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

Agneš Kovač

Ciklični kodovi

-master rad-

Mentor: dr Petar Đapić

Novi Sad, 2015.

Sadržaj

Predgovor

Kodiranje se javlja u svakodnevnom životu: svi elektronski uređaji, kompjuter i prateće komponente, CD-ovi, internet, telefon, barkodovi na raznim proizvodima ili ISBN brojevi na knjigama koriste se nekim kodiranjem. Zahvaljujući tome, nauka kodiranja počev od 20-og veka se brzo razvijala, jer je bilo važno da prenos informacije bude tačan i efikasan.

Kodiranja možemo demonstrirati na jednostavnom primeru. Neka reč "ne" bude kodirana sa 0, a reč "da" sa 1. Ukoliko dođe do greške prilikom slanja informacije, moguće je da dobijemo upravo suprotnu poruku od poslate. Da bismo to izbegli, "ne" možemo kodirati sa 00, a "da" sa 11. Ovako smo smanjili mogućnost da dobijemo sasvim netačnu informaciju ("da" umesto "ne" i obratno), odnosno lako ćemo uočiti ako umesto jedne nule dobijemo 1 ili obratno. Doduše ovu poslednju grešku ne možemo ispraviti, ali barem smo je konstatovali i možemo tražiti ponovno slanje informacije.

Kodiranje reči "da" i "ne" možemo proizvoljno produžiti na reči dužine n, ali onda to ide na račun brzine. Prepolovićemo brzinu prenosa informacije, kada u kodiranju umesto jedne cifre koristimo dve.

Ovaj master rad sa jedne strane se bavi pitanjem efikasnosti kodiranja, a sa druge strane ispravljanjem grešaka. Prvo ćemo se osvrnuti na osnovne pojmove teorije informacije - kako izgleda i funkcioniše sistem i informacijski kanal, šta je entropija i koje su njene osobine. Zatim prelazimo na teoriju kodiranja. Proučavaćemo kodiranje u kanalu bez smetnji i kodiranje u kanalu sa smetnjama. Pri kraju se bavimo blok-kodovima, zatim analiziramo linearne i ciklične kodove, gde ćemo se osvrnuti na nekoliko specifičnih cikličnih kodova.

Agneš Kovač

1. Osnovni pojmovi

Pre nego što pređemo na oblast teorije informacije i kodiranja, navedimo pojmove i osobine iz algebre i linearne algebre koje ćemo direktno koristiti u ovom master radu.

1.1. Algebarske strukture

Definicija 1.1. Uređeni par $(G,*)$ je **grupoid**, gde je G neprazan skup, a $*$ je binarna operacija na G.

Definicija 1.2. Grupoid $(G,*)$ je **asociativan** ako važi asocijativni zakon, tj. za sve $x, y, z \in G$ važi

$$x * (y * z) = (x * y) * z.$$

Definicija 1.3. Grupa $(G,*)$ je takav grupoid da važe sledeće osobine:

i. $(\forall x, y, z \in G)\ (x * y) * z = x * (y * z)$,
ii. $(\exists e \in G)\ (\forall x \in G)\ x * e = e * x$,
iii. $(\forall x \in G)\ (\exists a \in G)\ x * a = a * x = e$.

Elemenat e se zove **neutralni** elemenat, a elemenat a **inverzni**.

Definicija 1.4. Komutativna grupa je grupa, gde za sve $x, y \in G$ važi $x * y = y * x$. Komutativnu grupu zovemo još i **Abelova grupa**.

Definicija 1.5. Ha je **desna klasa (koset) razlaganja**

$$Ha = \{ha : h \in H\},$$

ako je H podgrupa grupe G i a je elemenat iz grupe G.

Napomena: U daljem tekstu desnu klasu razlaganja nazivamo samo klasa ili koset.

Osobine klasa:

1.) $x \in Ha$ ako i samo ako $xa^{-1} \in H$ (ako je $x \in Ha$ tada postoji $h \in H$ takav da je $x = ha$ pa imamo da $xa^{-1} = (ha)a^{-1} = h$),
2.) Klase Ha obrazuje particiju grupe G (klase su neprazne i međusobno ili disjunktne ili jednake),
3.) $Ha = Hb$ ako i samo ako $a \in Hb$.

Definicija 1.6. Prsten $(R, +, \cdot)$ je operacijska struktura sa dve binarne operacije sa sledećim osobinama

1.) $(R, +)$ je Abelova grupa,

2.) $(R, \cdot)$ je asociativan grupoid,

3.) za sve $x, y, z \in R$ važi

$$x \cdot (y + z) = x \cdot y + x \cdot z,$$

$$(x + y) \cdot z = x \cdot z + y \cdot z.$$

Definicija 1.7. Presten $(R, +, \cdot)$ je **prsten sa jedinicom**, ako za $(R, \cdot)$ postoji neutralni elemenat.

Definicija 1.8. Prsten $(R, +, \cdot)$ je **komutativan** ako za sve $x, y \in R$ važi $x \cdot y = y \cdot x$.

Definicija 1.9. Kažemo da je funkcija $f: P \longrightarrow R$ **homomorfizam** $(P, +, \cdot)$ u prsten $(R, +, \cdot)$, ako za sve $x, y \in P$ važi$f(x + y) = f(x) + f(y)$ i $f(x \cdot y) = f(x) \cdot f(y)$. Ako je funkcija f i bijekcija, onda to preslikavanje zovemo **izomorfizam**.

Definicija 1.10. Neka je R prsten. $I \subseteq R$ je **ideal** u prstenu R, $I \neq \emptyset$, ako

i) za svaki $a, b \in I$ sledi $a - b \in I$

ii) za svaki $r \in R,\ a \in I$ sledi $r \cdot a \in I$ i $a \cdot r \in I$.

Definicija 1.11. I je **glavni ideal** u komutativnom prstenu R ako postoji $g \in I$, koji generiše I, tj. svaki elemenat iz I možemo dobiti pomoću g:

$$I = \langle g \rangle = \{rg, r \in R\},$$

g se zove **generator ideala** I.

Definicija 1.12. Polje je komutativan prsten $(F, +, \cdot)$ sa jedinicom takav da je $(F \setminus \{0\}, \cdot)$ grupa, gde je 0 neutralni element za sabiranje.

Definicija 1.13. Kažemo da je α **primitivan element** iz F_q ako je on generator skupa F_q, tj.

$$F_q = \{0, \alpha, \alpha^2, \dots, \alpha^{q-1}\}.$$

Definicija 1.14. Potpolje P polja $(F, +, \cdot)$ je neprazni podskup skupa F, koji je zatvoren u odnosu na operacije + i $\cdot$.

Teorema 1.1. *Za svaki elemenat β iz polja F važi da je $\beta^q = \beta$, gde je $q = |F|$.*

Dokaz: Za $\beta = 0$ dokaz je trivijalan.

Neka je $\beta \neq 0$. Obeležimo sa F^* nenula elemente polja F,

$$F^* = \{\beta_1, \dots, \beta_{q-1}\}.$$

F^* se može napisati i na sledeći način: $F^* = \{\beta \cdot \beta_1, \dots, \beta \cdot \beta_{q-1}\}$, jer je $\beta \cdot \beta_i \in F^*$ za $i = 1, \dots, q - 1$ i pošto je $(F^*, \cdot)$ grupa, pa važi zakon kancelacije.

Posmatrajmo proizvod nenula elemenata polja F

$$\beta_1 \cdot \ldots \cdot \beta_{q-1} = (\beta \cdot \beta_1) \cdot \ldots \cdot (\beta \cdot \beta_{q-1}) = \beta^{q-1} \cdot (\beta_1 \cdot \ldots \cdot \beta_{q-1}).$$

Sledi da je $\beta^{q-1} = 1$.

■

Posledica 1.2. *Neka je F potpolje polja E i $|F| = q$. Elemenat $\beta \in E$ pripada potpolju F ako i samo ako $\beta^q = \beta$.*

Dokaz: ($\Longrightarrow$) Iz prethodne teoreme sledi ovaj smer.

($\Longleftarrow$) Pretpostavimo da važi $\beta^q = \beta$. Posmatrajmo polinom $x^q - x$. Ovaj polinom ima najviše q različitih korena nad poljem E. Pošto su elementi polja F koreni polinoma $x^q - x$, i $|F| = q$, zato je F skup svih korena polinoma $x^q - x$ nad poljem E. Pošto za bilo koji $\beta \in E$ za koji važi $\beta^q = \beta$, sledi da je β koren polinoma $x^q - x$, zato $\beta \in F$.

■

Definicija 1.15. Kompozicija polja $E \cdot F$ je najmanje polje koje sadrži oba polja E i F.

Definicija 1.16. Karakteristika polja F je najmanji pozitivan broj p za koji važi da je $p \cdot 1 = 0$. Ako ne postoji takav p, tada karakteristiku definišemo da je 0.

Može se pokazati da konačno polje sa karakteristikom p ima p^n elemenata za neki $n \in \mathbb{N}$. ([3], Teorema 3.1.14)

1.2. Vektorski prostor

Definicija 1.17. Neka je V sa operacijom $+$ Abelova grupa, F_q je polje. Definišimo preslikavanje $\cdot : F_q \times V \to V$ tako da važi za svaki $u, v, w \in V$, $\alpha, \beta \in F_q$

1. $\alpha \cdot (u + v) = \alpha \cdot u + \alpha \cdot v$,
2. $(\alpha + \beta) \cdot u = (\alpha \cdot u) + (\beta \cdot u)$,
3. $\alpha \cdot (\beta \cdot u) = (\alpha \cdot \beta) \cdot u$,
4. $1 \cdot u = u$,

tada se V naziva **vektorski prostor** nad poljem F_q.

Definicija 1.18. Skup $W \subseteq V$ je **potprostor** vektorskog prostora V nad poljem F ako je zatvoren u odnosu na operacije $+$ i $\cdot$, dakle i sam W je vektorski prostor nad istim poljem.

F_q^n je vektorski prostor nad poljem F_q, pri čemu je sabiranje vektora definisano po koordinatama, kao i množenje sa elementima iz F_q.

Definicija 1.19. Skalarni proizvod $\circ: F_q^n \times F_q^n \longrightarrow F_q$ je operacija koju definišemo na sledeći način: $x, y \in F_q^n$, $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n)$

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

Za skalarni proizvod ispunjeni su zakoni komutativnosti i distributivnosti prema sabiranju vektora:

$$x \circ y = y \circ x,$$

$$x \circ (y + z) = (x \circ y) + (y \circ z).$$

Definicija 1.20. Vektor x je **ortogonalan** na vektor y ako je

$$x \circ y = 0.$$

1.3. Prsten polinoma

Definicija 1.21. $F[x]$ je **prsten polinoma**, ako je F polje, gde je

$$F[x] = \left\{ \sum_{i=1}^{n} a_i x^i , a_i \in F, n \geq 0 \right\},$$

gde se elementi skupa $F[x]$ zovu **polinomi**. Neka je $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ polinom iz $F[x]$, tada se n zove **stepen polinoma** i označavamo ga sa $deg(f(x)) = n$.

$F[x]$ je prsten u odnosu na sabiranje i množenje polinoma definisano na uobičajen način. $F[x]$ je vektorski prostor nad poljem F, gde je sabiranje definisano uobičajno, a množenje sa skalarom (tj. elementom iz F) isto na uobičajen način.

Definicija 1.22. Polinom $f(x)$ je **normiran** ako $a_n = 1$.

Definicija 1.23. Polinom $f(x)$, $deg(f(x)) = n$ je **svodljiv** nad F ako postoje polinomi $g(x)$ i $h(x)$, $deg\big(g(x)\big)$, $deg(h(x)) < deg(f(x))$, tako da je

$$f(x) = g(x)h(x),$$

u suprotnom polinom je **nesvodljiv**.

Definicija 1.24. Najmanji zajednički sadržalac polinoma $f(x), g(x)$, u oznaci nzs$(f(x), g(x))$ je normirani polinom najmanjeg stepena koji je deljiv sa polinomima $f(x)$ i $g(x)$.

Najmanji zajednički sadržalac možemo proširiti i na više od dva polinoma. Važe sledeće osobine:

i) nzs$\big(f_1(x), \dots, f_{n-1}(x), f_n(x)\big)$ =nzs(nzs$\big(f_1(x), \dots, f_{n-1}(x)\big), f_n(x)$)

ii) $\text{nzs}\left(f_1(x), \dots, f_n(x)\right) = p_1(x)^{\max\ \{e_{11},\dots,e_{1n}\}} \dots p_n(x)^{\max\ \{e_{n1},\dots,e_{nn}\}}$,

gde je $f_i(x) = a_i p_1(x)^{e_{i1}} \dots p_n(x)^{e_{in}}$, $a_i \in F_q \setminus \{0\}$, $e_{ij} \geq 0$, i polinomi $p_i(x)$ su različiti normirani nesvodljivi polinomi nad F_q, $i, j \in \{1, \dots, n\}$.

$\boldsymbol{F_q[x]/(x^n - 1)}$ je skup svih ostataka polinoma iz $F_q[x]$ pri deljenju sa $(x^n - 1)$. $F_q[x]/(x^n - 1)$ je prsten zajedno sa sabiranjem $+$ i množenjem $\cdot$. $F_q[x]/f(x)$ je polje ako i samo ako $f(x)$ je nesvodljiv polinom, dakle, za $F_q[x]/(x^n - 1)$ polinom $(x^n - 1)$ je nesvodljiv jedino ako je $n = 1$. [3]

Može se pokazati da postoji nesvodljiv polinom stepena n nad $\mathbb{Z}_p$, gde je p prost broj.

Teorema 1.3. *Za svaki prost broj p i $n \in \mathbb{N}$ postoji jedinstveno konačno polje sa p^n elemenata.*

Dokaz: Egzistencija. Definišemo skup $\mathbb{Z}_p$ skup ostataka pri deljenju sa p. Neka je $f(x)$ nesvodljiv polinom stepena n nad $\mathbb{Z}_p$. Tada $\mathbb{Z}_p[x]/f(x)$ je polje i $\left|\mathbb{Z}_p[x]/f(x)\right| = p^n$.

Jedinstvenost. Neka su E i F polja koja imaju p^n elemenata. Posmatramo polinom $x^{p^n} - x$ nad poljem $E \cdot F$. Tada iz Posledice 1.2. sledi da E i F su skupovi svih korena polinoma $x^{p^n} - x$ nad $E \cdot F$, tj. $E = F$.

■

Definicija 1.25. Minimalni polinom za $\alpha \in F_{q^m}$ nad F_q je normiran polinom $f(x) \in F_q[x]$ sa najmanjim stepenom takav da je

$$f(\alpha) = 0.$$

Neka je α primitivan elemenat skupa F_{q^m}. Označavamo sa $M_i(x)$ minimalni polinom za α^i nad F_q.

Neka su p i m celi brojevi, $m > 0$. Tada sa $\boldsymbol{p \bmod m}$ označavamo ostatak pri deljenju p sa m. Slično $p(x) \bmod m(x)$ označava ostatak pri deljenju polinoma $p(x)$ sa polinomom $m(x)$.

Teorema 1.4. *Ideal u prstenu $F_q[x]/(x^n - 1)$ je glavni ideal.*

Dokaz: Treba dokazati da je $I = \langle g(x) \rangle$, za $g(x) \in I$ sa minimalnim stepenom. Ako je $I = \{0\}$, tada $I = \langle 0 \rangle$ je glavni ideal.

Pretpostavimo da $I \neq \{0\}$. Neka je $g(x) \in I$ nenula polinom najmanjeg stepena. Neka je $f(x) \in I$ proizvoljni polinom. Za polinome $f(x)$ i $g(x)$ postoje jedinstveni polinomi $q(x)$ i $r(x)$ takvi da je

$$f(x) = q(x)g(x) + r(x),$$

gde su $r(x)$ i $q(x)$ neki polinomi i $deg(r(x)) < deg(g(x))$.

Možemo izraziti $r(x)$ iz gornje jednakosti

$$r(x) = f(x) - q(x)g(x).$$

Iz $g(x), f(x) \in I$ na osnovu definicije ideala sledi da i $r(x)$ pripada I. $r(x)$ mora biti nula, jer bi u suprotnom imali polinom sa manjim stepenom polinoma od $g(x)$ što je kontradikcija sa pretpostavkom da polinom $g(x)$ ima najmanji stepen. Dobili smo da je

$$f(x) = q(x)g(x),$$

za svaki $f(x) \in I$, odnosno važi da $I = \langle g(x) \rangle$.

■

Definicija 1.26. V je potprostor vektorskog prostora F_q^n nad poljem F_q. **Klasa** ili **koset** vektorskog prostora V nad poljem F_q je skup $V + u$, za proizvoljno $u \in F_q^n$, gde je

$$V + u = \{v + u : v \in V\}.$$

Pošto u vektorskom prostoru važi komutativnost, onda je $V + u = u + V$.

Te klase su u stvari desni koseti na grupi F_q^n, pa zbog toga važe sledeće osobine:

1.) Svaki vektor iz F_q^n pripada nekom kosetu V.

2.) Za svaki vektor u iz F_q^n važi $|V + u| = |V| = q^k$.

3.) Ako $u, v \in F_q^n$, $u \in V + v$ tada je $V + u = V + v$.

4.) Za $u, v \in F_q^n$, $u - v \in V$ ako i samo ako u i v pripadaju istoj klasi.

Definicija 1.27. Vektor koji ima minimalnu normu u klasi zove se **lider** te klase.

Napomena: Lider klase ne mora biti jedinstven.

Definicija 1.28. Ciklotomični koset q-a (q-ciklotomični koset) modula n koji sadrži i je

$$C_i = \{iq^j \bmod n \in \mathbb{Z}_n, j = 0,1, \dots\},$$

gde su n i q relativno prosti brojevi.

Osobine:

i) Dva ciklotomična koseta su ili disjunktna ili jednaka.

ii) Broj elemenata q-ciklotomičnog koseta modula n koji sadrži i nije veći od m, ako je $n = q^m - 1$, $m \geq 1$.

iii) Ako je α primitivan elemenat skupa F_{q^m}, i $M_i(x)$ minimalni polinom za α^i nad F_q, tada je

$$M_i(x) = \prod_{j \in C_i} (x - \alpha^j),$$

gde je C_i q-ciklotomični koset modulo $q^m - 1$ koji sadrži i. (Videti [3].)

1.4. Vandermondova matrica

Vandremondova matrica je matrica koja ima sledeći oblik:

$$V = \begin{bmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_{n-1} & a_{n-1}^2 & \cdots & a_{n-1}^{n-1} \end{bmatrix}.$$

Ako su elementi $a_i, i = 0, \dots, n-1$ matrice V svi različiti, tada je Vandermondova matrica regularna. [5]

2. Elementi teorije informacije

Teorija kodiranja koristi se elementima teorije informacije. U ovom poglavlju navodimo najbitnije osnovne pojmove i teoreme koji će se koristiti kasnije, kao što su pojam sistema, entropije i komunikacijskog sistema.

2.1. Konačni verovatnosni sistemi

Definicija 2.1. Za dat konačan skup $X = \{x_1, \dots, x_n\}$ i za funkciju $p: X \to \mathbb{R}$, za koju važi:

1.) $p_i = p(x_i) \geq 0, i = 1, \dots, n,$

2.) $\sum_{i=1}^{n} p(x_i) = 1,$

definišemo **konačni verovatnosni sistem**, gde je $p(x)$ raspodela verovatnoće na skupu X. Označavamo sa $\{X, p(x)\}$. Elementi skupa X nazivaju se **stanjima**, a $p(x)$ su verovatnoće da se sistem nalazi u stanju x.

Primer 2.1. Ako je $\mathrm{X} = \{\text{pismo, grb}\}$, $\mathrm{p(pismo)} = \frac{1}{2}, \mathrm{p(grb)} = \frac{1}{2}$, tada sistem $\{\mathrm{X}, \mathrm{p(x)}\}$ odgovara ishodu pri jednom bacanju novčića.

□

Možemo proširiti pojam sistema i na direktne proizvode i preko toga na tzv. podsisteme na sledeći način:

$\{\mathrm{X} \times \mathrm{Y}, \mathrm{p(x,y)}\}$ je sistem, gde je $X \times Y = \{(x, y) | x \epsilon X, y \epsilon Y\}$, a $p(x, y)$ raspodela verovatnoće po uređenim parovima.

Definicija 2.2. Marginalna raspodela za složeni sistem $X \times Y$ definišemo kao

$$p(x_i) = \sum_{y_j \epsilon Y} p(x_i, y_j), \quad i = 1, \dots, n,$$

$$p(y_i) = \sum_{i \epsilon X} p(x_i, y_j), \quad j = 1, \dots, m,$$

i $\{\mathrm{X}, \mathrm{p(x)}\}$, $\{\mathrm{Y}, \mathrm{p(y)}\}$ su **podsistemi** složenog sistema $\{\mathrm{X} \times \mathrm{Y}, \mathrm{p(x,y)}\}$.

Kao što znamo iz verovatnoće, možemo definisati uslovne raspodele.

Definicija 2.3. Definicija **uslovne raspodele** na sistemu Y u odnosu na x_i je

$$p(y_j|x_i) = \frac{p(x_i,y_j)}{p(x_i)},$$

gde je $x_i \epsilon X, p(x_i) > 0,\ \forall j \epsilon \{1, \dots, m\}$.

Definicija 2.4. Sistemi X i Y su **nezavisni**, ako važi $p(x_i, y_j) = p(x_i) \cdot p(y_j)$, za sve $x_i \epsilon X,\ y_j \epsilon Y$, a u suprotnom sistemi su **zavisni**.

2.2. Definicija entropije i osnovne osobine

Neka je dat sistem {X, p(x)}. Taj sistem je neki izvor informacije. Zamislimo da smo izabrali element iz skupa X slučajno (prema raspodeli verovatnoće $p(x)$). Zbog definicije sistema, verovatnoća da smo izabrali element x_i je $p(x_i)$ (ili skraćeno p_i). Pre nego što smo uzeli element, imali smo određenu količinu neizvesnosti u vezi sa ishodom, a posle izbora dobijamo određenu količinu informacije o izvoru. Tako su pojmovi neizvesnosti (entropija) i informacije povezani.

Entropijom dakle merimo apriornu neodređenost sistema.

Kako možemo definisati funkciju $H(p_1, \dots, p_n)$ koja meri neizvesnost sistema? Treba voditi računa o sledećim osobinama neizvesnosti sistema kada definišemo funkciju:

1.) Tražimo takvu funkciju koja je definisana za svaki realni broj, za koju važi

$$p_i \leq 1, i \epsilon \{1, \dots, n\}, \sum_{i=1}^{n} p_i = 1.$$

Pored toga funkcija $H(p_1, \dots, p_n)$ treba da bude neprekidna, tj. mala promena u verovatnoći treba da izaziva malu promenu u neizvesnosti.

2.) Kada imamo jednako verovatne ishode, i ako imamo više ishoda, treba da imamo i veću entropiju, tj. što je veći broj stanja veća je i neodređenost

$$H\left(\frac{1}{n}, \dots, \frac{1}{n}\right) < H\left(\frac{1}{n+1}, \dots, \frac{1}{n+1}\right).$$

3.) Neka je skup $X = \{x_1, \dots, x_n\}$ podeljen na neprazne disjunktne blokove $Q_1, \dots, Q_k$, $k > 1$. Neka je verovatnoća da je elemenat x_i izabran $p_i = \frac{1}{n}$ za svako $i = 1, \dots, n$. Neka je $|Q_i| = q_i$, i = 1, …, k. (Tada važi $\sum q_i = n$). Izaberemo jedan blok na slučajan način. (Verovatnoće izbora blokova su srazmerne broju elemenata u tim blokovima, a to je $p(Q_i) = q_i/\text{n}$.) Posle toga iz tog bloka treba da izaberemo jedan element. Tada imamo sledeće uslovne raspodele, gde x_j pripada bloku Q_u:

$$p(x_j|Q_i) = \begin{cases} 0, & i \neq u \\ \dfrac{1}{q_u}, & i = u \end{cases}.$$

Tada možemo računati

$$p(x_j) = \sum_{i=1}^{n} p(x_j|Q_i)p(Q_i) = \frac{1}{q_u}\frac{q_u}{n} = \frac{1}{n}.$$

Dakle, verovatnoća da je element x_j izabran direktno iz skupa X jednaka je sa verovatnoćom da ćemo prvo izabrati blok gde se x_j nalazi, a onda izabrati element x_j iz bloka. To implicira da i entropija mora imati analogno svojstvo.

Sa jedne strane imamo entropiju sa ravnomernom raspodelom verovatnoće koja je $H\left(\frac{1}{n}, \dots, \frac{1}{n}\right)$. Sa druge strane, kada prvo odaberemo blok tada je neodređenost $H\left(\frac{q_1}{n}, \dots, \frac{q_k}{n}\right)$. Posle izabranog bloka još uvek imamo neodređenost elemenata iz bloka. Tako možemo izraziti prosečnu neodređenost na sledeći način:

$$\sum_{i=1}^{k} p(Q_i) \cdot (neodređenost\ izabiranja\ iz\ Q_i) = \sum_{i=1}^{k} \frac{q_i}{n} H\left(\frac{1}{q_i}, \dots, \frac{1}{q_i}\right).$$

Dakle, dobili smo da je entropija tada:

$$H\left(\frac{1}{n}, \dots, \frac{1}{n}\right) = H\left(\frac{q_1}{n}, \dots, \frac{q_k}{n}\right) + \sum_{i=1}^{k} \frac{q_i}{n} H\left(\frac{1}{q_i}, \dots, \frac{1}{q_i}\right).$$

Ako je $k = 1$, tada

$$H(1) = H(1) + \sum_{i=1}^{k} \frac{1}{1} H(1) = H(1) + H(1),$$

dakle,

$$H(1) = 0.$$

Teorema 2.1. *Funkcija H zadovoljava osobine 1.)-3.), za* $0 < p_i \leq 1, i\epsilon\{1, \dots, n\}, \sum_{i=1}^{n} p_i = 1$ *ako i samo ako ima oblik*

$$H_b(p_1, \dots, p_n) = -\sum_{i=1}^{n} p_i \log_b p_i,$$

gde je $b > 1$.

Dokaz: ($\Longleftarrow$) Prvo dokazujemo da H_b zadovoljava osobine 1.) - 3.).

1.) Funkcija H_b je dobro definisana i neprekidna je, jer je kompozicija neprekidnih funkcija.

2.) Treba dokazati da $H\left(\frac{1}{n},\dots,\frac{1}{n}\right) < H\left(\frac{1}{n+1},\dots,\frac{1}{n+1}\right), n\epsilon\mathbb{N}$. Sledeće nejednakosti su ekvivalentne:

$$-\sum_{i=1}^{n}\frac{1}{n}\log_b\frac{1}{n} < -\sum_{i=1}^{n+1}\frac{1}{n+1}\log_b\frac{1}{n+1},$$

$$-n\cdot\frac{1}{n}\log_b\frac{1}{n} < -(n+1)\cdot\frac{1}{n+1}\log_b\frac{1}{n+1},$$

$$\log_b\frac{1}{n} > \log_b\frac{1}{n+1},$$

$$\frac{1}{n} > \frac{1}{n+1}.$$

To jeste pravilno pošto je n prirodan broj i baza logaritma je $b > 1$.

3.)

$$H\left(\frac{q_1}{n},\dots,\frac{q_k}{n}\right) + \sum_{i=1}^{k}\frac{q_i}{n}H\left(\frac{1}{q_i},\dots,\frac{1}{q_i}\right) = -\sum_{i=1}^{k}\frac{q_i}{n}\log\frac{q_i}{n} + \sum_{i=1}^{k}\frac{q_i}{n}\log q_i$$

$$= \sum_{i=1}^{k}\frac{q_i}{n}\log\frac{\frac{q_i}{1}}{\frac{q_i}{n}} = \sum_{i=1}^{k}\frac{q_i}{n}\log n = n\cdot\frac{\log n}{n} = \log n$$

$$= H\left(\frac{1}{n},\dots,\frac{1}{n}\right)$$

što je i trebalo dokazati.

($\Longrightarrow$) Naka su m i n takvi da, $m,n\epsilon\mathbb{N}$, $m|n$, $b_i = m, \forall i\epsilon\{1,\dots,k\}$ i $k = \frac{n}{m}$. Tada je

$$m\cdot k = \sum_{i=1}^{k} b_i = n\,.$$

Na osnovu osobine 3.) imamo da je

$$H\left(\frac{1}{n},\dots,\frac{1}{n}\right) = H\left(\frac{m}{n},\dots,\frac{m}{n}\right) + \sum_{i=1}^{k}\frac{m}{n}H\left(\frac{1}{m},\dots,\frac{1}{m}\right)$$

$$= H\left(\frac{m}{n},\dots,\frac{m}{n}\right) + H\left(\frac{1}{m},\dots,\frac{1}{m}\right).$$

Neka sada bude $n = m^s,\ m,s\epsilon\mathbb{N}$, onda entropiju možemo napisati u sledećem obliku

$$H\left(\frac{1}{m^s},\dots,\frac{1}{m^s}\right) = H\left(\frac{1}{m^{s-1}},\dots,\frac{1}{m^{s-1}}\right) + H\left(\frac{1}{m},\dots,\frac{1}{m}\right).$$

Obeležimo sa h sledeću funkciju

$$h(n) \coloneqq H\left(\frac{1}{n}, \dots, \frac{1}{n}\right).$$

Do sada smo pokazali da za h važi

$$h(m^s) = h(m^{s-1}) + h(m).$$

Indukcijom po s dobijamo da je

$$h(m^s) = s \cdot h(m), \forall m, s \epsilon \mathbb{N}.$$

Sada koristeći osobinu 2.) dobijamo da je

$$h(m^s) < h(m^{s+1}),$$

jer je funkcija h strogo rastuća. Iz prethodne nejednakosti dobijemo

$$s \cdot h(m) < (s+1) \cdot h(m).$$

Pošto $s \epsilon \mathbb{N}$ sledi da je $h(m) > 0$.

Iz osobina prirodnih brojeva neposredno sledi da za proizvoljno $r, t \epsilon \mathbb{N}$, postoji s takav da važi

(1) $$m^s \leq r^t < m^{s+1}.$$

Za $m = 1$ to je $H(1) = h(1) = 0$

Za m različito od 1 i za $r = 1$ važi da ako $s = 0$

$$m^0 \leq 1^t < m^{0+1}$$

$$1 \leq 1 < m$$

što je u redu jer m nije 1.

Primenimo funkciju h na nejednakosti (1) i dobijemo

$$h(m^s) \leq h(r^t) < h(m^{s+1}),$$

$$s \cdot h(m) \leq t \cdot h(r) < (s+1) \cdot h(m).$$

Delimo izraz sa $t \cdot h(m)$ i dobijemo

(2) $$\frac{s}{t} \leq \frac{h(r)}{h(m)} < \frac{s+1}{t}.$$

Ako logaritmujemo $m^s \leq r^t < m^{s+1}$ dobijamo

$$s \cdot \log m \leq t \cdot \log r < (s+1) \cdot \log m,$$

(3) $$\frac{s}{t} \leq \frac{\log r}{\log m} < \frac{s+1}{t}.$$

Iz (2) zajedno sa (3) sledi

$$\left| \frac{h(r)}{h(m)} - \frac{\log r}{\log m} \right| < \frac{1}{t}.$$

Ako uzmemo da $t \longrightarrow \infty$, tada dobijamo

$$\frac{h(r)}{h(m)} = \frac{\log r}{\log m},$$

$$\frac{h(r)}{\log r} = \frac{h(m)}{\log m}.$$

$\frac{h(r)}{\log r}$ je konstantan izraz za sve r, tj. $\frac{h(r)}{\log r} = C$, pa je $h(r) = C \log r, C > 0$, zato je i $h(r) > 0$. Za specijalno izabrano b može se dobiti da je $C = 1$, tada za $r \epsilon \mathbb{N}$ važi

$$h(r) = \log_b r.$$

Iz osobine 3.) sledi

$$H\left(\frac{b_1}{n}, \dots, \frac{b_k}{n}\right) = h(n) - \sum_{i=1}^{k} \frac{b_i}{n} h(b_i) = \log_b n - \sum_{i=1}^{k} \frac{b_i}{n} \log_b b_i$$

$$= -\sum_{i=1}^{k} \frac{b_i}{n} \frac{\log_b b_i}{n}.$$

Svaki racionalan broj $p_1, \dots, p_k$ možemo napisati u obliku $\frac{b_1}{n}, \dots, \frac{b_k}{n}$ tako da svodimo na zajednički imenilac (a kada imamo realne brojeve zbog osobine 1.) svaki realan broj može se izraziti kao limes racionalnih brojeva jer je funkcija H neprekidna) i pri tome dobijemo

$$H_b(p_1, \dots, p_k) = -\sum_{i=1}^{k} p_i \log_b p_i.$$

■

Dakle, došli smo do definicije entropije:

Definicija 2.5. Neka je dat sistem $\{X, p(x)\}$, gde je $X = \{x_1, \dots x_n\}$, $p_i = p(x_i)$. Tada je **funkcija entropije** raspodele:

$$H(X) = H(p_1, \dots, p_n) = -\sum_{i=1}^{n} p_i \cdot \log_b p_i.$$

Napomena: Primetimo da važi:

$$\lim_{p \to 0^+} p \log_b p = 0$$

Ako definišemo da je $0 \cdot \log 0 = 0$, tada entropiju možemo računati i za raspodele u kojima se pojavljuje $p = 0$.

Primer 2.2. Neka imamo sistem $X = \{x_1\}$, $p(x_1) = 1$, tada

$$H(X) = H(x_1) = -p_1 \cdot \log_2 p_1 = -1 \cdot 0 = 0,$$

dakle nemamo neodređenost u ovom sistemu. Taj sistem može biti na primer nepravilan novčić koji ima sa obe strane grb.

□

Jedinica za entropiju je **bit** ako je baza logaritma $b = 2$. Do te baze možemo doći na sledeći način: Posmatramo binarni sistem sa dva jednakoverovatna stanja, tj. imamo

$$\mathrm{H}\left(\frac{1}{2},\frac{1}{2}\right) = -\mathrm{C}\sum_{i=1}^{2} p_i \cdot log_b p_i = h(2).$$

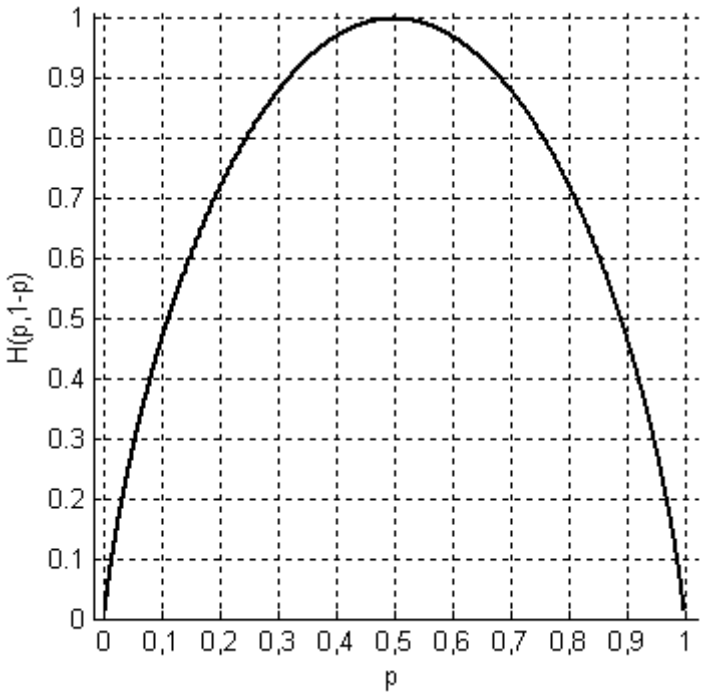
Hoćemo da dobijemo da je $h(2) = 1$, tj. treba tako izabrati konstante b i c da

$$c \log_b 2 = 1.$$

Za $c = 1$ dobijemo da je baza $b = 2$, pa je $h(2) = 1$ bit.

Napomena: U ovom radu bit smatramo kao meru entropije, a ne kao meru memorije. U navedenom Primeru 1.2. entropija sistema je 0 bitova, međutim, ako hoćemo sačuvati jedan ishod tog eksperimenta onda nam treba 1 bit memorije za direktno čuvanje te informacije.

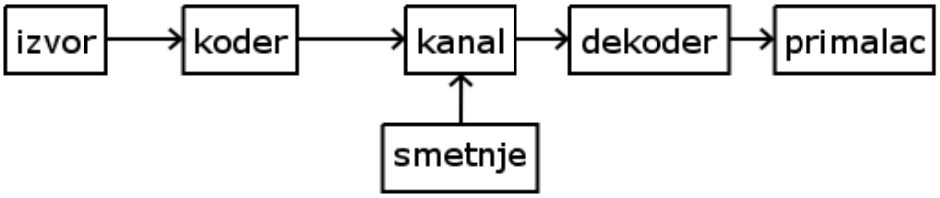
Ako posmatramo funkciju $H(p, 1-p) = -p \log p - (1-p)\log(1-p)$, tada dobijamo maksimalnu vrednost, za $p = 0.5$. Kao što i očekujemo intuitivno: neodređenost sistema je najveća ako je stanje sistema jednako verovatna (Slika 1.). To važi i za funkciju $H(p_1, \dots, p_n)$, ona maksimalnu vrednost dostiže kada je $p_1 = p_2 = \cdots = p_n = \frac{1}{n}$.



Slika 1.

2.3. Sistem komunikacije

Izvor informacije generiše poruku i šalje preko kodera. Koder transformiše poruku u odgovarajuću formu, u kodne reči i tako poruka ide kroz kanal. Informacije se prenose sa jednog mesta na drugo putem kanala. U kanalu su moguće smetnje, i zato su moguće greške u poruci. U opštem slučaju koder dodaje informacije (za poruku) koje služe da dekoder detektuje i ispravi greške. Posle toga poruka stiže primaocu koji je krajnji cilj informacije.



Slika 2.

Izvor informacije može biti na primer čovek koji telefonira, tada je kanal telefonski kabel, a primalac je drugi čovek. Drugi primer za komunikacijski sistem je e-mail koju šalje banka, tada je komunikacijski kanal internet kabel, izvor je automatizovan sistem koji šalje poruku, a primaoci smo mi.

2.4. Komunikacijski kanal

Definicija 2.6. Neka je dat konačan skup $X = \{x_1, \dots, x_n\}$, elemente skupa X nazivamo **slovima**, a skup X je **alfabet**. Uređene n-torke slova su **reči**, a skup

$$X^* = \bigcup_{i \in \mathbb{N}} X^i,$$

je skup svih reči nad X. **Dužina reči** je $n = |x|$ ako je $x \epsilon X^n$, tj. reč ima n slova.

Napomena: Zbog jednostavnosti reč $(x_1, \dots, x_n)$ obeležavaćemo sa $x_1 \dots x_n$.

Može se dodati skupu reči i prazna reč $\emptyset$, koja po definiciji ima dužinu nula, $|\emptyset| = 0$. Tada obeležimo sa $X^{\circledast} = X^* \cup \emptyset$.

Definicija 2.7. Neka su $x, y \epsilon X^{\circledast}$, $x = (x_1, \dots, x_n), y(y_1, \dots, y_m)$, tada binarna operacija **nadovezivanja** reči x i y je

$$z = xy = x_1 \cdots x_n y_1 \cdots y_m,$$

gde je x **prefiks** u reči z, a y je **sufiks**.

Definicija 2.8. Diskretni komunikacijski kanal K sa ulaznim alfabetom $U = \{u_1, \dots, u_a\}$ i izlaznim alfabetom $V = \{v_1, \dots, v_b\}$ definiše se kao uređena trojka $K = (U, P, V)$, gde je $P = \{p(y|(x,i)):\ x \epsilon U^n, y \in V^n,\ n \epsilon \mathbb{N},\ i \epsilon T = \{0,1,2,\dots\}\}$ kolekcija uslovnih raspodela verovatnoće, gde je $i \epsilon T = \{0,1,2,\dots\}$ trenutak emitovanja.

Kanal je diskretan jer su skupovi U i V konačni.

Verovatnoća $p(y|(x,i))$ je data zbog smetnje kanala, tu verovatnoću shvatamo intuitivno kao verovatnoću da se na izlazu pojavi reč y, ako je na ulazu primljena reč x.

Definicija 2.9. Komunikacijski kanal je **stacionaran** ako

$$p(y|(x,i)) = p(y|(x,j)), \qquad \forall i,j \epsilon T,$$

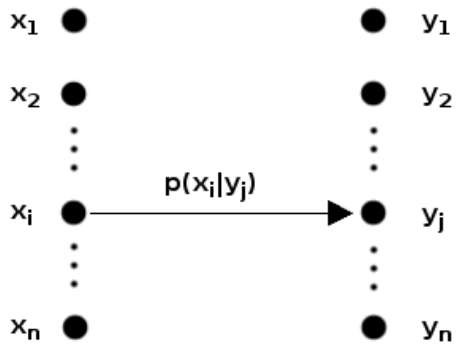
dakle vreme nema ulogu u prenošenju.

Definicija 2.10. Kažemo da je kanal K **bez memorije**, ako je K stacionaran i važi za svako n, $(x_1, \dots, x_n) \epsilon U^n, (y_1, \dots, y_n) \epsilon V^n$

$$p(y|x) = p((y_1, \dots, y_n)|(x_1, \dots, x_n)) = p(y_1|x_1) \cdot \dots \cdot p(y_n|x_n),$$

tj. ako je pojava bilo kog slova na izlazu nezavisna od pojave prethodnih izlaznih slova.

Jedan diskretan kanal bez memorije dat je na Slici 3.



Slika 3.

Definicija 2.11. Preko uslovnih verovatnoća definišemo **matricu kanala** Π formata $a \times b$

$$\Pi = \begin{bmatrix} p(v_1|u_1) & \cdots & p(v_b|u_1) \\ \vdots & \ddots & \vdots \\ p(v_1|u_a) & \cdots & p(v_b|u_a) \end{bmatrix},$$

gde je a broj elemenata ulaznog alfabeta ($a = |U|$), b je broj elemenata izlaznog alfabeta ($b = |V|$).

Tada kanal bez memorije označavamo sa $K = (U, \Pi, V)$.

Definicija 2.12. Kanal je **simetričan po ulazu** ako su sve vrste njegove matrice obrazovane permutacijama elemenata prve vrste.

Definicija 2.13. Kanal je **simetričan po izlazu** ako su sve kolone njegove matrice obrazovane permutacijama elemenata prve kolone.

Definicija 2.14. Kanal je **simetričan** ako je simetričan i po ulazu i po izlazu.

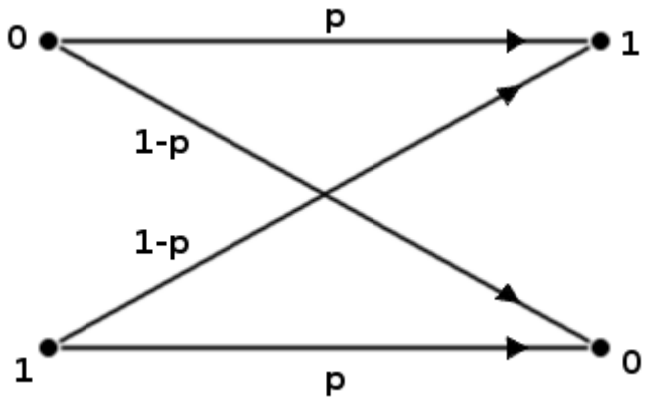
Primer 2.3. a) a-arni simetrični kanal je takav simetričan kanal koji ima matricu Π formata $a \times a$, $a > 1$.

b) Najznačajni simetrični kanal je *binarni simetrični kanal* (BSC), koji ima matricu kanala formata 2×2, tj. $a = b = 2,\ U = V = \{0,1\}$, $p < 0.5$

$$\Pi = \begin{bmatrix} 1-p & p \\ p & 1-p \end{bmatrix},$$

p je verovatnoća greške za jedan bit.

Na Slici 4. dat je binarni simetrični kanal.



Slika 4.

□

Lema 2.2. *Neka su dati brojevi* $p_1, \dots, p_n, q_1, \dots, q_n > 0$. *Ako* $\sum_{i=1}^{n} q_i \leq \sum_{i=1}^{n} p_i$ *tada*

$$\sum_{i=1}^{n} p_i \log_2 p_i \geq \sum_{i=1}^{n} p_i \log_2 q_i.$$

Jednakost važi pod uslovom da su $q_i = p_i$ *za sve* $i = 1, \dots, n$.

Dokaz: Znamo da važi $\ln x \leq x - 1$ i da $\log_a b = \frac{\log_c b}{\log_c a}$. Za $a = x$, $b = 2$ i $c = e$ imamo

$$\log_2 x = \frac{\ln x}{\ln 2}.$$

Vratimo u nejednakosti da je $\ln x = \log_2 x \ln 2$ i dobijamo

$$\log_2 x \ln 2 \leq x - 1.$$

Neka su $x_i = \frac{q_i}{p_i}, i = 1, \ldots, n$. Tada

$$\log_2 \frac{q_i}{p_i} \ln 2 \leq \frac{q_i}{p_i} - 1.$$

Množenjem nejednakosti sa $p_i / \ln 2$ i sumiranjem po i dobijamo

$$\sum_{i=1}^{n} p_i \log_2 \frac{q_i}{p_i} \leq \frac{1}{\ln 2} \sum_{i=1}^{n} q_i - p_i = \frac{1}{\ln 2} \left(\sum_{i=1}^{n} q_i - \sum_{i=1}^{n} p_i \right).$$

Po pretpostavci Leme $\sum_{i=1}^{n} q_i - \sum_{i=1}^{n} p_i \leq 0$ i $\frac{1}{\ln 2} > 0$ dobijamo da je

$$\sum_{i=1}^{n} p_i \log_2 \frac{q_i}{p_i} \leq 0,$$

odnosno,

$$\sum_{i=1}^{n} p_i \log_2 q_i - \sum_{i=1}^{n} p_i \log_2 p_i \leq 0,$$

što je i trebalo dokazati.

Jednakost dobijemo ako i samo ako $\ln x = x - 1$, tj. $x = 1$, tada je $q_i = p_i$ za sve $i = 1, \ldots, n$.

■

3. Teorija kodiranja

Definišemo najbitnije pojmove koji su neophodni da bismo se bavili analiziranjem strukture kodova. Sledi kratak osvrt na kodiranje bez smetnji, gde ćemo se baviti najviše prefiksnim kodovima.

3.1. Kodiranje

Definicija 3.1. Neka su dati konačni neprazni skupovi $A = \{\alpha_1, \dots, \alpha_a\}$ i $B = \{\beta_1, \dots, \beta_b\}$, A nazivamo **alfabetom izvora**, dok je B **alfabet koda**, broj $b = |B|$ je **baza koda**.

Definicija 3.2. Neka je $A' \subseteq A^*$. Svaka injekcija $f: A' \to B^*$ je jedno **kodiranje** nad alfabetom A. Skup $f(A') \subseteq B^*$ je **kod**. Elementi skupa $f(A')$ su **kodne reči** odgovarajućih reči iz A'. Kodiranje je **alfabetno** ako je $A' = A$, tj. ako se kodiraju tačno slova alfabeta A.

U nastavku se bavimo samo alfabetnim kodiranjem. Kao što smo definisali gore, to je injekcija $f: A \to B^*$, $A \subseteq A^*$, a kod $V = f(A)$ je skup reči, podskup od B^*. Svaka poruka – reč nad alfabetom A kodira se slovo po slovo. Tako dobijena reč nad alfabetom B se takođe nalazi u skupu B^*.

Primer 3.1. a) U alfabetno kodiranje spada i Morzeov kod koji se koristio u telegrafiji od 1837. godine.

A .-	F ..-.	K -.-	P .--.	U ..-	Z --..	4 ....-	9 ----.
B -..	G --.	L .-..	Q --.-	V ...-	0 -----	5	. .-.-.-
C -.-.	H	M --	R .-.	W .--	1 .----	6 -....	, --..--
D -..	I ..	N -.	S ...	X -..-	2 ..----	7 --...	? ..--..
E .	J .---	O ---	T -	Y -.--	3 ...--	8 ---..	! --.--

b) Srpski jezik: ako koristimo za kod latinicu, tada kodiranje nije alfabetno jer na primer imamo slovo „j“ i „l“ a imamo i slovo „lj“. A kada koristimo ćirilicu tada je kodiranje alfabetno.

□

Definicija 3.3. Neka je X' konačan podskup skupa X^*, tada je $\overrightarrow{X'}$ **skup svih prefiksa reči** iz X'.

Primer 3.2. Neka je dat $X = \{0, 1\}$, $X' = \{00, 10, 011, 111\}$, tada skup svih različitih prefiksa je

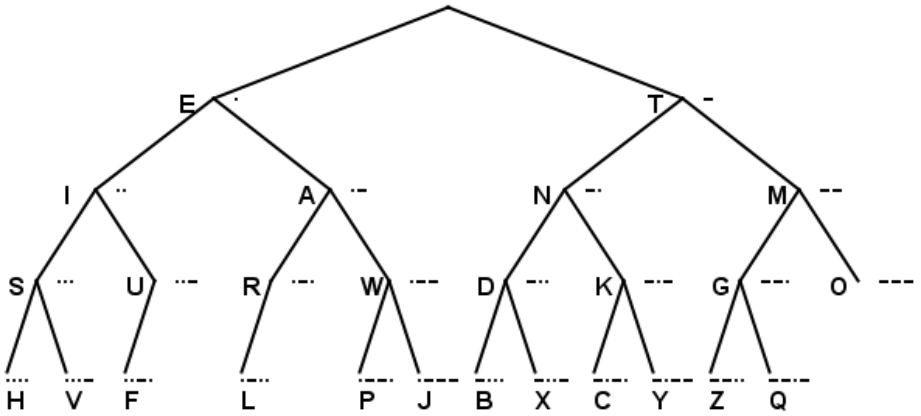
$$\overrightarrow{X'} = \{\emptyset, 0, 1, 00, 01, 10, 11, 011, 111\}.$$

□

Elementima skupa $\overrightarrow{X^*}$ mogu se jednoznačno pridružiti čvorovi jednog drveta (orijentisanog povezanog grafa bez konture) na sledeći način:

Čvorovi grafa su reči. Neka su x i y reči. Iz čvora x vodi grana u čvor y ako i samo ako $y = x\alpha$, gde je $\alpha \epsilon X$, dakle slovo.

Primer 3.3. Kodno drvo Morzeovog koda je dato na slici 5. (na slici se vidi samo engleska abeceda bez dodatnih simbola i brojeva)



Slika 5.

□

Možemo posmatrati problem dekodiranja na sledeća dva načina: u prvom slučaju dekodiramo u kanalu bez smetnje, tada se bavimo problemom kako treba da definišemo kodiranje da kod bude što efikasniji i da omogućuje jednoznačno dekodiranje. U drugom slučaju dekodiranje se dešava u kanalu sa smetnjama i onda ako detektujemo greške u toku dekodiranja, ako je moguće treba ispraviti te greške.

3.2. Kodiranje u kanalu bez smetnji

Definicija 3.4. Kod je **blok-kod** ako su sve njegove kodne reči iste dužine. Blok-kod se zove još i **kod sa fiksnom dužinom kodnih reči**. U suprotnom kod je **sa promenljivom dužinom kodnih reči**.

Primer 3.4. ASCII kod (American Standard Code for Information Interchange - Američki standardni kod za razmenu podataka) je blok-kod koji obrazuje kodne reči na 8 bitova. Od tih 8 bitova koristi se samo 7 bita, a na 8. –prvi bit sa leve strane- se stavi nula (pošto su računari koristili najčešće 8 bita za kodiranje, ponekad osmi bit je služio za ispravljanje grešaka – tada kreiramo takve kodne reči da svaka sadrži

paran broj jedinica, tada osmi bit može biti i 0 i 1), tako se ASCII kod sastoji od 128 kodnih reči. Od tih 128 kodnih reči 33 (prvih 32 i poslednja reč) su upravljački znakovi, koji se ne mogu štampati, nego upravljaju izlaznim uređajima (na primer kod 10 pravi „novi red"). Na preostala mesta su stavljeni znakovi koji se mogu štampati: mala i velika slova latinske abecede, brojevi i znakovi. U tabeli je dat ASCII kod.

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	nul	soh	stx	etx	eot	enq	ack	bel	bs	ht	lf	vt	ff	cr	so	si
1	dle	dc1	dc2	dc3	dc4	nak	syn	etb	can	em	sub	esc	fs	gs	rs	us
2		!	"	#	$	%	&	'	(	)	*	+	,	-	.	/
3	0	1	2	3	4	5	6	7	8	9	:	;	<	=	>	?
4	@	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
5	P	Q	R	S	T	U	V	W	X	Y	Z	[	\	]	^	_
6	`	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o
7	p	q	r	s	t	u	v	w	x	y	z	{	|	}	~	del

Tablica se koristi tako da prvo čitamo u kom redu je kodna reč, to prepišemo u binarnom zapisu sa 4 bita, a posle čitamo u kojoj je koloni (kolone A, B, C, D, E i F redom odgovaraju binarnom zapisu brojeva 11, 12, 13, 14 i 15), i to takođe prevodimo u binarni zapis sa 4 bita. Na primer, slovo N je u 4. redu, to je u binarnom kodiranju 0100, i nalazi se u 14. koloni (kolona E), to je 1110. Dakle, u ASCII kodu slovo N je 01001110.

UTF-8 (8-bit Unicode Transformation Format) je razvijenija verzija ASCII koda, koji se i danas koristi za kodiranje alfabeta na primer kod Microsoft Windos i Linux. On je sa promenljivom dužinom kodnih reči. Kodna reč iz ASCII koda kodira se sa 8 bit=1 bajt. Te kodne reči uvek počinju sa 0. Ostale simbole UTF-8 kod kodira sa više bajtova tako da prvi bajt počinje sa onoliko jedinica sa koliko bajtova se kodira dati simbol, a svaki sledeći bajt počinje sa 10.

□

Definicija 3.5. Kod V je **prefiksni kod** ako ne postoji takva kodna reč koja je prefiks neke druge kodne reči.

Primer 3.5. a) Morzeov kod nije prefiksni kod, na primer slovo K je „-.-", a to je prefiks kodne reči C i Y.

b) Kod $V = \{0,1,20,21,220,221\}$ je prefiksni.

c) bilo koji blok kod je prefiksni (jer u suprotnom imali bismo jednake kodne reči ili bi postojala bar jedna kodna reč koja ima različite dužine od ostalih.)

□

Prefiksni kodovi su važni pošto oni omogućuju jednoznačno dekodiranje kao što se vidi u sledećem tvrđenju.

Teorema 3.1. *Prefiksni kod omogućuje jednoznačno dekodiranje.*

Dokaz: Pretpostavimo suprotno, neka je x reč koju možemo dekodirati na bar dva načina:

$$x = v_{i_1} \dots v_{i_k} = v_{j_1} \dots v_{j_m},$$

gde su $v_{i_1}, \dots, v_{i_k}, v_{j_1}, \dots, v_{j_m} \epsilon V$.

Pošto dekodiranje nije jednoznačno, postoji bar jedan par v_{i_l} i v_{j_n} gde važi

$$|v_{i_l}| < \left|v_{j_n}\right| \;\; ili \;\; |v_{i_l}| > |v_{j_n}|.$$

To znači da je jedna kodna reč prefiks druge, a to je kontradikcija sa pretpostavkom da je kod prefiksni. Dakle, prefiksni kod omogućuje jednoznačno dekodiranje.

■

Primer 3.6. Morzeov kod nije prefiksni kod, ali omogućuje jednoznačno dekodiranje. Posle svakog slova šalje se pauza u poruci. Ako ne bi bilo te pauze, tada se ne bi znalo na primer kako da dekodiramo niz simbola „---“, tj. da li je to „TTT“, „MT“, „TM“ ili „O“.

□

O postojanju prefiksnog koda govori Kraftova nejednakost.

Teorema 3.2. *Neka su dati proizvoljni prirodni brojevi* $n_1, \dots, n_a, b$, $b > 1$. *Postoji prefiksni kod* $V = \{v_1, \dots, v_a\}$ *takav da je baza koda* b *i dužine kodnih reči su* $n_1 = |v_1|$,...,$n_a = |v_a|$ *ako i samo ako je ispunjena Kraftova nejednakost:*

$$\sum_{i=1}^{a} b^{-n_i} \leq 1.$$

Dokaz: ($\Longrightarrow$) Neka je dat prefiksni kod $V = \{v_1, \dots, v_a\}$, $b = |B|$, $n_1 = |v_1|$,...,$n_a = |v_a|$.

Označimo sa n maksimalnu dužinu kodne reči

$$n = \max\{n_1, \dots, n_a\}.$$

Definišimo skup B_{v_i} na sledeći načinin:

$$B_{v_i} = \{x \epsilon B^n : v_i \text{ je prefiks u } x.\}$$

Tada važi da je $B_{v_i} \cap B_{v_j} = \emptyset$, za $i \neq j$, $i, j \epsilon \{1, \dots, a\}$. Ako bi postojala neka reč koja se nalazi u oba skupa, tada bi jedna kodna reč bila

prefiks druge, a ovo je kontradikcija jer je V prefiksni kod. Pored toga, važi

$$\bigcup_{i=1}^{a} B_{v_i} \subseteq B^n,$$

jer smo elemente skupa B_{v_i} izabrali tako da pripadaju skupu B^n.

Pokažimo da je $|B_{v_i}| = b^{n-n_i}$. Znamo da je $|B^n| = b^n$. U svakoj reči prvih n_i elementa čine kodnu reč v_i, a na preostalih $n - n_i$ mesta raspoređuju se elementi iz skupa B.

Zbog gore navedenih osobina $\{B_{v_i}: 0 < i < a + 1\}$ je familija disjunktnih podskupova iz B^n, zato je ispunjeno

$$\sum_{i=1}^{a} |B_{v_i}| = \left| \bigcup_{i=1}^{a} B_{v_i} \right| \leq |B^n|,$$

tj.

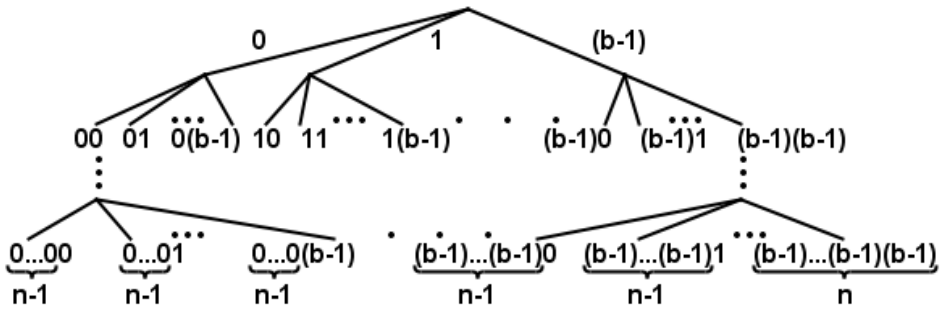
$$\sum_{i=1}^{a} b^{n-n_i} \leq b^n.$$

Ako podelimo nejednakost sa b^n dobićemo Kraftovu nejednakost:

$$\sum_{i=1}^{a} b^{-n_i} \leq 1.$$

($\Longleftarrow$) Neka je sada ispunjena Kraftova nejednakost. Bez umanjenja opštosti pretpostavimo da je $n_1 \leq n_2 \leq \cdots \leq n_a$.

Posmatrajmo kodno drvo, koje ima na poslednjim granama čvorove dužine n_a cifara, gde su cifre uzete iz skupa B. (Slika 6.)



Slika 6.

U prvom redu, dakle imamo b različitih reči sa 1 cifrom, u drugom b^2 dvocifrenih, i tako dalje do zadnjeg reda, gde se nalazi ukupno b^{n_a} reči koje su dužine n_a.

Kodne reči biramo na sledeći način: Prva kodna reč v_1, treba da ima kodnu dužinu n_1, zato sa kodnog drveta uzmemo prvi čvor sa leve

strane koji ima n_1 cifru. Sve ostale čvorove koji se nalaze ispod čvora v_1 brišemo. Na taj način ćemo obezbediti da v_1 ne bude prefiks nijedne reči u novom kodnom drvetu. Prilikom brisanja čvorova, obrisali smo b^{n-n_1} čvorova dužine n.

Za drugu kodnu reč v_2 ponovo izaberemo sledeći čvor sa kodnog drveta tako da on bude prvi sa leve strane koji ima n_2 cifara i razlikuje se od v_1. Ponovo brišemo sve čvorove koji izlaze iz v_2. Prilikom brisanja čvorova, obrisali smo b^{n-n_2} čvorova dužine n.

Postupak ponavljamo a puta i dobijamo prefiksni kod $V = \{v_1, \dots, v_a\}$.

Sve ostale čvorove koji su desno od v_a i nismo koristili brišemo.

Postavlja se pitanje da li imamo dovoljno čvorova kod kodnog drveta? Odgovor je da, pošto smo pretpostavili da važi Kraftova nejednakost i obrisali smo ukupno

$$b^{n-n_1} + b^{n-n_2} + \cdots + b^{n-n_a}$$

čvorova dužine n.

■

Kada govorimo o kanalu bez smetnji jedan bitan faktor je tzv. prosečna dužina kodnih reči, što meri efikasnost dekodiranja.

Definicija 3.6. Izvor informacije nad alfabetom $A = \{a_1, \dots, a_m\}$ je uređen par $(A, \mathcal{P})$, gde je $\mathcal{P} = \{A^n, p(a_1, \dots, a_n)\}$, za sve $n \in \mathbb{N}$.

Definicija 3.7. Entropija stacionarnog izvora A je

$$H(A) = \lim_{n\to\infty} \frac{H(A^n)}{n},$$

gde je $H(A^n) = -\sum_{(a_1,\dots,a_n)\in A^n} p(a_1, \dots, a_n) \log p(a_1, \dots, a_n)$.

Može se pokazati da svaki stacionaran izvor ima konačnu entropiju. Ako imamo da je A stacionaran izvor bez memorije. tada je entropija izvora A jednaka sa $H(A)$.

Definicija 3.8. Neka je dat izvor (A, P) i kod $V = f(A)$, pri čemu je $A = \{\alpha_1, \dots, \alpha_a\}$, $P = \{p_1, \dots, p_a\}$, raspodela verovatnoće, gde je $p_i = p(\alpha_i)$. Obeležimo sa $n_i = |\alpha_i|$ dužinu kodnih reči. Tada je **prosečna dužina kodnih reči**

$$\overline{n}_V = \sum_{i=1}^{a} p_i n_i.$$

Napomena: Prosečne dužine kodnih reči možemo uporediti ako razni kodovi imaju istu bazu koda. U opštem slučaju, što je veća baza koda, možemo formirati manju prosečnu dužinu kodnih reči.

Primer 3.7. Neka je dat $A = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4, \alpha_5\}$ i raspodela verovatnoća je $p_1 = 0.5$, $p_2 = 0.2$, $p_3 = 0.1$, $p_4 = 0.1$ i $p_5 = 0.1$. Dati su $V = \{0,10,110,1110,1111\}$ i $W = \{00,01,10,110,111\}$ dva binarna koda za izvor A. U tabeli su dati odgovarajuće dužine kodnih reči.

α_i	p_i	v	$n_i(v)$	w	$n_i(w)$
α_1	0.5	0	1	00	2
α_2	0.2	10	2	01	2
α_3	0.1	110	3	10	2
α_4	0.1	1110	4	110	3
α_5	0.1	1111	4	111	3

Po datoj formuli prosečne dužine kodnih reči su $\bar{n}_V = 2$ i $\bar{n}_W = 2{,}2$.

□

Sledeća dva tvrđenja određuju granice u kojima se kreće $\bar{n}_V$. Prvo posmatramo teoremu za donju granicu.

Teorema 3.3. *Neka je dat izvor (A, P) i baza koda b. Tada za svaki $V = f(A)$ koji omogućuje jednoznačno dekodiranje važi:*

$$\bar{n}_V \geq \frac{H(A)}{\log b},$$

gde je $H(A) = -\sum_{i=1}^{a} p_i \log p_i$ entropija izvora.

Dokaz: Znamo da važi $\sum p_i = 1$ i takođe znamo da zbog Kraftove nejednakost važi $\sum_{i=1}^{a} b^{-n_i} \leq 1$. Zadovoljene su pretpostavke Leme 1.2. (za q_i uzmemo $q_i = b^{-n_i}, i = 1, \ldots, a$), odnosno

$$\sum_{i=1}^{a} b^{-n_i} \leq \sum_{i=1}^{a} p_i,$$

pa prema lemi dobijamo

$$-\sum_{i=1}^{a} p_i \log b^{-n_i} \geq -\sum_{i=1}^{a} p_i \log p_i.$$

Pošto je

$$-\sum_{i=1}^{a} p_i \log p_i = H(A),$$

i

$$-\sum_{i=1}^{a} p_i \log b^{-n_i} = \sum_{i=1}^{a} p_i\, n_i \log b = \log b\, \bar{n}_V,$$

zato dobijamo

$$H(A) \leq \bar{n}_V \log b,$$

odnosno

$$\overline{n}_V \geq \frac{H(A)}{\log b}.$$

■

Napomena: Najmanja vrednost koju možemo dobiti za $\overline{n}_V$ je dakle $\overline{n}_V = \frac{H(A)}{\log b}$, koju dostižemo ako i samo ako je $p_i = b^{-n_i}, i = 1, \dots, a$. To znači da će $\overline{n}_V$ dostići navedenu donju granicu jedino ako se raspodela verovatnoće izvora sastoji od celobrojnih stepeni baze koda b.

Sledeće tvrđenje pokazuje da uvek možemo posmatrati prefiksni kod s kojim ćemo se dovoljno dobro približiti donjoj granici prosečne dužine kodnih reči.

Teorema 3.4. *Neka je dat izvor* (A, P) *i baza koda* b. *Tada postoji prefiksni kod* $V = f(A)$ *za koji je*

$$\overline{n}_V < \frac{H(A)}{log\, b} + 1.$$

Dokaz: Neka su $n_1, \dots, n_a$ prirodni brojevi takvi da

$$b^{-n_i} \leq p_i < b^{-n_i+1}, i = 1, \dots, a.$$

Sumiramo gornju nejednakost po i i iz leve strane dobijamo

$$\sum_{i=1}^{a} b^{-n_i} \leq \sum_{i=1}^{a} p_i = 1,$$

odnosno zadovoljena je Kraftova nejednakost, pa iz Teoreme 3.2. sledi da postoji prefiksni kod na datom izvoru (A, P) sa bazom koda b tako da su dužine kodnih reči $n_1, \dots, n_a$.

Sa druge strane imamo nejednakost

$$p_i < b^{-n_i+1}, i = 1, \dots, a.$$

Ako logaritmujemo izraz i pomnožimo sa p_i dobijamo

$$p_i \log p_i < p_i \log b^{-n_i+1}.$$

Sumiramo izraz po i

$$\sum_{i=1}^{a} p_i \log p_i < \sum_{i=1}^{a} (-n_i p_i + p_i) \log b,$$

$$-\frac{H(A)}{\log b} < \sum_{i=1}^{a} (-n_i p_i) + 1,$$

odnosno

$$\frac{H(A)}{\log b} > \bar{n}_V - 1.$$

■

4. Kodiranje u kanalu sa smetnjama. Blok-kod

Prelazimo na kodiranje sa smetnjama. U ovom poglavlju ćemo se osvrnuti na to, da li se desila greška u kodiranju. Za ispravljanje grešaka postoje raznovrsni kodovi, a najpoznatija klasa je blok-kod. U teoriji kodiranja blok-kodovi su veoma bitni pošto se u praksi koriste na puno mesta. Posebna klasa blok-kodova koja ima široku primenu, su linearni kodovi s kojima ćemo se kasnije baviti.

4.1. Definicija i osnovni pojmovi

Definicija 4.1. Neka su dati konačni skupovi $A = \{\alpha_1, \dots, \alpha_a\}$ i $B = \{\beta_1, \dots, \beta_b\}$, A je alfabet izvora, B je alfabet koda, $b = |B|$ je baza koda. Svako $1-1$ preslikavanje $f: A \to B^n$, $V = f(A) \subseteq B^n$ je **blok-kod** sa dužinom kodnih reči n, a broj $a = |A|$ je **kardinalnost** blok-koda.

Napomena: U nastavku rada analiziramo samo stacionarne kanale bez memorije.

Da bi postojao blok-kod $V \subseteq B^n$ za dati alfabet izvora i alfabet koda treba da bude zadovoljeno sledeće tvrđenje.

Teorema 4.1. *Za date brojeve* $a, b, n \in \mathbb{N}$ *postoji blok-kod* $V = f(A) \subseteq B^n$ *sa bazom koda* b *i kardinalnosti* a *ako i samo ako je*

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

Dokaz: Broj kodnih reči ne može biti veći od ukupnog broja reči nad B^n, tj.

$$a \leq b^n.$$

Logaritmujemo nejednakost da izrazimo n i dobijamo traženu nejednakost $n \geq \frac{\log a}{\log b}$.

■

Neka su $c = (c_1, \dots, c_n)$ i $d = (d_1, \dots, d_n)$ reči dužine n. Verovatnoća da se reč d pojavi na izlazu, ako je na ulazu primljena reč c je

$$p(d|c) = \prod_{i=1}^{n} p(d_i|c_i),$$

ili možemo napisati tu verovatnoću za BSC kanal i na sledeći način:

$$p(d|c) = p^e(1-p)^{n-e},$$

gde je e broj mesta gde se c i d razlikuju.

Pretpostavimo da je kodna reč poslata preko kanala i da je stigla reč x. Ako je x kodna reč pretpostavljamo da nemamo grešku, a ako x nije kodna reč tada treba ispraviti grešku. Jedna mogućnost je tzv. dekodiranje maksimalne verodostojnosti (MLD metoda-maximum likelihood decoding) koja uzima onu kodnu reč v_x čija je verovatnoća najveća da je prihvaćena reč x:

$$P(x|v_x) = \max_{v \in V} P(x|v).$$

Napomena: Pod greškom se uvek podrazumeva samo zamena simbola, a ne ispadanje ili umetanje simbola.

Primer 4.1. MLD ne mora da određuje kodnu reč jedinstveno. Na primer ako imamo $V = \{00,11\}$ i prihvaćena je reč $x = 01$ i neka je verovatnoća greške $p = 0.1$ tada je

$$P(01|00) = 0.9 \cdot 0.1 = 0.09,$$

$$P(01|11) = 0.1 \cdot 0.9 = 0.09.$$

□

Uvodimo binarne operacije $+$ i $\cdot$ na skupu $\{0,1\}$:

$+$	0	1
0	0	1
1	1	0

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

$(\{0,1\}, +, \cdot)$ je polje, koje označavamo sa F_2.

Operacija $+$ se može proširiti na skup $\{0,1\}^n$: $x, y \in \{0,1\}^n$, $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n)$ na sledeći način

$$x + y = (x_1 + y_1, \dots, x_n + y_n).$$

Definišimo operaciju $\cdot : \{0,1\} \times \{0,1\}^n \longrightarrow \{0,1\}^n$ na sledeći način: $a \in \{0,1\}, x \in \{0,1\}^n$

$$a \cdot x = (a \cdot x_1, \dots, a \cdot x_n),$$

ili drugačije

$$a \cdot x = \begin{cases} (0, \dots, 0), & a = 0 \\ x, & a = 1 \end{cases}.$$

Gore navedene operacije su date nad F_2.

Definicija 4.2. Nad $\mathbb{Z}_q = \{0,1, \dots q-1\}$, definišimo binarne operacije sabiranje $+$ i množenje $\cdot$, za svaki $a, b \in \mathbb{Z}_q$ tako da

$$a + b = (a + b) \mathrm{mod} q,$$

i

$$a \cdot b = (a \cdot b) \mathrm{mod} q.$$

Napomena: Za q prost broj ćemo $\mathbb{Z}_q$ obelezavati sa F_q. Koristićemo iste oznake i u F_q, ali one neće stvarati konfuziju u nastavku.

$(\mathbb{Z}_q, +, \cdot)$ je prsten.

Definicija 4.3. Norma vektora je unarno preslikavanje $\| \ \|: \{0,1\}^n \longrightarrow \mathbb{N}_0$ tako da za $x \in \{0,1\}^n$ je:

$$\|x\| = \sum_{i=1}^{n} x_i.$$

Definicija 4.4. Hemingovo rastojanje je binarno preslikavanje $d(\ ,\ ): \{0,1\}^n \times \{0,1\}^n \longrightarrow \mathbb{N}_0$ definisano za $x, y \in \{0,1\}^n$ na sledeći način

$$d(x,y) = \|x + y\| = \sum_{i=1}^{n} x_i + y_i.$$

Pojam Hemingovog rastojanja možemo uopštiti za bilo koji alfabet B. Najčešće dokaze tvrđenja ćemo izvoditi za $|B| = 2$, ali će važiti za proizvoljno $|B| > 2$. Pored toga u Primeru 4.3. navodimo kodove definisane nad B, gde je $|B|$ različito od 2.

Definicija 4.5. Hemingovo rastojanje između reči x i y nad alfabetom B (dužine reči je n) je broj koordinata na kojima se ti vektori razlikuju:

$$d(x,y) = d(x_1, y_1) + d(x_2, y_2) + \cdots + d(x_n, y_n),$$

gde vrednosti $d(x_i, y_i)$ dobijemo na sledeći način:

$$d(x_i, y_i) = \begin{cases} 1, x_i = y_i \\ 0, x_i \neq y_i \end{cases}.$$

Kako smo definisali Hemingovo rastojanje za bilo koji alfabet B, slično se može definisati i norma vektora za $|B| > 2$.

Definicija 4.6. Neka je data proizvoljna reč x iz skupa B^n **Norma vektora** x je broj nenula koordinata u reči, tj.

$$\|x\| = d(x, 0).$$

Možemo navesti metod koji koristi Hemingovo rastojanje za ispravljanje grešaka. To je metod minimalnog rastojanja (MDD-minimum distance decoding). Kao što smo već napomenili, možemo računati verovatnoću da je reč x stigla ako je v poslata kao

$$p(x|v) = p^e (1-p)^{n-e},$$

gde je $p < 0.5$. Ta verovatnoća je veća ako je $n - e$ veće, tj. što je e manje, odnosno što je manje $d(x, v)$. Dakle, reč x dekodiramo kao kodnu reč v_x koja je na minimalnom rastojanju od x

$$d(x, v_x) = \min_{v \in V} d(x, v).$$

Primer 4.2. Neka je $V = \{0000, 0011, 1111\}$. Neka je dobijena reč na izlazu $x = 1100$. x nije kodna reč pa primenimo metod minimalnog rastojanja. Kako je

$$d(1100, 0000) = 2,$$

$$d(1100, 0011) = 4,$$

$$d(1100, 1111) = 2,$$

dobijamo da je $d(x, v_x) = \min_{v \in V} d(x, v) = 2$, tj. ovaj metod ne daje jedinstveno rešenje.

□

Teorema 4.2. *Ako imamo BSC kanal, $p < \frac{1}{2}$, tada su MLD metod i MDD metod ekvivaletni.*

Dokaz: Neka je dat blok-kod $V = \{v_1, \dots, v_n\}$ i $x \in B^n$. Za $i \in \{0, \dots, n\}$ važi

(1) $$d(v, x) = i \iff p(x|v) = p^i (1 - p)^{n-i}.$$

Znamo da važi

$$p^0 (1 - p)^n > p^1 (1 - p)^{n-1} > \cdots > p^n (1 - p)^0,$$

jer je $p < \frac{1}{2}$.

MDD metod dekodira reč x sa v, ako je rastojanje između v i x minimalno, dok MLD metod dekodira x sa kodnom reči v, ako je verovatnoća da je poslat v ako je primljen x maksimalna. Pošto važi (1) MLD i MDD metodi su ekvivalentni.

■

Definicija 4.7. Neka je dat blok-kod V nad B. **Kodno rastojanje** za kod V, u oznaci $d(V)$ ili d je

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

Pomoću kodnog rastojanja utvrdićemo koliko grešaka može kod da ispravlja ili da otkrije.

Definicija 4.8. Prolaskom kroz kanala neka se x transformiše u y, za $x, y \in B^n$. Ako je $y = x - e$, tada vektor e zovemo **vektor greške**.

Neka je dat BSC kanal. Koordinata e_i u vektoru e je 0 sa verovatnoćom $1-p$, tj. u i-toj koordinati nije došlo do greške prilikom transformacije. $e_i = 1$ sa verovatnoćom p, tj. i-ta koordinata se menja.

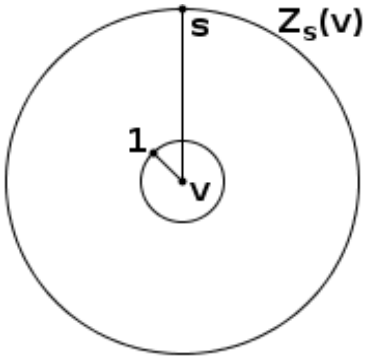
Definicija 4.9. Svako preslikavanje $f: B^n \longrightarrow V$ je jedno **dekodiranje**.

Ako se y razlikuje od x na s mesta, $x, y \in B^n$, tada je $\|e\| = s$ ili $d(x,y) = s$.

Neka je dat blok-kod V, neka je $v \in V$, i $0 \leq s \leq n, s \in \mathbb{N}$. Definišemo skup $Z_s(v)$ kao skup koji sadrži sve reči iz skupa B^n koje možemo dobiti od v usled najviše s grešaka:

$$Z_s(v) = \{x \in B^n : d(x,v) \leq s\}.$$

U metričkom prostoru $Z_s(v)$ je lopta sa centrom u v i poluprečnikom s (Slika 7).



Slika 7.

Definicija 4.10. Kod V **omogućuje ispravljanje s grešaka** ako postoji dekodiranje f tako da je za sve $v \in V$

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

Definicija 4.11. Kod V omogućuje **otkrivanje s grešaka** ako

$$x \in Z_s(v) \implies x \notin V \setminus \{v\}.$$

Sledeće tvrđenje daje potreban i dovoljan uslov za otkrivanje i ispravljanje grešaka.

Teorema 4.3. *Blok-kod V omogućuje:*

i) *ispravljanje s grešaka ako i samo ako $d(V) > 2s$,*

ii) *otkrivanje s grešaka ako i samo ako $d(V) > s$.*

Dokaz: **i)** Neka je dat blok-kod V. Iz definicijne znamo, da on omogućuje ispravljanje s grešaka ako i samo ako su sve lopte $Z_s(v)$ disjunktne, odnosno ako za sve $u, v \in V$, $d(u,v) > 2s$. Zato je po definiciji kodnog rastojanja $d(V) > 2s$.

ii) Analiziranjem koda V u metričkom prostoru primećujemo da u s-okolini kodne reči v ne može biti ni jedna druga kodna reč, tj. za svaki $u \in V, d(u,v) > s$. Po definiciji kodnog rastojanja to je tačno ako i samo ako je $d(V) > s$.

■

Poznat je Hemingov potreban uslov (videti [9], Tvrđenje 3.46.) za postojanje blok-koda $V \subseteq B^n$ kardinalnosti a koji omogućuje ispravljanje s grešaka, i glasi da je zadovoljena sledeća nejednakost:

$$\frac{2^n}{\sum_{i=0}^{s}\binom{n}{i}} \geq a.$$

Primer 4.3. Dva klasična primera blok-koda, koje svakodnevno koristimo, su ISBN kod i barkod. ISBN (International Standard Book Number) kod se koristi za obeležavanje knjiga. Dužina koda je $n = 10$. Prva cifra obeležava jezik na kome je knjiga napisana. Sledeće 3 cifre kodira izdavač knjige. Od 5. do 9. cifre je redni broj knjige kod izdavača. Zadnja cifra je kontrolna cifra, dobijena od gore navedenih 9 cifara, tako da svaku cifru pomnožimo sa rednim brojom cifre, tj prvu cifru sa jedinicom, drugu sa dvojkom, itd. Proizvode saberemo i transformišemo u skup F_{11}, tj. kodiranje se vrši na vektorskom prostoru F_{11}^{10}. Ta cifra će biti kontrolna cifra. Ako je kontrolna cifra 10, obeležićemo sa X. Na primer ako je ISBN knjige 867031024, množimo cifre sa rednim brojevima i sumiramo; $1 \cdot 8 + 2 \cdot 6 + 3 \cdot 7 + 4 \cdot 0 + 5 \cdot 3 + 6 \cdot 1 + 7 \cdot 0 + 8 \cdot 2 + 9 \cdot 4 = 114$, dakle kontrolna cifra je 4. ISBN je nelinearan (definisaće se linearan kod u sledećoj glavi) blok-kod, pomoću koga se mogu otkriti najviše 2 greške, ali se ne može ni jedna ispraviti.

Barkod je vrsta koda koji se može optički čitati sa odgovarajućim uređajima. Najčešće služi za identifikaciju proizvoda. Slično ISBN kodu bar kod ima jednu kontrolnu cifru. Sastoji se od tamnih i svetlih linija, čije su dužine 1, 2, 3 ili 4. Ispod linija kod najčešće sadrži niz brojeva od 13 cifara. Jednu cifru kodiramo sa tamnim i svetlim linijama dužine 7. Ovaj kod omogućuje otkrivanje grešaka i sadrži informacije o proizvodima.

□

5. Linearni kodovi

U praksi najčešće korišteni kodovi su linearni kodovi zbog svojih dobrih osobina. Njih lakše možemo konstruisati i dekodirati. Linearni kodovi su opisani parametrima, koji nam pomažu da lakše vidimo prednosti i mane koda.

5.1. Generišuća i kontrolna matrica

Definicija 5.1. Kod V je **linearni** $(\boldsymbol{n}, \boldsymbol{k})$**-kod** nad F_q ako je V potprostor vektorskog prostora F_q^n, i k je **dimenzija** koda.

Napomena: Konačno polje sa q elemenata obeležavaćemo sa $F_q = \{0,1, \dots, q-1\}$, pri čemu je q prost broj.

Definicija 5.2. Kod je **ortogonalna dopuna (dual)** linearnog (n, k)-koda V nad F_q ako sadrži svako y za koji važi

$$\forall x \in V, x \circ y = 0.$$

Oznaka za ortogonalnu dopunu je $V^{\perp}$.

Primer 5.1. a) Neka je dat linearan $(6,3)$ −kod nad F_2

$$V = \{000000,001101,010011,011110,100110,101011,110101,$$
$$111000\}.$$

Njegova ortogonalna dopuna je

$$V^{\perp} = \{000000,000111,011001,011110,101011,101100,110010,$$
$$110101\}.$$

b) Jedan linearan $(3,2)$-kod nad $F_3 = \{0,1,2\}$ je

$$W = \{000,001,002,100,200,101,102,201,202\}.$$

A njegova ortogonalna dopuna je

$$W^{\perp} = \{000,010,020\}.$$

□

Teorema 5.1. *Ako je V linearan kod nad poljem F_q tada je i njegova ortogonalna dopuna takođe linearan kod.*

Dokaz: Neka je dat linearan kod V i njegova ortogonalna dopuna $V^{\perp}$. Neka su $a \in V$ i $u, v \in V^{\perp}$. Tada važi $a \circ u = 0$ i $a \circ v = 0$, odnosno $a \circ u + a \circ v = 0 + 0 = 0$. Prema osobinama skalarnog proizvoda, važi da je

$$a \circ (u + v) = a \circ u + a \circ v = 0,$$

odnosno $V^{\perp}$ je zatvoren u odnosu na sabiranje vektora.

Neka je $\alpha \in F_q$ jedna konstanta i neka su dati $a \in V$ i $v \in V^{\perp}$. Tada i $\alpha \cdot a \in V$ i važi

$$(\alpha \cdot a) \circ v = \alpha \cdot (a \circ v) = \alpha \cdot 0 = 0.$$

Zbog gore navedene osobine kod $V^{\perp}$ je linearan.

■

Lema 5.2. *Nula vektor* $(0, \dots, 0)$ *(dužina* n*) uvek pripada linearnom* (n, k)*-kodu* V *nad poljem* F_q.

Dokaz: Neka je V linearan (n, k)-kod. Neka je v proizvoljna kodna reč. Pošto je kod linearan svaka linearna kombinacija kodnih reči pripada skupu V, pa i

$$0 \cdot v = (0 \cdot v_1, \dots, 0 \cdot v_n) = (0, \dots, 0) \in V.$$

■

Teorema 5.3. *Kodno rastojanje linearnog koda nad* F_q *je*

$$d(V) = \min_{v \in V, v \neq 0} \|v\|.$$

Dokaz: Kodno rastojanje po definiciji je $d(V) = \min_{u,v \in V, u \neq v} d(u, v)$. Znamo da je $d(u, v) = \|u - v\|$. Zbog zatvorensti skupa V prema $+$ važi osobina i zbog toga što se svaka kodna reč može dobiti kao zbir neke dve zbog Leme 5.2.

■

Primer 5.2. Za linearan (6,3)-kod u Primeru 5.1. kodno rastojanje $d(V) = 3$ jer kodna reč 100110 sadrži 3 jedinice, a ne postoji kodna reč različita od 0 sa manje jedinica. Njegov dual ima kodno rastojanje $d(V^{\perp}) = 3$.

□

Za linearan kod V kažemo da je (n, k, d)-kod, ako je n dužina koda, k dimenzija vektorskog prostora V i d kodno rastojanje koda V.

U svakoj kodnoj reči postoji k informacijskih koordinata, toliko koordinata je potrebno za prenos informacije. Preostalih $n - k$ koordinata su kontrolne koordinate, koje služe za ispravljanje grešaka.

Definicija 5.3. Generišuća matrica G formata $k \times n$ za linearni (n, k)-kod V je ona matrica čije vrste formiraju bazu vektorskog prostora V.

Može se pokazati da je broj elemenata baze ortogonalne dopune jednak razlici n i broja elemenata baze za V, tj. kod $V^{\perp}$ je linearan $(n, n-k)$-kod ([3], Teorema 4.2.4).

Definicija 5.4. Kontrolna matrica H formata $(n-k) \times n$ linearnog (n,k)-koda V je generišuća matrica koda $V^{\perp}$.

Definicija 5.5. Generišuća matrica G je u **standardizovanoj formi** ako ima oblik

$$G = [I_k | X],$$

gde je I_k jedinična matrica formata $k \times k$.

Napomena: Ne postoji uvek generišuća matrica u standardizovanoj formi. Na primer, ako uzmemo kod $V = \{0000,1100,0011,1111\}$, tada moguće generišuće matrice su

$$G_1 = \begin{bmatrix} 1100 \\ 0011 \end{bmatrix}, \qquad G_2 = \begin{bmatrix} 1100 \\ 1111 \end{bmatrix}, \qquad G_3 = \begin{bmatrix} 1111 \\ 0011 \end{bmatrix}.$$

Te matrice se očigledno nikad ne mogu transformisati u standardizovanu formu.

Definicija 5.6. Kontrolna matrica H je u **standardizovanoj formi** ako je

$$H = [Y | I_{n-k}].$$

Pomoću generišuće matrice možemo odrediti linearni (n,k)-kod, jer sve moguće linearne kombinacije vrsta matrice daju kod V. Zbog toga je i dobila ime generišuća matrica. Kontrolna matrica je dobila ime jer pokazuje da li reč pripada kodu V, jer $x \cdot H^{\intercal} = 0$ ako i samo ako je x kodna reč.

Pored toga, važi da

$$H \cdot G^{\intercal} = O,$$

gde je O nula matrica formata $(n-k) \times k$. Tu osobinu dobijamo pošto su G i H generišuće matrice koda V i $V^{\perp}$, redom, a oni su ortogonalni.

Primer 5.3. Možemo definisati generišuću matricu za linearni (6,3)-kod iz Primera 5.1. tako što ćemo izabrati 3 kodne reči, koje su linearno nezavisne. Na primer, tada G može biti

$$G = \begin{bmatrix} 100110 \\ 111000 \\ 010011 \end{bmatrix}.$$

Njegova kontrolna matrica je takva matrica čije su vrste ortogonalne na sve kodne reči koda V, odnosno čine bazu njegove ortogonalne dopune

$$H = \begin{bmatrix} 000111 \\ 101011 \\ 110010 \end{bmatrix}.$$

□

Teorema 5.4. *Ako je generišuća matrica G za kod V u standardizovanoj formi, $G = [I_k|X]$, tada kontrolna matrica za V ima oblik*

$$H = [-X^\intercal|I_{n-k}].$$

Dokaz: Dovoljno je pokazati da je $H \cdot G^\intercal = O$. Iz dimenzije matrice G sledi da je matrica X formata $k \times (n-k)$, i elemente matrice X obeležimo sa x_{ij}.

Neka elemente matrie $H \cdot G^\intercal$ obeležimo sa f_{ij}. Kako je

$$H \cdot G^\intercal = [-X^\intercal|I_{n-k}] \left[\frac{I_k}{X^\intercal}\right],$$

tada je

$$f_{ij} = -x_{i1} \cdot 0 - x_{i2} \cdot 0 - \cdots - x_{ij} \cdot 1 - \cdots - x_{ik} \cdot 0 + 0 \cdot x_{1j} + 0 \cdot x_{2j} + \cdots + 1 \cdot x_{ij} + \cdots + 0 \cdot x_{(n-k)j} = x_{ij} - x_{ij} = 0$$

Dakle, $H \cdot G^\intercal = O$.

■

Teorema 5.5. *Linearni (n,k)-kod nad F_q ima q^k kodnih reči.*

Dokaz: Neka je dat linearni kod V nad F_q. Njegova generišuća matrica G je formata $k \times n$, tj. G se sastoji od k linearno nezavisnih vektora. Obeležimo tih vektori sa $v_1, \ldots, v_k$. Linearnom kombinacijom tih k vektora su takođe kodne reči: $c_1 v_1 + \cdots + c_k v_k \in V$, gde su $c_i \in F_q$, za svaki $i = 1, \ldots, k$. To znači da imamo tačno q mogućnost za izbor svaki c_i, odnosno V ima q^k kodnih reči.

■

5.2. Algoritam za nalaženje generišuće matrice

Neka je dat linearni kod $V = \{v_1, \ldots, v_a\}$ nad F_q. Generišuću matricu određujemo na sledeći način:

1.) Kodne reči stavimo u matricu A

$$A = \begin{bmatrix} v_1 \\ \vdots \\ v_n \end{bmatrix}.$$

2.) A transformišemo u formu

$$A = \begin{bmatrix} I_k & X \\ O_{(a-k)\times k} & O_{(a-k)\times(n-k)} \end{bmatrix},$$

gde O označava nula matricu.

Možemo koristiti sledeće transformacije vrsta:

i) zamena vrsta,

ii) dodavanje jedne vrste drugoj,

iii) množenje vrste nenula skalarom.

Iz generišuće matrice lako se računa kontrolna matrica H pomoću Teoreme 5.4.

Primer 5.4. Već smo izračunali kodne reči za kod V u Primeru 5.3. Sa gore navedenim algoritmom možemo definisati generišuću matricu u standardizovanoj formi. Stavimo u matricu A kodne reči. Zamenimo redove matrice tako da u novoj matrici imamo sledeći redosled redova početne matrice: 53246781. U sledećem koraku transformišemo matricu tako da 4. redu dodamo drugi i treći red, 5. redu dodamo prvi i treći red, 6. redu dodamo prvi i drugi red, a 7. redu dodamo prvi drugi i treći red matrice.

$$A = \begin{bmatrix} 000000 \\ 001101 \\ 010011 \\ 011110 \\ 100110 \\ 101011 \\ 110101 \\ 111000 \end{bmatrix} \sim \begin{bmatrix} 100110 \\ 010011 \\ 001101 \\ 011110 \\ 101011 \\ 110101 \\ 111000 \\ 000000 \end{bmatrix} \sim \begin{bmatrix} 100110 \\ 010011 \\ 001101 \\ 000000 \\ 000000 \\ 000000 \\ 000000 \\ 000000 \end{bmatrix} = \begin{bmatrix} & 10 \\ I_3 & 11 \\ & 01 \\ 0_{5,3} & 0_{5,2} \end{bmatrix}.$$

□

Sledeće tvrđenje pokazuje vezu između kodnog rastojanja i kontrolne matrice koda.

Teorema 5.6. *Neka je dat linearan kod V i njegova kontrolna matrica H. Tada je kodno rastojanje $d(V) = r$, gde je r najmanji broj linearno zavisnih kolona u matrici H.*

Napomena: To znači da svaka linearna kombinacija od $r-1$ kolone je linearno nezavisna, a postoji r kolona matrice H koje su linearno zavisne.

Dokaz: Neka je data kontrolna matrica H za kod V nad F_q. $H = [h_1 \quad \dots \quad h_n]$, gde je h_i kolona matrice H. Neka je v kodna reč iz V, za koju važi da je $d(V) = \|v\| = r$. Dakle v ima minimalnu normu u V. Znamo da važi $vH^{\mathrm{T}} = 0$ ili u matričnom zapisu

$$[v_1 \quad \dots \quad v_n] \begin{bmatrix} h_1 \\ \vdots \\ h_n \end{bmatrix} = 0.$$

Uzmimo nenula koordinate vektora v, $i_1, \dots, i_r$, ima ih ukupno r, i dobijamo

$$v_1 h_1 + \cdots + v_n h_n = v_{i_1} h_{i_1} + \cdots + v_{i_r} h_{i_r} = 0.$$

Iz gornje jednakosti smo dobili linearnu zavisnu kombinaciju kolona matrice H. Za manje od r kolona matrice H dobijamo da su linearno nezavisne, jer smo pretpostavili da je $d(V) = \|v\| = r$, time je teorema dokazana.

■

5.3. Dekodiranje linearnih kodova

U praksi je bitno da dekodiranje bude efikasno, tj. što brže. Pomoću sledeća dva metoda dobijamo jednostavnu šemu za dekodiranje, koju možemo primeniti i za veće dužine kodova.

MDD dekodiranje za linearne kodove možemo opisati pomoću klase. Neka je V linearan (n, k)-kod. Kodna reč v je poslata preko kanala i prihvaćena je reč w. Tada greška e je

$$e = w - v.$$

Kako smo gore definisali klase, to znači da je $e \in w + V$, odnosno e i w pripadaju istoj klasi, i zbog osobine koseta tada $w - e = v \in V$. Zbog korišćenja MDD metode pretpostavimo da je greška e najmanja moguća, zato iz klase $w + V$ izaberemo po normi najmanji e, i w dekodiramo sa kodnom reči $v = w - e$.

Napomena: U BSC kanalu sabiranje i oduzimanje vektora je ista operacija.

5.3.1. Standardni niz

Standardni niz (Standard array – SA) dobijamo na sledeći način:

1.) Prvi red tablica popunjavamo sa kodnim rečima.

2.) U drugi red stavimo ispod nule jednu od reči vektora greške e koja ima minimalnu normu a da se ranije nije već pojavila. Na ostalim mestima ispod svake kodne reči v stavimo reč $v + e$.

3.) Ponavljamo drugi korak sve dok se ne pojavi svih q^n vektora u tablici (q je kardinalnost skupa alfabeta).

Pomoću SA reč w dekodiramo tako da u tablici nađemo u kom redu je reč w, iz tog reda isčitamo lidera e, i w dekodiramo tako da je $v = w - e$.

Primer 5.5. a) Neka je dat linearan $(4,2)$-kod $V = \{0000,0011,1100,1111\}$ nad $F_2 = \{0,1\}$. Primljena je reč $w = 1000$. Da bismo dekodiramo w prvo izračunamo SA tablicu, koja u našem slučaju izgleda na sledeći način:

0000	0011	1100	1111
0001	0010	1101	1110
0100	0111	**1000**	1011
0110	0101	1010	1001

Nađemo reč w u tabeli (treći red, prva kolona), tada je lider $e = 0100$, zato dekodiramo w tako da je

$$v = e + w = 0100 + 1000 = 1100.$$

Međutim u datoj tablici u 3. redu postoji još jedan vektor sa normom 1 (3. red 3. kolona 1000), dakle dekodiranje nije jedinstveno.

b) Neka je dat linearan (3,2)-kod nad poljem $F_3 = \{0,1,2\}$

$$V = \{000,011,022,100,111,122,200,211,222\}.$$

Primljena je reč $w = 002$. Za kod V SA tablica je:

000	011	022	100	111	122	200	211	222
001	012	020	101	112	120	201	212	220
010	021	**002**	110	121	102	210	221	202

Lider za koset, gde se w nalazi je 010, zato w dekodiramo kao

$$v = 002 - 010 = 022.$$

□

5.3.2. Standardni dekodirajući niz

Drugi metod je standardni dekodirajući niz (standard decoding array – SDA). Ako imamo malu dužinu n, tada SA metoda dobro funkcioniše. Ali kada imamo veliko n, treba previše vremena da pređemo po celoj tablici SA. Npr. ako imamo $(256,200)$-kod, to znači da se tablica sastoji od 256 redova i 2^{200} kolona, ali sa strane kodiranja kod ne smatramo velikim. Zbog efikasnosti zato uvodimo novi pojam: korektor.

Neka je V linearni (n,k)-kod nad F_q. H je njegova kontrolna matrica. Neka je w proizvoljan vektor iz vektorskog prostora F_q^n. **Korektor** za vektor w je vektor

$$s(w) = wH^{\mathsf{T}},$$

i $s(w)$ pripada vektorskom prostoru F_q^{n-k}.

Jasno je da je $s(w) = 0$ ako i samo ako je w kodna reč.

Važi da je $s(u) = s(v)$ ako i samo ako u i v pripadaju istoj klasi koda V. Prema teoremi V ima onoliko korektora koliko ima i klasa, a iz osobine klase. sledi da ih ima q^{n-k}. Šta više, svaki vektor iz F_q^{n-k} je korektor.

Tablica koja povezuje svaki lider koseta sa svojim korektorom zove se standardni dekodirajući niz (SDA), a dobijamo je na sledeći način:

1.) izaberemo iz svake klase lidera (vektor sa minimalnom normom), označimo ga sa u

2.) pomoću kontrolne matrice H za svaki lider računamo $s(u) = uH^{\intercal}$.

Napomena: Možemo brže generisati SDA ako znamo kodno rastojanje linearnog koda: za svaki vektor e, za koji važi

$$\|e\| \leq \left\lfloor \frac{d-1}{2} \right\rfloor,$$

(zagrada $\lfloor \ \rfloor$ označava najveći ceo deo broja, a d je kodno rastojanje), biće lider jednog koseta. S tom normom ne moramo da dobijemo sve lidere. U suštini treba da se pojavi svaki vektor dužine q^{n-k} u koloni korektora.

Dekodiranje pomoću SDA vektora w vršimo na sledeći način:

1.) izračunamo korektor za w: $s(w) = wH^{\intercal}$,

2.) iz SDA tablice izaberemo u, za koji važi $s(u) = s(w)$,

3.) dekodiramo sa $v = w - u$.

SDA tablica ima q^{n-k} redova, ali ima samo 2 kolone, dok SA tablica ima q^k kolona i q^{n-k} redova. Sa SDA tablicom možemo brže računati nego sa SA, ali za velike dužine n ta metoda još uvek nije efikasna.

Primer 5. 6. Neka je dat linearan (5,2)-kod $V = \{00000, 01011, 10110, 11101\}$, njegova generišuća matrica je

$$G = \begin{bmatrix} 10110 \\ 01011 \end{bmatrix},$$

pa kontrolnu matricu možemo računati pomoću tvrđenja 5.4.

$$H = \begin{bmatrix} 10100 \\ 11010 \\ 01001 \end{bmatrix}.$$

Pošto je dimenzija matrice $d = 3$, treba da stavimo sve lidere dužine 1 i 0. Tada dobijemo prvih šest redova tabele, fali još sedmi i osmi red, gde su korektori 101 i 111. Te korektore možemo dobiti

pomoću na primer greške 00101 i 10001. Dakle, naša SDA tablica je sledeća:

greška (u)	korektor (uH^{T})
00000	000
00001	001
00010	010
00100	100
01000	011
10000	**110**
00101	101
10001	111

Pretpostavimo da imamo reč $w = 00110$. Računamo $wH^{\mathsf{T}} = [110]$. Iz tablice isčitamo grešku za vektor 110, a to je $e = 10000$.

Dekodiramo w tako da

$$v = w + u = 00110 + 10000 = 10110.$$

□

5.4. Hemingovi kodovi

Specijalna klasa linearnih kodova su Hemingovi kodovi, koji su značajni jer se pomoću njih može lako ispraviti jedna greška. Mi ćemo se baviti samo binarnim Hemingovim kodovima.

Definicija 5.7. Binarni Hemingov kod je linearan kod, čija kontrolna matrica H ima m redova, $m \geq 2$, i njegove kolone se sastoje od brojeva $1, \dots, n$, $n = 2^m - 1$ u binarnom zapisu (nenula elementi polja F_2^m).

Pošto skup F_2^m ima $2^m - 1$ vektora bez nule, to znači da je za Hemingov kod $n = 2^m - 1$, a $k = 2^m - 1 - m$. Kodno rastojanje Hemingovog koda je $d = 3$. Iz Teoreme 5.6. znamo da je kodno rastojanje onoliko koliko kontrolna matrica ima najmanji broj zavisnih kolona. U ovom slučaju je $d > 1$, jer nula vektor ne pripada matrici. $d > 2$ jer su kolone matrice različite. Kodno rastojanje je $d = 3$, jer bilo koje dve kolone ako saberemo ponovo dobijemo vektor iz prostora F_2^m, jer je vektorski prostor zatvoren prema sabiranju.

Teorema 5.7. *Neka je dat Hemingov (n, k)-kod. Svaka reč r iz prostora F_2^n je ili kodna reč ili postoji kodna reč v tako da je rastojanje između v i r jednako 1, $d(v, r) = 1$.*

Dokaz: Znamo da Hemingov (n, k)-kod ima 2^k kodnih reči, i da je kodno rastojanje $d = 3$. U loptama $Z_1(v)$ imamo ukupno $n + 1$ reči. Pošto je $d = 3$, lopte su međusobno disjunktne. Imamo onoliko

disjunktnih lopti koliko i kodnih reči, 2^k. Ukupno u loptama imamo $2^k(n+1)$ reči, odnosno

$$2^k(n+1) = 2^{2^m-1-m}(2^m - 1 + 1) = 2^{2^m-1} = 2^n.$$

To znači da je sa tim loptama pokriven ceo F_2^n.

■

5.4.1. Dekodiranje Hemingovih kodova

Redosled kolona kontrolne matrice ne utiče na osobinu Hemingovog koda, ali ima prednost ako kolone matrice definišemo redom, od najmanjeg ka najvećem broju, od 1 do n u binarnom zapisu, jer tada je dekodiranje jednostavnije.

Kao što smo pokazali, kodno rastojanje Hemingovih kodova je $d = 3$, i zato oni omogućuju ispravljanje jedne greške. Vektor greške obeležimo sa $e_i = 0 \ldots 010 \ldots 0$, gde je na i-tom mestu jedinica, $i = 1, \ldots, n$. Možemo posmatrati kosete $0 + V,\ e_1 + V, \ldots, e_n + V$.

Za datu reč w vektor greške pripada nekom kosetu, recimo $e_i + V$, tj. korektor za nju je $e_i H^{\mathsf{T}}$. Pošto su kolone kontrolne matrice H binarni zapisi brojeva, sledi da je $e_i H^{\mathsf{T}}$ binaran zapis broja i. To znači da u reči w postoji greška na i-toj koordinati.

6. Ciklični kodovi

Kao što smo videli linearni kodovi imaju prednost da se mogu opisati pomoću algebarske strukture, generišućom ili kontrolnom matricom. S time je olakšano kodiranje i dekodiranje. U ovom poglavlju se upoznajemo sa cikličnim kodovima. Oni su specijalna podklasa linearnih kodova. Njihova struktura obezbeđuje efikasnije kodiranje, pošto smo videli da je kodiranje uz pomoć linearnih kodova sa većom dužinom kodnih reči suviše sporo.

6.1. Definicija cikličnog koda

Definicija 6.1. Potprostor W vektorskog prostora F_q^n je **cikličan**, ako za savaki $a = (a_0, a_1, \dots, a_{n-1}) \in W$ sledi da i desno **ciklično pomerenje** vektora a pripada W, tj. $\hat{a} = (a_{n-1}, a_0, \dots, a_{n-2}) \in W$.

Definicija 6.2. Kod V je **cikličan** ako

i) V je linearan kod i

ii) ako je $v \in V$, tada je i desno ciklično pomerenje vektora v $\hat{v} = (v_{n-1}, v_0, \dots, v_{n-2})$ pripada kodu V.

Dalje u radu ćemo podrazumevati jednoznačno pridruživanje vektora polinomima na sledeći način:

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

i često ćemo umesto kodne reči koristiti njen polinomni zapis.

Napomena: Na ovaj način se uopštava izomorfizam između vektorskih prostora F_q^n i $F_q[x]/(x^n - 1)$.

U strukturi $F_q[x]/(x^n - 1)$ možemo smatrati $x^n - 1 \equiv 0 \bmod(x^n - 1)$, tj. ostatak pri deljenju sa $x^n - 1$ je 0. Slično imamo da je $x^n \equiv 1$, $x^{n+1} \equiv x$, i tako dalje.

Desno ciklično pomeranje reči v se može predstaviti polinomom $xv(x)$ jer je

$$xv(x) \equiv v_0 x + v_1 x^2 + \cdots + v_{n-1} x^n - v_{n-1}(x^n - 1) \equiv x(v_0 + v_1 x + \cdots + v_{n-1} x^{n-1}) - v_{n-1}(x^n - 1),$$

jer je $-v_{n-1}(x^n - 1) \equiv 0$. Dakle,

$$xv(x) - v_{n-1}(x^n - 1) \equiv xv(x) \bmod(x^n - 1).$$

Dobili smo da je kod $V \subseteq F_q^n$ cikličan ako i samo ako $v(x) \in V \Longrightarrow xv(x) \bmod(x^n - 1) \in V$. Primetimo pošto je cikličan kod $V \subseteq F_q^n$

linearan, tada svaka konačna linearna kombinacija kodnih reči iz V pripada V, tj

$$\sum_i a_i x^i v(x) \in V,$$

za svaki $v(x) \in V$, $a_i \in F_q$.

Neka je dat cikličan kod V. Sa skupom $V[x]$ označavamo polinomni zapis kodnih reči iz V:

$$V[x] = \{v \in V, v = (v_0, \dots, v_{n-1}), v \mapsto v(x)\}.$$

Napomena: $V[x]$ je vektorski prostor (koji je potprostor od $F[x]/x^n - 1$) izomorfan sa prostorom V (koji je potprostor od F_q^n) pa ponekad elemente skupa V identifikujemo sa polinomima iz skupa $V[x]$. U daljem tekstu umesto $V[x]$ često pišemo samo V.

Primer 6.1. a) $V = \{000,100,010,001\}$ nije cikličan, jer kod nije linearan, npr.

$$100 + 001 = 101 \notin V.$$

b) U svakom F_q^n, $n \geq 3$ imamo četiri trivijalna ciklična koda

1.) $(n, 0)$-kod, koji ima samo jednu kodnu reč dužine n, čiji su elementi nule.

2.) $(n, 1)$-kod se sastoji od kodnih reči $(a, a, \dots, a)$, $a \in F_q$.

3.) $(n, n-1)$-kod, gde su kodne reči $(v_0, \dots, v_{n-1})$ tako da je $\sum_{i=0}^{n-1} v_i = 0$.

4.) (n, n)-kod, to su svi vektori dužine n.

c) $V = \{0000,1100,0110,0011,1001,1010,0101,1111\}$ je cikličan (4,3)-kod čija je generišuća matrica u standardizovanoj formi

$$G = \begin{bmatrix} 1001 \\ 0101 \\ 0011 \end{bmatrix}.$$

□

Teorema 6.1. *Ortogonalna dopuna cikličnog koda je cikličan kod.*

Dokaz: Kod V je linearan pa je i njegova ortogonalna dopuna $V^\perp$ takođe linearna.

Treba još pokazati cilkičnost. Neka $b \in V^\perp$. Pokažimo da $\hat{b} \in V^\perp$, $\hat{b} = (b_{n-1}, b_0, \dots b_{n-2})$,. Za proizvoljno $a \in V$ važi da je $0 = a \circ b$, a odavde sledi da je $0 = \hat{a} \circ \hat{b}$:

$$\begin{aligned} 0 = a \circ b &= a_0 \cdot b_0 + \cdots + a_{n-2} \cdot b_{n-2} + a_{n-1} \cdot b_{n-1} \\ &= a_{n-1} \cdot b_{n-1} + a_0 \cdot b_0 + \cdots + a_{n-2} \cdot b_{n-2} = \hat{a} \circ \hat{b}. \end{aligned}$$

Kako je $\widehat{V} = V$ sledi da $\widehat{b} \in V^{\perp}$.

■

Teorema 6.2. *Kod $V \in F_q^n$ je cikličan ako i samo ako je $V[x]$ ideal u $F_q[x]/(x^n - 1)$.*

Dokaz: ($\Longrightarrow$) Neka je V cikličan kod. Po definiciji to znači da

i) Za $a, b \in V$ važi $a + b \in V$. Prema tome iz $a(x), b(x) \in V[x]$ sledi $a(x) + b(x) \in V[x]$.

ii) Iz $a \in V$ sledi $\widehat{a} \in V$. Prema tome važi $a(x) \in V[x] \Longrightarrow xa(x) \in V[x]$.

Iz gore navedene osobine sledi da je $V[x]$ ideal.

($\Longleftarrow$) Sada pretpostavimo da je $V[x]$ ideal u $F_q[x]/(x^n - 1)$. To po definiciji ideala znači da važi sledeće dve osobine:

i) Ako je $a(x), b(x) \in V[x]$ tada $a(x) + b(x) \in V[x]$ – ova osobina odgovara linearnosti koda.

ii) Iz $a(x) \in V[x]$ sledi $xa(x) \in V[x]$. Ta osobina odgovara cikličnosti.

Dakle, kod V je cikličan.

■

Teorema 6.3. *Svaki cikličan kod V sadrži polinom $g(x)$ koji ima minimalan stepen i važi da je $V = \langle g(x) \rangle$.*

Dokaz: Dokaz sledi neposredno iz Teoreme 6.2. i iz dokaza Teoreme 1.4.

■

Teorema 6.4. *Za svaki cikličan kod V iz F_q^n postoji jedinstveni normirani polinom $g(x) \in V$ sa minimalnim stepenom tako da je $V = \langle g(x) \rangle$.*

Dokaz: U prethodnoj teoremi smo pokazali da postoji polinom sa minimalnim stepenom. Treba još pokazati da je minimalni normirani polinom jedinstven. Pretpostavimo suprotno, da postoji $g(x)$ i $h(x)$ dva normalizovana polinoma sa minimalnim stepenom. Razlika polinoma $g(x) - h(x)$ pripada skupu V, jer je V linearan kod. Pošto su $g(x)$ i $h(x)$ normirani i imaju isti stepen, sledi da njihova razlika ima manji stepen. To je kontradikcija sa pretpostavkom, da $g(x)$ i $h(x)$ imaju minimalni stepen, s time je jedinstvenost dokazana.

■

Definicija 6.3. U prethodnoj teoremi navedeni minimalani normirani polinom $g(x)$ iz V sa minimalnim setpenom, nazivamo **generišući polinom** koda V.

Primer 6.2. Neka je dat kod $V = \{0000,1100, 0110,0011,1001,1010,0101,1111\}$. Za ovaj kod generišući polinom je

$$g(x) = 1 + x.$$

□

Teorema 6.5. *Neka je $g(x)$ generišući polinom cikličnog koda $V \subseteq F_q^n$, tada je $g(x)$ delitelj polinoma $x^n - 1$.*

Dokaz: Neka je dat kod V i njegov generišući polinom $g(x)$. Napišimo $x^n - 1$ pomoću $g(x)$:

$$x^n - 1 = q(x)g(x) + r(x),$$

$deg(r(x)) < \deg(g(x))$. Delimo jednakost sa $x^n - 1$ i gledamo ostatak

$$0 = g(x)q(x) + r(x) \bmod (x^n - 1).$$

Znamo da $g(x)q(x) \bmod (x^n - 1)$ pripada kodu V zbog cikličnosti, pa i $r(x)$ pripada kodu V. Pošto je $g(x)$ generišući polinom koda V, sledi da je $r(x) = 0$. To znači da je

$$x^n - 1 = q(x)g(x),$$

dakle, $g(x)$ je delitelj polinoma $x^n - 1$.

■

Teorema 6.6. *Neka je dat q-aran cikličan kod V dužine n i njegov generišući polinom $g(x)$. Ako je stepen polinoma $g(x)$ $n - k$, tada je dimenzija koda k.*

Dokaz: Kodne reči imaju dužinu n, i njihov oblik je $v(x) = g(x)m(x)$, gde je $m(x)$ polinom stepena manjeg od k, $m(x) = m_0 + m_1x + \cdots + m_{k-1}x^{k-1}$. Tako je i dimenzija koda k jer pomoću polinoma $m(x)$ može se napisati tačno q^k različitih polinoma.

■

Kao i kod linearnih kodova, možemo definisati generišuću matricu i za ciklične kodove. Pošto je cikličan kod potpuno određen sa njegovim generišućim polinomom, taj polinom nam takođe pomaže da odredimo generišuću matricu.

Teorema 6.7. *Neka je dat generišući polinom cikličnog (n, k)-koda $V \subseteq F_q^n$: $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$. Tada je generišuća matrica koda V je*

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

Dokaz: Iz prethodne teoreme znamo da je dimenzija koda k. Matrica G se sastoji od k linearno nezavisnih redova, dakle G je generišuća matrica.

■

Pomoću generišućeg polinoma možemo definisati i kontrolni polinom.

Definicija 6.4. Neka je V cikličan (n, k)-kod sa generišućim polinomom $g(x)$. **Kontrolni polinom** koda V je normirani polinom

$$h(x) = \frac{(x^n - 1)}{g(x)}.$$

Napomena: Imamo da je $g(x)h(x) = (x^n - 1)$, gde je $g(x) = g_0 + g_1x + \cdots + g_{n-k}x^{n-k}$ i $h(x) = h_0 + h_1x + \cdots + h_kx^k$. Ako se kodiranje dešava nad poljem F_2 onda je $g_0 = h_0 = g_{n-k} = h_k = 1$. U svim ostalim slučajevima ne znamo sigurno koliki su ti koeficijenti zbog osobina množenja nad poljem F_q, jer jedinicu možemo dobiti tako da $1 \cdot 1 = 1$ i $((q-1) \cdot (q-1)) \text{mod} q = 1$.

Teorema 6.8. *Neka je $h(x)$ kontrolni polinom cikličnog (n, k)-koda V, tada je matrica*

$$H = \begin{bmatrix} \tilde{h}(x) \\ \vdots \\ x^{n-k-1}\tilde{h}(x) \end{bmatrix} = \begin{bmatrix} h_k & h_{k-1} & \cdots & h_0 & 0 & 0 & \cdots & 0 \\ 0 & h_k & \cdots & h_1 & h_0 & 0 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 0 & h_k & h_{k-1} & \cdots & h_0 \end{bmatrix}$$

kontrolna matrica koda V, gde je $\tilde{h}(x) = h_k + h_{k-1}x + \cdots + h_0x^k$.

Dokaz: Matrica H se sastoji od $n - k$ linearno nezavisnih redova. Treba još pokazati da je $H \cdot G^\intercal = O$.

Imamo

$$H \cdot G^\intercal = \begin{bmatrix} \tilde{h}(x) \\ \vdots \\ x^{n-k-1}\tilde{h}(x) \end{bmatrix} [g(x) \quad \cdots \quad x^{k-1}g(x)].$$

Neka su a_{ij} elementi matrice $H \cdot G^\intercal$, tada

$$a_{ij} = x^{k+i-j}h(x)g(x) = x^{k+i-j}\frac{(x^n - 1)}{g(x)}g(x) = x^{k+i-j}(x^n - 1),$$

gde su $i \in \{0, \dots, n-k-1\}, j \in \{0, \dots, k-1\}$. Pošto stepen x^{k+i-j} ide od 1 do $n-1$, dobijemo da je $a_{ij} = 0$ za svaki i i j. Odnosno H je kontrolna matrica.

■

Primer 6.3. Za kod V koji smo dali u Primeru 6.2. dobili smo da je $g(x) = 1 + x$. Odavde sledi da je generišuća matrica koju dobijamo pomoću generišućeg polinoma

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ x^2 g(x) \end{bmatrix} = \begin{bmatrix} 1100 \\ 0110 \\ 0011 \end{bmatrix},$$

koja nije u standardizovanoj formi, ali pomoću tranformacije vrsta možemo dobiti standardizovanu formu. Kontrolni polinom izračunavamo pomoću generišućeg polinoma:

$$h(x) = \frac{(x^4 - 1)}{g(x)} = 1 + x + x^2 + x^3.$$

Dakle, kontrolna matrica koda je

$$H = [1111].$$

□

6.2. Dekodiranje cikličnih kodova

Teorema 6.9. *Neka je dat cikličan kod V, njegov generišući polinom $g(x)$ i kontrolna matrica $H = [I_{n-k}|A]$. Tada korektor reči $w \in F_q^n$ je $w(x) \bmod g(x)$.*

Dokaz: Obeležimo kolone matrice A sa $a_i(x), \deg(a_i(x)) \leq n - k - 1$, tj.

$$A = [a_0(x)|a_1(x)| \dots |a_{k-1}(x)].$$

Znamo iz Teoreme 5.4. da generišuća matrica za V je $G = [-A^{\mathrm{T}}|I_k]$, odnosno

$$G = \begin{bmatrix} -a_0(x) & \\ -a_1(x) & \\ \vdots & I_k \\ -a_{k-1}(x) & \end{bmatrix}.$$

To znači da i-ti red matrice u polinomnom zapisu je $x^{n-k+i} - a_i(x)$ (polinom x^{n-k+i} dodajemo zbog identične matrice). Pošto polinom $x^{n-k+i} - a_i(x)$ odgovara i-toj vrsti generišuće matrice, to znači da je taj polinom kodna reč, pa ga možemo izraziti pomoću generišućeg polinoma:

$$x^{n-k+i} - a_i(x) = q_i(x)g(x),$$

gde je $q_i(x) \in F_q[x]/(x^k - 1)$. Možemo izraziti $a_i(x)$

$$a_i(x) = x^{n-k+i} - q_i(x)g(x).$$

Posmatrajmo reč $w \in F_q^n$, $w(x) = w_0 + w_1x + \cdots + w_{n-1}x^{n-1}$. Korektor reči w je

$$s(w) = wH^{\intercal}.$$

Ili u polinomnom zapisu

$$s(w) = w(x)[I_{n-k}|A]^{\intercal} =$$

$$= w_0 + w_1x + \cdots + w_{n-k-1}x^{n-k-1} + w_{n-k}a_0(x) + \cdots + w_{n-1}a_{n-1}(x)$$

$$= \sum_{i=0}^{n-k-1} w_i x^i + \sum_{j=0}^{k-1} w_{n-k+j}\left(x^{n-k+j} - q_j(x)g(x)\right)$$

$$= \sum_{i=0}^{n-k-1} w_i x^i + \sum_{j=0}^{k-1} w_{n-k+j}x^{n-k+j} - \sum_{j=0}^{k-1} w_{n-k+j}\, q_j(x)g(x)$$

$$= \sum_{i=0}^{n-1} w_i x^i - \sum_{j=0}^{k-1} w_{n-k+j}q_j(x)g(x)$$

Delimo izraz sa $g(x)$ i dobijemo

$$s(w) \equiv w(x) \bmod g(x).$$

■

Definicija 6.5. Ciklična cirkulacija 0 dužine l n-torke je vektor koji sadrži ciklično uzastopno 0 na l koordinata.

Primer 6.4. Reč 10010000001 ima cikličnu cirkulaciju 0 dužine 6. Reč 00012210100200 ima cikličnu cirkulaciju 0 dužine 5.

□

6.2.1. Algoritam za dekodiranje cikličnih kodova

Neka je dat cikličan (n, k)-kod sa generišućom matricom $g(x)$ i kodnim rastojenjem d. Reč $w(x)$ je primljena na izlazu. Neka je vektor greške $e(x)$, koji ima cikličnu cirkulaciju 0 dužine barem k, i čija je norma $\|e\| \leq \left\lfloor \frac{d-1}{2} \right\rfloor$.

Algoritam sastoji se od sledeća tri koraka:

1.) Izračunamo korektore $s_i(x) = x^i w(x) \bmod g(x)$ za $i = 0,1,2, \ldots.$, dok ne nađemo korektor $s_m(x)$ za koji važi

$$\|s_m\,(x)\| \leq \left\lfloor \frac{d-1}{2} \right\rfloor.$$

2.) Računamo grešku za $w(x)$ tako da je

$$e(x) = \left(x^{n-m} s_m(x)\right) \mathrm{mod}(x^n - 1).$$

3.) Dekodiramo $w(x)$ tako da je

$$v(x) = w(x) - e(x).$$

Teorema 6.10. *Gore naveden algoritam je dobro definisan.*

Dokaz: Prvo pokažimo da postoji $m \geq 0$ tako da je $\|s_m\,(x)\| \leq \left\lfloor \frac{d-1}{2} \right\rfloor$.

Pretpostavili smo da $e(x)$ ima cikličnu cirkulaciju 0 veću ili jednaku od k. To znači da postoji m takav da m desnih cikličnih pomeranja reči $e(x)$ pomera svaku nenula koordinatu na prvih $n-k$ koordinata. m cikličnih pomerenja su

$$x^m e(x) \mathrm{mod}(x^n - 1) = (x^m w(x) \mathrm{mod}(x^n - 1)) \mathrm{mod} g(x).$$

Norma vektora $x^m e(x)$ je isto što i norma vektora $e(x)$, zato $\|x^m e(x)\| \leq \left\lfloor \frac{d-1}{2} \right\rfloor$, dakle postoji $m \geq 0$ tako da je

$$\|s_m\,(x)\| = \|x^m e(x)\| = \|e(x)\| \leq \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Posmatramo $n-m$ ciklično pomeranje reči $s_m\, 00 \ldots 00 \in F_q^n$ (gde je $s_m \in F_q^{n-k}$), koju ćemo obeležiti sa $t(x)$, tj.

$$t(x) = x^{n-m} s_m(x) \mathrm{mod}(x^n - 1).$$

Znamo da važi

$$\|t(x)\| = \|x^{n-m} s_m(x)\| \leq \left\lfloor \frac{d-1}{2} \right\rfloor.$$

Posmatramo razliku

$$x^m\big(w(x) - t(x)\big) \equiv x^m\big(w(x) - x^{n-m} s_m(x)\big) \equiv x^m w(x) - x^n s_m(x) \equiv$$
$$(1 - x^n) s_m(x) \equiv 0 \mathrm{mod} g(x)$$

i znamo da jedini zajednički delitelj $g(x)$-a i x^m-a je 1 (jer u polinomu $g(x)$ prvi koeficijent je $g_0 = 1$), dakle $w(x) - t(x)$ je deljiv sa $g(x)$, a to znači da je $w(x) - t(x)$ kodna reč. Pošto $t(x)$ i $e(x)$ imaju istu normu i važi da je $\|t(x) - e(x)\| \leq \|t(x)\| + \|e(x)\|$, onda je norma vektora $t(x) - e(x)$ manja od d. Kako vektor $t(x) - e(x)$ pripada $V[x]$, i jedini vektor iz V koji ima normu manju od d je nula vektor, sledi da je $t(x) = e(x)$. Odnosno

$$e(x) = t(x) = x^{n-m} s_m(x) \mathrm{mod}(x^n - 1).$$

■

Primer 6.5. Neka je dat cikličan (7,4,3)-kod, generišući polinom je $g(x) = 1 + x^2 + x^3$, i data je reč $w = 0101001$. Napravimo odgovarajući polinom $w(x) = x + x^3 + x^6$. Prvi korak je da izračunamo korektore $s_i(x) = x^i w(x) \mathrm{mod} g(x)$ sve dok norma nije manja ili jednaka od 1. Za $i = 0$ već dobijamo da je $w(x) \mathrm{mod} g(x) = 1$. m=0 i $s_0(x) = 1$. U drugom koraku bi bilo $e(x) = x^n \cdot 1\ (mod\ g(x))$, pa je $e(x) = 1$. To znači da reč w dekodiramo kao $w - e = 0101001 - 1000000 = 1101001$.

□

U prethodnom primeru videli smo da je dekodiranje pomoću cikličnih kodova mnogo puta brže nego dekodiranje sa metodom SA ili SDA tablicom.

6.3. Pomerački registar (Shift register)

Pre nego što definišemo pomerački registar dokažimo teoremu, koja govori o vezi između kodne reči i informacije.

Teorema 6.11. *Neka je dat cikličan (n, k)-kod, njegov generišući polinom $g(x)$ i generišuća matrica G. Ako reč $r = r_0 r_1 \dots r_{k-1}$ kodiramo pomoću generišuće matrice i dobijemo kodnu reč $v = rG$, tada je u polinomnom zapisu $v(x) = r(x)g(x)$.*

Dokaz: Znamo da generišuću matricu možemo izraziti pomoću generišućeg polinoma:

$$v = rG = [r_0 \quad \cdots \quad r_{k-1}] \begin{bmatrix} g(x) \\ \vdots \\ x^k g(x) \end{bmatrix}$$
$$= r_0 g(x) + r_1 x g(x) + \cdots + r_{k-1} x^{k-1} g(x) = r(x)g(x).$$

■

Iz prethodne teoreme videmo da informaciju možemo brzo kodirati pomoću generišućeg polinoma. Pomerački registar služi za vršenje množenja proizvoljne informacije sa fiksiranim generišućim polinomom. Pomerački registar je objekat koji realizuje množenje generišućeg polinoma i informacijskog polinoma. Taj objekat se sastoji od 3 glavna dela, to su flip-flop, ader (adder) i multiplikator konstantom (constant multiplier).

Flip-flop služi za držanje elementa iz polja F_2. Sadržaj flip-flopa se menja u svakom trenutku, koju računa klok (clock), tako da u svakom trenutku jedan element izlazi iz flip-flopa i jedan uđe u skladu sa smerom strelica.

Slika 8.

Druga komponenta je **ader** koja vrši binarnu operaciju, sabira (dva) ulazna elementa nad F_2.

Slika 9.

Treći deo pomeračkog registra je **multiplikator konstantom**, čiji je zadatak množenje ulaznog elementa sa datom konstantnom vrednošću (na Slici 10. je to g_i).

Slika 10.

U Teoremi 6.10. smo pokazali da važi $v(x) = v_0 + xv_1 + \cdots + x^{n-1}v_{n-1} = r(x)g(x)$. Ako pomnožimo $r(x)$ i $g(x)$ i grupišemo koeficijente po stepenima x, dobijamo:

$$v_0 = r_0 g_0,$$

$$v_1 = r_0 g_1 + r_1 g_0$$

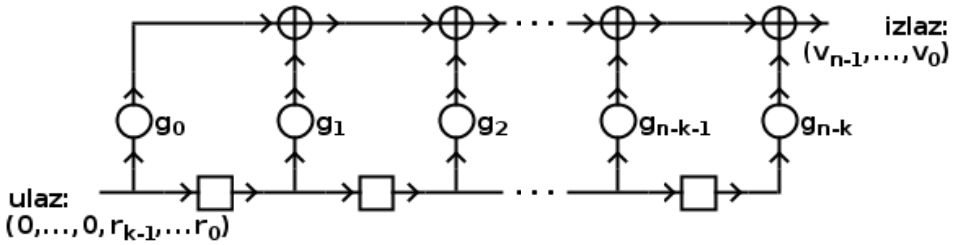
$$\vdots$$

$$v_i = r_0 g_i + r_1 g_{i-1} + \cdots + r_i g_0$$

$$\vdots$$

$$v_{n-1} = r_{k-1} g_{n-k}.$$

Na Slici 11. je prikazan pomerački registar za kodiranje informacija $r(x)$ dužine k pomoću cikličnog (n, k)-koda sa generišućim polinomom $g(x) = g_0 + \cdots + g_{n-k}x^{n-k}$. Ako hoćemo kodirati pomoću kodova dužine n, tada je potrebno n trenutaka $t_0, \ldots, t_{n-1}$. Množenje se vrši na sledeći način:



Slika 11.

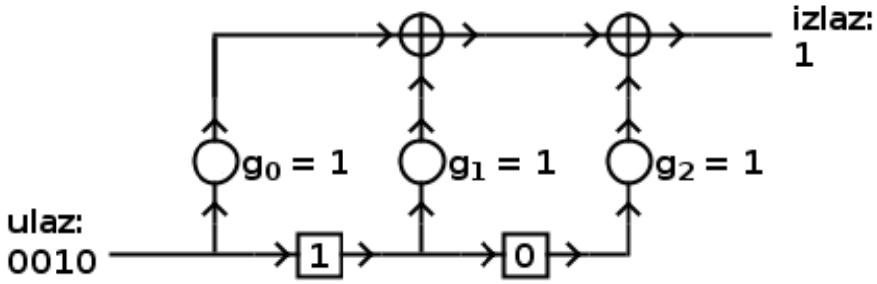
Pre prvog trenutka flip-flop je popunjen nulama. Na ulazu ulaze elementi $r_0, \ldots, r_{k-1}$ i još $n - k$ nula.

U trenutku t_0 uđe prvi elemenat r_0 u prvi flip-flop i u prvi multiplikator se množi r_0 sa g_0. Na svim ostalim delovima registra ulaze i izlaze nule odatle sledi da je izlaz (output) $r_0 g_0$.

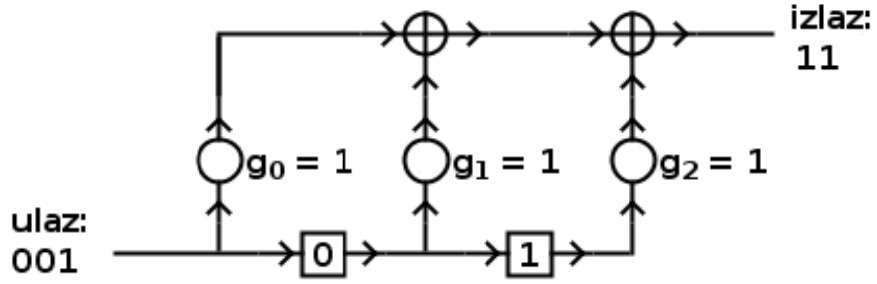
U t_1 trenutku izlazi $r_1 g_0$ iz prvog multiplikatora, a $r_0 g_1$ iz drugog, dok iz ostalih izlaze 0, pa na izlazu imamo $r_1 g_0 + r_0 g_1$.

U i-tom trenutku izlaz je $r_0 g_i + r_1 g_{i-1} + \cdots + r_i g_0$. Postupak se ponavlja n puta. Posle n-tog trenutka na izlazu je $r_{k-1} g_{n-k}$ i u pomeračkom registru imamo nule, stime smo dobili koeficijente polinoma $v(x)$.

Primer 6.6. Neka je dat cikličan (5,3)-kod, čiji je generišući polinom $g(x) = 1 + x + x^2$. Računamo kodiranje reči $r = 101$. Na slici 12. je dato stanje pomeračkog registra a) u trenutku t_0, b) u trenutku t_1.



Slika 12. a)



Slika 12. b)

6.4. Proširena greška

Ciklični kodovi imaju još jednu prednost pored dobre strukture, da oni omogućuju ispravljanje proširene greške. Do sada smo imali greške koje su slučajne, te greške su se pojavljivale u pojedinačnim bitovima. Proširene ili eksplozivne greške (burst error) javljaju se u grupi uzastopnih bitova u komunikacijskom kanalu. Primer za takav kanal je telefonski kabel ili internet kabel, CD, i tako dalje. U opštem slučaju kodovi koji omogućuju ispravljanje slučajne greške nisu efikasni za

ispravljanje proširene greške. Među kodovima ciklični kodovi su efikasni za ispravljanje te vrste greške.

Definicija 6.6. (**Ciklična) proširena greška** dužine b vektora greške e je broj ciklično uzastopnih koordinata od neke nenula koordinate do poslednje nenula kordinate različite od početne.

Svaka reč ima onoliko proširenih grešaka koliko ima nenula elemenata. Proširenu grešku možemo opisati sa **šemom** (pattern) i njenim **položajem** (location). Šema proširene greške je podreč vektora greške e od prve nenula koordinate do zadnje nenula koordinate. Položaj proširene greške je indeks koordinate vektora greške, gde se nalazi prva nenula koordinata.

U sledećem primeru videćemo da proširena greška nije jedinstvena.

Primer 6.7. Neka je dat vektor greške $e = 001011010000$. Proširena greška ima dužinu 6, njena šema je 101101, a položaj je 2 (numerišimo koordinate od 0 do 11). Zbog cikličnosti može biti proširena greška i 11, tada je šema 11010000001, položaj je 4, ili proširena greška je 12 koji ima šemu 101000000101, položaj je 5, ili proširena greška je 11, šema je 10000001011, položaj je 7.

□

Pošto proširena greška nije jedinstvena, da to ne bude zbunjujuće koristimo sledeći stav:

Neka je dat vektor greške dužine n. Neka su date dve proširene greške i svaka od njih sa njenim položajem i šemom. Ako je zbir dužina te dve šeme $\leq n + 1$, tada su te dve proširene greške identične, tj. jednake su im šeme i položaji. Zbog toga vektor greške dužine n može da ima najviše jednu proširenu grešku dužine b tako da je

$$b \leq \frac{n+1}{2}.$$

Teorema 6.12. *Neka je dat binaran* (n, k)*-kod koji ispravlja proširenu grešku dužine* $\leq b$*, za* $1 \leq b \leq (n+1)/2$*. Tada postoji tačno* $n2^{b-1} + 1$ *reči dužine* n *koji imaju proširenu grešku* $\leq b$*.*

Dokaz: Svaka proširena greška ima jedintsveni prikaz jer je $b \leq (n+1)/2$. Svaku proširenu grešku možemo staviti u jednoj reči na n različitih mesta jer su dužine reči n. Pošto šema proširene greške mora da počinje sa jedinicom, sledi da je ukupan broj mogućih šema 2^{b-1} (Smanjujemo b za 1 zbog fiksirane jedinice na početku greške.) Iz gore navedene osobine direktno sledi da je ukupan broj nenula reči sa manjom ili jednakom od b dužinom proširene greške $n2^{b-1}$. Na kraju treba još dodati nula proširenu grešku i sa time je dokazana teorema.

■

Sledeće teoreme daju granice broja kodnih reči.

Teorema 6.13. (Hemingova granica za kodne reči proširene greške) *Neka je dat binarni kod koji ispravlja proširenu grešku dužine* $\leq b$. *Ako* $1 \leq b \leq \frac{n+1}{2}$ *tada kod ima kodnih reči najviše*

$$\frac{2^n}{n2^{b-1}+1}.$$

Dokaz: Imamo ukupno $n2^{b-1}+1$ različitih reči čije su proširene greške dužine $\leq b$. Ukupan broj različitih vektora dužine n je 2^n. Da bi ispravili sve proširene greške, potrebno je da sve kodne reči budu različite i da lopte poluprečnika b budu disjunktne, zato je

$$broj\ kodnih\ reči\ \cdot (n2^{b-1}+1) \leq 2^n.$$

■

Posledica 6.14. (Abramsonova granica) *Da bi binarni linearni* (n,k)*-kod ispravljao sve proširene greške dužine* $\leq b$*, treba da važi*

i) jaka Abransomova granica

$$n \leq 2^{n-k-b+1}-1,$$

ii) slaba Abramsonova granica

$$n-k \geq \lceil log_2(n+1) \rceil + b - 1.$$

Dokaz: i) Kod je linearan, pa zato imamo 2^k kodnih reči. Iz prethodne teoreme znamo da tada važi

$$2^k \leq \frac{2^n}{n2^{b-1}+1}.$$

Odavde sledi da je

$$n \leq 2^{n-k-b+1} - 2^{1-b}.$$

n je ceo broj, zato umesto 2^{1-b} možemo pisati 1.

ii) Nejednakost pod i) logaritmujemo:

$$\log(n+1) \leq n-k-b+1$$

$$\log(n+1)+b-1 \leq n-k$$

uzmemo $\lceil \log_2(n+1) \rceil$ (najmanji ceo broj koji nije menji od broja koji je naveden u zagradi) jer mora da bude ceo broj, tada dobijamo traženi izraz.

■

Teorema 6.15. *Neka je dat binarni kod koji ispravlja proširenu grešku dužine* $\leq b$. *Ako je* $b \leq n/2$ *tada kod ima najviše* 2^{n-2b} *kodnih reči.*

Dokaz: Pretpostavimo suprotno, neka kod ima više od 2^{n-2b} kodnih reči. Tada mora da postoje bar dve kodne reči ($\dot{v}$ i $\ddot{v}$) prema Dirihletovom principu koje imaju oblik

$$\dot{v} = v_1 \dots v_{n-2b} * \dots * \in F_2^n,$$

i

$$\ddot{v} = v_1 \dots v_{n-2b} \# \dots \# \in F_2^n,$$

gde su $v_i \in F_2, i = 1, \dots, n-2b$. Prvih $n-2b$ koordinata vektora $\dot{v}$ i $\ddot{v}$ su isti, a na mestu „*“ i „#“ imamo proizvoljne simbole. Posmatrajmo reč w

$$w = v_1 \dots v_{n-2b} \underbrace{* \dots *}_{b} \underbrace{\# \dots \#}_{b},$$

koja se sa reči $\dot{v}$ razlikuje najviše na poslednjih b simbola, a od reči $\ddot{v}$ razlikuje najviše na predposlednjem bloku simbola dužine b.

Tada reč w ne znamo kako da dekodiramo, jer kodne reči $\dot{v}$ i $\ddot{v}$ imaju najviše b proširenih grešaka. Ovaj kod dakle ne ispravlja b proširenih grešaka, a to je kontradikcija sa pretpostavkom. Dakle, kod ima najviše 2^{n-2b} kodnih reči.

■

Posledica 6.16. *Neka je V linearan (n,k)-kod koji ispravlja b proširenih grešaka, $b \leq \frac{n}{2}$. Tada granica za bazu koda V je*

$$k \leq n - 2b.$$

Dokaz: Linearan kod ima tačno 2^k kodnih reči, pa iz prethodne teoreme znamo da važi

$$2^k \leq 2^{n-2b}.$$

Logaritmovanjem gornjeg izraza dobijamo traženu nejednakost.

■

Primer 6.8. a) Binarni ciklični $(n, 1)$-kod koji smo uveli u Primeru 6.1. ispravlja sve proširene greške $\leq \frac{n-1}{2}$.

b) Hemingovi $(2^m - 1, 2^m - 1 - m)$-kodovi ispravljaju jednu grešku, pa oni takođe ispravljaju proširenu grešku dužine jedan.

□

7. Specijalni ciklični kodovi

U ovom delu rada proučavamo neke klase cikličnih kodova, kao što su BCH kodovi, Rid-Solmon kodovi i Golej kodovi. Oni imaju posebne osobine pa je njihova primena široka u praksi. Ciklični kodovi su opisani sa njihovim generišućim polinomom, ali je teško isčitati kodno rastojanje iz generišućeg polinoma. Ti specijalni kodovi imaju poseban oblik generišućeg polinoma koji olakšavaju našu analizu.

7.1. BCH kodovi

Binarni BCH kodovi su dobili ime po njihovim pronalazačima. Binarni BCH kod prvo su opisali Hocquenghem, Bose i Chaudhuri. Kasnije Gorenstein i Zierler su opisali q-arni BCH kodove. Ti kodovi su bolje verzije Hemingovih kodova, jer BCH kodovi omogućuju ispravljanje više grešaka, dok sa Hemingovim kodovima moguće je ispraviti samo jednu grešku. Koriste se npr za kodiranje informacija na CD-ovima.

Definicija 7.1. Neka je α primitivan element skupa F_{q^m}. Neka su $M_i(x)$ minimalni polinomi za α^i nad F_q. **BCH kod** je q-arni cikličan kod nad F_q sa dužinom $n = q^m - 1$, njegovo planirano kodno rastojanje (designed distance) je dd i generišući polinom je

$$g(x) = \text{nzs}\big(M_a(x), M_{a+1}(x) \dots, M_{a+dd-2}(x)\big),$$

gde je a neki prirodan broj.

Sledeća teorema daje donju granicu dimenzije BCH koda.

Teorema 7.1. *q-arni BCH kod dužine $n = q^m - 1$ sa planiranim kodnim rastojanjem dd ima dimenziju k*

$$k \geq q^m - 1 - m(dd - 1).$$

Dokaz: Znamo da je generišući polinom BCH koda

$$g(x) = nzs\big(M_a(x), M_{a+1}(x) \dots, M_{a+dd-2}(x)\big).$$

Iz osobine ciklotomičnog koseta iii) sledi da možemo napisati generišući polinom pomoću ciklotomičnih koseta, jer je $M_i(x) = \prod_{j \in C_i}(x - \alpha^j)$, odnosno

$$g(x) = \text{nzs}\big(\prod_{i \in C_a}(x - \alpha^i), \prod_{i \in C_{a+1}}(x - \alpha^j), \dots, \prod_{i \in C_{a+dd-2}}(x - \alpha^i)\big).$$

Iz osobine najmanjeg zajedničkog sadržaoca ii) sledi da gornju jednakost možemo napisati na sledeći način

$$g(x) = \prod_{i \in C} \left(x - \alpha^i\right),$$

gde je $C = \bigcup_{i=a}^{a+dd-2} C_i$.

Stepen generišućeg polinoma je $n-k$, zato preko dužine koda i stepena generišućeg polinoma možemo izraziti dimenziju koda:

$$k = n - (n-k) = q^m - 1 - \deg\left(g(x)\right).$$

Preko ciklotomičnih koseta možemo naći granicu stepena generišućeg polinoma. Stepen polinoma je jednak broju elemenata skupa C, imamo proizvode $\left(x - \alpha^i\right)$ onoliko puta koliko elemenata imamo u C, odnosno

$$\deg\left(g(x)\right) = |C| = \left| \bigcup_{i=a}^{a+dd-2} C_i \right| \leq \sum_{i=a}^{a+dd-2} |C_i|.$$

Na osnovu osobine ii) cikličnog koseta znamo da $|C_i| \leq m$ zato

$$\sum_{i=a}^{a+dd-2} |C_i| \leq \sum_{i=a}^{a+dd-2} m = m(dd-1).$$

Dakle,

$$k = q^m - 1 - \deg\left(g(x)\right) \geq q^m - 1 - m(dd-1).$$

■

Postavlja se pitanje kako možemo formirati kontrolnu matricu. Pošto je BCH kod cikličan, koristićemo generišući polinom. Definisali smo da je $g(x) = \text{nzs}\left(M_a(x), M_{a+1}(x) \ldots, M_{a+dd-2}(x)\right)$, gde su $\alpha^a, \ldots, \alpha^{a+dd-2}$ koreni generišućeg polinoma, tj. $g\left(\alpha^i\right) = 0, i = a, \ldots, a+dd-2$. Kodnu reč $v(x)$ možemo napisati pomoću generišućeg polinoma na sledeći način $v(x) = g(x)q(x)$, za neki polinom $q(x)$. Pošto je $g\left(\alpha^i\right) = 0$ za sve $i = a, \ldots, a+dd-2$, onda je i $v\left(\alpha^i\right) = 0, i = a, \ldots, a+dd-2$. U polinomnom zapisu to je

$$v\left(\alpha^i\right) = v_0 + v_1\alpha^i + \cdots + v_{n-1}(\alpha^i)^{n-1} = 0,$$

ili u matričnom zapisu

$$\begin{bmatrix} 1 & \alpha^i & \ldots & \alpha^{(n-1)i} \end{bmatrix} \begin{bmatrix} v_0 \\ \vdots \\ v_{n-1} \end{bmatrix} = 0.$$

Stavimo u matricu H redove vektora $\begin{bmatrix} 1 & \alpha^i & \ldots & \alpha^{(n-1)i} \end{bmatrix}$ za različite i-ove i dobijemo da je

$$H = \begin{bmatrix} 1 & \alpha^a & \alpha^{2a} & \ldots & \alpha^{(n-1)a} \\ 1 & \alpha^{a+1} & \alpha^{2(a+1)} & \ldots & \alpha^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{a+dd-2} & \alpha^{2(a+dd-2)} & \ldots & \alpha^{(n-1)(a+dd-2)} \end{bmatrix}.$$

Matrica H je kontrolna matrica redovi su linearno nezavisni jer je matrica H Vandermondova i ona je ranga $dd-1$ ako su α^a,..., α^{a+dd-2} različiti i za bilo koju kodnu reč v važi da je $Hv=0$.

Sledeća teorema pokazuje odnos između kodnog rastojanja BCH koda i planiranog rastojanja.

Teorema 7.2. *Kodno rastojanje BCH koda nije manje od planiranog kodnog rastojanja*

$$d \geq dd.$$

Dokaz: Neka je dat BCH kod i njegov generišući polinom $g(x)$ =nzs$\big(M_a(x), M_{a+1}(x) \dots, M_{a+dd-2}(x)\big)$.

Pretpostavimo suprotno $d < dd$. To znači da postoji kodna reč v tako da je $\|v\| = d$ (jer po Teoremi 5.3. linearan kod ima kodno rastojanje $d = \min_{v \in V}\{\|v\|, v \neq 0\}$). Uzmemo kodnu reč v. Znamo da je $Hv = 0$, tj.

$$\begin{bmatrix} 1 & \alpha^a & \alpha^{2a} & \dots & \alpha^{(n-1)a} \\ 1 & \alpha^{a+1} & \alpha^{2(a+1)} & \dots & \alpha^{(n-1)(a+1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{a+dd-2} & \alpha^{2(a+dd-2)} & \dots & \alpha^{(n-1)(a+dd-2)} \end{bmatrix} \begin{bmatrix} v_0 \\ \vdots \\ v_{n-1} \end{bmatrix} = 0.$$

Uzmemo nenula elemnte vektora v, kojih ima tačno d, i obeležimo te elemente sa $v_{i_1}, \dots, v_{i_d}$. Sada je dovoljno da uzmemo iz jednakosti $Hv = 0$ samo nenula koordinate vektora v, tj.

$$\begin{bmatrix} \alpha^{ai_1} & \dots & \alpha^{ai_d} \\ \vdots & \ddots & \vdots \\ \alpha^{(a+dd-2)i_1} & \dots & \alpha^{(a+dd-2)i_d} \end{bmatrix} \begin{bmatrix} v_{i_1} \\ \vdots \\ v_{i_d} \end{bmatrix} = 0.$$

Uzmemo prvih d redova prethodnog sistema, tada dobijamo

$$\underbrace{\begin{bmatrix} \alpha^{ai_1} & \dots & \alpha^{ai_d} \\ \vdots & \ddots & \vdots \\ \alpha^{(a+d-1)i_1} & \dots & \alpha^{(a+d-1)i_d} \end{bmatrix}}_{V} \begin{bmatrix} v_{i_1} \\ \vdots \\ v_{i_d} \end{bmatrix} = 0.$$

V je matrica formata $d \times d$. Njegova determinanta je

$$\begin{aligned} |V| &= \begin{vmatrix} \alpha^{ai_1} & \dots & \alpha^{ai_d} \\ \vdots & \ddots & \vdots \\ \alpha^{(a+d-1)i_1} & \dots & \alpha^{(a+d-1)i_d} \end{vmatrix} \\ &= \alpha^{a(i_1+\dots+i_d)} \underbrace{\begin{vmatrix} 1 & \dots & 1 \\ \alpha^{i_1} & \dots & \alpha^{i_d} \\ \vdots & \ddots & \vdots \\ \alpha^{(d-1)i_1} & \dots & \alpha^{(d-1)i_d} \end{vmatrix}}_{W}. \end{aligned}$$

W je Vandermondova matrica, čija je determinanta različita od nule ako su elementi matrice različiti. U našem slučaju taj uslov je ispunjen, zato Hv biće nula ako i samo ako su svi elementi vektora v

jednaki nuli. To je kontradikcija sa pretpostavkom da je v različit od nula vektora. Dakle, važi $d \geq dd$.

■

Prethodnu teoremu možemo shvatiti tako da možemo konstruisati BCH kod tako da ispravlja bilo koju dužinu greške.

7.2. Rid-Solomon kodovi

Rid-Solmon (Reed-Solomon) kodovi (RS) pripadaju klasi BCH kodova.

Definicija 7.2. Posmatramo q-aran BCH kod dužine $n = q^m - 1$ sa generišućim polinomom $g(x) = \text{nzs}(M_a(x), M_{a+1}(x) \dots, M_{a+dd-2}(x))$. BCH kod naziva se **RS kod**, ako je $m = 1$, tj. ako je dužina koda $n = q - 1$, $a \geq 0$, i $2 \leq dd \leq q - 1$.

U tom slučaju

$$g(x) = \text{nzs}(M_a(x), M_{a+1}(x) \dots, M_{a+dd-2}(x)) = (x - \alpha^a) \dots (x - \alpha^{a+dd-2}),$$

gde je α primitivan elemenat nad F_q, $i = a, \dots, a + dd - 2$.

Napomena: Binarne RS kodove ne možemo konstruisati, jer tada bi dužina koda bila 1.

RS kodovi su ciklični kodovi sa parametrima $n = q - 1, k = q - dd$ (jer je stepen generišućeg polinoma $dd - 1$) i $d = dd$ (za BCH kodove smo pokazali da je $d \geq dd$, sa druge strane za linearne kodove uvek važi da je $k + d \leq n + 1$).

U praksi više se primenjuju binarni kodovi. RS kodovi nisu binarni ali ih možemo transformisati tako da dobijemo binarne kodove.

7.3. Golej kodovi

Golej (Golay) kodovi se koriste za digitalizovanu komunikaciju. Postoje binarni i ternarni Golej kodovi. Mi ćemo se baviti samo sa binarnim kodovima. Postoje dva binarna Golej koda: G_{24} i G_{23}.

Binarni Golej kod G_{24} ima generišuću matricu

$$G = [I_{12}|A],$$

gde je I_{12} jedinična matrica formata 12×12, a A je matrica

$$A = \begin{bmatrix} 011111111111 \\ 111011100010 \\ 110111000101 \\ 101110001011 \\ 111100010110 \\ 111000101101 \\ 110001011011 \\ 100010110111 \\ 100101101110 \\ 101011011100 \\ 110110111000 \\ 101101110001 \end{bmatrix}.$$

Može se definisati i kao ciklični kod, tada generišući polinom je

$$g(x) = x^{11} + x^{10} + x^6 + x^5 + x^4 + x^2 + 1.$$

Kodno rastojanje Golej G_{24} koda je $d = 8$, tj. sa tim kodom mogu se ispraviti 3 greške, dakle taj kod je binarni ciklični $(24,12,8)$-kod.

Drugi binarni Golej kod je G_{23}, koji dobijemo tako što brišemo zadnju cifru svake kodne reči iz G_{24}. Tako dobijamo jedan (23,12,7)-kod, koji je takođe cikličan.

Kod G_{23} je savršen kod. To znači da kod ima jednu specijalnu osobinu, a to je da važi jednakost kod Hemingovog potrebnog uslova za postojanje blok-koda $V \subseteq B^n$ kardinalnosti a (za linearne kodove $a = 2^k$) koji omogućuje ispravljanje s grešaka

$$\frac{2^n}{\sum_{i=0}^{s} \binom{n}{i}} = a.$$

U našem slučaju

$$s = \left\lfloor \frac{d-1}{2} \right\rfloor = 3.$$

To znači, da ima tačno toliko kodnih reči (G_{23} ima $2^k = 2^{12}$), da pokriva ceo vektorski prostor (F_2^{23}) u kome je definisan, odnosno ne otkriva samo greške najveće dužine s, nego ih i ispravlja. (U geometrijskom smislu to znači, da svaka reč iz F_2^{23} pripada nekoj lopti $Z_s(v)$, gde je v kodna reč.)

Zaključak

Ovaj rad se bavi cikličnim kodovima i pojmovima koji su u vezi sa njima. Definisani su pojmovi teorije informacija, kao što su entropija i komunikacijski sistem, i predstavljene su najvažnije osobine funkcije entropije.

Sem toga, ovim master radom dobijamo uvid u osnove teorije kodiranja. Analizirani su prefiksni kodovi kanala bez smetnji. Navedeni su neki rezultati kodiranja u kanalu sa smetnjama, kao što su granice prosečnih dužina kodnih reči optimalnog koda. U radu su takođe opisani blok-kodovi i njihova potklasa linearnih kodova. Predstavljene su neke njihove osobine kao što su generišuća i kontrolna matrica linearnih kodova, pomoću kojih je delotvornije i preglednije konstruisanje kodova i dekodiranje. Reprezentovani su linearni kodovi pomoću vektorskog prostora.

Predstavljeni su ciklični kodovi, koji su potklasa linearnih kodova opisanih pomoću generišućih polinoma. Kao jedno od najvažnijih tvrđenja u vezi sa cikličnim kodovima je Teorema 6.4. koja govori o postojanju generišućeg polinoma, kao u radu [1]. Predstavljeni su neki poznati ciklični kodovi kao što su BCH-kodovi, Rid-Solmon kodovi i Golej kodovi. Ti kodovi se koriste na primer u komunikaciji sa satelitima, skladištenja podataka na CD, DVD, Blue-ray disk.

Literatura

1. Norman L. Biggs: Codes An Introduction to Information Communication and Cryptography, Springer, London, 2008.,123.-162.

2. Lakatos Piroska: Kódelmélet Egyetemi jegyzet, Debreceni Egyetem Természettudományi kar Algebra és számelmélet tanszék, Debrecen, 2010., 3.-80.

3. San Ling, ChaopingC Xing: Coding Theory A First Course, Cambridge University Press, United States of America, 2004., 1.-92., 133.-183.

4. Robert J. McEliece: The Theory of Information and Coding, Cambridge University Press, United Kingdom, 2004., 139.-236.

5. Todd K. Moon: Error Correction Coding Mathematical Methods and Algorithms Wiley, New Jersey, 2005., 1.-14., 22.-39., 61.-98., 113.-128., 235.-241.

6. Steven Roman: Coding and Information Theory, Springer-Verlag, California, 1992.

7. Ron M. Roth: Introduction to Coding Theory, Cambridge University Press, United States of America, 2006., 1.-62., 218.-256.

8. Branimir Šešelja, Andreja Tepavčević: Algebra 1, Prirodno-matematički fakultet, Novi Sad, 2004.

9. Branimir Šešelja: Teorija informacije i kodiranja, Prirodno-matematički fakultet, Novi Sad, 2005.

10. en.wikipedia.org/wiki/Binary_Golay_code (10.3.2015.)

11. hu.wikipedia.org/wiki/ASCII (2.2.2015.)

12. hu.wikipedia.org/wiki/Morzekód (2.2.2015.)

13. hu.wikipedia.org/wiki/Vonalkód (10.3.2015.)

14. hu.wikipedia.org/wiki/UTF-8 (22.3.2015.)

15. sr.wikipedia.org/wiki/UTF-8 (22.3.2015.)

Biografija

Agneš Kovač je rođena 29. aprila 1989. godine u Senti. Godine 2004. završava Osnovnu školu "Stevan Sremac" u Senti kao nosilac Vukove diplome. Iste godine upisuje "Senćansku gimnaziju" u Senti koju završava 2008. godine. Po završetku sredje škole upisuje osnovne akademske studije primenjene matematike na Prirodno-matematičkom fakultetu u Novom Sadu koje završava u septembru 2012. godine. Iste godine u oktobru, upisuje master akademske studije primenjene matematike. Sve ispite predviđene planom i programom polaže zaključno sa septembarskim ispitnim rokom 2014. godine i time stiče uslov za odbranu ovog master rada.

U Novom Sadu, maj 2015. godine Agneš Kovač

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: Agneš Kovač
AU

Mentor: dr Petar Đapić
MN

Naslov rada: Ciklične kodove
MR

Jezik publikacije: Srpski (latinica)
JP

Jezik izvoda: srpski/engleski
JI

Zemlja publikovanja: Republika Srbija
ZP

Uže geografsko područje: Vojvodina
UGP

Godina: 2015.
GO

Izdavač: Autorski reprint
IZ

Mesto i adresa: Prirodno-matemati£ki fakultet, Departman za matematiku i informatiku, Trg Dositeja Obradovi¢a 4, Novi Sad
MA

Fizički opis rada: (7/*72/0/8/13/0/0*)
FO

Naučna oblast: Matematika
NO

Naučna disciplina: Teorija kodiranja
ND

Ključne reči: Ciklični kod, generišući polinom, generišuća matrica
PO

UDK

Čuva se: Biblioteka Departmana za matematiku i informatiku, Prirodno matemati£ki
fakultet, Univerzitet u Novom Sadu
ČU

Važna napomena:
VN

Izvod: Tema ovog rada su ciklični kodovi. Prvo definišemo osnovne pojmove teorije informacije. Nakon toga prelazimo na teoriju kodiranja. Tu se bavimo sa komunikacijskim kanalima bez smetnje, pri čemu posebnu pažnju posvećujemo prefiksnim kodovima. Zatim proučavamo kodiranje sa smetnjama. Definišemo blok-kodove i dokazujemo njihove osobine. Zatim se bavimo sa jednom širom potklasom blok-kodova, sa linearnim kodovima. Uvodimo određivanje koda pomoću generišuće i kontrolne matrice. Potom opisujemo ciklične kodove i neke specijalne klase cikličnih kodova pomoću generišućeg polinoma.

IZ

Datum prihvatanja teme od strane NN veća: 11.07.2014
DP

Datum odbrane:
DO

Članovi komisije:
KO

Predsednik: dr Andreja Tepavčević, redovni profesor Prirodno-matematičkog fakulteta, Univerziteta u Novom Sadu
Član: 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 umber:
INO

Document type: Monograph type
DT

Type of record: Printed text
TR

Contents Code: Master's thesis
CC

Author: Agneš Kovač
AU

Mentor: Petar Đapić, Ph. D.
MN

Title: Cyclic codes
TI

Language of text: Serbian (Latin)
LT

Language of abstract: English
LA

Country of publication: Republic of Serbia
CP

Locality of publication: Vojvodina
LP

Publication year: 2015.
PY

Publisher: Author's reprint
PU

Publ. place: Department of Mathematics and Informatics, Faculty of Science, Trg
Dositeja Obradovića 4, Novi Sad

PP

Physical description: (7/*72/0/8/13/0/0*)
PD

Scientific field:
Mathematics
SF

Scientific discipline: Coding theory
SD

Key words: Cyclic code, generator polynomial, generator matrix
KW

Holding data: Library of Department of Mathematics and Informatics, Faculty of
Science, University of Novi Sad

HD

Note:
N

Abstract: The main purpose of this work is to analyze cyclic codes. First, we define what information theory is. We deal with coding theory, and we also mention noiseless channels, where prefix codes are specially emphasized. After this, noisy coding is defined. Block-codes and their purposes are explained. We talk about linear codes, which make a subgroup of block codes. The use of the generator and parity check matrices are being introduced. Cyclic codes and their subgroups are defined with generator polynomials.

AB
Accepted by the Scientific Board on:
ASB

Defended:
DE

Thesis defend board:
DB
President: Andreja Tepavčević PhD, full professor, Faculty of Science, University of Novi Sad
Member: Branimir Šešelja PhD, full professor, Faculty of Science, University of Novi Sad
Member: Petar Đapić PhD, docent, Faculty of Science, University of Novi Sad