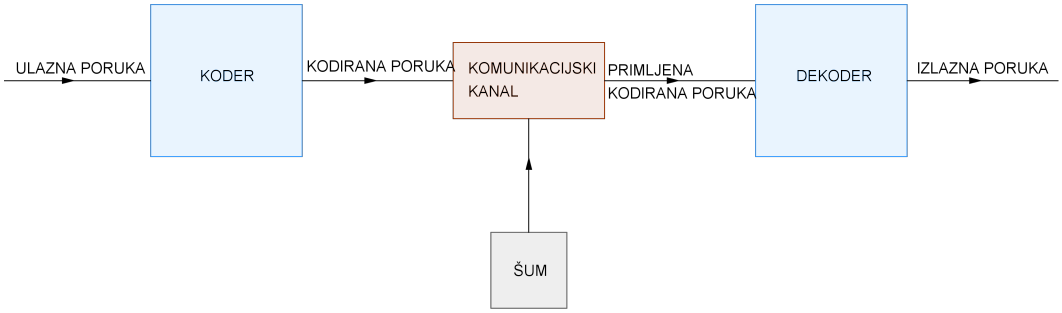
Linearni kodovi

Vedrana Mikulić Crnković i Andrea Švob
(Fakultet za matematiku, Sveučilište u Rijeci)

1 Uvod

Teorija kodiranja je bazirana na sljedećem komunikacijskom modelu. Pošiljatelj želi poslati poruku primatelju. Poruke se šalju kroz komunikacijski kanal, koji nije savršen pa može dodati grešku na originalnu poruku. Npr. gledajući TV program, često se javljaju šumovi i slabi prijem slike, upravo zbog atmosferskih pojava. Komunikacijski model je sljedećeg izgleda:



U koderu se kodira ulazna poruka i dobivamo kodiranu poruku. Kodirana poruka se šalje putem komunikacijskog kanala u kojemu se dodaje greška. Dekoder prima izmijenjenu kodiranu poruku i dekodira je kako bi se dobila izlazna poruka.

Neka je F konačan skup koji se sastoji od q elemenata. Skup F nazivamo **abecedom**, a njegove elemente **simbolima**. q-naran **kod** C duljine n nad poljem F je podskup $C \subseteq F^n$. Elemente koda zovemo **riječi koda**. Kodove nad abecedom duljine 2, tj. kodove koji koriste abecedu $F_2 = \{0, 1\}$, nazivamo **binarnim kodovima**.

Primjer 1. (Kod s ponavljajućim bitovima)

Pretpostavimo da želimo prenijeti informaciju zapisanu binarnim nizom duljine 1, npr. 1. S ciljem efikasnije detekcije greške, šaljemo sljedeći niz: 11111111.

U ovom smo primjeru informaciju od jednog simbola zapisali nizom simbola duljine 8. Takvim kodiranjem ćemo lako uočiti grešku (osim ako nije napravljena na svih 8 simbola u niz) te ćemo znati ispravno dekodirati riječ ako je napravljeno manje od 4 greške u prijenosu.

Primjer 2. (Kod s provjerom parnosti)

Pretpostavimo da želimo prenijeti informaciju zapisanu binarnim nizom duljine 7, npr. 1110001. Pri prijenosu ćemo dodati i osmi član niza a na sljedeći način:

- $a = 0$ ako u početnom nizu ima paran broj jedinica,
- $a = 1$ ako u početnom nizu ima neparan broj jedinica.

U primjeru to znači da šaljemo niz 11100010.

U ovom smo primjeru nizom duljine 8 prenijeli informaciju koja je zapisana nizom duljine 7 te možemo detektirati ako se dogodi neparan broj pogrešaka, ali ne znamo ispravno dekodirati riječ ni ako smo detektirali pogrešku. Naravno, u realnim situacijama često postoji mogućnost da od pošiljatelja tražimo da nam ponovno pošalje informaciju jer je došlo do pogreške u prijenosu.

Uočimo da smo u Primjeru 1 nizom duljine 8 prenijeli samo jednu informaciju, a da smo u Primjeru 2 nizom duljine 8 prenijeli 7 informacija. Međutim, velika je razlika u mogućnosti detekcije i ispravljanja pogrešaka koje se dogode u prijenosu.

Osnovni problem koji nas zanima u teoriji kodiranja je pronaći kod kojim možemo preko kodera i dekodera u komunikacijskom modelu prenijeti željene količine informacija uz zadovoljavajuću mogućnost detekcije greške i ispravljanja greške. Razumna je pretpostavka da se pri prijenosu informacija ne događa puno grešaka.

2 Minimalna udaljenost koda

Težina riječi x koda koda C, $w(x)$, je broj pozicija riječi koda na kojima se nalazi simbol 1.

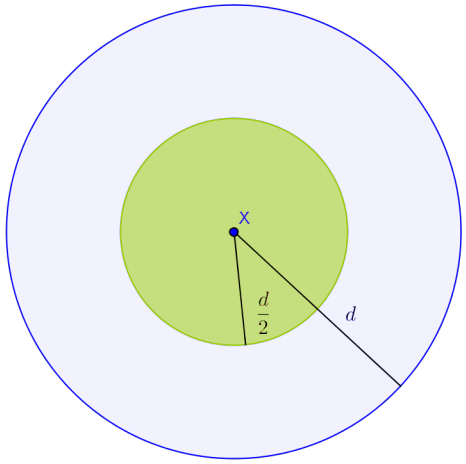
Hammingova udaljenost dviju riječi koda je broj pozicija na kojima se riječi koda razlikuju, tj. broj pozicija na kojima riječi koda imaju različite simbole. (Npr. Hammingova udaljenost riječi koda [10101] i [11001] je $d([10101], [11001]) = 2$).

Minimalna udaljenost d koda C je najmanja od Hammingovih udaljenosti među različitim riječima koda.

Težinu riječi koda C možemo definirati i kao Hammingovu udaljenost od nul riječi. Prema tome, minimalna težina koda C je minimum skupa težina njegovih riječi koje su različite od nul riječi.

Minimalna udaljenost koda je bitan parametar koda, pogotovo ako dekodiramo primljenu riječ koda najbližom riječju koda (što ima smisla ako pretpostavimo da se pri prijenosu ne događa puno grešaka i tako se dekodiranje često koristi).

Neka je minimalna udaljenost koda C jednaka d. Pretpostavimo da je poslana riječ koda X. Riječ koda C koja je najbliža riječi X pripada ili kružnici k polumjera d sa središtemu točki X (plava kružnica na slici) ili je izvan te kružnice.



Ukoliko se je pri prijenosu dogodilo manje od d grešaka, primit ćemo riječ koja pripada krugu omeđenom kružnicom k.

Ukoliko se pak u prijenosu dogodilo manje od $\frac{d}{2}$ pogrešaka, primit ćemo riječ koja pripada krugu sa središtem u točki X i polumjerom jednakom $\frac{d}{2}$ (krug obojan zelenom bojom na slici). U prvo slučaju znat ćemo da je došlo do pogreške, ali nećemo moći sa sigurnošću reći je li poslana riječ X ili recimo neka riječ Y koja pripada kružnici k. U drugom ćemo slučaju ispravno dekodirati primljenu riječ, odnosno ispraviti sve pogreške.

Zaključujemo da kod s minimalnom udaljenošću d može detektirati pogreške ako ih je manje od d te da ih može ispraviti ako ih je manje od $\frac{d}{2}$.

3 Definicija i osnovna svojstva linearnog koda

Svaku riječ koda, binarnog koda C duljine n, možemo predstaviti vektorom oblika $x = [x_1 \ ... \ x_n]$, gdje su $x_i \in F_2 = \{0, 1\}$. Tako definirane vektore nazivamo binarnim vektorima. Nad skupom F_2 moguće je definirati operacije zbrajanja i množenja na način kako je prikazano Tablicom 1.

Tablica 1: Zbrajanje i množenje u F_2

x_1	x_2	$x_1 + x_2$	$x_1 \cdot x_2$
0	0	0	0
0	1	1	0
1	0	1	0
1	1	0	1

Neka je $V(n)$ skup svih binarnih vektora duljine n. Ukupno ih ima 2^n. Neka su a, x_i, y_i elementi iz F_2, a x, y vektori iz skupa $V(n)$. Nad skupom $V(n)$ tada je moguće definirati operacije zbrajanja vektora i množenja vektora elementima iz F_2 na sljedeći način:

$$x + y = [x_1\ x_2\ x_3\ ...\ x_n] + [y_1\ y_2\ y_3\ ...\ y_n] = [x_1 + y_1\ x_2 + y_2\ x_3 + y_3\ ...\ x_n + y_n],$$

$$a \cdot x = a \cdot [x_1\ x_2\ x_3\ ...\ x_n] = [a \cdot x_1\ a \cdot x_2\ a \cdot x_3\ ...\ a \cdot x_n].$$

Kažemo da je binarni kod $C \subseteq V(n)$ **linearan**, ako se zbrajanjem bilo koje dvije riječi koda opet dobiva neka riječ koda ili ako se množenjem bilo koje riječi koda s elementom iz abecede opet dobiva riječ koda.

Za linearne kodove vrijedi sljedeće svojstvo: minimalna udaljenost koda C je jednaka njegovoj minimalnoj težini.

Važno svojstvo linearnih kodova je da sadrže bazu. **Baza linearnog koda** je skup svih linearno nezavisnih riječi koda. Iz svojstava vektora znamo da ako je poznata baza nekog prostora vektora, svaki drugi vektor tog prostora se može zapisati kao linearna kombinacija vektora baze. U tom slučaju, ako se kod C sastoji od k vektora u bazi, onda se svaka riječ koda može zapisati kao linearna kombinacija tih k vektora baze, gdje su skalari elementi skupa F_2. Vektori baze se mogu zapisati u generirajuću matricu koda. Linearan kod označavamo s $[n, k]$-kod.

Generirajuća matrica koda je matrica koja se sastoji od k redaka i n stupaca, a redci te matrice se sastoje od vektora baze koda. Npr. neka je zadan binarni kod C koji sadrži sljedeće riječi koda

$$C = \{[0\ 0\ 0\ 0\ 0], [1\ 1\ 1\ 0\ 0], [0\ 0\ 1\ 1\ 1], [1\ 1\ 0\ 1\ 1]\}.$$

Budući da vidimo na primjeru da su zadnje dvije riječi linearno nezavisne i da je

druga riječ jednaka njihovom zbroju, za bazu možemo uzeti zadnje dvije riječi. Sve riječi koda C se mogu dobiti kao linearna kombinacija riječi baze koda. Na taj način dobivamo generirajuću matricu koda pomoću koje je definiran cijeli kod C.

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

Dva ekvivalentna linearna koda imaju generirajuće matrice koje se jedna iz druge mogu dobiti sljedećim operacijama: zamjenom redaka, dodavanjem jednog retka drugom retku i zamjenom stupaca. Na postojećoj generirajućoj matrici G koda C možemo izvršiti operaciju zamjene drugog i trećeg stupca, a potom zamjenu prvog i drugog retka. Dobivamo generirajuću matricu

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

Kažemo da je generirajuća matrica G^* zapisana u standardnom obliku, tj. zapisana je u obliku $G = [I_k, A]$, gdje je I_k jedinična matrica. Matrica G^* ima strukturu $[I_2|A]$.

Paritetna matrica koda C je matrica oblika $H = [A^T, I_{n-k}]$.
U gornjem primjeru, paritetna matrica koda C je matrica oblika

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

Pretpostavimo da želimo poslati poruku [11]. Pomnožimo li poruku s generirajućom matricom dobivamo kodiranu poruku, odnosno riječ koda $[1\ 1] \cdot G^* = [1\ 1\ 1\ 0\ 0]$ koju šaljemo komunikacijskim kanalom. Množenjem dobivene riječi koda s transponiranom matricom matrice H dobivamo:

$$[1\ 1\ 1\ 0\ 0] \cdot \begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0\ 0\ 0].$$

Rezultat množenje riječi koda s transponiranom matricom matrice H će uvijek biti nul

vektor. Odnosno, množenjem primljene riječi s transponiranom matricom matrice H možemo provijeriti je li primljena riječ riječ koda (ako je, pretpostavljamo da je ta riječ i poslana, odnosno da nije doslo do pogreške u prijenosu).