Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Ana Buljubašić

Teorija kodiranja i linearni kodovi

Završni rad

Osijek, 2015.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Ana Buljubašić

Teorija kodiranja i linearni kodovi

Završni rad

Voditelj: doc.dr.sc. Ivan Matić

Osijek, 2015.

Sažetak. U ovom završnom radu bavit ćemo se teorijom kodiranja, njenim osnovnim pojmovima te detaljnije proučiti neke vrste kodova.
U prvom dijelu opisat ćemo zašto je došlo do potrebe za razvojem ove teorije te koja je njena osnovna primjena. Također, definirat ćemo pojam kodiranje te ga primjeniti na primjerima.
U drugom dijelu rada detaljnije ćemo opisati blokovne kodove te definirati Hammingovu udaljenost i Hammingovu težinu koje su nam potrebne za daljnje proučavanje. Zatim, definiranjem polja i prostora uvest ćemo pojam linearnih kodova kojima ćemo se baviti najvećim dijelom rada. Opisat ćemo njihova svojstva te navedeno potkrijepiti primjerima.
U završnom dijelu rada opisat ćemo najpoznatiji linearni kod - Hammingov kod, njegova svojstva te pokazati na primjeru princip rada toga koda.

Ključne riječi: kodiranje, kodna riječ, blokovni kod, Hammingova udaljenost, Hammingova težina, linearni kod, generator matrica, kontrolna matrica, Hammingov kod

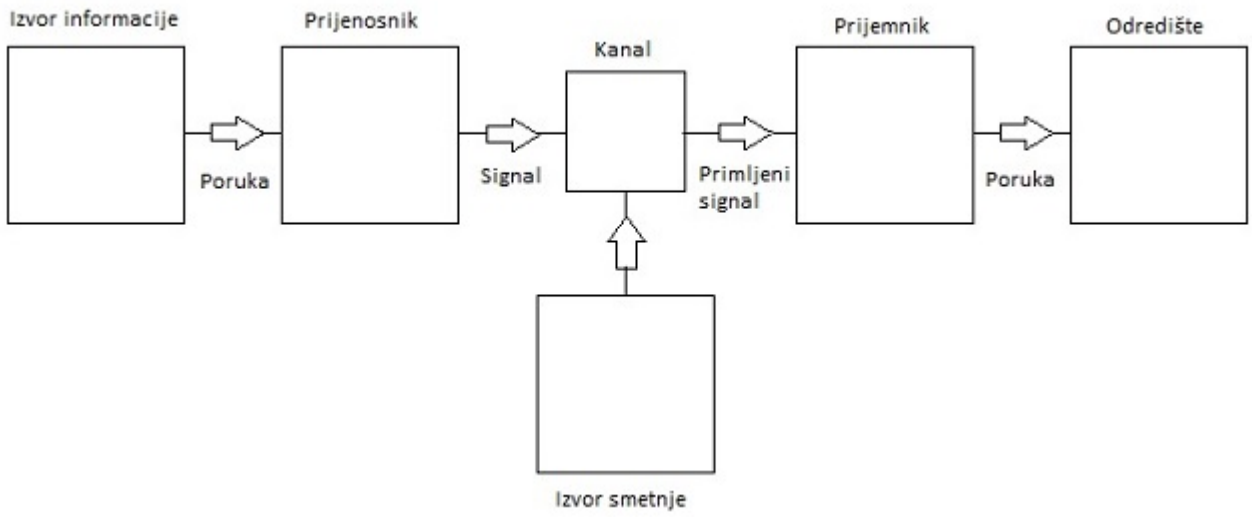
Abstract. In this final thesis we will deal with the coding theory, basic terms of coding and we will explain some of the code types in details.
In the first part we will describe why there was a need for the development of this theory and the main purpose of this theory. We will also define the term coding and use it on several examples.
In the second part we will explain block codes in details and define Hamming distance and Hamming weight which we will use in further study. Afterwards, by defining fields and spaces we will introduce the term of linear codes which are the main part of this thesis. We will describe their characteristics and corroborate them with examples.
In the final part of thesis we will describe most known linear code - Hamming code, explain code characteristics and demonstrate how it works on example.

Key words: Coding, codeword, block code, Hamming distance, Hamming weight, linear code, generator matrix, parity check matrix, Hamming code

Sadržaj

1 Uvod

U današnje digitalno i informacijsko doba učinkovit i pouzdan prijenos informacija vrlo je bitan, a oslanja se na metode grane matematike poznate kao teorija kodiranja.
Ova relativno nova znanost potiče od Claudea Shannona, američkog matematičara poznatog kao otac teorije informacija, i njegovog djela 'A mathematical Theory of Communication'. Teorija kodiranja i teorija informacija su srodne teorije koje za glavni cilj imaju učinkovitu i pouzdanu komunikaciju u često neprijateljskom okruženju, pri čemu prijenos mora zahtijevati što manju količinu vremena i napora.
Temelje ove znanosti uz Shannona postavio je Richard Hamming koji je istraživao ispravljanje pogrešaka kod tadašnjih računala i došao do prvih važnijih otkrića vezanih uz teoriju kodiranja.
Da bismo shvatili potrebu za kodiranjem, moramo se upoznati s osnovama komunikacije. Informacija (poruka) se prenosi od pošiljatelja (izvora) do primatelja (odredišta) kroz komunikacijski kanal pri čemu možemo birati na koji način ćemo strukturirati poslanu informaciju, ali ne možemo utjecati na ono što se događa unutar kanala tijekom prijenosa (Slika 1). Uzrokovano nekakvom smetnjom u kanalu, vrlo lako dolazi do pogreške koja može utjecati na točnost informacije koja stiže do primatelja. U svakodnevnom životu možemo to usporediti s, primjerice, razgovorom između osoba u bučnoj prostoriji, pri čemu zbog buke osoba može krivo čuti informaciju.



Slika 1: Shannonov komunikacijski model

Kako bismo smanjili mogućnost pogreške, dodajemo zalihost izvornoj poruci, odnosno dodatne informacije koje mogu pomoći u pronalaženju pogreške.
Idući primjer pokazat će jednu od najjednostavnijih metoda za otkrivanje pogreške.

Primjer 1.1. *Dodavanje bita parnosti Pretpostavimo da želimo poslati poruku u binarnom sustavu koja se sastoji od 7 bitova. Dodavanje bita parnosti znači da na kraj dodamo osmi bit čiju vrijednost odaberemo tako da ukupan broj nenul bitova bude paran. npr.* $0110010 \to 01100101$, $1100110 \to 11001100$.
Ukoliko dođe do pogreške tijekom prijenosa poruke, možemo ju uočiti jer će broj nenul bitova biti neparan. Nedostatak ovog načina otkrivanja pogreške je to što ne možemo sa sigurnošću reći koji bit je pogrešan, niti u slučaju više pogrešaka možemo prepoznati da je do pogreške uopće došlo.

Dakle, teorija kodiranja bavi se podacima koji se prenose kanalom sa smetnjama, ispravljanjem pogrešaka koje nastaju tijekom prijenosa, odnosno sprječavanjem istih, sve to koristeći se tehnikama ostalih grana matematike poput algebre i teorije brojeva.

Za početak, potrebno je definirati osnovne pojmove.

Definicija 1.2. *Neka su dani skupovi A (skup svih mogućih simbola izvorne poruke) i B (skup svih mogućih simbola koda). Kodiranje je pravilo koje svakom simbolu izvorne poruke pridružuje točno jednu riječ sastavljenu od simbola koda.*

Drugim riječima, kodiranje možemo opisati kao funkciju koja elementima skupa A pridružuje jedan ili više elemenata skupa B. Ono što dobijemo tim preslikavanjem kodirana je poruka, odnosno kod koji šaljemo kroz komunikacijski kanal.

Primjer 1.3. *Kodiranje ćemo nazvati binarno ako skup B sadrži dva simbola, B=$\{0,1\}$. Poruka 168 ima sljedeći kod: 110000011001001 (Tablica 1).*

Simbol	*Kodna riječ*
1	*11000*
2	*10100*
3	*01100*
4	*10010*
5	*01010*
6	*00110*
7	*10001*
8	*01001*
9	*00101*
0	*00011*

Tablica 1: Tablica kodnih riječi

Postupak pronalaženja originalne poruke x iz primljene poruke y naziva se dekodiranje. Kako je nemoguće navesti sve tipove kodiranja, u idućim poglavljima pokazat ćemo neke od najvažnijih.

2 Blokovni kodovi

Definicija 2.1. *Neka je F_q konačan skup koji sadrži q različitih elemenata, tj. simbola (npr. slova abecede). Kod (blokovni kod) C duljine n je podskup skupa F_q^n svih uređenih n-torki elemenata iz F_q. Elemente skupa C zovemo riječi, kodne riječi ili vektori.*

To znači da je blokovni kod sastavljen od kodnih riječi jednake duljine (svaka kodna riječ sastavljena je od n simbola) te da se svaka može zasebno dekodirati.

Primjer 2.2. *Za $q = 1$ kod zovemo trivijalni kod, za $q = 2$ binarni kod, za $q = 3$ ternarni kod, itd.*

Kako bismo primljenu poruku lakše dekodirali, bilo bi korisno znati koliko su poslana i primljena poruka slične, a to možemo s pomoću udaljenosti dvaju vektora.

Definicija 2.3. *Hammingova udaljenost $d(x, y)$ vektorska je norma vektora $x = (x_1, \ldots, x_n)$ i $y = (y_1, \ldots, y_n)$ i definira se kao broj komponenti u kojima se x i y razlikuju:*

$$d(x, y) = |\{i | x_i \neq y_i\}|.$$

Primjer 2.4. *Vektori $u = (1, 0, 1, 0, 1, 0, 1, 0)$ i $v = (1, 0, 1, 1, 1, 0, 0, 0)$ razlikuju se u četvrtoj i sedmoj komponenti, stoga je $d(u, v) = 2$.*

Definicija 2.5. *Minimalna udaljenost d koda C definira se kao najmanja Hammingova udaljenost između dva vektora iz C:*

$$d = \min\{d(x, y) : x, y \in C, x \neq y\}.$$

Kod možemo promatrati kao poruku koju šaljemo kroz komunikacijski kanal. Ako u kanalu dođe do smetnje, izvorna poruka $x = (x_1, \ldots, x_n)$ može biti izmjenjena. Stoga se primljena poruka $y = (y_1, \ldots, y_n)$ može razlikovati od poruke x. Udaljenost $d(x, y)$ označava broj pogrešaka u y, tj. koliko se primljena poruka razlikuje od poslane poruke.
Minimalna udaljenost d daje nam najmanji broj pogrešaka koje su potrebne da bi promijenile jednu kodnu riječ u drugu. Pogrešku najčešće onda ispravljamo tako da pronađ emo kodnu riječ čija je Hammingova udaljenost od kodne riječi u kojoj je pogreška pronađena najmanja moguća.

Kažemo da kod može detektirati do s pogrešaka ako promjenom jedne kodne riječi iz koda C u najviše s komponenti ne možemo dobiti drugu kodnu riječ iz koda C. Zatim, kod može ispraviti do t pogrešaka ako promjenom t ili manje komponenti kodne riječi c, najbliža kodna riječ i dalje ostaje c.

Definicija 2.6. *Neka je F^n skup svih kodnih riječi duljine n. Kod $C \subset F^n$ s minimalnom udaljenosti $2e + 1$ zove se savršeni kod ako za svaku kodnu riječ $x \in F^n$ postoji kodna riječ $y \in C$ takva da vrijedi $d(x, y) \leq e$.*

Definicija 2.7. *Hammingova težina $w(x)$ kodne riječi x definira se kao*

$$w(x) := d(x, 0).$$

Minimalna težina koda C definira se kao

$$\min\{w(x) | x \in C, x \neq 0\}.$$

Drugim riječima, težina kodne riječi broj je simbola različitih od 0, a minimalna težina koda najmanja je od svih težina nenul kodnih riječi toga koda.

Primjer 2.8. *Kodna riječ* 11000 *ima Hammingovu težinu* 2.

3 Linearni kodovi

Kako bismo mogli što brže i što učinkovitije dekodirati poruku, bilo bi nam najjednostavije kada bismo koristili kod koji ima neku strukturu. Najpoznatiji je primjer takvog koda linearni kod.
Da bismo mogli definirati linearni kod potrebno je poznavati polja i njihova svojstva.

Definicija 3.1. *Skup F s odgovarajućim operacijama zbrajanja $+$ i množenja $\cdot$ zovemo polje ako zadovoljava sljedeća svojstva:*

1. $\forall a, b \in F\ \exists! c \in F$ *takav da je* $a + b = c$
2. $(a + b) + c = a + (b + c),\ \forall a, b, c \in F$
3. $a + b = b + a,\ \forall a, b \in F$
4. $\exists 0 \in F$ *takav da je* $a + 0 = a,\ \forall a, b \in F$
5. $\forall a \in F\ \exists -a \in F$ *takav da je* $a + (-a) = 0$
6. $\forall a, b \in F\ \exists! d \in F$ *takav da je* $ab = d$
7. $(ab)c = a(bc),\ \forall a, b, c \in F$
8. $ab = ba,\ \forall a, b \in F$
9. $\exists 1 \in F$ *takav da je* $a \cdot 1 = a, \forall a \in F$
10. $\forall a \in F, a \neq 0, \exists a^{-1} \in F$ *takav da je* $aa^{-1} = 1$
11. $a(b + c) = ab + ac, (a + b)c = ac + bc, \forall a, b, c \in F.$

Također vrijedi da je skup F s operacijama zbrajanja $+$ i množenja $\cdot$ polje ako su $(F, +)$ i $(F \setminus \{0\}, \cdot)$ komutativne grupe.
S obzirom na broj elemenata, polje može biti konačno ili beskonačno. Ako je F konačno polje, tada $q = |F|$ zovemo red polja F.

Definicija 3.2. *Neka je F_q polje reda q. Tada je skup $F_q^n = \{(x_1, \ldots, x_n) | x_i \in F_q, 1 \leq i \leq n\}$ svih uređenih n-torki s elementima iz F_q n-dimenzionalan vektorski prostor uz operacije zbrajanja:*

$$(x_1, \ldots, x_n) + (y_1, \ldots, y_n) = (x_1 + y_1, \ldots, x_n + y_n)$$

i množenja skalarom:

$$\alpha(x_1, \ldots, x_n) = (\alpha x_1, \ldots, \alpha x_n), \alpha \in F_q.$$

Poznavajući ove strukture možemo definirati linearni kod.

Definicija 3.3. *Linearni potprostor n-dimenzionalnog vektorskog prostora F_q^n zovemo linearni kod nad F_q.*

Kako smo kod definirali kao linearni potprostor, analogno tome dimenziju koda definiramo kao dimenziju potprostora, odnosno broj kodnih riječi koje čine bazu koda C.
Kod $C \subset F_q^n$ dimenzije k označavamo s $[n, k]$ kod. Dakle, $[n, k]$ kod je skup koji se sadrži linearne kombinacije k baznih kodnih riječi duljine n. Nadalje, s $[n, k, d]$ označavamo $[n, k]$ kod s minimalnom Hammingovom udaljenosti d. Za takav $[n, k, d]$ kod kažemo da je linearan ako je on linearni potprostor n-dimenzionalnog vektorskog prostora F_q^n dimenzije k.

Primjer 3.4. *U Primjeru 1.1 koristili smo* $[8, 7]$ *kod. On sadrži binarne vektore duljine* 8 *čija je suma elemenata paran broj. Očito je da skup ovih vektora čini* 7*-dimenzionalan potprostor, a njegovu bazu čine vektori* $(1,0,0,0,0,0,0,1), (0,1,0,0,0,0,0,1), \ldots, (0,0,0,0,0,0,0,1)$.

Svaka baza linearnog $[n, k, d]$ koda C nad poljem F sadrži k kodnih riječi čije linearne kombinacije generiraju cijeli skup C, stoga vrijedi $|C| = q^k$.

Definicija 3.5. *Matrica* G *reda* $k \times n$ *čiji retci čine bazu* $[n, k]$ *koda* C *zove se generator od* C*.*

U većini slučajeva, ta matrica nije jedinstvena.

Primjer 3.6. *Matrica* $G = \begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ *je generator* $[3, 2, 2]$ *koda nad poljem* F_2*, kao i matrica* $\hat{G} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$.

Iz Definicije 3.5 možemo zaključiti da vektore koda C dobivamo kao linearne kombinacije redaka matrice G, pri čemu su koeficijenti iz polja F_q, tj. $C = \{aG | a \in F_q^n\}$.
Matricu G najčešće konstruiramo na način da je $G = [I_k, P]$, gdje je I_k $k \times k$ jedinična matrica, a P $k \times (n-k)$ matrica. Tada prvih k stupaca matrice G određuju kodne riječi, a preostalih $n-k$ stupaca predstavljaju zalihost.

Primjer 3.7. *Matrica koja je generator koda iz Primjera 1.1 je*

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \end{bmatrix}$$

Možemo vidjeti da je kodna riječ 11001001 *linearna kombinacija prvog, drugog i petog retka koja se dobije množenjem vektora* $(1,1,0,0,1,0,0)$ *s matricom* G*.*

Definicija 3.8. *Neka je dan kod* $C \subseteq F_q^n$*. Tada kod* $C^\perp$ *zovemo dualni kod koda* C *i definiramo kao ortogonalni prostor od* C*:*

$$C^\perp = \{y \in F_q^n | y \cdot x = 0, \forall x \in C\},$$

gdje je $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n)$ *i*

$$x \cdot y = x_1 y_1 + \cdots + x_n y_n$$

standardni skalarni produkt u F_q^n*.*

Dakle, dualni je kod skup svih vektora ortogonalnih na vektore iz C te je on ujedno i $[n, n-k]$ kod.

Definicija 3.9. *Generator matrica dualnog koda* $C^\perp$ *zove se kontrolna matrica koda* C*.*

Kontrolnu matricu koda C označavamo s H. Možemo reći da kod C sadrži vektore $x = (x_1, \ldots, x_n)$ koji su rješenja homogenog sustava linearnih jednadžbi s koeficijentima matrice H, tj. vrijedi $C = \{x \in F_q^n | Hx^T = 0\}$.

S obzirom da je linearni kod vektorski prostor, on mora sadržavati nul-vektor kao jednu od kodnih riječi. Sljedeća propozicija pokazuje da je minimalna udaljenost linearnog koda jednaka minimalnoj težini bilo koje kodne riječi različite od nul-vektora.

Propozicija 3.10. *Neka je C linearan $[n, k, d]$ kod nad poljem F. Tada vrijedi*

$$d = \min\big\{w(c) | c \in C \setminus \{0\}\big\}.$$

Dokaz. Neka su $c_1, c_2 \in C$ proizvoljni vektori. Zbog linearnosti vrijedi $c_1 - c_2 \in C$. Primijetimo da vrijedi $d(c_1, c_2) = w(c_1 - c_2)$.
$d = \min\{d(c_1, c_2) | c_1, c_2 \in C, c_1 \neq c_2\} = \min\{w(c_1 - c_2) | c_1, c_2 \in C, c_1 \neq c_2\} =$
$\min\big\{w(c) | c \in C \setminus \{0\}\big\}$. □

Vezu između minimalne težine i kontrolne matrice pokazuje nam idući teorem.

Teorem. 3.11. *Minimalna težina linearnog koda C s kontrolnom matricom H jednaka je najvećem cijelom broju d, takvom da su svakih $d-1$ stupaca matrice H linearno nezavisni.*

Korolar 3.12. *Linearni kod s kontrolnom matricom H može ispraviti jednostruke pogreške ako i samo ako su svaka dva stupca matrice H linearno nezavisni. Posebno, binarni linearni kod može ispraviti jednostruke pogreške ako i samo ako su svi stupci njegove kontrolne matrice međusobno različiti nenul vektori.*

Primjer 3.13. *Dana je matrica*

$$H = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Svi stupci matrice H su nenul i međusobno različiti, stoga je matrica H kontrolna matrica binarnog koda s minimalnom težinom $d \geq 3$.

4 Hammingovi kodovi

U ovom poglavlju opisat ćemo binarni linearni kod koji služi za otkrivanje i korekciju jednostrukih pogrešaka, a radi na principu dodavanja bitova parnosti, odnosno kontrolnih simbola koji pomažu otkriti točnu poziciju u kodnoj riječi na kojoj se pogreška nalazi.
Možemo ga vrlo lako odrediti s pomoću njegove kontrolne matrice. Pretpostavimo da želimo dodati m kontrolnih simbola poruci x duljine k koju šaljemo. Tada kontrolnu matricu kreiramo tako da u stupce upišemo sve binarne nenul vektore duljine m. S obzirom da takvih vektora ima $n = 2^m - 1$, kontrolna matrica je reda $m \times (2^m - 1)$.
Iz Teorema 3.11 i Korolara 3.12 znamo da linearni binarni kod ima minimalnu udaljenost $d \geq 3$ ako i samo ako su svi stupci kontrolne matrice međusobno različiti nenul vektori. Upravo to će nam pomoći pri definiranju Hammingovog koda.

Definicija 4.1. *Binarni linearni kod zovemo Hammingov ako za neki broj m njegova odgovarajuća kontrolna matrica sadrži $2^m - 1$ stupaca, pri čemu su svi stupci jedinstveni nenul vektori duljine m.*

Dakle, njegova je kontrolna matrica reda $m \times (2^m - 1)$, odnosno kodne riječi ovog koda su duljine $2^m - 1$. Broj m predstavlja zalihost, tj. broj kontrolnih simbola koje dodajemo poruci.

Primjer 4.2. *Za $m = 3$, kontrolna matrica H je reda 3×7.*

$$H = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Ovaj kod zovemo još i $[7, 4]$ Hammingov kod.

Korolar 4.3. *Minimalna udaljenost Hammingovog koda jednaka je 3.*

Dokaz. Ovaj rezultat izravna je posljedica Propozicije 3.10 i Teorema 3.11. Iz definicije Hammingovog koda očito je da su svaka dva stupca kontrolne matrice H linearno nezavisni. Iz Teorema 3.11 tada slijedi da je minimalna težina Hammingovog koda jednaka 3. Primjenivši Propoziciju 3.10 koja kaže da je minimalna udaljenost linearnog koda jednaka njegovoj minimalnoj težini toga koda, zaključujemo da je minimalna udaljenost Hammingovog koda jednaka 3. □

Kao što smo već spomenuli, izvornu poruku kodiramo na način da joj dodajemo zalihost, tj. simbolima poruke dodajemo kontrolne simbole koje možemo promatrati kao bitove parnosti. Za razliku od dosad već viđenog načina dodavanja bitova parnosti na kraj poruke, u ovom slučaju njihove pozicije određivat ćemo na sljedeći način:
c_1 - prvi kontrolni bit stavljamo na poziciju $2^0 = 1$
c_2 - drugi kontrolni bit stavljamo na poziciju $2^1 = 2$
c_3 - treći kontrolni bit stavljamo na poziciju $2^2 = 4$, itd.
pri čemu svaki od njih kontrolira parnost nad bitovima koji nose poruku. Tako c_1 služi za provjeru parnosti bitova čije pozicije pri dijeljenju s $2^1 = 2$ daju ostatak 1, c_2 služi za provjeru parnosti bitova čije pozicije pri dijeljenju s $2^2 = 4$ daju ostatak 2 i 3, c_3 služi za provjeru parnosti bitova čije pozicije pri dijeljenju s $2^3 = 8$ daju ostatke 4, 5, 6 i 7, itd.
Pri korištenju $[n, k]$ Hammingovog koda broj kontrolnih bitova koje dodajemo iznosi $n - k$.

Nadalje, pretpostavimo da je pri prijenosu poruke došlo do pogreške. Neka je $y \in F_2^n$ $(n = 2^m - 1)$ vektor dobiven iz neke kodne riječi $x \in F_2^n$ na način da je vektoru x promjenjena samo jedna komponenta. Hammingov kod nam omogućuje da otkrijemo pogrešku, tj. iz dobivene kodne riječi y odredimo izvornu kodnu riječ x na sljedeći način:
odredimo vektor $S = Hy^T$, gdje je H kontrolna matrica binarnog Hammingovog koda. Taj vektor zovemo sindrom. Ako je S jednak nulvektoru, možemo zaključiti da do pogreške nije došlo. U suprotnom, S će biti jednak jednom od stupaca matrice H. Ako je S jednak i-tom stupcu matrice H, tada možemo zaključiti da je došlo do pogreške na i-toj komponenti vektora x i možemo ju izračunati kao $x_i = 1 - y_i$.
Na idućem primjeru pokazat ćemo princip rada Hammingovog koda.

Primjer 4.4. *Hammingovim* $[7, 4]$ *kodom kodirat ćemo poruku* 1101.
$n = 7$, $k = 4 \Rightarrow n - k = 3$, *tj. potrebna su nam* 3 *kontrolna simbola.*

pozicija	1	2	3	4	5	6	7
simbol	c_1	c_2	i_1	c_3	i_2	i_3	i_4

gdje su c_1, c_2 *i* c_3 *kontrolni simboli, a* i_1, i_2, i_3, i_4 *bitovi koji nose informaciju, odnosno komponente poruke.*

pozicija	1	2	3	4	5	6	7
simbol	c_1	c_2	1	c_3	1	0	1

c_1 *služi za provjeru parnosti bitova na* 3., 5. *i* 7. *poziciji* $\Rightarrow c_1 = 1$
c_2 *služi za provjeru parnosti bitova na* 3., 6. *i* 7. *poziciji* $\Rightarrow c_2 = 0$
c_3 *služi za provjeru parnosti bitova na* 5., 6. *i* 7. *poziciji* $\Rightarrow c_3 = 0$

Kodirana poruka tada glasi $x = [1010101]$.
Pretpostavimo sada da je pri prijenosu poruke došlo do pogreške na 6. *poziciji.*
Kodirana poruka na odredištu tada će biti $y = [1010111]$.
Neka je H *kontrolna matrica navedena u Primjeru 4.2.*

$$S = Hy^T = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix}$$

Dobili smo vektor jednak 6. *stupcu matrice* H, *iz čega možemo zaključiti da je do pogreške zaista došlo na* 6. *poziciji vektora* x.

5 Literatura

[1] Jiri Adamek, Foundations of coding: theory and applications of errorcorrecting codes, with an introduction to cryptography and information theory, John Wiley & Sons, Inc., Chichester/ New York/ Brisbane/ Toronto/ Singapore, 1991.

[2] J.I.Hall, Notes on Coding Theory, Department of Mathematics, Michigan State University, East Lansing, 2010.
dostupno na:
`http://users.math.msu.edu/users/jhall/classes/codenotes/coding-notes.html`

[3] J. H. van Lint, Introduction to Coding Theory, Third Revised and Expanded Edition, Springer-Verlag, Berlin/Heidelberg, 1999.

[4] Ron M. Roth, Introduction to Coding Theory, Cambridge University Press, New York, 2006.

[5] Vladimir D. Tonchev, An Introduction to Coding Theory: Lecture Notes, Department of Mathematical Sciences, Michigan Technological University, Michigan, 2009.
dostupno na:
`http://www.math.mtu.edu/tonchev/Coding-Theory-Tohoku-June-09.pdf`