. Zaista, kad bi, primjerice, bilo $n_1 \geq n_2 + 2$, onda bi prebacivanjem jednog vrha iz V_1 u V_2 dobili $K_{n_1-1, n_2+1, \ldots, n_{r-1}}$, a taj ima $(n_1 - 1)(n_2 + 1) - n_1 n_2 = n_1 - n_2 - 1 \geq 1$ više bridova nego $K_{n_1, n_2, \ldots, n_{r-1}}$.

Graf $K_{n_1, \ldots, n_{r-1}}$ s $|n_i - n_j| \leq 1$, $\forall i, j$ zove se **ujednačeno potpun** $(r-1)$-**partitni graf** ili kratko **Turánov graf** $T_{r-1}(n)$. Očito, $K_r \not\subseteq T_{r-1}(n)$, jer čak ni $(r-1)$-partitni graf ne sadrži K_r. Dva Turánova grafa su na slici:



$K_{2,3,2} = T_3(7)$



$K_{2,3,3,2} = T_4(10)$

Broj bridova $t_{n-1}(n) := e(T_{r-1}(n))$ u Turánovom grafu je očito jednak

$$t_{r-1}(n) = \binom{n}{2} - \sum_{i=1}^{r-1} \binom{n_i}{2} = \sum_{1 \leq i < j \leq r-1} \left\lfloor \frac{n+i-1}{r-1} \right\rfloor \left\lfloor \frac{n+j-1}{r-1} \right\rfloor,$$

gdje je $n_i = \lfloor (n+i-1)/(r-1) \rfloor$ broj vrhova u i-toj najmanjoj klasi. Ako $r-1$ dijeli n, možemo uzeti $n_i = \frac{n}{r-1}$, za svako i, pa je tada broj bridova jednak

$$\binom{r-1}{2} \left(\frac{n}{r-1} \right)^2 = \left(1 - \frac{1}{r-1} \right) \frac{n^2}{2}.$$

Turánov teorem tvrdi da je to gornja međa za broj bridova svakog (jednostavnog) grafa s n vrhova bez r-klika i da je $T_{r-1}(n)$ jedini ekstremalni graf.

TEOREM 28 (P. Turán, 1941.). *Ako graf G na n vrhova nema r-klika, $r \geq 2$, onda je*

$$|E(G)| \leq \left(1 - \frac{1}{r-1}\right)\frac{n^2}{2}. \qquad (*)$$

Jednakost se dostiže ako i samo ako je G izomorfan s $T_{r-1}(n)$.

Dokaz. Indukcijom po n. Za $n = 1$, tvrdnja je trivijalna. Neka je G graf na n vrhova, bez r-klika i s maksimalnim brojem bridova. Tada G sadrži $(r-1)$-kliku, jer bi inače mogli dodati još bridova. Neka je $G_1 \subseteq G$ jedna $(r-1)$-klika, a $G_2 = G - V(G_1)$. Tada je $e(G_1) = \binom{r-1}{2}$. Sada ćemo ocijeniti $e(G_2)$ i broj e_{12} bridova između G_1 i G_2. Prvo, po pretpostavci indukcije je $e(G_2) \leq \frac{1}{2}(1 - \frac{1}{r-1})(n-r+1)^2$. Kako G nema r-kliku, to je svaki vrh $v \in V(G_2)$ spojen s najviše $r-2$ vrhova iz G_1. Zato je $e_{12} \leq (r-2)(n-r+1)$. Sve u svemu, dobivamo

$$|E(G)| \leq \binom{r-1}{2} + \frac{1}{2}(1 - \frac{1}{r-1})(n-r+1)^2 + (r-2)(n-r+1) = (1 - \frac{1}{r-1})\frac{n^2}{2}.$$

Treba još pokazati da je $T_{r-1}(n)$ jedini ekstremalni graf. Dakle, neka je G graf s n vrhova, $e(G) = t_{r-1}(n)$ i $G \not\supseteq K_r$. Tvrdimo da je $G \approx T_{r-1}(n)$. I ovo ide indukcijom po n.

No, prvo uočimo da su stupnjevi vrhova od $T_{r-1}(n)$ također gotovo jednaki, jer je minimalni stupanj $\delta(T_{r-1}(n)) =: \delta_{r-1}(n) = \lfloor 2t_{r-1}(n)/n \rfloor = \lfloor n - \frac{n}{r-1} \rfloor = n - \lceil \frac{n}{r-1} \rceil$, a maksimalni stupanj $\Delta(T_{r-1}(n)) =: \Delta_{r-1}(n) = \lceil 2t_{r-1}(n)/2 \rceil = \lceil n - \frac{n}{r-1} \rceil = n - \lfloor \frac{n}{r-1} \rfloor$. Ako je $x \in V(T_{r-1}(n))$ vrh minimalnog stupnja, onda je $T_{r-1}(n) - x \approx T_{r-1}(n-1)$, pa je $t_{r-1}(n) - \delta_{r-1}(n) = t_{r-1}(n-1)$. Konačno, kako je $\delta_{r-1}(n) = n - 1 - \lfloor \frac{n-1}{r-1} \rfloor$, slijedi da je vrh x spojen sa svim vrhovima od $T_{r-1}(n-1)$ osim s vrhovima iz najmanje klase.

Ako je $n \leq r-1$, nemamo što dokazivati, pa uzmimo $n \geq r$, i graf G reda n, veličine $t_{r-1}(n)$ i bez r-klike. Neka je x vrh u G minimalnog stupnja. Tada je $d(x) = \delta(G) \leq \lfloor 2e(G)/n \rfloor = \lfloor 2t_{r-1}(n)/n \rfloor = \delta_{r-1}(n)$. Neka je $H = G - x$. Tada je $e(H) = e(G) - d(x) \geq t_{r-1}(n) - \delta_{r-1}(n) = t_{r-1}(n-1)$. Kako $H \not\supseteq K_r$, po pretpostavci indukcije slijedi $H \approx T_{r-1}(n-1)$ i $d(x) = \delta_{r-1}(n)$. Vrh x ne može biti spojen s $r-1$ vrhova u različitim klasama od $H \approx T_{r-1}(n-1)$, jer bi inače tih r vrhova tvorilo K_r. Stoga u $T_{r-1}(n-1)$ postoji klasa čiji nijedan vrh nije spojen s x. Ta klasa mora biti najmanja, a x spojen sa svim ostalim vrhovima u svim ostalim klasama. To znači da G baš mora biti (izomorfan s) $T_{r-1}(n)$. □

Uočite da poseban slučaj $r = 2$ daje Mantelov teorem 3. Ako je zabranjeni graf potpun bipartitni graf $K_{r,s}$, može se pokazati da vrijedi sljedeće.

TEOREM. *Neka su $r \leq s$ čvrsti. Ako je G graf s n vrhova i bez $K_{r,s}$, onda je broj bridova od G najviše jednak $c_s n^{2-1/r}$, gdje je c_s izvjesna konstanta koja ovisi samo o s.*

Opišimo ukratko osnovni teorem ekstremalne teorije grafova. Turánov teorem kaže da ako graf G s n vrhova ima više od $|E(T_{r-1}(n))| = (1-1/(r-1))(n^2/2)+O(n)$ bridova, onda $G \supseteq K_r$. Erdös-Stoneov teorem kaže da ako je broj bridova od G barem $|E(T_{r-1}(n))| + \varepsilon n^2$, a n dovoljno velik, onda to osigurava egzistenciju potpunog r-partitnog podgrafa čije su klase velike, točnije, podgrafa $K_{t,t,\ldots,t} = T_r(rt)$.

TEOREM (P. Erdös - A. Stone, 1946.). *Neka su $r \geq 2$ i t dani čvrsti prirodni brojevi, a $\varepsilon > 0$. Tada postoji prirodni broj $n_0 = n_0(r,t,\varepsilon)$ takav da svaki graf G s $n \geq n_0$ vrhova i barem $(1 - \frac{1}{r-1} + \varepsilon)\frac{n^2}{2}$ bridova ima potpun r-partitni podgraf $K_{t,t,\ldots,t}$ koji u svakoj klasi ima t vrhova.*

Za $r = 2$, ovaj teorem kaže da za dovoljno velik n, graf s barem εn^2 bridova sadrži $K_{t,t}$, a to je posljedica i prethodnog teorema.

Zaključno kažimo da ekstremalna teorija grafova ima mnogobrojne primjene u kombinatornoj i računarskoj geometriji, npr. u proučavanju gustoće pakiranja danih tijela u neko područje, u teoriji brojeva itd. Čitatelja upućujemo na knjige [33] i [55*] i na članak B. Bollobása u [35*].

§ 9. Vjerojatnostne metode

Započnimo s kratkim "mini-kolegijem" iz (konačne) teorije vjerojatnosti. Konačni **prostor vjerojatnosti** je uređeni par (Ω, P), gdje je Ω konačni skup čiji se elementi zovu **elementarni događaji**, a $P : 2^\Omega \to [0,1]$ funkcija koja svakom podskupu $A \subseteq \Omega$ (tj. elementu iz 2^Ω), koji se zove **događaj**, pridružuje realni broj $P(A)$ koji se zove **vjerojatnost događaja** A, tako da vrijedi $P(\emptyset) = 0$, $P(\Omega) = 1$ i $P(A \cup B) = P(A) + P(B)$ za svaka dva disjunktna događaja $A, B \subseteq \Omega$.

Najjednostavniji (i možda najvažniji) primjer prostora vjerojatnosti je **Laplaceov prostor** u kojem svi elementarni događaji imaju jednaku vjerojatnost $P(\{w\}) = 1/|\Omega|$, pa je vjerojatnost u tom prostoru zadana formulom ("povoljni kroz mogući"):

$$P(A) = \frac{|A|}{|\Omega|}, \quad \text{za svaki događaj } A \subseteq \Omega.$$

U teoriji je grafova najvažniji prostor vjerojatnosti tzv. **slučajni grafovi** $\mathcal{G}_n$ čiji su elementarni događaji svi grafovi na skupu vrhova $\{1, 2, \ldots, n\}$, a svi imaju istu vjerojatnost $2^{-\binom{n}{2}}$.

Dva događaja $A, B \subseteq \Omega$ su **nezavisna** ako je $P(A \cap B) = P(A)P(B)$, a više događaja $A_1, A_2, \ldots, A_k$ su **nezavisni** ako je $P(\cap_{i \in I} A_i) = \prod_{i \in I} P(A_i)$, $\forall I \subseteq [k]$. **Slučajna varijabla** X na prostoru vjerojatnosti (Ω, p) je bilo koja funkcija $X : \Omega \to \mathbb{R}$. Na njezinoj slici $X(\Omega)$ definiramo prostor vjerojatnosti formulom $P(X = x) := \sum_{X(\omega)=x} P(\omega)$ (kraće pišemo $P(\omega)$ umjesto $P(\{\omega\})$).

Očekivanje slučajne varijable (engl. *expectation*) $E(X)$ od X definira se kao $E(X) := \sum_{\omega \in \Omega} P(\omega)X(\omega)$, tj. to je očekivani prosječni broj pojava X. U Laplaceovom prostoru očekivanje je baš aritmetička sredina (prosjek) vrijednosti od X, tj. $E(X) = 1/|\Omega| \sum_{\omega \in \Omega} X(\omega)$.

Za svaki događaj A, **indikator** od A je njegova karakteristična funkcija, tj. to je slučajna varijabla $I_A : \Omega \to \{0,1\} \subseteq \mathbb{R}$, $I_A(\omega) = 1$ za $\omega \in A$, $I_A(\omega) = 0$ za $\omega \notin A$. Jasno, $E(I_A) = P(A)$.

Važno je svojstvo očekivanja njezina linearnost. Naime, ako su X i Y slučajne varijable, onda je i $X + Y$ slučajna varijabla i imamo

$$E(X+Y) = \sum_{\omega\in\Omega} P(\omega)\,[X(\omega)+Y(\omega)] = \\ = \sum_{\omega\in\Omega} P(\omega)X(\omega) + \sum_{\omega\in\Omega} P(\omega)Y(\omega) = E(X) + E(Y), \tag{4}$$

a isto je tako i za $\lambda \in \mathbb{R}$, $E(\lambda X) = \lambda E(X)$.

Ako slučajna varijabla X poprima samo nenegativne vrijednosti, tj. $X(\omega) \geq 0$, $\forall\omega \in \Omega$, te ako je zadan pozitivan broj a, onda je vjerojatnost da X poprima vrijednosti barem a jednaka $P(X \geq a) = \sum_{\omega, X(\omega)\geq a} P(\omega)$. Za očekivanje $E(X)$ tada vrijedi sljedeće:

$$E(X) = \sum_{\omega, X(\omega)\geq a} P(\omega)X(\omega) + \sum_{\omega, X(\omega)<a} P(\omega)X(\omega) \geq a \sum_{\omega, X(\omega)\geq a} P(\omega),$$

pa odavde slijedi **Markovljeva nejednakost** $P(X \geq a) \leq \frac{E(X)}{a}$.

Ne samo u teoriji grafova, nego i uopće u diskretnoj matematici vjerojatnosnim se postupcima i metodama mogu napasti mnogi problemi. Grubo govoreći, bit te metode sastoji se u sljedećem. Recimo da želimo dokazati da postoji izvjesna struktura (npr. konfiguracija s nekim svojstvima). Tada konstruiramo izvjesni prostor vjerojatnosti za takve strukture i pokažemo da u tom prostoru, tražena struktura ima (strogo) pozitivnu vjerojatnost. Zato takva struktura postoji. Najbolje ćemo to opisati nekim primjerima. Sjetimo se da je **Ramseyev broj** $R(k,l)$ najmanji broj $n \in \mathbb{N}$, takav da za svako 2-bojenje bridova potpunog grafa K_n crvenom i plavom bojom, u K_n postoji ili crveni podgraf K_k ili plavi K_l, tj. jednobojni (ili monokromatski) podgraf dane veličine. Znamo kako je teško računati Ramseyeve brojeve. Vjerojatnosnom metodom ćemo sada dati jednu donju među za Ramseyeve brojeve $R(k,k)$.

PROPOZICIJA 28 (P. Erdös, 1947). *Ako je* $\binom{n}{k}\cdot 2^{1-\binom{k}{2}} < 1$, *onda je* $R(k,k) > n$. *Posebno, za* $k \geq 3$ *je* $R(k,k) > \lfloor 2^{k/2}\rfloor$. *(Ustvari, može se pokazati da je* $R(k,k) > \frac{1}{e\sqrt{2}}(1+o(1))k2^{k/2}$.*)*

Dokaz. Promotrimo prostor vjerojatnosti čiji su elementarni događaji sva slučajna 2-bojenja bridova potpunog grafa K_n s crvenom i plavom bojom; sva bojenja su jednako vjerojatna, tj. svaki se brid neovisno o drugima oboji crvenom bojom s jednako vjerojatna, tj. svaki se brid neovisno o drugima oboji crvenom bojom s vjerojatnošću $1/2$ (pa zato i plavom bojom s vjerojatnošću $1/2$). Za svaki (čvrst) skup $R \subseteq V(K_n)$ od k vrhova, neka je A_R događaj da je inducirani podgraf s R jednobojan (tj. da su mu svi bridovi crveni ili su mu svi bridovi plavi). Vjerojatnost da je taj podgraf crveni je $2^{-\binom{k}{2}}$, a da je plavi također $2^{-\binom{k}{2}}$. Stoga je vjerojatnost

$P(A_R) = 2^{1-\binom{k}{2}}$. Skup R možemo odabrati na $\binom{n}{k}$ načina, pa je vjerojatnost da se dogodi barem jedan od događaja iz A_R najviše jednaka $\binom{n}{k}2^{1-\binom{k}{2}} < 1$. Stoga je vjerojatnost da se ne dogodi nijedan od događaja A_R jednaka $1 - \binom{n}{k}2^{1-\binom{k}{2}} > 0$. To znači da je vjerojatnost da nijedna k-klika nije jednobojna pozitivna, pa stoga (zbog konačnosti skupa svih bojenja) postoji 2-bojenje bridova od K_n bez jednobojnih K_k. Zato je $R(k,k) > n$. Za $k \geq 3$, uzmemo li $n = \lfloor 2^{k/2}\rfloor$, imamo da je $\binom{n}{k}2^{1-\binom{k}{2}} < \frac{2^{1+k/2}}{k!}\cdot\frac{n^k}{2^{k^2/2}} = \frac{2^{1+k/2}}{k!}\cdot\left(\frac{n}{2^{k/2}}\right)^k \leq \frac{2^{1+k/2}}{k!} < 1$, pa je $R(k,k) > \lfloor 2^{k/2}\rfloor$. □

U ovoj se Propoziciji očituje bit vjerojatnosne metode. Da dokažemo postojanje dobrog bojenja, mi nismo našli neko eksplicitno bojenje, nego smo na nekonstruktivan način pokazali da ono postoji. Međutim, kako je za velike k, broj $\frac{2^{1+k/2}}{k!} << 1$, intuitivno je jasno da slučajno bojenje od K_n vrlo vjerojatno neće sadržavati jednobojni $K_{\lfloor 2\log_2 n\rfloor}$ podgraf. To znači da ako moramo naći neko 2-bojenje bridova od, recimo, K_{1024} bez jednobojnih K_{20}, onda K_{1024} obojimo na slučajan način, npr. bacanjem novčića $\binom{1024}{2}$ puta. Vjerojatnost da smo time dobili jednobojni K_{20} je manja od $2^{11}/20!$, dakle, vrlo, vrlo mala (sigurno manja od vjerojatnosti da u ovoj knjizi ima grešaka, a koja je ≈ 1). Takve analize vode do efikasnih **vjerojatnosnih algoritama**.

Pogledajmo sada jednu primjenu ovih metoda na turnire. Neka je T turnir s n igrača (tj. orijentirani K_n) označenih s $1, 2, \ldots, n$, dakle $V(T) = [n]$, a $(i,j) \in A(T)$ ako i samo ako je igrač i pobijedio igrača j. Kazat ćemo da turnir ima svojstvo S_k ako za svaki skup od k igrača postoji jedan koji je pobijedio sve ostale. Postoji li za svako k turnir sa svojstvom S_k? Prirodno je ovdje promotriti *slučajni* turnir, tj. turnir s vrhovima iz $[n]$, tako da za svako $i < j$, neovisno o drugima, biramo hoće li (i,j) ili (j,i) biti luk. Stoga ukupno imamo $2^{\binom{n}{2}}$ turnira s n vrhova, koji su svi jednako vjerojatni. Ako je n dovoljno velik s obzirom na k, onda je prilično vjerojatno da će slučajni turnir s n vrhova imati svojstvo S_k.

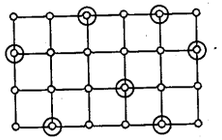
PROPOZICIJA 29. *Ako je* $\binom{n}{k}(1-2^{-k})^{n-k} < 1$, *onda postoji turnir s* n *vrhova koji ima svojstvo* S_k.

Dokaz. Promotrimo slučajni turnir na skupu $V = [n]$. Za svaki podskup $K \subseteq [n]$, $|K| = k$, neka je A_K događaj da nijedan igrač iz K nije pobijedio sve ostale igrače iz K. Za svako $i \in [n] \setminus K$ vjerojatnost da i nije pobijedio sve ostale iz K je $1 - 2^{-k}$, a za različite $i \in [n] \setminus K$, ti su događaji nezavisni. Stoga je vjerojatnost $P(A_K) = (1-2^{-k})^{n-k}$, pa je za dano k, vjerojatnost

$$P\Big(\bigcup_{\substack{K\subseteq[n]\\|K|=k}} A_K\Big) \leq \sum_{\substack{K\subseteq[n]\\|K|=k}} P(A_K) = \binom{n}{k}(1-2^{-k})^{n-k} < 1.$$

Prema tome, s pozitivnom se vjerojatnošću nijedan A_K ne pojavljuje, pa zato postoji turnir s n vrhova koji ima svojstvo S_k. □

Sljedeća se primjena odnosi na problem dominacije u grafu. Kažemo da skup vrhova $D \subseteq V$ **dominira** grafom $G = (V, E)$, ako svaki vrh $v \in V \setminus D$ ima susjeda u D. **Problem dominacije** je naći najmanji dominacijski skup ili barem izračunati (ili omeđiti) njegovu veličinu. Tako npr. na rešetki $P_6 \times P_4$ imamo dominacijski skup D:



I to je stari problem nastao iz igara; npr. na šahovsku ploču treba postaviti najmanji broj kraljica koje će dominirati cijelom pločom (pokušajte), ili problem TV predajnika - gdje i koliko ih najmanje treba postaviti tako da sve zadane točke primaju TV-signal?

PROPOZICIJA 30. *Neka je $G = (V, E)$ graf s n vrhova i minimalnim stupnjem vrhova $\delta > 1$. Tada G ima dominirajući skup vrhova s najviše $n^{(1+\ln(\delta+1))/(1+\delta)}$ vrhova.*

Dokaz. Uzmemo li neki čvrsti broj $p \in [0, 1]$, odaberimo slučajno i nezavisno svaki vrh iz V s vjerojatnošću p. Neka je X (slučajni) skup odabranih vrhova, a $Y = Y_X$ slučajni skup svih vrhova iz $V \setminus X$ koji nemaju susjeda u X. Očekivana vrijednost od $|X|$ je očito np. Za svaki čvrsti vrh $v \in V$, imamo $P(v \in Y) = P$ (v i njegovi susjedi nisu u X) $\leq (1-p)^{\delta+1}$. Slučajna varijabla $|Y|$ je suma indikatora I_v, $v \in V$, pri čemu je $I_v = 1$, ako je $v \in Y$, a $I_v = 0$ inače, pa zbog linearnosti očekivanja slijedi da je očekivana vrijednost od $|X|+|Y|$ najviše $np+n(1-p)^{\delta+1}$. Stoga postoji bar jedan $X \subseteq V$ tako da je $|X| + |Y_X| \leq np + n(1-p)^{\delta+1}$. Skup $D = X \cup Y_X$ je očito dominirajući skup od G, a ima najviše $np + (1-p)^{\delta+1}$ elemenata.

Broj p je bio čvrst, ali to vrijedi za svako $p \in [0, 1]$. Da pojednostavimo minimum, prvo imamo $1 - p \leq e^{-p}$, dobivamo $|D| \leq n\left[p + e^{-p(\delta+1)}\right]$. Deriviranjem nađemo minimum funkcije u zagradi i dobivamo

$$p = \frac{\ln(\delta+1)}{\delta+1}.$$

Stoga za tako odabrani p dobivamo dominirajući skup D s $|D| \leq n^{(1+\ln(\delta+1))/(\delta+1)}$, kao što smo tvrdili. (Iako možemo dobiti i malo bolji rezultat, za veliko δ to ne daje bitno poboljšanje.) □

Kao iduću primjenu ovih metoda, pokazat ćemo da u svakom grafu postoji veliki bipartitni podgraf.

PROPOZICIJA 31. *Neka je $G = (V, E)$ graf s n vrhova i $e(G) = m$ bridova. Tada G sadrži bipartitni podgraf s barem $m/2$ bridova.*

Dokaz. Neka je $S \subseteq V$ slučajno odabrani podskup s nezavisno odabranim elementima s vjerojatnošću $P(x \in S) = 1/2$ i neka je $T = V \setminus S$. Nazovimo brid $xy \in E$ *prijelazni* ako je $x \in S$, $y \in T$. Neka je X broj prijelaznih bridova. Izračunajmo

očekivanje $E(X)$ slučajne varijable X. Za brid $xy \in E$, neka je I_{xy} indikatorska slučajna varijabla za prijelazne bridove (tj. $I_{xy} = 1$ ako je xy prijelazni, a 0 inače). Tada je $X = \sum_{xy} I_{xy}$. Stoga je $E(X) = \sum_{xy} E(I_{xy})$. No, $E(I_{xy}) = P$ (xy prijelazni brid) $= 1/2$, jer je vjerojatnost da su dva idealna novčića različita jednaka $1/2$. Zato je $E(X) = \sum_{xy \in E} E(I_{xy}) = m/2$. Kako je očekivanje od X ovdje aritmetička sredina vrijednosti od X po svim podskupovima S, slijedi da postoji $S \subseteq V$ tako da je $X \geq m/2$ za taj S i očito prijelazni bridovi čine bipartitni graf. □

Na kraju ćemo vjerojatnosne metode uporabiti izvan teorije grafova. Prva je iz kombinatorike konačnih skupova, a druge dvije iz kombinatorne geometrije. Promotrimo skup $N = \{1, 2, \ldots, n\} = [n]$. Familiju podskupova $\mathcal{F}$ skupa N ćemo zvati **presječna familija** ako je $A \cap B \neq \emptyset$, za svako $A, B \in \mathcal{F}$. Ako je $\mathcal{F} \subseteq 2^{[n]}$ presječna familija, a $A \in \mathcal{F}$, onda komplement $\overline{A} \notin \mathcal{F}$. Stoga presječna familija $\mathcal{F}$ ima najviše polovicu od svih 2^n podskupova od $[n]$, pa je $|\mathcal{F}| \leq 2^{n-1}$. Presječna familija $\mathcal{F}_1 \subseteq 2^{[n]}$ čiji svaki član sadrži 1 ima očito $|\mathcal{F}_1| = 2^{n-1}$ članova. No, pitanje je kolika je presječna familija, ako su joj svi članovi iste veličine k? Takva se zove **presječna k-familija**. Ako je $n < 2k$, onda se svaka dva k-skupa sijeku, pa je stoga netrivijalni slučaj $n \geq 2k$. Ako je $\mathcal{F}_1$ presječna k-familija čiji svaki član sadrži čvrsti element, recimo n, onda ako dodamo n svakom $(k-1)$-podskupu od $[n-1]$ dobivamo $|\mathcal{F}_1| = \binom{n-1}{k-1}$.

TEOREM 29 (Erdös, Ko, Rado, 1961). *Neka je $n \geq 2k$, a $\mathcal{F}$ bilo koja presječna k-familija nekog n-članog skupa. Tada je $|\mathcal{F}| \leq \binom{n-1}{k-1}$.*

Dokaz. Neka je $\mathcal{F}$ takva familija skupa $\{0, 1, \ldots, n-1\}$. Prvo dokažimo ovu lemu.

LEMA 15. *Za $0 \leq s \leq n-1$, neka je $A_s = \{s, s+1, \ldots, s+k-1\}$, gdje je zbrajanje modulo n. Tada $\mathcal{F}$ sadrži najviše k od skupova A_s.*

Dokaz leme. Neka je $A_s \in \mathcal{F}$ čvrst. Svi drugi skupovi A_t koji sijeku A_s mogu se particionirati u $k-1$ parova $\{A_{s-i}, A_{s+k-i}\}$, $1 \leq i \leq k-1$, a članovi svakog takvog para su disjunktni. Kako $\mathcal{F}$ može sadržavati najviše jedan član svakog para, dobivamo tvrdnju.

Sada dokažimo teorem. Odaberimo slučajno, nezavisno i uniformno permutaciju π od $\{0, 1, \ldots, n-1\}$ i element $j \in \{0, 1, \ldots, n-1\}$, te neka je $A = \{\pi(j), \pi(j+1), \ldots, \pi(j+k-1)\}$ (tu je opet zbrajanje modulo n).

Iz leme očito slijedi da je vjerojatnost $P(A_j \in \mathcal{F}) \leq k/n$. Iz istih je razloga i $P(A \in \mathcal{F}) \leq k/n$. Međutim, A je uniformno izabran među svim k-podskupovima pa je

$$\frac{k}{n} \geq P(A \in \mathcal{F}) = \frac{|\mathcal{F}|}{\binom{n}{k}}.$$

Dakle,

$$|\mathcal{F}| \leq \frac{k}{n}\binom{n}{k} = \binom{n-1}{k-1}. \quad \text{(Ovo je dokaz G. Katone iz 1972.)}$$

□

Sada prvi geometrijski problem. Promotrimo konačni skup S točaka u prostoru $\mathbb{R}^d$ i kutove $\sphericalangle xyz$ koje određuju trojke $x, y, z \in S$. Geometrijski se može pokazati da ako su svi kutovi $\sphericalangle xyz \leq \pi/2$, onda je $|S| \leq 2^d$. No što je u slučaju da su svi kutovi šiljasti, tj. $\sphericalangle xyz < \pi/2$? Danzer i Grünbaum su konstruirali konfiguracije od $2d-1$ točaka u $\mathbb{R}^d$ sa samo šiljastim kutovima i dugo se smatralo da je to i najbolji rezultat, što se i potvrdilo za $d \leq 3$. No, u visokim dimenzijama to se pokazalo pogrešnim. Npr., u dimenziji $d = 35$ postoji skup od $76 > 2 \cdot 35 - 1$ točaka koje određuju samo šiljaste kutove. Pomalo je začuđujuće da se to dokazalo s vjerojatnosnim metodama.

TEOREM 30 (P. Erdös, Z. Füredi, 1983). *Za svako $d \geq 1$ postoji skup $S \subseteq \{0,1\}^d \subseteq \mathbb{R}^d$ vrhova jedinične d-kocke, veličine $|S| = \lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^d \rfloor$, koji određuju samo šiljaste kutove.*

Dokaz. Stavimo $n := \lfloor \frac{1}{2}\left(\frac{2}{\sqrt{3}}\right)^d \rfloor$ i odaberimo $2n$ vektora $x_1, x_2, \ldots, x_{2n} \in \{0,1\}^d$, birajući slučajno i nezavisno njihove koordinate kao 0 ili 1, svaku s vjerojatnošću $1/2$. Vektori x_i, x_j, x_k određuju pravi kut s vrhom x_j, ako i samo ako je skalarni produkt $(x_i - x_j) \cdot (x_k - x_j) = 0$. Pišemo li $x_i = (x_i^{(1)}), \ldots, x_i^{(d)})$ koordinatno, to je ekvivalentno s time da je

$$x_i^{(l)} - x_j^{(l)} = 0 \quad \text{ili} \quad x_k^{(l)} - x_j^{(l)} = 0,$$

za svaku koordinatu l. Takvu ćemo trojku (i,j,k) zvati *loša trojka*, a inače *dobra*. Vjerojatnost da je neka čvrsta trojka loša jednaka je $(3/4)^d$. Naime, trojka je dobra ako i samo ako postoji koordinata l za koju je

$$x_i^{(l)} = x_k^{(l)} = 0, \quad x_j^{(l)} = 1,$$
$$\text{ili } x_i^{(l)} = x_k^{(l)} = 1, \quad x_j^{(l)} = 0.$$

To nam daje šest loših od ukupno osam jednako mogućih trojki, a trojka je loša ako i samo ako jedna od loših mogućnosti (s vjerojatnošću $3/4$) nastupi za svaku od d koordinata.

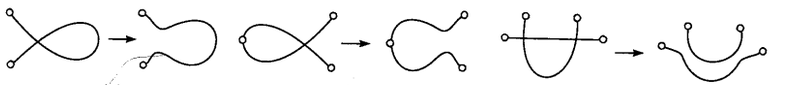
Ukupni broj trojki koji trebamo promatrati je jednak $3\binom{2n}{3}$, jer imamo $\binom{2n}{3}$ trojki vektora i za svaku po tri izbora za vrh kuta. Uočimo da događaji da su razne trojke loše nisu nezavisni. Zato ćemo uporabiti očekivanje (tj. prosječnost po svim izborima) i njezinu linearnost. Očekivani broj loših trojki je jednak $3\binom{2n}{3}\left(\frac{3}{4}\right)^d$. To znači (i to je glavna "kvaka") da postoji bar jedan izbor od $2n$ vektora, tako da je među njima najviše $3\binom{2n}{3}\left(\frac{3}{4}\right)^d$ loših trojki. No, zbog definicije od n imamo

$$3\binom{2n}{3}\left(\frac{3}{4}\right)^d < 3\frac{(2n)^3}{6}\left(\frac{3}{4}\right)^d = n(2n)^2\left(\frac{3}{4}\right)^d \leq n.$$

Ali, ako nema više od n loših trojki, onda možemo izbaciti n od $2n$ vektora x_i tako da u ostalih n vektora nema loših trojki, pa stoga oni određuju samo šiljaste kutove. □

Konačno problem iz kombinatorne geometrije. Sjetimo se da je **presječni broj** grafa G najmanji broj cr (G) presijecanja po dvaju bridova grafa među svim ravninskim realizacijama grafa G, pri čemu su vrhovi točke ravnine, a bridovi reprezentirani krivuljama u ravnini. Stoga je cr $(G) = 0$ ako i samo ako je G planaran.

U takvoj minimalnoj realizaciji jednostavnog grafa u ravnini pretpostavljamo da vrijede sljedeća pravila: (a) brid ne siječe samog sebe; (b) bridovi sa zajedničkim krajem se ne sijeku i (c) nikoja dva brida se ne sijeku dvaput. (Jasno je da izbjegavanjem sjecišta to uvijek možemo postići):



Neka je G realiziran u ravnini s cr (G) presijecanja. Definirajmo graf H ovako. Vrhovi od H su vrhovi od G i sve presječne točke od G, a bridovi od H su dijelovi bridova od G od presječne do presječne točke na svakom bridu:



Iz (a), (b), (c) odmah slijedi da je H jednostavni ravninski graf. Nadalje, ako je broj vrhova $v(G) = n$, a bridova $e(G) = m$, onda je $v(H) = n + \text{cr}\,(G)$, a $e(H) = m + 2\text{cr}\,(G)$, jer svi novi vrhovi imaju stupanj 4 u H. Kako je za planarni graf $e(H) \leq 3v(H) - 6$ (Propozicija 21 b)), slijedi da je

$$\text{cr}\,(G) \geq m - 3n + 6. \qquad (*)$$

Tako je npr. cr $(K_6) \geq 15 - 18 + 6 = 3$ (postoji realizacija od K_6 u ravnini s točno 3 presjecišta - nađite je). Ako m linearno ovisi o n, onda je $(*)$ dobra ocjena, no ako je m veći, onda vrijedi sljedeće.

TEOREM 31. *Neka je G jednostavni graf s n vrhova i m bridova, pri čemu je $m \geq 4n$. Tada je*

$$cr\,(G) \geq \frac{1}{64}\frac{m^3}{n^2}.$$

Dokaz. Neka je G realiziran u ravnini sa cr (G) presijecanja, a $p \in [0,1]$ (koji ćemo kasnije pogodno odabrati). Neka je G_p inducirani podgraf od G koji dobijemo tako da svaki vrh od G neovisno i slučajno odaberemo s vjerojatnošću p da bude vrh u G_p.

Neka su n_p, m_p i X_p slučajne varijable broja vrhova, bridova i presijecanja od G_p, redom. Iz $(*)$ slijedi da je cr $(G) - m + 3n \geq 0$ za svaki graf, pa je očekivanje

$$E(X_p - m_p + 3n_p) \geq 0. \qquad (**)$$

Očito je $E(n_p) = pn$, $E(m_p) = p^2 m$, jer je brid u G_p ako i samo ako su mu oba kraja u G_p. Konačno, $E(X_p) = p^4 \text{cr}\,(G)$, jer u G_p imamo presijecanje ako i samo ako dolazi od presijecanja dvaju bridova određena s 4 (različita) vrha.

Sada zbog linearnosti očekivanja imamo

$$0 \leq E(X_p) - E(m_p) + 3E(n_p) = p^4 \mathrm{cr}\ (G) - p^2 m + 3pn,$$

a odatle

$$\mathrm{cr}\ (G) \geq \frac{p^2 m - 3pn}{p^4}.$$

Stavimo li tu $p = 4n/m$ (≤ 1), tvrdnja slijedi. □

Tako se npr. $K_{6,12}$ ne može nacrtati u ravnini s manje od 18 presjecišta.

I sada kao zadnju primjenu to ćemo uporabiti za dokaz poznatog Szemerédi-Trotterovog teorema iz kombinatorne geometrije o tome da je maksimalni broj incidencije bilo kojeg **aranžmana** od n točaka i m pravaca u ravnini najviše jednak $c(m^{2/3}n^{2/3} + m + n)$, gdje je c konstanta. (Katkad se to naziva i **kompleksnost aranžmana** točaka i pravaca.) O aranžmanima i raznim kombinatorno-diskretnim i računarskim aspektima u geometriji vidi u [34*].

TEOREM 32 (E. Szemerédi, W. Trotter, 1983). *Neka je $\mathcal{T}$ bilo koji skup od n točaka, a $\mathcal{P}$ skup od m pravaca u ravnini. Tada je broj incidencija članova iz $\mathcal{T}$ i članova iz $\mathcal{P}$ (tj. broj parova (t,p), $t \in \mathcal{T}$, $p \in \mathcal{P}$, za koje je $t \in p$) najviše jednak $c(m^{2/3}n^{2/3} + m + n)$, gdje je $c > 0$ neka (apsolutna) konstanta.*

Dokaz. Označimo s $I = I(m,n)$ broj incidencija. Neka je $G = (V,E)$ graf čiji su vrhovi svi članovi iz $\mathcal{T}$, a dva su vrha susjedna ako i samo ako su to uzastopne točke iz $\mathcal{T}$ na nekom pravcu iz $\mathcal{P}$. Tada je $|V| = n$, a $|E| = I - m$. G je već realiziran u ravnini s bridovima koji su segmenti na pravcima iz $\mathcal{P}$. U toj realizaciji je svako presijecanje u G presječna točka članova iz $\mathcal{P}$. Stoga je $\mathrm{cr}\ (G) \leq \binom{m}{2} \leq m^2/2$. Iz prethodnog teorema slijedi da je ili $I - m = |E| < 4|V| = 4n$, tj. $I \leq m + 4n$, ili je

$$\frac{m^2}{2} \geq \mathrm{cr}\ (G) \geq \frac{(I-m)^3}{64n^2},$$

što povlači $I \leq (32)^{1/3} m^{2/3} n^{2/3} + m$. U oba je slučaja $I \leq 4(m^{2/3}n^{2/3} + m + n)$, čime je teorem dokazan. (Ovaj lijep i kratak dokaz dao je L. Székely, 1997.) □

Ako u ovom dokazu učinimo *mutatis mutandis*, dobivamo:

KOROLAR 24. *Maksimalni broj incidencija među n točaka i m jediničnih kružnica u ravnini je najviše $c(m^{2/3}n^{2/3} + m + n)$, za neku konstantu $c > 0$.*

KOROLAR 25. *Neka je $f(n)$ maksimalni broj koliko se puta jedinična udaljenost može pojaviti među bilo kojih n točaka u ravnini. Tada je*

$$f(n) \leq cn^{4/3},$$

gdje je $c > 0$ neka konstanta.

Dokaz. Primijenimo Korolar 24 za $m = n$ na bilo koji skup $\mathcal{T}$ od n točaka u ravnini i skup svih jediničnih kružnica sa središtima u $\mathcal{T}$. Svaki par točaka iz $\mathcal{T}$ na udaljenosti 1 računamo kao dvije incidencije među točkama i kružnicama. Odavde slijedi tvrdnja. (Inače, može se pokazati da je $f(n) > n^{1+c'/\log\log n}$, za neko $c' > 0$, i slutnja je da je ova međa asimptotski tijesna.) □

O vjerojatnosnim metodama i raznim primjenama čitatelj može naći u [3*].

§ 10. Protoci u transportnim mrežama

U teoriji, a naročito u primjenama, usmjereni težinski grafovi služe kao model za analizu protoka robe od proizvođača ("izvora") do potrošača ("ponora"); npr. to može biti protok nafte u naftovodu, prenošenje signala u telefoniji, prijenos (transport) artikala do trgovina itd. Težinu luka u takvom usmjerenom grafu možemo tumačiti kao maksimalni kapacitet količine nafte koji može proteći nekim dijelom naftovoda, ili kao maksimalna brzina prijenosa signala ili prijevoza artikala itd. Sada formalizirajmo te ideje.

Transportna mreža (ili kratko **mreža**, engl. *network*) $N = (V,A)$ povezani je digraf bez petlji za koji vrijedi sljedeće:

1) postoji jedinstveni vrh i s instupnjem $d^-(i) = 0$, koji se zove **izvor**;
2) postoji jedinstveni vrh p s outstupnjem $d^+(p) = 0$, koji se zove **ponor** ;
3) svakom je luku $a = (u,v) \in A$ pridružen realni broj $c(a) = c(u,v) \geq 0$, koji se zove **kapacitet** (ili **nosivost**) od a. Ako ne postoji luk (u,v), stavljamo $c(u,v) := 0$.

Protok (engl. *flow*) mreže N je funkcija $f : A \to \mathbb{R}^+$ koja svakom luku $a = (u,v)$ pridružuje broj $f(a) = f(u,v)$ (i tu stavljamo $f(u,v) = 0$ ako (u,v) nije luk) tako da vrijedi:

$$f(u,v) \leq c(u,v), \quad \forall u,v \in V, \quad \textbf{ograničenje kapacitetom}, \tag{1}$$

$$\sum_{v \in V} f(u,v) = \sum_{v \in V} f(v,u), \quad \forall u \neq i,p, \quad \textbf{uvjet očuvanja}. \tag{2}$$

Vrijednost $f(a)$ možemo tumačiti kao količinu ili brzinu prijevoza na luku a protoka f. Uvjet (1) znači da količina (ili brzina) robe duž $a = (u,v)$ ne može prijeći kapacitet od a, a uvjet (2), koji se katkad zove i **Kirchhoffov zakon**, znači da je količina robe pristigla u vrh u jednaka količini robe koja izlazi iz u, osim za izvor i ponor. Uočimo da na mreži N uvijek postoji protok, npr. trivijalni protok $f(a) = 0$, $\forall a \in A$.

Vrijednost protoka f na mreži N je $\mathrm{val}\ (f) := \sum_{v \in V} f(i,v)$. Nadalje, kažemo da je protok f^* **maksimalan protok** ako ne postoji protok f na mreži N tako da je $\mathrm{val}\ (f) > \mathrm{val}\ (f^*)$.

Osnovni je cilj ove teorije karakterizirati i algoritamski pronaći maksimalni protok. Prvo, za $S,T \subseteq V$, skup (S,T) je skup svih lukova s početkom u S, a krajem u T. **Vršni rez** (kratko **rez**, engl. *cut*) na mreži N je skup oblika $R = (S,\overline{S})$, $\overline{S} = V \setminus S$. Rez R **separira** (**razdvaja**) izvor i od ponora p, ako je $i \in S$, $p \in \overline{S}$. Kaže

se tada da je R *i-p* rez. **Kapacitet reza** R je $c(R) = c(S, \overline{S}) := \sum_{(u,v)\in R} c(u,v)$. Za protok f i takav rez definiramo $f(S, \overline{S}) = f^+(S)$ kao sumu vrijednosti $f(u,v)$ protoka svih lukova iz $(S, \overline{S})$, a $f^-(S) := f(\overline{S}, S)$.

PROPOZICIJA 32. *Za svaki protok f i svaki i-p rez $(S, \overline{S})$ transportne mreže N vrijedi val $(f) = f(S, \overline{S}) - f(\overline{S}, S)$.*

Dokaz. Iz definicije protoka i vrijednosti protoka slijedi da je za $u \in S$:

$$\sum_{v\in V} f(u,v) - \sum_{v\in V} f(v,u) = \begin{cases} \text{val } (f), & \text{za } u = i \\ 0, & \text{za } u \neq i. \end{cases}$$

Sumiramo li te jednakosti po svim $u \in S$, dobivamo

$$\sum_{u\in S}\sum_{v\in V} f(u,v) - \sum_{u\in S}\sum_{v\in V} f(v,u) = \text{val } (f).$$

Na lijevoj se strani sumandi $f(u,v)$ i $-f(v,u)$ za $u \in S$, $v \in S$ pojavljuju točno jedanput, pa se međusobno poništavaju. Nakon toga preostaje

$$\sum_{u\in S}\sum_{v\in \overline{S}} f(u,v) - \sum_{u\in S}\sum_{v\in \overline{S}} f(v,u) = \text{val } (f),$$

pa je $f(S, \overline{S}) - f(\overline{S}, S) = \text{val } (f)$, kako smo i tvrdili. □

KOROLAR 26. *Za svaki protok f i svaki i-p rez $R = (S, \overline{S})$ na mreži N vrijedi val $(f) \leq c(S, \overline{S})$, s jednakošću ako i samo ako je $f(S, \overline{S}) = c(S, \overline{S})$ i $f(\overline{S}, S) = 0$.*

Dokaz. Iz $f(u,v) \geq 0$, $\forall u, v$ i Propozicije 32 slijedi val $(f) = f(S, \overline{S}) - f(\overline{S}, S) \leq f(S, \overline{S}) \leq c(S, \overline{S})$. Druga je tvrdnja također jasna. □

KOROLAR 27. *Vrijednost protoka koji izlazi iz izvora mreže jednak je vrijednosti protoka koji ulazi u ponor.*

Dokaz. Uzmimo $S = \{i\}$ i $S' = V \setminus \{p\}$. Tada iz Propozicije 32 slijedi $f(S, \overline{S}) - f(\overline{S}, S) = \text{val } (f) = f(S', \overline{S'}) - f(\overline{S'}, S')$. Kako je $d^-(i) = 0$, slijedi $f(\overline{S}, S) = 0$, a zbog $d^+(p) = 0$ je $f(\overline{S'}, S') = 0$. □

Kažemo da je *i-p* rez R **minimalan** ako ne postoji *i-p* rez R' za koji je $c(R') < c(R)$.

KOROLAR 28. *Neka je f protok na mreži N, a R i-p rez za koji je val $(f) = c(R)$. Tada je f maksimalni protok, a R minimalni rez na N.*

Dokaz. Neka je f^* maksimalni protok, a R^* minimalni *i-p* rez na N. Iz Korolara 26 slijedi val $(f) \leq$ val $(f^*) \leq c(R^*) \leq c(R)$. No prema pretpostavci je val $(f) = c(R)$, pa svuda vrijedi jednakost i tvrdnja slijedi. □

Sada prelazimo na dokaz osnovnog teorema da je vrijednost maksimalnog protoka ustvari jednaka kapacitetu minimalnog reza.

Neka je f protok na mreži N, a $P = u_0 a_1 u_1 a_2 \ldots u_i a_{i+1} \ldots a_k u_k$, (u_0, u_k)-put u pripadnom (neorijentiranom) grafu mreže. Brid $a_i = u_{i-1}u_i$ puta P je **izravan** ili **direktan luk puta** P, ako je $a_i = (u_{i-1}, u_i) \in A(N)$, a inače **obrnuti luk** puta P. Za put P definiramo $\Delta(P) := \min_{a\in A(P)} \Delta(a)$, gdje je

$$\Delta(a) = \begin{cases} c(a) - f(a), & \text{ako je } a \text{ direktni luk,} \\ f(a), & \text{ako je } a \text{ obrnuti luk .} \end{cases}$$

Stoga je $\Delta(P)$ najveći iznos za koji se protok f može povećati duž P, tako da još uvijek vrijedi (1). Kažemo da je put P f-**zasićen** ako je $\Delta(P) = 0$, a f-**nezasićen** ako je $\Delta(P) > 0$, tj. onaj čiji kapacite nije iskorišten do kraja. f-**rastući** put je f-nezasićen *i-p* put. Dakle, *i-p* put P je f-rastući ako i samo ako je $\Delta(P) > 0$. Egzistencija f-rastućeg puta P u mreži N važna je zato što tada znamo da f nije maksimalni protok. Naime, vrijedi

LEMA 16. *Ako postoji f-rastući put u mreži N, onda f nije maksimalni protok.*

Dokaz. Uzmimo da je P neki f-rastući put u N. Definirajmo tada novi protok f' formulom

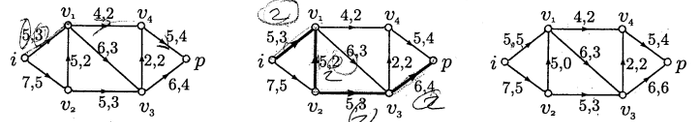
$$f'(a) = \begin{cases} f(a) + \Delta(P), & \text{ako je } a \text{ direktni luk od P,} \\ f(a) - \Delta(P), & \text{ako je } a \text{ obrnuti luk od } P, \\ f(a), & \text{inače.} \end{cases}$$

Tada se odmah vidi da je f' također protok i da je val (f') = val $(f) + \Delta(P)$, pa zbog $\Delta(P) > 0$ slijedi val (f') > val (f). Stoga f nije maksimalni protok. □

Protok f' iz Leme 16 zove se **izmijenjeni protok od f s obzirom na put P.**

Primjer 55. Na donjoj slici a) zadana je mreža N i na svakom luku a par brojeva $(c(a), f(a))$. Na slici b) je (podebljan) put $P = iv_1v_2v_3p$. Odredite izmijenjeni protok f' od f s obzirom na P i njihove vrijednosti.

Rješenje. Na putu P su iv_1, v_2v_3, v_3p direktni lukovi, a v_1v_2 obrnuti luk.



Mali račun i slika b) odmah daje da je $\Delta(P) = 2 > 0$, pa je P f-rastući put. Izmijenjeni protok f' od f s obzirom na P je na slici c). Uočimo da smo povećali sve direktne lukove iz P za $\Delta(P)$, a sve obrnute lukove iz P smanjili za $\Delta(P)$, dok su vrijednosti od f' na ostalim lukovima jednake vrijednostima od f. Vrijednosti protoka su val $(f) = 8$, val $(f') = 10$. □

PROPOZICIJA 33. *Protok f mreže N je maksimalan ako i samo ako N ne sadrži f-rastući put.*

Dokaz. Ako je f maksimalan protok, onda zbog Leme 16 ne postoji f-rastući put. Pretpostavimo sada da N ne sadrži f-rastući put. Neka je S skup svih vrhova iz N do kojih se iz izvora i može doći f-nezasićenim putom. Tada je $i \in S$, a ponor $p \in \overline{S}$ jer u N nema f-rastućih putova. Stoga je $R = (S, \overline{S})$ rez u N. Pokažimo da je val $(f) = c(S, \overline{S})$. Time će zbog Korolara 28 slijediti da je f maksimalni protok, a $(S, \overline{S})$ minimalni rez.

Neka je $a = uv \in (S, \overline{S})$. Kako je $u \in S$, slijedi da postoji f-nezasićeni (i, u)-put P. Luk a mora biti f-zasićen, jer bi inače njime mogli produljiti P i dobiti f nezasićen (i, v)-put, što je nemoguće zbog $v \in \overline{S}$. Analogno se vidi da $a \in (\overline{S}, S)$ povlači $f(a) = 0$. Dakle, $f(S, \overline{S}) = c(S, \overline{S})$ i $f(\overline{S}, S) = 0$. Stoga iz Propozicije 32 slijedi

$$\text{val}\,(f) = f(S, \overline{S}) - f(\overline{S}, S) = c(S, \overline{S}).$$

□

Time smo dokazali i osnovni teorem:

TEOREM 33 ("max-flow min-cut", L. Ford, D. Fulkerson, 1956.). *U transportnoj je mreži vrijednost maksimalnog protoka jednaka kapacitetu minimalnog reza.*

Ovaj je teorem također od velike važnosti u teoriji grafova i mnogi se drugi teoremi iz njega mogu izvesti pogodnim izborom mreže, kapaciteta i protoka na njoj. Izvest ćemo samo Mengerov teorem. Prvo dokažimo sljedeće.

PROPOZICIJA 34. *Neka je N transportna mreža s izvorom i, ponorom p, a svaki luk kapaciteta 1. Tada vrijedi:*

a) Vrijednost maksimalnog protoka na N jednaka je maksimalnom broju m lučno-disjunktnih usmjerenih (i, p)-putova u N;

b) Kapacitet minimalnog reza u N jednak je minimalnom broju r lukova čije izbacivanje prekida sve usmjerene (i, p)-putove.

Dokaz. a) Neka je f^* maksimalni protok na N, a N^* mreža dobivena iz N izbacivanjem f^*-nula lukova. Kako je kapacitet svakog luka iz N jednak 1, slijedi $f^*(a) = 1$, $\forall a \in A(N^*)$. Stoga je $d^+_{N^*}(i) - d^-_{N^*}(i) = \text{val}\,(f^*) = d^+_{N^*}(p) - d^-_{N^*}(p)$ i $d^+_{N^*}(v) = d^-_{N^*}(v)$, $\forall v \in V(N) \setminus \{i, p\}$. Tada iz Propozicije 12 b) lako slijedi da postoji val (f^*) lučno-disjunktnih (i, p)-diputova u N^*, pa stoga i u N. Zato je val $(f^*) \leq m$. Ako su $P_1, P_2, \ldots, P_m$ lučno disjunktni (i, p)-diputovi u N, definirajmo $f : A(N) \to \mathbb{R}$ s $f(a) = 1$, ako je a luk nekog P_i, te $f(a) = 0$, inače. Lako se provjeri da je f protok i val $(f) = m$. Kako je f^* maksimalni protok, slijedi da je val $(f^*) \geq m$. Time je a) dokazano.

b) Neka je R^* minimalni (i, p)-rez na N. Nakon izbacivanja R^*, u $N - R^*$ nema (i, p)-diputa, pa je $c(R^*) = |R^*| \geq r$. S druge strane, neka je $R \subseteq A(N)$ skup od r lukova čije izbacivanje prekida sve (i, p)-diputove u N, a $S \subseteq V(N)$ skup svih vrhova koji se mogu doseći nekim diputom iz izvora i u digrafu $N - R$. Kako je $i \in S$, $p \in \overline{S}$, slijedi da je $\widetilde{R} := (S, \overline{S})$ jedan i-p rez u N. Iz definicije od S slijedi da $N - R$ ne sadrži luk iz $\widetilde{R}$, pa je $\widetilde{R} \subseteq R$. Kako je R^* minimalni rez, to je $c(R^*) \leq c(R^*) \leq |R| = r$, čime je i b) dokazano. □

KOROLAR 29 (Mengerov teorem). *Neka su i, p dva vrha digrafa D. Tada je maksimalni broj lučno-disjunktnih (i, p)-diputova u D jednak minimalnom broju lukova čije izbacivanje prekida sve (i, p)-diputove u D.*

Dokaz. Neka je N mreža dobivena iz D s izvorom i, ponorom p, a kapacitetom svakog luka iz D jednakim 1. Tada tvrdnja odmah slijedi iz Propozicije 34 i max-flow min-cut Teorema 33. □

Jednostavnom dosjetkom odavde slijedi neusmjerena inačica.

KOROLAR 30 (Mengerov teorem). *Neka su i, p dva vrha grafa G. Maksimalni broj bridno-disjunktnih (i, p)-putova u G jednak je minimalnom broju bridova bridnog reza koji separira vrh i od vrha p.*

Dokaz. Grafu G pridružimo asocirani digraf $D(G)$ (tj. svaki brid iz G zamijenimo dvama suprotno orijentiranim lukovima.) Tada su putovi u G u bijekciji s diputovima u $D(G)$. Nadalje, za svaka dva vrha $i, p \in V(G)$, minimalni broj bridova iz G čije izbacivanje prekida sve (i, p)-putove u G, jednak je minimalnom broju lukova u $D(G)$ čije izbacivanje prekida (i, p)-diputove u $D(G)$. Drugim riječima, G je k-bridno povezan ako i samo ako je $D(G)$ k-lučno povezan. Stoga tvrdnja slijedi iz Korolara 29. □

Slično se dokazuje i vršni analogon:

KOROLAR 31 (Mengerov teorem). *Graf G s više od $k+1$ vrhova je k-povezan ako i samo ako se svaka dva različita vrha mogu povezati s barem k unutarnje disjunktnih putova.*

Dokaz prepuštamo čitatelju.

I mnogi drugi teoremi tipa max-min (ili "minimax") posljedica su (zapravo ekvivalentni njima) max-flow min-cut teorema, npr. König-Egervaryjev, Dilworthov, Hallov i drugi.

Ford-Fulkersonov algoritam označavanja

Sada ćemo konstruirati algoritam za nalaženje maksimalnog protoka transportne mreže. Taj se algoritam osniva na prethodnoj teoriji. Algoritam se sastoji od dvije etape.

U prvoj se etapi metodom označavanja, polazeći od protoka f, provjeri postoji li f-rastući put. Ako takvog nema, onda je, prema Propoziciji 33, protok f maksimalan. U protivnome, prelazimo na drugu etapu, u kojoj se, koristeći se označavanjem iz prve etape, konstruira f-rastući put P i izmijenjeni protok f' s obzirom na put P. Tada je val$(f') >$ val(f) pa se vratimo na prvu etapu. U prvoj se etapi svakom vrhu v pripiše oznaka (l_v, L_v). Prvi simbol l_v ukazuje na vrh iz kojeg je v dobio oznaku. Na to također ukazuje i smjer označavanja: direktno ili obrnuto. Poslije će biti jasno da ako vrh v dobiva oznaku, znači da postoji f-nezasićen i-p put P i da je za njega $\Delta(P) = L_v$.

Prva etapa počinje označavanjem izvora $(-, \infty)$. Tu je vrijednost l_i nebitna. Ostali se vrhovi označavaju poštujući sljedeća dva pravila.

Pretpostavimo da je vrh u već označen, a vrh v nije. Neka su oni incidentni s lukom a.

Direktno označavanje. Ako je $a = (u, v)$, onda je direktno označavanje v iz u duž luka a moguće ako je $c(a) > f(a)$. U tom slučaju v dobiva oznaku (u^+, L_v), gdje je $L_v = \min\{L_u, c(a) - f(a)\}$.

Obrnuto označavanje. Ako je $a = (v, u)$, onda je obrnuto označavanje v iz u duž a moguće ako je $f(a) > 0$. U tom slučaju v dobiva oznaku (u^-, L_v), gdje je $L_v = \min\{L_u, f(a)\}$.

U prvoj etapi vrhovi su označeni samo jedanput. Ta etapa završava kada 1) vrh p dobiva oznaku ili 2) vrh p nije označen i nijedan se vrh više ne može označiti. Ako je p označen u prvoj etapi, onda iz pravila označavanja slijedi da postoji f-rastući put P i $\Delta(P) = L_p$. U drugoj se etapi put P prolazi u obratnom smjeru (natraške), s pomoću simbola l_v i konstruira se izmijenjeni protok f' s obzirom na put P. Nakon toga se opet primijeni prva etapa na protok f'. Ako je prva etapa završila a da se nije označio ponor p, onda to znači da ne postoji f-rastući put pa je trenutni protok maksimalan.

Ford-Fulkersonov algoritam za nalaženje maksimalnog protoka mreže

Korak 1. Odabrati neki protok f na mreži N; npr. $f(a) = 0$, za svako $a \in A(N)$.

Korak 2. (Počinje 1. etapa.) Označiti i s $(-, \infty)$.

Korak 3. Ako postoji neoznačen vrh koji možemo označiti direktnim ili obrnutim označavanjem, onda odaberimo takav vrh v, označimo ga i prijeđimo na korak 4. U protivnome, stop (dobiven je maksimalni protok).

Korak 4. Ako je $v = p$, prijeći na korak 5. (Time je 1. etapa završena.) U protivnome, prijeći na korak 3.

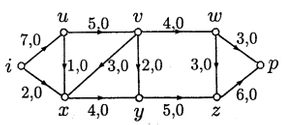
Korak 5. (Počinje 2. etapa.) Neka je (l_v, L_v) oznaka vrha v.

Ako je $l_v = u^+$, zamijeniti $f(u, v)$ sa $f(u, v) + L_p$

Ako je $l_v = u^-$, zamijeniti $f(v, u)$ sa $f(u, v) - L_p$.

Korak 6. Ako je $u = i$, izbrisati sve oznake (završena 2. etapa) i prijeći na korak 2., a ako je $u \neq i$, onda v postaje u i prijeći na korak 5.

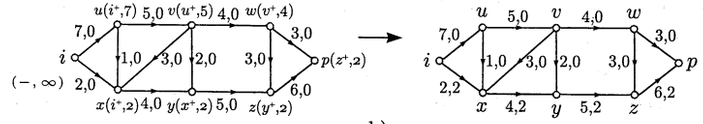
Primjer 56. Ford-Fulkersonovim algoritmom označavanja nađite maksimalni protok mreže N na slici a). (Svaki luk a nosi oznaku $c(a), f(a)$; na početku je $f(a) = 0$, $\forall a \in A(N)$.)



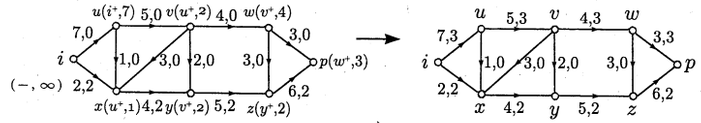
a)

Rješenje. Na slici b) je prva primjena algoritma. Izabran je ponor p za označavanje. Isto tako, odabrali smo za njegovu oznaku $(z^+, 2)$, umjesto $(w^+, 3)$. (To pokazuje da uvijek imamo više izbora, a mi odaberemo bilo koji mogući, što onda vodi i na možda različite

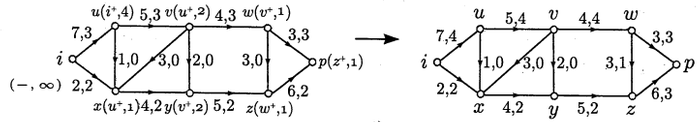
maksimalne protoke.) Sada gledamo unatrag od p do y do x do i te uvećamo protok na svakom luku na tom putu P za $\Delta(P) = L_p = 2$, čime dobivamo novi protok na desnoj slici b).



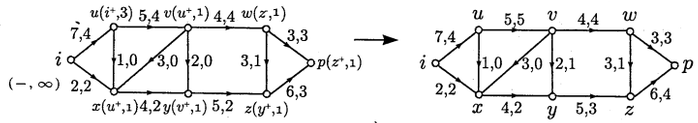
b)



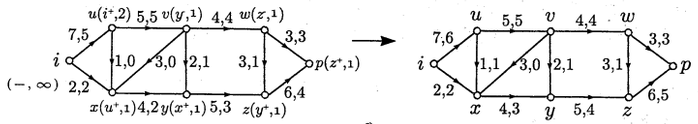
c)



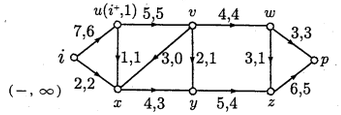
d)



e)



f)



g)

Na slikama c), d), e), f) daljnje su primjene algoritma. Na slici c) gledamo unatraške put $P = iuvwp$, sa $\Delta(P) = 3$, na slici d) $P = iuvwzp$, $\Delta(P) = 1$, na e) $P = iuvyzp$, $\Delta(P) = 1$ te na f) $P = iuxyzp$, $\Delta(P) = 1$. Posljednja primjena algoritma daje transportnu mrežu na slici g). Tu se vrh p ne može više označiti. Stavimo li $S = \{i, u\}$, $\overline{S} = \{x, v, y, w, z, p\}$ imamo

$$c(S, \overline{S}) = c(i, x) + c(u, x) + c(u, v) = 2 + 1 + 5 = 8 = f(z, p) + f(w, p),$$

što je protok koji ulazi u ponor. Tako smo dobili maksimalni protok. □

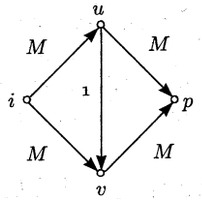
Treba napomenuti da se problem određivanja maksimalnog protoka u transportnoj mreži N može i malo poopćiti kada umjesto jednog izvora i jednog ponora imamo skup izvora I i skup ponora P, tako da se taj problem reducira na prethodni

sljedećim postupkom. Dodamo takvoj mreži N dva nova ekstra vrha i', p' i konstruiramo mrežu N' ovako: spojimo i' sa svakim vrhom iz I jednim lukom s početkom i' kapaciteta ∞, a svaki vrh iz P lukom kapaciteta ∞ s p' (s krajem u p'). Sada i', p' postaju jedinstveni izvor i ponor od N'. Ako je f protok u N tako da iz svakog izvora iz I izlazi, a u svaki ponor iz P ulazi nenegativan protok, onda definiramo funkciju f' formulom

$$f'(a) = \begin{cases} f(a), & \text{ako je } a \in A(N) \\ f^+(u) - f^-(u), & \text{ako je } a = (i', u),\ u \in I \\ f^-(v) - f^+(v), & \text{ako je } a = (v, p'),\ v \in P. \end{cases}$$

Lako se vidi da je protok f' na N' i $\mathrm{val}(f') = \mathrm{val}(f)$. Obratno, restrikcija protoka s mreže N' na mrežu N daje protok na N s istom vrijednošću.

Iako Ford-Fulkersonov algoritam označavanja u prosjeku dosta dobro funkcionira, ipak on teorijski nije efikasan. Naime, pogledajmo mrežu na slici



pri čemu je M velik cijeli broj. Algoritam počinje s 0-protokom i onda označavanje naizmjence rabi putove $P = iuvp$ i $Q = ivup$ kao rastuće putove. U svakom se koraku vrijednost protoka poveća točno za 1, a maksimalni protok vrijednosti $2M$ dostiže se nakon još $2M$ koraka. M može biti po volji velik, pa je i vrijeme izvršavanja algoritma funkcija od M.

No, malom modifikacijom tog algoritma, J. Edmonds i R. Karp su 1972. našli jedan efikasan algoritam označavanja transportne mreže složenosti $O(n^2m)$, a kasnije i još bolji algoritam složenosti $O(nm \log n)$. Više o tome čitatelj može naći u raznim knjigama o kombinatornoj optimizaciji, npr. [173], [232], [1*], [7*] itd.

VII. Odabrane teme kombinatorne i diskretne matematike

U prethodnim smo poglavljima uglavnom proučavali dvije "klasične" teme kombinatorne i diskretne matematike, a to su enumerativna kombinatorika i teorija grafova. U ovom ćemo završnom poglavlju u vrlo grubim crtama opisati neke pojmove, ideje i tehnike koje smo na pojedinim mjestima već i dotaknuli, a koje su zbog svoje važnosti i primjenjivosti u međuvremenu izrasle u samostalne discipline.

Odabrali smo ukratko prikazati četiri više–manje neovisne teme. To su blok dizajni, matroidi, Pólya-Redfieldova teorija i simetrične funkcije.

§ 1. Blok dizajni i konačne projektivne ravnine

U proučavanju raznih kombinatornih konfiguracija ili dizajna s izvjesnim prirodnim zahtjevima o pravilnostima na konačne skupove, malo po malo nastao je pojam blok dizajna, a njihov poseban slučaj su konačne projektivne ravnine.

Povijesno je tu važan primjer **Kirkmanov**[1] **problem 15 učenica**, a glasi ovako. Učitelj svakog dana šalje u šetnju svojih 15 učenica. One šeću u 5 grupa, u svakoj po 3. Može li se napraviti raspored šetnji za tjedan dana tako da svaka učenica u tih 7 dana bude točno jedanput u grupi sa svakom od preostalih učenica? (Općenitije, učitelj ima $6n+3$ učenica, a one šeću $3n+1$ dana za redom?) Za rješavanje ovog i niza drugih problema iskristalizirao se vrlo važan pojam **blok dizajna**[2], tj. uređenog para $(V, \mathcal{B})$, gdje je V konačni skup ("točaka"), a $\mathcal{B}$ familija ("blokovi") podskupova od V. Takva općenita struktura se, kao što znamo, naziva još i **hipergraf**, pri čemu se elementi iz V zovu **vrhovi**, a elementi $B \in \mathcal{B}$ (tj. blokovi) zovu se **hiperbridovi**. Ako je $|B| = k$, $\forall B \in \mathcal{B}$, onda se govori o k-**uniformnom hipergrafu**. Ako je $k = 2$, radi se o grafovima. No, među blok dizajnima posebno značenje ima sljedeći pojam. **Uravnoteženi nepotpuni blok dizajni** (engl. *balanced incomplete block design*, ili kraće $BIBD$) koji ćemo kratko zvati **blok dizajn**, sastoji se od skupa V od v elemenata (**vrhova** ili **točaka**) i familije $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$ podskupova (**blokova**) od V tako da vrijedi:

(1) $|B_i| = k$, $\forall i$, gdje je $k < v$ čvrst broj;

(2) Svaki vrh $x \in V$ nalazi se u točno $r(\leq b)$ blokova B_i.

[1] Rev. Thomas P. Kirkman (1806–1895), engleski matematičar, inače župnik

[2] Katkad se govori o **blok-nacrtima** ili **blok-shemama**

(3) Svakih t različitih vrhova iz V nalazi se zajedno u točno $\lambda(\leq b)$ blokova B_i;

Takav se blok dizajn zove t-(v,b,r,k,λ)-**dizajn**. Broj $n := r - \lambda$ se zove **red dizajna**. Parametri v, b, r, k, λ i t nisu posve neovisni i osnovna je zadaća teorije dizajna utvrditi postoji li za dane parametre dizajn sa zadanim parametrima (i ako ih postoji više, pokušati ih klasificirati).

Primjer 1. a) Neka je V konačni skup, a $k \in \mathbb{N}$ zadan čvrst broj. Neka je $\mathcal{B} = \binom{V}{k}$ familija svih k-podskupova od V. Tada je $(V, \mathcal{B})$ tzv. **trivijalni blok dizajn**. Lako se vidi da je za dane v, k i $t \in [k]$ ovdje $\lambda = \binom{v-t}{k-t}$, $r = \lambda(v-1)/(k-1)$, $b = vr/k$ i $b \geq v$.

b) Neka je $|V| = v$, a $k \in \mathbb{N}$ zadan broj koji dijeli v. Neka je $\mathcal{B} = \{B_1, B_2, \ldots, B_{v/k}\}$ particija od V u k-člane blokove. Tada je $(V, \mathcal{B})$ blok dizajn tipa 1-$(v, v/k, 1, k, 1)$.

Nije teško pokazati da svojstvo (2), tj. činjenica da svakim vrhom prolazi konstantni broj r blokova, slijedi iz svojstva (1) i (3). Prebrojavanjem parova incidencije na dva načina tada lako dobivamo da je $vr = bk$. U sljedećem ćemo teoremu, međutim, dokazati i jače tvrdnje.

Osnovni nužni uvjet za postojanje blok dizajna je sljedeći:

TEOREM 1. *Neka je $(V, \mathcal{B})$ blok dizajn tipa t-(v,b,r,k,λ). Tada vrijedi*

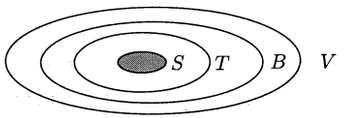
(i) **uvjet cjelobrojnosti***: Sljedeći brojevi su cijeli*

$$\lambda\frac{v(v-1)\ldots(v-t+1)}{k(k-1)\ldots(k-t+1)},\ \lambda\frac{(v-1)\ldots(v-t+1)}{(k-1)\ldots(k-t+1)},\ldots,\ \lambda\frac{v-t+1}{k-t+1}.$$

(ii) $b = \lambda\dfrac{v(v-1)\ldots(v-t+1)}{k(k-1)\ldots(k-t+1)}$, $r = \lambda\dfrac{(v-1)\ldots(v-t+1)}{(k-1)\ldots(k-t+1)}$ *i stoga* $b = \dfrac{vr}{k}$. *Prema tome, budući da su b i r potpuno određeni s v, k, λ i t, govorimo o t-(v,k,λ)-**dizajnu**.*

(iii) Za $t = 2$ vrijedi **Fischerova nejednakost** $b \geq v$.

Dokaz. (i) Neka je $(V, \mathcal{B})$ blok dizajn tipa t-(v,b,r,k,λ). Neka je s čvrst cijeli broj, $0 \leq s \leq t$, a $S \subseteq V$ čvrst skup od s elemenata. Na dva ćemo načina prebrojiti sve parove (T, B), za koje je $S \subseteq T \in \binom{V}{t}$, a $T \subseteq B \in \mathcal{B}$. Označimo s N broj takvih parova:



Skup T se može odabrati na $\binom{v-s}{t-s}$ načina, a svaki T je podskup od točno λ blokova $B \in \mathcal{B}$. Stoga je $N = \lambda\binom{v-s}{t-s}$.

S druge strane, neka je M broj blokova koji sadrže S. Svaki blok B koji sadrži S sadrži $\binom{k-s}{t-s}$ t-članih skupova T za koje je $S \subseteq T$, pa je $N = M\binom{k-s}{t-s}$. Stoga dobivamo

$$M = \lambda\frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}} = \lambda\frac{(v-s)\ldots(v-t+1)}{(k-s)\ldots(k-t+1)},$$

pa su razlomci iz (i) zaista cijeli brojevi.

(ii) Ako je $s = 0$ u dokazu tvrdnje (i), dobivamo točno broj b svih blokova, a ako je $s = 1$ dobivamo broj svih r blokova koji sadrže svaki element $x \in V$ (tzv. "stupanj od x").

(iii) Za 2-(v,k,λ)-dizajn $(V, \mathcal{B})$ s $V = \{x_1, x_2, \ldots, x_v\}$ i $\mathcal{B} = \{B_1, B_2, \ldots, B_b\}$ definirajmo $(v \times b)$-**matricu incidencije** $A = [a_{ij}]$ (slično kao za grafove) s $a_{ij} = 1$, ako je $x_i \in B_j$, $a_{ij} = 0$, inače. Neka je $M = AA^T = [m_{ij}]$. To je $(v \times v)$-matrica, čiji je (i,j)-ti član m_{ij} jednak $m_{ij} = \sum_{k=1}^{b} a_{ik}a_{jk}$. Stoga je m_{ij} jednak broju blokova B_k koji sadrže oba vrha x_i, x_j, pa iz definicije blok dizajna i tvrdnje (ii) za $t = 2$ dobivamo da je

$$m_{ij} = \begin{cases} \lambda & , \text{ za } i \neq j, \\ r = \lambda\frac{v-1}{k-1} & , \text{ za } i = j. \end{cases}$$

Prema tome, matrica M ima na glavnoj dijagonali brojeve r, a izvan glavne dijagonale brojeve λ. Elementarnim operacijama na recima od M lako dobivamo (učinite to sami) da je $\det M = (r+(v-1)\lambda)(r-\lambda)^{v-1}$. Jasno da je $r+(v-1)\lambda \neq 0$, a zbog $v > k$ slijedi $r > \lambda$. Stoga je $\det M \neq 0$. Zato M ima (puni) rang v. Kad bi bilo $b < v$, onda bi imali $rang(A), rang(A^T) < v$, pa bi zbog poznate nejednakosti $rang(AB) \leq \min\{rang(A), rang(B)\}$ slijedilo da je $rang(M) < v$. Zato je $b \geq v$. (Na drugi način: M je pozitivno definitna, tj. $x^T Mx > 0$, $\forall x \in \mathbb{R}^v \setminus \{0\}$, a takva uvijek ima puni rang, a $M = (r-\lambda)I + \lambda J$.) □

Uočite da je iz dokaza Teorema 1 jasno da je svaki t-(v,k,λ)-dizajn ujedno i s-(v,k,λ_s)-dizajn, za $s < t$ i

$$\lambda_s = \lambda\frac{\binom{v-s}{t-s}}{\binom{k-s}{t-s}}.$$

Primjer 2. Ispitajte postoji li dizajn tipa
a) 2-$(16,6,1)$; b) 2-$(21,6,1)$; c) 2-$(25,10,3)$.

Rješenje. a) Tu je $t = 2$, $v = 16$, $k = 6$, $\lambda = 1$, pa zbog Teorema 1 (ii) imamo da je $b = \lambda v(v-1)/k(k-1) = 16 \cdot 15/6 \cdot 5 = 8 < 16 = v$, što je u suprotnosti s Fischerovom nejednakosti, pa taj dizajn ne postoji (iako je uvjet cjelobrojnosti $r = 15/5 = 3$ zadovoljen). Iz sličnih razloga ne postoje dizajni iz b) i c). Dovršite to sami. □

Najzanimljiviji je, dakle, slučaj $t = 2$, i mi ćemo samo takve i promatrati u daljem i kratko reći da se radi o (v,k,λ)-dizajnu, i ustvari, skraćeni naziv BIBD se u literaturi uglavnom odnosi na 2-(v,k,λ)-dizajne (tj. (v,k,λ)-dizajne). Blok dizajni se rabe u matematičkoj statistici u kreiranju, planiranju i dizajniranju pokusa (eksperimenta), a rabe se i u poljoprivrednim eksperimentima. Odatle su uglavnom i došli nazivi i oznake. Evo jednog tipičnog "konkretnog" eksperimentiranja.

Primjer 3 (Degustacija vina). Od v vrsta vina degustacijom treba izabrati najbolje vino. Vino isprobava b degustatora. Iz razumljivih razloga ne može se od svakog degustatora zahtijevati da proba sva vina. Stoga će svaki degustator probati isti broj $k(< v)$ vina i to tako da svako vino bude isprobano isti broj r puta, a svaki par vina uspoređeno isti broj λ puta, tj. da ih proba isti broj λ degustatora.

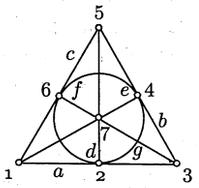
Ovdje se zato radi o shemi rasporeda degustacija (eksperimenata) tipa uravnoteženog nepotpunog blok dizajna tipa 2-(v, b, r, k, λ), tj. 2-(v, k, λ)-dizajna. Da smo zahtijevali da svaku trojku vina isproba isti broj λ degustatora, imali bismo 3-(v, k, λ)-dizajn itd. Ovdje se "uživo" vide i razlozi za nazive: uravnoteženost dizajna čini konstantnost parametra λ, jer se u općim 2-dizajnima definira broj λ_{xy} za svaki par $x, y \in V$, a nepotpunost dolazi otud što se ne traže sve k-kombinacije od v elemenata, nego samo njih b. Isto tako, u općim dizajnima umjesto konstantnog broja r ("repeticija") možemo gledati broj r_x, za svako $x \in V$.

Prvi netrivijalni blok dizajn za $t = 2$ je slučaj kada je $\lambda = 1, k = 3$. To je sustav trojki, tako da je svaki par točaka sadržan u točno jednoj trojki, ili u terminima grafova, to je način pokrivanja svih bridova potpunog grafa s bridno-disjunktnim trokutima. Zbog uvjeta cjelobrojnosti za $t = 2$ je općenito

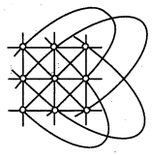
$$\begin{aligned} \lambda v(v-1) &\equiv 0 \pmod{k(k-1)} \\ \lambda(v-1) &\equiv 0 \pmod{k-1}, \end{aligned}$$

pa se odmah vidi da za $\lambda = 1$ i $k = 3$ dobivamo $v \equiv 1(\text{mod}6)$ ili $v \equiv 3(\text{mod}6)$. Stoga v mora biti iz skupa $\{3, 7, 9, 13, 15, 19, 21, 25, 27, 31, \ldots\}$. Za svaki takav v postoji blok dizajn tipa 2-$(v, 3, 1)$ i zove se **Steinerov sustav trojki**.

Za $v = 7$, Steinerov sustav trojki je projektivna ravnina reda 2 (vidi dalje), a za $v = 9$, to je afina ravnina dobivena iz projektivne ravnine reda 3 iz koje je izbačen jedan pravac i sve točke na tom pravcu:



Fanova konfiguracija ili Steinerov sustav trojki s $v = 7$ ili konačna projektivna ravnina reda 2 sa 7 točaka i 7 pravaca



Steinerov sustav trojki s $v = 9$

Tako je i Kirkmanov problem 15 učenica ekvivalentan problemu egzistencije Steinerovog sustava trojki za $v = 15$, uz dodatni uvjet "rješivosti", tj. da se blokovi dizajna raspadaju u klase tako da svaki element pripada točno jednom bloku iz svake klase. Takvi se blok dizajni zovu **rješivi**. U rješivom dizajnu mora biti v djeljiv s k, što vodi na $v \equiv 3(\text{mod}6)$. Može se pokazati da ako vrijede uvjeti cjelobrojnosti i $b \geq v$, da onda postoje 2-$(v, 3, \lambda)$-dizajni za sve moguće vrijednosti od v i λ. Taj je projekt (tj. dokaz) završen tek 1961., a potraga za dokazom iz "KNJIGE" traje i dalje.

Rješivi Steinerovi sustavi trojki zovu se **Kirkmanovi sustavi trojki**. Ray-Chaudhuri i R. J. Wilson su 1968. g. dokazali da Kirkmanov sustav trojki postoji ako i samo ako je $v \equiv (\text{mod}3)$, rješivši tako stoljeće star problem Kirkmana. Općenito, dizajni s $\lambda = 1$, nazivaju se **Steinerovi sustavi**, a blokovi se, iz geometrijskih razloga, u takvim sustavima nazivaju **pravci**. Pokazuje se da za $v = 2$, 3, 4, 5, 7, 8 postoje jedinstveni (do na izomorfizam) Steinerovi sustavi trojki, dok npr. postoje točno dva 2-$(13, 3, 1)$-dizajna, točno osamdeset 2-$(15, 3, 1)$-dizajna, preko jedne milijarde 2-$(19, 3, 1)$-dizajna, itd.

Iako uvjeti cjelobrojnosti nisu općenito i dovoljni uvjeti za egzistenciju dizajna, vrijedi sljedeći važan teorem (za dokaz vidi [14*]):

TEOREM 2 (R. J. Wilson, 1975). *Za zadane $k, \lambda \in \mathbb{N}$, postoji broj $v_0 = v_0(k, \lambda)$ tako da za svako $v \geq v_0$ za koje vrijede uvjeti iz Teorema 1 (uz $t = 2$), postoji 2-(v, k, λ)-dizajn.*

Drugim riječima, za dovoljno velik broj točaka v nužni uvjeti cjelobrojnosti (i $b \geq v$) su i dovoljni za postojanje dizajna za $t = 2$.

Primjer 4. Konstruirajte Steinerov sustav trojki s $v = 3m$ točaka, gdje je m neparan broj.

Rješenje. Definiramo $(V, \mathcal{B})$ ovako. $V := \{(x, i) | x = 0, 1, \ldots, m-1; i = 1, 2, 3\}$, a blokovi B se sastoje od svih trojki $\{(x, 1), (x, 2), (x, 3)\}$ i svih trojki oblika $\{(x, i), (y, i), (z, i+1)\}$, gdje je $x \neq y$, a $x+y \equiv 2z(\text{ mod } m)$, $i = 1, 2, 3$ (i+1 uzet mod 3). Sada nije teško provjeriti da je $(V, \mathcal{B})$ Steinerov sustav trojki s $v = 3m$ točaka. □

Od posebnog su interesa simetrični dizajni, u literaturi poznati pod kraticom SBIBD. **Simetrični 2-(v, k, λ)-dizajn** je blok dizajn $(V, \mathcal{B})$ kod kojeg je $b = v$ (i stoga $r = k$). Na svakom bloku tada leži k točaka, a kroz svake dvije točke prolazi točno λ blokova. Za svaki blok dizajn $(V, \mathcal{B})$ definirajmo **dualni dizajn** $(\mathcal{B}, V)$ kojem je matrica incidencije transponirana matrica blok dizajna $(V, \mathcal{B})$ (tu poistovjetimo točku x s blokom B koji sadrži x). U simetričnom dizajnu je i $k(k-1) = (v-1)\lambda$, a njegov dual je opet simetrični dizajn, jer za njegovu matricu incidencije A i matricu J (od samih jedinica) vrijedi $AJ = JA = kJ$, pa stoga $AA^T = (r-\lambda)I + \lambda J = A^T A$. Odavde slijedi da se u takvom dizajnu svaka dva različita bloka sijeku u točno λ točaka. Najpoznatiji nužni uvjeti na parametre simetričnog dizajna dani su sljedećim teoremom.

TEOREM 3 (Bruck-Chowla-Ryser, 1950). *Pretpostavimo da postoji simetrični 2-(v, k, λ)-dizajn, te $1 < k < v - 1$ ("netrivijalnost"). Broj $n := k - \lambda$ zove se tada* **red dizajna**. *Tada vrijedi*

(i) Ako je v paran, onda je red dizajna kvadrat prirodnog broja.

(ii) Ako je v neparan, onda diofantska jednadžba $z^2 = nx^2 + (-1)^{(v-1)/2}\lambda y^2$ ima rješenje $(x, y, z) \neq (0, 0, 0)$ u cijelim brojevima.

Skica dokaza. (i) To slijedi iz $(\det A)^2 = k^2(r-\lambda)^{v-1}$.
(ii) Uvjet iz ove tvrdnje je ekvivalentan činjenici da su kvadratne forme $\sum_{j=1}^{v} (\sum_{i=1}^{v} a_{ij}x_i)^2$ i $(k-\lambda)\sum_{i=1}^{v} x_i^2 + \lambda(\sum_{i=1}^{v} x_i)^2$ ekvivalentne. Ustvari je to nužan i dovoljan uvjet za egzistenciju racionalne matrice A koja zadovoljava gore navedene jednakosti. □

Tako npr., iz Teorema 3 (i) slijedi da ne postoji 2-$(22, 7, 2)$-dizajn, a iz tvrdnje (ii) da ne postoji 2-$(43, 7, 1)$-dizajn.

Za $\lambda = 1$, simetrični 2-$(v, k, 1)$-dizajn se zove **konačna projektivna ravnina**. U tom je slučaju $n = k - 1$ njezin red, pa je konačna projektivna ravnina simetrični blok dizajn s parametrima $v = b = n^2 + n + 1$, $r = k = n + 1$ i $\lambda = 1$. Odavno se zna (Veblen, 1906.) da postoje konačne projektivne ravnine čiji je red potencija prostog broja. Fanova ravnina je "najmanji" primjer (vidi prethodnu sliku) takve ravnine reda 2 s točkama $1, 2, \ldots, 7$ i pravcima $a, b, \ldots, g$. Evo jedne "konkretne" primjene Fanove ravnine.

Primjer 5 (Smjena čuvara). Tvornicu "Macrohard" osigurava sedam čuvara. Svaka se dnevna smjena sastoji od trojice čuvara, a raspored smjena treba sačiniti za sedam dana u tjednu. Kako treba napraviti raspored, tako da svaka dvojica imaju jednu zajedničku smjenu (jer tako svatko pazi na ostale da ne dođe do iznošenja tajnih podataka)?

Rješenje. Označimo čuvare s $1, 2, \ldots, 7$. Smjene su pravci $a, b, \ldots, g$ (u nekom poretku) Fanove ravnine (vidi prethodnu sliku). Svaki čuvar ima isti broj smjena (tj. 3) u tjednu, svaka dvojica su u jednoj smjeni, nitko nema više od dvije smjene za redom, a u svakoj smjeni je jedan koji je čuvao i prethodni dan, pa zna "friške tračeve" itd. □

Konstrukcija konačne projektivne ravnine reda $n = q$, u oznaci $PG(2, q)$ gdje je q potencija prostog broja je potpuno analogna geometrijskoj konstrukciji realne projektivne ravnine $\mathbb{R}P^2$ nad poljem $\mathbb{R}$ (tj. kao izvjesno proširenje obične euklidske ravnine s točkama u beskonačnosti). Pođemo od polja $\mathbf{F} = \mathbf{F}_q$ i na skupu $\mathbf{F}^3 \setminus \{(0,0,0)\}$ definiramo relaciju ekvivalencije $\sim$ ovako $(x, y, z) \sim (x', y', z') \iff \exists \alpha \in \mathbf{F} \setminus \{0\}$, $x' = \alpha x$, $y' = \alpha y$, $z' = \alpha z$. Točke od $PG(2, q)$ su klase ekvivalencije $[(x, y, z)]$. Za svaku trojku $(a, b, c) \in \mathbf{F}^3 \setminus \{(0,0,0)\}$ definiramo pravac $\mathcal{P}(a, b, c) := \{[(x, y, z)] | ax + by + cz = 0\}$. Analogno se definira i konačni d-dimenzionalni projektivni prostor $PG(d, q)$, gdje je q potencija prostog broja. Tu gledamo $(d+1)$-dimenzionalni prostor V nad $\mathbf{F}_q$ i analogno konstruiramo $PG(d, q)$. Za $0 < r < d$ se $(r+1)$-dimenzionalni potprostor zove r-ploska (engl. *flat*). Točke i r-ploske u $PG(d, q)$ tada čine vrhove i blokove jednog 2-(v, k, λ)-dizajna, pri čemu je $v = \binom{d+1}{1}_q$, $k = \binom{r+1}{1}_q$ i $\lambda = \binom{d-1}{r-1}_q$, gdje je $\binom{n}{k}_q$ q-binomni koeficijent (vidi pogl. II). Posebno, ako je $r = d - 1$, onda se $(d-1)$-ploska zove **hiperravnina** u $P(d, q)$. Hiperravnine u $PG(d, q)$ su dizajni s $v = (q^{d+1} - 1)/(q - 1)$, $k = (q^d - 1)/(q - 1)$, $\lambda = (q^{d-1} - 1)/(q - 1)$ i red $n = k - \lambda = q^{d-1}$.

Postoje li konače projektivne ravnine (ili prostori) ostalih redova? Za $n = 2$, 3, 4 ili 5 postoje (to su potencije prostih brojeva). Za $n = 6$ ne postoji projektivna ravnina reda 6, jer Bruck-Chowla-Ryserova jednadžba $x^2 + y^2 = 6z^2$ nema netrivijalnih rješenja. Projektivne ravnine reda $7, 8, 9$ opet postoje. Nakon dugotrajnih potraga i golemog kompjuterskog računanja 1989. Lam, Thiel i Swiercz uspjeli su dokazati da ne postoji projektivna ravnina reda 10 (vidi Canad. J. Math 41 (1989), 1117–1123). Sljedeći slučaj $n = 12$, tj. pitanje egzistencije projektivne ravnine reda 12 je otvoren problem i čini se da je za provjeru gigantskog broja svih konfiguracija sadašnja kompjuterska tehnologija još prespora.

Konačna afina ravnina reda n, u oznaci $AG(2, n)$, je blok dizajn s parametrima $v = n^2$, $b = n^2 + n$, $r = n + 1$, $k = n$, $\lambda = 1$, tj. to je 2-$(n^2, n, 1)$-dizajn , $n \geq 2$, a dobije se iz projektivne ravnine tako da se odstrane jedan pravac i sve točke tog pravca. Obratno, ako je dana afina ravnina , uvijek se može dodati $n + 1$ novih

točaka tako da se dobije projektivna ravnina. Naime, definiramo li relaciju paralelnosti $\|$ pravaca afine ravnine s $p \| p' \iff p \cap p' = \emptyset$ (ili $p = p'$), onda svakoj klasi ekvivalencije od $\|$ dodamo novu točku "u beskonačnosti" i tu točku dodamo svakom pravcu iz te klase, a sve točke iz "beskonačnosti" stavimo na novi pravac. Na taj se način dobiva $1 - 1$ korespondencija između afinih ravnina reda n i projektivnih ravnina reda n. Analogno se definira i d-dimenzionalni afini prostor $AG(d, q)$ reda q.

Podsjetimo se da je **latinski kvadrat** reda n kvadratna tablica (ili matrica) tipa $n \times n$ čiji je svaki član iz skupa $[n] = \{1, \ldots, n\}$, a svaki se broj iz $[n]$ pojavljuje točno jedanput u svakom retku i svakom stupcu. Dva su latinska kvadrata **ortogonalna** ako njihovim sparivanjem, član po član, dobijemo svih n^2 uređenih parova $(i, j) \in [n] \times [n]$. Promotrimo sada neki skup međusobno ortogonalnih latinskih kvadrata reda n.

LEMA 1. *Neka su $A_1, A_2, \ldots, A_t$ međusobno ortogonalni latinski kvadrati reda n. Tada je $t \leq n - 1$.*

Dokaz. Uočimo prvo sljedeće. Neka su A i B ortogonalni latinski kvadrati reda n, a π permutacija od $\{1, 2, \ldots, n\}$. Neka je A' dobiven iz $A = [a_{ij}]$ tako da je $A' = [\pi(a_{ij})]$. Tada odmah iz definicije ortogonalnosti $A \perp B$ slijedi $A' \perp B$, tj. "preimenovanjem" članova ortogonalnost se čuva. Sada u svakom A_i permutirajmo članove tako da prvi redak postane $(1, 2, \ldots, n)$ i neka je tako dobiven latinski kvadrat A_i', $i = 1, 2, \ldots, t$.

Tako dobivamo $A_1', A_2', \ldots, A_t'$ i vrijedi $A_i' \perp A_j'$ za $i \neq j$. Pogledajmo poziciju $(2, 1)$ latinskog kvadrata A_i'. Tu ne može biti 1, jer je 1 već u prvom stupcu prvog retka. Nadalje, za $i \neq j$, ne mogu A_i' i A_j' imati isti broj na mjestu $(2, 1)$. Kad bi, naime, imali takav broj k na tom mjestu, onda bi sparivanje dalo (k, k) na poziciji $(2, 1)$, a to je nemoguće, jer se (k, k) sparivanjem A_i', A_j' pojavljuje na k-tom mjestu prvog retka. Stoga na poziciji $(2, 1)$ svakog A_i' može doći samo jedan od brojeva $2, 3, \ldots, n$. Zato je $t \leq n - 1$. □

TEOREM 4. *Za $n \geq 2$ postoji konačna projektivna ravnina reda n ako i samo ako postoji skup od $n - 1$ međusobno ortogonalnih latinskih kvadrata reda n.*

Dokaz. Prema gornjoj napomeni dovoljno je dokazati egzistenciju pripadne afine ravnine. Pretpostavimo da imamo $\leq n - 1$ međusobno ortogonalnih latinskih kvadrata reda n. Tada su točke pripadne afine ravnine svih n^2 uređenih parova $(i, j) \in [n] \times [n]$. Za dani latinski kvadrat $A = [a_{ij}]$ pravac čine n točaka (i, j) za koje je $a_{ij} = k$, gdje je $k \in \{1, 2, \ldots, n\}$ čvrst broj. Svih n pravaca tako dobivenih za sve vrijednosti od k su paralelni. Prema tome, svaki latinski kvadrat daje jednu klasu paralela. Skup svih parova (i, j) za čvrsto i također je pravac, a isto tako za čvrsto j. Ovih $n^2 + n$ pravaca i n^2 točaka čini afinu ravninu reda n. Provjera da se zaista radi o afinoj ravnini reda n slijedi iz ortogonalnosti latinskih kvadrata (i Leme). Ova se konstrukcija može lako i obrnuti. Detalje prepuštamo čitatelju. □

Označimo li s $N(n)$ maksimalni broj međusobno ortogonalnih latinskih kvadrata reda n, onda je zbog Leme $N(n) \leq n - 1$ za $n \geq 2$, a $N(q) = q - 1$, ako je q potencija

prostog broja. No, može se pokazati da je $\lim_{n\to\infty} N(n) = \infty$. Stoga, ako je n_r najveći broj za koji ne postoji r međusobno ortogonalnih latinskih kvadrata (stoga $N(n) \geq r$ za $n > n_r$), onda je poznato sljedeće: $n_2 = 6$ (Tarry, 1901), $n_3 \leq 10$ (Wilson, 1978), $n_4 \leq 42$ (Abel, 1993), $n_5 \leq 62$ (Hanani, 1970) itd., asimptotski $n_r = O(r^{14.8})$.

Spomenimo da je teorija dizajna u uskoj vezi s teorijom kodiranja i kriptografijom (vidi npr. knjige [43], [151], [10*], [49*], [72*]). Neka je $\mathbf{F}_q$ konačno polje s q elemenata, a V vektorski prostor nad $\mathbf{F}_q$ s bazom $(e_1, e_2, \ldots, e_n)$. **Kôd** $\mathcal{C}$ definiramo kao podskup od V, **linearni kôd** kao potprostor od V. **Hammingova udaljenost** $d_H(u,v)$ vektora $u, v \in V$ je broj koordinata u kojima se u i v razlikuju ako su razvijeni po bazi (e_i): $u = \sum u_i e_i$, $v = \sum v_i e_i$, tj. $d_H(u,v) = \#\{i | u_i \neq v_i\}$. **Težina vektora** u je broj nenul koordinata, tj. $d_H(u,0)$. **Minimalna distanca** $d = d(\mathcal{C})$ kôda $\mathcal{C}$ je $\min\{d_H(u,v) | u, v \in \mathcal{C}, u \neq v\}$, a **nosač vektora** $u = \sum u_i e_i$ je skup $\{i | u_i \neq 0\}$.

Parametar d posebno je važan u primjenama, jer kôd s minimalnom distancom d ima tzv. sposobnost ispravljanja e pogrešaka, pri čemu je $e = \lfloor \frac{d-1}{2} \rfloor$.

Najizravnija veza kôdova i dizajna jest sljedeća. Neka je $\mathcal{C}$ kôd s duljinama riječi n (tj. $\mathcal{C} \subseteq \mathbf{F}_q^n$). Tada pogledamo familiju nosača riječi iz $\mathcal{C}$ težine w. To daje dizajn s blokovima veličine w na n točaka.

Obrnuto, ako je $(V, \mathcal{B})$ dizajn, a $\mathbf{F}$ konačno polje, pogledamo vektorski potprostor od $\mathbf{F}^v$ razapet sa svim karakterističnim vektorima blokova iz $\mathcal{B}$. To daje linearni kôd riječi duljine v.

Najpoznatiji među kodovima su **Golayev binarni kôd** s parametrima $n = 23$, $q = 2$, $d = 7$ i $|\mathcal{C}| = 2^{12} = 4096$ i **prošireni Golayev binarni kod** s $n = 24$, $q = 2$, $d = 8$ i $|\mathcal{C}| = 4096$. Ovaj potonji se dobije tako da se brojevi $0, 1, 2, \ldots, 2^{24} - 1$ napišu u binarnom sustavu (kao binarni vektori duljine 24) i prekriži svaki vektor s distancom manjom od 8 s prethodno neprekriženim vektorima. Neprekriženih 4096 vektora čine taj kôd. To je, zapravo, leksikografski prvi kôd s duljinom riječi $n = 24$ i s minimalnom distancom jednakom 8. To vodi na egzistenciju dizajna 5-$(24, 8, 1)$. Ovaj se dizajn katkad zove i **Wittov dizajn**. Grupa permutacija na 24 koordinate koje čuvaju kôd (tj. grupa automorfizama proširenog Golayevog kôda $\mathcal{C}$) zove se **Mathieuova grupa** M_{24}. To je grupa reda $24 \cdot 23 \cdot 22 \cdot 21 \cdot 20 \cdot 16 \cdot 3$ i pokazuje se da djeluje 5-tranzitivno na 24 koordinatnih pozicija. Pritom kažemo da grupa (nekih permutacija) G djeluje t-**tranzitivno** na skupu X ako za svake dvije uređene t-torke $(x_1, \ldots, x_t)$, $(x'_1, \ldots, x'_t)$ različitih elemenata iz X, postoji element $g \in G$ koji prevodi x_i u x'_i, $i = 1, \ldots, t$. Očito t-tranzitivnost povlači $(t-1)$-tranzitivnost.

Najpoznatije beskonačne serije simetričnih blok dizajna (SBIBD) su osim već spomenutih hiperravnina i ploski u konačnim projektivnim prostorima $PG(d,q)$ i **Hadamardovi dizajni** s parametrima $v = 4n-1$, $k = 2n-1$, $\lambda = n-1$ koji postoje ako i samo ako postoji **Hadamardova matrica** reda $4n$, tj. matrica s članovima ± 1 čiji su retci uzajamno ortogonalni. Poznato je da takve matrice postoje za sve $n \leq 166$ ($n \neq 107$) i za $4n = 2^s m$, $m^2 \leq 2^s$ s još nekim slučajevima. Slutnja je da Hadamardove matrice reda $4n$ postoje za svako n. Postoje i druge beskonačne serije SBIBD-ova, ali su i neki "sporadični" dizajni konstruirani specijalnim metodama, npr. s parametrima $v = 71$, $k = 21$, $\lambda = 6$, $n = 15$ čiju su egzistenciju dokazali

Janko[3] i dr. 1984.

Proučavaju se i mnoge generalizacije u teoriji dizajna, npr. latinski pravokutnici, Roomovi kvadrati itd. Zatim razne varijacije dijelova definicije blok dizajna; npr. u parovima uravnoteženi dizajni (s varijabilnim veličinama blokova), parcijalno uravnoteženi dizajni (kod koji je "konstantan λ" modificiran), pa ciklički dizajni, dizajni na grafovima itd.

S druge strane, blok dizajni su poseban slučaj vrlo općenitih struktura, poznatih kao **sustav incidencija**. To je trojka (X, Y, R), pri čemu je $R \subseteq X \times Y$ binarna relacija među (konačnim nepraznim) skupovima X i Y, koja se zove **relacija incidencije**. Za $x \in X$ i $y \in Y$ za koje je $(x,y) \in R$ kažemo da je (vrh) x **incidentan** s (blokom) y. Svaki se blok obično poistovjeti sa skupom vrhova koji su s njim incidentni, pa tako dobijemo prirodno preslikavanje $f : Y \to 2^X$, $f(y) = \{x \in X | xRy\}$. Ta funkcija f definira familiju podskupova od X indeksiranu skupom Y, pa stoga sustav incidencija možemo zamišljati i kao **hipergraf** (X, E) s vrhovima iz X i hiperbridovima iz E. Ako se E sastoji samo od dvočlanih podskupova od X, dobivamo graf.

Kad na skupu X istovremeno imamo nekoliko binarnih relacija koje zadovoljavaju neke prirodne uvjete presijecanja, onda govorimo o **shemi relacija** ili **asocijativnoj shemi**. Njihovo algebarsko proučavanje preko njihovih matrica incidencija dovodi u vezu kombinatoriku s teorijom grupa i drugim algebarskim strukturama. Tim i sličnim pitanjima bavi se tzv. **algebarska kombinatorika** (v. [13]).

O blok dizajnima i konačnim geometrijama postoji opsežna literatura, npr. [16], [27], [37], [43], [54],[108], [111], [119], [219], [227], [9*], [14*], [48*] i dr.

§ 2. Matroidi

Teorija matroida ili "kombinatorne geometrije" postaje sve važnija u kombinatorici, računarskim znanostima i primjenama. Prvi poticaj toj teoriji dao je H. Whitney 1935., a nazivom matroid sugerirao je generalizaciju pojma matrice. Ideja je da mnoga svojstva linearne zavisnosti u vektorskim prostorima ne ovise o definiciji zavisnosti, nego samo o nekim aksiomima tzv. "apstraktnim svojstvima linearne zavisnosti". Stoga se katkad ta teorija zove "bezkoordinatna linearna algebra". Kasnije se uvidjelo da isti aksiomi vrijede za relaciju zavisnosti i u drugim područjima, kao što je teorija grafova, teorija rešetaka itd.

Matroid M na konačnom skupu S je uređeni par $(S, \mathcal{B})$, gdje je $\mathcal{B}$ familija podskupova od S za koju vrijedi

(B1) **Jednakobrojnost**. Za svaka dva elementa $B, B' \in \mathcal{B}$ je $|B| = |B'|$;

(B2) **Aksiom zamjene**. Za svako $B, B' \in \mathcal{B}$ i svako $x \in B$, postoji $y \in B'$ tako da je $(B \setminus \{x\}) \cup \{y\} \in \mathcal{B}$.

Elementi od $\mathcal{B}$ zovu se **baze** matroida M, a podskupovi baza **nezavisni skupovi** od M. **Rang matroida** M je broj elemenata $r(M)$ bilo koje baze.

[3] Zvonimir Janko (r. 1932), hrvatski matematičar, profesor na Universität Heidelberg, Njemačka

Tipični primjer matroida je konačan skup S vektora u vektorskom prostoru, a baze čine maksimalni linearno nezavisni skupovi vektora iz S.

Primjer 1. Promotrimo matricu

$$A = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 0 \end{bmatrix}.$$

Neka je $S = [5]$, a $A_1, A_2, \ldots, A_5$ stupci od A. Za podskup $I \subseteq S$, neka je A_I podmatrica od A koja se sastoji od stupaca čiji su indeksi iz I. Familija $\mathcal{B}_A = \{\{1,2,3\}, \{1,2,4\}, \{1,3,4\}, \{1,3,5\}, \{1,4,5\}, \{2,3,5\}, \{2,4,5\}, \{3,4,5\}\}$ čine bazu matroida $M_{(A)}$ na skupu $[5]$.

Matroid $M_{(A)}$, kao u gornjem primjeru, zove se **matroid stupaca matrice** A. Stupci od A_I čine bazu prostora stupaca od A. Slično se, naravno, može provesti za retke matrice A.

Neka je S n-člani skup, a za $k \leq n$, $\mathcal{P}_k(S)$ svi k-člani podskupovi od S. Tada je očito $(S, \mathcal{P}_k(S))$ matroid koji se označava sa $U_{k,n}$ i zove k-**uniformni**. Za $k = n$, $U_{n,n}$ se zove **slobodni matroid** na S.

Dva matroida $M = (S, \mathcal{B})$ i $M' = (S', \mathcal{B}')$ su **izomorfna** u oznaci $M \approx M'$ ako postoji bijekcija $f : S \to S'$ takva da je $f(B) \in \mathcal{B}' \iff B \in \mathcal{B}$.

Neka je $M = (S, \mathcal{B})$ matroid, a $s_1 < s_2 < \cdots < s_n$ linearni uređaj na skupu S. Tada se $(m \times n)$-matrica A s elementima iz nekog polja $\mathbf{F}$ zove **matrična reprezentacija matroida** M s obzirom na uređaj $s_1 < s_2 < \cdots < s_n$, ako je preslikavanje $f : S \to [n]$ $f(s_i) = i$, $i = 1, 2, \ldots, n$, izomorfizam matroida M i matroida stupaca $M_{(A)}$ matrice A. Ako postoji takva matrica A nad poljem $\mathbf{F}$, onda kažemo da je M **reprezentabilan**. Ako je M ranga k, obično se uređaj odabere tako da $\{s_1, s_2, \ldots, s_k\}$ bude baza od M.

Tako je npr. matroid $U_{2,4}$ reprezentabilan s matricom $A = \begin{bmatrix} 1 & 0 & 1 & 1 \\ 0 & 1 & x & y \end{bmatrix}$, gdje su $x, y \neq 0$ i $x \neq y$. Stoga je $U_{2,4}$ reprezentabilan nad svakim poljem, osim nad poljem s dva elementa (jer bi tada moralo biti $x = y$). Općenito je $U_{k,n}$ reprezentabilan. Naime, ako je $Z = [z_{ij}]$ $(k \times n)$-matrica čiji su članovi z_{ij} varijable shvaćene kao elementi polja racionalnih funkcija $\mathbb{Q}(z_{ij})$, onda je determinanta svake $(k \times k)$-podmatrice od Z nenul polinom u varijablama z_{ij}, tj. nenul element u polju $\mathbb{Q}(z_{ij})$, pa je svakih k stupaca matrice Z linearno nezavisno. Stoga je matroid stupaca matrice Z izomorfan matroidu $U_{k,n}$. Dakle, svaki unimorfni matroid je reprezentabilan nad nekim poljem. Postoje matroidi koji nisu reprezentabilni.

Katkad je pogodnije aksiomatski zadati matroid s nezavisnim skupovima, katkad s rangom, katkad s tzv. operacijom zatvaranja, katkad s tzv. hiperravninama, a katkad s tzv. ciklusima. Svi ti načini zadavanja matroida su ekvivalentni. Ta je tvrdnja sadržaj sljedećeg osnovnog teorema.

TEOREM. *Neka je S konačan skup. Tada je u svakom od sljedećih slučajeva na S definiran matroid, ako je još zadano:*

a) **Nezavisni skupovi.** *Familija $\mathcal{J}$ podskupova od S za koju vrijedi*

(N1) $\emptyset \in \mathcal{J}$,

(N2) $Y \in \mathcal{J}$, $X \subseteq Y \Rightarrow X \in \mathcal{J}$,

(N3) $X, Y \in \mathcal{J}$, $|X| < |Y| \Rightarrow \exists y \in Y \setminus X$, *tako da je* $X \cup \{y\} \in \mathcal{J}$.

b) **Aksiomi ranga.** *Funkcija $r : 2^S \to \mathbb{N}_0$ za koju vrijedi*

(R1) $0 \leq r(X) \leq |X|$, $\forall X \in 2^S$,

(R2) $X \subseteq Y \Rightarrow r(X) \leq r(Y)$, $\forall X, Y \in 2^S$ *(monotonost)*

(R3) $r(X \cup Y) + r(X \cap Y) \leq r(X) + r(Y)$, $\forall X, Y \in 2^S$ *(semimodularnost).*

c) **Operacija zatvaranja.** *Preslikavanje* $\mathrm{cl} : 2^S \to 2^S$ *za koje vrijedi (*cl *dolazi od engl. closure)*

(CL1) $X \subseteq \mathrm{cl}(X), \forall X \in 2^S$,

(CL2) $X \subseteq Y \Rightarrow \mathrm{cl}(X) \subseteq \mathrm{cl}(Y)$,

(CL3) $\mathrm{cl}(\mathrm{cl}(X)) = \mathrm{cl}(X)$, $\forall X \in 2^S$,

(CL4) $x, y \in S$, $X \in 2^S$, $y \notin \mathrm{cl}(X)$, $y \in \mathrm{cl}(X \cup \{x\}) \Rightarrow x \in \mathrm{cl}(X \cup \{y\})$.

d) **Hiperravnine.** *Familija $\mathcal{H}$ pravih podskupova od S za koju vrijedi*

(H1) $H_1, H_2 \in \mathcal{H}$, $H_1 \neq H_2 \Rightarrow H_1 \not\subseteq H_2$,

(H2) $H_1, H_2 \in \mathcal{H}$, $H_1 \neq H_2$, $x \notin H_1 \cup H_2 \Rightarrow \exists H_3 \in \mathcal{H}$, $H_3 \supset (H_1 \cap H_2) \cup \{x\}$.

e) **Ciklusi.** *Familija $\mathcal{C}$ podskupova od S za koju vrijedi*

(C1) $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2 \Rightarrow C_1 \not\subseteq C_2$,

(C2) $C_1, C_2 \in \mathcal{C}$, $C_1 \neq C_2$, $z \in C_1 \cap C_2 \Rightarrow \exists C_3 \in \mathcal{C}, C_3 \subseteq (C_1 \cup C_2) \setminus \{z\}$.

(Dakako, tamo gdje u ovim aksiomima nema znaka $\forall$, trebalo bi ga pisati na početku; nadamo se da ovo izostavljanje neće zbuniti čitatelja.)

Skup $X \subseteq S$ za koji je $\mathrm{cl}\, X = X$ zove se **zatvoren skup** (ili **ploska**, engl. *flat*), a ako je $\mathrm{cl}\, X = S$, **razapinjući skup.** Objasnimo ukratko veze među svim navedenim pojmovima. U slučaju (a), bazu čine nezavisni skupovi s najviše elemenata. U slučaju (b) dokaže se da funkcija ranga ima svojstva

(R1') $r(\emptyset) = 0$,

(R2') $r(X) \leq r(X \cup \{y\}) \leq r(X) + 1$, $\forall X \in 2^S$, $\forall y \in S$,

(R3') $r(X \cup \{y\}) = r(X \cup \{z\}) = r(X) \Rightarrow r(X \cup \{y\} \cup \{z\}) = r(X)$

i da su ta svojstva (zajedno) ekvivalentna s (R1), (R2), (R3). Skup B je baza ako je on minimalan skup za koji je $r(B \cup \{x\}) = r(B)$, $\forall x \in S$. Za reprezentabilne matroide ranga $r(X)$ je rang podmatrice čiji stupci odgovaraju skupu X. Ako imamo zatvorene skupove, onda je skup $X \subseteq S$ nezavisan ako $x \notin \mathrm{cl}(X \setminus \{x\})$, $\forall x \in X$. Ako je matroid zadan pomoću ranga, onda $\mathrm{cl}(X) = \{y \in S | r(X \cup \{y\}) = r(X)\}$. Ako je matroid zadan s operacijom zatvaranja, onda je hiperravnina definirana kao zatvoreni skup $H \neq S$ za koji je $\mathrm{cl}(H \cup \{x\}) = S$, $\forall x \notin H$. Obratno, ako imamo hiperravnine, zatvoreni skupovi su S, sve hiperravnine i svi mogući presjeci hiperravnina. Ako je $M = (S, \mathcal{B})$ matroid ranga k, onda je hiperravnina zatvoren skup

$H \subseteq S$ ranga $k-1$. Napokon, ako je matroid zadan s ciklusima, onda je skup nezavisan ako ne sadrži nijedan ciklus. Obratno, ako je matroid zadan s nezavisnim skupovima, onda su ciklusi svi oni skupovi C koji nisu nezavisni, ali postaju nezavisni nakon uklanjanja bilo kojeg elementa, tj. ciklusi su "minimalni zavisni skupovi". Ako je M reprezentabilan, $M \approx M_{(A)}$ i ako je $C = \{x_1, x_2, \ldots, x_p\}$ ciklus tako da x_i odgovara i-tom stupcu matrice A, onda (nakon pogodno odabrane baze) A se može zapisati za neke $a_1, \ldots, a_p \neq 0$ u obliku:

$$A = \begin{array}{c} \begin{array}{cccccc} x_1 & x_2 & \ldots & x_{p-1} & x_p & \ldots \end{array} \\ \left[\begin{array}{cccccc} 1 & 0 & \ldots & 0 & a_1 & * \\ 0 & 1 & \ldots & 0 & a_2 & * \\ \cdot & \cdot & & \cdot & \cdot & \\ \cdot & \cdot & & \cdot & \cdot & \\ 0 & \ldots & \ldots & 1 & a_p & * \\ & & 0 & & & \end{array}\right] \end{array}.$$

Osnovne konstrukcije novih matroida iz starih su sljedeće. **Dualni matroid** M^* matroida $M = (S, \mathcal{B})$ je matroid $M^* = (S, \mathcal{B}^*)$, gdje je $\mathcal{B}^* = \{S \setminus B | B \in \mathcal{B}\}$. Ako je M reprezentabilan, onda je to i M^*. **Direktna suma** $M \oplus M_2$ matroida $M_i = (S_i, \mathcal{B}_i)$, $i = 1, 2$ je matroid $M = (S_1 \cup S_2, \mathcal{B}_1 \cup \mathcal{B}_2)$. **Unija matroida** $M_i = (S, \mathcal{J}_i)$, $i = 1, 2$ zadanih s nezavisnim skupovima je matroid $M = (S, \mathcal{J})$, gdje je $\mathcal{J} = \{J_1 \cup J_2 | J_1 \in \mathcal{J}_1, J_2 \in \mathcal{J}_2\}$. **Restrikcija** matroida $M = (S, \mathcal{J})$ na podskup $T \subseteq S$ je matroid $M|_T = (T, \mathcal{J}|_T)$, gdje je $X \in \mathcal{J}|_T \iff X \in \mathcal{J}$. Za $M|_T$ se još kaže da je dobiven iz M **odstranjivanjem** $S \setminus T$. **Kontrakcija** matroida $M = (S, \mathcal{J})$ s obzirom na podskup $T \subseteq S$ je matroid $M/_T = (S \setminus T, \mathcal{J}/T)$, gdje za $X \subseteq S \setminus T$ vrijedi: $X \in \mathcal{J}/T \iff X \cup C \in \mathcal{J}, \forall C \in \mathcal{J}, C \subseteq T$. **Minora matroida** dobiva se nizom odstranjivanja i kontrakcija.

Baze, ciklusi i rang dualnog matroida M^* zovu se redom **kobaze**, **kociklusi** i **korang** od M. C^* je kociklus od M (nad S) ako i samo ako je $C^* = S \setminus H$, gdje je H hiperravnina od M. Stoga su ciklusi i hiperravnine dualni pojmovi. Isto tako su i restrikcija i kontrakcija dualne operacije na matroidima jer vrijedi $M|_T = (M^*/T)^*$ i $M/_T = (M^*|_T)^*$. Još jedna važna konstrukcija bazira se na ovom teoremu.

TEOREM (J, Edmonds). *Neka je $f : 2^S \to \mathbb{N}_0$ funkcija za koju je $f(\emptyset) = 0$ i koja je monotona i semimodularna (tj. vrijede (R2) i (R3) iz osnovnog teorema). Neka je familija $\mathcal{J} \subseteq 2^S$ definirana s $X \in \mathcal{J} :\iff |A| \leq f(A)$, $\forall A \subseteq X$. Tada je $\mathcal{J}$ familija nezavisnih skupova nekog matroida na S. Rang skupa X je $r(X) = \min_{A \subseteq X}(f(A) + |X \setminus A|)$.*

Neka je $G = (V(G), E(G))$ povezan graf. Tada mu je pridružen tzv. **ciklički matroid** $M_G = (E(G), \mathcal{B})$, gdje je tipičan član od $\mathcal{B}$ (tj. baza od M_G) skup bridova nekog razapinjućeg stabla od G. Ako je graf G nepovezan, onda je M_G direktna suma matroida pridruženih svakoj komponenti povezanosti od G. **Grafički matroid** je onaj koji je izomorfan nekom M_G. Nezavisni skupovi od M_G jesu bridovi podšume od G, rang od M_G je broj bridova bilo koje razapinjuće šume od G, ciklusi od M_G su upravo skupovi bridova ciklusa grafa G, zatvarač skupa bridova E' grafa

G je skup E' zajedno sa svim bridovima od G čija su oba kraja u istoj komponenti od $G[E']$, a zatvoreni skup u M_G je skup E' sa svojstvom da je svaki brid od G s oba kraja u istoj komponenti od $G[E']$, sadržan u E'. Rang podskupa $E' \subseteq E(G)$ je $r(E') = |V(G) - c(G[E'])$. Ako je $M (\approx M_G)$ grafički matroid, onda se $M^* (\approx M_G^*)$ zove **kografički matroid**. Njihove su baze komplementi razapinjućih stabala (ako je G povezan), tj. **kostabla**. $U_{2,4}$ je najmanji negrafički matroid.

Grafički matroidi su reprezentabilni nad svakim poljem. Ta činjenica omogućava razne veze između teorije grafova i linearne algebre. S druge strane, mnogi rezultati iz teorije grafova mogu se interpretirati u terminima matroida. Tako npr. restrikcija i kontrakcija matroida odgovaraju izbacivanju bridova (tj. $G - E'$), odnosno kontrakcijama bridova u grafu.

Neka je $\rho \subseteq X \times Y$ relacija incidencije. Za $A \subseteq X$ označimo $\rho(A) := \{y \in Y | \exists x \in A, (x, y) \in \rho\}$. Ovo preslikavanje $\rho : 2^X \to 2^Y$ ima svojstva $\rho(\emptyset) = 0$, $A \subseteq B \subseteq X \Rightarrow \rho(A) \subseteq \rho(B)$ i $\rho(A \cup B) = \rho(A) \cup \rho(B)$, $\rho(A \cap B) \subseteq \rho(A) \cap \rho(B)$, $\forall A, B \subseteq X$. Odatle proizlazi da funkcija $f : 2^X \to \mathbb{N}_0$, $f(A) := |\rho(A)|$ zadovoljava uvjete Edmondsovog teorema, pa stoga inducira matroid koji se označava s $T(X, Y, \rho)$. Skup $T \subseteq X$ je nezavisan u tome matroidu ako i samo ako je

$$|S| \leq |\rho(S)|, \quad \forall S \subseteq T. \tag{$*$}$$

Ako na relaciju ρ gledamo kao na sustav incidencije, pri čemu su elementi od X točke, elementi od Y blokovi, a relacija ρ kaže je li neka točka u nekom bloku ili nije, onda se vidi da je $(*)$ zapravo uvjet iz Hallovog teorema o sparivanju. Stoga nezavisni skupovi matroida $T(X, Y, \rho)$ odgovaraju (parcijalnim) **transversalama**. Zato se svaki matroid izomorfan s nekim $T(X, Y, \rho)$ zove **transverzalni matroid**. U terminima teorije matroida mogu se time dobiti značajne generalizacije Hallovog teorema koje vode na **teoriju transverzalnosti**.

Spomenimo vezu matroida i **teorije rešetaka**. Podsjetimo da je **rešetka** p.u. skup u kojem svaki par elemenata ima jedinstvenu najmanju gornju među (supremum) i najveću donju među (infimum). Takve su npr. rešetka particija skupa ili rešetka vektorskih prostora. Svakom matroidu je pridružena **rešetka ploski matroida** s inkluzijom kao uređajem. Takva klasa rešetki, tzv. **geometrijske rešetke** imaju lijepa geometrijska svojstva. I obratno, svaka geometrijska rešetka definira matroid koji se zove **jednostavni matroid** (ili **kombinatorna geometrija**). Time se dobiva veza između projektivne geometrije, teorije rešetaka, teorije grafova i teorije p.u. skupova.

U poliedarskoj kombinatorici i drugdje važan je pojam orijentiranog matroida. **Involucija** na skupu E je funkcija $* : E \to E$, tako da je $(x^*)^* = x$, $\forall x \in E$, a kažemo da je **bez fiksnih točaka** ako je $x^* \neq x$, $\forall x \in E$. **Orijentirani matroid** je uređena trojka $(E, \mathcal{C}, *)$ gdje je E konačni skup, $\mathcal{C}$ familija nepraznih podskupova od E, a $*$ involucija na E bez fiksnih točaka, tako da vrijedi:

(a) $\mathcal{C}$ je **gomila** (engl. *clutter*), tj. $A \not\subset B$, $\forall A, B \in \mathcal{C}$;

(b) $A \in \mathcal{C} \Rightarrow A^* \in \mathcal{C}$ i $A \cap A^* = \emptyset$;

(c) Ako su $A, B \in \mathcal{C}$, $x \in A \cap B^*$ i $A \neq B^*$, onda postoji $C \in \mathcal{C}$ tako da je

$$C \subseteq (A \cup B) \setminus \{x, x^*\}.$$

Članovi familije $\mathcal{C}$ se zovu **ciklusi orijentiranog matroida**.

Primjer 1. Neka je E konačni skup nenul vektora vektorskog prostora nad uređenim poljem takav da je $E = -E$. Za $x \in E$, neka je $x^* = -x$. Familija $\mathcal{C}$ neka se sastoji od minimalnih podskupova $C \subseteq E$ tako da vrijedi sljedeće: 1) $C \cap C^* = \emptyset$, 2) postoje $\alpha_v \in \mathbb{R}$, $\alpha_v > 0$ za $v \in C$ tako da je $\sum_{v \in C} \alpha_v v = 0$. Tada je $(E, \mathcal{C}, *)$ orijentirani matroid. Drugim riječima, $C \in \mathcal{C}$ ako i samo ako je C skup vrhova nekog simpleksa kojemu je ishodište u unutrašnjosti i nije oblika $\{u, -u\}$.

Za orijentirani matroid $(E, \mathcal{C}, *)$, element $x \in E$ i podskup $X \subseteq E$, definiramo $\overline{x} = \{x, x^*\}$, $\overline{A} = \{\overline{x} | x \in A\}$, $\overline{\mathcal{C}} = \{\overline{C} | C \in \mathcal{C}\}$. Tada je familija $\overline{\mathcal{C}}$ podskupova od $\overline{E}$ skup ciklusa jednog matroida na $\overline{E}$.

S kombinatornog i računarskog stajališta važni su i matroidni algoritmi i veze sa strukturama podataka i složenost matroidnih algoritama. O matroidima također postoji opsežna literatura, npr. [197], [230], [15*] i [54*].

§ 3. Pólya-Redifieldova teorija

G. Pólya je 1937. razvio tehnike prebrojavanja objekata na koje djeluje neka grupa simetrija. Slične je ideje 1927. imao i J. H. Redfield, pa odatle i naziv te teorije. Pólya je prvenstveno imao u vidu primjene u kemiji. Osnovni je pojam te teorije izvjesna funkcija izvodnica $Z_G(x_1, x_2, \dots)$ koja će odražavati cikličku strukturu elemenata podgrupe G simetrične grupe S_n nekog n-članog skupa.

Neka je, dakle, $\pi \in S_n$ permutacija nekog n-članog skupa i neka je ona cikličkog tipa $(a_1, a_2, \dots, a_n)$; podsjetimo se da to znači da π ima a_i ciklusa duljine i, $i = 1, 2, \dots, n$ (vidi II§3). Njezina je **težina** prirodni broj $w = 1^{a_1} 2^{a_2} \dots n^{a_n}$.

Neka je sada G podgrupa grupe permutacija S_n n-članog skupa, a $g \in G$ neka ima ciklički tip $(a_1, a_2, \dots, a_n)$. Tada **ciklički indeks** od g definiramo kao monom (od njem. *Zyklenzeiger*):

$$Z(g; x_1, x_2, \dots, x_n) := x_1^{a_1} x_2^{a_2} \dots x_n^{a_n} = \prod_j x_j^{a_j},$$

a **ciklički indeks grupe**[4] G kao srednju vrijednost svih takvih monoma po svim $g \in G$, tj. kao polinom nad $\mathbb{Q}$

$$Z_G(x_1, x_2, \dots, x_n) := \frac{1}{|G|} \sum_{g \in G} Z(g; x_1, x_2, \dots, x_n).$$

Primjer 1. Odredite ciklički indeks čitave simetrične grupe S_n.

[4]Pojam cikličkog indeksa grupe uveo je njemački matematičar Georg Frobenius (1849–1917) u vezi s određivanjem ireducibilnih karaktera simetrične grupe.

Rješenje. Prema Propoziciji 5 u pogl. II, znamo da je broj permutacija u S_n cikličkog tipa $(a_1, a_2, \dots, a_n)$ jednak $n!/1^{a_1} a_1! 2^{a_2} a_2! \dots n^{a_n} a_n!$. Stoga je

$$Z_{S_n}(x_1, x_2, \dots, x_n) = \frac{1}{n!} \sum \frac{n!}{1^{a_1} a_1! \dots n^{a_n} a_n!} x_1^{a_1} \dots x_n^{a_n} = \sum \frac{1}{a_1! \dots a_n!} \left(\frac{x_1}{1}\right)^{a_1} \dots \left(\frac{x_n}{n}\right)^{a_n},$$

gdje se sumira po svim cjelobrojnim rješenjima $a_i \geq 0$ jednadžbe $1 \cdot a_1 + 2 \cdot a_2 + \dots + n \cdot a_n = n$, tj. po svim particijama od n. □

Primjer 2. Neka je $X = \{1, 2, 3, 4\}$ skup vrhova kvadrata, a G diedralna grupa svih (euklidskih) simetrija tog kvadrata koja tako djeluje na skupu X. Odredite ciklički indeks od G.

Rješenje. Grupa G (diedralna grupa D_4) sastoji se od rotacija (u pozitivnom smislu) za $0°, 90°, 180°$ i $270°$, horizontalne i vertikalne simetrije te dviju dijagonalnih simetrija. Sada se vidi (nacrtajte sliku) da rotacija za $0°$ (tj. identiteta) ima ciklički indeks x_1^4, rotacije za $90°$ ili $270°$ imaju ciklički indeks x_4, rotacija za $180°$ ima ciklički indeks x_2^2, horizontalna i vertikalna simetrija također x_2^2, a dijagonalne simetrije $x_1^2 x_2$. Npr., simetrija oko dijagonale 13 daje permutaciju vrhova (1)(3)(24), pa je stoga njezin ciklički indeks $x_1^2 x_2$. Stoga je

$$Z_G(x_1, x_2, x_3, x_4) = \frac{1}{8}(x_1^4 + 2x_1^2 x_2 + 3x_2^2 + 2x_4).$$

□

Funkciju f iz konačnog skupa X u skup "boja" (ili "kolora") $C = \{c_1, c_2, \dots\}$ zamišljamo kao "bojenje" skupa X tako da $x \in X$ obojimo s $f(x)$. Skup C^X je onda skup svih bojenja od X s bojama iz C. Neka je $G \leq S(X)$, tj. G je podgrupa grupe permutacija od X. Ako je $|X| = n$, onda je $S(X) \approx S_n$. Kazat ćemo da su dva bojenja $f, g : X \to C$ **G-ekvivalentna** (ili da ih ne razlikujemo) **s obzirom na grupu** G ako postoji permutacija $\pi \in G$ tako da je $g = f \circ \pi$. Pišemo tada $f \sim_G g$. Jasno je da je to relacija ekvivalencije. Neka je C^X/G skup klasâ ekvivalencije s obzirom na $\sim_G$. Svaki element tog kvocijentnog skupa zove se **uzorak** (s obzirom na grupu G).

Uvedimo sada sljedeće nazive. Neka je G bilo koja (konačna) grupa, a X bilo koji (konačni) skup. **Djelovanje grupe** G na skup X je homomorfizam $G \to S(X)$, $g \mapsto g \cdot x$. Skup $Gx := \{g \cdot x | g \in G\}$ zove se **G-orbita** od x, skup $G_x = \{g \in G | g \cdot x = x\}$ zove se **stabilizator** od x, a skup $\mathrm{Fix}(g) := \{x \in X | g \cdot x = x\}$, tj. skup točaka fiksnih za g se zove **permutacijski karakter** od g. Skup svih orbita $\{Gx | x \in X\}$ djelovanja grupe G na X označavamo s X/G. Uočite da je stabilizator G_x podgrupa od G.

Vratimo se u gornju situaciju gdje smo imali $G \leq S(X)$ i samim tim imamo inkluziju $G \hookrightarrow S(X)$ kao djelovanje grupe G na X. To onda daje i prirodno djelovanje grupe G na skup C^X. Naime, ako je $\pi \in G$, a $f \in C^X$, onda je za $x \in X$ to djelovanje dano s

$$(\pi \cdot f)(x) = f(\pi \cdot x).$$

Tada je C^X/G skup orbita toga djelovanja grupe G. Dakle, uzorak je jedna orbita tog djelovanja. Dva su bojenja (preslikavanja) $X \to C$ G-ekvivalentna ako pripadaju istoj G-orbiti iz C^X/G. Osnovni problem Pólya-Redfieldove teorije jest u tome da se za zadane X, C i G nađe broj uzoraka.

Neka je $C = \{c_1, c_2, \dots\}$ skup "boja", a $f : X \to C$ funkcija (tj. "bojenje") od X, gdje $x \in X$ "obojimo" bojom $f(x)$. Definiramo **težinu** x^f od $f \in C^X$ s

$$x^f := \prod_{i \geq 1} x_i^{\#f^{-1}(c_i)} .$$

Drugim riječima, x^f je monom stupnja $n = \#X$ u varijablama $x_1, x_2, \dots$, koji nam kaže za svako i koliko je elemenata iz X obojeno bojom c_i. Ekvivalentna preslikavanja (bojenja) imaju istu težinu, tj. $f \sim_G g \Rightarrow x^f = x^g$. Naime, ako je $g = f \circ \pi$, za neko $\pi \in G$, onda $\#g^{-1}(c_i) = \#(f \circ \pi)^{-1}(c_i) = \#\pi^{-1} f^{-1}(c_i) = \#f^{-1}(c_i)$, pa je $x^f = x^g$.

Stoga ako je $\mathcal{O} \in C^X/G$ neka orbita, tj. uzorak, onda definiramo **težinu uzorka** $\mathcal{O}$ kao

$$x^{\mathcal{O}} = x^f,$$

za bilo koji $f \in \mathcal{O}$. **Inventar uzoraka** od C^X/G je funkcija izvodnica

$$F_G(x_1, x_2, \dots) := \sum_{\mathcal{O} \in C^X/G} x^{\mathcal{O}}.$$

Dakle, inventar uzoraka F_G je suma monoma po svim uzorcima. Koeficijent monoma x^α u F_G je broj orbita težine x^α, gdje je $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots$ za $\alpha = (\alpha_1, \alpha_2, \dots)$.

Osnovni teorem Pólya-Redfieldove teorije je sljedeći.

TEOREM 1 (G. Pólya, 1937.). *Neka je X konačni skup, a G bilo koja podgrupa od $S(X)$. Tada je*

$$F_G(x_1, x_2, \dots) = Z_G(\sum_i x_i, \sum_i x_i^2, \sum_i x_i^3, \dots).$$

Posebno, ako su sve težine jednake 1, tj. ako je $x_1 = x_2 = \dots = 1$, a broj boja jednak r (tj. $|C| = r$), onda je ukupni broj uzoraka jednak $Z_G(r, r, r, \dots)$.

Prije dokaza teorema pogledajmo jednostavan ali poučan primjer.

Primjer 3. Neka je kao u Primjeru 2 $X = \{1, 2, 3, 4\}$ skup vrhova kvadrata, $C = \{c, p\}$ skup od dviju boja: crvene (c) i plave (p), a G diedralna grupa. Odredite inventar uzoraka, ukupni broj uzoraka i same uzorke.

Rješenje. Dva bojenja vrhova kvadrata su ekvivalentna ako postoji simetrija kvadrata koja prevodi jedno bojenje u drugo. Ako u formulu za Z_G iz Primjera 2

$$Z_G(x_1, x_2, x_3, x_4) = \frac{1}{8}(x_1^4 + 2x_1^2 x_2 + 3x_2^2 + 2x_4)$$

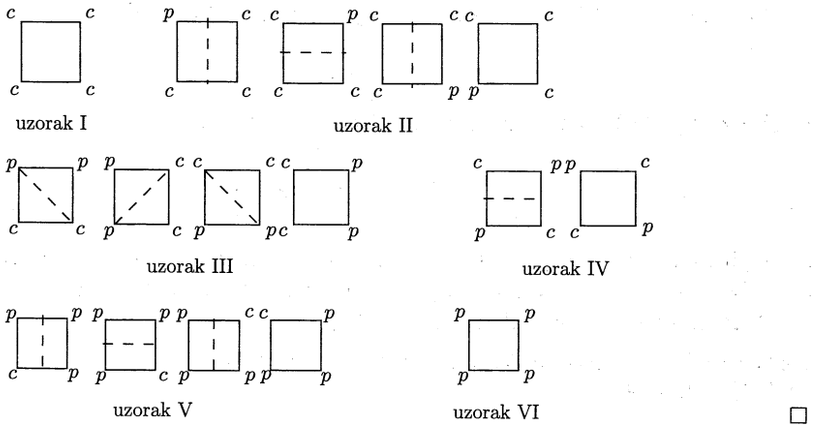
uvrstimo $x_1 = c + p$, $x_2 = c^2 + p^2$, $x_3 = c^3 + p^3$, $x_4 = c^4 + p^4$, dobivamo da je inventar uzoraka prema Pólyinom teoremu tada jednak

$$\begin{aligned} F_G(c, p) &= \frac{1}{8}[(c+p)^4 + 2(c+p)^2(c^2+p^2) + 3(c^2+p^2)^2 + 2(c^4+p^4)] = \\ &= c^4 + c^3 p + 2c^2 p^2 + c p^3 + p^4. \end{aligned}$$

To znači da imamo jedan uzorak u kojem su 4 vrha obojena crveno, jedan uzorak u kojem su 3 crvena i 1 plavi vrh, dva uzorka s 2 crvena i 2 plava vrha, jedan uzorak s jednim crvenim i 3 plava vrha i jedan uzorak s 4 plava vrha. Stavimo li u Z_G da je $r = 2$ dobivamo da je ukupni broj uzoraka jednak

$$Z_G(2, 2, 2, 2) = \frac{1}{8}(2^4 + 2 \cdot 2^2 \cdot 2 + 3 \cdot 2^2 + 2 \cdot 2) = 6.$$

Na idućoj je slici pokazano kako svih $2^4 = 16$ bojenja svrstavamo u 6 uzoraka. Unutar svakog uzorka zrcaljenje bojenja s naznačenom osi simetrije kvadrata daje odmah desno (ekvivalentno) bojenje. (Valja također zamijetiti da dva bojenja mogu biti ekvivalentna i s više nego jednom simetrijom; npr. drugo bojenje u uzorku IV također se dobiva rotacijom za 90° od prvoga.)



□

Sada prijeđimo na dokaz teorema. U tu nam svrhu prvo treba fundamentalni rezultat poznat kao Burnsideova lema.

LEMA (Burnside). *Neka je Y konačni skup, a $G \leq S(Y)$ podgrupa grupe permutacija od Y. Za $\pi \in G$ je $\mathrm{Fix}(\pi) = \{y \in Y | \pi(y = y)\}$ skup svih fiksnih točaka permutacije π. Neka je Y/G skup svih G-orbita djelovanja $G \hookrightarrow S(Y)$. Tada je*

$$\#(Y/G) = \frac{1}{\#G} \sum_{\pi \in G} \#\,\mathrm{Fix}(\pi).$$

Drugim riječima, broj orbita je jednak prosječnom broju fiksnih točaka svih permutacija iz G.

Dokaz leme. Za $y \in Y$, neka je $G_y = \{\pi \in G | \pi(y) = y\} \leq G$ stabilizator od y. Tada imamo

$$\begin{aligned} \frac{1}{\#G} \sum_{\pi \in G} \#\,\mathrm{Fix}(\pi) &= \frac{1}{\#G} \sum_{\pi \in G} \sum_{\substack{y \in Y \\ \pi(y) = y}} 1 = \\ &= \frac{1}{\#G} \sum_{y \in Y} \sum_{\substack{\pi \in G \\ \pi(y) = y}} 1 = \frac{1}{\#G} \sum_{y \in Y} \#G_y. \end{aligned}$$

Orbita Gy sastoji se od različitih elemenata $\pi(y)$, $\pi \in G$. Zbog $\pi'(y) = \pi(y) \iff \pi^{-1}\pi'(y) = y \iff \pi^{-1}\pi' \in G_y \iff \pi' G_y = \pi G_y$, slijedi da različiti elementi $\pi(y)$ definiraju različite (lijeve) susjedne klase πG_y u G, i obratno. Stoga su i njihovi brojevi elemenata jednaki, pa je

$$\#Gy = \frac{\#G}{\#G_y}.$$

Nastavljajući gornji račun, stoga dobivamo

$$\frac{1}{\#G}\sum_{\pi\in G} \#\operatorname{Fix}(\pi) = \frac{1}{\#G}\sum_{y\in Y}\frac{\#G}{\#Gy} = \sum_{y\in Y}\frac{1}{\#Gy}.$$

Za čvrstu orbitu $\mathcal{O} \in Y/G$ je očito $Gy = \mathcal{O} \iff y \in \mathcal{O}$. Stoga se u posljednjoj sumi član $1/\#\mathcal{O}$ javlja točno $\#\mathcal{O}$ puta. Zato je ta suma jednaka broju orbita. □

Ova se važna lema rabi u raznim problemima prebrojavanja, a u nekom se obliku ona već javlja u radovima Cauchyja i Frobeniusa.

Primjer 4. Na koliko (bitno različitih) načina n ljudi može sjesti oko okruglog stola?

Rješenje. Znamo da je odgovor $(n-1)!$ (usp. pogl. II, Primjer 22), ali ga sada izvedimo s Burnsideovom lemom. Problem je očito ekvivalentan sljedećem. Na koliko načina možemo vrhove pravilnog n-terokuta obojiti sa svih n boja, pri čemu dva bojenja ne razlikujemo ako jedno iz drugog dobijemo rotacijom n-terokuta? Na skupu Y svih bojenja vrhova n-terokuta (očito $\#Y = n!$) djeluje ciklička grupa $G \approx \mathbb{Z}_n$ permutacija generirana s rotacijom oko središta n-terokuta za kut $2\pi/n$. Naš je problem odrediti broj orbita $\#(Y/G)$. Za $\pi \in G$, $\pi \neq \mathrm{id}$, očito je $\operatorname{Fix}(\pi) = \emptyset$, dok je $\#\operatorname{Fix}(\mathrm{id}) = n!$. Iz Burnsideove leme tada slijedi

$$\#(Y/G) = \frac{n!}{n} = (n-1)!.$$

□

Dokaz Teorema. Neka je $\alpha = (\alpha_1, \alpha_2, \dots)$ slabi rastav od $n = \#X$, a $\mathcal{C}_\alpha$ skup svih "bojenja" $f \in C^X$ u kojima je boja c_j rabljena točno α_j puta, tj. $\#f^{-1}(c_j) = \alpha_j$, $\forall j$. Tada je skup $\mathcal{C}_\alpha$ invarijantan s obzirom na djelovanje grupe G na C^X, jer za $\pi \in G$ i $f \in \mathcal{C}_\alpha$ je $\pi \cdot f$ bojenje od X i vrijedi $\#(\pi \cdot f)^{-1}(c_j) = \#f^{-1}(c_j) = \alpha_j$, pa je $\pi \cdot f \in \mathcal{C}_\alpha$. Neka je π_α pripadno djelovanje od π na $\mathcal{C}_\alpha$. Da primijenimo Burnsideovu lemu i nađemo broj orbita, prvo treba izračunati $\#\operatorname{Fix}(\pi_\alpha)$.

Neka je π cikličkog tipa $(a_1, a_2, \dots, a_n)$. Ako je $f \in \operatorname{Fix}(\pi_\alpha)$, onda bojenje f ima svojstvo da su na svakom ciklusu od π svi njegovi elementi obojeni istom bojom (tj. f je konstantno na svakom ciklusu od π) i svaka boja c_j se ukupno pojavljuje α_j puta (tj. $\#f^{-1}(c_j) = \alpha_j$, $\forall j$). Iz definicije inventara uzoraka slijedi (izvedite to) da je

$$\#\operatorname{Fix}(\pi_\alpha) = \langle x^\alpha \rangle \prod_j (\sum_i x_i^j)^{a_j} = \langle x^\alpha \rangle Z(\pi; \sum x_i, \sum x_i^2, \dots).$$

Stoga je

$$Z(\pi; \sum x_i, \sum x_i^2, \dots) = \sum_\alpha \#\operatorname{Fix}(\pi_\alpha) x^\alpha.$$

Ako ovo sumiramo po svim $\pi \in G$ i podijelimo s $\#G$, onda na lijevoj strani dobivamo $Z_G(\sum x_i, \sum x_i^2, \dots)$, a prema Burnsideovoj lemi na desnoj strani $F_G(x_1, x_2, \dots)$. □

Dakle, inventar uzoraka (a time i broj uzoraka) računa se s cikličkim indeksom grupe. Stoga je poželjno da na raspolaganju imamo što više raznih pravila za računanje cikličkih indeksa grupe. Jedno od osnovnih pravila je sljedeće.

PROPOZICIJA 1 (Pravilo produkta za cikličke indekse). *Neka su X, Y disjunktni konačni skupovi, a $G \leq S(X)$, $H \leq S(Y)$. Tada direktni produkt $G \times H$ djeluje kao grupa permutacija od $X \cup Y$ kao $(\sigma, \tau)(x) = \sigma(x)$, za $x \in X$ i $(\sigma, \tau)(y) = \tau(y)$ za $y \in Y$. Vrijedi $Z_{G\times H} = Z_G Z_H$.*

Dokaz. Neka je npr. $n = \#X \geq m = \#Y$ i neka su redom $(a_1, \dots, a_n)$, $(b_1, \dots, b_n)$ ciklički tipovi od $\sigma \in G$ i $\tau \in H$. Tada je (σ, τ) cikličkog tipa $(a_1 + b_1, a_2 + b_2, \dots, a_m + b_m, a_m, a_{m+2}, \dots, a_n, 0, \dots, 0)$ i tada iz definicije cikličkog indeksa lako slijedi tvrdnja. □

Pokažimo sada primjerom da izomorfne grupe ne moraju imati isti ciklički indeks.

Primjer 5. Neka je $X = \{1, 2, 3, 4\}$ skup vrhova romba, grupa $G \leq S(X)$ neka je $G = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$, $\sigma_1 = \mathrm{id}$, $\sigma_2 = (12)$, $\sigma_3 = (34)$, $\sigma_4 = (12)(34)$, a $Y = \{1', 2', 3', 4'\}$ i $H = \{\tau_1, \tau_2, \tau_3, \tau_4\} \leq S(Y)$, $\tau_1 = \mathrm{id}$, $\tau_2 = (1'2')$, $\tau_3 = (1'3')(2'4')$, $\tau_4 = (1'4')(2'3')$. Dokažite da je $G \approx H$, ali $Z_G \neq Z_H$.

Rješenje. Permutacija σ_1 ima 4 ciklusa duljine 1, pa joj je doprinos x_1^4, a σ_2 i σ_3 imaju dva ciklusa duljine 1 i jedan ciklus duljine 2, pa je njihov doprinos $2x_1^2x_2$, a doprinos od σ_4 je x_2^2. Stoga je

$$Z_G(x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + 2x_1^2x_2 + x_2^2).$$

Slično se vidi da je

$$Z_H(x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + 3x_2^2).$$

S druge strane, $\sigma_i \mapsto \tau_i$, $i = 1, 2, 3, 4$ jedan je izomorfizam grupe G u grupu H. Obje su grupe izomorfne **Kleinovoj četvornoj grupi** $\mathbb{Z}_2 \times \mathbb{Z}_2$. □

Dvije su grupe $G \leq S(X)$ i $H \leq S(Y)$ **permutacijski izomorfne** ako postoji bijekcija $f : X \to Y$ i izomorfizam $\varphi : G \to H$ tako da je $f \circ \sigma = \varphi(\sigma) \circ f$, $\forall \sigma \in G$. Lako se vidi da permutacijski izomorfne grupe imaju jednake cikličke indekse.

Primjer 6. Neka je $X = [n]$, a $\sigma = (12 \dots n)$ ciklička permutacija od $[n]$ i neka je $G = \langle \sigma \rangle$ ciklička grupa reda n generirana sa σ. Dokažite da je

$$Z_G(x_1, \dots, x_n) = \frac{1}{n}\sum_{d|n} \varphi(d) x_d^{n/d},$$

gdje je $\varphi(r) = \#\{k \in [r] | n.z.m.(k, r) = 1\}$ Eulerova funkcija.

Rješenje. Prvo ciklički tip svakog elementa $\sigma^k \in G$ je uređena n-torka u kojoj je samo jedna komponenta različita od nule. Stoga su joj svi ciklusi iste duljine, pa su zato djelitelji od n (laganu provjeru ove činjenice prepuštamo čitatelju). Neka je $\tau \in G$ reda d. Odatle slijedi da se τ sastoji od n/d ciklusa duljine d, pa je zato

$$Z(\tau; x_1, x_2, \ldots, x_n) = x_d^{n/d}.$$

No, za svaki djelitelj $d|n$, grupa G sadrži točno $\varphi(d)$ elemenata reda d, pa zbrajanjem ovih jednakosti po $d|n$ i dijeljenjem s $|G| = n$ tvrdnja slijedi.

Tako, primjerice za $n = 4$ imamo grupu $G = \langle(1234)\rangle = \{\mathrm{id}, (1234), (13)(24), (1432)\}$ i iz gornje formule nalazimo

$$Z_G(x_1, x_2, x_3, x_4) = \frac{1}{4}(x_1^4 + x_2^2 + 2x_4).$$

□

Primjer 7. Odredite ciklički indeks **diedralne grupe** D_n reda $2n$ svih izometrija (simetrija) koje prevode pravilni n-terokut u samog sebe.

Rješenje. Grupa D_n se sastoji od podgrupe $G = \langle\sigma\rangle$ generirane s rotacijom σ za kut $2\pi/n$ oko središta n-terokuta i svih zrcaljenja. No ova podgrupa G je točno grupa iz prethodnog primjera, pa je njezin ukupni doprinos

$$P = \sum_{d|n} \varphi(d) x_d^{n/d}.$$

Da izračunamo doprinos zrcaljenja, razlikujemo slučajeve kada je n paran i n neparan. Ako je n paran, $n = 2m$, neka je ρ permutacija vrhova dobivena zrcaljenjem na pravac koji spaja polovišta bridova $\overline{m, m+1}$ i $\overline{1, 2m}$. Tada je $\rho\sigma$ permutacija vrhova inducirana zrcaljenjem oko pravca koji spaja vrhove m i $2m$, $\rho\sigma^2$ zrcaljenje od spojnica polovišta $\overline{m-1, m}$ i $\overline{2m-1, 2m}$ itd. vidimo da se os zrcaljenja rotira za $2\pi/4m$. Stoga je za $n = 2m$ $D_{2m} = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{2m}, \tau, \tau\sigma, \tau\sigma^2, \ldots, \tau\sigma^{2m}\}$. Prema tome, za n paran imamo $n/2$ zrcaljenja cikličkog tipa $(0, n/2, 0, \ldots, 0)$ (bez fiksnih točaka) i $n/2$ zrcaljenja cikličkog tipa $(2, (n-2)/2, 0, \ldots, 0)$ (dvije fiksne točke). Njihov doprinos cikličkom indeksu je

$$\mathbb{Q}_0 = \frac{n}{2}(x_2^{n/2} + x_1^2 x_2^{(n-2)/2}).$$

Za n neparan imamo n zrcaljenja cikličkog tipa $(1, (n-1)/2, 0, \ldots, 0)$ koja doprinose cikličkom indeksu

$$Q_1 = n x_1 x_2^{(n-1)/2}.$$

Konačno dobivamo

$$Z_{D_n}(x_1, \ldots, x_n) = \begin{cases} \frac{1}{2n}(P + Q_0) & , \text{ za } n \text{ paran} \\ \frac{1}{2n}(P + Q_1) & , \text{ za } n \text{ neparan} \end{cases}.$$

□

Sada jedan "konkretan" problem o **broju ogrlica**.

Primjer 8. Imamo 9 perli od kojih su 2 crvene (c), 3 bijele (b) i 4 plave (p). Koliko se ukupno ogrlica može načiniti od tih perli, pri čemu ih sve koristimo, a dvije ogrlice smatramo jednakim ako jednu iz druge dobivamo rotacijom ili zrcaljenjem?

Rješenje. Ako uzimamo u obzir samo rotacije, onda na perle djeluje ciklička grupa $\mathbb{Z}_9$, pa iz Primjera 4 dobivamo

$$Z_{\mathbb{Z}_9}(x_1, x_2, \ldots, x_9) = \frac{1}{9}(x_1^9 + 2x_3^3 + 6x_9).$$

Iz Pólyinog teorema dobivamo da je inventar uzoraka jednak

$$F_{\mathbb{Z}_9}(c, b, p) = \frac{1}{9}[(c+b+p)^9 + 2(c^3+b^3+p^3)^3 + 6(c^9+b^9+p^9)].$$

Ako na ogrlice djeluju samo rotacije, onda je njihov broj jednak

$$\langle c^2 b^3 p^4 \rangle F_{\mathbb{Z}_9} = \frac{1}{9}\left(\frac{9!}{2!3!4!} + 0 + 0\right) = 140.$$

No, budući da ogrlice ne razlikujemo i zbog zrcaljenja, onda na perle djeluje diedralna grupa D_9. Iz Primjera 5 dobivamo

$$Z_{D_9}(x_1, \ldots, x_9) = \frac{1}{18}(x_1^9 + 2x_3^3 + 6x_9 + 9x_1 x_2^4),$$

a odavde i iz Pólyinog teorema da je inventar uzoraka

$$F_{D_9}(c, b, p) = \frac{1}{2}F_{\mathbb{Z}_9} + \frac{1}{2}(c+b+p)(c^2+b^2+p^2)^4.$$

Stoga je traženi broj jednak

$$\langle c^2 b^3 p^4 \rangle F_{D_9} = \frac{1}{2} \cdot 140 + \frac{1}{2}(0 + \frac{4!}{1!1!2!} + 0) = 76.$$

(Pokušajte s ovom teorijom riješiti Primjer 14 u pogl. IV.) □

Sljedeća dva primjera su iz kemije. Već smo kazali da su prebrojavanja u kemiji i bila jedan od motiva Pólyae da razvije ovu teoriju.

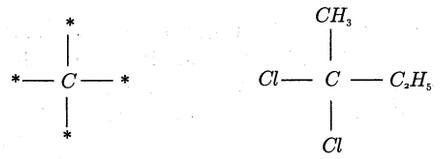
Primjer 9. Benzenoidni prsten je graf koji predstavlja ugljikovodik benzena C_6H_6 i sastoji se od pravilnog 6-terokuta u čijem je svakom vrhu jedna grupa spojeva tipa CH. Ako se svakom vrhu mogu privjesiti dvije vrste radikala, odredite broj različitih spojeva koji se mogu dobiti iz benzenoidnog prstena.

Rješenje. Kao grupa simetrija na vrhove 6-terokuta ovdje očito djeluje diedralna grupa D_6. Iz Primjera 7 dobivamo da je ciklički indeks

$$Z_{D_6} = \frac{1}{12}(x_1^6 + 3x_1^2 x_2^2 + 4x_2^3 + 2x_6).$$

Iz Pólyinog teorema slijedi da je traženi broj jednak $Z_{D_6}(2, 2, 2, 2, 2, 2) = 13$. □

Primjer 10. Na donjoj je slici a) tip molekule s atomom ugljika C u sredini, a na mjestima $*$ mogu doći CH_3 (metil), C_2H_5 (etil), H vodik i Cl (klor). Npr. na slici b) je diklorbutan. Koliko ima takvih molekula? Koliko je takvih spojeva s 0, 1, 2, 3, 4 atoma H?



a)

b)

Rješenje. Matematički model takvih molekula je pravilni tetraedar u čijem je središtu atom ugljika, a na skupu vrhova $X = \{1,2,3,4\}$ gledamo funkcije $f : X \to \{H, Cl, CH_3, C_2H_5\}$. Neka je G grupa permutacija vrhova dobivenih rotacijskim simetrijama tetraedra. Grupa G se sastoji od a) identitet; b) 8 rotacija za 120° oko spojnica vrhova i središta tetraedra; c) 3 rotacije za 180° oko spojnica polovišta nasuprotnih bridova. Tako npr. (nacrtajte sliku) ako tetraedar rotiramo oko spojnice vrha 1 i središta za +120° i −120° dobivamo permutacije (1)(234) i (1)(243), a ako ga rotiramo oko polovišta bridova $\overline{12}$ i $\overline{34}$ za 180° dobivamo permutaciju (12)(34). Odatle dobivamo ciklički indeks za grupu G tetraedra, $|G| = 12$:

$$Z_G(x_1,x_2,x_3,x_4) = \frac{1}{12}(x_1^4 + 8x_1x_3 + 3x_2^2).$$

Traženi je broj jednak broju G-neekvivalentnih funkcija, tj. ukupni broj uzoraka, a taj dobijemo tako da stavimo da su sve težine 1, tj. to je broj $Z_G(4,4,4,4) = 36$.

Ako želimo naći broj molekula u kojima nema atoma H, onda uzmemo da su težine od CH_3, C_2H_5, Cl jednake 1, a od H jednaka 0, pa je taj broj $Z_G(3,3,3,0) = 15$. Za klasifikaciju ostalih 21 molekula uzmimo da su težine od CH_3, C_2H_5 i Cl jedinice, a od vodika H. Tada je

$$Z_G(H+3, H^2+3, H^3+3, H^4+3) = H^4 + 3H^3 + 6H^2 + 11H + 15,$$

odakle čitamo koeficijente, pa imamo jednu molekulu CH_4 (metan), 3 molekule s 3 atoma H, 6 molekula s 2 atoma H, 11 molekula s jednim H i 15 molekula bez atoma H. □

Primjer 11. Odredite cikličke indekse na skupu vrhova svakog od pet pravilnih poliedara (“**Platonovih tijela**”) pod djelovanjem grupe simetrije koja ga prevodi u sama sebe.

Rješenje. Za tetraedar T smo u prethodnom primjeru našli Z_T. Za kocku K s vrhovima $1,2,\ldots,8$, osim identitete (i pripadnim članom x_1^8) imamo (crtajte) a) rotacije oko spojnica središta nasuprotnih strana s doprinosom $3x_2^4$, b) rotacijama oko osi kao u a) za $\pm 90°$ s doprinosom $6x_4^2$, c) rotacijama za 180° oko spojnica polovišta nasuprotnih bridova s doprinosom $6x_2^4$, d) rotacijama za $\pm 120°$ oko dijagonala s doprinosom $8x_1^2x_3^2$. Tako dobivamo (red grupe rotacija kocke je $1+3+3+3+6+4+4 = 24$):

$$Z_K(x_1,x_2\ldots,x_8) = \frac{1}{24}(x_1^8 + 9x_2^4 + 8x_1^2x_3^2 + 6x_4^2).$$

Oktaedar O i kocka su geometrijski duali u smislu da vrhove oktaedra možemo zamišljati da leže u središtima strana kocke i dva vrha spojena bridom ako i samo ako su pripadne strane kocke incidentne. Na taj način vrhovi oktaedra odgovaraju stranama kocke, pa je ciklički indeks oktaedra jednak cikličkom indeksu simetrija kocke koje prevode strane u strane. Sličnim razmatranjima kao za vršne simetrije dobivamo

$$Z_O(x_1,x_2,\ldots,x_6) = \frac{1}{24}(x_1^6 + 3x_1^2x_2^2 + 6x_2^3 + 6x_1^2x_4 + 8x_3^2).$$

Za ikozaedar I (12 vrhova, 30 bridova, 20 strana-trokuta, u svakom vrhu 5 trokuta) imamo osim id, rotacije za 72°, 144°, 216° i 288° oko spojnica antipodalnih vrhova, ukupno takvih 24, zatim 20 simetrija oko spojnica središta nasuprotnih strana za $\pm 120°$ i 15 simetrija oko spojnica polovišta nasuprotnih bridova za 180°. Ukupno imamo $1+24+20+15 = 60$ simetrija. Dobiva se

$$Z_I(x_1,x_2,\ldots,x_{12}) = \frac{1}{60}(x_1^{12} + 15x_2^6 + 20x_3^4 + 24x_1^2x_5^2).$$

Dodekaedar D je geometrijski dual ikozaedra i ima 20 vrhova i 12 strana - peterokuta. Stoga je dovoljno promatrati simetrije strana ikozaedra. Slično kao gore dobiva se

$$Z_D(x_1,x_2,\ldots,x_{20}) = \frac{1}{60}(x_1^{20} + 15x_2^{10} + 20x_1^2x_3^6 + 24x_5^4).$$

Tako primjerice ukupni broj (neekvivalentnih) bojenja vrhova dodekaedra dvjema bojama iznosi $Z_D(2,2,\ldots,2) = 17824$. □

Jedna od važnih primjena Pólya-Redfieldove teorije je u prebrojavanju grafova (do na izomorfizam). Naime, na graf sa skupom vrhova $V = \{1,2,\ldots,n\}$ i skupom bridova E možemo gledati i kao funkciju $f : \binom{V}{2} \to \{0,1\}$ koja dvočlanom skupu $\{i,j\}$ pridruži 1 ili 0 već prema tome je li $\{i,j\} \in E$ ili $\notin E$. Dva grafa sa skupom vrhova V su izomorfna ako postoji permutacija vrhova koja čuva susjednost vrhova. Dakle, na V djeluje S_n i to inducira prirodno djelovanje na $\binom{V}{2}$ ovako: za $\{i,j\} \in \binom{V}{2}$ je $\pi\{i,j\} = \{\pi i, \pi j\}$. Tako imamo podgrupu $S_n \approx G \subset S(\binom{V}{2}) \approx S_{\binom{n}{2}}$ koja je izomorfna sa S_n, ali joj nije permutacijski izomorfna (osim za $n = 2$). Ona se označava s $S_n^{(2)}$ i zove **dvojna grupa**. Iz Pólyinog teorema sada nije teško dokazati ovo.

TEOREM. *Funkcija izvodnica za brojeve (neoznačenih) jednostavnih grafova s n vrhova je jednaka*

$$G_n(x) = Z_{S_n^{(2)}}(1+x, 1+x^2, \ldots, 1+x^n).$$

Koeficijent $\langle x^m\rangle G_n(x)$ jednak je broju grafova s n vrhova i m bridova, a ukupni broj grafova s n vrhova $G_n(1) =: g_n$.

Između ostalog, ovo može poslužiti za razna konkretna računanja (npr. pokušajte se uvjeriti da je $g_4 = 11$ i $g_5 = 34$), razne asimptotike kao npr. $g_n \sim \frac{1}{n!}2^{\binom{n}{2}}$ itd. No, u to se nećemo upuštati.

Spomenimo da je oko 1960. N. G. de Bruijn poopćio ovu teoriju u raznim smjerovima, ponajprije promatrajući težinske verzije navedenih pojmova Pólya-Redfieldove teorije. Također treba spomenuti da je ciklički indeks u koji uvrštavamo sume, sume kvadrata itd. kao u osnovnom Pólyinom teoremu simetrična funkcija (vidi idući paragraf), pa se razna svojstva cikličkog indeksa mogu proučavati sa stajališta teorije simetričnih funkcija. Čitatelja upućujemo na knjigu [180], kao i [3], [17], [51], [105], [186], [43*], [60*] i dr.

§ 4. Simetrične funkcije

Simetrične funkcije se odavno promatraju u raznim granama matematike jer obično odražavaju neko svojstvo simetrije promatranih objekata. To naročito dolazi do izražaja u kombinatorici, pa je proučavanje kombinatornih svojstava simetričnih funkcija od velike važnosti u kombinatorici. Podsjetimo da je polinom $f(x_1, x_2, \ldots, x_n)$ od n varijabli **simetrični polinom** ako je $f(x_1, x_2, \ldots, x_n) = f(x_{\pi(1)}, x_{\pi(2)}, \ldots, x_{\pi(n)})$ za svaku permutaciju $\pi \in S_n$. No, ovo je preuzak okvir, pa stoga imamo sljedeću općenitu definiciju.

Neka je $x = (x_1, x_2, \ldots)$ skup (komutirajućih) varijabli, a $n \geq 0$ cijeli broj. **Homogena simetrična funkcija** stupnja n nad komutativnim prstenom R (s jedinicom) formalni je red potencija

$$f(x) = \sum_{\alpha} c_\alpha x^\alpha,$$

gdje se sumira po svim slabim kompozicijama $\alpha = (\alpha_1, \alpha_2, \ldots)$ od n (bilo koje duljine), pri čemu su $c_\alpha \in R$, $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \ldots$, a $f(x_{\pi(1)}, x_{\pi(2)}, \ldots) = f(x_1, x_2, \ldots)$ za svaku permutaciju π skupa $\mathbb{N}$. (Simetrična funkcija stupnja 0 je naprosto element iz R.) Skup svih homogenih simetričnih funkcija stupnja n nad R označavamo s Λ_R^n. Najvažniji je slučaj $R = \mathbb{Q}$ i stavimo $\Lambda_{\mathbb{Q}}^n := \Lambda^n$. Očito je Λ^n vektorski prostor nad $\mathbb{Q}$. Nadalje, ako je $f \in \Lambda^m$, a $g \in \Lambda^n$, onda je $fg \in \Lambda^{m+n}$ (fg je produkt formalnih redova potencija). Stoga, definiramo li direktnu sumu vektorskih prostora

$$\Lambda := \Lambda^0 \oplus \Lambda^1 \oplus \Lambda^2 \oplus \ldots,$$

imamo da je element $f \in \Lambda$ formalni red potencija oblika $f = f_0 + f_1 + f_2 + \ldots$, gdje je $f_n \in \Lambda^n$ i svi $f_n = 0$ osim njih konačno mnogo. Na taj način Λ postaje $\mathbb{Q}$-algebra koja se zove **algebra simetričnih funkcija** (nad $\mathbb{Q}$). Ta je algebra komutativna i ima jedinični element $1 \in \Lambda^0$. Ta je algebra i graduirana, tj. $f \in \Lambda^m$, $g \in \Lambda^n \Rightarrow fg \in \Lambda^{m+n}$.

Osnovna tema teorije simetričnih funkcija jest iznalaženje raznih baza vektorskih prostora Λ^n i/ili Λ i proučavanje matrica prijelaza iz jedne u drugu bazu. Pritom obično članovi matrice prijelaza imaju neko kombinatorno značenje. U tom se smislu teorija simetričnih funkcija može shvatiti kao dio **algebarske kombinatorike** koja, grubo govoreći, proučava objekte koji imaju i algebarsko i kombinatorno značenje. Tipični je primjer kada veličinu nekog kombinatorno definiranog skupa možemo interpretirati kao dimenziju nekog vektorskog prostora. Tako je npr. i teorija matroida (vidi §2.) dio algebarske kombinatorike.

Raznim specijalizacijama vrijednosti varijabli, poglavito ako za $f \in \Lambda$ stavimo $x_{n+1} = x_{n+2} = \cdots = 0$, dobivamo simetričnu funkciju od n varijabli $f(x_1, \ldots, x_n) = f(x_1, \ldots, x_n, 0, 0, \ldots)$. Mi se ovdje nećemo upuštati detaljno u ovu fascinantnu teoriju, nego ćemo samo pokušati objasniti ključne pojmove, ideje i činjenice. "State of the Art" ove teorije najpotpunije je i detaljno prikazano u knjigama [152] i [65*].

Prvo se podsjetimo da je **particija** λ cijelog broja $n \geq 0$ niz $\lambda = (\lambda_1, \lambda_2, \ldots, \lambda_k) \in \mathbb{N}_0^k$ za koji je $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_k \geq 0$, a $\sum \lambda_i = n$. Svi nenul članovi λ_i

od λ zovu se **dijelovi** od λ. Članovi $\lambda_i = 0$ particije λ su nevažni, pa stoga λ možemo identificirati s beskonačnim nizom $(\lambda_1, \lambda_2, \ldots, \lambda_k, 0, 0, \ldots)$. Skup $\mathrm{Par}(n)$ je skup svih particija od n ($\mathrm{Par}(0)$ se sastoji od prazne particije $\emptyset$ ili $(0, 0, \ldots)$), a $\mathrm{Par} = \bigcup_{n \geq 0} \mathrm{Par}(n)$ je skup svih particija.

Za $\lambda \in \mathrm{Par}(n)$ još pišemo $\lambda \vdash n$ (ili $|\lambda| = n$), a broj dijelova od λ još zovemo **duljina** od λ i označavamo s $\ell(\lambda)$. Ako je $m_i = m_i(\lambda)$ broj dijelova od λ jednakih i, onda pišemo $\lambda = \langle 1^{m_1} 2^{m_2} \ldots \rangle$ ili još kraće $1^{m_1} 2^{m_2} \ldots$. Svakoj particiji $\lambda = (\lambda_1, \lambda_2, \ldots)$ pridružen je **Youngov** (ili **Ferrerov**) **dijagram** koji se sastoji od λ_1 kvadratića u prvom retku, λ_2 kvadratića u drugom retku itd. (usp. pogl. II §7).

Konjugirana (spregnuta) **particija** $\lambda' = (\lambda_1', \lambda_2', \ldots)$ od λ dobiva se transponiranjem Youngovog dijagrama od λ, ili ekvivalentno, $m_i(\lambda') = \lambda_i - \lambda_{i+1}$. Na skupu Par postoje tri prirodna parcijalna uređaja. Prvi je **inkluzija** $\lambda \subseteq \mu$ za $\lambda, \mu \in \mathrm{Par}$, što znači da je $\lambda_i \leq \mu_i$, $\forall i$ (tj. Youngov dijagram od λ je sadržan u Youngovom dijagramu od μ). **Dominacija** (ili **majorizacija**) $\leq$ je parcijalni uređaj na svakom $\mathrm{Par}(n)$, pri čemu za $\lambda, \mu \in \mathrm{Par}(n)$ definiramo da je $\lambda \leq \mu$, ako je $\lambda_1 + \lambda_2 + \cdots + \lambda_i \leq \mu_1 + \mu_2 + \cdots + \mu_i$, $\forall i$. **Reverzni (obrnuti) leksikografski uređaj** $\overset{R}{\leq}$ definira se za $|\lambda| = |\mu|$ kao $\mu \overset{R}{\leq} \lambda$ ako je ili $\lambda = \mu$ ili u protivnome za neko i vrijedi $\mu_1 = \lambda_1, \ldots, \mu_i = \lambda_i$, $\mu_{i+1} < \lambda_{i+1}$. **Rang particije** rang (λ) je najveći i za koji je $\lambda_i \geq i$.

Sada opišimo neke od najvažnijih baza vektorskog prostora Λ simetričnih funkcija. Za particiju $\lambda = (\lambda_1, \lambda_2, \ldots) \vdash n$ definiramo **monomijalnu simetričnu funkciju** $m_\lambda = m_\lambda(x) \in \Lambda^n$ formulom

$$m_\lambda = \sum_{\alpha} x^\alpha,$$

pri čemu sumiramo po svim permutacijama $\alpha = (\alpha_1, \alpha_2, \ldots)$ članova od $\lambda = (\lambda_1, \lambda_2, \ldots)$. Primjerice, $m_\emptyset = 1$, $m_1 = \sum_i x_i$, $m_2 = \sum_i x_i^2$, $m_{11} = \sum_{i<j} x_i x_j$, $m_{21} = \sum_{i \neq j} x_i^2 x_j$, $m_{221} = \sum_{i<j, i,j \neq k} x_i^2 x_j^2 x_k$ itd.

Ako je $f = \sum_\alpha c_\alpha x^\alpha \in \Lambda^n$, onda je $f = \sum_{\lambda \vdash n} c_\lambda m_\lambda$, pa je skup $\{m_\lambda | \lambda \vdash n\}$ baza vektorskog prostora Λ^n i dimenzija $\dim \Lambda^n = p(n) =$ broj particija od n. Skup $\{m_\lambda | \lambda \in \mathrm{Par}\}$ je baza od Λ.

Elementarna simetrična funkcija e_λ za $\lambda \in \mathrm{Par}$ definirana je kao

$$e_n = m_{1^n} = \sum_{i_1 < \cdots < i_n} x_{i_1} x_{i_2} \ldots x_{i_n}, n \geq 1, e_0 = m_\emptyset = 1,$$

$$e_\lambda = e_{\lambda_1} e_{\lambda_2} \ldots \text{ ako je } \lambda = (\lambda_1, \lambda_2, \ldots).$$

Primjerice, $e_1 = m_1, e_2 = m_{11}$, $e_3 = m_{111}$, ili $e_{11} = m_2 + 2m_{11}$, $e_{111} = m_3 + 3m_{21} + 6m_{111}$, $e_{21} = m_{21} + 3m_{111}$, $e_{22} = m_{22} + 2m_{211} + 6m_{1111}$, $e_{211} = m_{31} + 2m_{22} + 5m_{211} + 12m_{1111}$ itd.

Neka je $A = [a_{ij}]_{i,j \geq 1}$ cjelobrojna (beskonačna) matrica u kojoj je samo konačno članova $\neq 0$. Neka su $r_i := \sum_j a_{ij}$, $s_j := \sum_i a_{ij}$ redom sume i-tog retka, odn. j-tog stupca, a $\mathrm{red}(A) := (r_1, r_2, \ldots)$, $\mathrm{stup}(A) := (s_1, s_2, \ldots)$ vektori suma redaka odn. stupaca od A. Ako su članovi od A samo 0 ili 1, onda se A zove $(0,1)$-matrica.

PROPOZICIJA 1. *Neka je* $\lambda \vdash n$, *a* $\alpha = (\alpha_1, \alpha_2, \dots)$ *slaba kompozicija od* n. *Tada je koeficijent* $M_{\lambda\alpha}$ *od* x^α *u zapisu*

$$e_\lambda = \sum_{\lambda \vdash n} M_{\lambda\mu} m_\mu \ , \tag{1}$$

jednak broju $(0,1)$*-matrica* $A = [a_{ij}]_{i,j \geq 1}$ *sa svojstvom* $\mathrm{red}(A) = \lambda$, $\mathrm{stup}(A) = \alpha$.

Dokaz. Promotrimo matricu

$$X = \begin{bmatrix} x_1 & x_2 & x_3 & \dots \\ x_1 & x_2 & x_3 & \dots \\ \vdots & \vdots & \vdots & \end{bmatrix}.$$

Član iz e_λ dobijemo tako da odaberemo λ_1 članova iz prvog retka iz X, λ_2 iz drugog retka itd. Neka je produkt odabranih članova x^α. Ako proglasimo sve tako odabrane članove da su 1, a ostale 0, dobivamo $(0,1)$-matricu A s $\mathrm{red}(A) = \lambda$, $\mathrm{stup}(A) = \alpha$. Obrnuto, svaka takva matrica odgovara članu iz e_λ. Odavde slijedi tvrdnja. □

Ekvivalentna reformulacija Propozicije (1) ima sljedeće kombinatorno značenje.

PROPOZICIJA 2. *Neka su* $x = (x_1, x_2, \dots)$ *i* $y = (y_1, y_2, \dots)$ *dva skupa varijabli. Tada je*

$$\prod_{i,j}(1 + x_i y_i) = \sum_{\lambda,\mu} M_{\lambda,\mu} m_\lambda(x) m_\mu(y) = \sum_\lambda m_\lambda(x) e_\lambda(y), \tag{2}$$

pri čemu se sumira po $\lambda, \mu \in \mathrm{Par}$ *(a dovoljno je po* $|\lambda| = |\mu|$, *jer je inače* $M_{\lambda\mu} = 0$*).*

Dokaz. Nakon svih izvršenih množenja u $\prod(1 + x_i y_i)$, dobivamo da je to suma monoma $x_1^{\alpha_1} x_2^{\alpha_2} \dots y_1^{\beta_1} y_2^{\beta_2} \dots = x^\alpha y^\beta$. Taj monom dobijemo tako da odaberemo $(0,1)$-matricu $A = [a_{ij}]$ sa samo konačno mnogo jedinica za koju je $\prod_{i,j}(x_i y_j)^{a_{ij}} = x^\alpha y^\beta$. No očito je $\prod_{i,j}(x_i y_j)^{a_{ij}} = x^{\mathrm{red}(A)} y^{\mathrm{stup}(A)}$, pa je koeficijent uz $x^\alpha y^\beta$ u produktu $\prod(1 + x_i y_i)$ jednak broju $(0,1)$-matrica za koje je $\mathrm{red}(A) = \alpha$, $\mathrm{stup}(A) = \beta$, odakle slijedi prva jednakost u (2), a druga jednakost slijedi iz (1). □

TEOREM 1 (Osnovni teorem o simetričnim funkcijama). *Neka su* $\lambda, \mu \vdash n$. *Tada je* $M_{\lambda\mu} = 0$, *osim ako je* $\mu \leq \lambda'$, *a* $M_{\lambda\lambda'} = 1$. *Stoga je skup* $\{e_\lambda | \lambda \vdash n\}$ *baza prostora* Λ^n *(pa je* $\{e_\lambda | \lambda \in \mathrm{Par}\}$ *baza od* Λ*). Ekvivalentno,* $e_1, e_2, \dots$ *su algebarski nezavisni i generiraju* $\mathbb{Q}$*-algebru* Λ, *tj.* $\Lambda = \mathbb{Q}[e_1, e_2, \dots]$.

Dokaz. Ako je $M_{\lambda\mu} \neq 0$, onda zbog Propozicije 1 postoji $(0,1)$-matrica $A = [a_{ij}]$ za koju je $\mathrm{red}(A) = \lambda$, $\mathrm{stup}(A) = \mu$. Formirajmo $(0,1)$-matricu $A' = [a'_{ij}]$ za koju je $a'_{ij} = 1 \iff 1 \leq j \leq \lambda_i$, $\forall i$. Tada je $\mathrm{red}(A') = \lambda$. Za svako i je broj jedinica u prvih i stupaca od A veći ili jednak broju jedinica u prvih i stupaca od A, pa iz uređaja dominacije slijedi da je $\lambda' = \mathrm{stup}(A') \geq \mathrm{stup}(A) = \mu$, tj. $\lambda' \geq \mu$, što smo i tvrdili. Dalje, lako se vidi da je A' i jedina $(0,1)$-matrica sa svojstvom $\mathrm{red}(A') = \lambda$, $\mathrm{stup}(A') = \lambda'$, pa je $M_{\lambda\lambda'} = 1$. Odatle se lako vidi da je (u nekom poretku) matrica $[M_{\lambda\mu}]$ gornja trokutasta s jedinicama na glavnoj dijagonali, pa je invertibilna i zato je $\{e_\lambda | \lambda \vdash n\}$ baza od Λ^n, a odatle slijede ostale tvrdnje. □

KOROLAR 1. *Ako su* $M_{\lambda\mu}$ *kao u* (1), *onda je* $M_{\lambda\mu} = M_{\mu\lambda}$, *tj. matrica prijelaza među bazama* $\{m_\lambda | \lambda \vdash n\}$ *i* $\{e_\lambda | \lambda \vdash n\}$ *je simetrična.*

Dokaz. To odmah slijedi iz Propozicije 1 i Teorema 1 i činjenice da ako za $(0,1)$-matricu A vrijedi $\mathrm{red}(A) = \lambda$, $\mathrm{stup}(A) = \mu$, onda (i samo onda) za transponiranu matricu A^T vrijedi $\mathrm{red}(A^T) = \mu$ i $\mathrm{stup}(A^T) = \lambda$. □

Ako je $u = \{u_\lambda\}$ bilo koja baza od Λ, a $f = \sum_\lambda a_\lambda u_\lambda$ razvoj od f po bazi $\{u_\lambda\}$, onda ćemo reći da je f u**-pozitivan**, ako je $a_\lambda \geq 0$, $\forall \lambda$. U takvim slučajevima a_λ obično ima neko kombinatorno značenje (npr. dimenziju nekog vektorskog prostora itd.) Tako je npr. e_λ m-pozitivan zbog Propozicije 1. Često je veliko umijeće dokazati da je neki f u-pozitivan.

Neka je $\lambda \in \mathrm{Par}$. Tada definiramo **potpuno homogenu simetričnu funkciju** kao

$$\begin{aligned} h_n &= \sum_{\lambda \vdash n} m_\lambda = \sum_{i_1 \leq \dots \leq i_n} x_{i_1} x_{i_2} \dots x_{i_n}, n \geq 1, h_0 = m_0 = 1, \\ h_\lambda &= h_{\lambda_1} h_{\lambda_2} \dots \quad , \text{ ako je } \lambda = (\lambda_1, \lambda_2, \dots). \end{aligned} \tag{3}$$

h_n je očito suma svih monoma stupnja n. Analogon Propozicije 1 je sljedeći:

PROPOZICIJA 3. *Neka je* $\lambda \vdash n$, *a* $\alpha = (\alpha_1, \alpha_2, \dots)$ *slaba kompozicija od* n. *Tada je koeficijent* $N_{\lambda\alpha}$ *od* x^α *u* h_λ *u zapisu*

$$h_\lambda = \sum_{\lambda \vdash n} N_{\lambda\mu} m_\mu \ , \tag{4}$$

jednak broju $\mathbb{N}_0$ *matrica* $A = [a_{ij}]_{i,j \geq 1}$ *za koje je* $\mathrm{red}(A) = \lambda$, $\mathrm{stup}(A) = \alpha$.

Dokaz. Analogno dokazu Propozicije 1, član x^α iz $h_\lambda = h_{\lambda_1} h_{\lambda_2} \dots$ dobivamo odabirom člana $x_1^{a_{i1}} x_2^{a_{i2}} \dots$ iz svakog h_{λ_i} tako da je $\prod_i (x_1^{a_{i1}} x_2^{a_{i2}} \dots) = x^\alpha$. No ovaj je produkt isti kao i odabir $\mathbb{N}_0$-matrice $A = [a_{ij}]$ sa svojstvom $\mathrm{red}(A) = \lambda$, $\mathrm{stup}(A) = \alpha$. □

Primjerice, $h_1 = m_1$, $h_{11} = 2m_{11} + m_2$, $h_2 = m_{11} + m_2$, $h_{111} = 6m_{111} + 3m_{21} + m_3$, $h_{21} = 3m_{111} + 2m_{21} + m_3$, $h_{211} = 12m_{1111} + 7m_{211} + 4m_{22} + 3m_{31} + m_4$ itd.

Brojevi $M_{\lambda\mu}$ i $N_{\lambda\mu}$ iz Propozicija 1 i 3 mogu se i ovako kombinatorno protumačiti. Uzmimo da imamo λ_i kuglica označenih s i, a ukupno n (tj. $\lambda \vdash n$), a želimo ih pospremiti u kutije označene s 1, 2, ... Tada je $M_{\lambda\mu}$ broj načina da kuglice pospremimo u kutije tako da svaka kutija sadrži najviše jednu kuglicu svake oznake, a svaka kutija i sadrži točno μ_i kuglica. Broj $N_{\lambda\mu}$ je broj načina da se kuglice pospreme u kutije uz jedini uvjet da svaka kutija i sadrži točno μ_i kuglica.

S kombinatornog se stajališta, različitost i dualnost među e_λ i h_λ odražava kao različitost među $(0,1)$-matricama i $\mathbb{N}_0$-matricama, ili ekvivalentno stavljanje kuglica u kutije, pri čemu nema, odnosno ima, ponavljanja. To donekle podsjeća na recipročnost među $\binom{n}{k}$ i $\left(\!\binom{n}{k}\!\right) = (-1)^k \binom{-n}{k}$ iz pogl. II. I zaista, to se može ovako

protumačiti. Neka je $f(x)$ simetrična funkcija, a $n \in \mathbb{N}_0$.
Definirajmo

$$f(1^n) := f(x_1 = 1, \dots x_n = 1, x_{n+1} = 0, x_{n+2} = 0, \dots).$$

Tada je

$$e_k(1^n) = \sum_{1 \le i_1 < \dots < i_k \le n} 1 = \binom{n}{k},$$
$$h_k(1^n) = \sum_{1 \le i_1 \le \dots \le i_k \le n} 1 = \left(\!\binom{n}{k}\!\right) = \binom{n+k-1}{k}.$$

Možemo stoga reći da e_k i h_k odražavaju "recipročnost" među skupovima i multiskupovima. Sljedeći teorem daje puni algebarski smisao te recipročnosti.

Kako je Λ kao $\mathbb{Q}$-algebra generirana s $e_1, e_2, \dots$, tj. $\Lambda = \mathbb{Q}[e_1, e_2, \dots]$, slijedi da je homomorfizam algebri $f : \Lambda \to \Lambda$ potpuno određen s vrijednostima $f(e_n)$, $n \ge 1$. Definirajmo homomorfizam algebri $\omega : \Lambda \to \Lambda$ s $\omega(e_n) = h_n$, $n \ge 1$, pa stoga $\omega(e_\lambda) = h_\lambda$, $\forall \lambda \in \mathrm{Par}$.

TEOREM 2. *ω je involucija, tj. $\omega^2 = \mathrm{id}$, ili ekvivalentno $\omega(h_n) = e_n$ (i stoga $\omega(h_\lambda) = e_\lambda$, $\forall \lambda \in \mathrm{Par}$).*

Dokaz. Promotrimo formalne redove potencija (zapravo funkcije izvodnice za (h_n) i (e_n)):

$$H(t) := \sum_{n \ge 0} h_n t^n, \quad E(t) := \sum_{n \ge 0} e_n t^n \in \Lambda[[t]].$$

Iz definicije h_n i e_n lako se vidi da vrijedi

$$H(t) = \prod_n (1 - x_n t)^{-1}, \quad E(t) = \prod_n (1 + x_n t).$$

Odatle slijedi da je $H(t)E(-t) = 1$, pa uzimanjem koeficijenata uz x^n dobivamo za svaki $n \ge 1$:

$$\sum_{i=0}^{n} (-1)^i e_i h_{n-i} = 0. \tag{5}$$

I obrnuto, ako za neke $u_i \in \Lambda$, $u_0 = 1$ vrijedi $\sum_{i=0}^{n} (-1)^i u_i h_{n-i} = 0$, za svako $n \ge 1$, onda je $u_i = e_i$ (zašto?). Sada "napadnimo" (5) s ω. Dobivamo

$$\sum_{i=0}^{n} (-1)^i h_i \omega(h_{n-i}) = (-1)^n \sum_{i=0}^{n} (-1)^i \omega(h_i) h_{n-i} = 0,$$

a to povlači $\omega(h_i) = e_i$, kao što smo tvrdili. □

KOROLAR 2. *a) Skup $\{h_\lambda | \lambda \vdash n\}$ je baza prostora Λ^n (pa je $\{h_\lambda | \lambda \in \mathrm{Par}\}$ baza od Λ). Ekvivalentno, $h_1, h_2, \dots$ su algebarski nezavisni i generiraju Λ kao $\mathbb{Q}$-algebru, tj. $\Lambda = \mathbb{Q}[h_1, h_2, \dots]$.*

b) Ako su $N_{\lambda\mu}$ brojevi definirani s jednakošću (4), onda je $N_{\lambda\mu} = N_{\mu\lambda}$, tj. matrica prijelaza među bazama $\{m_\lambda | \lambda \vdash n\}$ i $\{h_\lambda | \lambda \vdash n\}$ je simetrična.

c) $\prod_{i,j} (1 - x_i y_j)^{-1} = \sum_{\lambda,\mu} N_{\lambda\mu} m_\lambda(x) m_\mu(y) = \sum_\lambda m_\lambda(x) h_\lambda(y)$.

Dokaz. a) Iz Teorema 2 slijedi da homomorfizam $\omega : \Lambda \to \Lambda$, $\omega(e_n) = h_n$, ima inverz $\omega^{-1} = \omega$, pa je automorfizam, a kako je prema Teoremu 1 $\{e_\lambda | \lambda \vdash n\}$ baza, slijedi da je i $\{h_\lambda | \lambda \vdash n\}$ baza od Λ^n.

b) Ovo se dokazuje potpuno analogno kao i Korolar 1

c) Slijedi slično kao i Propozicija 2 rabeći Propoziciju 3. □

Neka je opet $\lambda \in \mathrm{Par}$. **Sume potencija** definiramo kao simetrične funkcije

$$p_n = m_n = \sum_i x_i^n, n \ge 1, p_0 = m_\emptyset = 1,$$
$$p_\lambda = p_{\lambda_1} p_{\lambda_2} \dots, \text{ ako je } \lambda = (\lambda_1, \lambda_2, \dots).$$

Kombinatorno značenje keoficijenata razvoja p_λ po bazi $\{m_\lambda\}$ je sljedeće.

PROPOZICIJA 4. *Neka je $\lambda = (\lambda_1, \dots, \lambda_l) \vdash n$, gdje je $l = \ell(\lambda)$ i neka je*

$$p_\lambda = \sum_{\mu \vdash n} R_{\lambda\mu} m_\mu. \tag{6}$$

Tada je $R_{\lambda\mu}$ jednak broju uređenih particija $(B_1, \dots, B_k)$ skupa $[\ell]$, tako da je $\mu_j = \sum_{i \in B_j} \lambda_i$, $1 \le j \le k$, pri čemu je $k = \ell(\mu)$.

Dokaz. $R_{\lambda\mu}$ je koeficijent od $x^\mu = x_1^{\mu_1} x_2^{\mu_2} \dots$ u $p_\lambda = (\sum x_i^{\lambda_1})(\sum x_i^{\lambda_2}) \dots$. Da dobijemo monom u x^μ, treba iz svakog od faktora $\sum x_i^{\lambda_j}$ odabrati član $x_{i_j}^{\lambda_j}$ tako da je $\prod_j x_{i_j}^{\lambda_j} = x^\mu$. Stavimo $B_r = \{j | i_j = r\}$. Tada $(B_1, \dots, B_k)$ čine uređenu particiju kao što se tvrdi i obrnuto, svaka takva uređena particija daje član x^μ. □

KOROLAR 3. *Neka je $R_{\lambda\mu}$ kao u (6). Tada je $R_{\lambda\mu} = 0$, osim ako je $\lambda \le \mu$. Ako je $\lambda = \langle 1^{m_1(\lambda)} 2^{m_2(\lambda)} \dots \rangle$, onda je $R_{\lambda\lambda} = \prod_i m_i(\lambda)!$. Stoga je $\{p_\lambda | \lambda \vdash n\}$ baza od Λ^n (pa je $\{p_\lambda | \lambda \in \mathrm{Par}\}$ baza od Λ). Ekvivalentno, $p_1, p_2, \dots$ su algebarski nezavisni i $\Lambda = \mathbb{Q}[p_1, p_2, \dots]$.*

Dokaz. Ako je $R_{\lambda\mu} \ne 0$, onda iz Propozicije 4 slijedi da postoji uređena particija $(B_1, \dots, B_k)$ skupa $[\ell] = [\ell(\lambda)]$ za koju vrijedi $\mu_j = \sum_{i \in B_j} \lambda_i$. Za $1 \le r \le \ell$, neka su $B_{i_1}, \dots, B_{i_r}$ različiti blokovi te particije koje sadrže bar jedan od brojeva $1, 2, \dots, r$. Stoga je $\mu_{i_1} + \dots + \mu_{i_s} \ge \lambda_1 + \dots + \lambda_r$. No $\mu_1 + \dots + \mu_r \ge \mu_{i_1} + \dots + \mu_{i_s}$ jer je $r \ge s$ i $\mu_1 \ge \mu_2 \ge \dots$. Zato je $\lambda \ge \mu$, kao što smo i tvrdili.

Ako je $\lambda = \mu$, onda je svaki blok B_i jednočlani skup $\{j\}$, koji ćemo jednostavno označavati kao j. Sada $B_1, \dots, B_{m_1}$ možemo urediti kao i $1, \dots, m_1$. Onda i $B_{m_1} +$

$1, \dots, B_{m_1+m_2}$ možemo urediti kao i $m_1+1, \dots, m_1+m_2$ itd. To daje ukupno $R_{\lambda\lambda} = m_1!m_2! \dots$ uređaja takvih particija. Da je $\{p_\lambda | \lambda \vdash n\}$ baza, sada slijedi slično kao i u dokazu Teorema 1. □

Za particiju $\lambda = \langle 1^{m_1} 2^{m_2} \dots \rangle$ definiramo $z_\lambda = 1^{m_1} m_1! 2^{m_2} m_2! \dots$, i $\varepsilon_\lambda = (-1)^{m_2+m_4+\dots} = (-1)^{n-\ell(\lambda)}$, ako je $\lambda \vdash n$. Uočite da je zbog Propozicije 5 u pogl. II. broj permutacija $\pi \in S_n$ cikličkog tipa $(m_1, m_2, \dots)$ jednak $n! z_\lambda^{-1}$.

PROPOZICIJA 5. *Vrijedi*

a) $\prod_{i,j}(1 - x_i y_j)^{-1} = \exp \sum_{n\geq 1} \frac{1}{n} p_n(x) p_n(y) = \sum_\lambda z_\lambda^{-1} p_\lambda(x) p_\lambda(y)$.

b) $\prod_{i,j}(1 + x_i y_j) = \exp \sum_{n\geq 1} \frac{(-1)^{n-1}}{n} p_n(x) p_n(y) = \sum \varepsilon_\lambda z_\lambda^{-1} p_\lambda(x) p_\lambda(y)$.

Dokaz. a) $\log \prod_{i,j}(1 - x_i y_j)^{-1} = \sum_{i,j} \log(1 - x_i y_j)^{-1} = \sum_{i,j} \sum_{n\geq 1} \frac{1}{n} x_i^n y_j^n =$

$= \sum_{n\geq 1} \frac{1}{n} (\sum_i x_i^n)(\sum_j y_j^n) = \sum_{n\geq 1} \frac{1}{n} p_n(x) p_n(y)$,

čime je dokazana prva jednakost, a druga tada slijedi iz eksponencijalne formule; izvedite je sami;

b) slijedi slično. □

Posebno, uvrstimo li u a) $y = (t, 0, 0, \dots)$ slijedi $h_n = \sum_{\lambda\vdash n} z_\lambda^{-1} p_\lambda$, i slično iz b) slijedi $e_n = \sum_{\lambda\vdash n} \varepsilon_\lambda z_\lambda^{-1} p_\lambda$. Iz Teorema 2 tada dobivamo funkciju izvodnicu za (p_n):

$$P(t) := \sum_{n\geq 1} p_n t^{n-1} = \frac{d}{dt} \log H(t) = \frac{H'(t)}{H(t)} = \frac{d}{dt} \log E(-t) = \frac{E'(-t)}{E(-t)}.$$

Skalarni produkt $\langle\ ,\ \rangle$ na prostoru Λ definira se formulom

$$\langle m_\lambda, h_\mu \rangle = \delta_{\lambda\mu}, \tag{7}$$

za svako $\lambda, \mu \in \mathrm{Par}$, tj. zahtjevom da su $\{m_\lambda\}$ i $\{h_\lambda\}$ dualne baze. Simetričnost skalarnog produkta $\langle\ ,\ \rangle$ slijedi odmah iz Korolara 2 b), tj. iz $\langle h_\lambda, h_\mu \rangle = \langle h_\mu, h_\lambda \rangle$. Nadalje, iz Teorema 2 nije teško pokazati da involucija ω djeluje na p_λ ovako: $\omega p_\lambda = \varepsilon_\lambda p_\lambda$ (tj. p_λ je svojstveni vektor s pripadnom svojstvenom vrijednošću ε_λ). Baza $\{p_\lambda\}$ od Λ je ortogonalna. Točnije, vrijedi $\langle p_\lambda, p_\mu \rangle = z_\lambda \delta_{\lambda\mu}$. Ako je $f = \sum c_\lambda p_\lambda$, onda slijedi $\langle f, f \rangle = \sum c_\lambda^2 z_\lambda$, pa je $\langle f, f \rangle \geq 0$, jer je $z_\lambda > 0$ i $\langle f, f \rangle = 0 \iff f = 0$. Stoga je $\langle\ ,\ \rangle$ pozitivno definitan. Involucija ω je izometrija, tj. $\langle \omega f, \omega g \rangle = \langle f, g \rangle$, $\forall f, g \in \Lambda$, jer to slijedi iz gornjih formula za $f = p_\lambda$, $g = p_\mu$.

Osim spomenutih četiriju baza $m_\lambda, e_\lambda, h_\lambda, p_\lambda$ od Λ, za kombinatoriku je od velike važnosti vrlo suptilna baza s_λ od Λ koje se zovu **Schurove funkcije**. Klasična (algebarska) definicija Schurovih funkcija je sljedeća. Neka je $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbb{N}_0^n$, a $\pi \in S_n$. Ako je $x^\alpha = x_1^{\alpha_1} x_2^{\alpha_2} \dots x_n^{\alpha_n}$, onda ćemo pisati $\pi(x^\alpha) := x_1^{\alpha_{\pi(1)}} \dots x_n^{\alpha_{\pi(n)}}$.

Definirajmo polinom

$$a_\alpha = a_\alpha(x_1, \dots, x_n) = \sum_{\pi\in S_n} \varepsilon_\pi \pi(x^\alpha)\ , \tag{8}$$

gdje je $\varepsilon_\pi = 1$, ako je π parna, a $\varepsilon_\pi = -1$, ako je π neparna permutacija. Uočimo da je desna strana od (8) razvoj determinante, tj.

$$a_\alpha = \det(x_i^{\alpha_j})_{i,j=1,\dots n}\ .$$

Nadalje, vrlo je važno uočiti da je a_α kososimetrična (ili antisimetrična), tj. da je $\pi(a_\alpha) = \varepsilon_\pi a_\alpha$. Zato je $a_\alpha = 0$, osim ako su svi brojevi α_i različiti. Stoga možemo pretpostaviti da je $\alpha_1 > \alpha_2 > \dots > \alpha_n \geq 0$, pa je $\alpha = \lambda + \delta$, gdje je $\lambda \in \mathrm{Par}$, $\ell(\lambda) \leq n$, a $\delta = \delta_n = (n-1, n-2, \dots, 0)$ i stoga $\alpha_j = \lambda_j + n - j$. Tako dobivamo da je

$$a_\alpha = a_{\lambda+\delta} = \det(x_i^{\lambda_j+n-j})_{i,j=1,\dots n}\ .$$

Posebno, za $\lambda = (0, 0, \dots)$ dobivamo Vandermondeovu determinantu

$$a_\delta = \det(x_i^{n-j}) = \prod_{1\leq i<j\leq n} (x_j - x_i).$$

Kako je a_α antisimetrična, stavimo li $x_i = x_j$ za neke $i \neq j$, dobivamo da je $a_\alpha = 0$, pa je zato a_α djeljiv s $x_j - x_i$ i stoga djeljiv s a_δ u prstenu polinoma $\mathbb{Z}[x_1, \dots, x_n]$. Kvocijent a_α / a_δ je zato opet iz $\mathbb{Z}[x_1, \dots, x_n]$, a kako su oba a_α i a_δ antisimetrični, slijedi da je a_α / a_δ simetrična i homogena funkcija stupnja $|\alpha| - |\delta| = |\lambda|$. **Schurova funkcija** s_λ se upravo i definira kao

$$s_\lambda(x_1, \dots, x_n) = \frac{a_{\lambda+\delta}}{a_\delta} = \frac{\det(x_i^{\lambda_j+n-j})}{\det(x_i^{n-j})}.$$

Primjer 2. Odredite Schurovu funkciju s_λ ako je $n = 3$ i $\lambda = \langle 21 \rangle$.

Rješenje. Iz definicije Schurove funkcije imamo

$$s_{21}(x_1, x_2, x_3) = \begin{vmatrix} x_1^4 & x_1^2 & 1 \\ x_2^4 & x_2^2 & 1 \\ x_3^4 & x_3^2 & 1 \end{vmatrix} : \begin{vmatrix} x_1^2 & x_1 & 1 \\ x_2^2 & x_2 & 1 \\ x_3^2 & x_3 & 1 \end{vmatrix} = \frac{(x_2^2 - x_1^2)(x_3^2 - x_1^2)(x_3^2 - x_2^2)}{(x_2 - x_1)(x_3 - x_1)(x_3 - x_2)} =$$

$= (x_1 + x_2)(x_1 + x_3)(x_2 + x_3) = x_1^2 x_2 + x_1^2 x_3 + x_2^2 x_1 + x_2^2 x_3 + x_3^2 x_1 + x_3^2 x_2 + 2x_1 x_2 x_3 =$

$= m_{21}(x_1, x_2, x_3) + 2m_{111}(x_1, x_2, x_3)$, tj. $s_{21} = m_{21} + 2m_{111}$.

□

Kako je Schurova funkcija simetrična, možemo je razviti po bazi (m_μ). Pri tome dodajemo onoliko varijabli koliko nam treba i stavivši da su sve dodatne varijable 0, možemo smatrati da opet imamo beskonačno varijabli kao i u definiciji monomijalnih i ostalih simetričnih funkcija. Neka je

$$s_\lambda = \sum_{\mu\vdash\lambda} K_{\lambda\mu} m_\mu\ ,$$

razvoj od s_λ, $\lambda \vdash n$, po (m_μ). Brojevi $K_{\lambda\mu}$ se zovu **Kostkini brojevi**. Kao u prethodnom primjeru nije teško izvesti da je npr. $s_1 = m_1$, $s_{11} = m_{11}$, $s_2 = m_{11} + m_2$, $s_{211} = m_{211} + 3m_{1111}$, $s_{31} = m_{31} + m_{22} + 2m_{211} + 3m_{1111}$ itd. Ne zna se neka korisna formula za Kostkine brojeve $K_{\lambda\mu}$ (a vjerojatno i ne postoji). No rabeći prethodnu teoriju (Propozicija 3, Korolar 2 c) itd.) može se pokazati da vrijede sljedeća osnovna svojstva Schurovih funkcija.

TEOREM 3. *a) Neka su $\mu, \nu \vdash n$ čvrste particije. Tada je*

$$\sum_{\lambda \vdash n} K_{\lambda\mu} K_{\lambda\nu} = N_{\mu\nu} = \langle h_\mu, h_\nu \rangle = \text{broj } \mathbb{N}_0\text{-matrica } A, \operatorname{red}(A) = \mu, \operatorname{stup}(A) = \nu.$$

b) Neka su $\lambda, \mu \in \mathrm{Par}$, $|\lambda| = |\mu|$. Ako je $K_{\lambda\mu} \neq 0$, onda je $\lambda \leq \mu$ (u uređaju dominacije za particije), $K_{\lambda\lambda} = 1$.

c) Skup $\{s_\lambda | \lambda \vdash n\}$ je baza prostora Λ^n (pa je $\{s_n | \lambda \in \mathrm{Par}\}$ baza od Λ), jer je matrica prijelaza $(K_{\lambda\mu})$ od $\{s_\lambda\}$ pomoću $\{m_\mu\}$ zbog b) (a s obzirom na neki uređaj od $\mathrm{Par}(n)$ koji proširuje dominaciju) donja trokutasta s jedinicama na glavnoj dijagonali.

d) **Cauchyjev identitet** $\prod_{i,j} (1 - x_i y_i)^{-1} = \sum_\lambda s_\lambda(x) s_\lambda(y)$.

e) $\langle s_\lambda, s_\mu \rangle = \delta_{\lambda\mu}$, tj. $\{s_\lambda\}$ je ortonormirana baza od Λ.

f) $\prod_{i,j} (1 + x_i y_j) = \sum_\lambda s_\lambda(x) s_{\lambda'}(y)$.

g) $\omega(s_\lambda) = s_{\lambda'}$, gdje je λ' konjugirana particija od λ.

h) **Jacobi-Trudijev identitet**. $s_\lambda = \det(h_{\lambda_i - i + j})_{i,j=1,\dots,n}$, $n = \ell(\lambda)$, *(pri čemu je $h_0 = 1$ i $h_k = 0$, $k < 0$).*

Sada ćemo kombinatorno opisati Schurove funkcije. Osnovni kombinatorni objekt vezan uz Schurove funkcije je polustandardna tablica. Neka je λ particija. **Polustandardna Youngova tablica** (engl. *semistandard Young tableau*, skraćeno SSYT) **oblika** λ je tablica $T = (T_{ij})$ prirodnih brojeva oblika λ, tj. $1 \leq i \leq \ell(\lambda)$, $1 \leq j \leq \lambda_i$, čiji je svaki redak rastući, a svaki stupac strogo rastući. **Veličina** SSYT-a je broj članova tablice. Drugim riječima, SSYT je Youngov dijagram particije λ čiji su kvadratići ispunjeni brojevima T_{ij}. Tako je npr. jedna SSYT oblika $\lambda = (6,4,4,2)$ veličine 16 sljedeća:

1	2	2	3	4	4
2	3	4	4		
6	6	7	7		
8	9				

odnosno

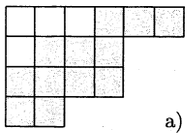
1	2	2	3	4	4
2	3	4	4		
6	6	7	7		
8	9				

SSYT T je tipa $\alpha = (\alpha_1, \alpha_2, \dots)$ i pišemo $\alpha = \mathrm{tip}(T)$, ako T ima $\alpha_i = \alpha_i(T)$ članova jednakih i. Tip tablice iz gornjeg primjera je $(1,3,2,4,0,2,2,1,1)$. Za SSYT tipa α definiramo

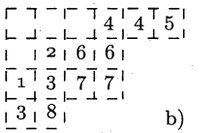
$$x^T = x_1^{\alpha_1(T)} x_2^{\alpha(T)} \dots$$

U našem je primjeru $x^T = x_1 x_2^3 x_3^2 x_4^4 x_6^2 x_7^2 x_8 x_9$. Prirodno poopćenje SSYT-a je sljedeće. Neka su λ i μ particije i $\lambda \subseteq \mu$ (tj. $\lambda_i \leq \mu_i$, $\forall i$). Tada definiramo

polustandardnu Youngovu tablicu (SSYT) **kosog oblika** λ/μ kao tablicu $T = (T_{ij})$ prirodnih brojeva oblika λ/μ, tj. $1 \leq i \leq \ell(\lambda)$, $\mu_i < j \leq \lambda_i$, čiji svaki redak raste, a svaki stupac strogo raste. Pogledajmo SSYT oblika $(6,4,4,2)/(3,1)$. Nađimo prvo pozicije koje u Youngovom dijagramu od λ zauzimaju oblik λ/μ (na sl. a)) zatamnjeni kvadratići, a tada ih ispunimo brojevima kao na sl. b):



a)



b)

Tip ovakve SSYT tablice T, $\mathrm{tip}(T)$ i x^T definiraju se kao i prije. Sada konačno definiramo za kosi oblik **kosu Schurovu funkciju** $s_{\lambda/\mu}$ **oblika** λ/μ u varijablama $x = (x_1, x_2, \dots)$ kao formalni red potencija

$$s_{\lambda/\mu}(x) = \sum_T x^T,$$

gdje sumiramo po svim $SSYT$ oblika λ/μ. Ako je $\mu = \emptyset$, onda je $\lambda/\emptyset = \lambda$, i $s_\lambda(x)$ je **Schurova funkcija** oblika λ. Tako npr. svi SSYT oblika $(2,1)$ s najvećim dijelom ≤ 3 su:

1	1	1	2	1	1	1	3	2	2	2	3	1	2	1	3
2		2		3		3		3		3		3		2	

Stoga je

$$s_{21}(x_1, x_2, x_3) = x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2 + 2x_1 x_2 x_3 = \\ = m_{21}(x_1, x_2, x_3) + 2m_{111}(x_1, x_2, x_3),$$

dakle, isti rezultat kao u Primjeru.

Fundamentalni je teorem da se algebarski i kombinatorno definirane Schurove funkcije podudaraju, tj. omjer determinanti je (obična) Schurova funkcija:

$$a_{\lambda+\delta}/a_\delta = s_\lambda(x_1, \dots x_n).$$

Ako je $\lambda \vdash n$, a α slaba kompozicija od n, onda je Kostkin broj $K_{\lambda\alpha}$ broj SSYT-ova oblika λ i tipa α i vrijedi

$$s_\lambda = \sum_\alpha K_{\lambda\alpha} x^\alpha,$$

pri čemu se sumira po svim slabim kompozicijama α od n, odnosno

$$s_\lambda = \sum_{\lambda \vdash n} K_{\lambda\mu} m_\mu.$$

Općenitije, **kosi Kostkin broj** $K_{\lambda/\nu,\alpha}$ je broj SSYT-ova oblika λ/ν i tipa α, tako da je $|\lambda/\nu| = n$ i vrijedi

$$s_{\lambda/\nu} = \sum_{\mu \vdash n} K_{\lambda/\nu,\mu} m_\mu \quad .$$

Osnovni kombinatorni postupak u teoriji simetričnih funkcija je tzv. RSK-**algoritam** (ili RSK-**korespondencija**) ili, punim nazivom, Robinson-Schensted-Knuthov algoritam koji omogućava da se kombinatorno dokažu razna svojstva Schurovih funkcija. Ideje o tome nastale su 1960-ih godina. Glavni rezultat o RSK-algoritmu jest sljedeći.

TEOREM 4. *RSK algoritam daje bijekcija skupa svih $\mathbb{N}_0$-matrica A s konačnim nosačem (tj. samo je konačno članova $\neq 0$) i skupa svih uređenih parova (P,Q) SSYT-ova istog oblika. Pišemo $A \xrightarrow{RSK} (P,Q)$. Pritom vrijedi* $\mathrm{tip}(P) = \mathrm{stup}(A)$, $\mathrm{tip}(Q) = \mathrm{red}(A)$. *Nadalje, ako $A \xrightarrow{RSK} (P,Q)$, onda $A^T \xrightarrow{RSK} (Q,P)$.*

Elaboraciju RSK algoritma i dokaz ovog teorema nećemo provesti, nego ćemo samo primjera radi pokazati kako se on primjenjuje za dokazivanje raznih činjenica o Schurovim funkcijama.

Dokaz Cauchyjevog indentiteta. (iz Teorema 3 d)).
Razvijmo svaki član produkta na lijevoj strani u geometrijski red:

$$\prod_{i,j}(1-x_iy_j)^{-1} = \prod_{i,j}\left[\sum_{a_{ij}\geq 0}(x_iy_j)^{a_{ij}}\right]. \tag{9}$$

Nakon provedenih množenja na desnoj strani vidimo da je član $x^\alpha x^\beta$ u tom razvoju dobiven odabirom $\mathbb{N}_0$-matrice $A^T = [a_{ij}]^T$ (transponirane od A) s konačnim nosačem za koju je $\mathrm{red}(A) = \alpha$, $\mathrm{stup}(A) = \beta$. Zato je koeficijent uz $x^\alpha x^\beta$ u (9) jednak broju $N_{\alpha\beta}$ svih $\mathbb{N}_0$-matrica A za koje je $\mathrm{red}(A) = \alpha$, $\mathrm{stup}(A) = \beta$ (ustvari je to ekvivalentno s Korolarom 2 c)). S druge strane, koeficijent uz $x^\alpha y^\beta$ u $\sum_\lambda s_\lambda(x)s_\lambda(y)$ je jednak broju parova (P,Q) svih SSYT-ova istog oblika λ tako da je $\mathrm{tip}(P) = \alpha$, $\mathrm{tip}(Q) = \beta$. No RSK algoritam daje bijekciju među takvim matricama A i parovima (P,Q), iz čega slijedi Cauchyjev identitet. □

Iy Cauchyjevog identiteta sada odmah slijedi svojstvo iz Teorema 3 a) (uzimanjem koeficijenata $x^\mu y^\nu$ na objema stranama). I druga svojstva Schurovih funkcija se mogu sada dokazivati kombinatorno, i to ne samo za obične nego i za kose Schurove funkcije. Jedno od takvih osnovnih svojstava odnosi se na skalarni produkt $\langle\ ,\ \rangle$ u Λ.

TEOREM 5. *Za svako $f \in \Lambda$ vrijedi*

$$\langle fs_\mu, s_\lambda\rangle = \langle f, s_{\lambda/\mu}\rangle,$$

tj. linearni operatori $f \mapsto fs_\mu$ i $s_\lambda \mapsto s_{\lambda/\mu}$ su adjungirani. Posebno je za $f = s_\nu$:

$$\langle s_\nu s_\mu, s_\lambda\rangle = \langle s_\nu, s_{\lambda/\mu}\rangle.$$

Cijeli broj $\langle s_\nu, s_{\lambda/\mu}\rangle$ se označava sa $c^\lambda_{\mu\nu}$ i zove **Littlewood-Richardsonov koeficijent**. Vrijedi

$$s_{\lambda/\mu} = \sum_\nu c^\lambda_{\mu\nu}s_\nu.$$

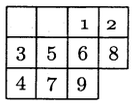
Jedna od važnih posljedica ovoga je **poopćeni Jacobi-Trudijev identitet** za $\lambda = (\lambda_1,\dots,\lambda_n)$ i $\mu = (\mu_1,\dots,\mu_n) \subseteq \lambda$:

$$s_{\lambda/\mu} = \det(h_{\lambda_i-\mu_j-i+j})_{i,j=1,\dots,n}.$$

Evo kako kombinatorno možemo "očitati" Littlewood-Richardsonove koeficijente (i zbog toga su oni nenegativni cijeli brojevi, tj. s-pozitivni).

TEOREM 6 (Littlewood-Richardsonovo pravilo). *Littlewood-Richardsonov koeficijent $c^\lambda_{\mu\nu}$ jednak je broju onih SSYT oblika λ/μ tipa ν, čije je obrnuto čitanje rešetkasta permutacija.*

Obrnuto čitanje SSYT-a T je nadovezivanje redaka od T i njihovo nizanje članova od T čitanih redom od prvog retka prema dolje u obrnutom poretku u svakom retku. Npr. za



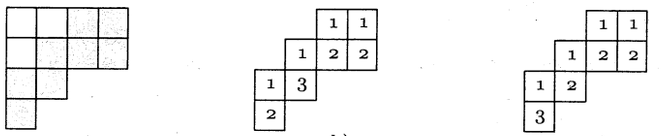
, obrnuto čitanje od T je 2 1 8 6 5 3 9 7 4.

Rešetkasta permutacija tipa $\lambda \in \mathrm{Par}$ je niz $a_1a_2\dots a_n$ brojeva iz $[\ell(\lambda)]$ u kojem se broj i pojavljuje λ_i puta, a u svakom lijevom faktoru $a_1a_2\dots a_j$, broj i-ova je $\geq$ broju $(i+1)$-ova, za svako i.

Pogledajmo "konkretni" primjer.

Primjer 3. Neka je $\lambda = (4,4,2,1)$, $\mu = (2,1)$ i $\nu = (4,3,1)$. Odredite Littlewood-Richardsonov koeficijent $c^\lambda_{\mu\nu}$.

Rješenje. Prvo odredimo oblik λ/μ; na sl. a) to su sivi kvadratići. U te kvadratiće tada upisujemo brojeve tipa ν.



Ispunjavanje sivih kvadratića tako da bude $\nu_1 = 4$ brojeva 1, $\nu_2 = 3$ brojeva 2 i $\nu_3 = 1$ brojeva 3 i to tako da u svakom retku brojevi rastu (bolje reći ne padaju), a u svakom stupcu strogo rastu, može se učiniti na samo dva načina kao na gornjim slikama b) i c). Obrnutim čitanjem ovih tablica dobivamo redom nizove 1 1 2 2 1 3 1 2 i 1 1 2 2 1 2 1 3. Lako je provjeriti da su oba ova niza rešetkaste permutacije (tipa ν). Stoga je $c^\lambda_{\mu\nu} = 2$. □

Postoje i druge kombinatorne interpretacije Littlewood-Richardsonovih koeficijenata. Jedna od važnijih dolazi iz primjene RSK algoritma na ravninske particije. **Ravninska particija** od n je tablica $T = (T_{ij})_{i,j\geq 1}$ cijelih brojeva $T_{ij} \geq 0$ s konačnim nosačem (tj. samo konačno $T_{ij} \neq 0$), rastuća u svakom retku i svakom stupcu i $\sum_{i,j} T_{ij} = n$. Obična particija $\lambda \vdash n$ je 1-dimenzionalna tablica $(\lambda_1,\lambda_2,\dots)$

cijelih brojeva $\lambda_i \geq 0$ s konačnim nosačem čija je suma n. Zato su ravninske particije prirodna poopćenja običnih particija. (Slično se definiraju d-dimenzionalne particije, ali se o njima ne zna gotovo ništa za $d \geq 3$.)

Littlewood-Richardsonovi koeficijenti su od 1940-ih god. jedna od središnjih tema teorije simetričnih funkcija. Tako je 1999. dokazano da za $\lambda = (\lambda_1, \lambda_2, \dots) \in$ Par, $m\lambda = (m\lambda_1, m\lambda_2, \dots)$ za $m \in \mathbb{N}_0$, $c^{m\lambda}_{m\mu,m\nu} \neq 0$ povlači $c^{\lambda}_{\mu\nu} \neq 0$ (v. A. Knutson, T.Tao, The honeycomb model of $GL_n(\mathbb{C})$ tensor product I: proof of the saturation conjecture, J. Amer. Math. Soc. 12 (1999), 1055 – 1090, kao i A. Buch, The saturation conjecture, Enseign, Math. 46 (2000), 43–60).

Spomenimo na samome kraju da teorija simetričnih funkcija, a poglavito Schurove funkcije, igraju prvorazrednu ulogu u teoriji reprezentacija grupa i algebri (npr. jer su karakteri ireducibilnih polinomskih reprezentacija opće linearne grupe Schurove funkcije). Zatim u algebarskoj geometriji i topologiji (napose za računanja kohomologije raznih prostora) i drugim granama matematike, a s druge se strane do simetričnih funkcija dolazi iz fizikalnih svojstava simetrija u "majci prirodi". Literatura o tome je opsežna.

Bibliografija

Prvo navodimo literaturu iz D. Veljan, *Kombinatorika s teorijom grafova*, Školska knjiga, Zagreb, 1989, označenu s [1]–[236], a potom uglavnom noviju literaturu, označenu s [1*]–[76*]. Nova izdanja nekih starijih knjiga ne navodimo ponovno.

[1] Abhyankar S. S., *Enumerative Combinatorics of Young Tableux*, Marcel Dekker, New York, 1987.

[2] Aho A., Hopcroft J., Ullman J., *Data Structures and Algorithms*, Addison-Wesley, Reading Mass., 1983.

[3] Aigner M. *Combinatorial Theory*, Springer Verlag, Berlin, 1979, (ruski prijevod Mir, Moskva, 1982.)

[4] Aigner M. *Graphentheorie. Eine entwicklung aus dem 4-Farben problem*, Teubner, Stuttgart, 1984.

[5] Anderson, I., *A First Course in Combinatorial Mathematics*, Clarendon Press, Oxford, 1974.

[6] Anderson, I., *Combinatorics of Finite Sets*, Clarendon Press, Oxford, 1987.

[7] Anderson, S. S., *Graph Theory and Finite Combinatorics*, Markham, Chicago, 1970.

[8] Andrásfai B., *Introductory Graph Theory*, Akadémiai Kiadó, Budapest, 1977.

[9] Andrews G., *The Theory of Partitions*, Encyclopedia of Math. and its Appl., vol. 12, Addison-Wesley, Reading, Mass., 1976 (ruski prijevod Mir, Moskva, 1983.)

[10] Aršinov M. N., Sadovskii L. E., *Kodi i matematika*, Bibl. Kvant 30, Nauka, Moskva, 1983.

[11] Averbach B., Chien O., *Mathematics; Problem Solving through Recreational Mathematics*, Freeman, San Francisco, 1980.

[12] Bajc D., Pisanski T., *Najnujnejše o grafih*, Bibl. Presek, vol. 6, DMFA SR Slovenije, Ljubljana, 1985.

[13] Bannai E., Ito T., *Algebraic Combinatorics I. Association Schemes*, The Benjamin Cummings, Menlo Park, Calif., 1984. (ruski prijevod Mir, Moskva, 1987.)

[14] Barnette D. D., *Map Coloring, Polyhedra and the Four-Color Problem*, Math. Assoc. Amer., Washington D.C., 1983.

[15] Batagelj V., *Diskretne Strukture. Naloge*, FNT Matematični rokopisi 5., DMFA SR Slovenije, Ljubljana, 1986.

[16] Batten L. M., *Combinatorics of Finite Geometries*, Cambridge Univ. Press, Cambridge, 1986.

[17] Beckenbach E. F. (Ed.), *Applied Combinatorial Mathematics*, John Wiley & Sons, New York, 1964 (ruski prijevod Mir, Moskva, 1968.)

[18] Behzad M., Chartrand G., *Introduction to the Theory of Graphs*, Allyn and Bacon, Boston, 1971.

[19] Bezhad M., Chartrand G., Lesniak-Foster L.,*Graphs and Digraphs*, Prindle-Weber-Schmidt, Boston, 1979.

[20] Beineke L., Wilson R. J., (Eds.) *Application of Graph Theory*, Academic Press, New York, 1979.

[21] Beineke L., Wilson R. J., (Eds.), *Selected Topics in Graph Theory I, II*, Academic Press, New York, 1978, 1983.

[22] Bekišev G. A., Kratko M. I., *Elementarnoe vvedenie v geometričeskoe programirovanije*, Nauka, Moskva, 1980.

[23] Berezina L. Ju., *Grafi i ih primenenie*, Prosveščenie, Moskva, 1979.

[24] Berge C., *Graphs and Hypergraphs*, North Holland, Amsterdam, 1973.

[25] Berge C., *Graphs*, North Holland, Amsterdam, 1985.

[26] Berge C., Gouila-Houri A., *Programming, Games and Transportation Networks*, John Wiley & Sons, New York, 1965.

[27] Beutelspacher A., *Einführung in die endliche Geometrie. I, Blockplane*, Bibliographisches Inst., Mannheim, 1982.

[28] Biggs N., *Algebraic Graph Theory*, Cambridge Univ. Press, Cambridge, 1974.

[29] Biggs N., *Discrete Mathematics*, Clarendon Press, Oxford, 1985.

[30] Biggs N., Lloyd E. K., Wilson R. J., *Graph Theory 1736-1936*, Clarendon, Oxford, 1986.

[31] Biggs N., White A. T., *Permutation Groups and Combinatorial Structures*, Cambridge Univ. Press, Cambridge, 1979.

[32] Bogart K. P., *Introductory Combinatorics*, Pitman, London, 1983.

[33] Bollobás B., *Extremal Graph Theory*, Academic Press, New York, 1978.

[34] Bollobás B., *Random Graphs*, Academic Press, New York, 1985.

[35] Bondy J. A., Murty U. S. R., *Graph Theory with Applications*, North Holland/Elsevier, Amsterdam, 1976.

[36] Borgwardt K. H., *The Simplex Method. A Probabalistic Analysis*, Series Algorithms and Combinatorics vol.1, Springer Verlag, New York, 1987.

[37] Bose R. C., Manvel B., *Introduction to Combinatorial Theory*, John Wiley & Sons, New York, 1984.

[38] Brualdi R., *Introductory Combinatorics*, North Holland, Amsterdam, 1977.

[39] Bryant V., Perfect H., *Independence Theory in Combinatorics*, Chapman and Hall, New York, 1980.

[40] Burkov V., Gordidze A., Loveckii S. E., *Prikladnije zadači teorii grafov*, Vyč. Centr. Akad. Nauk. Gruz., Tbilisi, 1974.

[41] Busacker R., Saaty T., *Finite Graphs and Networks. An Introduction with Applications*, McGraw-Hill, New York, 1965.

[42] Calude C., *Theories of Computational Complexity*, Ann. Discr. Math. vol. 35, North Holland, Amsterdam, 1988.

[43] Cameron P. J., Lint van J. H., *Graphs, Codes and Designs*, London Math. Soc. LN Ser. 43, Cambridge Univ. Press, Cambridge, 1980.

[44] Capobianco M., Molluzzo J., *Examples and Counterexamples in Graph Theory*, North Holland, Amsterdam, 1978.

[45] Carré B., *Graphs and Networks*, Oxford Appl. Math. and Comp. Sci. Series, Clarendon, Oxford, 1979.

[46] Chartrand G., *Graphs as Mathematical Models*, Prindle-Weber-Schmidt, Boston, 1977.

[47] Chartrand G., Lesniak L., *Graphs & Digraphs*, Wadsworth, Monterey, Calif., 1986.

[48] Chen W., *Applied Graph Theory. Graphs and Electrical Networks*, American Elsevier, New York, 1976.

[49] Christofides N., *Graph Theory. An Algorithmic Approach*, Academic Press, New York, 1975. (ruski prijevod Mir, Moskva, 1978.)

[50] Cohen D. I. A., *Basic Techniques of Combinatorial Theory*, John Wiley & Sons, New York, 1978.

[51] Comtet L., *Advanced Combinatorics*, Reidel, Boston, 1974.

[52] Conway J. H., *On Numbers and Games*, Academic Press, New York, 1976.

[53] Coxeter H., Ball W., *Mathematical Recreations and Essays*, Univ. of Toronto Press, Toronto, 1972.

[54] Crapo H. H., Rota G.-C., *On the Foundations of Combinatorial Theory II; Combinatorial Geometries*, MIT Press, Cambridge Mass., 1970.

[55] Crawley P., Dilworth R. P., *Algebraic Theory af Lattices*, Prentice-Hall, Englewood Cliffs, 1973.

[56] Cvetković D., *Teorija grafova i njene primene*, Naučna knjiga, Beograd, 1986.

[57] Cvetković D., *Kombinatorna teorija matrica sa primenama u elektrotehnici, hemiji i fizici*, Naučna knjiga, Beograd, 1987.

[58] Cvetković D., Doob M., Gutman I., Torgašev A., *Recent Results in the Theory of Graph Spectra*, Ann. Discr. Math. vol. 36, North Holland, Amsterdam, 1988.

[59] Cvetković D., Milić M., *Teorija grafova i njene primene*, Naučna knjiga, Beograd, 1977.

[60] Cvetković D., Simić S., *Kombinatorika, klasična i moderna*, Naučna knjiga, Beograd, 1984.

[61] Cvetković D., Doob M., Sachs H., *Spectra of Graphs-Theory and Applications*, Academic Press, New York, 1982 (ruski prijevod Naukova dumka, Kijev, 1984.)

[62] Danzer L., Grünbaum B., Klee V., *Helly's Theorem and its Relatives*, Proc. Symp. Pure Math. 7, Amer. Math. Soc., Providence R. I., 1963. (ruski prijevod Mir, Moskva, 1968.)

[63] David F. N., *Games, Gods and Gamblings*, Hafner, New York, 1962.

[64] Denes J., Keedwell A. D., *Latin Squares and Their Applications*, Akademiai Kiadó Budapest, 1974.

[65] Deo N., *Graph Theory with Applications to Engineering and Computer Science*, Prentice-Hall, Englewood Cliffs, 1974.

[66] Egoričev G. P., *Integraljnoe predstavlenie i vičesljenije kombinatornih sum*, Nauka, Novosibirsk, 1977. (engleski prijevod Amer. Math. Soc., Providence, R. I., 1984.)

[67] Emeličev V. A., Kovalev M. M., Kravcov M. K., *Mnogogranniki, grafi, optimizacija*, Nauka, Moskva, 1981. (engleski prijevod Cambridge Univ. Press, 1985.)

[68] Erdös P., *The Art af Counting*, MIT Press, Cambridge Mass., 1975.

[69] Erdös P., Spencer J., *Probabilistic Methods in Combinatorics*, Akademiai Kiadó, Budapest, 1974. (ruski prijevod, Mir, Moskva, 1976.)

[70] Even S., *Graph Algorithms*, Computer Software Eng. Ser., Comp. Sci. Press, Woodland Hills, Calif., 1979.

[71] Evstigneev A., *Primenenie teorii grafov v programmirovanii*, Nauka, Moskva, 1985.

[72] Evstigneev V. A., Meljnikov L. S., *Zadači i upražnenija po teorii grafov i kombinatorike*, Novasibirsk. Gos. Univ., Novosibirsk, 1980.

[73] Feller W., *An Introduction to Probability Theory and its Applications I, II*, John Wiley & Sons, New York, 1971. (ruski prijevod Mir, Moskva, 1984.)

[74] Fiorini S., Wilson R. J., *Edge-Colourings of Graphs*, Pitman, London, 1977.

[75] Flachsmeyer J., *Kombinatorik*, Deutscher Verlag der Wiss., Berlin, 1969.

[76] Ford L. R., Fulkerson D. R., *Flows in Networks*, Princeton Univ. Press, Princeton, 1962. (ruski prijevod Mir, Moskva, 1966.)

[77] Garey M. R., Johnson D. S., *Computers and Intractibility. A Guide to the Theory of NP-Completness*, Freeman, San Francisco, 1979.

[78] Gavrilov G. P. (red.), *Perečisliteljnie zadači kombinatornova analiza*, Mir, Moskva, 1979.

[79] Gavrilov G. P., Sapoženko A. A., *Sbornik zadač po diskretnoj matematike*, Nauka, Moskva, 1977.

[80] Gelfond A. O., *Isčislenije konečnih raznostjei*, Nauka, Moskva, 1967.

[81] Gersting J. L., *Mathematical Structures for Computer Science*, Freeman, San Francisco, 1987.

[82] Gessel I., Rota G.-C. (Eds.), *Classic Papers in Combinatorics, Birkhäuser*, Boston, 1987.

[83] Gibbons C., *Algorithmic Graph Theory*, Cambridge Univ. Press, Cambridge, 1985.

[84] Giblin P. J., *Graphs, Surfaces and Homology. An Introduction to Algebraic Topology*, Chapman & Hall, London, 1981.

[85] Golumbic M. C., *Algorithmic Graph Theory and Perfect Graphs*, Academic Press, New York, 1980.

[86] Gould H..W., *Combinatorial Identities*, West Virginia Univ., Morgantown, 1972.

[87] Goulden I. P., Jackson D. M., *Combinatorial Enumeration*, John Wiley & Sons, New York, 1983. (ruski prijevod Mir, Moskva, 1988.)

[88] Graham R. L., *Rudiments of Ramsey Theory*, Amer. Math. Soc., CBMS 45, Providence R. I., 1981. (ruski prijevod Mir, Moskva, 1984.)

[89] Graham R. L., Knuth D E., Patashnik O., *Concrete Mathematics*, Addison-Wesley, Reading, Mass., 1987.

[90] Graham R. L., Rotschild B. L., Spencer J. H., *Ramsey Theory*, John Wiley & Sons, New York, 1980.

[91] Gratzer G., *General Lattice Theory*, Akademie Verlag, Berlin, 1978. (ruski prijevod Mir, Moskva, 1982.)

[92] Graver J., Watkins M. E., *Combinatorics with Emphasis on the Theory of Graphs*, Springer Verlag, New York, 1977.

[93] Grčanac T., *Logo programski jezik*, Lips, Mladost, Zagreb, 1987.

[94] Greene D. H., Knuth D. E., *Mathematics for the Analysis of Algorithms*, Birkhäuser, Boston, 1982 (ruski prijevod Mir, Moskva, 1987.)

[95] Grimaldi R. P., *Discrete and Combinatorial Mathematics. An Applied Introduction*, Addison-Wesley, Reading, Mass., 1985.

[96] Gross J. L., Tucker T. W., *Topological Graph Theory*, John Wiley & Sons, New York, 1987.

[97] Grötschel M., Lovász L., Schrijver A., *Geometric Algorithms and Combinatorial Optimization*, Series Algorithms and Combinatorics, vol. 2, Springer Verlag, New York, 1988.

[98] Grünbaum B., *Convex Polytopes*, John Wiley & Sons, New York, 1967.

[99] Gutman I., Polansky O. E., *Mathematical Concepts in Organic Chemistry*, Springer Verlag, Berlin, 1986.

[100] Hage P., Harary F., *Structural Models in Anthropology*, Cambridge Univ. Press, Cambridge, 1983.

[101] Halder H. R., Heise W., *Einführung in die Kombinatorik*, Carl Hanser Verlag, Munchen-Wien, 1976.

[102] Hall M. Jr., *Combinatorial Theory*, John Wiley & Sons, New York, 1986. (ruski prijevod 1. izd. Mir, Moskva, 1970.)

[103] Harary F., *Graph Theory*, Addison-Wesley, Reading, Mass., 1969. (ruski prijevod Mir, Moskva, 1973.)

[104] Harary F. (Ed.), *Graph Theory and Theoretical Physics*, Academic Press, London, 1967.

[105] Harary F., Palmer E. M., *Graphical Enumeration*, Academic Press, New York, 1973. (ruski prijevod Mir, Moskva, 1978.)

[106] Harris B. (Ed.), *Graph Theory and its Applications*, Academic Press, New York, 1970.

[107] Henley E. J., Williams R. A., *Graph Theory in Modern Engineering*, Academic Prress, New York, 1973.

[108] Hirschfeld J. W. P., *Projective Geometries over Finite Fields*, Clarendon Press, Oxford, 1979.

[109] Horowitz E., Sahni S., *Fundamentals of Data Structures*, Pitman, London, 1981.

[110] Hu T.C., *Combinatorial Algorithms*, Addison-Wesley, Reading, Mass., 1982.

[111] Hughes D. R., Piper F. C., *Design Theory*, Cambridge Univ. Press, Cambridge, 1985.

[112] Ireland K., Rosen M., *A Classical Introduction to Modern Number Theory*, Springer Verlag, New York, 1982. (ruski prijevod Mir, Moskva, 1987.)

[113] Jablonski S. V., *Vveddenie v diskretnuju matematiku*, Nauka, Moskva, 1986.

[114] Jaglom I. M., *Buleva struktura i je modeli*, Sovetskoe radio, Moskva, 1980.

[115] Ježov I., Skorohod A., Jadrenko M., *Elementi kombinatoriki*, Nauka, Moskva, 1977.

[116] Junger M., *Polyhedral Combinatorics and the Acyclic Subdigraph Problem*, Heldermann Verlag, Berlin, 1985.

[117] Jungnickel D., *Transversaltheorie*, Akad. Verlags. Geest-Portig, Leipzig, 1982.

[118] Kalužnin L. A., Sušanskii V. I., *Preobrazovanija i perestanovki*, Nauka, Moskva, 1985.

[119] Kartési F., *Introduction to Finite Geometries*, North Holland, Amsterdam, 1976. (ruski prijevod Mir, Moskva, 1980.)

[120] Kaucký J., *Kombinatorické identitety*, Veda, Bratislava, 1975.

[121] Kaufmann A., *Introduction a la Combinatorique en Vue des Applications*, Dunod, Paris, 1968. (ruski prijevod Mir, Moskva, 1973.)

[122] Klavžar S., Lokar M., Petkovšek M., Pisanski T., *Izbrana poglavlja iz računalništva*, 2. del. Diskretna optimizacija, Matematički rokopisi I5, DMFA SR Sl. Ljubljana, 1986.

[123] Knuth D. E., *The Art of Programming, vol. I, II, III*, Addison-Wesley, New York, 1973, 1981. (ruski prijevod 1. izd. Mir, Moskva, 1978.)

[124] Kolmogorov A. N., *Osnovnie ponjatija teorii verojatnostjei*, Nauka, Moskva, 1974.

[125] König D., *Theorie der endlichen und unendlichen Graphen*, Akad. Verlagsgesellschaft, Leipzig, 1936 (ponovljeno) Chelsea, New York, 1950.)

[126] Korfhage R. R., *Discrete Computational Structures*, Academic Press, New York, 1984.

[127] Korte B., Lovász L., Schrader R., *Greedoids, Series Algorithms and Combinatorics* vol. 4, Springer Verlag, New York, 1988.

[128] Kostrikin A. I., *Vvedenie v algebru*, Nauka, Moskva, 1977. (engleski prijevod Springer Verlag, New York, 1984) i Sbornik zadač po algebre (red. Kostrikin A. I.), Nauka, Moskva, 1987.

[129] Kostrikin A. I., Manin Ju. I., *Linejnaja algebra i geometrija*, Moskovski Gos. Univ., Moskva, 1980.

[130] Kovacs L. B., *Combinatorial Methods of Discrete Programming*, Akademiai Kiadó, Budapest, 1980.

[131] Krishnamurty V., *Combinatorics. Theory and Practice*, Ellis Horwood, Chichester, 1986.

[132] Kurepa S., *Konačno dimenzionalni vektorski prostori i primjene*, Liber, Zagreb, 1975.

[133] Kurepa S., *Matematička analiza I, II, III*, Tehnička knjiga, Zagreb, 1979.

[134] Kurepa S., Kraljević H., *Matematička analiza IV/1*, Tehnička knjiga, Zagreb, 1986.

[135] Lacher R. C. (Ed.), *Studies in Physical and Theoretical Chemistry*, vol. 54, Math/ /Chem/Comp. 1987, Elsevier, Amsterdam, 1988.

[136] Lallement G., *Semigroups and Combinatorial Applications*, John Wiley & Sons, New York, 1979. (ruski prijevod Mir, Moskva, 1985.)

[137] Lawler E. L., *Combinatorial Optimization, Networks and Matroids*, Holt-Rinehart- -Winston, New York, 1976.

[138] Lesner G., *Elemente der Topologie und Graphentheorie*, Herder Verlag, Freiburg, 1980.

[139] Levy H., Lessman F., *Finite Difference Equations*, Macmillan, New York, 1961.

[140] Lewis E. R., *Network Models in Populatian Biology*, Biomath. 7, Springer Verlag, New York, 1977.

[141] Lint van J. H., *Introduction to Coding Theory*, Grad. Text Math. vol. 86, Springer Verlag, Berlin, 1982.

[142] Liu C. L., *Introduction to Combinatorial Mathematics*, McGraw-Hill, New York, 1968.

[143] Liu C. L., *Topics in Combinatorial Mathematics*, Math. Assoc. Amer., Washington D. C., 1972.

[144] Liu C. L., *Elements of Discrete Mathematics*, McGraw-Hill, New York, 1987.

[145] Lotharie M. (Ed.), *Combinatorics on Words*, Encyclopedia of Math. and its Appl., 17, Addison-Wesley, Reading, 1983.

[146] Lovász L., *Combinatorial Problems and Exercises*, North Holland, Amsterdam, 1979.

[147] Lovász L., *An Algorithmic Theory of Numbers, Graphs and Convexity*, CBMS Series in Appl. Math. vol. 50, Amer. Math. Soc., Providence R. I., 1987.

[148] Lovász L., Plummer M. D., *Matching Theory*, Ann. Discr. Math. vol. 29, North Holland, Amsterdam, 1986.

[149] Lüneburg H., *Kombinatorik*, Birkhäuser, Basel, 1971.

[150] MacMahon P. A., *Combinatory Analysis I, II*, Chelsea, New York, 1960.

[151] MacWilliams F. J., Sloane N. J., *The Theory of Error-Correcting Codes*, North Holland, Amsterdam, 1977. (ruski prijevod Mir, Moskva, 1979.)

[152] Macdonald I. G., *Symmetric Functions and Hall Polynomials*, Clarendon, Oxford, 1979. (ruski prijevod Mir, Moskva, 1985.)

[153] Mardešić S., *Matematička analiza u n-dimenzionalnom realnom prostoru I, II*, Školska knjiga, Zagreb; 1977.

[154] Markov A. A., Nagornij N. M., *Teorija algoritmov*, Nauka, Moskva, 1984.

[155] Markushevich A. I., *Recursion Sequences*, Mir, Moskva, 1983.

[156] Menjšikov M. V., Revjakin A. M., Kopilova A. N., *Kombinatornii analiz*, Nauka, Moskva, 1982.

[157] Minc H., *Permanents, Encyclopedia of Math. and its Appl., vol. 16*, Addison-Wesley, Reading, Mass., 1978. (ruski prijevod Mir, Moskva, 1982.)

[158] Minieka E., *Optimization Algorithms for Networks and Graphs*, Industr. Eng. l, Marcel Dekker, New York, 1978.

[159] Mirkin B. G., Rodin S. N., *Grafi i geni*, Nauka, Moskva, 1977.

[160] Mirsky L., *Transversal Theory*, Academic Press, New York,1971.

[161] Mohanty S. G., *Lattice Path Counting and Applications*, Academic Press, New York, 1979.

[162] Moon J. W., *Topics on Tournaments*, Holt-Rinehart-Winston, New York, 1968.

[163] Nagl M., *Graph-Grammatiken. Theorie, Implementierung, Anwendungen*, Friedr. Vieweg & Sohn, Braunschweig, 1979.

[164] Narayana T. V., *Lattice Path Combinatorics with Statistical Applications*, Univ. Toronto Press, Toronto, 1979.

[165] Netto E., *Lehrbuch der Kombinatorik*, Teubner, Leipzig, 1901.

[166] Nijenhuis A., Wilf H. S., *Combinatorial Algorithms*, Academic Press, New York, 1978.

[167] Nishizeki T., Chiba N., *Planar Graphs. Theory and Algorithms*, Ann. Discr. Math. vol. 32, North Holland, Amsterdam, 1988.

[168] Niven I., *Mathematics of Choice, or How to Count without Counting*, New Math. Library, vol. 15, Math. Assoc. Amer., Washington D. C., 1975.

[169] Noltemeier H., *Graphentheorie mit Algorithmen und Anwendungen*, Walter de Gruyter, Berlin, 1976.

[170] Ore O., *Graphs and their Uses*, Random House, New York, 1962. (ruski prijevod Mir, Moskva, 1965.)

[171] Page E. S., Wilson C. B., *An Introduction to Computational Combinatorics*, Cambridge Univ. Press., Cambridge, 1979.

[172] Palmer E., *Graphical Evolution*, John Wiley & Sons, New York, 1985.

[173] Papadimitriou C. H., Steiglitz K., *Combinatorial Optimization. Algorithms and Complexity*, Prentice-Hall, Englewood Cliffs, N. J., 1982.

[174] Pearl M., *Matrix Theory and Finite Mathematics*, McGraw-Hill,. New York, 1973.

[175] Percus J. K., *Combinatorial Methods*, Springer Verlag, New York, 1971.

[176] Perl J., *Graphentheorie. Grundlagen und Anwendungen.* Studien-Texte Inf., Akademische Verlagsgesellschaft, Wiesbaden, 1981.

[177] Petkovšek M., Pisanski T., *Izbrana poglavlja iz računalništva, 1. a del - Izračunjivost in rešljivost. Jeziki. NP polnost. Naloge*, DMFA SR Slovenije, Ljubljana, 1986.

[178] Picard C. F., *Graphs and Questionnaires*, North Holland, Amsterdam, 1980.

[179] Platonov M. L., *Kombinatornie čisla klasa otobraženii i ih priloženija*, Nauka, Moskva, 1979.

[180] Pólya G., Read R. C., *Combinatarial Enumeration of Groups, Graphs and Chemical Compounds*, Springer Verlag, New York, 1987.

[181] Pólya G., Szegö G., *Aufgaben und Lehrsätze aus der Analysis I, II*, Springer Verlag, Berlin, 1971.

[182] Pólya G. Tarjan R. E., Woods D. R., *Notes on Introductory Combinatorics*, Birkhäuser, Boston, 1983.

[183] Postnikov M. M., *Magičeskie kvadrati*, Fizmatgiz, Moskva, 1963.

[184] Potts R. B., Oliver R. M., *Flows in Transportation Networks*, Academic Press, New York, 1972.

[185] Prömel H. J., *Aspects of Ramsey Theory*, Series Algorithms and Combinatorics, vol. 7, Springer Verlag, New York, 1988.

[186] Read R. C. (Ed.), *Graph Theory and Computing*, Academic Press, New York, 1972.

[187] Recski A., *Matroid Theory and its Applications*, Series Algorithms and Combinatorics vol. 6, Springer Verlag, New York, 1987.

[188] Reingolt E. M., Nievergelt J., Deo N., *Combinatorial Algorithms. Theory and Practice*, Prentice-Hall, Englewood Cliffs, N. J., 1977. (ruski prijevod Mir, Moskva, 1980.)

[189] Ribnikov K. A., *Vvedenie v kombinatornii analiz*, Izd. Moskovski Univ., Moskva, 1985.

[190] Ribnikov K. A., (red.), *Problemi kombinatornova analiza.* Novoe v zarubežnoi nauke, Mat. 19, Mir, Moskva, 1980.

[191] Ribnikov K. A. (red.), *Kombinatornii analiz. Zadači i upražnenija*, Nauka, Moskva, 1982.

[192] Ringel G., *Map Color Theorem*, Springer Verlag, Berlin, 1974.

[193] Riordan J., *An Introduction to Combinatorial Analysis*, John Wiley & Sons, New York , 1958. (ruski prijevod In. Lit., Moskva, 1963.)

[194] Riordan J., *Combinatorial Identities*, John Wiley & Sons, New York, 1968. (ruski prijevod Mir, Moskva, 1982.)

[195] Roberts F. S., *Applied Combinatorics*, Prentice-Hall, Englewood Cliffs, N. J., 1984.

[196] Robinson D. F. Foulds L. D., *Digraphs. Theory and Techniques*, Gordon and Breach, New York, 1980.

[197] Roman S., *The Umbral Calculus*, Academic Press, New York, 1984.

[198] Rota G.-C., *Finite Operator Calculus*, Academic Press, New York, 1975.

[199] Rota G.-C. (Ed.), *Studies in Combinatorics*, MAA Studies in Mathematics, vol. 17, Math. Assoc. Amer., Washington D. C., 1978.

[200] Ryser H. J., *Combinatorial Mathematics*, MAA Carus Math. Monographs, vol. 14, Math. Assoc. Amer., Washington D. C., 1963. (ruski prijevod Mir, Moskva, 1966.)

[201] Saaty T., Kainen P., *The Four Color Problem - Assaults and Conquest*, McGraw-Hill New York, 1977.

[202] Sachs H., *Einfuhrung in die Theorie der endlichen Graphen I, II*, Teubner Verlag, Leipzig, 1972.

[203] Sačkov V. N., *Kombinatornie metodi diskretnoi matematiki*, Nauka, Moskva, 1977.

[204] Sačkov V. N., *Verojatnostnie metodi v kombinatornom analize*, Nauka, Moskva, 1978.

[205] Sačkov V. N., *Vvedenie v kombinatornie metodi diskretnoj matematiki*, Nauka, Moskva, 1982.

[206] Sarapa N., *Teorija vjerojatnosti*, Školska knjiga, Zagreb, 1987.

[207] Saveljev L. J., *Kombinatorika i verojatnost*, Nauka, Novosibirsk, 1975.

[208] Seshu S., Read M. B., *Linear Graphs and Electrical Networks*, Addison-Wesley, Reading, Mass., 1961.

[209] Stanley R. P., *Enumerative Combinatorics I*, Wadsworth, Monterey, Calif., 1986.

[210] Stanley R. P., *Combinatorics and Commutative Algebra*, Birkhäuser, Boston, 1983.

[211] Stanton D., White D., *Constructive Combinatorics*, Springer Verlag, New York, 1986.

[212] Stone H. S., *Discrete Mathematical Structures and their Applications*, Science Research Assoc., Chicago, 1973.

[213] Swamy M. N., Thulasiraman K., *Graphs, Networks and Algorithms*, John Wiley & Sons, New York, 1981. (ruski prijevod Mir, Moskva, 1984.)

[214] Širjajev A. N., *Verojatnost*, Nauka, Moskva, 1980. (engleski prijevod Springer Verlag, New York, 1985.)

[215] Tarakanov V. E., *Kombinatornie zadači i (0, 1)-matrici*, Nauka, Moskva, 1985.

[216] Tarjan R., *Data Structures and Networks Algorithms*, CBMS Series in Appl. Math. vol. 44, Amer. Math. Soc., Providence R. I., 1985.

[217] Todd M. J., *The Computation of Fixed Points and Applications*, Springer Verlag, New York, 1976. (ruski prijevod Nauka, Moskva, 1983.)

[218] Tomescu I., *Problems in Combinatorics and Graph Theory*, John Wiley & Sons, New York, 1985.

[219] Tončev V. D., *Kombinatornie konfiguratsii*, Nauka i Izkustvo, Sofia, 1984.

[220] Trinajstić N., *Chemical Graph Theory*, CRC Press, Boca Raton Fla., 1983.

[221] Tucker A., *Applied Combinatorics*, John Wiley & Sons, New York, 1984.

[222] Tutte W. T. *Graph Theory*, Addison-Wesley, Reading, Mass., 1984. (ruski prijevod Mir, Moskva, 1988.)

[223] Tutte W. T. (Ed.), *Recent Progress in Combinatorics*, Academic Press, New York, 1969.

[224] Veljan D., *Konačna matematika*, skripta, Sveučilište u Zagrebu, Zagreb, 1986.

[225] Vilenkin N. J., *Kombinatorika*, Nauka, Moskva, 1969.

[226] Vorobjev N. N., *Čisla Fibonači*, Popularnie lekcii mat. 6, Nauka, Moskva, 1969.

[227] Wallis W. D., *Combinatorial Designs*, Marcel Dekker, New York, 1988.

[228] Walter P., *An Introduction to Ergodic Theory*, Grad. Text. Math. vol. 79, Springer Verlag, New York, 1982.

[229] Walther H., *Ten Applications of Graph Theory*, Reidel, Amsterdam, 1985.

[230] Welsh D. J. A., *Matroid Theory*, Academic Press, New York, 1976.

[231] White A. T., *Graphs, Groups and Surfaces*, North Holland, Amsterdam, 1984.

[232] Wilf H. S., *Algorithms and Complexity*, Prentice-Hall, Englewood Cliffs, N. J., 1986.

[233] Williams N. H., *Combinatorial Set Theory*, North Holland, Amsterdam, 1977.

[234] Williamson S. G., *Combinatorics for Computer Science*, Computer Science Press, Rockville, Md., 1985.

[235] Wilson R. J., *Introduction to Graph Theory*, Longman, Harlow, Essex, 1985. (ruski prijevod 1. izd. Mir, Moskva, 1977.)

[236] Zykov A. A., *Osnovy teorii grafov*, Nauka, Moskva, 1987.

[1*] R. Ahuja, T. Magnanti, J. Orlin, *Network Flows: Theory, Algorithms and Applications*, Prentice Hall, Englewood Cliffs, N. J., 1993.

[2*] M. Aigner, G. Ziegler, *Proofs from THE BOOK*, Springer Verlag, Berlin, 1999.

[3*] N. Alon, J. Spencer, *The Probabilistic Method*, John Wiley, New York, 2000.

[4*] V. Arnold, M. Atiyah, P. Lax, B. Mazur (Eds.), *Mathematics: Frontiers and Perspectives*, Int. Math. Union /Amer. Math. Soc., 2000.

[5*] J. Anderson, J. Bell, *Discrete Mathematics with Combinatorics*, Prentice Hall, New York, 2000.

[6*] B. Andrasfai, *Graph Theory: Flows, Matrices*, Akadèmiai Kiadó, Budapest, 1991.

[7*] V. K. Balakrishnan, *Network Optimization*, Chapman and Hall, New York, 1995.

[8*] V. K. Balakrishnan, *Schaum's Outline of Theory and Problems of Combinatorics*, McGraw-Hill, New York 1995.

[9*] L. Batten, *Combinatorics of Finite Geometries*, Cambridge University Press, Cambridge, 1997.

[10*] J. Baylis, *Error Correcting Codes*, CRC Press, Boca Roton, 1998.

[11*] E. A. Bender, S. G. Williamson, *Foundations of Applied Combinatorics*, Addison Wesley, New York, 1991.

[12*] E. R. Berlekamp, *Algebraic Coding Theory*, McGraw Hill, New York, 1986.

[13*] E. R. Berlekamp, J. H. Conway, R. K. Guy, *Winning Ways for Your Mathematical Plays, Vol. I, II*, Academic Press, New York, 1982.

[14*] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, Cambridge University Press, Cambridge, 2000.

[15*] A. Björner, M. Las Vergnas, B. Sturmfels, N. White, G. Ziegler, *Oriented Matroids*, Cambridge University Press, Cambridge, 1993.

[16*] B. Bollobás, *Graph Theory. An Introductory Course*, Springer Verlag, Berlin, 1990.

[17*] B. Bollobás, *Combinatorics*, Cambridge University Press, Cambridge, 1986.

[18*] B. A. Bondarenko, *Generalized Pascal Trinagles and Pyramids*, The Fibonacci Assoc., Santa Clara, 1993.

[19*] G. Bredon, *Topology and Geometry*, Springer Verlag, New York, 1993.

[20*] R. Brualdi, H. Ryser, *Combinatorial Matrix Theory*, Cambridge University Press, Cambridge, 1991.

[21*] P. Cameron, *Combinatorics: Topics, Techniques, Algorithms*, Cambridge University Press, Cambridge, 1994.

[22*] F. Chung, R. Graham, *Erdős on Graphs*, AK Peters Ltd., London, 1999.

[23*] J. Conway, *Sphere Packings, Lattices and Groups*, Springer Verlag, New York, 1998.

[24*] J. H. Conway, R. K. Guy, *The Book of Numbers*, Springer Verlag, New York, 1986.

[25*] R. Crandall, *Projects in Scientific Computation*, Springer Verlag, New York, 2000.

[26*] R. Crandall, *Topics in Advanced Scientific Computations*, Springer Verlag, New York, 1996.

[27*] M. Cvitković, *Kombinatorika, zbirka zadataka*, Element, Zagreb, 1994.

[28*] R. Diestel, *Graph Theory*, Springer Verlag, Berlin, 1996.

[29*] A. Dujella, *Fibonaccijevi brojevi*, Hrv. Mat. Društvo, Zagreb, 2000.

[30*] M. Erickson, *Introduction to Combinatorics*, John Wiley, New York, 1996.

[31*] P. Flajolet, R. Sedgewick, *Analytic Combinatorics*, u pripremi

[32*] I. M. Gelfand, M. M. Kapranov, A. V. Zelevinsky, *Discriminants, Resultants and Multidimensional Determinants*, Birkhäuser Boston, Cambridge, Mass., 1994.

[33*] C. Godsil, *Algebraic Combinatorics*, Chapman and Hall, New York, 1993.

[34*] J. E. Goodman, J. O'Rourke, (Eds.), *Handbook of Discrete and Computational Geometry*, CRC Press, Boca Raton, 1997.

[35*] R. Graham, M. Grőtschel, L. Lóvasz (Eds.), *Handbook of Combinatorics, I, II*, Elsevier, Amsterdam, 1995.

[36*] R. Graham, J. Nešetřil (Eds.), *The Mathematics of Paul Erdős*, Springer Verlag, New York, 1996.

[37*] G. R. Grimmet, D. R. Stirzaker, *Probability and Random Processes*, Oxford University Press, Oxford, 1992.

[38*] J. L. Gross, J. Yellen, *Graph Theory and its Applications*, CRC, Boca Raton, 1999.

[39*] B. Grünbaum, G. C. Shephard, *Tilings and Patterns*, W. H. Freeman, New York, 1987

[40*] J. Harris, *Combinatorics and Graph Theory*, Springer Verlag, New York, 2000.

[41*] P. Hoffman, *The Man Who Loved Only Numbers*, Hyperion, New York, 1998.

[42*] M. Hofri, *Analysis of Algorithms*, J. Wiley, New York, 1996.

[43*] A. Kerber, *Algebraic Combinatorics via Finite Group Actions*, Wissenschaftsverlag, Mannheim/Wien/Zürich, 1991.

[44*] N. Koblitz, *A Course in Number Theory and Cryptography*, Springer Verlag, Berlin, 1994.

[45*] D. L. Kreher, D. R. Stinson, *Combinatorial Algorithms*, CRC Press, Boca Roton, 1999.

[46*] T. R. Jensen, B. Toft, *Graph Coloring Problems*, J. Wiley, New York, 1995.

[47*] M. Juvan, P. Potočnik, *Teorija grafov in kombinatorika, Primeri in rešene naloge*, DMFA Slovenije, Ljubljana, 2000.

[48*] C. C. Lindner, C. A. Rodger, *Design Theory*, CRC Press, Boca Raton, 1997.

[49*] J.H. van Lint, R.M. Wilson, *A Course in Combinatorics*, Cambridge University Press, Cambridge, 1996.

[50*] J. Matoušek, J. Nešetřil, *Invitation to Discrete Mathematics*, Oxford University Press, Oxford, 1998.

[51*] O. V. Melnikov (Ed.), *Exercises in Graph Theory*, Kluwer, Amsterdam, 1998.
[52*] D. Miklós, V. T. Sös, T. Szönyi (Eds.), *Combinatorics, Paul Erdös is Eighty, I, II*, J. Bolyai Math. Soc., Budapest, 1993.
[53*] B. Mohar, C. Thomassen, *Graphs on Surfaces*, John Hopkins University Press, Baltimore, Md., 1997.
[54*] J. G. Oxley, *Matroid Theory*, Oxford University Press, Oxford, 1992.
[55*] J. Pach, P. K. Agarwal, *Combinatorical Geometry*, John Wiley, New York, 1995.
[56*] B. Pavković, D. Veljan, *Elementarna matematika I/II*, Tehnička knjiga/Školska knjiga, Zagreb, 1992./1995.
[57*] M. Petkovšek, H. Wilf, D.Zeilberger, *A=B*, AK Peters Ltd., Wellesley, Mass., 1996.
[58*] K. Roman, *An Introduction to Coding and Information Theory*, Springer Verlag, New York, 1996.
[59*] K. Rosen, *Elementary Number Theory and its Application*, Addison Wesley, Reading, Mass., 1993.
[60*] K. Rosen (Ed.), *Handbook of Discrete and Combinatorial Mathematics*, Chapman and Hall / CRC Press, Boca Raton, 2000.
[61*] B. Sagan, *The Symmetric Group*, Wadsworth & Brooks / Cole, Pacific Grove, Ca, 1991.
[62*] A. Schrijver, *Theory of Linear and Integer Programming*, John Wiley, New York, 1986.
[63*] J. Seberry, J. Pieprzyk, *Cryptography. An Introduction to Computer Science*, Prentice Hall, New York, 1989.
[64*] R. Sedgewick, P. Flajolet, *An Introduction to the Analysis of Algorithms*, Addison-Wesley, Reading, Mass., 1996.
[65*] R. Stanley, *Enumerative Combinatorics, Vol.2*, Cambridge University Press, Cambridge, 1999.
[66*] J. Stillwell, *Classical Topology and Combinatorical Group Theory*, Springer Verlag, New York, 1980.
[67*] D. R. Stinson, *Cryptography. Theory and Practice*, Chapman and Hall/CRC, New York, 2000.
[68*] D. Thoro, B. Jackson, *Applied Combinatorics with Problem Solving*, Addison-Wesley, New York, 1990.
[69*] W. Thurston, *Three Dimensional Geometry and Topology*, Princeton University Press, Princeton, NJ., 1997.
[70*] W. Trotter, *Combinatorics and Partially Ordered Sets*, John Hopkins University Press, Baltimore, Md., 1992.
[71*] S. Vajda, *Fibonacci and Lucas Numbers and Golden Section, Theory and Application*, Ellis Horwood, Chicester, 1989.
[72*] D. Welsh, *Codes and Cryptography*, Oxford University Press, Oxford, 1989.
[73*] H. Wilf, *Generatingfunctionology*, Academic Press, New York, 1994.
[74*] R. J. Wilson, J. J. Watkins, *Graphs. An Introductory Approach*, J. Wiley & Sons, New York, 1990.
[75*] G. Ziegler, *Lectures on Polytopes*, Springer Verlag, Berlin, 1995.
[76*] D. Žubrinić, *Diskretna matematika*, Element, Zagreb, 1997.

Indeks

Abelovi identiteti, 209
acikličan digraf, 275
aciklički graf, 258
aksiom izbora, 29
alfabet, 232
algebarski formalni red, 222, 233
algebarski jezik, 233
algebra, 24
algebra incidencije, 162
algoritam, 7, 24, 25
alternirajući put, 329
anagram, 76
analiza algoritama, 26
antilanac, 158, 159
aranžman, 350
argument, 17
asimptotsko ponašanje, 26
atom, 161

Bellov broj, 102, 193
Bergeov teorem o maksimalnom sparivanju, 329
Bernoullijevi brojevi, 216
Bertrandov problem glasovanja, 134
beskonačan skup, 19
Besselova funkcija, 210
bijekcija, 19
bijektivni dokaz, 47
bijektivni skupovi, 19
binarna operacija, 18
binarna relacija, 16
binarni broj, 49
binarno pretraživanje, 132
binarno stablo, 134
Binet-Cauchyjeva formula, 269
Binetova formula, 120
binomna formula, 78
binomna inverzija, 140
binomna konvolucija, 187
binomna parcijalna suma, 187
binomne formule
  poopćene, 209
binomni koeficijent, 61, 93
binomni red, 88
  poopćeni, 206
binomni teorem, 78
biparticija, 236
Birkhoff-von Neumannov teorem, 335
bit, 49
Blanušin graf, 300
Blissardov simbolični račun, 217
blok dizajn, 359
  trivijalni, 360
blok grafa, 290
blok particije, 20, 99
božanski omjer, 117
bojenje po listama, 325
Bollobásov teorem, 284
Bondyjev teorem, 285
Bondyjeva lema, 304
Bonferronijeve nejednakosti, 155
Booleova algebra, 164
Booleova funkcija, 49
Borsuk-Ulamov teorem, 247
breadth-first search tree, 272
brid grafa
  kontraktiran, 241
  pravi, 235
bridna povezanost $\kappa'(G)$, 289
bridni pokrivač, 328
bridni rez, 264, 289
bridno k-bojenje, 295
bridno disjunktna familija diputova, 289
bridno kromatski broj $\gamma'(G)$, 296
bridno-tranzitivan graf, 243
broj elemenata konačnog skupa, 44
broj permutacija s ponavljanjem, 76
broj uspona permutacije, 107
Brooksov teorem, 298
Brouwerov teorem o fiksnoj točki, 245
Bruck-Chowla-Ryserov teorem, 363
byte, 49

Camionov teorem, 287
Cantor, 29
Cassinijev identitet, 118
Cassinijevi ovali, 118
Catalanov broj, 74, 133
  poopćeni, 206
  poopćeni, 139
Cauchy-Schwartzova nejednakost, 30
Cauchyjev identitet, 57, 390

Cayleyev teorem, 59, 265
Cayleyeva šuma, 200
Cayleyeva stabla, 199
Chvátal-Erdösov teorem, 293
Chvatálov teorem, 284
ciklička permutacija, 54
ciklička strana, 310
ciklički niz, 166
ciklički rastav grafa, 258
ciklički rastav permutacije, 54
ciklički tip permutacije, 56
ciklus
    trivijalni, 54
    usmjereni, 275
ciklus grafa, 41, 236
ciklus permutacije, 54
cjelobrojna mreža, 64
Clausenov ${}_4F_3$ identitet, 212
Coxeterov graf, 282

Čebiševljeva nejednakost, 30
Čebišljev polinom prve vrste, 253
Čebišvljev polinom druge vrste, 253
ćelijski kompleks, 321
čvor, 38

d-poliedar, 172
de Morganove formule, 15
debljina grafa, 307
defekt grafa, 333
Dehn-Sommervilleove jednakosti, 173
depth-first search tree, 272
deranžmani, 146
diciklus, 275
diedarska grupa, 239
diferencijabilno konačan (D-konačan) red potencija, 224
diferencijalna jednadžba za hipergeometrijske redove, 212
diferencijska jednadžba, 127
digraf, 274
    pridruženi, 275
    striktni, 275
dijagonala 0-1 matrice, 334
dijagram toka, 25
dijametar grafa, 250
Dilworthov teorem, 159, 304
dimenzija simplicijalnog kompleksa, 171
dimeri, 333
Dinitzov problem, 326
diput, 275
Diracov teorem, 283, 340
direktan luk puta, 353
direktna suma p.u. skupova, 161
direktni prethodnik, 20
direktni produkt, 15, 161
direktni sljedbenik, 20
Dirichletov princip, 31
Dirichletova funkcija izvodnica, 217
disjunktni skupovi, 15
diskretan, 3
diskretno uređen skup, 20
distributivna rešetka, 161
Dixonov ${}_3F_2$ identitet, 211
dobro uređen skup, 17
događaj prostora vjerojatnosti, 343
domena, 17
donja međa, 16
drvo, 5, 41
dualni graf, 311
"dvanaest načina za broj funkcija", 109
dvostruki faktorijeli, 58
dvostruko stohastička matrica, 334
Dyckov jezik, 233
Dyckov put, 134
Dyckova riječ, 233

Edmondsov teorem, 370
EFI, 177
efikasan algoritam, 27
eksponencijalna formula, 198
eksponencijalna funkcija izvodnica (EFI), 177
eksponencijalni algoritam, 272
eksponencijalni Bellovi polinomi, 219
eksponencijalni red
    poopćeni, 206
ekstenzija, 18
ekvipotentni skupovi, 19
element, 14
Eratostenovo sito, 143
Erdös-de Bruijnov teorem, 317
Erdös-Füredijev teorem, 348
Erdös-Faber-Lovászova slutnja, 299
Erdös-Gallai-Sylvesterov teorem, 11, 316
Erdös-Ko-Rado teorem, 347
Erdös-Stoneov teorem, 343
Erdös-Szekereszov teorem, 39
Erdösov teorem o Ramseyevim brojevima, 344
Erdösova slutnja, 41
Euklidov algoritam, 25
Eulerov broj permutacije, 107
Eulerov graf, 277
Eulerov p.u. skup, 175
Eulerov teorem o particijama, 98, 182
Eulerova formula, 312
Eulerova funkcija $\varphi(n)$, 145
Eulerova karakteristika, 171, 258, 312, 321
Eulerova konstanta, 129
Eulerova staza, 278
Eulerova tura, 277
Eulerovi brojevi za permutacije, 107

f-polinom politopa, 174
f-vektor politopa, 171, 172
Fáryjev teorem, 319
Faá di Brunova formula, 219
faceta, 172
faktorijel, 21, 52
familija podskupova, 15
Fanov hipergraf, 277, 362
Ferrerov dijagram, 98, 383
FI, 177
Fibonaccijevi brojevi, 73, 115
fiksna točka, 146
filotaksa, 117
Fischerova nejednakost, 360
Fleuryjev algoritam, 280
f-nezasićen put, 353
Ford-Fulkersonov algoritam za maksimalni protok, 356
Ford-Fulkersonov teorem, 354
forma, 72
formalna derivacija, 24, 178
formalni integral, 24, 178
formalni jezik, 233
formalni red potencija, 23, 232
formalni red u n varijabli, 24
formula dualiteta za h-polinome, 174
formula inverzije, 163
formula uključivanja-isključivanja (FUI), 143
f-rastući put, 353
Frobeniusov teorem, 248
Fruchtov teorem, 239
funkcija, 17
funkcija incidencije, 162
funkcija izbora, 29
funkcija izvodnica, FI, 177
funkcija ranga, 159
funkcijski p.u. skup, 162
f-zasićen put, 353

Gallai-Milgramov teorem, 304
Gallai-Royov teorem, 303
Gallaijev teorem, 328
gama funkcija, 61, 211
Gaussov ${}_2F_1$ identitet, 211
Gaussova formula, 165
Gaussova inverzija, 141
Gaussova krivulja, 95
Gaussovi binomni koeficijenti, 95
genus grafa, 310
genus plohe, 309
geometrijska rešetka, 168
geometrijska realizacija, 171
glavni uređajni ideal, 161
Golayev binarni kôd, 366
gornja međa p.u. skupa, 17, 161
Grötzschov graf, 296
graduirani lanac, 159
graf, 4, 38, 41, 235
    d-regularan, 241
    automorfizam, 239
    beskonačan, 235
    bipartitan, 236
    bridovi, 41, 235
    dvodijelni, 236
    izomorfizam, 235
    izomorfni, 41, 235
    jednostavan, 41, 235
    komplementarni, 239
    konačan, 235
    krajevi bridova, 235
    kubni, 236
    minora, 241
    nepovezan, 250
    netrivijalan, 235
    potpun, 236
    povezan, 41, 250
    prazan, 235
    regularan, 241
    stupanj, 241
    trivijalan, 235
    usmjereni, 43
    vrhovi, 41, 235
graf dodekaedra, 280
graf incidencije hipergrafa, 277
graf Mycielskog, 297
graf permutacije, 153
graf poliedra, 314
graf politopa, 315
grafički niz brojeva, 243
gust skup, 35

h-polinom politopa, 174
h-vektor, 174
Hadamardov produkt, 223
Hadamardova matrica, 366
Hadwigerova slutnja, 299
Hallov teorem o sparivanju, 330
Hamiltonov ciklus, 280
Hamiltonov graf, 280
Hamiltonov put, 280
    usmjereni, 286
Hammingova ograda, 89
Hammingova udaljenost, 88, 366
Hararyjev teorem, 294
Hardy-Ramanujanova asimptotska formula, 98
harmonijski broj, 128, 182
Hasseov dijagram, 158
Hauptvermutung, 321
Heawoodov graf, 277
Heawoodov teorem, 324
Heronov algoritam, 130

Herschelov graf, 281
hiperbrid, 276
hiperbridovi, 89
hipergeometrijski red, 210
hipergeometrijski red potencija, 90
hipergraf, 89, 276
homogen polinom, 72
homogena rekurzija, 126

identiteta, 18
incidentnost vrha i brida, 41
infimum, 16, 161
injekcija, 19
inkluzija, 15, 18
instancija problema, 273
instupanj, 275
interval, 17
inverz, 19
inverzija permutacije, 59
inverzna slika, 18
inverzno preslikavanje, 19
izomorfni grafovi, 41
izračunljiv niz, 25
izvor transportne mreže, 351

Jacobi-Trudijev identitet, 390
jaka komponenta, 275
jaka lučna povezanost digrafa $\kappa'(D)$, 289
jaka povezanost digrafa $\kappa(D)$, 289
jako k-povezan digraf, 289
jako lučno povezan digraf, 289
jako povezan digraf, 275
jednostavan graf, 41
jednostavna krivulja, 307
jezgra digrafa, 276
jezgra preslikavanja, 20, 101
Jordanov teorem, 307
Jordanova krivulja, 307

k-bridno povezan graf, 289
k-knjiga, 308
k-kritičan graf, 295
k-obojivost, 295
k-strana, 170
König-Egerváryjev teorem, 330
Königov teorem, 255
kôd, 366
kapacitet okoliša, 130
kapacitet reza transportne mreže, 352
karakteristična funkcija, 18, 48
karakteristična jednadžba rekurzije, 122
karakteristični korijeni rekurzije, 122
karakteristični polinom grafa, 252
karakteristični polinom p.u. skupa, 168
kardinalni broj, 19, 44
kardinalnost multiskupa, 69
karika, 235
Kartezijev produkt, 15
k-bojenje vrhova, 295
k-ciklička permutacija, 54
k-ciklus, 54
Kekuléova struktura, 328
Kempeov lanac, 301
Keplerova slutnja, 319
kičma grafa, 263
Kirchhoffov zakon, 124, 351
Kirkmanov problem 15 učenica, 359
Kirkmanovi sustavi trojki, 362
klika, 240, 340
Kneserov graf, 300
koatom, 168
kodiranje s ispravljanjem, 89
kodomena, 17
Koebeov teorem, 318
koeficijenti formalnog reda, 23
koeficijenti polinoma, 22
Kohov digraf, 276
kombinacija bez ponavljanja, 61
kombinacija s ponavljanjem, 61
kombinatorika, 2
kombinatorna eksplozija, 50
kombinatorni dizajni, 9
kombinatorni dokaz, 47
kompleks susjedstva, 301
komplement, 15
komponenta digrafa, 275
komponenta grafa, 250, 335
kompozicija preslikavanja, 18
kompozicijski inverz, 202
konačan graf, 41
konačna afina ravnina, 364
konačna projektivna ravnina, 364
konačne aritmetike, 9
konačni multiskup, 69
konjugirana particija, 99
kontaktni graf, 318
kontekstno-slobodan jezik, 233
konveksna kombinacija matrica, 334
konveksni d-politop, 172
konvolucija, 162
korijen polinoma, 22
korijen stabla, 134, 198, 199
korijenska šuma, 270
korub, 289
kosa Schurova funkcija, 391
Kostkin broj, 390
    kosi, 391
kotač, 306
Kotzigova slutnja, 258
k-particija, 20
kratnost u multiskupu, 69
kromatski broj $\gamma(G)$, 295
kromatski broj plohe, 327
kromatski polinom, 306
Kruskalov algoritam, 274
kubni graf, 236
Kummerov ${}_2F_1$ identitet, 211
Kuratowski-Pontrjaginov teorem, 319
Kuratowskijev teorem, 319
kvocijentni skup, 16
kvocijentno preslikavanje, 18

lûk u digrafu, 43, 274
Lagrangeov identitet, 30
Lagrangeova formula inverzije, 203
lanac, 158, 159
Laplaceova transformacija, 187
latinski kvadrat, 8, 332
latinski pravokutnik, 332
Laurentov formalni red, 203
leksikografski uređaj, 55
lema o lepezi, 293
lema o listovima, 258
lema o rukovanju, 42, 242
linearna homogena rekurzija, 122
linearni kôd, 366
linearni uređaj, 16
linearno programiranje, 27
linearno uređen skup, 158
linijski graf, 297
Lipton-Tarjanov teorem, 319
list stabla, 199
listno kromatski broj, 325
Littlewood-Offordov problem, 161
Littlewood-Richardsonov koeficijent, 392
log-konkavnost, 94
log-konveksnost, 94
logistička diferencijalna jednadžba, 130
logistička jednadžba, 129
lokalno konačan p.u. skup, 158
Lovászov teorem, 301
Lucasovi brojevi, 120
LYM-nejednakost, 160

m-arno stablo, 199
MacLaneov teorem, 324
Maclaurinov red, 23
MacMahonov teorem, 152
magična suma, 7
magični kvadrat, 7, 31
majorizirani niz, 285
maksimalan element p. u. skupa, 157
maksimalan protok transportne mreže, 351
maksimalno sparivanje, 328
maksimum, 17
mali Fermatov teorem, 87
Mantelov teorem, 261
Markovljeva nejednakost, 344
Mathieuova grupa, 366
matrični teorem o stablima, 268
matrica
    incidencije, 238
    susjedstva, 238
matrica relacije, 31
matrica susjedstva digrafa, 275
matroid, 367
"max-flow min-cut" teorem, 354
mađarska metoda, 339
Mengerov teorem, 38, 289, 333, 355
mergesort, 189
metoda kreativnog teleskopiranja, 214
metoda sita, 143
minimalan element p. u. skupa, 157
minimalni rez transportne mreže, 352
minimum, 17
minora grafa, 320
Möbiusova traka, 309
Möbiusova formula inverzije, 163
Möbiusova funkcija, 163
modularna rešetka, 161
monom, 23
Motzkinov broj, 227
Motzkinov put, 227
multinomna Pascalova formula, 85
multinomni koeficijent, 76
multinomni teorem, 85
multiplicitet $\mu(G)$, 301
multiskup, 69

Nörlundova formula, 81
nadgraf, 240
nadovezivanje šetnji, 250
nadskup, 15
nadstrana politopa, 172
najmanja gornja međa, 17
Narayanin broj, 137
nasljednici, 199
n-člani skup, 20
n-dimenzionalna (jedinična) sfera, 247
nekomutativni polinom, 232
nekomutativni racionalni red, 232
neparna komponenta grafa, 335
neplanaran graf, 306
neprekidni razlomci, 118
Newtonova lema, 106
nezasićen vrh, 328
nezavisna varijabla, 17
niz, 21
niz inverzija permutacije, 59
niz stupnjeva grafa, 243
normirani polinom, 22
nosač formalnog reda, 233
NP-klasa, 273
NP-potpuni problemi, 273

NP-teški problemi, 273
nulpolinom, 22
nultočka, 22

očekivanje slučajne varijable, 343
obostrano jednoznačno preslikavanje, 19
obrnuti luk puta, 353
obrnuto čitanje, 393
odozgo omeđen skup, 17
$O(f(n))$-algoritam, 27
Ohmov zakon, 124
omeđen skup, 16
opće rješenje linearne homogene rekurzije s konstantnim koeficijentima, 123, 125
opći binomni koeficijent, 81
opći položaj hiperravnina, 111
operator diferencije, 127
optimalna tura, 280
Oreov teorem, 284
original, 18
orijentabilna ploha, 309
orijentacija grafa, 274
orijentirani graf, 43
ortogonalni latinski kvadrati, 8
osnovni teorem aritmetike, 46
otac vrha stabla, 199, 272
outstupanj, 275

P-rekurzivna funkcija, 225
p.u. skup, 157
padajuća potencija, 51
padajući faktorijel, 51
pakiranje bridova, 328
pakiranje vrhova, 328
parcijalni uređaj, 16, 157
parcijalno (djelimično) uređen skup, 157
parna komponenta grafa, 335
particija broja, 97, 181
particija inducirana preslikavanjem, 20
particija skupa, 99
partikularno rješenje rekurzije, 126
partitivni skup, 15
Pascalov trokut, 67
Pascalova formula, 65
permanenta matrice, 338
permutacija, 52
permutacija multiskupa, 75
permutacijska matrica, 334
Petersenov graf, 238, 282, 300
petlja, 41, 235
Pfaffov reciprocitet, 212
Pickova formula, 317
Pitagorin poučak
    poopćeni, 270
P-klasa, 273
planaran graf, 306
Platonova tijela, 315
početni uvjeti rekurzije, 110
podgraf, 38, 41, 240
    induciran bridovima, 240
    inducirani, 240
    pravi, 240
    presjek, 240
    razapinjajući, 240
    unija, 240
podijeli pa ovladaj, 131
podmultiskup, 70
područje definicije funkcije, 17
područje vrijednosti funkcije, 17
podskup, 15
    pravi, 15
podstablo, 198
pohlepni algoritmi, 274
pokrivač grafa, 328
polinom, 22
polinom sparivanja, 337
polinomski algoritam, 27, 272
polinomski rekurzivna funkcija, 225
polustandardna Youngova tablica (SSYT), 390
ponderirana sredina, 30
ponor transportne mreže, 351
poopćena Vandermondeova determinanta, 125
poopćeni FUI, 149
popločavanje šahovske ploče, 3
populacijska jednadžba, 129
Pósin teorem, 285
potpun $(r-1)$-partitni graf, 341
potpun graf, 38
povezan graf, 250
povezanost $\kappa(G)$, 289
prava strana, 172
pravi algebarski sustav jednadžbi, 232
pravilno bojenje, 295
pravilo bijekcije, 44
pravilo produkta, 44
pravilo računanja, 25
pravilo sume, 44
prazan skup, 14
presječna familija, 347
presječni broj, 307
presječni graf, 298
presjek, 15
preslikavanje 1–1, 19
preslikavanje, 17
preslikavanje na, 19
prethodnik, 199
priječnica, 331
Primov algoritam, 273
princip definicije indukcijom, 21
princip matematičke indukcije, 20
princip zrcaljenja, 73
pripadna homogena rekurzija, 126
pripadni graf, 275
prirodna projekcija, 18
proširenje, 18
probléme des ménages, 154
probléme des recontres, 146
problem 36 časnika, 8
problem četiri boje, 324
problem četiriju boja, 9
problem binarnih stabala, 134
problem dimera, 4
problem Dyckovih putova, 134
problem Königsberških mostova, 6
problem kineskog poštara, 280
problem konjićevog skoka, 281
problem konstrukcije komunikacijske mreže, 294
problem odluke, 273
problem optimalnog zapošljavanja, 339
problem pakiranja, 318
problem permutacija sa zabranjenim pozicijama, 153
problem putova u cjelobrojnoj mreži, 134
problem razmnožavanja zečeva, 114
problem rekonstrukcije, 241
problem sortiranja, 189
problem spajanja, 274
problem trgovačkog putnika, 281
problem triangulacije, 133
problem zagrada, 133
problem zapošljavanja, 338
produkt brojeva, 21
produktna formula za Möbiusovu funkciju, 164
profinjenje particije, 158
program, 25
projekcija, 18
prosječna složenost, 26
prostor bridova, 324
prostor ciklusa, 324

q-binomna formula, 169
q-binomna inverzija, 141
q-binomni koeficijenti, 95
q-Catalanov broj, 139
q-faktorijel, 96
q-multinomni koeficijent, 97
q-Pascalova formula, 97
quicksort, 189

r-kombinacija s ponavljanjem tipa $(K_1, \ldots, K_n)$, 215
r-permutacija tipa $(K_1, \ldots, K_n)$, 216
Rédeijev teorem, 286
računarska metoda, 25
računarska stanja, 25
računarski postupak, 25
racionalan jezik, 233
racionalna funkcija izvodnica, 219
Ramseyev broj, 37, 344
Ramseyev teorem, 37, 41
Ramseyeva teorija, 37
Raneyeva lema, 137
rang 0-1 matrice, 334
rang konačnog p.u. skupa, 159
rast stabla, 259
rastav (kompozicija) prirodnog broja, 67
rastav skupa, 77
rastuća potencija, 51
rastući faktorijel, 51
ravninska particija broja, 393
ravninski graf, 306
razapinjuće stablo, 263
razlika
    simetrična, 15
razlika skupova, 15
r-bojenje skupa, 40
rešetka
    distributivna, 161
    modularna, 161
recipročnost za Stirlingove brojeve, 107
red dizajna, 360
reducirana Eulerova karakteristika, 171
refleksivna relacija, 16
regularni jezik, 233
rekurzija, 6, 110
rekurzivna formula, 21, 110
rekurzivna relacija, 6, 110
relacija
    antisimetrična, 16
relacija ekvivalencije, 16
relacija klasifikacije, 16
restrikcija preslikavanja, 18
rešetka, 161
retrakcija topološkog prostora, 248
rezni brid, 263
rezni vrh, 264
Richardsonov teorem, 276
Riemannova hipoteza, 218
Riemannova zeta funkcija, 218
Ringel-Youngsov teorem, 327
r-kombinacija s ponavljanjem, 70
r-kombinacija, 61
Robertson-Seymourov teorem, 320
rod grafa, 310
r-permutacija, 78
r-permutacija, 57
RSK-algoritam, 392
RSK-korespondencija, 392
rub simpleksa, 172
rub strane ravninskog grafa, 310

Saalschűtzov ${}_3F_2$ identitet, 211
savršeno pokrivanje dominima, 332
savršeno sparivanje grafa, 328
Schläflijev teorem, 113
Schurov teorem, 40
Schurova funkcija, 388, 389, 391
segment, 17, 158
sekundarna struktura, 229
separator, 333
separirajući skup u grafu, 289
sfera s ručkama, 308
Shannonov teorem, 302
shema relacija, 367
simbolička metoda, 196
simetrična funkcija, 382
    u-pozitivna, 385
    potpuno homogena, 385
simetrična grupa, 52
simetrična razlika, 15
simetrična relacija, 16
simetrični polinom, 382
simetrija binomnih koeficijenata, 65
simpleks, 170
simpleks metoda, 27
simplicijalna subdivizija, 245
simplicijalni kompleks, 171
simplicijalni politop, 172
sin vrha stabla, 199, 272
sistem diputova, 288
skoro trianguliran graf, 325
skup, 14
skup padova permutacije, 59
skup susjeda vrhova grafova, 330
skup uspona permutacije, 107
slabi rastav broja n, 68
slabo povezan digraf, 275
slika skupa, 18
složenost "najgoreg slučaja", 26
složenost algoritma, 26, 272
slučajna varijabla, 346
slučajni grafovi, 343
snarks, 300
sparivanje, 327
Spernerov teorem o antilancima, 159
Spernerova familija, 159
Spernerova lema o označavanju, 246
spoj disjunktnih grafova, 285
SSYT, 390
    veličina, 390
SSYT kosog oblika, 391
stabilan skup vrhova, 293
stabilnost grafa, 293
stabljika, 260, 275
stablo, 5, 41, 198
    neuređeno, 199
    ravninsko, 199
standardna transpozicija, 54
standardni ciklički zapis permutacije, 56
staza u grafu, 250
Steinerov sustav trojki, 362
Steinerovi sustavi, 362
Steinitzov teorem, 315
Stirlingov broj druge vrste, 100
Stirlingov broj prve vrste, 57
Stirlingov broj prve vrste s predznakom, 57
Stirlingov particijski broj, 100
Stirlingov trokut, 100
Stirlingova aproksimacija, 61
Stirlingova inverzija, 105, 141
Stirlingovi brojevi, 99
strana politopa, 170, 172, 310
Strassenovo brzo množenje matrica, 132, 252
striktni digraf, 275
struk grafa, 250
stupanj polinoma, 22
stupanj strane, 310
stupanj vrha grafa, 42, 241
suženje, 18
subdivizija brida, 291
subdivizija grafa, 291
subfaktorijel, 147
suma, 21
sume potencija, 387
supremum, 17, 161
surjekcija, 19
susjedni vrhovi, 41
sustav incidencija, 367
svojstvo apsorpcije binomnih koeficijenata, 65
Szemerédi-Trotterov teorem, 350

šetnja u grafu, 249
širina p.u. skupa, 159
šuma, 199

Taylorov red, 23
teleskopiranje, 111
teorem Balinskog, 315
teorem Grünbauma i Motzkina, 315
teorem o četiri boje, 324
teorem o braku, 331
teorem o klasifikaciji ploha, 308
teorem o prijateljstvu, 13, 255
"teorem o sendviču sa šunkom", 249
teorija algoritama, 26
teorija grafova, 6
težina brida, 273
težina podgrafa, 273
težinski graf, 273
Thomassenov teorem, 276
Thomassenov teorem o listnom bojanju, 325
topovski polinom, 153
torus, 36, 308
totalno uređen skup, 158
Touchardov teorem, 155
traženo stablo, 272
transportna mreža, 351
transpozicija, 54
transverzala familije skupova, 331
tranzitivna relacija, 16
triangulacija, 171, 245
trijadski broj, 50
Turánov graf, 341
Turánov teorem, 261, 342
turnir, 275
Tutteov graf, 300
Tutteov teorem o savršenim sparivanjima, 335
Tutteova slutnja, 300

ulaganje, 18
Ulamova slutnja, 241
umjetnost prebrojavanja, 45
unija, 15
unimodalan niz, 93
unutarnje disjunktna familija diputova, 289
unutarnji vrh, 199
uravnoteženi nepotpuni blok dizajn BIBD, 359
uređeni par, 15
uređajna suma p.u. skupova, 161
uređajni ideal p.u. skupa, 161
uređajni kompleks, 171
usmjerena Eulerova tura, 279
usmjereni graf, 43, 274
usmjereni Hamiltonov put, 286
usmjereni put, 275
uspon permutacija, 107
ušni rastav, 292
uvećani put, 329
uvjet cjelobrojnosti dizajna, 360

Van der Waerdenova slutnja, 338
van der Waredenov teorem, 40
Vandermondeova formula, 80
Vandermondeove konvolucije, 82
    poopćene, 209
varijacija, 57
VC-dimenzija, 89
Veblenov teorem, 258
veliki Fermatov teorem, 87
vez grafa, 264, 289
višestruki lukovi, 275
visina konačnog p.u. skupa, 159
Vizingov teorem, 301
vlakno preslikavanja, 18
vršni pokrivač, 328
vršni rez, 265, 289, 351
vršno-tranzitivan graf, 243
vrh, 38
    izolirani, 241
    list, 241
    stupanj, 42
    vanjski, 199
vrhovi
    incidentni, 235
    susjedni, 235
vrhunac unimodalnog niza, 93
vrijednost preslikavanja, 17
vrijednost protoka na transportnoj mreži, 351

Wagnerov teorem, 320
Whitneyev broj p.u. skupa, 168
Whitneyev teorem o 2-povezanosti, 290
Whitneyev teorem o planarnosti, 324
Wilsonov teorem, 363
Wittov dizajn, 366
WZ - metoda, 214

Youngov dijagram, 98, 383

zabranjene minore, 320
zabranjeni podgraf, 340
zakon asocijacije, 18
zakon recipročnosti za binomne koeficijente, 81
zasićen vrh sparivanja, 328
zatvarač grafa, 284
zatvorena jednostavna krivulja, 307
zavisna varijabla, 17
Zeckendorfov teorem, 118
Zermelov teorem, 29
zeta funkcija, 163
zlatni rez, 117
Zornova lema, 29

O autoru

Prof. dr. Darko Veljan diplomirao je na matematičkom odjelu Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu 1971. godine. Na istom je fakultetu magistrirao 1975., a doktorat znanosti stekao je 1979. na Cornell University, SAD. Darko Veljan je od 1971. godine neprekidno zaposlen na matematičkom odjelu PMF-a Sveučilišta u Zagrebu, gdje je sada redoviti profesor. Njegov znanstveni i stručni interes uključuje algebarsku topologiju, kombinatoriku, geometriju, nastavu matematike i drugo. O tome je objavio brojne znanstvene i stručne radove u zemlji i inozemstvu, sudjelovao na mnogim konferencijama iz područja matematike i njezinih primjena te posjetio mnoge sveučilišne centre. Autor je nekoliko sveučilišnih i srednjoškolskih udžbenika iz matematike. Član je Hrvatskog matematičkog društva, American Mathematical Society i drugih strukovnih udruženja.

.....

.....

.....

.....

Narodne novine d.d., Zagreb – (123) 110735
Oznaka za narudžbu: **UT-XI/11-8**