Erna Oklapi i Sanela Numanović

Hamingov kôd kao savršen kôd

Teorija kodiranja je grana matematike bazirana na analizi podataka koji se prenose kroz kanale sa šumom i na ispravljanju eventualnih grešaka koje pri tom nastaju. U ovom radu predstavljen jedan od najkorišćenijih kodova, Hamingov kôd. On služi za otkrivanje najviše dve i ispravljanje jedne greške koje su nastale prenosom podataka. Ovaj rad se bavi matematičkom pozadinom funkcionisanja koda koji se koristi svakodnevno u računarstu. Na osnovu primera pronađenih u navedenoj literaturi izveden je opšti algoritam za otkrivanje i ispravljanje grešaka pomoću ovog koda.

Savršeni kodovi

Pre definisanja Hamingovog koda, pokazaćemo najbitnije karakteristike savršenih kodova u koje spada i sam Hamingov kôd. U teoriji kodiranja posmatra se skup F od q različitih simbola (slova) koji se naziva azbuka. U praktičnim problemima je obično $q = 2$ i $F = \{0, 1\}$, dok se u teorijskim razmatranjima uzima da je $q = p^r$, tako da je p prost broj i $F = GF(q)$. Tako je moguće formirati q^n n-torki koristeći slova skupa F koje se nazivaju reči. Sa F^n se obeležava skup svih reči dužine n. Kada je $q = pr$ reči se mogu predstaviti kao n-dimenzionalni vektori nad poljem $GF(q)$ i tada je F^n vektorski prostor nad tim poljem. Poruke koje se šalju kroz telekomunikacioni kanal kodiraju se pomoću reči iz skupa F^n. Ovakav način kodiranja naziva se blokovsko kodiranje. Možemo pretpostaviti da se reč prenosi slovo po slovo kroz kanal. Usled smetnji svako slovo može se pogrešno preneti i na kraju kanala korisnik ga registruje kao neko drugo slovo. Neka je p verovatnoća da se slovo na kraju kanala registruje kao neko drugo, tada je np srednja vrednost broja grešaka prilikom prenošenja reči dužine n. Na osnovu te verovatnoće može se odrediti maksimalan broj grešaka e koje se mogu praktično pojaviti. Osnovni zadatak teorije kodova je da razradi metode za korekciju greške.

Erna Oklapi (1989), Novi Pazar, Kompleks "Jezero" b/11, učenica 3. razreda Gimnazije u Novom Pazaru

Sanela Numanović (1990), Žabare (Kruševac), učenica 2. razreda Gimnazije u Kruševcu

MENTOR:
Zlatko Emeđi, Bačinci (Šid), student Fakulteta tehničkih nauka u Novom Sadu

Definicija 1. Rastojanje $d(x, y)$ reči x i y iz F^n je jednako broju koordinata u kojima se reči x i y razlikuju.

Skup $S(x, r) = \{x | y \in F^n, d(x, y) \leq r\}$ n-torki y koje su od n-torke x udaljene za najviše r naziva se (zatvorena) kugla poluprečnika r sa centrom u x. Svaki podskup C skupa F^n naziva se kôd. Minimalno međusobno rastojanje n-torki iz jednog koda C naziva se kodovsko rastojanje. Kôd kodovskog rastojanja $2e + 1$ ima osobinu da se njegove n-torke mogu rekonstruisati na kraju telekomunikacionog kanala ako se prilikom prenošenja svake n-torke ne napravi više od e grešaka, tj. ako bar $n - e$ prenete reči tačno primi na kraju kanala.

Definicija 2. Kod $C = \{x_1, x_2, \ldots x_m\}$ $(\subseteq F^n)$, kodovskog rastojanja $2e + 1$ se naziva savršen ako je

$$\bigcup_{i=1}^{m} S(x_i, e) = F_n$$

tj. ako je unija kugli poluprečnika e opisanih oko n-torki koda C jednaka skupu svih n-torki F^n.

Hamingov kôd

"Mašine treba da rade. Ljudi treba da razmišljaju.", reči su američkog matematičara koji se zvao Ričard Vesli Haming (*Richard Wesley Hamming*). On je definisao kôd pomoću kojeg se otkriva i ispravlja jedna greška. Pre predstavljanja tog koda, nužno je definisati osnovne pojmove u teoriji kodiranja.

Definicija 3. Kôd C je podskup skupa A^n gde je A alfabet nad kojim se vrši kodiranje, a A^n je skup svih uređenih n-torki.

Definicija 4. Reč je element A^n. Kodna reč je element C.

Definicija 5. Za dati kôd C, skup svih reči naziva se kodni prostor.

Definicija 6. n-torka sastavljena od nula i jedinica naziva se kodna reč. Može se uzeti da je svaka kodna reč n-dimenzionalni vektor polja Z_2.

Jačina koda zavisi od mogućnosti da greška nastala prilikom prenosa informacije bude detektovana i ispravljena. Ovaj proces naziva se dekodiranje. Da bi se dekodirala poruka najčešće se koriste matrice.

Definicija 7. Kontrolna matrica ima funkciju dekodiranja za kôd C. Dobijena poruka se množi sa kontrolnom matricom.

Definicija 8. Sindrom je vektor nastao množenjem primljene reči i kontrolne matrice. Dužina vektora sindroma određuje koliko grešaka treba ispraviti.

Granica detekcije greške i njenog ispravljanja zavisi od rastojanja između vektora u kodnom prostoru C.

Definicija 9. Hamingova težina vektora u iz kodnog prostora definiše se kao $d(u, 0)$.

Drugim rečima, to je broj nenultih pozicija u kodnoj reči. Dimenzija koda je broj vektora u bazi koda. Linearni kodovi dužine n i dimenzije k će se opisivati kao $[n, k]$ kodovi. Hamingov kôd je linearan, opisuje se kao $[n, k]$ i on određuje q kao kardinalnost baze F_q, sa $q = 2$ jer je $F_q = \{0, 1\}$.

Hamingov kôd radi na principu dodavanja pomoćnih bitova parnosti na pozicijama stepena dvojke reči koju treba da prenesemo. Definisaćemo matricu B pomoću koje određujemo zavisnost vrednosti bitova parnosti od ostalih bitova kodne reči.

Definicija 10. Matrica $B[2^n - 1, n]$, gde je $b_{ij} \in \{0, 1\}$, se konstruiše tako što se svako i izrazi u obrnutom binarnom zapisu u i-toj vrsti, a ostala polja b_{ij} imaju vrednost nula.

Matrica za specijalan slučaj gde je $n = 3$ izgleda:

•	x_1	x_2	x_4
1	1	0	0
2	0	1	0
3	1	1	0
4	0	0	1
5	1	0	1
6	0	1	1
7	1	1	1

Definicija 11. Bit parnosti 2^j je određen nekim i iz j-te kolone ako je $b_{ij} = 1$.

Za specijalni slučaj imamo:

$$x_4 = x_5 + x_6 + x_7$$
$$x_2 = x_2 + x_6 + x_7$$
$$x_1 = x_3 + x_5 + x_7$$

Iz gore navedenog se može primetiti da svaki bit parnosti zavisi od bitova reči u čijem se indeksu sadrži indeks samog bita parnosti.

Ako želimo preneti reč (1011) onda se ona kodira na sledeći način:

1. $(x_1 \quad x_2 \quad 1 \quad x_4 \quad 1 \quad 1)$
2. $(x_1 \quad x_2 \quad 1 \quad 0 \quad 1 \quad 1)$
3. $(x_1 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1)$
4. $(0 \quad 1 \quad 1 \quad 0 \quad 1 \quad 1)$

Za reč 1011 potrebna su 3 bita parnosti, što znači da ce primalac dobiti reč od 7 bitova. Kodiranje se vrši tako što se ne popunjavaju mesta na kojima se bitovi parnosti nalaze već se datom rečju redom popunjavaju

3, 5, 6. i 7. mesto kodne reči. x_1, x_2, x_4 se izračunavaju po gore navedenim formulama.

Za proveru greške u ovom slučaju koristićemo sledeće jednačine:

$$z_1 = x_4 + x_5 + x_6 + x_7$$

$$z_2 = x_2 + x_3 + x_6 + x_7$$

$$z_3 = x_1 + x_3 + x_5 + x_7$$

$z_1z_2z_3$ predstavlja binarni zapis indeksa bita na kojem se nalazi greška. Ako je $z_1 = 1$, $z_2 = 0$ i $z_3 = 1$, onda se greška nalazi na 5. bitu, jer je $(5)_2 = 101$. Ukoliko je $z_1z_2z_3 = 000$, onda nema greške u primljenoj reči. Ovo treba dokazati u opštem slučaju.

Predstavljanje Hamingovog koda u opštem slučaju

Svaki z se predstavlja zbirom odgovarajućeg bita parnosti i bitova od kojih taj bit zavisi.

1. Ako je $\forall z = 0$, onda nema greške u kodnoj reči, jer zbir 2 istovetna bita treba da bude 0.

2. Ako $\exists! z_i = 1$, gde je $z \in \{z_1, z_2, \ldots z_n\}$, onda je greška na 2^{n-i}-tom bitu parnosti.

3. Ako postoji m z_i takvih da je $z_i \neq 0$ i $m \geq 2$, onda je greška u bitovima reči koje se prenosi (ne u bitovima parnosti koji se naknadno dodaju), a mesto koda predstavlja binarni zapis svih z_j.

Dokaz: Ako imamo grešku na x_i bitu, posmatrajmo sledeće:

$z_n = x_1 + x_3 + \ldots + x_{2^n-1}$

$z_{n-1} = x_2 + x_3 + x_6 + x_7 + \ldots$

$z_{n-2} = x_4 + x_5 + x_7 + \ldots$

$\ldots$

$z_{n-k} = x_{2^k} + \ldots$

$\ldots$

$z_1 = x_{2^k-1}$

Ako je i indeks bita na kom je greska tada je $\{z_1 z_2 \ldots z_n\}$, gde je $j = 1, 2, 3, \ldots n$, ako x_i bit učestvuje u sumi z_j. $x_{2^{n-j}}$ bitovi parnosti bit z_j i on će čekirati x_i ako 2^{n-j} učestvuje u zapisu broja i. Posmatrajmo binarni zapis broja i. Neka je to:

$(a_1a_2..a_n)_2 = i = a_1 2^0 + a_2 2^1 + \ldots + a_{n-j}2^j + \ldots + a_{n-1}2^{n-2} + a_n 2^{n-1}$

$\Rightarrow a_j = 1 \Rightarrow a_j = z_j \Rightarrow i = (z_1 z_2 \ldots z_n)_2$

Ovim je dokaz završen.

Definicija 12. k-dimenzionalni potprostor C vektorskog prostora F^n naziva se linearni (n, k)-kôd nad poljem $GF(q)$.

Linearni kodovi C se obično predstavljaju pomoću generišuće matrice koda. Vrste generišuće matrice obrazuju bazu vektorskog prostora C. Ako C predstavlja (n, k)-kôd, njegova generišuća matrica je dimenzija $k \times n$. Vektori koda C se dobijaju kao linearne kombinacije vrsta matrice G, pri čemu se koeficijenti uzimaju iz odgovarajućeg polja $GF(q)$.

Skup svih vektora koji su ortogonalni na sve vektore koda C naziva se *dualni kôd* koda C i obeležava se sa $C^{\perp}$. Ako je C linearni (n, k)-kôd, dualni kôd $C^{\perp}$ je linearni $(n, n - k)$-kôd. Generišuća matrica H dualnog koda C naziva se kontrolna matrica koda C. Generišuća matrica G i kontrolna matrica H koda C povezane su jednakošću:

$$GH^T = 0$$

odnosno $C = \{x | Hx^T = 0\}$, koja se neposredno proverava na osnovu navedenih definicija.

Definicija 13. Neka je H matrica tipa $m \times 2^m - 1$ čije su kolone binarni zapisi brojeva $1, 2, \ldots 2^m - 1$

Ova matrica predstavlja kontrolnu matricu Hamingovog koda, a kôd je dimenzija $[2^m - 1, 2^m - 1 - m]$, gde je m prirodan broj. Skup C svih n-torki $(n = 2^m - 1)$ iz F^n $(F = GF(2))$ koje su ortogonalne na sve vrste matrice H predstavlja Hamingov kod. Kontrolna matrica $[7, 4]$ binarnog Hamingovog koda za ovaj specijalni slučaj gde je $m = 3$ ima sledeći oblik:

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

a kôd sačinjavaju:

(0 0 0 0 0 0 0), (1 0 0 0 0 1 1), (0 0 1 1 0 0 1), (0 0 1 0 0 1 1)
(0 1 1 0 1 1 1), (0 1 0 1 1 1 1), (0 1 1 0 0 0 0), (1 0 0 1 1 0 0)
(0 1 0 0 1 0 1), (0 0 0 1 1 1 1), (0 0 1 0 1 1 0), (0 1 1 0 0 1 1)
(1 0 0 0 0 1 1), (1 0 1 1 0 1 0), (1 1 0 0 1 1 0), (1 1 1 1 1 1 1)

Za proveravanje grešaka pomoću matrice, neophodno je definisati pojam Hamingove distance.

Lema 1. Minimalna distanca između dve kodne reči u Hamingovom kodu je 3.

Dokaz: Neka su x i y dve kodne reči Hamingovog koda C sa kontrolnom matricom H. Kada $x - y \in C$, C je linearan kôd. Ako je $d_H(x,y) = 1$ onda je matrica $H(x - y)$ jedna od kolona matrice H. Sve kolone matrice H su različite od nule, ali ako je $(x - y)$ kodna reč, onda je $H(x - y) = 0$. Kontradikcija. Ako je $d_H(x, y) = 2$ onda je $H(x - y) = 0$ akko u matrici H postoje dve kolone koje su linearno zavisne. Pošto ne važi, sledi da je $d_H(x, y) \geq 3$ za svaku x, y kodnu reč. Svaka kontrolna matrica Hamingovog koda će imati tri kolone koje su linearno zavisne, i iz te činjenice

proizilazi da Hamingova kodna distanca svih kodnih reči iznosi 3. Ovim je tvrđenje dokazano.

Hamingov kôd je linearan blokovski $(n, n-m)$-kôd. Svaka nenulta n-torka koda sadrži bar 3 simbola jednaka 1, zato je kodovsko rastojanje koda jednako 3 i on može ispravljati jednu grešku. Broj n-torki u kodu je 2^{n-m}, a kugla poluprečnika 1 sadrži $n + 1$ n-torku. Pošto je $2^{(n-m)(n+1)} = 2^n$ sve n-torke su pokrivene kuglama, pa je Hamingov kôd savršen.

Za proizvoljno polje $GF(q)$ sa q^2 elemenata konstrukcija matrice H je složenija.

Broj kolona ove matrice iznosi $\dfrac{q^m - 1}{q - 1}$.

Matrica Hamingovog koda se koristi za proveravanje i ukazivanje na samo jednu grešku u primljenoj kodnoj reči. Pošto je $Mx^T = 0$ i ako je $x = y$, gde je y primljena kodna reč, važiće: $My^T = 0$ što znači da nije došlo do greške u prenosu. Ukoliko $Mx^T \neq 0$, onda je greška na bitu čija pozicija odgovara broju koji je u binarnom zapisu dobijen množenjem M i x^T. Za specijalan slučaj imamo Hamingovu matricu kod koje je $m = 3$ i primljenu kodnu reč [0110111].

Iz ovoga se vidi da je greška na 5. bitu kodne reči jer je $(101)_2 = 5$. Za opšti slučaj treba dokazati sledeću teoremu.

Teorema 1. Proizvod matrica $A[2^{m-1}, m]$ i B_{1i} je binarni zapis indeksa bita na kome se nalazi greška.

Dokaz: Neka se greška nalazi na i-tom mestu u kodnoj reči. Po definiciji Hamingove matrice A njena i-ta kolona predstavlja binarni zapis broja i. Pošto je nula neutralni element za operaciju konjukcije, onda sve jedinice koje se nalaze na a_{ij} poziciji postaju z_1. Posle operacije konjukcije, bitovi se sabiraju po modulu dva i to daje konačan rezultat.

1. Ukoliko $x_i = 0$ greškom prelazi u $x_i = 1$, onda se na osnovu navedenog postupka za vrednost z_j dobija 1. Kako je $1 \wedge 0 = 0$, nakon greške to prelazi u $(1 \wedge 1 = 1) \Rightarrow$

$$\sum_{j=1}^{2^m - 1} a_{ij}\, b_{ij} = {}_2 1$$

2. Za $x = 1$, analogno prethodnom, važi $1 \wedge 1 = 1$, gde zbog greške prelazi u $1 \wedge 0 = 0$, pa se zbog promene nakon sabiranja po modulu 2 umesto nule dobija 1.•

Hamingov kôd se koristi i za pronalaženje više od jedne greške u nekoj kodnoj reči. Za tu svrhu potrebna nam je proširena Hamingova matrica. Ako na primer imamo primljenu reč (1110111), gde su greške na 1. i 5. mestu, i ukoliko tu reč pomnožimo sa kontrolnom Hamingovom matricom dobićemo sledeće:

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

(100) je binarni zapis broja 4 i iz prethodnog sledi da je greška na 4. bitu, što ovde nije slučaj. Pošto se prethodno opisan način koristi za određivanje greške na jednom bitu mora postojati neka složenija kontrolna matrica koja ukazuje na dve greške. Zato se konstruiše proširena Hamingova matrica koja će biti u mogućnosti da detektuje dve greške. Da bi se konstruisala potreban je još jedan bit parnosti bit x_0 koji je određen na sledeći način:

$$x_0 = x_1 + x_2 + x_3 + x_4 + x_5 + x_6 + x_7$$

Sada kôd ima dužinu 8, ali je i dalje linearan sa dimenzijom 4. Sada se konstruiše $[8, 4]$ prošireni Hamingov kôd koji za bilo koju dužinu dodaje novi bit parnosti. Proširena Hamingova matrica se lako konstruiše iz kontrolne matrice običnog Hamingovog koda tako što se nule dodaju sa leve strane, a jedinice na dno matrice:

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

Neka su x i y binarne reči Hamingovog koda distance 3, gde jedna od x i y ima paran, a druga neparan broj bitova parnosti sa vrednošću 1. Uzmimo da x ima paran broj bitova parnosti. Ako su x' i y' kodne reči proširene Hamingove matrice, onda je $x_0 = 0$, pošto x ima paran broj bitova parnosti, a $y_0 = 1$, zato što je broj bitova parnosti u reči y neparan.

Distanca između x' i y' je veća od distance između x i y, tako da je minimalna kodna distanca proširenog Hamingovog koda 4. Ako primimo reč koja u odnosu na poslatu reč ima distancu 1, onda možemo da ispravimo tu grešku jer se ona javlja samo na jednom bitu. Ukoliko se poslata i primljena reč razlikuju za 2, onda se ukazuje na to da su u prenosu nastale greške na dva bita u reči. Dekodiranje proširenom Hamingovom matricom je malo komplikovanije. Njegova kontrolna matrica proširenog Hamingovog koda je M, a H matrica običnog Hamingovog koda od kojeg je proširena matrica nastala i neka je $y = (y_0, y_1, \ldots, y_n)$ primljena reč. Pretpostavimo da se pojavila greška na samo jednom bitu i to na poslednjem. My^{T} množenje je ekvivalentno $M(y_0, y_1, \ldots, y_n)^T$ množenju. Poslednji red My^T ce biti 1 zato sto postoji samo jedna greška,

tako da binarni zapis broja n odgovara koloni M koja je brojem r određena.

Pretpostavimo da je greška na bitu parnosti. Tada je:

$$M'(y_0, y_1, \ldots, y_n)^T = 0,$$

tako da će prvih n kolona biti jednako 0, ali poslednja će imati vrednost 1, jer je greška samo na onom bitu parnosti koji odgovara jednoj koloni matrice M.

Na kraju pretpostavimo da su se javile dve greške u primljenoj reči. Bilo gde da su detektovani, bitovi parnosti će biti tačni zato što će proizvod biti 0 u poslednjoj vrsti i to neće biti kolona kontrolne matrice. Možemo generalisati konstrukciju linearnog q-Hamingovog koda gde je $[n, k]$ Hamingov kôd linearni prostor nad poljem određenim sa q'. Za dato r izaberimo r-torku elemenata iz F_q. Izaberimo jos jednu r-torku koja je linearno nezavisna od prve. To pravi 2 kolone. Nastavlja se sabiranje r-torki sve dokle je moguće da one budu linearno nezavisne. Ove r-torke se rasporedjuju kao kolone matrice M. Postoji q^{r-1} takvih r-torki. Broj kolona matrice M je $\frac{q^r - 1}{q - 1}$. Definišimo linearan kôd čija kontrolna matrica ima sledeće dimenzije: $(q^r - 1)(q - 1), \frac{q^r - 1}{q - 1} - r$. Kontrolna matrica je generišuća matrica dualnog koda, koji u ovom slučaju mora da ima dimenziju r, jer dimenzija našeg Hamingovog koda mora da bude:

$$n - r = \frac{q^{r-1}}{q - 1} - r$$

Za $[4, 2]$ Hamingov kôd ($q = 3$) kontrolna matrica će biti:

$$\begin{bmatrix} 0 & 1 & 2 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$$

a kôd će imati izgled:

(0 0 0 0), (0 1 1 1), (0 2 2 2), (1 0 1 2), (2 0 2 1), (1 1 2 0)
(2 2 1 0), (2 1 0 1), (2 1 0 2)

Isti $[4, 2]$ Hamingov kôd se može predstaviti i sledećom matricom:

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

čiji je kôd:

(0 0 0 0), (0 1 2 1), (0 2 1 2), (1 0 1 1), (2 0 2 2), (1 1 0 2)
(2 2 0 1), (1 2 2 0), (2 1 1 0)

Dakle, imamo proizvod My^T za kontrolnu matricu M, a primljenu reč y. Ako je proizvod nula, onda nema greške, a ako nije nula onda proizvod

odgovara nekoj koloni matrice M. Ukoliko je proizvod αm_i gde $\alpha \in F_q$ i i iz m_i predstavlja redni broj kolone matrice M i uzmimo da je to vektor greške koji je kodu dodat prilikom prenosa poruke. To je vektor $(0 \ldots 0\, 1\, \alpha 0 \ldots 0)$, gde je α na i-tom mestu. Sledi da je vektor koji predstavlja primljenu reč $y - (0 \ldots 0\, 1\, \alpha 0 \ldots 0)$.

Definicija 14. Kôd koji ispravlja e grešaka (e-kod) nazivamo e-perfektni kod ako je $|C| \cdot |S_e(x)| \leq |F_q|^n$ ili:

$$|F_q|^n = |C| \sum_{i=0}^{e} \binom{n}{i} (q-1)^i$$

Lema 2. Za Hamingov kôd važi $|C| = q^{n-r}$.

Dokaz: Od q elemenata možemo izabrati tačno qn n-torki. Pošto vrednosti bitova parnosti kojih ima tačno r zavise od vrednosti ostalih bitova, onda se broj n-torki smanjuje $2r$ puta.

Teorema 2. Hamingov kôd je 1-perfektan kôd.

Dokaz: Na osnovu definicije perfektnog koda imamo da je:

$$|F_q|^n = |C| \sum_{i=0}^{1} \binom{n}{i} (q-1)^i$$

a iz definicije Hamingovog koda da je $|C| = q^{n-r}$. Kombinacijom ovih dveju jednakosti dobijamo sledeće:

$$|F_q|^n = q^{n-r}(1 + n(q-1))$$

pa kako je $n = \dfrac{q^r - 1}{q-1}$ onda:

$$|F_q|^n = q^{n-r}(1 + q^r - 1)$$

$$|F_q|^n = q^n$$

što je i trebalo dokazati. •

Literatura

Cvetković D., Simić S. 2006. *Kombinatorika i grafov*i. Beograd: Računarski fakultet

Kalajdžić G. 1994. *Linearna algebra*. Beograd: Matematički fakultet

Davis P. J. 1965. *Mathematics of matrices*. GINN and Company

Đorđević R. Ž., Milovanović, G. V. 2004. *Linearna algebra*. Beograd: Osnovni udžbenici

Fiedler J. Hamming Codes. Dostupno na http://orion.math.iastate.edu/linglong/Math690F04/HammingCodes.pdf.

Erna Oklapi and Sanela Numanović

Hamming Code like a Perfect Code

In this paper the Hamming code was demonstrated. This code assists in detecting and correcting errors that appear in information transport, for example in telecommunications. Apart from special occurencies, it was also demonstrated how the Hamming code functions in general.