UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
DEPARTMAN ZA
MATEMATIKU I INFORMATIKU

Bojan Berleković

NEKE KLASE LINEARNIH KODOVA

-master rad-

Mentor
prof. dr Branimir Šešelja

Novi Sad, 2016.

Sadržaj:

Predgovor

Matematika kao egzaktna nauka i fundament na koji se sve prirodno nadograđuje, a opet se sve i njoj vraća, dopire do suštine mnogih naučnih dostignuća, bili mi svesni te činjenice ili ne. Od tog okeana ideja i disciplina izabrao sam da tema ovog master rada budu linearni kodovi. Spoj teorije i prakse u oblasti teorije informacije i kodiranja me posebno privukao, zbog direktne veze sa osnovama matematičke pismenosti uopšte, kao što je algebra. Polazeći od jednostavnih algebarskih struktura, kao što su grupoidi, već u sledećem koraku definišemo polugrupe, asocijativne grupoide. Reči i jezik, videćemo, mogu da se posmatraju upravo kao jedna polugrupa. Reči čine kod, koji u kontekstu vektorskog prostora, ako se radi o linearnim kodovima, može da se izučava i daje izuzetna svojstva. Koncept ovog rada je da na neki optimalan način prikaže put od nekih osnova kodiranja do linearnih kodova. Upoznaćemo se samo sa najznačajnijim klasama, jer je teorija linearnih kodova zaista impozantna. Voleo bih da ovaj rad bude od koristi, bar kao početna literatura, onima koji žele da se detaljnije i opširnije bave linearnim kodovima. Na kraju bih izrazio zahvalnost mentoru profesoru Branimiru Šešelji, članovima komisije profesorici Andreji Tepavčević i profesoru Petru Đapiću, koji su mi pomogli i usmeravali savetima i sugestijama, kako bih ovaj master rad izložio i formulisao na najbolji način.

Bojan Berleković

Uvod

Sredinom dvadesetog veka intenzivira se razvoj visokih tehnologija, kompjuterskih nauka, uopšteno novih sredstava i načina komunikacije. Kao posledica pojavljuju se nove grane primenjene matematike kao što su teorijsko računarstvo, teorija informacije, teorija kodiranja, sve sa ciljem da se pronađu što optimalniji matematički modeli, koji će se moći što jednostavnije i što efikasnije implementirati u kompjuterskom inženjerstvu. Sintaktički, osnovni računarski jezici postaju (s obzirom na digitalnu tehnologiju), u suštini, nizovi nula i jedinica.

Ovaj rad bavi se temom iz teorije kodiranja. Smatra se da je ova teorija kao posebna disciplina započela razvoj radom Claude-a Shannon'-a „A mathematical theory of communication", objavljenim 1948. godine (*Bell.System Tech. J.* 27(1948), 623-656.). Time su počela istraživanja i u teoriji informacija, povezanoj sa kodiranjem. Teorija kodiranja razvijala se paralelno i u skladu sa napretkom kompjuterske tehnologije. Pored značajnih teorijskih rezultata u samoj matematici, ova teorija neposredno se primenjuje praktično u svim oblastima komunikacije kao što su satelitska i telefonska transmisija, optički kodovi, smeštanje podataka na kompakt diskove itd.

Pojam kodiranja odnosi se, pre svega, na prevođenje prirodnog meta-jezika na jezik računara. Postavljaju se razni zahtevi, prvenstveno vezano za optimalnost kodiranja, odnosno na pronalaženje kodova kojima će se informacija što brže prenositi komunikacijskim kanalom (u odnosu na broj kodnih simbola po jednom simbolu meta-jezika). Pored toga, istražuje se nalaženje takvih kodova uz pomoć kojih će biti moguće efikasno otkrivanje i ispravljanje grešaka nastalih u transmisiji podataka. Kodovi koji se koriste u digitalnoj tehnologiji su pre svega blok-kodovi i to binarni, sa bazom 2, ali se teorija kodiranja bavi istraživanjem širih klasa kodova, blok-kodova sa proizvoljnom bazom, kao i kodova sa promenljivom dužinom kodnih reči. Matematičke oblasti na kojima se zasnivaju istraživanja u teoriji kodiranja zavise od cilja istraživanja. Za probleme optimalnosti i analizu svojstava izvora informacije i komunikacijskih kanala koristi se statistička teorija informacija, dakle teorija verovatnoće. Proučavanje metoda ze otkrivanje i ispravljanje grešaka bazira se na algebarskim strukturama (grupe, prsteni, polja, polinomi), linearnoj algebri (vektorski prostori) i diskretnoj matematici. Za određene klase kodova (aritmetički kodovi), kao i za ispravljanje specifičnih grešaka (ispadanje i umetanje simbola) koristi se teorija brojeva.

Ovaj rad baviće se značajnom oblašću teorije kodiranja, koja se odnosi na kodove za ispravljanje grešaka. Najvažnija klasa kodova u ovom kontekstu su linearni kodovi, koji su se pokazali kao veoma efikasni u konkretnim primenama. Predstavićemo pre svega Hamming-ove, Golay-eve, Reed-Muller-ove kodove, opisaćemo njihove konstrukcije i metode dekodiranja, a bavićemo se i najznačajnijim vrstama polinomnih kodova, cikličnim i BCH kodovima.

S obzirom da se u konstrukciji i proučavanju ovih kodova koriste neke oblasti klasične algebre, kao što su grupe, vektorski prostori, konačna polja i polinomi nad njima, i odabrane teme iz ovih oblasti biće adekvatno izložene u radu.

1 Osnovne definicije i tvrđenja

1.1 Opšti pregled algebarskih struktura

DEFINICIJA 1.1.1 **Grupoid** $(G,*)$ je algebarska struktura, gde je skup G nosač, a „$*$“ binarna operacija definisana na nosaču G. Grupoid $(G,*)$ je **polugrupa** ako važi zakon asocijativnosti tj. $(\forall x,y,z \in G)((x*y)*z = x*(y*z))$. Polugrupa $(G,*)$ je **grupa** ako ispunjava sledeća dva uslova: $(\exists e \in G)(\forall x \in G)(e*x = x*e = x)$ (postojanje neutralnog elementa) i $(\forall x \in G)(\exists x^{-1} \in G)(x*x^{-1} = x^{-1}*x = e)$ (postojanje inverznog elementa). Ako grupa ispunjava zakon komutativnosti odnosno $(\forall x,y \in G)(x*y = y*x)$, zovemo je još i **Abelova** grupa.

PRIMER 1.1.2 $(\mathbb{N},+)$ je grupoid, koji je ujedno i polugrupa. Poznata je i tzv. polugrupa transformacija $(\{f|f: A \longrightarrow A\}, \circ)$, čiji su elementi funkcije jednog skupa samog u sebe, i operacija je kompozicija funkcija. $(\mathbb{Z},+)$ je grupa celih brojeva i ona je Abelova.

□

DEFINICIJA 1.1.3 $(H,*)$ je **podgrupa** grupe $(G,*)$ ako važi da je $\emptyset \neq H \subseteq G$ i $(\forall x,y \in H)(x*y^{-1} \in H)$. Levi **koset** ili leva **klasa** aH po podgrupi H, grupe $(G,\cdot)$ je skup $\{ah|h \in H\}$ (analogno se definiše i desni koset). Ako važi $(\forall g \in G)(gH = Hg)$, podgrupu H zovemo **normalnom** podgrupom grupe G, u oznaci $H \lhd G$.

PRIMER 1.1.4 $(\mathbb{Q}\backslash\{0\},\cdot)$ je normalna podgrupa grupe $(\mathbb{R}\backslash\{0\},\cdot)$.

□

DEFINICIJA 1.1.5 **Prsten** $(R,+,\cdot)$ je algebarska struktura sa dve binarne operacije, koja ispunjava sledeće uslove:

1. $(R,+)$ je Abelova grupa;
2. $(R,\cdot)$ je polugrupa;
3. $(\forall x,y,z \in R)(x\cdot(y+z) = x\cdot y + x\cdot z \ \wedge (x+y)\cdot z = x\cdot z + y\cdot z)$ (zakoni distributivnosti druge operacije prema prvoj, $\cdot$ prema $+$).

Prsten je **sa jedinicom** ako postoji neutralni element za $(R,\cdot)$, a **komutativan** je ako važi $(\forall x,y \in G)(x\cdot y = y\cdot x)$. Prsten je **bez delitelja nule** ako $(\forall x,y \in G)(x\cdot y = 0 \Rightarrow x = 0 \vee y = 0)$, gde je 0 neutralni element za $(R,+)$.

DEFINICJA 1.1.6 Komutativni prsten sa jedinicom bez delitelja nule $(R,+,\cdot)$ naziva se **integralni domen**.

PRIMER 1.1.7 Neka je $\mathbb{Z}_n = \{0,1,2,\dots,n-1\}$ skup ostataka pri deljenju celog broja sa n. Tada je struktura $(\mathbb{Z}_n, +_n, \cdot_n)$ prsten tzv. prsten ostataka gde su binarne operacije, redom, sabiranje i množenje po modulu n. Prsten celih brojeva $(\mathbb{Z}, +, \cdot)$ je poznati integralni domen.

□

DEFINICIJA 1.1.8 Funkcija $f: (R, +, \cdot) \longrightarrow (P, +, \cdot)$, čiji su domen i kodomen prsteni, je **homomorfizam** ako $(\forall x, y \in R)(f(x+y) = f(x) + f(y) \wedge f(x \cdot y) = f(x) \cdot f(y))$. Ako je f i bijekcija onda je zovemo **izomorfizam** i za R i P kažemo da su **izomorfni** i to označavamo sa $R \cong P$.

PRIMER 1.1.9 Ako je $\mathbb{Z}/_{\equiv_n}$, gde je $(\forall a, b \in \mathbb{Z})(a \equiv_n b \Leftrightarrow n | a-b)$, jedna particija skupa celih brojeva po ovoj relaciji kongruencije (kongruencija prstena ρ je binarna relacija koja ispunjava dva uslova, (1) ρ je relacija ekvivalencije i (2) $(\forall x, y, z, t \in \mathbb{Z})(x \rho y \wedge z \rho t \Rightarrow x + z \rho y + t \wedge x \cdot z \rho y \cdot t)$) onda važi $\left(\mathbb{Z}/_{\equiv_n}, +, \cdot\right) \cong (\mathbb{Z}_n, +_n, \cdot_n)$ tj. ovi prsteni su izomorfni.

□

DEFINICIJA 1.1.10 Neprazni podskup I prstena $(R, +, \cdot)$ je **ideal**, ako važi:

1. $(\forall a, b \in I)(a - b \in I)$;
2. $(\forall r \in R)(\forall a \in I)(a \cdot r \in I \wedge r \cdot a \in I)$.

Ideal u komutativnom prstenu je **glavni** ako postoji element $g \in I$ tako da je $I = \langle g \rangle = \{r \cdot g \mid r \in R\}$. Element g je **generator** glavnog ideala.

PRIMER 1.1.11 Skup parnih brojeva $2\mathbb{Z}$ je glavni ideal u $\mathbb{Z}$, i generator je 2.

□

DEFINICIJA 1.1.12 Komutativni prsten sa jedinicom $(F, +, \cdot)$, gde je $(F \backslash \{0\}, \cdot)$ Abelova grupa je **polje**. Podskup E polja F je njegovo **potpolje** ako je $(E, +, \cdot)$ takođe polje za sebe, gde su operacije definisane na E restrikcije operacija polja F.

PRIMER 1.1.13 $(\mathbb{C}, +, \cdot)$ je polje kompleksnih brojeva, a polje realnih brojeva $(\mathbb{R}, +, \cdot)$ je njegovo potpolje.

□

DEFINICIJA 1.1.14 **Kompozicija** dva polja $E \cdot F$ je najmanje polje (u smislu poretka " $\subseteq$ ") koje sadrži polja E i F. **Karakteristika** polja F je najmanji prirodan broj n takav da je za svako $x \in F$, $x + \cdots + x = 0$, gde se x pojavljuje n puta u datoj jednakosti. Ako takvo n ne postoji kažemo da je polje beskonačne karakteristike ili karakteristike 0.

DEFINICIJA 1.1.15 Skup svih polinoma nad poljem F, $\{a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 | a_n, a_{n-1,\ldots,} a_{1,} a_0 \in F, n \in \mathbb{N}_0\}$ obrazuje **prsten polinoma**, u oznaci $F[x]$. Polinom $p(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$, $a_n \neq 0$ je **stepena n**. Ako je $a_n = 1$, polinom je **normiran**. Broj $\alpha \in F$ je **nula** ili **koren** polinoma $p(x)$ ako $p(\alpha) = 0$. Polinom najmanjeg stepena za koji je $p(\alpha) = 0$ zovemo **minimalni** polinom za α.

TVRĐENJE 1.1.16 (*Bezuov stav*) $p(\alpha) = 0 \Leftrightarrow x - \alpha | p(x)$.

■

TVRĐENJE 1.1.17 *Za svaka dva polinoma $p(x)$ i $q(x)$ postoje jedinstveni polinomi $s(x)$ i $r(x)$ koje redom nazivamo **količnik** i **ostatak**, a za koje važi $p(x) = s(x)q(x) + r(x)$, i stepen ostatka je strogo manji od stepena polinoma delioca $q(x)$.*

■

DEFINICIJA 1.1.18 $p(x) \equiv q(x)\ mod\ t(x)$ ako $p(x)$ i $q(x)$ daju isti ostatak pri deljenju sa polinomom $t(x)$, odnosno $t(x)|p(x) - q(x)$. **Najmanji zajednički sadržalac** za polinome $p(x)$ i $q(x)$ je polinom najmanjeg stepena, koji je deljiv sa oba polinoma. **Najveći zajednički delilac** je polinom najvećeg stepena sa kojim su deljiva oba polinoma. Polinom je **svodljiv** nad poljem F ako može da se predstavi kao proizvod dva polinoma stepena strogo manjih od stepena samog polinoma sa koeficijentima iz polja F. U suprotnom je **nesvodljiv**. Direktno imamo da su polinomi prvog stepena nad proizvoljnim poljem nesvodljivi.

PRIMER 1.1.19 Nad poljem $\mathbb{R}$, $NZS(x^3 - x^2 + x - 1, x^4 - 5x^3 + 8x^2 - 4x) = NZS\big((x-1)(x^2+1), x(x-2)^2(x-1)\big) = x(x-1)(x-2)^2(x^2+1)$, dok je $NZD(x^3 - x^2 + x - 1, x^4 - 5x^3 + 8x^2 - 4x) = x - 1$, a npr. polinom $x^2 + 1$ je nesvodljiv.

□

1.2 Konačna polja

DEFINICIJA 1.2.1 Konačna polja F su polja konačne kardinalnosti q, u oznaci $\boldsymbol{F_q}$ ili $\boldsymbol{GF(q)}$. **Primitivni element** polja F_q je element koji generiše celo polje, tj. $\alpha \in F_q$ takvo da je $F_q = \{0, \alpha^1, \alpha^2, \ldots, \alpha^{q-1}\}$, gde se stepenovanje odnosi na drugu operaciju u polju.

PRIMER 1.2.2 Prsteni ostataka po prostom modulu $(\mathbb{Z}_p, +_p, \cdot_p)$ su konačna polja i imaju kardinalnost p. Za $p = 2$, operacije polja su date sledećim Kejlijevim tablicama:

$\oplus$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

□

TVRĐENJE 1.2.3 *Svaki konačni integralni domen je konačno polje*.

Dokaz. Neka je F konačan integralni domen. Iz definicije 1.1.6 sledi da je $(F\backslash\{0\},\cdot)$ komutativna polugrupa sa jedinicom. Pokažimo još da svaki element iz $F\backslash\{0\}$ ima inverzni u ovoj polugrupi. Neka je a ne-nula element iz F, tada u nizu $a, a^2, a^3, \dots, a^n, \dots$ moraju postojati jednaki elementi, jer je F konačno, neka su to $a^s = a^t$, i bez umanjenja opštosti $s - t > 0$. Tada je $a^{s-t}a^t = a^t$, pa je dalje $a^{s-t}a^t - a^t = 0$, $a^t(a^{s-t} - 1) = 0$, a kako je F integralni domen direktno imamo da je $a^t \neq 0$ i onda mora $a^{s-t} - 1 = 0$, $a^{s-t} = 1$. Odavde dobijamo da $a^{s-t-1}a = 1$, $s - t - 1 \geq 0$, pa je $a^{-1} = a^{s-t-1}$. Dakle, $(F\backslash\{0\},\cdot)$ je Abelova grupa, pa je F polje.

■

DEFINICIJA 1.2.4 Prsten ostataka polinoma po modulu $f(x)$, gde je stepen polinoma $f(x)$, n nad konačnim poljem F_q, u oznaci $\left({F_q[x]}/{f(x)}, +, \cdot\right)$ je skup $\left\{a_m x^m + a_{m-1}x^{m-1} + \cdots + a_1 x + a_0 \middle| a_m, a_{m-1,\dots,} a_1, a_0 \in F_q, m < n\right\}$.

TVRĐENJE 1.2.5 *Svaki ideal u prstenu* $\left({F_q[x]}/{x^n - 1}, +, \cdot\right)$ *je glavni ideal*.

Dokaz. Neka je $g(x)$ ne-nula polinom u idealu I datog prstena ostataka najmanjeg stepena. Kako je po tvrđenju 1.1.17, $f(x) = k(x)g(x) + r(x)$, za proizvoljan polinom $f(x)$ iz ideala I, dobijamo da je stepen polinoma $r(x)$ manji od stepena polinoma $g(x)$, ali i da je $r(x) = f(x) - k(x)g(x) \in I$, što je kontradikcija sa izborom polinoma $g(x)$.

■

TVRĐENJE 1.2.6 $\left({F_q[x]}/{f(x)}, +, \cdot\right)$ *je integralni domen ako i samo ako je polinom* $f(x)$ *nesvodljiv nad poljem* F_q.

Dokaz. Prsten ostataka polinoma je svakako zbog svojstava polinoma komutativan i ima jedinicu. Ako je $f(x)$ nesvodljiv, a on je nula ovog prstena, onda nema delitelja nule, pa je dati prsten integralni domen. Suprotno, ako je $f(x)$ svodljiv postojaće delitelji nule i ovaj prsten neće biti integralni domen.

■

TVRĐENJE 1.2.7 *Za svaki prost broj* p i $n \in \mathbb{N}$ *postoji jedinstveno polje kardinalnosti* p^n. *A važi i obrat tj. svako konačno polje je kardinalnosti* p^n.

Dokaz. Daćemo samo skicu dokaza bez dokaza jedinstvenosti i obrata. Može se pokazati da će uvek postojati polinom $f(x)$ stepena n nad poljem $\mathbb{Z}_p$ koji je nesvodljiv. Tada je struktura $\left(\mathbb{Z}_p[x]/_{f(x)}, +, \cdot\right)$ na osnovu tvrđenja 1.2.3 i 1.2.6 konačan integralni domen odnosno konačno polje i ima p^n elemenata, jer se svaki od n koeficijenata polinoma iz ovog polja može izabrati na p načina.

■

PRIMER 1.2.8 Polinom $x^2 + x + 1$ je nesvodljiv nad poljem $\mathbb{Z}_2$. Sada imamo da je polje $GF(4) = \left(\mathbb{Z}_2[x]/_{x^2 + x + 1}, +, \cdot\right) = \{0, 1, x, x + 1\}$. Tablice operacija su sledeće:

$+$	0	1	x	$x+1$
0	0	1	x	$x+1$
1	1	0	$x+1$	x
x	x	$x+1$	0	1
$x+1$	$x+1$	x	1	0

$\cdot$	0	1	x	$x+1$
0	0	0	0	0
1	0	1	x	$x+1$
x	0	x	$x+1$	1
$x+1$	0	$x+1$	1	x

□

1.3 Vektorski prostori nad konačnim poljima

DEFINICIJA 1.3.1 Neka je $(V, +)$ Abelova grupa i $(F, +, \cdot)$ polje. Ako postoji funkcija "$\cdot$" : $F \times V \to V$ koja za sve $\alpha, \beta \in F$ i $a, b \in V$ ispunjava uslove:

(i) $\alpha \cdot (a + b) = (\alpha \cdot a) + (\alpha \cdot b)$;

(ii) $(\alpha + \beta) \cdot a = (\alpha \cdot a) + (\beta \cdot a)$;

(iii) $\alpha \cdot (\beta \cdot a) = (\alpha\beta) \cdot a$;

(iv) $1 \cdot a = a$, gde je 1 neutralni element za operaciju $\cdot$ u polju F,

strukturu $(V, +, \cdot, F)$ nazivamo **vektorskim prostorom V nad poljem F**. Elemente polja F zovemo **skalarima**, a elemente prostora V **vektorima**. Izraz $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n$ je **linearna kombinacija** vektora, gde su $\alpha_1, \alpha_2, \ldots, \alpha_n$ skalari, a $v_1, v_2, \ldots, v_n$ vektori.

DEFINICIJA 1.3.2 Vektori $v_1, v_2, \ldots, v_n$ su **linearno nezavisni** ako $\alpha_1 v_1 + \alpha_2 v_2 + \cdots + \alpha_n v_n = 0 \ \ (0 \in V) \Leftrightarrow \alpha_1 = \alpha_2 = \cdots = \alpha_n = 0 \ \ (0 \in F)$. Skup

linearno nezavisnih vektora $\{v_1, v_2, \dots, v_n\}$ je **baza** prostora V, ako se svaki vektor iz V može predstaviti kao linearna kombinacija nekih vektora iz tog skupa. Kardinalnost baze je **dimenzija** prostora V, u oznaci $dimV$.

DEFINICIJA 1.3.3 Skup $W \subseteq V$ je **potprostor** prostora V ako za sve $\alpha, \beta \in F$ i $a, b \in W$ sledi da je $\alpha a + \beta b \in W$, i to označavao sa $W \leq V$.

PRIMER 1.3.4 Vektorski prostor je skup uređenih n-torki realnih brojeva nad poljem realnih brojeva $(\mathbb{R}^n, +, \cdot, \mathbb{R})$, gde funkciju "$\cdot$" definišemo na sledeći način $a \cdot x \coloneqq (a \cdot x_1, \dots, a \cdot x_n)$ gde je operacija na koordinatama množenje u polju $\mathbb{R}$, a jedan njegov potprostor je skup uređenih n-torki gde su nule na parnim pozicijama. Operacija "+" se odnosi na sabiranje uređenih n-torki po koordinatama, tj. za $x, y \in \mathbb{R}^n$, $x + y = (x_1 + y_1, \dots, x_n + y_n)$, gde je operacija "+" na koordinatama sabiranje realnih brojeva.

□

DEFINICIJA 1.3.5 Definišimo binarnu operaciju „$\oplus$“ na skupu F_q^n za proizvoljno $n \in \mathbb{N}$. Za $x, y \in F_q^n$ $(x = (x_1, \dots, x_n)\ ,\ y = (y_1, \dots, y_n))$ je $x \oplus y = (x_1 \oplus y_1, \dots, x_n \oplus y_n)$, gde je na desnoj strani sa $\oplus$ označena prva operacija iz $GF(q)$.

PRIMER 1.3.6 Neka je $x = (1,0,1)$, $y = (0,0,1)$ tada je $x \oplus y = (1 \oplus 0, 0 \oplus 0, 1 \oplus 1) = (1,0,0)$ na osnovu tablice operacije $\oplus$ iz $GF(2)$.

□

TVRĐENJE 1.3.7: $(F_q^n, \oplus)$ *je Abelova grupa*.

Dokaz. Kao posledicu odgovarajućih osobina operacija na koordinatama imamo asocijativnost i komutativnost operacije $\oplus$ na F_q^n, neutralni elemenat je $(0, \dots, 0)$, a inverzni elemenat za $(x_1, \dots, x_n)$ je elemenat $(-x_1, \dots, -x_n)$, jer je u $GF(q)$ za svako $i = 1,2, \dots, n$, $x_i \oplus 0 = x_i$, $x_i \oplus (-x_i) = 0$.

■

DEFINICIJA 1.3.8 Preslikavanje $F_q \times F_q^n \to F_q^n$ u oznaci "$\cdot$" , definišemo na sledeći način:
Ako je $a \in F_q$ i $x = (x_1, \dots, x_n) \in F_q^n$, onda je $a \cdot x \coloneqq (a \cdot x_1, \dots, a \cdot x_n)$, gde je na desnoj strani sa $\cdot$ označena druga operacija polja $GF(q)$. Ovo je tzv. „množenje vektora skalarom“ (jer a ima jednu koordinatu, dok ih x ima n).

PRIMER 1.3.9 Za $a \in \{0,1\}$ i $x = (x_1, \dots, x_n) \in \{0,1\}^n$ $a \cdot x = (0, \dots, 0)$ za $a = 0$ i $a \cdot x = x$ za $a = 1$. Npr. neka je $a = 1$ i $x = (0,1,1,0)$, biće $a \cdot x = (0,1,1,0)$ jer $1 \cdot 0 = 0$ i $1 \cdot 1 = 1$ (na osnovu tablice operacije $\cdot$ na $GF(2)$).

□

TVRĐENJE 1.3.10 *Abelova grupa* $(F_q^n, \oplus)$ *je u odnosu na prethodno definisanu operaciju vektorski prostor nad* $GF(q)$ (*označavaćemo ga sa* S_q^n).

Dokaz. Neposrednim proveravanjem, koristeći osobine polja F_q, može se zaključiti da su za sve $\alpha, \beta \in F_q$ i $a, b \in F_q^n$ ispunjeni uslovi:

(i) $\alpha \cdot (a \oplus b) = (\alpha \cdot a) \oplus (\alpha \cdot b)$;

(ii) $(\alpha \oplus \beta) \cdot a = (\alpha \cdot a) \oplus (\beta \cdot a)$;

(iii) $\alpha \cdot (\beta \cdot a) = (\alpha \cdot \beta) \cdot a$;

(iv) $1 \cdot a = a$, gde je 1 neutralni element za operaciju $\cdot$ u polju $GF(q)$.

Važno je napomenuti da su četiri operacije označene sa dva znaka, $\oplus$ i $\cdot$, ali se prema objektima na koje se odnose vidi o kojim operacijama je reč.

■

PRIMER 1.3.11 Vektorski prostor S_2^4 čine vektori (0,0,0,0), (0,0,0,1)...(1,1,1,1) i ima ih ukupno 16. U njemu npr.

$$(1, 0, 1, 0) \oplus (0, 1, 1, 0) = (1, 1, 0, 0),$$
$$(1, 0, 0, 0) \oplus (1, 0, 0, 0) = (0, 0, 0, 0),$$
$$0 \cdot (1, 1, 1, 0) = (0, 0, 0, 0),$$
$$1 \cdot (0, 1, 1, 1) = (0, 1, 1, 1).$$

Inače, S_2^n je n-dimenzionalan vektorski prostor i jedna baza mu je skup {(1,0,…,0), (0,1,0,…,0),…,(0,0,…,1)}.

□

DEFINICIJA 1.3.12 **Norma** (težina) vektora $x \in \{0,1\}^n$, $x = (x_1, \dots, x_n)$, u oznaci $\|x\|$, definiše se jednakošću $\|x\| := \sum_{i=1}^n x_i$, gde je na desnoj strani zbir elemenata iz skupa {0,1}, kao prirodnih brojeva (ovo je dakle preslikavanje $\{0,1\}^n \to \mathbb{N}_0$).

PRIMER 1.3.13 Ako je $x = 11101011$, onda je $\|x\| = 1 + 1 + 1 + 0 + 1 + 0 + 1 + 1 = 6$.

□

(Vektore često označavamo i kao reči, tj. bez zagrada i zareza, ovde $x = 11101011$ i $x = (1,1,1,0,1,0,1,1)$ predstavljaju jedan isti vektor.)
Preko norme uvodimo još jedan važan pojam:

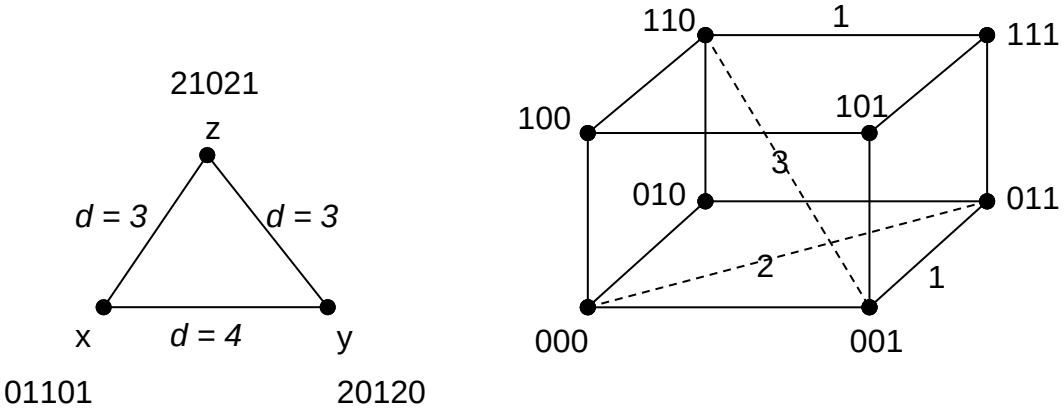
DEFINICIJA 1.3.14 **Hemingovo rastojanje** $d(x, y)$ vektora x i y iz $\{0,1\}^n$ definiše se jednakošću $d(x, y) := \|x \oplus y\| = \sum_{i=1}^n x_i \oplus y_i$. Uopšteno ako su vektori iz F_q^n imamo da je: $d(x, y) := d(x_1, y_1) + d(x_2, y_2) + \cdots + d(x_n, y_n)$ gde je za svako $i = 1,2,\dots,n$, $d(x_i, y_i) := \begin{cases} 1, & ako\ x_i \neq y_i \\ 0, & ako\ x_i = y_i \end{cases}$. Tada je norma vektora $\|x\| = d(x, 0)$, pa je $d(x, y) := \|x \oplus (-y)\| = \|x - y\|$. Možemo

zaključiti: norma vektora jednaka je broju njegovih ne-nula koordinata, a Hemingovo rastojanje između x i y jednako je broju koordinata na kojima se ti vektori razlikuju.

PRIMER 1.3.15 Ako je $x = 11001101$, $y = 10101010$ onda je $d(x,y) = \|01100111\| = 5$, gde su x i y iz $\{0,1\}^8$. Ako posmatramo F_3^6 tamo je npr. $d(012210,121200) = 4$, $\|102010\| = 3$.

□

PRIMER 1.3.16 Na crtežu levo su vektori iz F_3^5, a desno iz F_2^3:



Slika 1

□

LEMA 1.3.17 *Norma ima sledeće osobine*:

1. $\|x\| = 0$ *akko je* $x = (0,0,\ldots,0)$;
2. $\|x \oplus y\| \leq \|x\| + \|y\|$;
3. $|\|x\| - \|y\|| \leq \|x - y\|$.

Dokaz. Osobina 1 sledi iz definicije $\|x\| = d(x,0)$, a osobina 2 sledi direktno iz nejednakosti $x_i \oplus y_i \leq x_i + y_i$, $x_i, y_i \in F_q \subseteq \mathbb{N}_0$, gde su $\oplus$ i $+$ redom sabiranje po modulu q i obično sabiranje. Kako je na osnovu 2, $\|x\| = \|x - y + y\| \leq \|x - y\| + \|y\|$, pa je $\|x\| - \|y\| \leq \|x - y\|$ i slično od $\|y\|$, dobijamo $\|y\| - \|x\| \leq \|x - y\|$, pa sledi osobina 3.

■

LEMA 1.3.18 *Ako su* x, y, z iz F_q^n *onda je*:

a) $d(x,y) = 0$ *akko* $x = y$;
b) $d(x,y) = d(y,x)$;
c) $d(x,y) \leq d(x,z) + d(z,y)$.

Dokaz. Iskaz pod a) sledi iz činjenice da je rastojanje između dva vektora 0 akko se oni ne razlikuju. Iskaz pod b) važi zbog simetričnosti definicije

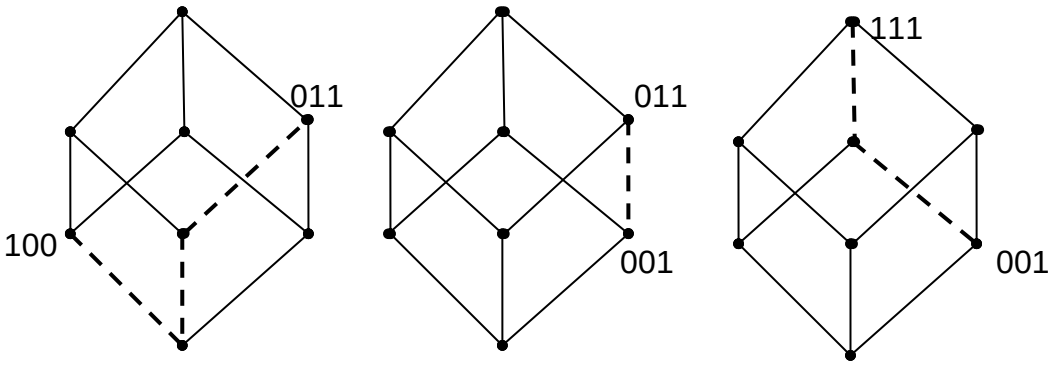
Hemingovog rastojanja, dok pod c) treba konstatovati da važi $d(x_i, y_i) \leq d(x_i, z_i) + d(z_i, y_i)$ za svako $i = 1,2,\ldots,n$.

■

POSLEDICA 1.3.19 *Uređeni par* (F_q^n, d) *je metrički prostor, pri čemu je* d: $F_q^n \times F_q^n \to \mathbb{N}_0$, *preslikavanje definisano Hemingovim rastojanjem*.

■

PRIMER 1.3.20 Metrički prostor $(\{0,1\}^n, d)$ ima jednostavnu geometrijsku interpretaciju. Elemente skupa $\{0,1\}^n$ možemo shvatiti kao temena n-dimenzionalne jedinične kocke u $\mathbb{R}^n$. Tada je $d(x, y)$ minimalan broj ivica kocke u nizu koji povezuje temena x i y. Rastojanje između vektora $x = 100$ i $y = 011$ je 3, $x = 001$ i $y = 011$ je 1, $x = 001$ i $y = 111$ je 2, odgovarajuća interpretacija na trodimenzionalnim jediničnim kockama data je na sledećoj slici, redom:



Slika 2

□

Izneti osnovni pojmovi teorije polinoma i vektorskih prostora nad konačnim poljima su osnova na kojoj ćemo predstaviti, uopšte, linearne kodove i ciklične kodove, kao jednu od značajnijih potklasa linearnih kodova. U narednim poglavljima biće prezentovana i osnova teorije kodiranja, koja nas uvodi u same linearne kodove kao potprostore vektorskih prostora nad konačnim poljima tj. u datom kontekstu, azbukama. Ciklični kodovi će baš zbog svoje osnovne osobine cikličnosti moći biti prezentovani kao ideali u prstenu ostataka polinoma po modulu $x^n - 1$. Akcenat će i biti, pre svega na algebarskim svojstvima , koje ispoljavaju ove klase kodova.

2 Osnove teorije kodiranja

2.1 Osnovni pojmovi

DEFINICIJA 2.1.1 Neprazan konačan skup X zovemo **alfabetom**, a njegove elemente **slovima**, dok **skup reči** nad alfabetom X definišemo na sledeći način:

$$X^* = X^1 \cup X^2 \cup \ldots \cup X^n \cup \ldots = \bigcup_{i\in\mathbb{N}} X^i$$

Uređene n-torke $(x_1, x_2, \ldots, x_n)$ iz X^* obeležavamo kao reči: $x_1x_2 \ldots x_n$.

DEFINICIJA 2.1.2 **Dužina** reči $x = x_1x_2 \ldots x_n$, u oznaci $|x|$, je broj slova od kojih je ona sastavljena (odnosno: $|x| = n$ ako i samo ako $x \in X^n$).

PRIMER 2.1.3 Nad alfabetom $X = \{0,1\}$, reči su 0,1,00,01,10,11,000, itd. a dužine su im redom 1,1,2,2,2,2,3, itd.

□

DEFINICIJA 2.1.4 Na skupu X^* uvodi se binarna operacija **nadovezivanja** (dopisivanja, konkatenacije):

Ako su x, y iz X^*, $x = x_1x_2 \ldots x_n$, $y = y_1y_2 \ldots y_m$, onda je
$z = xy$,
gde je $z = x_1x_2 \ldots x_ny_1y_2 \ldots y_m$.

Reč x je **prefiks** u reči z ako i samo ako postoji reč y, tako da je $z = xy$.
Slično, y je **sufiks** u z ako i samo ako postoji x, tako da je $z = xy$.

PRIMER 2.1.5 Neka su date reči $x = 2010$ i $y = 010$ nad alfabetom $X = \{0,1,2\}$, tada je reč dobijena primenom operacije nadovezivanja x i y, $z = xy = 2010010$.

□

DEFINICIJA 2.1.6 Skup reči nad alfabetom X možemo proširiti sa praznim skupom $\emptyset$ za koji kažemo da je **prazna reč** (označava se i sa Λ).
Tako proširen skup reči označavamo sa $X^{\circledast} = X^* \cup \{\emptyset\}$.
Prazna reč je po definiciji prefiks, odnosno sufiks svake reči x iz $X^{\circledast}$:

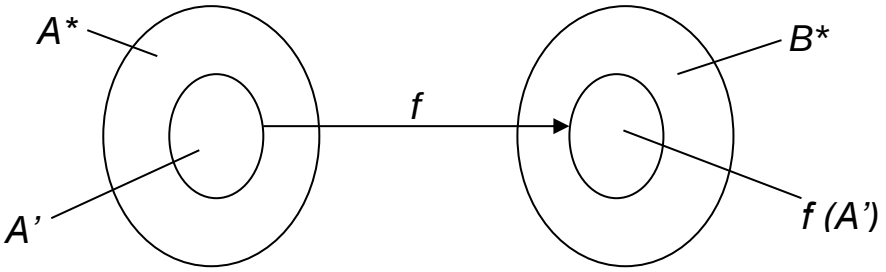
$$\emptyset x := x \text{ i } x\emptyset := x.$$

Dužina prazne reči je nula, takođe po dogovoru. U ovom skupu reči je zato svaka reč svoj (nepravi) prefiks, odnosno sufiks.

Kako je dopisivanje asocijativna operacija (jer za bilo koje reči x, y, z važi $(xy)z = x(yz)$), a prazna reč se ponaša kao neutralni element za ovu operaciju, zaključujemo da je uređeni par $(X^{\circledast}, \cdot)$ polugrupa sa jedinicom – monoid (sa „·“ smo označili operaciju dopisivanja).

DEFINICIJA 2.1.7 Konačni skupovi $A = \{\alpha_1, \ldots, \alpha_a\}, a > 1$, i $B = \{\beta_1, \ldots, \beta_b\}, b > 1$ predstavljaće redom **alfabet izvora** i **alfabet koda**. Prirodan broj b je **baza koda**.

DEFINICIJA 2.1.8 Neka je $A' \subseteq A^*$. Svako $1-1$ preslikavanje (injekcija) $f : A' \to B^*$ je jedno **kodiranje** reči nad alfabetom A.



Slika 3

Skup $V = f(A') \subseteq B^*$ je **kod**, a njegovi elementi su **kodne reči** odnosno kodne zamene odgovarajućih reči iz A'. Ako je $A' = A$, tada je kodiranje alfabetno, i tim kodiranjem ćemo se u nastavku i baviti.

PRIMER 2.1.9 Neka je $A = \{1,2,\ldots,9,0\}$ i $B = \{0,1\}$. Alfabet koda B je binaran, pa ilustrujemo binarno kodiranje dekadnih cifara (ovde se radi baš o alfabetnom kodiranju):

$$1 \to 10$$
$$2 \to 110$$
$$3 \to 1110$$
$$\ldots\ldots$$
$$9 \to 1111111110$$
$$0 \to 11111111110$$

□

DEFINICIJA 2.1.10 Što se tiče problema **dekodiranja**, ono se razmatra na dva načina:

a) Neka se poruke tj. reči iz skupa B^* kanalom bez smetnji upućuju primaocu. Tada je **dekodiranje** definisano na skupu B^* i to je postupak kojim se za svaku reč x iz B^* određuju (ako postoje) kodne reči $v_1, \dots, v_n$ iz V, tako da je $x = v_1 \cdots v_n$.

Ovo dekodiranje je jednoznačno ako se svaka reč iz B^*može na najviše jedan način predstaviti nadovezivanjem kodnih reči, tj. ako iz svake jednakosti: $v_1 \cdots v_m = w_1 \cdots w_n$, gde $v_1, \dots, v_m, w_1, \dots, w_n \in V$ sledi $m = n$ i $v_i = w_i, i = 1, \dots, m$.

NAPOMENA 2.1.11 Pojam **kanala** se odnosi na medijum za transmisiju poruka od kodera do dekodera, koji su sastavni delovi sistema za prenošenje poruka od izvora do primaoca.

b) Ako se poruke dekodiraju po prolasku kroz kanal sa smetnjama, svaka kodna reč x može se transformisati u neku drugu iz B^*. U kasnijem izlaganju više ćemo govoriti o ovom dekodiranju.

Kodovi mogu biti sa fiksiranom dužinom kodnih reči ili sa promenljivom dužinom kodnih reči. Mi ćemo se fokusirati na ove prve.

2.2 Kodiranje u kanalu sa smetnjama

DEFINICIJA 2.2.1 Poznatiji naziv za kodove sa fiksiranom dužinom kodnih reči je **blok-kodovi**, i oni se uvode na sledeći način:
Neka su:

$A = \{\alpha_1, \dots, \alpha_a\}$ alfabet izvora i
$B = \{\beta_1, \dots, \beta_b\}$ alfabet koda (b je baza koda)

Svako 1 – 1 preslikavanje $f : A \to B^n$, za neko $n \in \mathbb{N}$, je kodiranje sa fiksiranom dužinom (n) kodnih reči alfabeta A.
Skup $V = f(A) \subseteq B^n$ je **blok-kod**, n je njegova dužina i ako je $|B| = b = 2$, kažemo da je on binaran.
Da bi svako slovo alfabeta A mogli na jedinstven način kodirati (kodiranje je jedna injekcija) B^n mora biti određene minimalne kardinalnosti, pa imamo sledeće tvrđenje, koje nam daje potreban i dovoljan uslov za postojanje blok-koda iz B^n.

TVRĐENJE 2.2.2 *Da bi postojao blok-kod* $V \subseteq B^n$, $|B| = b$, b, $n \in \mathbb{N}$, *kardinalnosti* $a \in \mathbb{N}$, *potrebno je i dovoljno da važi*:

$$n \geq \frac{log\, a}{log\, b}$$

Dokaz. Kodnih reči ne može biti više od svih reči u skupu B^n. Otuda, ako postoji takav kod, važi $a \leq b^n$. Logaritmovanjem se sada neposredno dobija tražena nejednakost. Slično je i u obrnutom smeru.

■

PRIMER 2.2.3 Tako npr. za kodiranje dekadnih cifara binarnim kodom, gde zahtevamo kod od 10 kodnih reči, moramo imati njihovu dužinu od najmanje 4, jer je $\log_2 10 \approx 3{,}2$. Evo primera najpoznatijih kodova dekadnih cifara:

cifra	BCD kod	kod Gray-a	kod „plus 3“	kod Gray Stibitz-a	Kod Aiken-a
0	0000	0000	0011	0010	0000
1	0001	0001	0100	0110	0001
2	0010	0011	0101	0111	0010
3	0011	0010	0110	0101	0011
4	0100	0110	0111	0100	0100
5	0101	0111	1000	1100	1011
6	0110	0101	1001	1101	1100
7	0111	0100	1010	1111	1101
8	1000	1100	1011	1110	1110
9	1001	1101	1100	1010	1111

Tabela 1

□

PRIMER 2.2.4 ISBN-10 (International Standard Book Number) odnosno Međunarodni standardni knjižni broj je kod sa dužinom kodne reči 10, kojim se označavaju izdate knjige. Prve dve cifre označavaju jezičku grupu kome pripada izdanje, od 3. do 6. pozicije su cifre kojim se označava izdavač knjige, od 7. do 9. cifre su redni broj same knjige, i poslednja cifra je kontrolna a računa se tako da se svaka cifra množi svojim rednim mestom i sve se sabere i izračuna po modulu 11, ako se dobije 10, stavlja se oznaka X. Npr. kontrolna cifra za broj 790122467? je $7 \cdot 1 + 9 \cdot 2 + 0 \cdot 3 + 1 \cdot 4 + 2 \cdot 5 + 2 \cdot 6 + 4 \cdot 7 + 6 \cdot 8 + 7 \cdot 9\ (mod\ 11) = 190\ (mod\ 11) = 3$. Kod ISBN-13 poslednja kontrolna trinaesta cifra se računa kao $x_{13} = (10 - (x_1 + 3x_2 + x_3 + 3x_4 + \cdots + x_{11} + 3x_{12}))\ (mod\ 10)$.

□

U drugom delu ovog poglavlja biće predstavljen opšti metod dekodiranja blok-kodova i otkrivanja grešaka. Pre svega upoznaćemo se sa pojmovima matrice kanala, tj. medijuma za prenos poruka.

DEFINICIJA 2.2.5 **Matrica kanala sa uslovnim verovatnoćama**. Neka su U i V redom ulazni i izlazni alfabet, i $|U| = a$ i $|V| = b$. Tada sa $p(v_s|u_t)$ označavamo verovatnoću da se ulazno slovo u_t pretvorilo na izlazu iz kanala u slovo v_s (zbog eventualnih smetnji u transmisiji). Da bi ovo jednostavnije beležili za čitave alfabete U i V koristimo sledeći matrični prikaz:

$$P = \begin{bmatrix} p(v_1|u_1) & \cdots & p(v_b|u_1) \\ \vdots & \vdots & \vdots \\ p(v_1|u_a) & \cdots & p(v_b|u_a) \end{bmatrix} \quad ili \quad P = [P_{ij}] = \begin{bmatrix} P_{11} & \cdots & P_{b1} \\ \vdots & \vdots & \vdots \\ P_{1a} & \cdots & P_{ba} \end{bmatrix}$$

gde je i redni broj vrste tj. ulaznog simbola, a j redni broj kolone tj. izlaznog simbola.

Dakle matrica P je matrica kanala i ona ima sledeće osobine:

1. $p(v_j|u_i) \geq 0, i = 1, \ldots, a, j = 1, \ldots, b$;
2. $\sum_{j=1} p(v_j|u_i) = 1$, tj. zbir verovatnoća po vrstama je jednak 1 za svako $i = 1, \ldots, a$.

PRIMER 2.2.6 Iz matrice kanala za koji je $U = \{u_1, u_2\}, V = \{v_1, v_2, v_3\}$:

$$P = \begin{bmatrix} 0.35 & 0.4 & 0.25 \\ 0.35 & 0.4 & 0.25 \end{bmatrix}$$

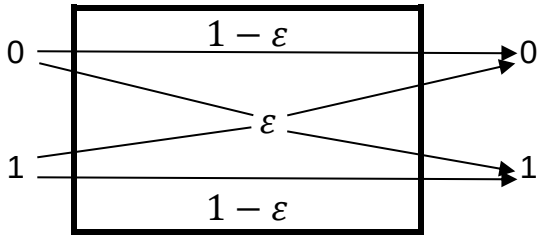
dobija se $p(v_1|u_1) = p(v_1|u_2) = 0.35$; $p(v_2|u_1) = p(v_2|u_2) = 0.4$; $p(v_3|u_1) = p(v_3|u_2) = 0.25$.

□

DEFINICIJA 2.2.7 Od posebnog značaja je binarni simetrični kanal BSC, čija je matrica oblika:

$$P = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix}, 0 \leq \varepsilon < \frac{1}{2}$$

U ovom slučaju je $U = V = \{0,1\}$, a verovatnoća greške tj. verovatnoća da 0 pređe u 1, ili obratno, je manja od 0.5 zbog korisnosti kanala. Ovaj kanal možemo prezentovati i pomoću sledećeg dijagrama:



Slika 4

U nastavku ćemo pretpostavljati da se elementi binarnog koda (sa kojim prvenstveno radimo) upućuju upravo kroz BSC.

DEFINICIJA 2.2.8 Za kod $V \subseteq \{0,1\}^n$ definiše se tzv. **kodno rastojanje** u oznaci $d(V)$, kao broj:

$$d(V) := \min_{u \neq v \in V} d(u,v)$$

gde je $d(u,v)$ Hemingovo rastojanje između vektora u i v. Definicija se odnosi i na kodove $V \subseteq B^n$, gde je B alfabet koda i $|B| > 2$.

PRIMER 2.2.9

a) Kodno rastojanje samog skupa $\{0,1\}^n$ iznosi 1(na primer $d(x,y) = 1$ gde je $x = (0,\ldots,0)$, $y = (0,1,0,\ldots,0)$);

b) Za kod $V = \{0101,1010,1100,0011,1111\}$ je $d(V) = 2$, jer je na primer $d(x,y) = 2$, gde je $x = 1111$, a $y = 1100$ i manjeg rastojanja između ma koja dva vektora iz V nema. Slično je za kod $V = \{01010,10111,10000\}$ $d(V) = 3$ jer je npr. $d(x,y) = 3$ za $x = 01010$ i $y = 10000$ i manjeg rastojanja nema.

c) Ternarni kod $V = \{012,211,010,200\}$ ima kodno rastojanje $d(V) = 1$, jer imamo da je $d(012,010) = 1$ i očigledno nema manjeg rastojanja.

□

Sposobnost koda da otkrije ili ispravi greške zavisi upravo od kodnog rastojanja između svih parova kodnih reči koda V, čime se bavimo u nastavku.

NAPOMENA 2.2.10 Naredne definicije, tvrđenja i primeri u ovoj glavi će se odnositi isključivo na binarne kodove, uz činjenicu da one mogu uvek da se sagledavaju i sa aspekta kodova gde je alfabet kardinalnosti veće od 2, imajući u vidu uopštenu definicuju Hemingovog rastojanja.

DEFINICIJA 2.2.11 Prolaskom kroz binarni simetrični kanal, reč $x \in \{0,1\}^n$ transformiše se u reč $y \in \{0,1\}^n$, gde je $y = x \oplus e$. Vektor $e = e_1 \ldots e_n \in \{0,1\}^n$ je **vektor greške**.
Šematski:

$$x = x_1 \ldots x_n \rightarrow \text{KANAL} \rightarrow y = y_1 \ldots y_n$$

$$\uparrow$$

$$e = e_1 \ldots e_n$$

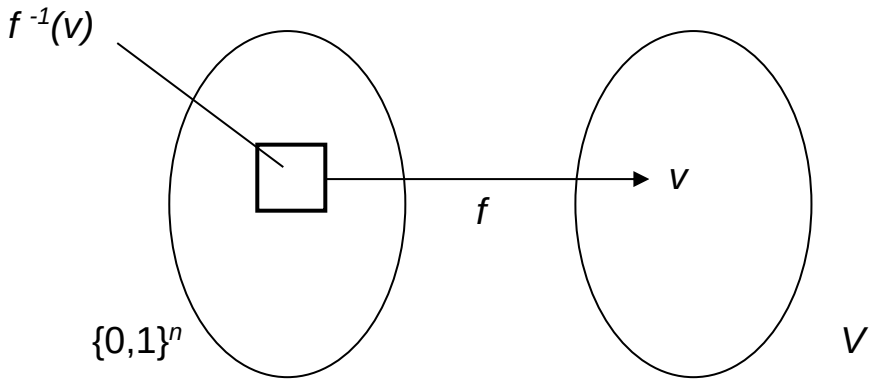
Slika 5

S obzirom na spomenutu prirodu BSC, $e_i = 0$ sa verovatnoćom $1 - \varepsilon$ (u kom slučaju se i-ta koordinata ne menja), a $e_i = 1$ sa verovatnoćom ε (na i-toj koordinati došlo je do greške oblika $0 \to 1$ ili $1 \to 0$). Ako se y razlikuje od x na s $(0 \leq s \leq n)$ koordinata, kažemo da je y dobijeno iz x usled s grešaka (ustvari to se događa kada je $\|e\| = s$).

PRIMER 2.2.12 Ako je $x = 1001110$ onda je reč $y = 1111110$ dobijena iz x usled 2 greške, a $z = 1000000$ usled tri greške.
Dakle, Hemingovo rastojanje izmedju reči x i y (dobijene iz x) iznosi baš s.

□

DEFINICIJA 2.2.13 Svako preslikavanje f skupa $\{0,1\}^n$ na skup V (kod V) je jedno **dekodiranje** reči iz $\{0,1\}^n$. Dekodiranjem f kao funkcijom određeno je jedno razbijanje skupa $\{0,1\}^n$ na disjunktne podskupove $f^{-1}(v), v \in V$ (to je jezgro funkcije f, odnosno jedna particija skupa $\{0,1\}^n$):



Slika 6

Sledeći stav daje opšti postupak dekodiranja kojim se prevazilaze eventualne smetnje u transmisiji.

TVRĐENJE 2.2.14 *Neka je BSC dat matricom*:

$$P = \begin{bmatrix} 1-\varepsilon & \varepsilon \\ \varepsilon & 1-\varepsilon \end{bmatrix}, 0 < \varepsilon < \frac{1}{2}$$

i kod $V \subseteq \{0,1\}^n$. *Tada za sve* $u, v \in V$ i $x \in \{0,1\}^n$, *važi*:

$$p(x|u) > p(x|v) \text{ akko } d(u,x) < d(v,x)$$

Dokaz. BSC je kanal bez memorije, pa je za $x = x_1 \cdots x_n$ i $u = u_1 \cdots u_n$ ispunjeno:

$$p(x|u) = p(x_1 \cdots x_n|u_1 \cdots u_n) = p(x_1|u_1) \cdots p(x_n|u_n)$$

(kada je kanal bez memorije, svako slovo ulazne reči u može nezavisno od ostalih slova postati odgovarajuće slovo reči x, pa zato važi navedena jednakost), pa je zato dalje:

$$p(x|u) = \varepsilon^{d(u,x)}(1-\varepsilon)^{n-d(u,x)}$$

($d(u,x)$ je, kao što smo uočili, broj grešaka zamene na reči u, a verovatnoća svake od tih grešaka je ε).

Slično je $p(x|v) = \varepsilon^{d(v,x)}(1-\varepsilon)^{n-d(v,x)}$. Odatle je:

$$(*)\ \frac{p(x|u)}{p(x|v)} = \frac{\varepsilon^{d(u,x)}(1-\varepsilon)^{n-d(u,x)}}{\varepsilon^{d(v,x)}(1-\varepsilon)^{n-d(v,x)}} = \left(\frac{1-\varepsilon}{\varepsilon}\right)^{d(v,x)-d(u,x)}$$

S obzirom da je po pretpostavci $0 < \varepsilon < \frac{1}{2}$, ispunjeno je $\frac{1-\varepsilon}{\varepsilon} > 1$, pa dokaz sledi neposredno iz (*).

■

U raznim literaturama ovo tvrđenje naziva se još i princip dekodiranja najbližim susedom.

Jednostavnije rečeno na osnovu ovog tvrđenja imamo da je verovatnoća da, pri propuštanju kodne reči $u \in V$ kroz BSC, na izlazu dobijemo reč x veća od verovatnoće da se od $v \in V$ (na ulazu) dobije x na izlazu akko je rastojanje Heminga izmedju u i x manje od Hemingovog rastojanja između v i x. U skladu sa ovim dekodiranje $f : \{0,1\}^n \to V$ treba definisati tako da se svaka reč iz $\{0,1\}^n$ preslika u njoj najbližu, u smislu metrike Heminga, kodnu reč iz V. Taj postupak nije u opštem slučaju jednoznačan, jer može postojati više reči iz V koje su na istom rastojanju od reči koju preslikavamo. U sledećem primeru izloženo je jedno dekodiranje datog koda V, zadavanjem klasa $f^{-1}(v), v \in V$.

PRIMER 2.2.15 Neka je $V = \{0000,1100,0101,1101\}$. Jedno dekodiranje skupa $\{0,1\}^4$ motivisano prethodnim tvrđenjem je sledeće razbijanje tog skupa:

$f^{-1}(0000)$	$f^{-1}(1100)$	$f^{-1}(1101)$	$f^{-1}(0101)$
0000	1100	1101	0101
1000	0100	1001	0001
0010	1110	0111	0110
0011	1010	1011	1111

Tabela 2

Ovo dekodiranje f razbija skup $\{0,1\}^4$ (ovaj skup ima 2^4 elemenata) na četiri klase pri čemu svakoj klasi pripada kodna reč iz V koja „određuje“ tu klasu jer je tada rastojanje Heminga najmanje moguće i iznosi 0, a ostali članovi klase su joj bliski po rastojanju Heminga i to rastojanje u ovom primeru je najviše 2. Važno je napomenuti da kodna reč koja pripada jednoj klasi ne može istovremeno pripadati i još nekoj klasi jer one tada ne bi bile disjunktne i da ovo razbijanje skupa $\{0,1\}^4$ nije jednoznačno, npr. u tablici 1000 i 0100 mogu zameniti mesta (klase) jer su oba na rastojanjima 1 od reči 0000 i 1100.

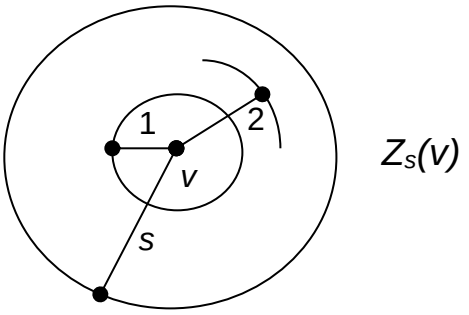
□

U nastavku se opisuju kodovi koji omogućuju ispravljanje odnosno otkrivanje određenog broja grešaka do kojih dolazi u transmisiji.

DEFINICIJA 2.2.16 Neka je dat kod $V \subseteq \{0,1\}^n$. Za $v \in V$ i $0 \leq s \leq n$, neka je

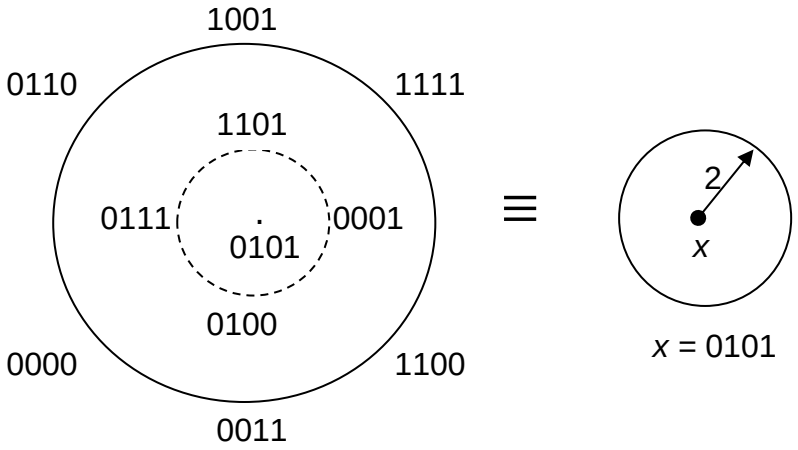
$$Z_s(v) = \{x \mid x \in \{0,1\}^n \ i \ d(v,x) \leq s\}.$$

$Z_s(v)$ je dakle skup svih reči iz $\{0,1\}^n$ koje se iz v mogu dobiti usled najviše s grešaka. U metričkom prostoru $(\{0,1\}^n, d)$ $Z_s(v)$ je lopta sa centrom u v i poluprečnikom s (kao na sledećoj slici).



Slika 7

PRIMER 2.2.17 $v = 0101, s = 2$:



Slika 8

$d=0$	$d=1$	$d=2$
		1001
	1101	1111
0101	0001	1100
	0100	0011
	0111	0000
		0110

Tabela 3

□

NAPOMENA 2.2.18 Ako je reč $x \in \{0,1\}^n$ nastala iz reči $v \in V$ usled s grešaka, onda je jasno da se x ispravno dekodira funkcijom $f : \{0,1\}^n \to V$, ako važi

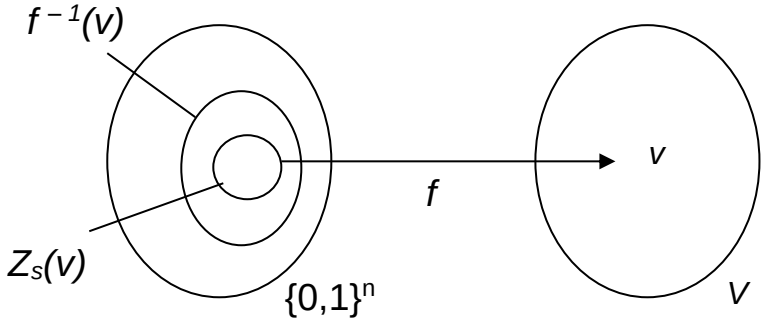
$$x \in Z_s(v) \cap f^{-1}(v),$$

tj. ako $f^{-1}(v)$ klasa sadrži x koje se nalazi na rastojanju s od reči v.

DEFINICIJA 2.2.19 Za kod $V \subseteq \{0,1\}^n$ kažemo da omogućuje **ispravljanje s grešaka** ($0 \leq s \leq n$) ako postoji dekodiranje f takvo da važi:

$$Z_s(v) \subseteq f^{-1}(v),$$

za svako $v \in V$ (kao na slici),



Slika 9

tj. kod V omogućuje ispravljanje s grešaka ako se sve reči $x \in \{0,1\}^n$ koje se nalaze na rastojanju najviše s od $v \in V$ nalaze u klasi $f^{-1}(v)$.

Drugačije rečeno, ako postoji dekodiranje koda V po kome se sve reči koje se od kodne reči v razlikuju na najviše s mesta dekodiraju kao v, onda V omogućuje ispravljanje s grešaka.
Za razliku od ispravljanja grešaka, otkrivanje shvatamo kao blaži uslov:
-znamo da se primljena poruka razlikuje od poslate, ali ne znamo koji su simboli pogrešno preneti. Sledi definicija odgovarajućeg koda.

DEFINICIJA 2.2.20 Kod $V \subseteq \{0,1\}^n$ omogućuje **otkrivanje s grešaka** ($0 \leq s \leq n$) ako za svako $v \in V$ važi:

$$\text{Ako je } x \in Z_s(v), \text{ onda } x \notin V / \{v\}.$$

Drugim rečima ako se prilikom javljanja najviše s grešaka na kodnoj reči ne dobije neka druga kodna reč, onda kod omogućuje otkrivanje s grešaka.

Iz prve definicije zaključuje se da kod V omogućuje ispravljanje s grešaka akko su svi skupovi $Z_s(v)$, $v \in V$ u parovima disjunktni u $\{0,1\}^n$. Prema drugoj definiciji , kod V otkriva s-grešaka akko nijedna kodna reč nije u s-okolini neke druge kodne reči. O ovome govori naredno tvrđenje.

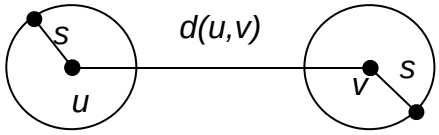
TVRĐENJE 2.2.21

a) *Kod* $V \subseteq \{0,1\}^n$ *omogućuje ispravljanje* s *grešaka ako i samo ako je* $d(V) > 2s$;

b) *Kod* $V \subseteq \{0,1\}^n$ *omogućuje otkrivanje* s *grešaka ako i samo ako je* $d(V) > s$.

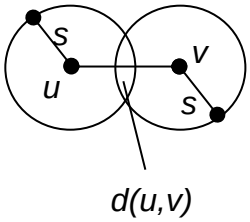
Dokaz.

a) V omogućuje ispravljanje s grešaka ako i samo ako su klase $Z_s(v)$, $v \in V$ disjunktne tj. ako i samo ako je za sve $u, v \in V, d(u,v) > 2s$ (kao na sledećoj slici).



Slika 10

b) Implikacija u definiciji koda koji otkriva s grešaka važi ako i samo ako u s-okolini kodne reči $v \in V$ nema nijedne druge reči iz V, a to važi tačno kada je $d(V) > s$ (videti sliku).



Slika 11

■

PRIMER 2.2.22

a) Neka je dat kod $V \subseteq \{0,1\}^3$, $V = \{000, 011, 101, 110\}$. Proverom možemo utvrditi da je $d(V) = 2$ odakle na osnovu prethodno pokazanog tvrdjenja sledi da je $s = 1$ tj. da ovaj kod omogućuje otkrivanje najviše jedne greške i da se u s-okolini svake od kodnih reči ne nalazi ni jedna druga kodna reč iz V. Uočljivo je da ovaj kod ne omogućava ispravljanje grešaka.

b) Kod $V = \{00000000, 00011111, 11111000, 11100111\}$ omogućuje ispravljanje najviše dve greške s obzirom da je $d(V) = 5$. Npr. reč 01011011 dekodira se kao njoj najbliža kodna reč 00011111, od koje je i postala usled dve greške, ili recimo reč 11111010 dekodira se kao 11111000 jer je od nje nastala usled jedne greške. Isti kod otkriva najviše četiri greške. Npr. reč 00111100 (u kanalu u kome se ne može desiti više od četiri greške) može se dekodirati kao bilo koja od kodnih reči 11111000,00011111 jer se od svake razlikuje na tri mesta, reč 10101100 može se dekodirati kao reč 11111000 jer je ona po rastojanju Heminga ovoj reči najbliža i to rastojanje iznosi 3.

□

Hemingov uslov. Sledeći zadatak je jedan od osnovnih u teoriji kodiranja. Za dati alfabet izvora kardinalnosti a, odrediti kod najmanje dužine n, tako da se mogu ispraviti sve greške kojih po pretpostavci u kanalu može biti najviše s $(0 \leq s \leq n)$.
Naredni stav daje delimično odgovor na to pitanje, jer govori o odnosu tih parametara: broja a slova u alfabetu, dužine koda n i broja grešaka s.

TVRĐENJE 2.2.23 *Neka je dat kod* $V \subseteq \{0,1\}^n$, $|V| = a$, *čiji se elementi propuštaju kroz BSC i neka u kanalu može biti najviše* s *grešaka, na reči dužine* n. *Tada, da bi* V *omogućavao ispravljanje* s *i manje grešaka, potrebno je da važi*:

$$\frac{2^n}{\sum_{i=0}^{s}\binom{n}{i}} \geq a \quad (\textit{Hemingov uslov}).$$

Dokaz. Posmatrajmo skupove $Z_k(V), v \in V, k = 0, \dots, s$, odnosno njihove kardinalne brojeve: za dati $v \in V$, $|Z_0(v)| = 1$(tom skupu pripada samo v);

$|Z_1(v)| = 1 + n$ (pored vektora v u $Z_1(v)$ su svi oni koji se od njega razlikuju na jednom mestu, a takvih ima n);
$|Z_2(v)| = 1 + n + \binom{n}{2}$ i slično:
$|Z_s(v)| = 1 + n + \binom{n}{2} + \cdots + \binom{n}{s} = \sum_{i=0}^{s}\binom{n}{i}$.

Kod V omogućuje ispravljanje s grešaka ako i samo ako su sve klase $Z_s(v)$, $v \in V$ disjunktne. U tom slučaju za konstrukciju klasa potrebno je bar $a \cdot |Z_s(v)|$ elemenata u $\{0,1\}^n$. S obzirom da je $|\{0,1\}^n| = 2^n$, treba da važi:

$a \cdot \sum_{i=0}^{s}\binom{n}{i} \leq 2^n$, a odatle sledi i traženi uslov.

■

PRIMER 2.2.24 Pomenuti uslov je samo potreban jer ako je on zadovoljen to ne znači da se odgovarajući kod može konstruisati. Npr. brojevi $n = 4, s =$

1 i $a = 3$ zadovoljavaju Hemingov uslov, ali se ne može konstruisati binarni kod dužine 4 sa 3 elementa, koji ispravlja jednu grešku. Ako je recimo $v = v_1v_2v_3v_4$ jedna kodna reč onda već sledeća kodna reč ima na bar tri koordinate različite vrednosti na primer $w = v_1\overline{v}_2\overline{v}_3\overline{v}_4$ ($\overline{0}$=1 i $\overline{1}$=0). Treća kodna reč , koja se od obe razlikuje na bar tri koordinate ne postoji (tj. u četvoro-dimenzionalnoj jediničnoj kocki nije moguće izdvojiti tri disjunktne sfere poluprečnika 1).

	$s = 1$	$s = 2$
n	a	a
5	5	2
6	9	2
7	16	4
8	28	6
9	51	11
10	93	18

Tabela 4

U ovoj tablici izračunate su maksimalne vrednosti broja a koje zadovoljavaju nejednakost Heminga, za različite dužine kodnih reči n i jednu, odnosno dve(maksimalno) greške u kanalu. Npr. Za $s = 2$ i $n = 5$ biće $\frac{2^5}{1+5+\binom{5}{2}} = \frac{32}{16} = 2 \geq a$ odakle sledi da je $a = 2$. Vidimo da je za kodiranje dekadnih cifara ($a = 10$) u kanalu koji dopušta dve greške, potrebno uzeti dužinu kodnih reči bar 9, ako se želi kod koji omogućuje ispravljanje tih grešaka (jer je na osnovu tablice za $n = 9$ i $s = 2$ $a \leq 11$, pa je po Hemingovom uslovu ispravljanje moguće i za $a = 10$). Dakle od mogućih $2^9 = 512$ reči dužine 9 koristi se samo 10.

□

U dosadašnjem delu teksta, obradili smo teoriju vezanu za blok-kodove, odnosno kodove sa fiksnom dužinom kodnih reči. Među takvim kodovima nalaze se i linearni kodovi koji su predmet i cilj ovog master rada.

3 Linearni kodovi

3.1 Konstrukcija linearnih kodova

DEFINICIJA 3.1.1 Kod $V \subseteq B^n$, gde je $B = F_q$, je **linearan** (n,k)-kod $(0 \leq k \leq n)$ ako skup njegovih elemenata (vektora) obrazuje potprostor dimenzije k vektorskog prostora $S_q^n = (B^n, \oplus)$ nad poljem $GF(q)$. Za sam linearni kod V se može reći da je dimenzije k.

Zbog toga što su linearni kodovi definisani kao potprostori od S_q^n dobijamo niz osobina i svojstava, koje ih izdvajaju u jednu od najznačajnih kategorija u teoriji kodiranja. Sledeći deo ovog rada je zato posvećen baš njima.

LEMA 3.1.2 *Kod* $V \subseteq \{0,1\}^n$ *je linearan ako i samo ako je skup njegovih vektora (kodnih reči) zatvoren u odnosu na operaciju* $\oplus$ *sabiranja vektora*.

Dokaz. Ako je $(V, \oplus)$ potprostor od S_2^n, zatvorenost prema $\oplus$ očito važi. Obrnuto, ako važi taj uslov, onda je $0 \in V$ (zbog $x \oplus x = 0$, za $x \in V$), pa važi i implikacija:

$$\text{Ako } x \in V \text{ onda i } \alpha x \in V,\ \alpha \in \{0,1\}.$$

■

PRIMER 3.1.3

a) Kod $V = \{0000,0001,0100,0101\}$ je binaran linearan (4,2)-kod, jer je baza ovog potprostora kardinalnosti 2 (skup linearno nezavisnih vektora koji ga generiše) {0001,0100}.
b) V={000,001,002,010,011,012,020,021,022} je primer jednog ternarnog (3,2)-koda, gde je baza npr. {001,020}.

□

TVRĐENJE 3.1.4 *Kodno rastojanje* $d(V)$ *linearnog koda jednako je minimalnoj normi njegovih ne-nula vektora*.

Dokaz. Kako je $d(u,v) = \|u \oplus (-v)\| = \|u - v\|$, a $u - v \in V$, jer je V linearan kod, pa je $(V, \oplus)$ Abelova grupa, sledi tvrđenje.

■

TVRĐENJE 3.1.5 *Linearni* (n,k)*-kod* V *ima* q^k *elemenata*.

Dokaz. Kako u navedenom kodu V po pretpostavci ima k linearno nezavisnih vektora, svi vektori u njemu se mogu izraziti kao sledeća linearna kombinacija: $v = \alpha_1 x_1 \oplus \alpha_2 x_2 \oplus \ldots \oplus \alpha_k x_k$, $v \in V$, gde su $x_1, \ldots, x_k$ nekih k linearno nezavisnih vektora iz V. Kako $\alpha_i \in B$, za sve $1 \leq i \leq k$,

broj vektora iz V se svodi na broj nizova elemenata skupa B dužine k, a kojih ima q^k, jer je $|B| = q$.

■

DEFINICIJA 3.1.6 Zbog određenosti linearnog (n, k)-koda njegovom bazom, dovoljno nam je da je samo ona zadata. Vektore baze koda prezentujemo pomoću tzv. **generišuće matrice** $(k \times n)$ linearnog (n, k)-koda. Sledeći primer će ilustrovati konstrukciju linearnog koda, znajući njegovu generišuću matricu.

PRIMER 3.1.7 Neka je data matrica G binarnog linearnog (5,3) koda:

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

Pošto su $x_1 = 10011, x_2 = 11001$ i $x_3 = 11100$ vektori baze koda V, onda kodu V pripadaju sledeći vektori (reči):

$$\begin{aligned} 0 \cdot x_1 \oplus 0 \cdot x_2 \oplus 0 \cdot x_3 &= 00000 \\ 1 \cdot x_1 \oplus 0 \cdot x_2 \oplus 0 \cdot x_3 &= 10011 = x_1 \\ 0 \cdot x_1 \oplus 1 \cdot x_2 \oplus 0 \cdot x_3 &= 11001 = x_2 \\ 0 \cdot x_1 \oplus 0 \cdot x_2 \oplus 1 \cdot x_3 &= 11100 = x_3 \\ 0 \cdot x_1 \oplus 1 \cdot x_2 \oplus 1 \cdot x_3 &= 00101 \\ 1 \cdot x_1 \oplus 0 \cdot x_2 \oplus 1 \cdot x_3 &= 01111 \\ 1 \cdot x_1 \oplus 1 \cdot x_2 \oplus 0 \cdot x_3 &= 01010 \\ 1 \cdot x_1 \oplus 1 \cdot x_2 \oplus 1 \cdot x_3 &= 10110 \end{aligned}$$

Tako je $V = \{00000, 10011, 11001, 11100, 00101, 01111, 01010, 10110\}$. Kodno rastojanje $d(V)$ je 2, jer je npr. $\|00101\| = 2$.

□

DEFINICIJA 3.1.8 Za $x = x_1 \dots x_n$, $y = y_1 \dots y_n$, $x, y \in B^n$, definišemo **skalarni proizvod** na sledeći način:

$$x \circ y := x_1 y_1 \oplus \dots \oplus x_n y_n,$$

gde su „$\oplus$“ i „$\cdot$“ operacije polja $GF(q)$.
(„$\circ$“ je dakle, preslikavanje $(B^n)^2 \to B$, koje paru vektora iz S_q^n dodeljuje elemenat polja $GF(q)$).

Za ovo skalarno množenje ispunjeni su zakoni komutativnosti i distributivnosti prema sabiranju vektora: za sve $x, y, z \in B^n$

$$x \circ y = y \circ x$$
$$x \circ (y \oplus z) = (x \circ y) \oplus (x \circ z)$$

Vektori x i y su **ortogonalni** ako je $x \circ y = 0$.

PRIMER 3.1.9 Ako su $x = 000001$, $y = 100111$ i $z = 100010$, onda je npr. $x \circ y = 1$, a $y \circ z = 0$, tj. y i z su ortogonalni, a to su i x i z, jer je $x \circ z = 0$. Dok su $x = 1122$ i $y = 0101$ takođe ortogonalni.
Treba primetiti da za vektore iz $\{0,1\}^n$ sa parnom normom važi $v \circ v = 0$.

□

DEFINICIJA 3.1.10 Skup vektora iz B^n ortogonalnih sa svim vektorima linearnog (n, k)-koda V, je **ortogonalna dopuna** koda V i označava se sa $\bar{V}$.

TVRĐENJE 3.1.11 *Ako je V linearan (n, k)-kod, onda je $\bar{V}$ linearan $(n, n-k)$-kod.*

Dokaz. Skup $\bar{V}$ zatvoren je u odnosu na sabiranje vektora: Ako su x i y iz $\bar{V}$, onda je za svaki vektor $v \in V$: $x \circ v = 0$ i $y \circ v = 0$, pa je zbog osobine skalarnog proizvoda, $(x \oplus y) \circ v = 0$, tj. $x \oplus y \in \bar{V}$.
Da bismo pokazali da je $dim(\bar{V}) = n - k$, primetimo da se svi vektori iz $\bar{V}$ mogu dobiti iz matrične jednačine:

$$G \cdot x = 0,$$

gde je G generišuća matrica koda V (formata $k \times n$), x vektor kolona $(n \times 1)$, a 0 nula vektor $(k \times 1)$. (Ako je x ortogonalan na sve vektore baze prostora V, on je ortogonalan i na svaku njihovu linearnu kombinaciju, tj. na svaki vektor iz V). Kako je rang matrice G baš k, odgovarajući sistem:

$$\begin{aligned} &\alpha_{11}x_1 \oplus \ldots \oplus \alpha_{1n}x_n = 0 \\ &\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots, \quad \alpha_{ij} \in B \\ &\alpha_{k1}x_1 \oplus \ldots \oplus \alpha_{kn}x_n = 0 \end{aligned}$$

ima tačno $n - k$ slobodnih promenljivih $x_{i1}, \ldots, x_{in-k}$.
Neposredno se zaključuje da svih rešenja ima baš q^{n-k} odnosno da je $dim(\bar{V}) = n - k$.

■

NAPOMENA 3.1.12 Kodovi V i $\bar{V}$ su jedno drugom ortogonalne dopune.

DEFINICIJA 3.1.13 Značaj ortogonalne dopune se ogleda u tome da za vektor $x \in B^n$ možemo proveriti da li pripada kodu V, ako proverimo da li je x ortogonalan na bazu $\bar{V}$. Generišuća matrica koda $\bar{V}$ se označava sa F i formata je $((n-k) \times n)$ i naziva se **kontrolna matrica** koda V. Prethodnu konstataciju

vezanu za proveru pripadnosti vektora x kodu V, sada možemo beležiti kao:

$$F \cdot x = 0 \text{ ako i samo ako } x \in V.$$

PRIMER 3.1.14 Neka je:

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

kontrolna matrica jednog binarnog linearnog (6,3)-koda. Sam kod V odredićemo iz jednačine:

$$F \cdot x = 0, \text{ odnosno iz}$$

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 \end{bmatrix} \cdot \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \\ x_5 \\ x_6 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$$

Odatle je

$$\begin{aligned} x_1 \oplus x_3 \oplus x_5 &= 0 \\ x_2 \oplus x_3 \oplus x_6 &= 0 \\ x_4 \oplus x_5 \oplus x_6 &= 0 \end{aligned}$$

odnosno

$$\begin{aligned} x_1 &= x_3 \oplus x_5 \\ x_2 &= x_3 \oplus x_6 \\ x_4 &= x_5 \oplus x_6 \end{aligned}$$

Dakle, slobodne promenljive su x_3, x_5 i x_6. Ostale koordinate ćemo dobijati kada umesto ovih slobodnih promenljivih budemo uvrštavali vrednosti od (0,0,0) do (1,1,1). Na taj način ćemo dobiti 8 vektora koda V.

□

DEFINICIJA 3.1.15 U prethodnom primeru uočavamo da je k koordinata (gore: x_3, x_5 i x_6) dovoljno da se prenese informacija odnosno konstruišu sve kodne reči iz V. Te koordinate se zovu **informacijske**. A preostalih $n - k$ koordinata su **kontrolne** (one su tu zbog kontrole ako se jave greške u kanalu).

TVRĐENJE 3.1.16 *Neka je F kontrolna matrica linearnog (n, k)-koda V. Tada važi: za $r \in \mathbb{N}$, $d(V) \geq r$ ako i samo ako je svakih $r - 1$ kolona matrice F linearno nezavisno.*

Dokaz. Neka je za dati linearan kod V, $d(V) \geq r$ i neka je:

$$F = \begin{bmatrix} f_{11} & \cdots & f_{1n} \\ \vdots & \ddots & \vdots \\ f_{n-k,1} & \cdots & f_{n-k,n} \end{bmatrix} = [F_1 \quad F_2 \quad \ldots \quad F_n]$$

njegova kontrolna matrica ($F_i, i = 1, \ldots, n$ su vektori kolone te matrice).

Vektor $x = x_1 \ldots x_n$ iz B^n pripada kodu V ako i samo ako je $F \cdot x = 0$ tj.

$$[F_1 \quad F_2 \quad \ldots \quad F_n] \cdot \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

Ovo poslednje je ekvivalentno sa uslovom:

$$x_1 F_1 \oplus \ldots \oplus x_n F_n = 0 \ (*)$$

I zato, ako kolone $F_{i_1}, \ldots, F_{i_{r-1}}$ nisu linearno nezavisne, postoje $y_1, \ldots, y_{r-1}$ iz B koji nisu svi nule, tako da je

$$y_1 F_{i_1} \oplus \ldots \oplus y_{r-1} F_{i_{r-1}} = 0$$

gde je sa 0 označen vektor kolona sa $n - k$ nula. Ali, iz toga sledi da vektor y, koji ima nekih $r - 1$ koordinata $y_1 \ldots y_{r-1}$, a sve ostale koordinate su mu 0, pripada kodu V, a $\|y\| < r$, što nije moguće.

Obratno, ako je svakih $r - 1$ kolona linearno nezavisno, iz uslova (*) neposredno sledi da minimalna dužina ne-nula vektora u V mora biti bar r.

■

POSLEDICA 3.1.17 *Kako je kardinalitet od binarnog linearnog (n, k)-koda 2^k modifikacijom Hemingovog uslova za linearne kodove dobijamo sledeću nejednakost*:

$$\frac{2^n}{\sum_{i=0}^{s} \binom{n}{i}} \geq 2^k, \text{ odnosno } 2^{n-k} \geq \sum_{i=0}^{s} \binom{n}{i}.$$

■

DEFINICIJA 3.1.18 Neka su L_1 i L_2 dva linearna koda tako da važi $L_2 \subseteq L_1$. Skup $L_1|L_2 = \{(l_1|l_1 \oplus l_2) : l_1 \in L_1 \wedge l_2 \in L_2\}$, gde je $(a|b)$ oznaka za konkatenaciju kodnih reči a i b, nazivamo **konkatenacijski proizvod** dva linearna koda (u nekim knjigama se definiše kao $|u|u + v|$ konstrukcija ili direktna suma dva linearna koda).

TVRĐENJE 3.1.19 *Ako su L_1 i L_2 redom linearni (n, k_1) i (n, k_2) kodovi tako da $L_2 \subseteq L_1$ tada je $L_1|L_2$ linearan $(2n, k_1 + k_2)$ kod.*

Dokaz. Neka su $\{x_1, x_2, \dots, x_{k_1}\}$ i $\{y_1, y_2, \dots, y_{k_2}\}$ redom baze kodova L_1 i L_2. Tada je $\{(x_1|x_1), (x_2|x_2), \dots, (x_{k_1}|x_{k_1})\} \cup \{(0|y_1), (0|y_2), \dots, (0|y_{k_2})\}$ baza koda $L_1|L_2$, jer je očigledno linearno nezavisan skup reči i svaku reč oblika $(l_1|l_1 \oplus l_2)$ možemo izraziti kao linearnu kombinaciju reči iz ove unije.

■

TVRĐENJE 3.1.20 $d(L_1|L_2) = min\{2d(L_1), d(L_2)\}$.

Dokaz. Za svako $l_1 \in L_1$ važi da je $(l_1|l_1 + 0) \in L_1|L_2$ i $\|(l_1|l_1)\| = 2\|l_1\|$, takođe za svako $l_2 \in L_2$ je $(0|l_2) \in L_1|L_2$ i $\|(0|l_2)\| = \|l_2\|$, za l_1 i l_2 za koje su ove vrednosti minimalne dobijamo $2d(L_1)$ i $d(L_2)$, tako da je $d(L_1|L_2) \leq min\{2d(L_1), d(L_2)\}$. Sa druge strane ako su $l_1 \in L_1$ i $l_2 \in L_2$, tako da nisu oba 0, koristeći osobinu norme 3. iz leme 1.3.17 imamo da ako je $l_2 \neq 0$, $\|(l_1|l_1 \oplus l_2)\| = \|l_1\| + \|l_1 \oplus l_2\| = \|l_1\| + \|l_1 - (-l_2)\| \geq \|l_1\| + \|-l_2\| - \|l_1\| = \|-l_2\| = \|l_2\| \geq d(L_2)$, a ako je $l_2 = 0$, $\|(l_1|l_1 \oplus l_2)\| = \|(l_1|l_1)\| = 2\|l_1\| \geq 2d(L_1)$, tako da je $d(L_1|L_2) \geq min\{2d(L_1), d(L_2)\}$, pa sledi tvrđenje.

■

3.2 Dekodiranje linearnih kodova

O nekom opštem postupku dekodiranja već je bilo reči kada se spominjao princip dekodiranja najbližim susedom. Ovakvom logikom se i dalje vodimo, ali postepeno dolazimo i do važnih postupaka u dekodiranju kod linearnih kodova koristeći se posebnim svojstvima ovakvih kodova kao potprostora u odnosu na operaciju sabiranja vektora. Sada ćemo definisati pojmove koji će igrati ključnu ulogu prilikom dekodiranja linearnih kodova.

DEFINICIJA 3.2.1 Neka je, dakle, V linearan (n, k)-kod. Za proizvoljan vektor $x \in B^n$ neka je:

$$x \oplus V := \{x \oplus v \mid v \in V\}$$

Iz definicije koda V kao potprostora S_q^n sledi da je $(V,\oplus)$ (Abelova) podgrupa grupe $(B^n,\oplus)$. Zato je $x \oplus V$ **klasa** po (podgrupi) V u B^n. Sada ćemo navesti i dokazati leme, koje će nam biti od koristi u nastavku.

LEMA 3.2.2:

a) *Svaki vektor y iz B^n nalazi se u nekoj klasi po V;*
b) *x i y su u istoj klasi po V ako i samo ako $x - y \in V$ $(x \oplus (-y) \in V)$;*
c) *$x \oplus V = y \oplus V$, za svako $y \in x \oplus V$;*
d) *svaka klasa po V ima tačno q^k elemenata.*

Dokaz.

a) Trivijalno: y je bar u $y \oplus V$ (jer je vektor 0 u V);
b) Ako $x, y \in z \oplus V$, onda je $x = z \oplus u$ i $y = z \oplus v, u, v \in V$. Sledi, $x - y = u - v \in V$. Obrnuto, ako $x - y \in V$ onda je $x - y = v \in V$, pa je $x = y \oplus v \in y \oplus V$ i $y \in y \oplus V$.
c) Neka je $y \in x \oplus V$. Odatle $y = x \oplus v$, odnosno, $x = y - v$, za neko v iz V. Ako sada $z \in x \oplus V$, onda $z = x \oplus w$, za $w \in V$. Sledi $z = (y \oplus (-v)) \oplus w = y \oplus ((-v) \oplus w) \in y \oplus V$, pa $x \oplus V \subseteq y \oplus V$. Slično se dokazuje i obratna inkluzija.
d) Funkcija $f : V \to x \oplus V$, definisana sa $f(v) = x \oplus v$ je bijekcija, što se neposredno proverava. Zato vektora u svakoj klasi ima tačno onoliko, koliko i vektora u V, tj. q^k.

■

LEMA 3.2.3 *Familija* $\{x \oplus v \mid x \in B^n\}$ *je particija skupa* B^n.

Dokaz. Unija svih klasa je prema lemi 3.2.2 a) ceo skup B^n. Dalje ako $z \in (x \oplus V) \cap (y \oplus V)$, onda je:

$$z = x \oplus u = y \oplus v, u, v \in V.$$

Odatle, $y = x \oplus (u \oplus (-v))$, pa $y \in x \oplus V$ i zato prema lemi 3.2.2 c) $x \oplus V = y \oplus V$. Dakle, dve klase su ili disjunktne, ili se poklapaju.

■

Treba napomenuti da je i sam kod V jedna klasa, tj. to je klasa $0 \oplus V$.

Pretpostavimo sada da se na izlazu iz kanala pojavio vektor $y \in B^n$. Prema prethodnim lemama y pripada klasi $y \oplus V$. Ako je na ulazu u kanal bila predata reč $v \in V$, onda za vektor greške e važi:

$$e = y \oplus (-v) \in y \oplus V, \text{ jer je } y = v \oplus e$$

Otuda, klasu $y \oplus V$ čine svi (mogući) vektori greške za y.
Po principu najbližeg suseda, dekodiranjem se vektoru y pridružuje vektor $v = y \oplus (-e) = y - e$, gde je e vektor sa minimalnom normom u skupu $y \oplus V$.

DEFINICIJA 3.2.4 Jedinstveni vektor e sa minimalnom normom je **lider** odgovarajuće klase. Ako u $y \oplus V$ ima više vektora sa minimalnom normom, dekodiranje nije jednoznačno – može se uzeti bilo koji od njih.

Obično se uz kod V konstruiše i tablica klasa $x \oplus V, x \in B^n$ (sledeći primer to ilustruje).
Kako bi se jednostavno pronašla klasa $y \oplus V$ u toj tablici, može se primeniti praktičan algoritam do koga dolazimo sledećom analizom.

DEFINICIJA 3.2.5 Ako je F kontrolna matrica (n, k)-koda V, a $y \in B^n$ (vektor koji se pojavio na izlazu iz kanala), onda se vektor: $c = F \cdot y$ zove **korektor**

za y. Važi $c \in B^{n-k}$ i taj vektor je jednak nuli ako i samo ako $y \in V$. U opštem slučaju ako je $y = v \oplus e, v \in V$, imamo:

$$c = F \cdot y = F(v \oplus e) = F \cdot v \oplus F \cdot e = F \cdot e.$$

Na osnovu izloženog važi:

TVRĐENJE 3.2.6 *Dva vektora pripadaju istoj klasi po V ako i samo ako imaju isti korektor c.*

Dokaz. Ako su x i y iz iste klase i e vektor te klase sa minimalnom normom, kako su $v = x - e$ i $w = y - e$ iz V odnosno $x = v \oplus e$ i $y = w \oplus e$, dobijamo da x i y imaju isti korektor. Obratno, ako x i y nisu iz iste klase tada na osnovu leme 3.2.2 b) $x - y \notin V$. Dalje, neka su e_1 i e_2 redom vektori sa minimalnom normom iz klasa gde su x i y, a v i w iz V koji su dobijeni sabiranjem x sa e_1 i y sa e_2. Tada $0 \neq F(x - y) = F\big((v \oplus e_1) - (w \oplus e_2)\big) = F \cdot e_1 - F \cdot e_2 = c_1 - c_2$, pa sledi da korektori za x i y nisu isti.

■

Za dati vektor $y \in B^n$ na izlazu iz kanala se obavlja sledeća procedura:

a) odredi se korektor c iz jednačine $F \cdot y = c$;
b) u klasi koju određuje taj korektor (tj. u $y \oplus V$) pronađe se vektor e sa minimalnom normom, lider;
c) y se dekodira kao $v = y - e$.

PRIMER 3.2.7

a) Neka je $F = \begin{bmatrix} 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{bmatrix}$ kontrolna matrica (4,2) koda $V = \{0000,0101,1011,1110\}$.

	lider				korektor
klase po V	0000	0101	1011	1110	00
	0001	0100	1010	1111	01
	0010	0111	1001	1100	10
	1000	0011	0110	1101	11

Tabela 5

Ova tablica predstavlja razbijanje skupa $\{0,1\}^4$ na disjunktne klase $x \oplus V$, $x \in \{0,1\}^4$ i uz svaku klasu naveden je korektor c. Možemo zapaziti da korektori uvek vrše određenu numeraciju klasa, pošto klasa ima 2^{n-k}, a korektori različitih klasa su različiti i iz skupa su $\{0,1\}^{n-k}$, pa na taj način dobijamo redne brojeve klasa u binarnom zapisu počevši od nulte.

Neka se npr. na izlazu pojavio vektor $y = 1001$, njegov korektor dobijen iz jednačine $F \cdot y = c$ je 10, pa y dekodiramo kao $v = y \oplus e$, gde je $e = 0010$, pa je $v = 1011$. U ovoj klasi nije bilo problema, jer je e jedinstveni lider, dok bi se u slučaju klase u drugoj vrsti u tablici gde su i 0001 i 0100 minimalni, vektor y iz te klase mogao na više načina dekodirati.

Ovaj postupak ipak dolazi do punog izražaja u slučaju kodova sa mnogo većim brojem kodnih reči i većom dužinom.

b) Neka je $F = [0 \quad 2 \quad 0]$ kontrolna matrica jednog ternarnog (3,2) koda $V = \{000,001,002,100,101,102,200,201,202\}$, tada razbijanje izgleda ovako

	lider									korektor
klase po V	000	001	002	100	101	102	200	201	202	0
	020	021	022	120	121	122	220	221	222	1
	010	011	012	110	111	112	210	211	212	2

Tabela 6

Neka se na izlazu pojavila reč $y = 121$, korektor te reči je 1, tako da se ona nalazi u drugoj vrsti (klasi) tablice, lider te klase je reč 020, tako da izlaznu reč dekodiramo kao reč $v = 121 - 020 = 101$.

□

3.3 Hemingovi[1] kodovi

Sada ćemo navesti primere dva tipa linearnih kodova sa posebnim svojstvima, tj. one koji omogućavaju otkrivanje i one koji omogućavaju ispravljanje greške, tzv. **Hemingove kodove**.

DEFINICIJA 3.3.1 **Kodovi koji omogućavaju otkrivanje jedne greške**

Neka je za $n \in \mathbb{N}$:

$$V_H(n) = \{ x \in \{0,1\}^n \mid \|x\| \equiv 0 \ (mod\ 2)\}$$

Odnosno izdvojeni su vektori dužine n sa parnom normom.

TVRĐENJE 3.3.2 *$V_H(n)$ je linearan kod*.

Dokaz. Zaista, ako su x i y iz $V_H(n)$, onda je $\|x\| \equiv 0 \ (mod\ 2)$, $\|y\| \equiv 0 \ (mod\ 2)$, pa je $\|x \oplus y\| \equiv 0 \ (mod\ 2)$, tj. $x \oplus y \in V_H(n)$. Dalje,

[1] Richard Wesley Hamming (1915-1998) američki matematičar i inženjer

$d(V_H(n)) = 2$, što je očigledno. Ovaj kod omogućuje otkrivanje jedne greške (neposredno proverom parnosti norme), a broj njegovih kodnih reči je 2^{n-1} (polovina ukupnog broja reči 2^n). Odgovarajuća generišuća matrica je npr.:

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

formata $(n - 1) \times n$, a kontrolna:

$$F = [1 \quad 1 \quad \dots \quad 1]$$

formata $1 \times n$.

■

PRIMER 3.3.3 $V_H(4) = \{0000,0011,0101,1001,0110,1010,1100,1111\}$.

□

DEFINICIJA 3.3.4 **Kodovi koji omogućuju ispravljanje jedne greške**. Neka je $n = 2^s - 1$, $s = 2,3,\dots$ i neka je data kontrolna matrica F formata $s \times (2^s - 1)$, čije su kolone redom binarni zapisi brojeva $1,2,\dots,2^s - 1$, sa s cifiara.

$$F = \begin{bmatrix} 0 & 0 & 0 & \dots & 1 & 1 \\ 0 & 0 & 0 & \dots & 1 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & 1 & \dots & 0 & 1 \end{bmatrix}$$

TVRĐENJE 3.3.5 *Kod $W_H(n)$, čija je F kontrolna matrica, ima dimenziju $n - s = 2^s - 1 - s$, i ispravlja jednu grešku.*

Dokaz. Iz formata matrice imamo da je $dim(W_H(n)) = n - s$. Pokažimo da je $d(W_H(n)) \geq 3$. Neka je $x \in W_H(n)$, $x = (x_1, \dots, x_n)$ i neka je $x \neq 0$. Jasno, $F \cdot x = 0$, a to je, ako sa $F_1, \dots, F_n$ označimo kolone u F, ekvivalentno sa:

$$x_1F_1 \oplus \dots \oplus x_nF_n = 0 \ (= nula - vektor)$$

Kako je $F_i \neq 0$, $i = 1, \dots, n$ sledi da je $\|x\| \neq 1$. Pored toga, $\|x\| \neq 2$, jer u slučaju da je $x_i = x_j = 1$ (za $i \neq j$), a da su sve ostale koordinate nule, dobijamo $F_i \oplus F_j = 0$, tj. $F_i = F_j$, što opet nije tačno. Zato je najmanja norma ne-nula vektora u $W_H(n)$ veća od 2, pa taj kod zaista ispravlja jednu grešku.

■

Postupak za otkrivanje greške kod ovog koda proizilazi iz konstrukcije matrice F. Neka je na vektoru x iz $W_H(n)$ došlo do greške na i-toj koordinati,

pa se na izlazu iz kanala pojavio vektor y:

$$y = x \oplus e = (x_1, \dots, x_n) \oplus (0, \dots, 1, \dots 0) = (x_1, \dots, x_i \oplus 1, \dots, x_n).$$

Tada je

$$F \cdot y = F(x \oplus e) = F \cdot x \oplus F \cdot e = 0 \oplus F_i = F_i.$$

($F \cdot y$ jeste vektor binarnog zapisa koordinate na kojoj je došlo do greške, a u slučaju da je to nula-vektor, greška se nije desila).

PRIMER 3.3.6 Kod $W_H(7)$ dat je tablicom:

0000000	1110000
1101001	0011001
0101010	**1011010**
1000011	0110011
1001100	0111100
0100101	1010101
1100110	0010110
0001111	1111111

do ovog koda se dolazi rešavanjem jednačine $F \cdot x = 0$, gde je:

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

Ako se, npr. na izlazu iz kanala pojavio vektor $y = 1010010$, onda je

$$F \cdot y = 1 \cdot \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} \oplus 0 \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \oplus 1 \cdot \begin{bmatrix} 0 \\ 1 \\ 1 \end{bmatrix} \oplus 0 \cdot \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \oplus 0 \cdot \begin{bmatrix} 1 \\ 0 \\ 1 \end{bmatrix} \oplus 1 \cdot \begin{bmatrix} 1 \\ 1 \\ 0 \end{bmatrix} \oplus 0 \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix}$$

100 je binarni zapis broja 4 tako da je y nastao od kodne reči 1011010 prelaskom 1 u 0 na četvrtom mestu.

□

DEFINICIJA 3.3.7 Kodovi Heminga poseduju još neke značajne osobine. Za kod $V \subseteq \{0,1\}^n$, $n \in \mathbb{N}$, koji omogućuje ispravljanje s grešaka kažemo da je **maksimalan**, ako za svaki kod $W \subseteq \{0,1\}^n$, koji takođe omogućuje ispravljanje s grešaka važi: $card\ W \leq card\ V$.

TVRĐENJE 3.3.8 *Ako je* $n = 2^s - 1$, $s = 2,3, \dots$ *onda n-dimenzionalna jedinična kocka* $\{0,1\}^n$ *može biti razbijena na familiju disjunktnih lopti poluprečnika* 1.

Dokaz. U n-dimenzionalnoj jediničnoj kocki (gde je $n = 2^s - 1$) izdvojimo tačke koje obrazuju kod Heminga $W_H(n)$. Taj skup sadrži 2^{2^s-s-1} kodnih reči, jer mu je dimenzija $2^s - s - 1$. Oko svake tačke (kodne reči) opišimo sferu poluprečnika 1. Te sfere u parovima su disjunktne (jer ovaj kod omogućava ispravljanje 1 greške), pa je ukupan broj tačaka koje sadrži familija sfera:

$$(1+n)\cdot 2^{2^s-s-1} = 2^s \cdot 2^{2^s-s-1} = 2^{2^s-1} = 2^n$$

jer svaka okolina (sfera) sadrži tačno $n + 1$ tačku (centar tj. kodnu reč i reči koje se od kodne razlikuju na jednom mestu, a njih ima n, jer je dužina reči n). Tako su sve tačke iz $\{0,1\}^n$ obuhvaćene sferama.

■

POSLEDICA 3.3.9 *Hemingov kod* $W_H(n)$ $(n = 2^s - 1)$ *je maksimalan.*

Dokaz. Ako bismo postupak iz tvrđenja 3.3.8 radili za kod veće kardinalnosti od Hemingovog vodeći se pretpostavkom da taj kod ispravlja takođe 1 grešku dobili bismo da nisu sve sfere disjunktne, jer bi se u njima nalazilo više (gledajući ukupan broj tačaka u svim sferama) od 2^n reči, tj. više sfera bi sadržalo istu reč.

■

PRIMER 3.3.10 Za $s = 2$ Hemingov kod $W_H(2^s - 1) = W_H(3)$ sadrži dve kodne reči 000 i 111, a na trodimenzionalnoj jediničnoj kocki možemo izdvojiti dve odgovarajuće disjunktne sfere:

$$Z_1(000) = \{000,001,010,100\} \text{ i } Z_1(111) = \{011,101,110,111\}$$

□

DEFINICIJA 3.3.11 Kada je $n \neq 2^s - 1$ govorimo o **skraćenim Hemingovim kodovima**, pri čemu se s određuje tako da $2^{s-1} \leq n < 2^s$ tj. $s = \lfloor log_2 n \rfloor + 1$, dok su kolone kontrolne matrice F binarni zapisi redom brojeva $1,2,\dots,n$.

PRIMER 3.3.12 Kontrolna matrica koda $W_H(5)$ je:

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

pa posle rešavanja odgovarajuće jednačine $F \cdot x = 0$ dobijamo da je $W_H(5) = \{00000,11100,10011,01111\}$.

□

3.4 Golejevi[2] kodovi

Treba primetiti da generišuća i kontrolna matrica igraju ključnu ulogu kada je reč o linearnim kodovima. Predstavićemo sada primer jedne klase kodova kod kojih se i njihove glavne osobine, npr. vezane za kodno rastojanje mogu izvesti analizom generišuće matrice. Doći ćemo i do vrlo interesantne i značajne osobine koje kod može imati, a to je savršenost.

DEFINICIJA 3.4.1 **Presek** dva vektora $x = x_1x_2 \dots x_n$ i $y = y_1y_2 \dots y_n$ iz $\{0,1\}^n$ je vektor $z = x \cap y = z_1z_2 \dots z_n$, gde je $z_i = \begin{cases} 1, & x_i = y_i = 1 \\ 0, & inače \end{cases}$.

NAPOMENA 3.4.2 Operacija preseka je asocijativna tj. $\forall x, y, z \in \{0,1\}^n (x \cap y) \cap z = x \cap (y \cap z)$.

PRIMER 3.4.3 Ako su $x = 11011$ i $y = 10110$ onda je $x \cap y = 10010$.

□

TVRĐENJE 3.4.4 *Neka su x i y iz $\{0,1\}^n$. Tada važi sledeća jednakost*:

$$\|x + y\| = \|x\| + \|y\| - 2\|x \cap y\|.$$

Dokaz. Vektor $x + y$ nema jedinice na koordinatama na kojima i x i y imaju jedinice tako da od $\|x\|$ i $\|y\|$ treba oduzeti svaku jedinicu iz preseka i za x i za y, pa dobijamo da je $\|x + y\| = \|x\| - \|x \cap y\| + \|y\| - \|x \cap y\|$

■

DEFINICIJA 3.4.5 Ortogonalnu dopunu $\bar{V}$ linearnog koda V nazivamo još i **dual** koda V. Kod V za koji važi $V = \bar{V}$ je **samodualan**.

TVRĐENJE 3.4.6 *Linearan kod V, za koji je G generišuća matrica formata $k \times 2k$ je samodualan ako i samo ako za svake dve vrste x i y iz G važi $x \circ y = 0$.*

Dokaz. Tvrđenje sledi direktno iz definicije.

■

PRIMER 3.4.7 Lako možemo konstatovati da je samodualan sledeći kod V, čija je generišuća matrica:

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

□

TVRĐENJE 3.4.8 *Ako za samodualan binaran linearan kod V važi da je $\|x\| \equiv 0 \ (mod\ 4)$ za svaku vrstu x generišuće matrice G, onda je $d(V) \equiv 0 \ (mod\ 4)$.*

[2] Marcel J. E. Golay (1902-1989) švajcarsko-američki matematičar i fizičar

Dokaz. Na osnovu tvrđenja 3.4.3 imamo da je za svake dve vrste x i y iz G $\|x+y\| = \|x\| + \|y\| - 2\|x \cap y\| \equiv 0 + 0 - 2\|x \cap y\| \equiv 2\|x \cap y\| \ (mod\ 4)$. Ako bi $\|x \cap y\|$ bilo neparno dobili bismo da je $x \circ y$ neparan broj, što je nemoguće, jer je kod samodualan. Tako da je $2\|x \cap y\| \equiv 0\ (mod\ 4)$. Kako se svaka kodna reč $v \in V$, može predstaviti kao suma nekih vrsta iz G, sledi da je $\forall v \in V, \|v\| \equiv 0\ (mod\ 4)$, pa je onda i $d(V) \equiv 0\ (mod\ 4)$.

■

DEFINICIJA 3.4.9 **Golejev kod** G_{24} je linearan kod za koji je generišuća matrica tog koda sledeća blok-matrica: $[I_{12} \quad A]$ gde je I_{12} jedinična matrica formata 12×12 (matrica koja ima jedinice na glavnoj dijagonali, dok su sve ostale pozicije popunjene nulama) i matrica A koju konstruišemo na sledeći način: Označimo vrste i kolone matrice redom sa $\infty, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10$. U vrsti i koloni ∞ na prvoj poziciji nalazi se 0, dok su sve ostale pozicije 1. U vrsti 0, postavimo 1 na pozicijama, koje predstavljaju ostatke pri deljenju kvadrata celog broja sa 11, to su $0^2 \equiv 0\ (mod\ 11)$, $1^2 \equiv 1\ (mod\ 11)$, $2^2 \equiv 4\ (mod\ 11)$, $3^2 \equiv 9\ (mod\ 11)$, $4^2 \equiv 5\ (mod\ 11)$, $5^2 \equiv 3\ (mod\ 11)$, posle toga imamo beskonačan ciklus ponavljanja ovih ostataka. Vrsta 1 je dobijena od prethodne tako što su vrsti 0 ciklično pomerene pozicije od 0 do 10 levo, pa je 1 na poziciji 0, sada na poziciji 10, 1 na poziciji 1 je sada na poziciji 0, 0 na poziciji 2 je pomerena na poziciju 1, itd. Analogno, vrstu 2 dobijamo od vrste 1, i tako redom svaku sledeću vrstu dobijamo cikličnim pomeranjem prethodne vrste za jednu poziciju levo, ostavljajući kolonu ∞ bez promene.

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

TVRĐENJE 3.4.10 *Golejev kod je samodualan*.

Dokaz. Prema tvrđenju 3.4.6 dovoljno je pokazati da je skalarni proizvod bilo koje dve vrste iz generišuće matrice Golejevog koda jednak nuli. Prvo, svaka vrsta x ima po paran broj jedinica 8 ili 12, pa važi $x \circ x = 0$, dok se direktnom proverom može ustanoviti da presek svake dve vrste ima paran broj jedinica,

pa je skalarni proizvod bilo koje dve vrste takođe 0.

■

TVRĐENJE 3.4.11 $d(G_{24}) = 8$.

Dokaz. Na osnovu tvrđenja 3.4.8 i 3.4.10 imamo da je $d(G_{24}) \equiv 0\ (mod\ 4)$, jer su sve vrste generišuće matrice deljive sa 4. Kako očigledno postoji vektor u ovom kodu koji je po normi 8 (npr. poslednja vrsta u gen. matrici) sledi da je $d(G_{24}) = 4$ ili $d(G_{24}) = 8$. Pretpostavimo da je $d(G_{24}) = 4$, tj. da postoji kodna reč c, koja ima normu 4, i neka je $c = (a|b)$, gde su $a, b \in \{0,1\}^{12}$. Bez umanjenja opštosti neka je $\|a\| \leq \|b\|$. Ako je $\|a\| = 0$, onda je c nula-vektor, što je kontradikcija. Ako je $\|a\| = 1$, onda c mora biti jedan od generišućih vektora, što je opet kontradikcija, jer $\|c\| = 4$. A ako je $\|a\| = 2$, onda je c zbir dva generišuća vektora i $\|b\| = 2$, i b mora biti zbir dve vrste matrice A. Direktnom proverom možemo ustanoviti da je zbir svake dve vrste iz A po normi 6, što je ponovo protivrečnost. Dakle, $d(G_{24}) = 8$.

■

DEFINICIJA 3.4.12 **Golejev kod** G_{23}, tačnije njegovu generišuću matricu, dobijamo tako što uklonimo bilo koju kolonu iz matrice $[I_{12} \quad A]$. Zbog jednostavnosti možemo ukloniti poslednju kolonu. Na taj način dobijamo jedan binaran linearni (23,12) kod. Takođe, od generišuće matrice za G_{23} možemo dobiti matricu za G_{24}, tako što svaku vrstu dopunimo sa 0 ili 1, da svaka vrsta ima paran broj jedinica.

TVRĐENJE 3.4.13 $d(G_{23}) = 7$.

Dokaz. Kako je ovaj kod dobijen od G_{24}, uklanjanjem jedne kolone, i $d(G_{24}) = 8$, sledi da minimalna norma vektora iz G_{23} može biti 7 ili 8. Pošto postoji kodna reč iz generišuće matrice (vektor u trećoj vrsti), čija je norma 8, 00100000110111000101, ako npr. uklonimo poslednju kolonu matrice, dobićemo reč 00100000110111000010 ∈ G_{23}, koja ima normu 7, pa sledi tvrđenje.

■

POSLEDICA 3.4.14 *Kodovi G_{23} i G_{24} omogućavaju ispravljanje* 3 *greške*.

Dokaz. Direktno iz tvrđenja 2.2.21, 3.4.11 i 3.4.13.

■

DEFINICIJA 3.4.15 Linearan (n, k) kod V je ***s*-savršen** kod ako se prostor B^n može razbiti na familiju disjunktnih lopti $Z_s(v)$, $v \in V$.

PRIMER 3.4.16 Zbog tvrđenja 3.3.8, Hemingovi kodovi su 1-savršeni.

□

TVRĐENJE 3.4.17 *Kod G_{23} je* 3*-savršen kod*.

Dokaz. Važi sledeći identitet, $|Z_3(v)| = \sum_{i=0}^{3}\binom{23}{i} = 2^{11}$, $v \in G_{23}$ (reči koje se od v razlikuju redom na 0, 1, 2, 3 mesta). Bazu koda G_{23} čini 12 vektora, pa je $|G_{23}| = 2^{12}$, odnosno toliko ima disjunktnih lopti, i imamo da je $2^{11} \cdot 2^{12} = 2^{23} = |\{0,1\}^{23}|$ (ove lopte poluprečnika 3 vrše razbijanje skupa $\{0,1\}^{23}$).

■

PRIMER 3.4.18 Generišuća matrica za **ternarni Golejev kod G_{12}** je:

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

Matricu za ternarni kod G_{11} dobili bismo postupkom analognim za dobijanje koda G_{23} od koda G_{24}.

□

3.5 Rid-Milerovi[3] kodovi

Kada se šestdesetih i sedamdesetih godina intenziviralo istraživanje kosmičkih prostranstava i udaljenih planeta i satelita, američka astronomska i astronautička organizacija NASA, je zbog što bržeg, ali i preciznijeg prenosa informacija, raznoraznih podataka i fotografija, na velike udaljenosti, želela što optimalnije kodove. Ova optimalnost se ogledala u tome da kod ima dužinu kodne reči što kraću, a da omogućava ispravljanje što je moguće više grešaka. Npr. Golejevi kodovi su bili među takvim kodovima, koji su se upotrebljavali. U nastavku navodimo specijalne kodove, kod kojih je konstrukcija generišuće matrice posebno interesantna i biće ujedno i primer konkatenacijskog proizvoda, a našli su primenu u praksi prenosa informacija.

DEFINICIJA 3.5.1 $H_i = \{y \in F_2^m | \, y_i = 0\}$ su **hiper-površi** u vektorskom prostoru F_2^m.

DEFINICIJA 3.5.2 Neka je dat skup $X = F_2^m = \{x_1, x_2, \dots, x_{2^m}\}$. **Rid-Milerov** $RM(r,m)$ kod je linearni $(2^m, k)$ kod, gde je $k = \sum_{i=0}^{r}\binom{m}{i}$, koji generišu vektori $v_0 = (1,1,\dots,1)$ (ima 2^m jedinica) i $v_i = \chi_{H_i}, i \in \{1,2,\dots,m\}$, gde je χ_{H_i} karakteristična funkcija podskupa H_i u skupu F_2^m, odnosno:

[3] Irving S. Reed (1923-2012), David E. Muller (1924-2008) američki matematičari i inženjeri

$$\chi_{H_i}(x_i) = \begin{cases} 1, x_i \in H_i \\ 0, x_i \notin H_i \end{cases},$$

$$v_i = \begin{pmatrix} x_1 & x_2 & \dots & x_{2^m} \\ \chi_{H_i}(x_1) & \chi_{H_i}(x_2) & \dots & \chi_{H_i}(x_{2^m}) \end{pmatrix},$$

kao i svi dvočlani, tročlani,… , r-točlani preseci prethodno navedenih vektora $(v_i \cap v_j, \dots, v_{i_1} \cap v_{i_2} \cap \dots \cap v_{i_r})$. Ubuduće, v_i poistovećujemo sa nizom slika.

PRIMER 3.5.3 Generišuća matrica za $RM(2,3)$, gde je $X = \{(0,0,0), (0,0,1), (0,1,0), (0,1,1), (1,0,0), (1,0,1), (1,1,0), (1,1,1)\}$. Vrste ove matrice su redom vektori $v_0, v_1, v_2, v_3, v_1 \cap v_2, v_1 \cap v_3, v_2 \cap v_3$:

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

□

TVRĐENJE 3.5.4 *Skup svih r-točlanih preseka vektora v_i, gde $i, r \in \{0,1,2, \dots, m\}$ čini bazu vektorskog prostora F_2^n, $n = 2^m$.*

Dokaz. Prvo primetimo da takvih preseka ima $\sum_{r=0}^{m} \binom{m}{r} = 2^m$, jer za $r = 0$, uzimamo da je presek v_0, a od preostalih v_i, $i \in \{1,2, \dots, m\}$, pravimo sve moguće kombinacije preseka, od jednočlanih do m-točlanih. Preostaje da se pokaže da je formirani skup vektora generatorni. Tvrdimo da vektore standardne baze prostora F_2^n, $e_1, e_2, \dots, e_n$, gde je e_j vektor dužine n koji ima jedinicu na j-tom mestu, a na ostalim mestima nule, možemo predstaviti na sledeći način:

$$e_j = (v_1 \oplus z_1) \cap (v_2 \oplus z_2) \cap \dots \cap (v_m \oplus z_m), (*)$$

gde je $z_i = v_0$, ako vektor v_i ima 0 na j-tom mestu, a $z_i = 0 - vektor$, inače. Na ovaj način postižemo da svi vektori u zagradama u izrazu (*), a to su vektori $v_i \oplus z_i$ imaju 1 na j-tom mestu, pa i njihov presek takođe ima tu osobinu. Na kraju uočimo da ovaj presek na ostalim mestima ima 0. Treba zapaziti da su sve kolone u matrici, čiji su redovi vektori $v_0, v_1, v_2, \dots, v_m$ različite (u protivnom bismo imali da postoje bar dve različite reči iz skupa X koje imaju isti raspored 0 i 1, što je nemoguće), pa dodajući v_0 proizvoljnoj vrsti i dalje sve kolone ostaju različite. Uz prethodne zaključke dobijamo da samo jedna kolona može imati sve jedinice, tako da je presek u (*) vektor koji ima jedinicu samo na j-tom mestu, odnosno da je zaista jednak sa e_j. Kako je operacija ∩ distributivna prema operaciji ⊕ zbog distributivnosti u polju F_2,

e_j možemo predstaviti kao linearnu kombinaciju vektora $v_0, v_1, v_2, \dots, v_m$ i njihovih preseka. Iz pokazanog sledi tvrđenje.

■

PRIMER 3.5.5 Neka je $n = 2^3$ i dat prostor F_2^8, tada važi:

$$e_2 = (v_1 \oplus 0) \cap (v_2 \oplus 0) \cap (v_3 \oplus v_0) = v_1 \cap v_2 \cap (v_3 \oplus v_0) =$$
$$= (v_1 \cap v_2 \cap v_3) \oplus (v_1 \cap v_2 \cap v_0) = (v_1 \cap v_2 \cap v_3) \oplus (v_1 \cap v_2)$$

□

POSLEDICA 3.5.6 *Dimenzija koda* $RM(r,m)$ *je* $\sum_{i=0}^{r}\binom{m}{i}$.

Dokaz. Na osnovu tvrđenja 3.5.4 sve vrste generišuće matrice G su linearno nezavisne, a njih ima $\sum_{i=0}^{r}\binom{m}{i}$.

■

TVRĐENJE 3.5.7 $RM(r,m) = RM(r,m-1)|RM(r-1,m-1)$.

Dokaz. Neka su kodovi $RM(r,m-1)$ i $RM(r-1,m-1)$ redom generisani vektorima $u_0, u_1, \dots, u_{m-1}$ i r-točlanim presecima istih, i $v_0, v_1, v_2, \dots, v_{m-1}$ i njihovim $(r-1)$-točlanim presecima. Tada je $RM(r,m)$ generisan sledećim nizom vektora $w_0, w_1, w_2, \dots, w_m$ i njihovim r-točlanim presecima. Pritom, su $w_0 = (u_0|v_0), w_1 = (u_0|0), w_2 = (u_1|v_1), \dots, w_m = (u_{m-1}|v_{m-1})$, a preseci su (bez w_0) $\bigcap_{j=1}^{k} w_{i_j} = \left(\bigcap_{j=1}^{k} u_{i_j-1} \middle| \bigcap_{j=1}^{k} v_{i_j-1}\right)$, $k \le r-1$ ako među $w_{i_1}, w_{i_2}, \dots, w_{i_k}$ nije w_1, a ako jeste onda su oblika $\bigcap_{j=1}^{k} w_{i_j} = \left(\bigcap_{j=1}^{k} u_{i_j-1} \middle| 0\right)$, $k \le r-1$. Za $k = r$, $\bigcap_{j=1}^{r} w_{i_j} = \left(\bigcap_{j=1}^{r} u_{i_j-1} \middle| \bigcap_{j=1}^{r} u_{i_j-1}\right)$ ili $\bigcap_{j=1}^{r} w_{i_j} = \left(\bigcap_{j=1}^{r} u_{i_j-1} \middle| 0\right)$. Vektor w_0 je neutralni element za operaciju preseka.

■

PRIMER 3.5.8 $RM(2,3) = RM(2,2)|RM(1,2)$, i generišuća matrica za kod $RM(2,3)$ je data u primeru 3.5.3, a za kodove $RM(2,2)$ i $RM(1,2)$ su redom generišuće matrice sledeće:

$$G_1 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix} \quad \text{i} \quad G_2 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

□

POSLEDICA 3.5.9 $d\big(RM(r,m)\big) = 2^{m-r}$, *tj. kod* $RM(r,m)$ *omogućava otkrivanje najviše* $2^{m-r}-1$ *i ispravljanje najviše* $2^{m-r-1}-1$ *grešaka.*

Dokaz. Indukcijom po r. Za $r = 0$ kod $RM(0, m)$ je generisan samo sa vektorom v_0 koji ima 2^m jedinica, pa je očigledno $d\big(RM(0, m)\big) = 2^{m-0} = 2^m$. Za $r = m$, na osnovu tvrđenja 3.5.4 je $RM(m, m) = F_2^n, n = 2^m$, a važi $d(F_2^n) = 2^{m-m} = 2^0 = 1$. Neka je sada $0 < r < m$, i neka važi $d\big(RM(r, m-1)\big) = 2^{(m-1)-r} = 2^{m-r-1}$ i $d\big(RM(r-1, m-1)\big) = 2^{(m-1)-(r-1)} = 2^{m-r}$. Na osnovu tvrđenja 3.1.20 i 3.5.7 dobijamo da je $d\big(RM(r, m)\big) = min\{2d\big(RM(r, m-1)\big), d\big(RM(r-1, m-1)\big)\} = min\{2 \cdot 2^{m-r-1}, 2^{m-r}\} = min\{2^{m-r}\} = 2^{m-r}$. Drugi deo posledice sledi iz tvrđenja 2.2.21.

■

Na osnovu prethodne posledice uviđamo značaj Rid-Milerovih kodova, jer za povoljno izabrane parametre r i m možemo postizati sve veće kodno rastojanje, što se direktno odražava i na veće mogućnosti otkrivanja i ispravljanja grešaka. Ipak, treba imati u vidu da se povećanjem parametra m dužina kodne reči eksponencijalno povećava, jer je $n = 2^m$.

PRIMER 3.5.10 Kod $RM(1,5)$ ima kodno rastojanje $2^4 = 16$, pa omogućava otkrivanje i do 15 grešaka, a ispravljanje 7. Dok npr. za $RM(0,5)$, imamo da su nabrojane vrednosti čak 32, 31, 15, što smo postigli smanjenjem parametra r za samo 1.

□

U narednom poglavlju pažnju ćemo posvetiti specijalnim linearnim kodovima, koji se mogu posmatrati i sa nešto drugačijeg aspekta, osim kao potprostori vektorskih prostora nad konačnim poljima. Teorija o polinomima izneta u uvodnom delu rada dobiće u nastavku pun smisao. Ciklični kodovi su zato i izdvojeni kao posebno poglavlje, jer su zaista značajna potklasa linearnih kodova, i zavređuju posebnu pažnju.

4 Ciklični kodovi

4.1 Definicija i osnovne osobine cikličnog koda

DEFINICIJA 4.1.1 Linearan (n, k) kod C je **cikličan** ako ispunjava uslov:

$$(\forall c = (c_0, c_1, \dots, c_{n-1}) \in C)((c_{n-1}, c_0, \dots, c_{n-2}) \in C).$$

Ovaj uslov može da se opiše rečima kao zatvorenost operacije **cikličnog pomeranja desno** kodnih reči iz koda C. Trivijalni primer za ovakav tip kodova su nula-prostor $\{00 \dots 00\}$ (reč sa n nula) ili ceo prostor F_q^n.

PRIMER 4.1.2 Hemingov kod $V_H(n) = \{ x \in \{0,1\}^n \mid \|x\| \equiv 0 \ (mod\ 2)\}$ je cikličan, što se može zaključiti upravo iz osobine da sve reči iz datog koda imaju paran broj jedinica i da je taj broj invarijantan na ciklično pomeranje. □

Postoje i primeri kodova koji ispunjavaju dodatni uslov „cikličnosti“, ali nisu ciklični, jer nisu uopšte linearni.

PRIMER 4.1.3 Kod $V = \{0000,1000,0100,0010,0001\}$ nije cikličan, jer npr. $1000 \oplus 0100 = 1100 \notin V$, pa nije linearan. □

Ciklični kodovi kao izdvojena potklasa linearnih kodova se ističe zbog svojevrsnog izomorfizma cikličnog koda C posmatranog kao vektorski prostor i potprostora $C[x]$ od $\left(F_q[x]/_{x^n - 1}, +, \cdot, F_q\right)$, gde je polje F_q azbuka koda C, a druga operacija " $\cdot$ " se odnosi na množenje vektora skalarom. Izomorfizam, koji se najprirodnije uspostavlja u ovom slučaju je sledeća funkcija:

$$(\forall c = (c_0, c_1, \dots, c_{n-1}) \in C)\ \varphi(c_0, c_1, \dots, c_{n-1}) = c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}$$

Ciklično pomeranje desno sada ostvarujemo množeći odgovarajući polinom kodne reči, u oznaci $c(x)$ sa x. Zaista kako je $x^n \equiv 1 \ (mod\ x^n - 1)$ imamo da je:

$$xc(x) = c_0 x + c_1 x^2 + \cdots + c_{n-1} x^n = c_{n-1} + c_0 x + \cdots + c_{n-2} x^{n-1}$$

NAPOMENA 4.1.4 Sa $C[x]$ označavamo skup svih polinoma pridruženih kodnim rečima iz C.

TVRĐENJE 4.1.5 *Ortogonalna dopuna $\bar{C}$ cikličnog koda C je cikličan kod*.

Dokaz. Pošto je C linearan sledi da je i $\bar{C}$ linearan kod (tvrđenje 3.1.11).

Pretpostavimo sada da je data proizvoljna reč $c = (c_0, c_1, \dots, c_{n-1}) \in C$ i neka je $d = (d_0, d_1, \dots, d_{n-1}) \in \bar{C}$, tada važi $c \circ d = c_0 d_0 \oplus \dots \oplus c_{n-1} d_{n-1} = 0$. Dalje imamo da je $(c_{n-1}, c_0, \dots, c_{n-2}) \in C$, zbog cikličnosti, pa iz prethodno pokazane jednakosti dobijamo da $(d_{n-1}, d_0, \dots, d_{n-2}) \in \bar{C}$. Dakle, $\bar{C}$ je cikličan.

■

Pošto ćemo u nastavku ove lekcije kod C posmatrati kao potprostor $C[x]$ prstena ostataka polinoma pri deljenju sa $x^n - 1$, definisaćemo nove pojmove i navešćemo jednu korisnu lemu bez dokaza, vezanu za faktorizaciju minimalnih polinoma, kao i $x^n - 1$.

DEFINICIJA 4.1.6 Neka su prirodni brojevi q i n uzajamno prosti, odnosno nemaju zajedničkih delilaca osim jedinice, $s \in \{0,1,2, \dots, n-1\}$ i r najmanji prirodan broj takav da je $sq^r \equiv s \ (mod\ n)$. Tada skup $C_s = \{s, sq, \dots, sq^{r-1}\}$ $(mod\ n)$ nazivamo **q-ciklotomični koset** od s po modulu n. **Red elementa** q po modulu n u oznaci $t = ord_n(q)$ je najmanji prirodan broj t za koji je $q^t \equiv 1 \ (mod\ n)$.

PRIMER 4.1.7 Neka je $q = 3$, $s = 2$ i $n = 8$. Tada je $C_2 = \{2, 2 \cdot 3\} = \{2,6\}$ $(mod\ n)$, a $t = ord_8(3) = 2$.

□

LEMA 4.1.8 *Neka su dati uzajamno prosti brojevi q i n, i neka je* $t = ord_n(q)$. *Ako je α primitivni element polja* F_{q^t}, *tada za svaki broj* $s \in \{0,1,2, \dots, n-1\}$ *minimalni polinom za* α^s, $m_{\alpha^s}(x) = \prod_{i \in C_s}(x - \alpha^i)$. *Takođe važi i sledeća faktorizacija* $x^n - 1 = \prod_s m_{\alpha^s}(x)$, *gde s ide po predstavnicima q-ciklotomičnih koseta po modulu n.*

■

PRIMER 4.1.9 Neka je $q = 2$, $s = 1$ i $n = 7$, tada je $t = ord_7(2) = 3$, pa posmatramo polje $F_{2^3} = F_8$. U ovom polju, koje je izomorfno sa poljem $\left(\mathbb{Z}_2[x]/_{x^3 + x + 1}, +, \cdot\right)$ može da se pokaže da je primitivni element $\alpha = 1 + x$. On generiše sve nenula elemente ovog polja npr. $\alpha^2 = (1 + x)^2 = 1 + 2x + x^2 = 1 + x^2$, $\alpha^3 = (1 + x)^3 = (1 + x)^2(1 + x) = 1 + x + x^2 + x^3 = x^2$ itd. (koristili smo osobine ovog polja). Kako je $C_1 = \{1, 1 \cdot 2, 1 \cdot 2^2\} = \{1,2,4\}$ po lemi 4.1.8 dobijamo da je minimalni polinom za α^1 tj. za α, sledeći polinom $m_\alpha(x) = (x - \alpha)(x - \alpha^2)(x - \alpha^4) = 1 \ + \ (\alpha^6 + \alpha^5 + \alpha^3)x \ + \ (\alpha^4 + \alpha^2 + \alpha)x^2 + x^3 = 1 + x^2 + x^3$.

□

TVRĐENJE 4.1.10 *Neka je dat ciklični nenula kod (u polinomnom obliku)* $C[x]$ *kao potprostor od* $\left(F_q[x]/_{x^n - 1}, +, \cdot, F_q\right)$ *tada je* $C[x]$ *glavni ideal u datoj strukturi posmatranoj kao prsten, tj. postoji polinom* $g(x)$ *koji generiše ceo* $C[x]$ *i polinom* $x^n - 1$ *je deljiv polinomom* $g(x)$.

Dokaz. Zbog tvrđenja 1.2.5 dovoljno je pokazati da je $C[x]$ ideal. Kako je $C[x]$ zapis cikličnog koda C, koji je linearan, dobijamo da zbir dva polinoma iz $C[x]$ pripada $C[x]$, jer je zbir odgovarajućih kodnih reči iz C ponovo u C. Dalje imamo da zbog osobine cikličnosti, ako polinom $c(x) \in C[x]$, onda i $xc(x) \in C[x]$. Iz toga sledi da za svaki $f(x) \in {F_q[x]}/{x^n - 1}$ važi $f(x)c(x) \in C[x]$, jer je svaki polinom zapravo linearna kombinacija stepena od x. Dakle postoji $g(x)$ takav da je $C[x] = \langle g(x) \rangle$, pokažimo da $g(x) | x^n - 1$. Polinom $x^n - 1$ je nula u ovom prstenu, pa pripada i idealu $C[x]$. Na osnovu tvrđenja 1.1.17 imamo da postoje polinomi $p(x)$ i $r(x)$ tako da je $x^n - 1 = p(x)g(x) + r(x)$, gde je $r(x)=0$ ili stepena manjeg od stepena $g(x)$. Druga opcija vodi u kontradikciju, jer bi ispalo da je $r(x) = (x^n - 1) - p(x)g(x)$ u idealu, a manjeg je stepena od polinoma $g(x)$, pa je $g(x) | x^n - 1$.

■

Takođe se može pokazati da je $g(x)$ jedinstveno određen i da svakom idealu ovog prstena odgovara jedan ciklični kod. Dokaz se izvodi po definiciji.

POSLEDICA 4.1.11 *Neka su data dva ciklična koda* $C_1[x] = \langle g_1(x) \rangle$ i $C_2[x] = \langle g_2(x) \rangle$ *tada je* $C_1[x] \subseteq C_2[x]$ *ako i samo ako* $g_2(x) | g_1(x)$.

Dokaz. ($\Longrightarrow$) Neka je $C_1[x] \subseteq C_2[x]$ tada za svaki polinom $c(x) \in C_1[x]$ postoji polinom $f(x)$ tako da je $c(x) = f(x)g_2(x)$, pa i za $c(x) = g_1(x)$.
($\Longleftarrow$) Ako $g_2(x) | g_1(x)$ onda za svaki $c(x) \in C_1[x]$, važi $c(x) = f(x)g_1(x) = h(x)g_2(x)$, pa je $c(x) \in C_2[x]$.

■

PRIMER 4.1.12 Hemingov kod $V_H(4)$ može da se posmatra kao ideal u prstenu $\left({\mathbb{Z}_2[x]}/{x^4 - 1}, +, \cdot\right)$ generisan polinomom $1 + x$. Golejev G_{24} kod je cikličan kod i ideal u prstenu $\left({\mathbb{Z}_2[x]}/{x^{24} - 1}, +, \cdot\right)$ generisan polinomom $1 + x^2 + x^4 + x^5 + x^6 + x^{10} + x^{11}$.

□

TVRĐENJE 4.1.13 *Ako je* $C[x] = \langle g(x) \rangle$, *a* n *dužina kodne reči i* $n = deg\big(g(x)\big) + k$, *gde je* $deg(g(x))$ *stepen normiranog polinoma* $g(x) = g_0 + g_1 x + \cdots + x^{n-k}$ *tada je dimenzija koda* k *i generiše ga skup* $\{g(x), xg(x), \dots, x^{k-1}g(x)\}$.

Dokaz. Neka je $c(x) \in C[x]$ proizvoljno dato. Tada je $c(x) = f(x)g(x)$ za neki polinom $f(x)$, takav da je $deg(f(x))$ najviše $k - 1$ stepena, jer je $deg\big(c(x)\big) < n$. Ako je $f(x) = f_0 + f_1 x + \cdots + f_{k-1}x^{k-1}$ vidimo da pošto su elementi $f_0, f_1, \dots, f_{k-1} \in F_q$, ovakvih polinoma ima q^k, pa je zato dimenzija ovog koda upravo k. Posmatrajmo sledeću matricu koju čine polinomi iz $\{g(x), xg(x), \dots, x^{k-1}g(x)\}$ zapisani kao reči koda C:

$$G = \begin{bmatrix} g_0 & g_1 & \dots & g_{n-k} & 0 & 0 & \dots & 0 \\ 0 & g_0 & g_1 & \dots & g_{n-k} & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & g_0 & g_1 & \dots & g_{n-k} \end{bmatrix} = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix}$$

U navedenoj matrici možemo primetiti da su redovi linearno nezavisni vektori, ima ih k, tako da oni čine bazu ovog koda i matrica G je generišuća matrica koda.

■

DEFINICIJA 4.1.14 Neka je dat ciklični (n, k) kod $C[x] = \langle g(x) \rangle$. Polinom $h(x)$ za koji važi $h(x)g(x) = x^n - 1$ naziva se **kontrolni polinom** koda $C[x]$. Sada ćemo dokazati tvđenje koje povezuje kontrolni polinom i kontrolnu matricu datog koda.

TVRĐENJE 4.1.15 *Ako je* $h(x) = h_0 + h_1x + \cdots + h_kx^k$ *kontrolni polinom koda* $C[x]$ *generisanog sa* $g(x) = g_0 + g_1x + \cdots + x^{n-k}$ *tada je kontrolna matrica datog koda*:

$$H = \begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & h_k & h_{k-1} & \dots & h_0 \end{bmatrix}$$

Dokaz. Uzmimo proizvoljan polinom $c(x) \in C[x]$ i posmatrajmo ga kao kodnu reč $c = (c_0, c_1, \dots, c_{n-1})$, treba pokazati da je $Hc^T = 0$ vektor. Ali kako je $c(x)h(x) = f(x)g(x)h(x) = f(x)(x^n - 1) = f(x)x^n - f(x)$ (računajući po modulu $x^n - 1$ i $c(x) = f(x)g(x)$) i $f(x)$ je polinom najviše $k - 1$ stepena dobijamo da su u izrazu $f(x)x^n - f(x)$ koeficijenti uz $x^k, x^{k+1}, \dots, x^{n-1}$ nule. Kako je taj izraz zapravo $c(x)h(x)$ imamo da važe sledeće jednakosti:

$$\sum_{i=0}^{l} c_i h_{l-i} = 0, \forall l \in \{k, k+1, \dots, n-1\}, h_{k+1} = h_{k+2} = \cdots = h_{n-1} = 0$$

Zato imamo da je:

$$Hc^T = \begin{bmatrix} h_k & h_{k-1} & \dots & h_0 & 0 & 0 & \dots & 0 \\ 0 & h_k & h_{k-1} & \dots & h_0 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & h_k & h_{k-1} & \dots & h_0 \end{bmatrix} \cdot \begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

pa dobijamo da je H zaista kontrolna matrica koda $C[x]$.

■

PRIMER 4.1.16 Neka je dat binarni ciklični (7,3) kod generisan sa polinomom $g(x) = 1 + x^2 + x^3 + x^4$, tada je $h(x) = \frac{x^7-1}{g(x)} = 1 + x^2 + x^3$ i generišuća i kontrolna matrica ovog koda su:

$$G = \begin{bmatrix} 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \quad \text{i} \quad H = \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

□

Navešćemo jednu lemu koja pokazuje faktorizaciju generišućeg polinoma $g(x)$, a posledica je leme 4.1.10 i činjenice da je $g(x)|x^n - 1$ i biće značajna u lekciji o dekodiranju koja sledi.

LEMA 4.1.17 $g(x) = \prod_s m_{\alpha^s}(x)$ *gde se* s *kreće po nekom podskupu skupa svih predstavnika* q*-ciklotomičnih koseta po modulu* n.

■

4.2 Dekodiranje cikličnih kodova

Videli smo kako mogu da se dobiju generišuća i kontrolna matrica cikličnog koda i u tom slučaju ciklični kod zapravo posmatramo kao klasičan linearan kod za koji smo ranije u poglavlju 3 opisali postupak dekodiranja. Sada ćemo prikazati kako možemo ciklične kodove dekodirati algoritmom, koji pre svega koristi polinomne i ciklične osobine cikličnog koda. Zato ćemo u nastavku ponovo posmatrati kod više kao $C[x]$ nego C. Prvo pokažimo tvrđenje, koja daje donju granicu za kodno rastojanje datog koda C, jer ćemo na osnovu nje imati predstavu o tome koliko grešaka neki cikličan kod može otkriti i ispraviti.

TVRĐENJE 4.2.1 (**BCH[4] granica**) *Neka je* $C[x] = \langle g(x) \rangle$ *cikličan kod nad poljem* F_q, *a dužina kodne reči* n *uzajamno prosta sa* q. *Neka je* T *unija* q*-ciklotomičnih koseta, čiji predstavnici učestvuju u faktorizaciji polinoma* $g(x)$ *i neka sadrži podskup od* $\delta - 1$ *uzastopnih elemenata odnosno za neko* $b \in \mathbb{N}, \{b, b+1, \dots, b+\delta-2\} \ (mod\ n) \subseteq T$. *Tada* $d(C[x]) \geq \delta$.

Dokaz. Na osnovu definicije skupa T i leme 4.1.17 možemo zaključiti da za sve $i \in T$, pa tako i za sve $i \in \{b, b+1, \dots, b+\delta-2\}\ (mod\ n)$ važi $g(\alpha^i) = 0$, gde je α primitivni element polja F_{q^t} i $t = ord_n(q)$. Pretpostavimo suprotno,

[4] Alexis Hocquenghem (1908 – 1990) francuski matematičar, R. C. Bose (1901-1987) i D. K. Ray-Chaudhuri (1933-) američko-indijski matematičari

da postoji $c(x) \in C[x]\backslash\{0\}$ takvo da je $\|c(x)\| = k < \delta$. Tada je $c(x) = \sum_{i=1}^{k} c_{j_i} x^{j_i}$ i pošto je $C[x] = \langle g(x) \rangle$, imamo da važi $c(\alpha^i) = 0$ za sve $i \in \{b, b+1, \dots, b+k-1\}$, jer je $k < \delta$. Matrično to možemo prikazati na sledeći način:

$$\begin{bmatrix} \alpha^{bj_1} & \alpha^{bj_2} & \dots & \alpha^{bj_k} \\ \alpha^{(b+1)j_1} & \alpha^{(b+1)j_2} & \dots & \alpha^{(b+1)j_k} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(b+k-1)j_1} & \alpha^{(b+k-1)j_2} & \dots & \alpha^{(b+k-1)j_k} \end{bmatrix} \cdot \begin{bmatrix} c_{j_1} \\ c_{j_2} \\ \vdots \\ c_{j_k} \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

Matrica sa leve strane, označimo je sa M, množi nenula vektor c i dobija se nula vektor. Dakle, ovaj kvadratni homogeni sistem jednačina sa koeficijentima iz matrice M ima i netrivijalno rešenje, pa je $detM = 0$. Sa druge strane $detM = \alpha^{(j_1+j_2+\dots+j_k)b} detV$, gde je $detV$ poznata **determinanta Vandermonda**:

$$detV = \begin{vmatrix} 1 & 1 & \dots & 1 \\ \alpha^{j_1} & \alpha^{j_2} & \dots & \alpha^{j_k} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha^{(k-1)j_1} & \alpha^{(k-1)j_2} & \dots & \alpha^{(k-1)j_k} \end{vmatrix} = \prod_{1 \le p < q \le k} (\alpha^{j_q} - \alpha^{j_p})$$

a kako su svi stepeni primitivnog elementa u drugoj vrsti različiti, dobijamo da je i $detV \neq 0$, pa samim tim i $detM$, što je kontradikcija. Sledi $d(C[x]) \geq \delta$. ■

Videli smo u tvrđenju 4.2.1 kako na osnovu faktorizacije generišućeg polinoma $g(x)$ zaključujemo nešto i o kodnom rastojanju datog koda. U nastavku ćemo definisati pojmove koji će se koristiti prilikom postupka dekodiranja cikličnog koda, kao i sam algoritam dekodiranja.

DEFINICIJA 4.2.2 Neka je $C[x] = \langle g(x) \rangle$ i vektor $v(x) \in F_q[x]$ i neka je $v(x) = g(x)f(x) + r(x)$, gde je naravno $r(x) = 0$ ili je $deg\, r(x) < deg(g(x))$. Uvedimo **funkciju ostatka** na sledeći način $R_{g(x)}(v(x)) = r(x)$. Sa $e(x) = e_0 + e_1 x + \dots + e_{n-1} x^{n-1}$ označićemo **polinom greške**.

TVRĐENJE 4.2.3 *Funkcija ostatka zadovoljava sledeće osobine*:

a) $R_{g(x)}(av(x) + bw(x)) = aR_{g(x)}(v(x)) + bR_{g(x)}(v(x))$ *za svako* $a, b \in F_q$ i $v(x), w(x) \in F_q[x]$;
b) $R_{g(x)}(v(x) + a(x)(x^n - 1)) = R_{g(x)}(v(x))$;
c) $R_{g(x)}(v(x)) = 0$ *ako i samo ako* $v(x)\ mod(x^n - 1) \in C[x]$;
d) *Ako je* $c(x) \in C[x]$ *onda je* $R_{g(x)}(c(x) + e(x)) = R_{g(x)}(e(x))$;

e) *Ako* $R_{g(x)}(e(x)) = R_{g(x)}(e'(x))$ *gde* $e(x)$ *i* $e'(x)$ *imaju težinu najviše* t, *gde je* $t = \left\lfloor \frac{d-1}{2} \right\rfloor$, $d = d(C)$ (*kodno rastojanje*) *onda je* $e(x) = e'(x)$;

f) $R_{g(x)}\big(v(x)\big) = v(x)$ *ako je* $deg\ v(x) < n - k$.

Dokaz:

a) Sledi iz $\big(av(x) + bw(x)\big) : g(x) = av(x) : g(x) + bw(x) : g(x)$;

b) Kako je $g(x) | x^n - 1$ i na osnovu a) dobijamo tvrđenje;

c) Ako je $R_{g(x)}\big(v(x)\big) = 0$ onda $g(x) | v(x)$ i $v(x)\ mod(x^n - 1)$ mora biti deljivo sa $g(x)$, pa pripada $C[x]$. Ako $v(x)\ mod(x^n - 1) \in C[x]$ onda je $v(x)\ mod(x^n - 1)$ deljivo sa $g(x)$, pa opet kako je i $g(x) | x^n - 1$, sledi $R_{g(x)}\big(v(x)\big) = 0$;

d) Slično kao pod b);

e) Neka je $R_{g(x)}(e(x)) = R_{g(x)}(e'(x))$ sledi zbog a) i c) da je $R_{g(x)}(e(x) - e'(x)) = 0$ i $e(x) - e'(x) \in C[x]$. Ali $\|e(x) - e'(x)\| \leq 2t < d(C)$, pa $e(x) - e'(x)$ mora biti 0 tj. $e(x) = e'(x)$;

f) Ako je $deg\ v(x) < n - k = deg\ g(x)$ onda je očigledno $R_{g(x)}\big(v(x)\big) = v(x)$, jer je količnik pri deljenju $v(x)$ sa $g(x)$ nula.

■

TVRĐENJE 4.2.4 *Neka je* $g(x)$ *normirani delitelj polinoma* $x^n - 1$ *stepena* $n - k$. *Ako je* $R_{g(x)}\big(v(x)\big) = s(x)$ *tada je* $R_{g(x)}\big(xv(x)\ mod(x^n - 1)\big) = R_{g(x)}\big(xs(x)\big) = xs(x) - g(x)s_{n-k-1}$, *gde je* s_{n-k-1} *koeficijent uz* x^{n-k-1} *u polinomu* $s(x)$.

Dokaz. Po definiciji je $v(x) = g(x)f(x) + s(x)$, gde je $s(x) = s_0 + s_1x + \cdots + s_{n-k-1}x^{n-k-1}$. Tada je $xv(x) = xg(x)f(x) + xs(x) = xg(x)f(x) + g(x)f_1(x) + s'(x)$, gde je $s'(x) = R_{g(x)}\big(xs(x)\big)$. Takođe je $xv(x)\ mod(x^n - 1) = xv(x) - (x^n - 1)v_{n-1}$, pa dobijamo da je

$$xv(x) mod(x^n - 1) = xg(x)f(x) + g(x)f_1(x) + s'(x) - (x^n - 1)v_{n-1}$$
$$= (xf(x) + f_1(x) - h(x)v_{n-1})g(x) + s'(x)$$

gde je $h(x)g(x) = x^n - 1$. Zato je $R_{g(x)}\big(xv(x)\ mod(x^n - 1)\big) = s'(x) = R_{g(x)}\big(xs(x)\big)$, jer je $deg\ s'(x) < n - k$. Kako je $g(x)$ normirani polinom stepena $n - k$, imamo da je $R_{g(x)}\big(xs(x)\big) = xs(x) - g(x)s_{n-k-1}$.

■

DEFINICIJA 4.2.5 **Sindrom polinom** je $S(v(x)) = R_{g(x)}\left(x^{n-k}v(x)\right)$. Zbog tvrđenja 4.2.3 c), imamo da $v(x) \in C[x]$ ako i samo ako je $S\big(v(x)\big) = 0$.

Sada ćemo opisati tzv. **Meggit-algoritam** za dekodiranje cikličnog koda $C[x] = \langle g(x) \rangle$. Algoritam ćemo ilustrovati kroz prateći primer:

1. FAZA Naći ćemo sindrom polinome $S(e(x))$ za sve polinome greške $e(x)$ kod kojih je $e_{n-1} \neq 0$ i $\|e(x)\| \leq t = \left\lfloor \frac{d-1}{2} \right\rfloor$, $d = d(C)$.
Neka je dat binaran cikličan kod, dužina kodne reči neka je 15. Može se pokazati da se u faktorizaciji polinoma $x^{15} - 1$ nalazi i polinom $g(x) = 1 + x^4 + x^6 + x^7 + x^8$, čiji je odgovarajući skup $T = \{1,2,3,4,6,8,9,12\}$ definisan u tvrđenju 4.2.1. Primetimo da u skupu T postoje četiri uzastopna elementa 1, 2, 3 i 4, pa ako je $\delta - 1 = 4$ onda je $\delta = 5$, pa je $d(C[x]) \geq 5$, tako da ovaj kod omogućava ispravljanje 2 greške (jer je $d(C[x]) = 5$, zbog $\|g(x)\| = 5$). Napravimo sada tabelu svih sindrom polinoma $S(e(x))$, gde je $e_{14} \neq 0$ i $\|e(x)\| \leq 2$, a računamo ih po formuli $S\big(e(x)\big) = R_{g(x)}\big(x^8 e(x)\big)$ (zbog tvrđenja 4.2.3 e) imamo da su svi sindromi različiti za različite $e(x)$):

$e(x)$	$S(e(x))$	$e(x)$	$S(e(x))$
x^{14}	x^7	$x^6 + x^{14}$	$x^3 + x^5 + x^6$
$x^{13} + x^{14}$	$x^6 + x^7$	$x^5 + x^{14}$	$x^2 + x^4 + x^5 + x^6 + x^7$
$x^{12} + x^{14}$	$x^5 + x^7$	$x^4 + x^{14}$	$x + x^3 + x^4 + x^5 + x^7$
$x^{11} + x^{14}$	$x^4 + x^7$	$x^3 + x^{14}$	$1 + x^2 + x^3 + x^4 + x^7$
$x^{10} + x^{14}$	$x^3 + x^7$	$x^2 + x^{14}$	$x + x^2 + x^5 + x^6$
$x^9 + x^{14}$	$x^2 + x^7$	$x + x^{14}$	$1 + x + x^4 + x^5 + x^6 + x^7$
$x^8 + x^{14}$	$x + x^7$	$1 + x^{14}$	$1 + x^4 + x^6$
$x^7 + x^{14}$	$1 + x^7$		

Tabela 7

Koristeći svojstva iz tvrđenja 4.2.3 dobili smo $S(x^{14}) = R_{g(x)}(x^8 x^{14}) = R_{g(x)}(x^7) = x^7$, jer radimo po modulu $x^{15} - 1$, dalje slično dobijamo drugu kolonu, npr. $S(x^{13} + x^{14}) = R_{g(x)}(x^8(x^{13} + x^{14})) = R_{g(x)}(x^6 + x^7) = x^6 + x^7$, ... , $S(x^7 + x^{14}) = R_{g(x)}(x^8(x^7 + x^{14})) = R_{g(x)}(1 + x^7) = 1 + x^7$. Dalje možemo da primetimo kako je $g(x) = 1 + x^4 + x^6 + x^7 + x^8$ da je npr. $R_{g(x)}(x^8) = 1 + x^4 + x^6 + x^7$, pa to iskoristi za dobijanje četvrte kolone:

$$S(1 + x^{14}) = R_{g(x)}(x^8(1 + x^{14})) = R_{g(x)}(x^8 + x^7) = 1 + x^4 + x^6,$$

a na osnovu tvrđenja 4.2.4 imamo:

$$\begin{aligned} S(x + x^{14}) &= R_{g(x)}(x^8(x + x^{14})) = R_{g(x)}(x^9 + x^7) = R_{g(x)}(x^9) + R_{g(x)}(x^7) \\ &= R_{g(x)}(xx^8) + x^7 = R_{g(x)}(x(1 + x^4 + x^6 + x^7)) + x^7 \\ &= x + x^5 + x^7 + R_{g(x)}(x^8) + x^7 = 1 + x + x^4 + x^5 + x^6 + x^7 \end{aligned}$$

Analgno dobijamo i ostale sindrom polinome.

2. FAZA Neka je primljena reč $y(x) = c(x) + e(x)$, tada računamo $S(y(x))$, i na osnovu tvrđenja 4.2.3 d) imamo da je $S\big(y(x)\big) = S(e(x))$.

Npr. $y(x) = 1 + x^4 + x^7 + x^9 + x^{10} + x^{12}$, tada je

$$S\big(y(x)\big) = R_{g(x)}\big(x^8(1 + x^4 + x^7 + x^9 + x^{10} + x^{12})\big) =$$

$$R_{g(x)}(x^8) + R_{g(x)}(x^{12}) + R_{g(x)}(x^{15}) + R_{g(x)}(x^{17}) + R_{g(x)}(x^{18}) + R_{g(x)}(x^{20})$$

$$= 1 + x^4 + x^6 + x^7 + R_{g(x)}(x^{12}) + 1 + x^2 + x^3 + x^5 =$$

$$= x + x^2 + x^6 + x^7$$

(Kako je $S(x^4 + x^{14}) = R_{g(x)}(x^{12}) + R_{g(x)}(x^7)$, iz tablice smo mogli izračunati da $R_{g(x)}(x^{12}) = x + x^3 + x^4 + x^5 + x^7 - x^7 = x + x^3 + x^4 + x^5$).

3. FAZA Ako je $S(y(x))$ jednak nekom $S(e(x))$ u tablici sindrom polinoma, $y(x)$ dekodiramo kao kodnu reč $c(x) = y(x) - e(x)$. Ako se ne nalazi u tablici prelazimo na fazu 4.

U našem primeru se ne nalazi, pa prelazimo dalje na sledeću fazu.

4. FAZA Računamo sindrom polinome $S\big(xy(x)\big), S\big(x^2y(x)\big)$, … sve dok se ne bude našao u tablici. Tada ako je $S\left(x^iy(x)\right)$ u tablici i jednak je nekom $S\big(e'(x)\big)$, reč $y(x)$ dekodiramo kao kodnu reč $c(x) = y(x) - x^{n-i}e'(x)$, jer je $x^iy(x) = c'(x) + e'(x)$, pa je odatle $y(x) = x^{n-i}c'(x) + x^{n-i}e'(x)$, ali kako je kod cikličan $x^{n-i}c'(x) = c(x) \in C[x]$.

$$S\big(xy(x)\big) = R_{g(x)}\left(x^{n-k}xy(x)\right) = R_{g(x)}(x(x^{n-k}y(x))) = R_{g(x)}(xS(y(x))) =$$

$= xS\big(y(x)\big) - g(x)s_{n-k-1}$ (koristili smo tvrđenje 4.2.4). Isto bismo radili i za sindrom polinome $S\big(x^2y(x)\big)$, … s_{n-k-1} je koeficijent koji stoji uz x^{n-k-1} u razvoju polinoma $S\big(y(x)\big)$.

Kako u našem primeru nismo realizovali treću fazu, moramo računati:

$$S\big(xy(x)\big) = xS\big(y(x)\big) - g(x)s_7 = x(x + x^2 + x^6 + x^7) - 1g(x) =$$

$$= x^2 + x^3 + x^7 + x^8 - 1 - x^4 - x^6 - x^7 - x^8 =$$

$$= 1 + x^2 + x^3 + x^4 + x^6$$

Opet ni ovog sindroma nema u tablici, pa računamo:

$S\big(x^2y(x)\big) = xS\big(xy(x)\big) - g(x)s_7 = x(1 + x^2 + x^3 + x^4 + x^6) - 0g(x) =$
$= x + x^3 + x^4 + x^5 + x^7$, ovaj sindrom postoji u tablici i odgovara mu polinom greške $e(x) = x^4 + x^{14}$, pa $y(x)$ dekodiramo kao kodnu reč

$$c(x) = y(x) - x^{15-2}e(x) = 1 + x^4 + x^7 + x^9 + x^{10} + x^{12} - x^2 - x^{12} =$$
$$= 1 + x^2 + x^4 + x^7 + x^9 + x^{10} = (1 + x^2)g(x)$$

Odnosno reč $y = 10\mathbf{0}010010110\mathbf{1}00$ dekodiramo kao $c = 10\mathbf{1}010010110\mathbf{0}00$, vidimo da su se desile dve greške na trećoj i trinaestoj koordinati.

□

Primetimo da je dimenzija ovog koda 7, a dužina kodnih reči čak 15, tako da bi procedura iz poglavlja 3 kojim dekodiramo linearni kod, praveći kosete bila mukotrpan i obiman posao, nezamisliv bez upotrebe računara. Za ciklične kodove prikazani algoritam je dosta optimalniji od univerzalnog za linearne kodove. Ključnu ulogu je odigrao naravno generišući polinom koda, jer smo na osnovu njega mogli zaključiti i podatak o kodnom rastojanju, ali i sama funkcija $R_{g(x)}\big(v(x)\big)$ je zasnovana na $g(x)$.

4.3 BCH i Rid-Solomonovi[5] kodovi

U tvrđenju 4.2.1 prikazana je tzv. BCH granica. Sada ćemo posvetiti pažnju specijalnim cikličnim BCH kodovima, koji su dobili naziv kao akronim od tri početna slova prezimena tri matematičara koji su ih otkrili, a to su Hocqenghem, francuski matematičar, koji ih je osmislio 1959. i američko-indijski matematičari Bose i Ray-Chaudhuri, koji su 1960. nezavisno konstruisali ovu klasu kodova. Rid-Solomonovi kodovi su specijalna potklasa BCH kodova. BCH kodovi su našli primenu u industriji DVD-jeva i CD-ova.

DEFINICIJA 4.3.1 Neka je dato polje F_q i neka je α primitivni element polja F_{q^t}. Neka su $m_{\alpha^i}(x)$ minimalni polinomi za α^i nad poljem F_q. **BCH** kod, nad azbukom F_q, gde je dužina kodne reči $n = q^t - 1$, je cikličan kod generisan polinomom:

$$g(x) = NZS(m_{\alpha^a}(x), m_{\alpha^{a+1}}(x), \dots, m_{\alpha^{a+dd-2}}(x))$$

gde je $a \in \mathbb{N}$, a dd planirano kodno rastojanje (design distance).

[5] Gustave Solomon (1930-1996) američki matematičar i inženjer

PRIMER 4.3.2 Neka je $q = 2$, $s = 1$, $n = 7$, $t = 3$, i $a = 1$, a $dd = 3$. Uočimo primitivni element α polja F_8. Tada imamo binaran BCH kod koji je generisan sa $g(x) = NZS(m_{\alpha^1}(x), m_{\alpha^2}(x))$. Kako su 2-ciklotomični koseti po modulu 7 isti za 1 i 2, onda su po lemi 4.1.8 i primeru 4.1.9 $m_{\alpha^1}(x) = m_{\alpha^2}(x) = 1 + x^2 + x^3$, pa je $g(x) = 1 + x^2 + x^3$, a na osnovu tvrđenja 4.1.13 generišuća matrica ovog koda je:

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

□

TVRĐENJE 4.3.3 *Dimenzija BCH koda k nad F_q i $n = q^t - 1$, sa planiranim kodnim rastojanjem dd zadovoljava sledeću nejednakost*:

$$k \geq n - t(dd - 1)$$

Dokaz. Posmatrajmo generišući polinom ovog koda

$$g(x) = NZS(m_{\alpha^a}(x), m_{\alpha^{a+1}}(x), \dots, m_{\alpha^{a+dd-2}}(x))$$

Za svako $s \in \{a, a+1, \dots, a+dd-2\}$ minimalni polinomi su oblika $m_{\alpha^s}(x) = \prod_{i \in C_s}(x - \alpha^i)$. Kako je $g(x)$ najmanji zajednički sadržalac za ove polinome možemo zaključiti da je $g(x) = \prod_{i \in C}(x - \alpha^i)$, gde je $C = \bigcup_{s=a}^{a+dd-2} C_s$, tako da je stepen polinoma $g(x)$ zapravo $|C|$. Dalje je,

$$|C| = \left| \bigcup_{s=a}^{a+dd-2} C_s \right| \leq \sum_{s=a}^{a+dd-2} |C_s| \leq \sum_{s=a}^{a+dd-2} t = t(dd - 1)$$

Poslednja nejednakost važi zato što se u jednom q-ciklotomičnom kosetu po modulu n može naći maksimalno t elemenata, jer je $q^t \equiv 1 \ (mod\ n)$. Na osnovu tvrđenja 4.1.13 stepen polinoma $g(x)$ je jednak $n - k$, pa je $|C| = n - k$, kada ubacimo ovaj izraz u gornju nejednakost dobijamo $n - k \leq t(dd - 1)$, odnosno $k \geq n - t(dd - 1)$.

■

TVRĐENJE 4.3.4 *Neka je C q-naran BCH kod. Tada je $d(C) \geq dd$.*

Dokaz. Direktno sledi iz tvrđenja 4.2.1, ako uzmemo da je $\delta = dd$.

■

BCH kodovi mogu da ostvare svoje planirano kodno rastojanje, i u tome se ogleda njihov veliki značaj. U primeru 4.3.2 kako je $dd = 3$ i $\|g(x)\| = 3$ dobijamo da je kodno rastojanje datog koda baš 3. Za kraj ovog master rada navodimo još jednu klasu linearnih kodova, specijalne BCH kodove, a to su Rid-Solomonovi kodovi.

DEFINICIJA 4.3.5 q-naran BCH kod, gde je $q > 2$, naziva se **Rid-Solomonov** kod ako je $n = q - 1$, tj. parametar $t = 1$. Ovde se minimalni polinom $m_{\alpha^s}(x)$ svodi na izraz $m_{\alpha^s}(x) = x - \alpha^s$.

PRIMER 4.3.6 Neka je $q = 5$, α primitivni element polja $GF(5)$ koje je zapravo polje $\mathbb{Z}_5$, pa je npr. $\alpha = 2$. Ako je $dd = 3$ i $a = 1$, generišući polinom je oblika:

$$g(x) = NZS\big(m_{\alpha^1}(x), m_{\alpha^2}(x)\big) = NZS\big((x-\alpha),(x-\alpha^2)\big) = (x-2)(x-4)$$

tj. $g(x) = (x+3)(x+1) = x^2 + 4x + 3$, jer se nalazimo u polju $\mathbb{Z}_5$

Generišuća matrica ovog koda je sledeća:

$$G = \begin{bmatrix} 3 & 4 & 1 & 0 \\ 0 & 3 & 4 & 1 \end{bmatrix}$$

□

Rid-Solomonovi kodovi su verovatno najpoznatiji i najprimenjiviji nebinarni linearni kodovi, jer za $q = 2$ dužina kodne reči bi bila 1, što nije interesantno.

Zaključak

Linearni kodovi su zaista bogata familija blok-kodova, ali ovaj rad se pozabavio najznačajnijim i najinteresantnijim među njima. U 3. poglavlju uopšteno smo obradili linearne kodove posmatrajući ih kao vektorske potprostore nad konačnim poljima. Prikazan je opšti postupak dekodiranja, za koji se može reći da je prilično neoptimalan u poređenju sa metodama dekodiranja kod specijalne klase linearnih kodova, koje smo posebno obradili, cikličnih kodova. Najbitnije od svega je bilo pronaći kodno rastojanje datog koda, napraviti ga što većim, ali opet ne ugroziti previše ekonomičnost koda, odnosno dužinu kodne reči, i imati što efikasniji algoritam za dekodiranje. Kod Rid-Milerovih i BCH kodova, vidimo da kodno rastojanje zavisi od povoljno izabranih parametara. Golejev binarni kod G_{23} ima osobinu da je to 3-savršen. To znači da se sve reči iz skupa $\{0,1\}^{23}$ mogu jednoznačno rasporediti po disjunktnim sferama, poluprečnika 3 sa centrima u kodnim rečima ovog koda. Ovakvo svojstvo omogućava vrlo precizno dekodiranje, jer za bilo koju reč, pronađemo sferu kojoj pripada, i u toj sferi je samo centar, kodna reč. Rid-Milerovi kodovi su već po samoj svojoj konstrukciji fascinantni, dok kod Hemingovih kodova koji omogućavaju ispravljanje jedne greške, dobijamo i podatak u binarnom zapisu o mestu gde je greška nastala, što je opet vrlo zanimljivo. Svaka klasa linearnih kodova ima neku specifičnost za sebe, ali su opet svi dizajnirani da budu što efikasniji u prenosu informacija.

Literatura

[1] B. Šešelja, Teorija informacije i kodiranja, Symbol, Novi Sad, 2005.

[2] B. Šešelja i A. Tepavčević, Algebra 2, Symbol, Novi Sad, 2005.

[3] W.C. Huffman and V. Pless, Fundamentals of Error-Correcting Codes, Cambridge UP, 2003.

[4] R.H. Morelos-Zaragoza, The Art of Error Correcting Coding, John Willey and Sons, 2002.

[5] R.E. Blahut, Algebraic Codes for Data Transmission, Cambridge UP, 2003.

[6] O. Pretzel, Error Correcting Codes and Finite Fields, Clarendon Press, Oxford, 1992.

[7] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, A. Wassermann, Error-Correcting Linear Codes, Classification by Isometry and Applications, Springer, 2006.

[8] F.J. MacWilliams, N.J.A. Sloane, The Theory of Error-Correcting Codes, North-Holland Publishing Company, 1981.

[9] Ron M. Roth, Introduction to Coding theory, Cambridge UP, 2007.

[10] Robert J. McEliece, The Theory of Information and Coding, Cambridge UP, 2004.

Biografija

Bojan Berleković je rođen 14.02.1991. godine u Somboru. Osnovnu školu „Dositej Obradović“ je završio kao nosilac Vukove diplome i Srednju ekonomsku školu kao učenik generacije. Zbog afiniteta prema matematici upisao je 2010. godine osnovne studije iz matematike na Prirodno-matematičkom fakultetu u Novom Sadu. 2013. godine je završio osnovne studije i upisao master studije iz matematike – modul Nastava matematike na istom fakultetu. U junu 2015. godine položio je poslednji ispit i stekao pravo da odbrani master rad.

Novi Sad, avgust 2016. Bojan Berleković

UNIVERZITET U NOVOM SADU
PRIRODNO-MATEMATIČKI FAKULTET
KLJUČNA DOKUMENTACIJSKA INFORMACIJA

Redni broj:
RBR
Identifikacioni broj:
IBR
Tip dokumentacije: Monografska dokumentacija
TD
Tip zapisa: Tekstualni štampani materijal
TZ
Vrsta rada: Master rad
VR
Autor: Bojan Berleković
AU
Mentor: dr Branimir Šešelja
MN
Naslov rada: Neke klase linearnih kodova
MR
Jezik publikacije: Srpski (latinica)
JP
Jezik izvoda: Srpski/Engleski
JI
Zemlja publikovanja: Republika Srbija
ZP
Uže geografsko područje: Vojvodina
UGP
Godina: 2016.
GO
Izdavač: Autorski reprint
IZ
Mesto i adresa: Prirodno-matematički fakultet, Departman za matematiku i informatiku, Trg Dositeja Obradovića 4, Novi Sad
MA
Fizički opis rada: (4/69/0/7/11/0/0)
Naučna oblast: Matematika
NO
Naučna disciplina: Teorija kodiranja
ND
Ključne reči: Vektorski prostori nad konačnim poljima, linearni kodovi, generišuća i kontrolna matrica, ciklični kodovi, dekodiranje

PO
UDK:
Čuva se: Biblioteka Departmana za matematiku i informatiku, Prirodno-matematički fakultet, Univerzitet u Novom Sadu
ČU
Važna napomena:
VN
Izvod: Tema ovog master rada su linearni kodovi. U prvom poglavlju je izneta teorijska osnova za linearne kodove kao što su polinomi, konačna polja, vektorski prostori. U drugom poglavlju se predstavljaju osnove teorije kodiranja, ali se blok-kodovi stavljaju u prvi plan. Treće poglavlje se odnosi na specijalne blok-kodove, a to su linearni kodovi, gde se izlaže njihova konstrukcija i uopštena metoda dekodiranja, ali primeri poznatih klasa linearnih kodova, Hemingovi, Golejevi i Rid-Milerovi kodovi. Četvrto poglavlje se odnosi na jednu značajnu klasu linearnih kodova, koji se nazivaju ciklični kodovi. U ovom poslednjem poglavlju se izlaže posebna metoda za dekodiranje cikličnih kodova, kao i primeri cikličnih BCH i Rid-Solomonovih kodova.
IZ
Datum prihvatanja teme od strane NN veća: 21.04.2015.
DP
Datum odbrane:
DO
Članovi komisije:
KO
Predsednik: dr Andreja Tepavčević, redovni profesor Prirodno-matematičkog fakulteta, Univerziteta u Novom Sadu
Mentor: dr Branimir Šešelja, redovni profesor Prirodno-matematičkog fakulteta, Univerziteta u Novom Sadu
Član: dr Petar Đapić, docent Prirodno-matematičkog fakulteta, Univerziteta u Novom Sadu

UNIVERSITY OF NOVI SAD
FACULTY OF SCIENCE
KEY WORDS DOCUMENTATION

Accession number:
ANO
Identification number:
INO
Document type: Monograph type
DT
Type of record: Printed text
TR
Contents Code: Master's thesis
CC
Author: Bojan Berleković
AU
Mentor: Branimir Šešelja, Ph. D.
MN
Title: Some classes of linear codes
TI
Languarge of text: Serbian (Latin)
LT
Language of abstract: Serbian/English
LA
Country of publication: Republic of Serbia
CP
Locality of publication: Vojvodina
LP
Publication year: 2016
PY
Publisher: Author's reprint
PU
Public place: Department of Mathematics and Informatics, Faculty of Science, Trg Dositeja Obradovića 4, Novi Sad
PP
Physical description: (4/69/0/7/11/0/0)
PD
Scientific field: Mathematics
SF
Scientific discipline: Coding theory
SD

Key words: Vector spaces above finite fields, linear codes, generator and control matrix, cyclic codes, decoding
KW
Holding data: Library of Department of Mathematics and Informatics, Faculty of Science, University of Novi Sad
HD
Note:
N
Abstract: The theme of this master's thesis are linear codes. The first chapter presents theoretical basis for linear codes such as polynomials, finite fields, vector spaces. The second chapter presents the basics of coding theory, but block codes in the foreground. The third chapter refers to the special block codes, which are linear codes, where they exhibited their construction and generalized method of decoding, or examples of known classes of linear codes, Hamming, Golay and Reed –Miller codes. The fourth chapter relates to an important class of linear codes, also called cyclic codes. In this final chapter presents a special method for decoding cyclic codes, as well as examples of cyclic BCH and Reed – Solomon codes.
AB
Accepted by the Scientific Board on: 21.04.2015.
ASB
Defended:
DE
Thesis defend board:
DB
President: Andreja Tepavčević PhD, full professor, Faculty of Science, University of Novi Sad
Mentor: Branimir Šešelja PhD, full professor, Faculty of Science, University of Novi Sad
Member: Petar Đapić PhD, docent, Faculty of Science, University of Novi Sad