Mrežno kodiranje

Nikoletić, Karlo

Mrežno kodiranje

Nikoletić, Karlo

Sveučilište u Zagrebu
Prirodoslovno-matematički fakultet
Matematički odsjek

Karlo Nikoletić

Mrežno kodiranje

Diplomski rad

Voditelj rada:
izv.prof.dr.sc. Vedran Krčadinac

Zagreb, srpanj 2020.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____ , predsjednik
2. _____ , član
3. _____ , član

Povjerenstvo je rad ocijenilo ocjenom _____ .

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Sadržaj

1 Uvod

Teorija kodiranja proučava učinkovite metode prijenosa informacija kroz kanal sa šumom, a prvi puta se spominje 1948. godine u članku Claudea Shannona "A mathematical Theory of communication". Efikasnije metode daje mrežno kodiranje razvijeno početkom tisućljeća. U mrežnom kodiranju čvorovi prosljeđuju linearne kombinacije primljenih paketa, umjesto odvojenih paketa u klasičnoj teoriji kodiranja. Takvom elegantnom tehnikom kodiranja postižu se veće brzine i bolja robusnost u slučaju pogrešaka pri prijenosu.

U prvom poglavlju bavimo se klasičnom teorijom kodiranja. Prvo ćemo definirati klasične kodove i njihove parametre. Pokazat ćemo da je Hammingova udaljenost kodnih riječi metrika te proučiti mogućnosti otkrivanja i ispravljanja pogrešaka. Zatim ćemo definirati linearne kodove kojima su kodne riječi potprostor vektorskog prostora i proučiti svojstva dviju vrsta linearnih kodova, Hammingovih i Reed-Mullerovih.

U drugom poglavlju uspoređujemo prijenos paketa u klasičnoj teoriji kodiranja s prijenosom tehnikom mrežnog kodiranja. Dokazat ćemo teorem minimalnog reza i maksimalnog toka te glavni teorem mrežnog kodiranja. Glavni teorem mrežnog kodiranja pokazuje, pozivajući se na teorem minimalnog reza i maksimalnog toka, da se linearnim kombiniranjem paketa na čvorovima jednakom brzinom, kojom u klasičnoj teoriji kodiranja prenesemo informaciju na jedno odredište, može prenijeti informacija na više odredišta.

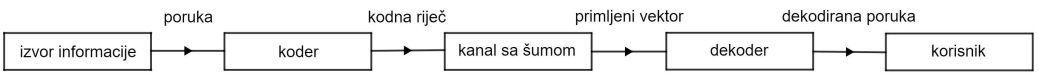
U posljednjem poglavlju proučit ćemo slučajno mrežno kodiranje u kojem se paketi nasumično linearno kombiniraju na čvorovima. Također ćemo proučiti svojstva potprostornih kodova analogno kao kod klasičnih kodova. Pokazat ćemo da je minimalna udaljenost dvaju potprostora metrika te proučiti mogućnosti otkrivanja i ispravljanja pogrešaka.

2 Klasična teorija kodiranja

Teorija kodiranja proučava učinkovite metode prijenosa informacija kroz kanal sa šumom. Tijekom prijenosa informacija putem kanala sa šumom javljaju se pogreške. Glavni cilj teorije kodiranja, za razliku od kriptografije, je pouzdano slanje informacija kroz komunikacijske kanale odnosno detekcija i korekcija pogrešaka. Prvi zapis o teoriji kodiranja je članak Claudea Shannona 'A mathematical Theory of communication' iz 1948. godine.

Primjer 2.1. *ISBN (International Standard Book Number) je kod koji se dodjeljuje svakoj knjizi. Od 2007. godine se koristi 13 znamenkasti kod ISBN-13. Prije se koristio 10 znamenkasti kod ISBN-10. ISBN-13 se sastoji od 12 znamenki koje jednoznačno određuju 13. odnosno kontrolnu znamenku. Posljednja znamenka predstavlja zalihost. Knjigama sa ISBN-10 kodom je 10. znamenka bila kontrolna. Prilikom prelaska na ISBN-13 svim knjigama sa ISBN-10 kodom je dodan prefiks 978 te je ponovno izračunata kontrolna znamenka (ne nužno jednaka 10. znamenki u ISBN-10 zapisu). Formula kojom se računa kontrolna znamenka je* $x_{13} = (x_1 + 3x_2 + x_3 + 3x_4 + x_5 + 3x_6 + x_7 + 3x_8 + x_9 + 3x_{10} + x_{11} + 3x_{12}) \pmod{10}$*, pri čemu je* x_i *znamenka na i-tom mjestu u ISBN-13. Kontrolna znamenka nam omogućuje otkrivanje pogrešaka. Naprimjer, ako se znamenka na neparnom mjestu promijeni za a tijekom prijenosa kanalom kontrolna znamenka će se promijeniti za a* $\pmod{10} \neq 0, \forall a \in \{1, ..., 9\}$ *te ćemo otkriti pogrešku. Također vrijedi i za promjenu znamenki na parnim mjestima. Kod ne otkriva transpozicijske pogreške na parnim mjestima i neparnim mjestima, odnosno pogreške do kojih dolazi zamjenama znamenaka na određenim mjestima pri čemu se kontrolna znamenka ne promijeni. Npr. ako se zamijene znamenke na* 1. *i* 3. *mjeste te znamenke na* 2. *i* 4. *mjestu. No otkriva zamjene dvije znamenki od kojih je jedna na parnom mjestu, a druga na neparnom mjestu, posebno zamjene dvaju uzastopnih znamenki.*

OIB (osobni identifikacijski broj) i serijski brojevi novčanica također imaju kontrolnu znamenku koja omogućuje otkrivanje pogrešaka.



Slika 1: Skica komunikacijskog kanala

Na slici 2 je objašnjeno slanje poruka komunikacijskim kanalom. Sa izvora informacija se šalje poruka koja se pretvara u kodnu riječ. Kodna riječ se

prenosi komunikacijskim kanalom. Primljeni vektor se pomoću dekodera pretvara u poruku koju dobiva krajnji korisnik. Kod za ispravljanje pogrešaka se koristi kako bi poslana poruka bila jednaka dekodiranoj poruci, odnosno kako bi ispravili potencijalne promjene koje se mogu dogoditi tijekom slanja komunikacijskim kanalom. Prije nego što formalno definiramo kod za ispravljanje pogrešaka, definirajmo Hammingovu udaljenost.

Definicija 2.2. *Hammingova udaljenost vektora* $x = (x_1, ..., x_n)$ *i* $y = (y_1, \ldots, y_n)$ *se definira kao broj mjesta na kojima se razlikuju:*

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

Kod nazivamo *blokovnim kodom* ako se kodirana informacija može rastaviti u blokove duljine n. Blokove nazivamo *kodnim riječima*, a n je *duljina bloka*.

Definicija 2.3. *Neka je* Q *konačan skup koji se sastoji od* q *različitih elemenata. Kod* C *duljine* n *je podskup skupa* Q^n *svih uređenih* n*-torki elemenata iz* Q*. Elemente skupa* C *nazivamo kodnim riječima. Kod* C *ima parametre* (n, M, d, q)*. Pritom je* M *broj kodnih riječi* $(M = |C|)$*,a* d *je minimalna udaljenost koda,* $d(C) = min\{d(x, y) \mid x, y \in C, x \neq y\}$*.*

Skup Q još nazivamo abecedom, a njegove elemente slovima. Kod nazivamo prema veličini parametra q. Trivijalni kod za $q = 1$, binarni kod za $q = 2$, terarni kod za $q = 3$, a q-arni kod za proizvoljan $q \in \mathbb{N}$.

Propozicija 2.4. *Hammingova udaljenost je metrika na skupu* Q^n*.*

Dokaz. Nenegativnost $d(x, y) \geq 0$ i simetričnost $d(x, y) = d(y, x)$ očito vrijede. Također očito je $d(x, y) = 0$ ako i samo ako je $x = y$. Preostaje nam provjeriti nejednakost trokuta. Broj $d(x, y)$ interpretiramo kao minimalan broj promjena koje su dovoljne da iz x dobijemo y. Transformaciju možemo napraviti na više načina. Uzmimo proizvoljni vektor z iz Q^n. Prvo prebacimo x u z sa $d(x, z)$ promjena te onda z u y pomoću $d(z, y)$ promjena. Zbog minimalnosti dobivamo $d(x, y) \leq d(x, z) + d(z, y)$. □

Sada ćemo na jednostavnom primjeru promotriti problem dekodiranja.

Primjer 2.5. *Komunikacijskim kanalom želimo poslati poruku DA ili NE. Poruke šaljemo u obliku kodnih riječi 00000 kao NE te 11111 kao DA,* $C = \{00000, 11111\}$*. Poruke šaljemo kao nizove od pet slova kako bismo smanjili vjerojatnost pogreške. Ako je kodna riječ 11111 prenesena kao vektor 10110 dekoder ju ispravlja u „najbližu" kodnu riječ odnosno, 11111.*

Ispravak je uspio ukoliko je dekodirana poruka jednaka poruci koja je poslana sa izvora informacija. U primjeru 2.5 dekoder je promatrao Hammingove udaljenosti vektora 10110 od elemenata iz C 11111 i 00000. Izračunao je $d(10110, 11111) = 2 < d(10110, 00000) = 3$ te zbog toga ispravio primljeni vektor u kodnu riječ 11111. Metoda koju koristimo se naziva *metoda najbližeg susjeda*. Sada ćemo objasniti zašto smo smanjili vjerojatnost prenošenja pogrešne poruke povećanjem duljine niza, iako su nam bili dovoljni nizovi duljine jedan. Pretpostavimo da je vjerojatnost slanja pogrešnog slova kroz kanal $p = 0.01$. Kad bismo slali niz duljine $n = 1$, vjerojatnost da pošaljemo pogrešnu poruku bi bila p, dok bi za $n = 5$ vjerojatnost da je poruka pogrešno prenesena bila $\binom{5}{2}p^3(1-p)^2 + \binom{5}{1}p^4(1-p) + \binom{5}{0}p^5 \approx 0.00000985$. Zaključak je da bi slanjem niza duljine jedan krivo prenijeli otprilike 1 od 100 poruka, a slanjem niza duljine 5 slova približno 1 od 100000 poruka.

Teorem 2.6. *(i) Kod C može otkriti s ili manje pogrešaka u kodnoj riječi ako vrijedi $d(C) \geq s + 1$.*
(ii) Kod C može ispraviti t ili manje pogrešaka u kodnoj riječi ako vrijedi $d(C) \geq 2t + 1$.

Dokaz. (i) Pretpostavimo da vrijedi $d(C) \geq s+1$ i da je kodna riječ x prenesena sa s ili manje pogrešaka. Tada primljeni vektor ne može biti neka druga kodna riječ jer je s manji od minimalne udaljenosti, stoga možemo otkriti pogreške.
(ii) Sada pretpostavimo da vrijedi $d(C) \geq 2t + 1$ i da je kodna riječ x prenesena kao vektor y sa t ili manje pogrešaka. Tvrdimo da za bilo koju kodnu riječ $x' \in C, x' \neq x$ vrijedi $d(x', y) \geq t + 1$. Pretpostavimo suprotno, $d(x', y) \leq t$. Hammingova udaljenost je metrika pa vrijedi nejednakost trokuta odnosno $d(x, x') \leq d(x, y) + d(x', y) \leq 2t$, što je kontradikcija. Dakle, x je „najbliža" kodna riječ vektoru y, tj. uvijek možemo ispraviti t ili manje pogrešaka. □

Korolar 2.7. *Ako kod C ima minimalnu udaljenost d, tada C može:*
(i) pronaći $d - 1$ ili manje pogrešaka,
(ii) ispraviti $\lfloor \frac{d-1}{2} \rfloor$ ili manje pogrešaka.

Propozicija 2.8. *(Ocjena pakiranja kugli) Neka je C (n, M, d, q) i $e = \lfloor \frac{d-1}{2} \rfloor$, tada vrijedi*

$$M \leq \frac{q^n}{\Sigma_{i=0}^{e} \binom{n}{i}(q-i)^i}. \tag{1}$$

Dokaz. Promotrimo skup $K(x, e) = \{y \in Q^n \mid d(x, y) \leq e\}$, pri čemu je d Hammingova udaljenost (metrika). Skup $K(x, e)$ je kugla polumjera e u metričkom prostoru Q^n. Broj vektora udaljenih od x za i je jednak $\binom{n}{i}(q-i)^i$.

Kugle sa središtima u kodnim riječima $x \in C$ su međusobno disjunktne (inače bi kodne riječi bile udaljene manje od d). Zbog toga umnožak broja kodnih riječi i broj vektora u kugli ne može biti veći od ukupnog broja vektora. $\square$

Kodove koji dostižu ocjenu pakiranja kugli nazivamo *savršenim kodovima*. Takvi kodovi imaju svojstvo da za svaki primljeni vektor $y \in Q^n$ postoji jedinstvena kodna riječ $x \in C$ takva da je $d(x, y) \leqslant e$.

2.1 Linearni kodovi

Kodiranje i dekodiranje su jednostavniji ako imamo neku algebarsku strukturu. Neka je q prim potencija ($q = p^d$, p prim broj) i neka je Q abeceda. Skup Q možemo snabdjeti strukturom konačnog polja. Konačno polje je polje koje sadrži konačan broj elemenata, broj elemenata nazivamo red polja. Konačno polje se označava $\mathbb{F}_q$, pri čemu je q red polja. Podsjetimo se sada definicije polja.

Definicija 2.9. *Polje $(F, +, \cdot)$ je neprazan skup F s binarnim operacijama zbrajanja i množenja koje zadovoljavaju sljedeće uvjete za sve $a, b, c \in F$:*

1. $a + b = b + a, \quad a \cdot b = b \cdot a$ *(komutativnost)*
2. $a + (b + c) = (a + b) + c, \quad a(bc) = (ab)c$ *(asocijativnost)*
3. $a \cdot (b + c) = a \cdot b + a \cdot c$ *(distributivnost)*
4. $a + 0 = a$ *(neutralni element za zbrajanje)*
5. $a \cdot 1 = a$ *(neutralni element za množenje)*
6. $\forall a \in F, \exists(-a) \in F \quad t.d. \quad a + (-a) = 0$
7. $\forall a \in F \setminus \{0\}, \exists(a^{-1}) \in F \quad t.d. \quad a \cdot a^{-1} = 1.$

Najmanje konačno polje sadrži samo dva elementa. Iz definicije znamo da polje mora sadržavati neutralne elemente za zbrajanja (0) i množenja (1). Operaciju množenja definiramo kao kod cijelih brojeva, dok zbrajanje definiramo kao operaciju zbrajanja modulo 2 ($1 + 1 = 0$). Polje na skupu $\{0, 1\}$ sa operacijama zbrajanje modulo 2 i množenje označavamo sa $\mathbb{Z}_2$. Općenito, ako je m prim broj tada je $\mathbb{Z}_m$ konačno polje.

Primjer 2.10. *(a) $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$ s operacijama zbrajanja i množenja modulo 5 je polje. Neutralni element za zbrajanje je 0, neutralni element za množenje je 1, a 1 i 4 su sami sebi inverz za množenje te 2 i 3 su međusobno inverzni.*

(b) $\mathbb{Z}_{11}$ *s operacijama zbrajanja i množenja modulo* 11 *je također polje. Elementi* 1 *i* 10 *su sami sebi inverzni za množenje, a* 2 *i* 6, 3 *i* 4, 5 *i* 9 *te* 7 *i* 8 *su međusobno inverzni za množenje.*

Sada iskazujemo teorem koje karakterizira egzistenciju konačnih polja.

Teorem 2.11. *Polje reda q postoji ako i samo ako je q prim potencija. Za svaku prim potenciju q postoji samo jedno polje reda q do na izomorfizam.*

Sada formalno definiramo linearni kod. Neka je abeceda $Q = \mathbb{F}_q$ i $Q^n = \mathbb{F}_q^n = \{(x_1, ..., x_n) \mid x_i \in Q, 1 \leq i \leq n\}$ vektorski prostor nad $\mathbb{F}_q$ sa operacijama zbrajanja $(x_1, ..., x_n) + (y_1, ..., y_n) = (x_1 + y_1, ..., x_n + y_n)$ i množenja skalarom $\alpha(x_1, ..., x_n) = (\alpha x_1, ..., \alpha x_n), \forall \alpha \in Q$.

Definicija 2.12. *Linearni kod s parametrima* $[n, m, d, q]$ *je m-dimenzionalni potprostor* $C \leq Q^n$ *n-dimenzionalnog vektorskog prostora* Q^n*. Pritom je d minimalna udaljenost.*

Vektorski potprostor je podskup vektorskog prostora Q^n koji je zatvoren na operacije zbrajanja (aditivnost) i množenja skalarom (homogenost). Parametre linearnog koda pišemo u uglatim zagradama te drugi parametar više nije broj kodnih riječi nego dimenzija potprostora C. Linearne kodove često označavamo samo sa $[n, k]$ ili sa $[n, k, d]$ ako imamo minimalnu udaljenost. Umjesto minimalne udaljenosti kod linearnih kodova možemo gledati minimalnu težinu kodnih riječi.

Definicija 2.13. *Težina vektora* $x \in Q^n$ *je broj koordinata različitih od nule:* $w(x) = |\{i \mid x_i \neq 0\}|$*. Minimalna težina koda je broj min* $\{w(x) \mid x \in C, x \neq 0\}$.

Lema 2.14. *Ako su* $x, y \in Q^n$*, tada je* $d(x, y) = w(x - y)$.

Dokaz. Vektor $x - y$ nema nulu samo na mjestima gdje se x i y razlikuju. □

Teorem 2.15. *Neka je C linearni kod i* $w(C)$ *minimalna težina koda C. Tada je* $d(C) = w(C)$.

Dokaz. Postoje kodne riječi $x, y \in C$ takve da je $d(C) = d(x, y)$. Tada po lemi 2.14 vrijedi $d(C) = w(x - y) \geq w(C)$, jer je $x - y$ također kodna riječ linearnog koda C. Obratno, za kodnu riječ $x \in C$ vrijedi $w(C) = d(x, 0) \geq d(C)$. Nulvektor je element koda C jer je C potprostor vektorskog prostora. Stoga vrijedi $w(C) = d(C)$. □

Definicija 2.16. *Generirajuća matrica* $[n, k]$*-koda C je matrica G reda* $k \times n$ *čiji su retci baza od C.*

Ako je G generirajuća matrica koda C iz definicije zaključujemo da vektore koda možemo dobiti kao linearne kombinacije vektora redaka matrice G, odnosno $C = \{aG \mid a \in Q^k\}$. Generirajuća matrica koda nije jedinstvena. Generirajuća matrica G je u *standardnom obliku* ako je oblika $[I_k \ P]$, pri čemu je I_k jedinična matrica reda k te P je matrica reda $k \times (n-k)$ koja predstavlja zalihost.

Primjer 2.17. *(a) Matrica* $G = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ *je generirajuća matrica linearnog* $[3, 2, 2]$*-koda nad poljem* $\mathbb{F}_2$*. Matrica* $G' = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 1 & 0 \end{bmatrix}$ *je također generirajuća matrica istog koda.*
(b) Mrežom želimo poslati broj. Svaku znamenku možemo prikazati u $4-$*bitnom binarnom zapisu, a* 5*. znamenka će predstavljati bit parnosti. Generirajuća matrica je* $G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{bmatrix}$*. Pretpostavimo da želimo poslati broj* 146*. Znamenke dobivamo množeći matricu* G *s vektorima* $\begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix}$, $\begin{bmatrix} 0 & 1 & 0 & 0 \end{bmatrix}$ *i* $\begin{bmatrix} 0 & 1 & 1 & 0 \end{bmatrix}$*. Tada bismo poslali blokovni kod* 000110100101100 *mrežom čijih bi prvih* 5 *znamenki predstavljalo broj* 1*, drugih pet* 4 *te trećih pet* 6*.*

Sada ćemo formalno pokazati kako različite generirajuće matrice mogu predstavljati iste kodove. Prvo definiramo ekvivalentnost kodova.

Definicija 2.18. *Kodovi* $C_1, C_2 \subseteq \mathbb{F}_q^n$ *su ekvivalentni ako se kodne riječi jednog od kodova mogu dobiti permutacijama na pojedinim koordinatama kodnih riječi drugog koda te permutiranjem simbola iz abecede na pojedinim koordinatama. Permutacije se izvršavaju istovremno na svim kodnim riječima.*

Definicija 2.19. *Linearni kodovi* $C_1, C_2 \leq \mathbb{F}_q^n$ *su ekvivalentni ako kodne riječi jednog od kodova možemo dobiti permutiranjem koordinata kodnih riječi drugog koda te množenjem elemenata na pojedinim koordinatama drugog koda nenul skalarom* $\alpha \in \mathbb{F}_q$*.*

Teorem 2.20. *Dvije* $k \times n$ *matrice generiraju ekvivalentne linearne kodove ako se iz jedne matrice može dobiti druga pomoću operacija:*
(a) permutacijom redaka
(b) množenjem redaka nenul skalarom
(c) dodavanjem retka pomnoženog skalarom drugom retku
(d) permutacijom stupaca
(e) množenjem stupca nenul skalarom

Dokaz. Operacije $(a)-(c)$ su elementarne transformacije nad retcima i njima ne mijenjamo potprostor. Operacije (d) i (e) su iste kao u definiciji 2.19. □

Korolar 2.21. *Neka je G generirajuća matrica linearnog $[n,k]$ koda. Tada generirajuću matricu operacijama iz teorema 2.20 možemo dovesti u standardni oblik.*

Dokaz. Operacijama iz teorema 2.20 bilo koju matricu reda $k \times n$ ranga k možemo svesti na matricu standardnog oblika $\begin{bmatrix} I_k & P \end{bmatrix}$. □

Korolar pokazuje da su različite generirajuće matrice istog koda povezane preko standardnog oblika. Npr. u primjeru 2.17 obe matrice možemo pretvoriti u matricu $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{bmatrix}$ koja je u standardnom obliku.

Definicija 2.22. *Produkt vektora $x = (x_1, x_2, \ldots, x_n), y = (y_1, y_2, \ldots, y_n) \in \mathbb{F}_q^n$ definiramo kao $x \cdot y = \Sigma_{i=1}^n x_i y_i$. Kažemo da su vektori ortogonalni ako vrijedi $x \cdot y = 0$.*

Produkt nad $\mathbb{F}_q^n$ nema ista svojstva kao skalarni produkt, ali ima slična. Pozitivnost nema smisla promatrati jer nemamo uređaj. Svojstvo $x \cdot x = 0 \iff x = 0$ npr. u $\mathbb{F}_2$ ne vrijedi jer je $x \cdot x = 1 + 1 = 0$, za $x = (1,1)$. Simetričnost $x \cdot y = y \cdot x, \forall x, y \in \mathbb{F}_q^n$, distributivnost $(x + y) \cdot z = x \cdot z + y \cdot z, \forall x, y, z \in \mathbb{F}_q^n$ i kvaziasocijativnost $(\alpha x) \cdot y = \alpha(x \cdot y), \forall \alpha \in \mathbb{F}_q, \forall x, y \in \mathbb{F}_q^n$ vrijede.

Definicija 2.23. *Neka je $C \leqslant \mathbb{F}_q^n$ linearni kod. Dualni kod $C^\perp$ linearnog koda C definiramo kao:*

$$C^\perp = \left\{ x \in \mathbb{F}_q^n : x \cdot y = 0, \forall y \in C \right\}.$$

Teorem 2.24. *Neka je $\mathbb{F}_q^n$ konačno polje te neka je $C \leqslant \mathbb{F}_q^n$ linearni $[n,k]$-kod. Tada je $C^\perp$ linearni $[n, n-k]$-kod.*

Dokaz. Prvo želimo pokazati da je $C^\perp$ linearan. Neka su $x_1, x_2 \in C^\perp, \alpha, \beta \in \mathbb{F}_q$, tada za svaki $y \in C$ vrijedi $(\alpha x_1 + \beta x_2) \cdot y = \alpha x_1 \cdot y + \beta x_2 \cdot y = \alpha \cdot 0 + \beta \cdot 0 = 0$. Preostaje nam još pokazati da je dimenzija dualnog koda $n - k$. Neka je G generirajuća matrica, a $r_1, r_2, \ldots, r_k$ retci od G. Za $x \in \mathbb{F}_q^n$ vrijedi da je u $C^\perp$ ako i samo ako je $x \cdot r_i = 0$, za svaki $i \in \{1, \ldots, k\}$. Element $x \in C^\perp$ mora biti ortogonalan na sve vektore iz C odnosno mora vrijediti $x \cdot \Sigma_{i=1}^k \alpha_i r_i = 0$ za proizvoljne skalare iz $\mathbb{F}_q$. Zbog linearnosti imamo $x \cdot \Sigma_{i=1}^k \alpha_i r_i = \Sigma_{i=1}^k \alpha_i (x \cdot r_i) = \Sigma_{i=1}^k (\alpha_i \cdot 0) = 0$. Dobivamo da je potprostor $C^\perp$ rješenje homogenog sustava k linearnih jednadžbi, $xG = 0$. Zbog linearne nezavisnosti vektora $r_1, r_2, \ldots, r_k$ rješenje je $n - k$ dimenzionalni potprostor od $\mathbb{F}_q^n$. Stoga je $\dim(C^\perp) = n - k$.

□

Primjer 2.25. *Promotrimo sada linearne kodove nad poljem* $\mathbb{F}_2$.
(a) Neka je $C = \{0000, 1100, 0011, 1111\}$ *, tada je* $C = C^{\perp}$.
(b) Neka je $C = \{000, 110, 011, 101\}$ *, tada je* $C^{\perp} = \{000, 111\}$.

Teorem 2.26. *Neka je* $C \leqslant \mathbb{F}_q^n$ *linearni* $[n, k]$*-kod. Tada je* $(C^{\perp})^{\perp} = C$.

Dokaz. Znamo da je $C \subseteq (C^{\perp})^{\perp}$ jer su svi elementi iz C ortogonalni na elemente iz $C^{\perp}$. Za dimenziju vrijedi sljedeće: $\dim((C^{\perp})^{\perp}) = n-(n-k) = k$. Zbog toga što je C podskup od $(C^{\perp})^{\perp}$, a $(C^{\perp})^{\perp}$ ima istu dimenziju kao C slijedi tvrdnja. □

Definicija 2.27. *Neka je* $C \leqslant \mathbb{F}_q^n$ *linearni kod. Matrica provjere parnosti koda* C *je generirajuća matrica dualnog koda* $C^{\perp}$.

Neka je G generirajuća matrica $[n, k]$-koda C te neka je H $(n-k) \times n$ matrica koja zadovoljava $GH^T = 0$, pri čemu 0 predstavlja nulmatricu. Tada po teoremu 2.26 kod C možemo zapisati pomoću matrice provjere parnosti $C = \left\{x \in \mathbb{F}_q^n \mid xH^T = 0\right\}$. Znači da je linearni kod u potpunosti određen matricom provjere parnosti. Npr. u primjeru 2.25 (a) matrica $\begin{bmatrix} 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}$ je generirajuća matrica koda te istovremeno matrica provjere parnosti. Dok je u 2.25 (b) matrica provjere parnosti $\begin{bmatrix} 1 & 1 & 1 \end{bmatrix}$.

Teorem 2.28. *Ako je* $G = [I_k \mid P]$ *generirajuća matrica lineranog* $[n, k]$*-koda u standardnom obliku, tada je matrica provjere parnosti jednaka* $H = [-P^T \mid I_{n-k}]$.

Dokaz. Znamo da vrijedi $GH^T = \begin{bmatrix} I_k & P \end{bmatrix} \cdot \begin{bmatrix} -P \\ I_{n-k} \end{bmatrix} = -P + P = 0$. Zaključujemo da su retci matrice H ortogonalni na retke generirajuće matrice G pa razapinju potprostor od $C^{\perp}$. Retci razapinju $n-k$ dimenzionalni potprostor, a po teoremu 2.24 znamo da je $\dim(C^{\perp}) = n-k$. Zbog toga slijedi da retci razapinju $C^{\perp}$. □

Za matricu provjere parnosti kažemo da je u *standardnom obliku* ako je oblika $H = [-P^T \mid I_{n-k}]$ te teorem govori da onda imamo generirajuću matricu koda $G = [I_k \mid P]$. Mnogi kodovi se lakše definiraju pomoću matrice provjere parnosti, npr. Hammingovi kodovi koje ćemo upoznati u idućoj cjelini.

U binarnom kodu možemo zanemariti negativni predznak u matrici provjere parnosti jer u $\mathbb{F}_2$ vrijedi $-1 = 1$.

Primjer 2.29. *Neka je generirajuća matrica linearnog koda*

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

tada je

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

Propozicija 2.30. *Neka je C linearni kod s pripadnom matricom provjere parnosti H. Minimalna težina koda C jednaka je minimalnom broju linearno zavisnih stupaca matrice H. Točnije, minimalna težina od C jednaka je d ako i samo ako u H postoji d linearno zavisnih stupaca, a bilo kojih $d-1$ stupaca od H su linearno nezavisni.*

Dokaz. Prepostavimo da je težina od C jednaka d. Neka su $h_1, \ldots, h_n$ stupci matrice H i $x \in \mathbb{F}_q^n$. Znamo da je $x \in C$ ako i samo ako vrijedi $xH^T = 0$, odnosno $x_1h_1 + \ldots + x_nh_n = 0$. Uzmimo sada $x \in C$ takav da je $w(x) = d$, dobivamo d linearno zavisnih stupaca.

Obratno, pretpostavimo da je d minimalni broj linearno zavisnih stupaca u H. Tada postoje indeksi $i_1, \ldots, i_d$ i skalari $x_{i_1}, \ldots, x_{i_d}$ takvi da je $x_{i_1}h_{i_1} + \ldots + x_{i_d}h_{i_d} = 0$. Za vektor x koji na mjestima $i_1, \ldots, i_d$ ima skalare $x_{i_1}, \ldots, x_{i_d}$, a na ostalim mjestima 0 vrijedi $xH^T = 0$. Time smo dobili da je $x \in C$, pa je $w(C)$ manja ili jednaka od minimalnog broja linearno zavisnih stupaca čime smo dokazali jednakost. □

2.2 Hammingovi kodovi

Hammingovi kodovi su linearni kodovi koji služe za detekciju i ispravljanje jednostrukih pogrešaka. Propozicija 2.30 nam otkriva na koji način bismo mogli definirati klasu kodova minimalne težine 3 pomoću matrice provjere parnosti. Kod je jednostavno odrediti pomoću matrice provjere parnosti pa ćemo prvo definirati tu matricu.

Neka je $r \in \mathbb{N}$, H je $r \times (q^r - 1)/(q - 1)$ matrica te $Q = \{\alpha_0 = 0, \alpha_2 = 1, \ldots, \alpha_{q-1}\}$. Za stupce od H uzimamo sve vektore kojima je vodeća nenul koordinata jednaka 1. Prvi stupac ima vodeću jedinicu na r. koordinati, idućih q stupaca ima vodeću jedinicu na $(r-1)$. koordinati, ..., posljednjih q^{r-1} stupaca ima jedinicu na prvoj koordinati. Time smo dobili matricu provjere parnosti oblika:

$$H = \begin{bmatrix} 0 & 0 & 0 & 0 & \dots & 0 & \dots\dots & 1 & 1 & 1 & \dots & 1 \\ 0 & 0 & 0 & 0 & \dots & 0 & \dots\dots & 0 & 0 & 0 & \dots & \alpha_{q-1} \\ \vdots & \vdots & \vdots & \vdots & & \vdots & & \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & 1 & 1 & \dots & 1 & \dots\dots & 0 & 0 & 0 & \dots & \alpha_{q-1} \\ 1 & 0 & 1 & \alpha_2 & \dots & \alpha_{q-1} & \dots\dots & 0 & 1 & \alpha_2 & \dots & \alpha_{q-1} \end{bmatrix}. \qquad (2)$$

Matricu H smo definirali tako da su svaka dva stupca međusobno linearno nezavisna, a tri stupca mogu biti linearno zavisna pa prema propoziciji 2.30 zaključujemo da je minimalna težina koda jednaka 3. Duljina koda je $n = (q^r - 1)/(q - 1)$, to jest broj stupaca matrice H. Po teoremu 2.24 dimenzija koda je $n - r$.

Definicija 2.31. *Linearni kod nad poljem $\mathbb{F}_q$ definiran matricom provjere parnosti oblika* (2) *sa parametrima $[(q^r - 1)/(q - 1), (q^r - 1)/(q - 1) - r, 3, q]$ nazivamo* Hammingov kod *s parametrima (r, q), kraće ga označavamo* $\mathrm{Ham}(r, q)$.

Primjer 2.32. *(a) Matrica provjere parnosti koda* $\mathrm{Ham}(2, 2)$ *je*

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

a po teoremu 2.28 *generirajuća matrica je*

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

Ovaj kod se podudara s kodom kod kojeg bitove ponavljamo tri puta.
(b) Za kod $\mathrm{Ham}(3, 2)$ *imamo matricu*

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

koju također možemo zapisati u obliku

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

Prema teoremu 2.28 generirajuća matrica je

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

Teorem 2.33. *Hammingov kod je savršen.*

Dokaz. Tvrdnju dokazujemo koristeći nejednakost (1). Pokazat ćemo da vrijedi $M = \frac{q^n}{\Sigma_{i=0}^{e}\binom{n}{i}(q-i)^i}$. Parametri $Ham(r,q)$ su $k = \frac{q^r-1}{q-1} - r$, $n = \frac{q^r-1}{q-1}$ i $M = q^k$ pa imamo $1 + \binom{n}{1}(q-1) = q^{n-k}\binom{n}{i} \iff 1 + \frac{q^r-1}{q-1}(q-1) = q^r$. □

2.3 Reed-Mullerovi kodovi

Reed-Mullerovi kodovi jedni su od najstarijih kodova. Otkrio ih je David Eugene Muller, a algoritam za dekodiranje je otkrio Irving Stoy Reed 1954. godine. Kodovi su prvotno bili binarni, a kasnije su generalizirani za svaku prim potenciju q. Mi ćemo se fokusirat isključivo na binarne. Reed-Mullerovi kodovi se mogu definirati na više načina. Mi ćemo ih definirati rekurzivno.

Neka su $m \in \mathbb{N}$ i $r \in \mathbb{N}$ takvi da vrijedi $0 \leqslant r \leqslant m$. Definirat ćemo postepeno Reed-Mullerov kod reda r, kojeg označavamo sa $\mathcal{R}(r,m)$. Vektor sastavljen od samih jedinica označavat ćemo $j = (1,\ldots,1)$.

Definicija 2.34. *Reed-Mullerov kod reda* 1 $\mathcal{R}(1,m)$ *je binarni linearni kod definiran za svaki* $m \in \mathbb{N}$ *rekurzivno sa:*

(i) $\mathcal{R}(1,1) = \{00, 01, 10, 11\}$,
(ii) $\mathcal{R}(1,m) = \{(u,u), (u,u+j) \mid u \in \mathcal{R}(1,m-1)\}, \forall m \geqslant 2.$

Primjer 2.35. *(i)* $\mathcal{R}(1,2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$.
(ii) $\mathcal{R}(1,3) = \{00000000, 01010101, 10101010, 11111111, 00110011, 01100110, 10011001, 11001100, 00000111, 01010010, 10101101, 11111000, 00110100, 01100001, 10011110, 11001011\}$.

Kod smo definirali kao linearan, ali nismo naveli parametre koda. Sljedeći teorem nam pomaže u određivanju parametara Reed-Mullerovog koda.

Teorem 2.36. *Neka je* C_1 *linearni* $[n, k_1, d_1, q]$*-kod i* C_2 *linearni* $[n, k_2, d_2, q]$*-kod. Tada je kod definiran sa*

$$C = \{(u, u+v) \mid u \in C_1, v \in C_2\}$$

linearni $[2n, k_1 + k_2, min\{2d_1, d_2\}, q]$*-kod.*

Dokaz. Primijetimo kako je duljina koda C jednaka $n+n=2n$. Kako bi odredili dimenziju koda definiramo funkciju $f : C_1 \times C_2 \to C$ kao preslikavanje $f(c_1, c_2) = (c_1, c_1 + c_2),\ c_1 \in C_1, c_2 \in C_2$. Funkcija f je bijekcija pa znamo da je veličina od C jednaka veličini od $C_1 \times C_2$. Veličina od $C_1 \times C_2$ je $q^{k_1}q^{k_2} = q^{k_1+k_2}$, iz čega dobivamo je dimenzija od C jednaka $k_1 + k_2$. Preostaje nam još odrediti minimalnu težinu. Uzmimo sada nenul vektor $(c_1, c_1 + c_2) \in C$. Ako je $c_2 = 0$ tada imamo $w((c_1, c_1 + c_2)) = w((c_1, c_1)) = 2w(c_1) \geqslant 2d_1 \geqslant min\{2d_1, d_2\}$. U slučaju $c_2 \neq 0$ imamo $w((c_1, c_1 + c_2)) = w(c_1)+w(c_1+c_2) \geqslant w(c_1)+w(c_2)-w(c_1) \geqslant w(c_2) \geqslant d_2 \geqslant min\{2d_1, d_2\}$. Ako sa d označimo minimalnu težinu od C dobili smo $d \geqslant min\{2d_1, d_2\}$. Obratno, uzmimo $x \in C_1$ takav da je $w(x) = d_1$ i $y \in C_2$ takav da je $w(y) = d_2$. Tada su $(x, x), (0, y) \in C$ te vrijedi $w((x, x)) = 2d_1$ i $w((0, y)) = d_2$ pa vrijedi $d \leqslant min\{2d_1, d_2\}$. Time smo dobili jednakost $d = min\{2d_1, d_2\}$. □

Sada smo spremni odrediti parametre Reed-Mullerovog koda.

Propozicija 2.37. *Neka je $m \in \mathbb{N}$, tada je Reed-Mullerov kod $\mathcal{R}(1, m)$ binarni linearni $[2^m, m + 1, 2^{m-1}]$-kod, kojemu su sve kodne riječi težine 2^{m-1} izuzevši vektor j i nulvektor.*

Dokaz. Tvrdnju dokazujemo indukcijom. Za $\mathcal{R}(1, 1)$ znamo da je $[2, 2, 1]$-kod. Pretpostavimo sada da je $\mathcal{R}(1, m-1)$ $[2^{m-1}, m, 2^{m-2}]$-kod. Uzmimo da je $C_1 = \mathcal{R}(1, m-1)$ te $C_2 = \mathcal{R}(0, 1) = \{00\ldots0, 11\ldots1\}$. Za C_2 vrijedi $dimC_2 = 1$ i $w(C_2) = 2^{m-1}$. Pa po konstrukciji iz teorema 2.36 slijedi da je $\mathcal{R}(1, m)$ linearni $[2^m, m + 1, min\{2 \cdot 2^{m-2}, 2^{m-1}\}]$-kod.

Preostaje nam pokazati da je težina svih kodnih riječi osim nulvektora i vektora j jednaka 2^{m-1}. Kodna riječ koda $\mathcal{R}(1, m)$ može biti oblika (u, u) ili $(u, u + j)$, pri čemu je $u \in \mathcal{R}(1, m-1)$. Ako je oblika (u, u) tada u nije 0 ili j jer bi kodna riječ iz $\mathcal{R}(1, m)$ također bila 0 ili j. Za neku drugu proizvoljnu kodnu riječ vrijedi $w((u, u)) = 2w(u) = 2 \cdot 2^{m-2}$. Ako je kodna riječ oblika $(u, u + j)$ imamo sljedeće slučajeve. Prvi slučaj je $u = 0$, tada je $w((0, j)) = 2^{m-1}$. Drugi slučaj za $u = j$ vrijedi $w((j, 0)) = 2^{m-1}$. U općem slučaju kada je u različit od 0 i j imamo $w((u, u + j)) = w(u) + w(u + j) = 2^{m-2} + (2^{m-1} - 2^{m-2}) = 2^{m-1}$. Time smo dokazali tvrdnju o težinama. □

Generirajuće matrice Reed-Mullerovih kodova definiramo također rekurzivno. Lako ih intuitivno konstruiramo po uzoru na rekurzivnu definiciju kodova. Za $\mathcal{R}(1, 1)$ imamo

$$G_1 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}.$$

Neka je G_m generirajuća matrica koda $\mathcal{R}(1,m)$, tada je generirajuća matrica $\mathcal{R}(1,m+1)$ jednaka

$$G_{m+1} = \begin{bmatrix} G_m & G_m \\ 0\ldots0 & 1\ldots1 \end{bmatrix}.$$

Sada definiramo Reed-Mullerove kodove reda r, za proizvoljan $r \in \mathbb{N}_0$.

Definicija 2.38. *Reed-Mullerov kod reda nula $\mathcal{R}(0,m) = \{0, j\}$ je kod duljine 2^m.*
Za $r \geqslant 2$, Reed-Mullerov $\mathcal{R}(r,m)$ definiramo rekurzivno:

$$\mathcal{R}(r,m) = \begin{cases} \mathbb{Z}_2^{2r},\ m = r \\ \{(u, u+v) : u \in \mathcal{R}(r, m-1), v \in \mathcal{R}(r-1, m-1)\},\ m > r \end{cases}.$$

Ako imamo generirajuću matricu $G_{m,r}$ od $\mathcal{R}(r,m)$, tada je

$$G_{r+1,m+1} = \begin{bmatrix} G_{r+1,m} & G_{r+1,m} \\ 0 & G_{r,m} \end{bmatrix}. \tag{3}$$

Dimenzija od $\mathcal{R}(r,m)$ je

$$1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}. \tag{4}$$

Minimalna težina koda $\mathcal{R}(r,m)$ je 2^{m-r}.

Propozicija 2.39. *Kod $\mathcal{R}(m-1,m)$ se sastoji od kodnih riječi duljine 2^m koje imaju parnu težinu. Za $r < m$, kod $\mathcal{R}(r,m)$ također sadrži samo riječi parnih težina.*

Dokaz. Tvrdnju dokazujemo indukcijom. Za $\mathcal{R}(0,1) = \{00, 11\}$ vidimo da su kodne riječi težine 0 i 2. Pretpostavimo sada da tvrdnja vrijedi za kod $\mathcal{R}(m-2, m-1)$. Kodne riječi koda $\mathcal{R}(m-1,m)$ su oblika $(u, u+v)$ pri čemu je $u \in \mathcal{R}(m-1, m-1)$, a $v \in \mathcal{R}(m-2, m-1)$. Promotrimo sada $w((u,u+v)) = w((u,u)) + w((0,v)) - 2(u,u)\cdot(0,v)$, $w((u,u)) = 2w(u)$ te $2(u,u)\cdot(0,v)$ su parni, a $w((0,v))$ je paran po pretpostavci indukcije. Zbog $\mathcal{R}(r,m) \subseteq \mathcal{R}(m-1,m)$ slijedi drugi dio tvrdnje teorema. □

Teorem 2.40. *Kodovi $\mathcal{R}(m-r-1,m)$ i $\mathcal{R}(r,m)$ su međusobno dualni.*

Dokaz. Želimo dokazati ortogonalnost navedenih kodova indukcijom. Za $m = 2$, bez smanjenja općenitosti uzmimo da je $r = 0$. Imamo $\mathcal{R}(0,2) = \{0000, 1111\}$ i $\mathcal{R}(1,2) = \{0000, 0101, 1010, 1111, 0011, 0110, 1001, 1100\}$. Po propoziciji 2.39 sve kodne riječi iz $\mathcal{R}(1,2)$ imaju parnu težinu pa su ortogonalne na sve kodne riječi iz $\mathcal{R}(0,2)$. Prepostavimo sada da tvrdnja vrijedi

za $m-1$. Kako bi dokazali da tvrdnja vrijedi za m pokazat ćemo kako su generirajuće matrice međusobno ortogonalne. Po (3) imamo generirajuće matrice:

$$G_{m-r-1,m} = \begin{bmatrix} G_{m-r-1,m-1} & G_{m-r-1,m-1} \\ 0 & G_{m-r-2,m-1} \end{bmatrix} \quad G_{r,m} = \begin{bmatrix} G_{r,m-1} & G_{r,m-1} \\ 0 & G_{r-1,m-1} \end{bmatrix}.$$

Retci matrice $G_{m-r-1,m}$ oblika $(u,u), u \in \mathcal{R}(m-r-1,m-1)$ su ortogonalni na retke matrice $G_{r,m}$ oblika $(v,v), v \in \mathcal{R}(r,m-1)$ te na retke oblika $(0,v), v \in \mathcal{R}(r-1,m-1)$ po pretpostavci indukcije. Također po pretpostavci indukcije retci matrice $G_{r,m}$ oblika $(v,v), v \in \mathcal{R}(r,m-1)$ su ortogonalni na retke matrice $G_{m-r-1,m}$ oblika $(0,u), u \in \mathcal{R}(m-r-2,m-1)$. Konačno jer je $\mathcal{R}(m-r-2,m-1) \subseteq \mathcal{R}(m-r-1,m-1)$ vrijedi su retci matrice $G_{m-r-1,m}$ oblika $(0,u), u \in \mathcal{R}(m-r-2,m-1)$ ortogonalni na retke matrice $G_{r,m}$ oblika $(0,v), v \in \mathcal{R}(m-r-1,m-1)$. Ovime smo dobili $\mathcal{R}(m-r-1,m) \subseteq \mathcal{R}(r,m)^{\perp}$ pa po (4) imamo $dim(\mathcal{R}(r,m)^{\perp}) = 2^m - [1 + \binom{m}{1} + \binom{m}{2} + \ldots + \binom{m}{r}] = \binom{m}{r+1} + \binom{m}{r+2} + \ldots + \binom{m}{m} = \binom{m}{m-r-1} + \binom{m}{m-r-2} + \ldots + 1 = dim(\mathcal{R}(m-r-1,m))$. □

Teorija kodiranja je u povijesti imala veoma zanimljive primjene. Naprimjer, fotografije s Marsa su slane u obliku koda.

Primjer 2.41. *Mariner 9 je svemirska letjelica koja je 1971. godine lansirana u svemir. Letjelica je zabilježene fotografije slala kao Reed-Mullerove* $[32,6,16,2]$*-kodove, točnije* $\mathcal{R}(1,5)$*. Svaka slika je sadržavala* 700×832 *piksela. Kodne riječi su bile duljine* 32 *bita, prvih* 6 *bitova je predstavljalo svjetlinu (informaciju) dok je preostalih* 26 *bitova predstavljalo zalihost. Kod može ispraviti najviše 7 pogrešaka. Sada ćemo opisati kako se pogreške ispravljaju. Prvo od svih kodnih riječi napravimo vektore* ± 1*, jedinice ostavljamo dok* 0 *mijenjamo sa* -1*. Nakon toga računamo skalarni produkt primljenog vektora sa svim kodnim riječima, skalarni produkt računamo u* $\mathbb{R}^{32}$*. Ako je skalarni produkt s jednom od kodnih riječi veći od* 16 *onda primljeni vektor dekodiramo kao tu kodnu riječ. Ako se nije dogodila nijedna pogreška tada je skalarni produkt jednak* 32*, a sa bilo kojom drugom kodnom riječi skalarni produkt je* 0 *ili* -32*. To slijedi iz činjenice da je Hammingova udaljenost dviju kodnih riječi jednaka težini razlike tih dviju kodnih riječi koja može biti* 0*,* 16 *ili* 32*. U slučaju kada je* 0 *kodne riječi su jednake, a ako je* 32 *onda se kodne riječi ne poklapaju niti na jednoj koordinati odnosno skalarni produkt je* -32*. Ako je težina jednaka* 16*, tada je skalarni produkt jednak* $16-16=0$ *te se tada primljeni vektor i kodna riječ poklapaju na pola koordinata (*16 *koordinata). Za svaki pogrešno preneseni simbol skalarani produkt se smanjuje za* 2 *pa je skalarni produkt veći ili jednak od* 18 *ako je* 7 *ili manje simbola krivo preneseno, u suprotnom bi skalarni produkt bio manji ili jednak od* 16*.*

Promotrimo sada slučaj gdje imamo dvije kodne riječi iz Reed-Mullerovog $[32, 6, 16, 2]$-koda:

$$x = [10101010101010101010101010101010],$$
$$y = [11111111111111111111111111111111].$$

Ako vektore $x, y \in \mathcal{R}(1, 5)$ pretvorimo u ± 1 vektore kao u primjeru 2.41 dobivamo $x \cdot y = 16$. Komunikacijskim kanalom prenosimo vektor x, a primljeni vektor je

$$x' = [11111111111111111010101010101010].$$

Tada prebacimo x' također u ± 1 vektor te imamo $x \cdot x' = 16$, no također imamo $y \cdot x' = 16$ pa ne možemo ispraviti 8 pogrešaka (pogreške su na prvih 8 parnih koordinata u vektoru x. Sada uzmimo da se primljeni vektor razlikuje od x na prvih 7 parnih koordinata:

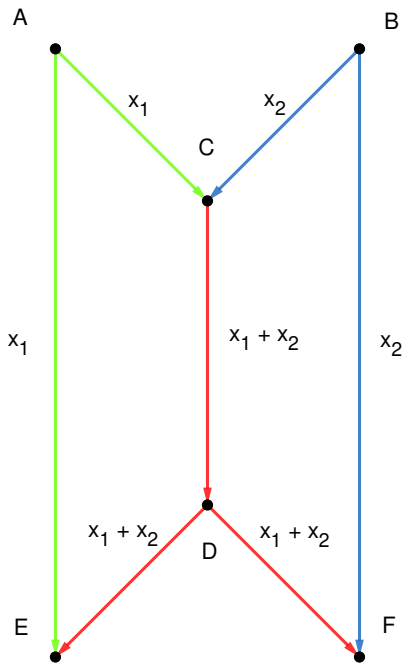
$$x'' = [11111111111111101010101010101010]$$

te ga pretvorimo u ± 1 vektor. Dobivamo $x \cdot x'' = 18$ te $y \cdot x'' = 14$ pa ga dekodiramo u x.

3 Osnove mrežnog kodiranja

Mrežno kodiranje je tehnika kodiranja podataka koja je nastala početkom 21. stoljeća. Cilj mrežnog kodiranja je povećanje propusnosti, smanjenje kašnjenja i robusnija mreža. Kod tradicionalnog usmjeravanja čvor koji prima više poruka od više različitih izvora primljene poruke prosljeđuje jednu po jednu. U mrežnom kodiranju poruke se linearno kombiniraju na posredničkim čvorovima te se spojene šalju do odredišta. Na odredištu se poruke dekodiraju kako bi dobili poslane poruke. Spajanjem poruka na posredničkim čvorovima izbjegavamo višestruki prijenos i povećamo protok kroz mrežu.

Sada demonstriramo prednosti mrežnog kodiranja pri *višesmjernom prijenosu podataka* (prema engleskom *multicasting*).



Slika 2: Butterfly network

Primjer 3.1. *Podatke šaljemo s dva izvora A i B k odredištima E i F. Svaki izvor emitira* 1 *bit po jedinici vremena, pripadne bitove označavamo sa* x_1 *i*

x_2. Ako E koristi sve mrežne resurse za sebe može prihvatiti oba bita. Bit x_1 šaljemo bridom AE, a x_2 usmjeravamo bridovima BC, CD, DE. Slično možemo usmjeriti bitove x_1 i x_2 na odredište F. Navedeni prijenos je jednosmjeran jer u jednom vremenskom intervalu bitovi stignu na jedno odredište. No, ako dopustimo da posrednički čvorovi kombiniraju bitove možemo postići da bitovi stignu na oba odredišta istovremeno. U jednosmjernom prijenosu bi npr. bit x_1 prvi prošao bridom CD prema F, nakon toga bi x_2 prošao istim bridom prema E. Pri višesmjernom prijenosu bit $x_1 + x_2$ prolazi istovremeno prema E i F čime dolazimo do bržeg prijenosa. Promotrimo sada usmjeravanje u višesmjernom prijenosu. U tom slučaju bit x_1 šaljemo direktno do E, također bit x_2 do F. Oba bita šaljemo i do čvora C. Umjesto da čvor C proslijedi samo jedan od bitova prosljeđuje $x_1 + x_2$ bridom CE. Nakon toga se od čvora D šalje do E i F. Promotrimo sada E, na to odredište su stigli bitovi $x_1 + x_2$ i x_1. Pomoću operacije isključivo ili (XOR), točnije operacije zbrajanja nad $\mathbb{F}_2$, možemo doći do bita x_2. Pretpostavimo da sa izvora šaljemo $x_1 = 1$ i $x_2 = 1$, tada na odredištu E imamo $x_1 = 1$ i $x_1 + x_2 = 0$. Sada koristimo isključivo ili kako bi izračunali $x_2 : 1 = x_1 + (x_1 + x_2) = 0 + x_2 = x_2$. Na sličan način dolazimo do bita x_1 na čvoru F. Stoga, bitovi x_1 i x_2 su poslani na oba odredišta samo jednim slanjem bitova x_1 i x_2 sa izvora. Inače bi prvo slali oba bita na odredište E, nakon toga na odredište F. Ovakvo usmjeravanje karakteristično za mrežno kodiranje je prikazano na slici 3.

Prikazali smo kako možemo povećati propusnost pri višesmjernom prijenosu dopuštajući da posrednički čvor C kombinira bitove. Ovaj primjer je generaliziran u glavnom teoremu višesmjernog prijenosa.

Mrežni višesmjerni prijenos predstavlja prijenos iste informacije u jednom vremenskom intervalu na više različitih odredišta u mreži. Zanimaju nas nužni i dovoljni uvjeti za višestruki prijenos pri određenoj brzini. Glavni teorem mrežnog kodiranja dokazuje zanimljivu činjenicu da su nužni i dovoljni uvjeti za jednosmjerni prijenos informacije na jedno odredište pri određenoj brzini jednaki nužnim i dovoljnim uvjetima za višesmjerni prijenos na više odredišta istom brzinom. Zbog toga prvo dokazujemo slučaj jednosmjernog prijenosa te nakon toga prelazimo na tvrdnju teorema. Teorem dokazujemo algebarski, no prvo uvodimo osnovne oznake koje koristimo u mrežnom kodiranju.

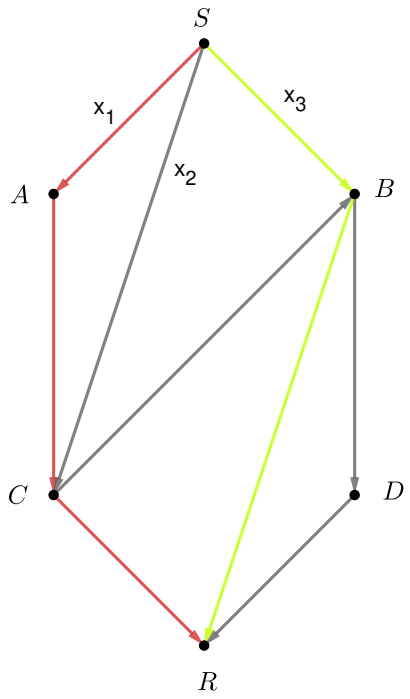
3.1 Teorem minimalnog reza i maksimalnog toka

Neka je $G = (V, E)$ graf (mreža) sa skupom vrhova V i skupom bridova $E \subseteq V \times V$. Pretpostavljamo da svi bridovi imaju jediničnu težinu te da su dopušteni višestruki bridovi. Promotrimo sada sljedeću situaciju, čvor $S \in V$

želi prenijeti informaciju do čvora $R \in V$.

Definicija 3.2. Rez *između vrhova R i S je skup bridova čijim uklanjanjem bi vrhovi postali nepovezani.* Minimalni rez *je rez s minimalnom vrijednošću. Vrijednost minimalnog reza je suma težina uklonjenih bridova.*

Vrijednost minimalnog reza za jedinične bridove je jednaka broju bridova u rezu. Minimalni rez slikovito možemo prikazati kao usko grlo odnosno maksimalnu količinu informacija koju možemo odjednom poslati kroz mrežu.



Slika 3: Jednosmjerni prijenos bridovima jedinične težine

Promotrimo sada sliku 3. Primijetimo kako je vrijednost minimalnog reza jedinstvena, dok postoji više minimalnih rezova (skupova). Vrijednost minimalnog reza je 3, a minimalni rezovi su $\{SA, SC, SB\}, \{CR, BR, BD\}, \{AC, SC, SB\}, \ldots$

Teorem 3.3. *Neka je $G = (V, E)$ mreža s bridovima jedinične težine, izvorom S i odredištem R. Vrijednost minimalnog reza jednaka je maksimalnom broju bridno disjunktnih puteva između S i R. Taj broj je maksimalna količina informacija koju možemo prenijeti istovremeno od S do R.*

Dokaz. Pretpostavimo da je vrijednost minimalnog reza između S i R jednaka h. Tada ne možemo naći više od h disjunktnih puteva, u suprotnom bi S i R ostali povezani nakon uklanjanja h bridova. Zbog toga je broj bridno disjunktnih puteva manji ili jednak od h. Sada pokazujemo obrat odnosno da je vrijednost minimalnog reza h manja ili jednaka od broja bridno disjunktnih puteva. Želimo pronaći h bridno disjunktnih puteva. Tražimo ih algoritmom *dodavanja puteva*. Definiramo varijablu p^e_{uv} koja je vezana uz brid e te vrhove u i v. Prvi korak je da postavimo p^e_{uv} na nulu za sve $e \in E$. U drugom koraku pronalazimo prvi put $P_1 = \{v^1_0 = S, v^1_1, .., v^1_{l_1} = R\}$ od S do R, pri čemu je l_1 duljina puta. Postavljamo $p^e_{v_i v_{i+1}} = 1$, za sve $i \in \{0, \ldots, l_1 - 1\}$ pri čemu je e brid između v_i i v_{i+1} (može biti više takvih bridova). U k-tom koraku tražimo put $P_k = \{v^k_0 = S, v^k_1, .., v^k_{l_k} = R\}$, za sve $k, (2 \leq k \leq h)$, od S do R sa duljinom puta l_k tako da su zadovoljeni uvjeti:

$$p^e_{v_i v_{i+1}} = 0 \quad \text{ili} \quad p^e_{v_{i+1} v_i} = 1, \ za\ 0 \leqslant i < l_k. \tag{5}$$

Varijable $p^e_{v_i v_{i+1}}$ ($p^e_{v_{i+1} v_i}$) postavljamo na 1 (0), za sve pripadujuće bridove puta P_k. Uvjet (5) garantira da koristimo bridove koji nisu bili korišteni do sada ili su korišteni u suprotnom smjeru (dopušteni su višestruki bridovi). Kako bi dokazali tvrdnju da je h manji ili jednak od maksimalnog broja bridno disjunktnih puteva moramo pokazati da algoritam može pronaći h bridno disjunktnih puteva. Pretpostavimo suprotno, za neki $k \in \{2 \ldots, h\}$ ne možemo pronaći put $P_k = \{v^k_0 = S, v^k_1, .., v^k_{l_k} = R\}$ takav da vrijedi (5). Sada rekurzivno definiramo skup $\mathcal{V} \subseteq V$. Na početku je $\mathcal{V}$ jednočlan skup koji sadrži samo izvor S. Nadalje, tražimo vrhove $u \in \mathcal{V}$ i $v \in V \setminus \mathcal{V}$ između kojih postoji brid $e \in E$ tako da zadovoljavaju (5) te takve vrhove dodajemo u $\mathcal{V}$. Nastavljamo s traženjem sve dok više ne postoje vrhovi $v \in V \setminus \mathcal{V}$ i $u \in \mathcal{V}$ te brid $e \in E$ koji zadovoljavaju (5). Po pretpostavci ne možemo naći put sa disjunktnim bridovima pa slijedi da $R \notin \mathcal{V}$ i $R \in \overline{\mathcal{V}} = V \setminus \mathcal{V}$. Definiramo $\partial\mathcal{V} = \{e \mid e = (u, v), u \in \mathcal{V}, v \in \overline{\mathcal{V}}\}$, skup svih bridova koji spajaju skupove $\mathcal{V}$ i $\overline{\mathcal{V}}$. Zbog načina konstrukcije skupa $\mathcal{V}$ za sve bridove $e = (u, v)$ iz $\partial\mathcal{V}$ vrijedi $p^e_{v_i v_{i+1}} = 0$ i $p^e_{v_{i+1} v_i} = 1$. Po pretpostavci da ne možemo naći k-ti bridno disjunktni put vrijedi $\Sigma_{e \in \partial\mathcal{V}} p^e_{uv} \leq k - 1$. Stoga je vrijednost minimalnog reza najviše $k - 1 < h$. Ako bi vrijednost minimalnog reza bila h tada bi vrijedilo $h \leqslant \Sigma_{e \in \partial\mathcal{V}} p^e_{uv}$. Time smo dobili kontradikciju s pretpostavkom da je vrijednost minimalnog reza jednaka h, čime smo dokazali teorem. □

3.2 Glavni teorem mrežnog kodiranja

Promatramo višesmjerni prijenos mrežom $G = (V, E)$ sa h izvora $S_1, ..., S_h$, koji se nalaze na istom vrhu, te N odredišta $R_1, ..., R_N$. Mreža G je aciklički usmjereni graf sa bridovima jedinične težine. Aciklički graf je graf u kojem ne postoji put čiji su početni i krajnji vrh jednaki. Pod bridovima jedinične težine podrazumijevamo da svaki brid prenese jedan element nekog konačnog polja $\mathbb{F}_q$ u jedinici vremena. U praksi se mrežom prenose bitovi, tj. elementi binarne abecede $\{0, 1\}$, no možemo pretpostaviti da je $q = 2^m$ te da informacije šaljemo u paketima od m bitova. Tih m bitova su jedan simbol iz $\mathbb{F}_q$ nad kojim se odvijaju operacije tijekom prijenosa kroz mrežu. Takav način prijenosa kroz mrežu nazivamo shemom. Pod dovoljno velikim konačnim poljem $\mathbb{F}_q$ podrazumijevamo da postoji dovoljno veliki paket za prijenos informacija, odnosno da svaku informacija možemo prenijeti kao paket od m bitova. Sada iskazujemo glavni teorem mrežnog kodiranja.

Teorem 3.4. *Pretpostavimo da je minimalni rez od vrha u kojem su smješteni izvori do svakog odredišta jednak h. Tada postoji shema višesmjernog prijenosa koristeći dovoljno veliko konačno polje $\mathbb{F}_q$, u kojoj posrednički čvorovi stvaraju linearne kombinacije informacija nad $\mathbb{F}_q$, koja prenosi informaciju (skup od h simbola) istovremeno do N odredišta.*

Po teoremu 3.3 postoji h disjunktnih puteva između izvora i odredišta. Ako informacije šaljemo samo do jednog odredišta možemo korisiti resurse čitave mreže te je prijenos jednostavan. No kada informacije šaljemo istovremeno prema više odredišta dolazi do preklapanja puteva. Zbog toga je intuitivno da odredišta dijele resurse. Kombinirajući podatke na posredničkim čvorovima možemo istovremeno prenositi informacije na više odredišta.

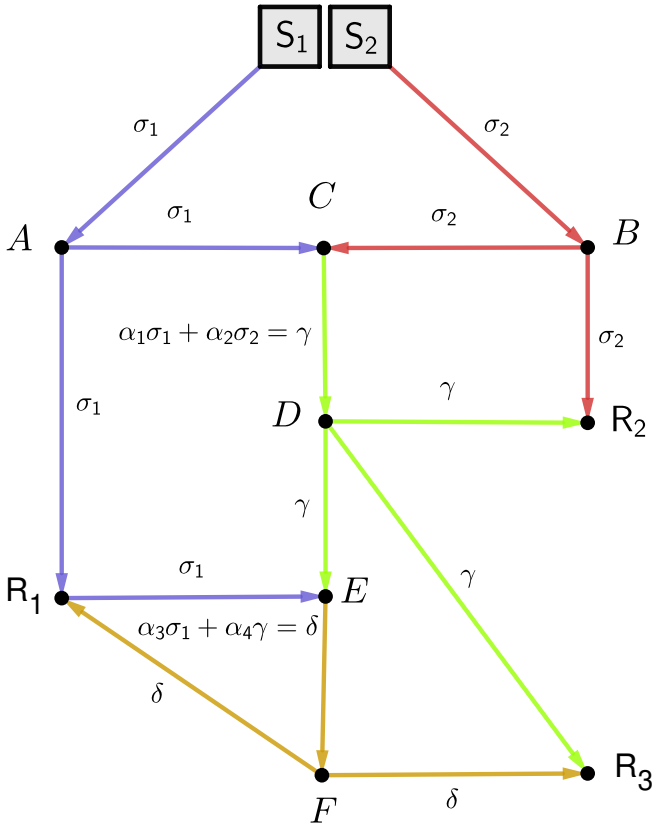
Promotrimo sada mrežu na slici 4. Šaljemo dva simbola σ_1 i σ_2 na tri odredišta R_1, R_2 i R_3. Ako oba simbola šaljemo redom na R_1, R_2, pa na R_3 lako nalazimo puteve za slanje. Mi želimo poslati oba simbola istovremeno na sva tri odredišta te za takav prijenos koristimo linearne kombinacije na posredničkim čvorovima.

Koeficijenti iz $\mathbb{F}_q$ koje koristimo za linearne kombinacije tvore lokalne kodne vektore.

Definicija 3.5. *Lokalni kodni vektor sa pripadnim bridom e je vektor, čiji su elementi iz $\mathbb{F}_q$, s kojim množimo dolazeće simbole. Dimenzija vektora je $1 \times |In(e)|$, pri čemu je $In(e)$ skup bridova kojima je početni vrh brida e krajnji vrh. Vektor označavamo $c^l(e)$.*

Na slici 4 vidimo lokalne kodne vektore $c^l(CD) = \begin{bmatrix}\alpha_1 & \alpha_2\end{bmatrix}$ i $c^l(EF) = \begin{bmatrix}\alpha_3 & \alpha_4\end{bmatrix}$. Koeficijenti $\alpha_1, \alpha_2, \alpha_3$ i α_4 su nepoznati te za njih vrijedi $\alpha_1, \alpha_2, \alpha_3, \alpha_4 \in$

$\mathbb{F}_q$ jer kodni vektori koji se prenose bridovima moraju biti elementi vektorskih potprostora početnih vektora (simbola) koji su poslani s izvora.



Slika 4: Višesmjerni prijenos dvaju simbola na tri odredišta

Što ako želimo poslati h različitih simbola na više odredišta? Tada vektore koji pojedini brid prenosi možemo zapisivat u obliku:

$$c_1(e)\sigma_1 + c_2(e)\sigma_2 + \ldots + c_h(e)\sigma_h = \begin{bmatrix} c_1(e) & c_2(e) & \ldots & c_h(e) \end{bmatrix} \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_h \end{bmatrix},$$

vektor $c(e) = \begin{bmatrix} c_1(e) & c_2(e) & \ldots & c_h(e) \end{bmatrix}$ nazivamo *globalni kodni vektor*.

Definicija 3.6. *Globalni kodni vektor sa pripadnim bridom e je vektor koeficijenata c(e) koji se tijekom prolaska bridom e nalaze uz izvorne simbole. Dimenzija vektora je* $1 \times h$*, pri čemu je h minimalni rez.*

Bridovi kojima je jedno od odredišta krajnji vrh tvore sustav linearnih jednadžbi. Sustav se rješava na odredištu. Neka je ρ_i^j simbol na zadnjem bridu puta između S_i i R_j, a A_j matrica čiji je i-ti redak globalni kodni vektor posljednjeg brida na putu između S_i i R_j. Tada odredište rješava sljedeći sustav:

$$\begin{bmatrix} \rho_1^j \\ \rho_2^j \\ \vdots \\ \rho_h^j \end{bmatrix} = A_j \begin{bmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_h \end{bmatrix}. \tag{6}$$

Stoga, ako izabremo koeficijente globlanih kodnih vektora tako da su matrice $A_1, \dots A_N$ punog ranga, odredišta će moći doći do rješenja sustava odnosno do vrijednosti simbola σ_1, σ_2,..., σ_h. Kodni vektori moraju zadovoljavati još jedan uvjet, da kodni vektor na izlaznom bridu nekog čvora mora biti u vektorskom potprostoru kojeg razapinju vektori ulaznih bridova.

Globalni kodni vektori vezani uz mrežu na slici 4 su $c(CD) = \begin{bmatrix} \alpha_1 & \alpha_2 \end{bmatrix}$ i $c(EF) = \begin{bmatrix} \alpha_3 + \alpha_1\alpha_4 & \alpha_2\alpha_4 \end{bmatrix}$ Matrice A_j mogu biti prikazane pomoću komponenata lokalnih kodnih vektora. U našem primjeru tri odredišta prihvaćaju linearne kombinacije izvornih simbola koje su zapisane u matrice:

$$A_1 = \begin{bmatrix} 1 & 0 \\ \alpha_3 + \alpha_1\alpha_4 & \alpha_2\alpha_4 \end{bmatrix}, A_2 = \begin{bmatrix} 0 & 1 \\ \alpha_1 & \alpha_2 \end{bmatrix} \quad i \quad A_3 = \begin{bmatrix} \alpha_1 & \alpha_2 \\ \alpha_3 + \alpha_1\alpha_4 & \alpha_2\alpha_4 \end{bmatrix}.$$

Odabir koeficijenata $\{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$ takvih da su sve matrice $A_j, j \in \{1, 2, 3\}$ punog ranga je problem dizajna mreže u mrežnom kodiranju.

Glavni teorem mrežnog kodiranja 3.4 sada možemo algebarski iskazati.

Teorem 3.7. *U linearnom mrežnom kodiranju postoje vrijednosti koeficijenata* $\{\alpha_1, \alpha_2, \dots, \alpha_k\}$ *lokalnih kodnih vektora u nekom dovoljnom velikom konačnom polju* $\mathbb{F}_q$ *tako da su sve matrice* $A_j, 1 \leq j \leq N$*, koje definiraju dolazne podatke na odredišta, punog ranga.*

Prvo dokazujemo lemu koja povezuje stupanj polinoma i dovoljnu veličinu konačnog polja kako bi postojali elementi polja za čije bi vrijednosti polinom poprimio nenul vrijednost. Promotrimo matrice nad $\mathbb{F}_2$:

$$A_1 = \begin{bmatrix} x^2 & x(x+1) \\ x(x+1) & x^2 \end{bmatrix} \quad i \quad A_2 = \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}.$$

Za elemente iz $\mathbb{F}_2$ barem je jedna od determinanti jednaka 0. Za $x = 0$ je $det(A_1) = 0$, za $x = 1$ je $det(A_2) = 0$. Ako uzmemo elemente iz $\mathbb{F}_3$, točnije $x = 2$, determinante obiju matrica su različite od 0.

Lema 3.8. *Neka je $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ polinom više varijabli $\alpha_1, \alpha_2, \ldots, \alpha_n$. Pretpostavimo da je maksimalni stupanj varijabli jednak d. Tada na svakom konačnom polju $\mathbb{F}_q$, pri čemu je $q > d$, na kojemu $f(\alpha_1, \alpha_2, \ldots, \alpha_n)$ nije nulpolinom postoje, elementi $p_1, p_2, \ldots, p_n \in \mathbb{F}_q$ takvi da je $f(p_1, p_2, \ldots, p_n) \neq 0$.*

Dokaz. Tvrdnju leme dokazujemo indukcijom po n. Za $n = 1$ imamo polinom jedne varijable stupnja najviše d. Znamo da polinom može imati najviše d nultočaka pa zbog $q > d$ vrijedi tvrdnja. Pretpostavimo sada da tvrdnja vrijedi za sve polinome koji imaju manje od n varijabli. Uzmimo sada polinom sa n varijabli, prikazujemo ga u obliku:

$$f(\alpha_1, \alpha_2, \ldots, \alpha_n) = \sum_{i=0}^{d} f_i(\alpha_1, \alpha_2, \ldots, \alpha_{n-1})\alpha_n^i,$$

$f_1, \ldots, f_d$ su polinomi u varijablama $\alpha_1, \alpha_2, \ldots, \alpha_{n-1}$. Uzmimo sada konačno polje $\mathbb{F}_q$ na kojemu polinom f nije nulpolinom. Tada postoji npr. f_j različit od nule. Polinom f_j je polinom najviše $n-1$ varijable, uzmimo da ima točno $n-1$ varijablu, pa po pretpostavci indukcije slijedi da postoje $p_1, p_2, \ldots, p_{n-1}$ takvi da $f_j(p_1, p_2, \ldots, p_{n-1}) \neq 0$. Sada promotrimo polinom $f(p_1, p_2, \ldots, p_{n-1}, \alpha_n)$ koji je polinom jedne varijable α_n stupnja najviše d pa tvrdnja slijedi po bazi indukcije. □

Sada dokazujemo algebarsku verziju glavnog mrežnog teorema 3.7.

Dokaz. Kako bismo dokazali da su sve matrice punog ranga definiramo funkciju f:

$$f(\alpha_1, \alpha_2, \ldots, \alpha_k) := det(A_1)det(A_2) \cdot \ldots \cdot det(A_N),$$

čiji su argumenti koeficijenti lokalnih kodnih vektora. Uvjet da su sve matrice punog ranga je ekvivalentan uvjetu

$$f(\alpha_1, \alpha_2, \ldots, \alpha_k) \neq 0. \tag{7}$$

Radi pretpostavke da je mreža G aciklička te činjenice da na posredničkim čvorovima linearno kombiniramo dolazne vektore slijedi da su elementi matrica A_j polinomi više varijabli $\alpha_1, \alpha_2, \ldots, \alpha_k$ konačnog stupnja. Tada je funkcija f kao produkt polinoma također polinom više varijabli $\alpha_1, \alpha_2, \ldots, \alpha_k$

konačnog stupnja. Tvrdnja teorema odnosno egzistencija konačnog polja $\mathbb{F}_q$ takvog da postoji elementi $\alpha_1, \alpha_2, \ldots, \alpha_k \in \mathbb{F}_q$ za koje vrijedi (7) slijedi iz leme 3.8. □

Primijetimo kako teorem 3.7 pokazuje egzistenciju mreže za višesmjerni prijenos, ali ne i konstrukciju. Pokazali smo kako uvođenjem linearnih kombinacija na posredničkim čvorovima jednakom brzinom, kojom u jednosmjernom prijenosu (teorem 3.3) prenosimo informaciju na jedno odredište, možemo prenijeti informaciju na više odredišta.

4 Slučajno mrežno kodiranje

U ovom poglavlju proučavamo slučajno mrežno kodiranje i potprostorne kodove. Slučajno mrežno kodiranje je vrsta mrežnog kodiranja u kojem posrednički čvorovi proslijeđuju nasumične linearne kombinacije dolaznih kodnih riječi. U prethodnoj cjelini vidjeli smo da u odredišnim čvorovima moraju biti poznate matrice A_j da bismo mogli dekodirati primljene vektore rješavanjem sustava (6). Matrice A_j ovise o mreži i o kodnim vektorima bridova, tj. o koeficijentima linearnih kombinacija koje rade posrednički čvorovi. Veličinu polja q i te koeficijente birali smo pažljivo da bismo osigurali puni rang matrica $A_1, \ldots, A_N$. Postavlja se pitanje kako je moguće dekodirati primljene vektore ako nije poznata detaljna shema mreže i koeficijenti linearnih kombinacija, koje posrednički čvorovi biraju nasumično?

Osnovna ideja slučajnog mrežnog kodiranja je promotriti koje svojstvo se ne mijenja kad radimo linearne kombinacije poslanih vektora. Riječ je o potprostoru razapetom tim vektorima, zato kao kodne riječi ne uzimamo vektore, nego potprostore nekog vektorskog prostora W. Takve potprostorne kodove proučit ćemo uspoređujući njihova svojstva sa svojstvima klasičnih kodova iz drugog poglavlja.

Problem slučajnog mrežnog kodiranja ćemo prvo formulirati za jednosmjerni prijenos, a generalizacija za višesmjerni prijenos slijedi direktno. Komunikacija u mreži, između izvora i odredišta, se odvija u serijama. Tijekom jedne serije prenese se određen broj vektora nad poljem $\mathbb{F}_q$, preneseni vektori su duljine n. Svaki put kada posrednički čvor proslijeđuje primljene vektore generira nasumičnu linearnu kombinaciju koristeći skalare iz $\mathbb{F}_q$. Na odredište stiže skup nasumičnih linearnih kombinacija izvornih vektora i iz njega se pokušavaju izvesti izvorni vektori. Veličina skupa primljenih vektora tijekom jedne serije je omeđena odozgo vrijednošću minimalnog reza.

Neka su $p_1, \ldots, p_M \in \mathbb{F}_q^n$ vektori poslani sa izvora. U slučaju bez pogrešaka vektori na odredištu su oblika $y_j = \Sigma_{i=1}^{M} h_{j,i} p_i$, $j = 1, \ldots, L$ pri čemu

su $h_{j,i}$ nasumično generirani skalari iz $\mathbb{F}_q$. Odredišne vektore označimo sa $y_1, \ldots, y_L$. Broj L ne mora biti fiksan. Ako uzmemo u obzir pogrešno poslane vektore, npr. $e_1, \ldots, e_T$, dobivamo odredišne vektore oblika $y_j = \Sigma_{i=1}^{M} h_{j,i} p_i + \Sigma_{i=1}^{T} g_{j,i} e_i$. Pritom su $g_{j,i}$ također nasumično generirani skalari iz $\mathbb{F}_q$. Dobili smo model $y = Hp + Ge$, pri čemu je y matrica tipa $L \times n$ čiji su retci odredišni vektori, H i G su $L \times M$ i $L \times T$ matrice nasumičnih skalara, p je $M \times n$ matrica čiji su retci izvorni vektori, a e je $T \times n$ matrica čiji su retci pogrešno poslani vektori.

Neka je $W = \mathbb{F}_q^n$ vektorski prostor. Za proizvoljni prirodni broj k definiramo stohastički operator $\mathcal{H}_k : \mathcal{P}(W) \longrightarrow \mathcal{P}(W)$, pri čemu je $\mathcal{P}(W)$ skup svih potprostora od W. Uzmimo potprostor V od W. Ako je $dim(V) > k$ operator vraća nasumično k-dimenzionalni potprostor od V, inače vraća V. Za svaka dva potprostora $U, V \leqslant W$ postoji potprostor $E \leqslant W$ takav da je $U = (U \cap V) \oplus E$, odnosno $U = \mathcal{H}_k(V) \oplus E$ ako pretpostavimo $k = dim(U \cap V)$ i $\mathcal{H}_k(V) = U \cap V$. Znak $\oplus$ predstavlja direktnu sumu odnosno skup $\{u + v \mid u \in \mathcal{H}_k(V),\ v \in E\}$, pri čemu je $\mathcal{H}_k(V) \cap E = \emptyset$.

Definicija 4.1. Operatorski kanal *povezan s vektorskim prostorom W je komunikacijski kanal kojim se šalju potprostori od W, tj. kanal s izlaznom i ulaznom abecedom $\mathcal{P}(W)$. Poslani potprostor V i primljeni potprostor U povezani su formulom $U = \mathcal{H}_k(V) \oplus E$, pri čemu je $k = dim(U \cap V)$ i E je prostor pogrešaka. Kažemo da je operatorski kanal napravio $dim(V) - k$ brisanja i $t = dim(E)$ pogrešaka prilikom prijenosa.*

Jednostavnije, operatorski kanal uzima vektorski potprostor te vraća drugi vektorski potprostor potencijalno s izbrisanim vektorima i pogrešno dodanim vektorima tijekom prijenosa. Ovakve pogreške ćemo nazivati brisanjima i dodavanjima u daljnjem tekstu.

Kodove koje ćemo promatrati nastaju jednim djelovanjem operatorskog kanala nad kodnom riječi. Želimo konstruirati kodove koji ispravljaju brisanja i dodavanja. Prvo definiramo metriku na skupu svih potprostora vektorskog prostora W.

Definicija 4.2. *Neka je W vektorski prostor i $A, B \leqslant W$. Udaljenost dvaju potprostora definiramo funkcijom $d : \mathcal{P}(W) \times \mathcal{P}(W) \longrightarrow \mathbb{N}_0$ za koju vrijedi:*

$$d(A, B) = dim(A + B) - dim(A \cap B). \tag{8}$$

Za $A + B$ vrijedi $dim(A + B) = dim(A) + dim(B) - dim(A \cap B)$, pa udaljenost možemo zapisati i kao $d(A, B) = dim(A) + dim(B) - 2dim(A \cap B)$.

Lema 4.3. *Udaljenost dvaju potprostora definirana s* (8) *je metrika na skupu $\mathcal{P}(W)$.*

Dokaz. Neka su $A, B, X \in \mathcal{P}(W)$. Svojstvo pozitivnosti $d(A,B) \geqslant 0$ očito vrijedi, a jednakost $d(A,B) = 0$ vrijedi ako i samo ako je $A = B$. Simetričnost $d(A,B) = d(B,A)$ također očito vrijedi jer je $dim(A+B) = dim(B+A)$ te $dim(A \cap B) = dim(B \cap A)$. Preostaje nam pokazati da vrijedi $d(A,B) \leqslant d(A,X) + d(X,B)$. Uzmimo $\frac{1}{2}(d(A,B) - d(A,X) - d(X,B)) = dim(A \cap X) + dim(B \cap X) - dim(X) - dim(A \cap B) = \underbrace{dim((A \cap X) + (B \cap X)) - dim(X)}_{\leqslant 0}$
$+ \underbrace{dim(A \cap B \cap X) - dim(A \cap B)}_{\leqslant 0} \leqslant 0$. Prva nejednakost vrijedi zato što je $(A \cap X) + (B \cap X) \leqslant X$, a druga zato što je $A \cap B \cap X \leqslant A \cap B$. Stoga d je metrika na $\mathcal{P}(W)$. □

Na vektorskom prostoru $W = \mathbb{F}_q^n$ za vektore $x, y \in W$ definiramo uobičajeni skalarni produkt sa $(x,y) = \Sigma_{i=1}^n x_i y_i$. Ako je U k-dimenzionalni potprostor, tada je ortogonalni potprostor $U^\perp = \{v \in W \mid (u,v) = 0,\ \forall u \in U\}$ $(n-k)$-dimenzionalni potprostor. Za svaka dva potprostora U, V od W znamo da vrijedi $(U^\perp)^\perp = U$, $(U+V)^\perp = U^\perp \cap V^\perp$ i $(U \cap V)^\perp = U^\perp + V^\perp$. Iz toga slijedi

$$\begin{aligned} d(U^\perp, V^\perp) = {} & dim(U^\perp + V^\perp) - dim(U^\perp \cap V^\perp) = \\ & dim((U \cap V)^\perp) - dim((U+V)^\perp) = \\ & (n - dim(U \cap V)) - (n - dim(U+V)) = \\ & dim(U+V) - dim(U \cap V) = \\ & d(U,V). \end{aligned} \tag{9}$$

Stoga udaljenost od U i V je jednaka udaljenosti ortogonalnih potprostora $U^\perp$ i $V^\perp$.

Definicija 4.4. *Neka je W vektorski prostor nad $\mathbb{F}_q$.* Kod $\mathcal{C}$ *za operatorski kanal je neprazan skup potprostora od W, odnosno $\mathcal{C} \subseteq \mathcal{P}(W)$, $\mathcal{C} \neq \emptyset$.* Minimalna udaljenost *koda je $d(\mathcal{C}) = min\{d(X,Y) \mid X, Y \in \mathcal{C},\ X \neq Y\}$.* Maksimalna dimenzija *koda je $l(\mathcal{C}) = max\{dim(X) \mid X \in \mathcal{C}\}$. Potprostore iz $\mathcal{C}$ nazivamo kodnim riječima.*

Ako je dimenzija svake kodne riječi jednaka, tada kod $\mathcal{C}$ nazivamo *kod konstantne dimenzije.* Analogno tome kako linearne kodove označavamo s parametrima $[n,k,d]$, kodove konstantne dimenzije za operatorski kanal označavamo uređenom četvorkom $[n, l(\mathcal{C}), log_q|\mathcal{C}|, d(\mathcal{C})]$. *Komplementaran kod* kodu $\mathcal{C}$ je $\mathcal{C}^\perp = \{U^\perp \mid U \in \mathcal{C}\}$. Zbog činjenice da je udaljenost dvaju potprostora jednaka udaljenosti njihovih ortogonalnih potprostora imamo $d(\mathcal{C}) = d(\mathcal{C}^\perp)$. Ako je $\mathcal{C}$ $[n,l,m,d]$-kod konstantne dimenzije, tada je $\mathcal{C}^\perp$ $[n, n-l, m, d]$-kod konstantne dimenzije.

Dekoder najbližeg susjeda kodova za operatorski kanal isto kao i kod klasičnog kodiranja za primljeni potprostor U traži "najbliži" potprostor $V \in \mathcal{C}$ i vraća ga umjesto U. Točnije, traži potprostor $V \in \mathcal{C}$ takav da za svaki $V' \in \mathcal{C}$ vrijedi $d(U,V) \leqslant d(U,V')$. Sljedeći teorem nam pokazuje mogućnosti ispravljanja brisanja i dodavanja. Prije teorema definiramo $(x)_+$ kao $max\{0,x\}$.

Teorem 4.5. *Kodne riječi iz $\mathcal{C}$ prenosimo operatorskim kanalom. Neka je $V \in \mathcal{C}$ potprostor kojeg prenosimo i $U = \mathcal{H}_k(V) \oplus E$ primljeni potprostor. Neka je $t = dim(E)$ i $\rho = (l(\mathcal{C}) - k)_+$ najveći mogući broj brisanja u kanalu. Ako vrijedi*

$$2(t+\rho) < d(\mathcal{C}) \tag{10}$$

onda dekoder minimalne udaljenosti vraća poslani potprostor V, odnosno ispravlja brisanja i dodavanja nastala tijekom prijenosa.

Dokaz. Neka je $V' = \mathcal{H}_k(V)$. Po nejednakosti trokuta imamo $d(V,U) \leqslant d(V,V') + d(V',U) \leqslant t + \rho$. Ako je $T \in \mathcal{C},\ T \neq V$, tada $d(\mathcal{C}) \leqslant d(V,T) \leqslant d(V,U) + d(U,T)$. Iz toga slijedi $d(U,T) \geqslant d(\mathcal{C}) - d(V,U) \geqslant d(\mathcal{C}) - (\rho + t) > \rho + t \geqslant d(V,U)$. U predzadnjoj nejednakosti smo koristili (10). Dobili smo $d(U,T) > d(V,U)$, stoga dekoder vraća potprostor V. □

Teorem pokazuje kako brisanja i dodavanja imaju jednak utjecaj na dekoder, odnosno brisanja i dodavanja su pogreške jednake "težine". Sljedeći korolar prikazuje dva specijalna slučaja teorema 4.5, prvi kada nema brisanja, drugi kada nema dodavanja.

Korolar 4.6. *Neka je $\mathcal{C}$ kod kojeg koristimo za prijenos operatorskim kanalom i $V \in \mathcal{C}$ potprostor kojeg prenosimo. Neka je $U = \mathcal{H}_{dim(W)}(V) \oplus E = V \oplus E$ primljeni potprostor i neka vrijedi $2t < d(\mathcal{C})$, pri čemu je $t = dim(E)$. Tada će dekoder najbližeg susjeda vratiti V. Slično, ako je $U = \mathcal{H}_k(V) \oplus \{0\}$ primljeni potprostor i vrijedi $2\rho < d(\mathcal{C})$, pri čemu je $\rho = (l(\mathcal{C}) - k)_+$, tada će dekoder najbližeg susjeda vratiti V.*

Korolar pokazuje da u slučaju kada nema brisanja dekoder može ispraviti najviše $\lfloor \frac{d(\mathcal{C})-1}{2} \rfloor$ pogrešaka, kao i kod klasičnog kodiranja (korolar 2.7).

Sada ćemo se ograničiti na kodove konstantne dimenzije, slično kaošto se u klasičnom kodiranju nekad promatraju kodovi konstante Hammingove težine. Također promatramo $[n,l,m,d]$-kodove za koje vrijedi $l \leqslant n - l$. Ako je $l > n - l$ tada uzimamo komplementarni kod. Udaljenost u takvim kodovima povezana je s takozvanim Grassmanovim grafom.

Definicija 4.7. *Neka je $P(W,l)$ skup svih potprostora vektorskog prostora W dimenzije l.* Grassmannov graf *je graf čiji je skup vrhova $P(W,l)$ i brid spaja vrhove U,V ako i samo ako je $d(U,V) = 2$.*

Pokazuje se da je za U, V iz $\mathcal{P}(W, l)$ udaljenost $d(U, V)$ jednaka dvostrukoj udaljenosti u Grassmanovom grafu, tj. dvostrukoj duljini najkraćeg puta od U do V.

Tijekom prijenosa ovakvih kodova pretpostavimo da odredište zna dimenziju koda koji se prenosi kanalom. Tada odredište prikuplja vektore sve dok primljeni vektori ne razapinju l-dimenzionali potprostor od W. U tom slučaju operatorski kanal vraća $U = \mathcal{H}_{t(E)}(V) \oplus E$, pri čemu je broj izbrisanih vektora $t(E)$ i broj pogrešaka je također $t(E)$. Prema teoremu 4.5 tada dekoder može ispraviti najviše $\lfloor \frac{d(\mathcal{C})-1}{4} \rfloor$ pogrešaka.

Promotrimo sada primjer koda u $P(W, l)$.

Primjer 4.8. *Neka je W vektorski prostor čiji su vektori uređene n-torke iz $\mathbb{F}_q^n$ i neka je $\mathcal{C} \subset P(W, l)$ skup prostora U_i, $i = 1, \ldots, |\mathcal{C}|$ čije su generirajuće matrice $G_i = (I_l \mid A_i)$, pri čemu je I_l jedinična matrica tipa $l \times l$, a A_i su sve moguće različite $l \times (n - l)$ matrice. Takve generirajuće matrice generiraju različite prostore. Presjek bilo koja dva prostora je najviše dimenzije $l - 1$. Stoga je minimalna udaljenost jednaka $2l - 2(l - 1) = 2$ i imamo $[n, l, l(n - l), 2]$-kod konstantne dimenzije.*

Takav kod nije dobar za ispravljanje pogrešaka (ne može ispraviti niti jednu pogrešku), ali se unatoč tome često koristi.

Primjer 4.9. *Neka je W vektorski prostor čiji su vektori uređene n-torke nad $\mathbb{F}_q$. Uzmimo sada kod $\mathcal{C}' = \mathcal{P}(W, l)$. To je $[n, l, log_q|\mathcal{P}(W, l)|, 2]$-kod konstante dimenzije, puno veći od koda $\mathcal{C}$. Broj $|\mathcal{P}(W, l)|$ je jednak Gaussovom koeficijentu $\begin{bmatrix} n \\ l \end{bmatrix}_q$.*

Gaussov ili q-binomni koeficijent $\begin{bmatrix} n \\ l \end{bmatrix}_q$ definiramo kao broj l-dimenzionalnih potprostora n-dimenzionalnog vektorskog prostora nad konačnim poljem $\mathbb{F}_q$. Možemo ga računati po formuli:

$$\begin{bmatrix} n \\ l \end{bmatrix}_q = \frac{(q^n - 1)(q^{n-1} - 1) \cdots (q^{n-l+1} - 1)}{(q^l - 1)(q^{l-1} - 1) \cdots (q - 1)} = \prod_{i=0}^{l-1} \frac{q^{n-i} - 1}{q^{l-i} - 1}.$$

Sljedeća lema daje ocjenu za Gaussove koeficijente.

Lema 4.10. *Q-arni Gaussov koeficijent $\begin{bmatrix} n \\ l \end{bmatrix}_q$ zadovoljava:*

$$1 < q^{-l(n-l)} \begin{bmatrix} n \\ l \end{bmatrix}_q < 4,$$

za $0 < l < n$, tako da Gaussov koeficijent možemo zapisat kao $\begin{bmatrix} n \\ \lambda n \end{bmatrix}_q = \Theta(q^{n^2\lambda(1-\lambda)}), 0 < \lambda < 1$.

Dokaz. Broj $q^{l(n-l)}$ interpretiramo kao broj l-dimenzionalnih potprostora od $\mathbb{F}_q^n$ koje razpinju retci matrica oblika $[I_l, A]$, pri čemu je A proizvoljna matrica tipa $l \times (n-l)$ nad $\mathbb{F}_q$. Zbog $l > 0$, skup takvih potprostora ne sadrži sve l-dimenzionalne potprostore od $\mathbb{F}_q^n$. Iz toga slijedi $1 < q^{-l(n-l)} \begin{bmatrix} n \\ l \end{bmatrix}_q$.

Za gornju granicu imamo:

$$\begin{aligned}\begin{bmatrix} n \\ l \end{bmatrix}_q =& q^{l(n-l)} \frac{(1-q^{-n})(1-q^{-n+1})\cdots(1-q^{-n+l-1})}{(1-q^{-l})(1-q^{-l})\cdots(1-q^{-1})} < \\ & q^{l(n-l)} \frac{1}{(1-q^{-l})(1-q^{-l+1})\cdots(1-q^{-1})} < \\ & q^{l(n-l)} \prod_{j=1}^{\infty} \frac{1}{(1-q^{-j})} \qquad .\end{aligned}$$

Funkcija $f(x) = \prod_{j=1}^{\infty} \frac{1}{(1-x^j)}$ je rastuća na $\langle 0, +\infty \rangle$ [8] . Nas zanima $f(\frac{1}{q})$, za $q \geqslant 2$ imamo:

$$\prod_{j=1}^{\infty} \frac{1}{(1-q^{-j})} \leqslant \prod_{j=1}^{\infty} \frac{1}{(1-2^{-j})} = 1/Q_0 < 4,$$

pri čemu je $Q_0 \approx 0.288788095$ vjerojatnosno-kombinatorna konstanta [1]. Točnije, vjerojatnost da jako velika nasumična kvadratna matrica nad $\mathbb{F}_2$ nije singularna. □

Slično kao kod klasičnog kodiranja želimo dati ocjenu pakiranju kugli. Prvo definiramo kuglu na skupu potprostora.

Definicija 4.11. *Neka je W n-dimenzionalni vektorski prostor i $\mathcal{P}(W, l)$ skup svih l-dimenzionalnih potprostora od W. Kuglu $S(V, l, t)$ radijusa t s centrom u V definiramo kao skup:*

$$\{U \in \mathcal{P}(W, l) \mid d(U, V) \leqslant 2t\},$$

pri čemu je $t \in \mathbb{N}_0$.

Sljedeći teorem pokazuje da je broj potprostora u $S(V, l, t)$ nezavisan od V.

Teorem 4.12. *Broj potprostora u kugli $S(V, l, t)$ ne ovisi o V i jednak je $\Sigma_{i=o}^{t} q^{i^2} \begin{bmatrix} l \\ i \end{bmatrix}_q \begin{bmatrix} n-l \\ i \end{bmatrix}_q$, za $t \leqslant l$.*

Dokaz. Izračunat ćemo broj potprostora $U \in \mathcal{P}(W,l)$ koji sijeku V u $(l-i)$-dimenzionalnom potprostoru. Presjek $U \cap V$ možemo izabrati na $\begin{bmatrix} l \\ l-i \end{bmatrix}_q = \begin{bmatrix} l \\ i \end{bmatrix}_q$ načina. Nakon toga možemo dopuniti taj presjek do potprostora U na $\frac{(q^n-q^l)(q^n-q^{l+1})\cdots(q^n-q^{l+i-1})}{(q^l-q^{l-i})(q^l-q^{l-i+1})\cdots(q^l-q^{l-1})} = q^{i^2}\begin{bmatrix} n-l \\ i \end{bmatrix}_q$ načina. Zato je broj potprostora udaljenih $2i$ od V jednak $q^{i^2}\begin{bmatrix} n-l \\ i \end{bmatrix}_q \begin{bmatrix} l \\ i \end{bmatrix}_q$. Tvrdnju teorema dobivamo sumom po svim udaljenostima. □

Iz (9) slijedi $|S(V,l,t)| = |S(V,n-l,t)|$. Sada smo spremni pokazati ocjenu pakiranja kugli za potprostorne kodove.

Teorem 4.13. *Neka je $\mathcal{C}$ podskup od $\mathcal{P}(W,l)$ takav da je $d(\mathcal{C}) \geqslant 2t$ i neka je $s = \lfloor \frac{t-1}{2} \rfloor$. Tada $\mathcal{C}$ zadovoljava*

$$|\mathcal{C}| < 4q^{(l-s)(n-s-l)}.$$

Dokaz. Tvrdnju dokazujemo koristeći teorem 4.12 i lemu 4.10. Imamo $|\mathcal{C}| \leqslant \frac{|\mathcal{P}(W,l)|}{|S(V,l,s)|} = \frac{\begin{bmatrix} n \\ l \end{bmatrix}_q}{|S(V,l,s)|} < \frac{\begin{bmatrix} n \\ l \end{bmatrix}_q}{q^{s^2}\begin{bmatrix} n-l \\ s \end{bmatrix}_q \begin{bmatrix} l \\ s \end{bmatrix}_q} < 4q^{(l-s)(n-s-l)}$. □

Literatura

[1] E. R. Berlekamp, *The technology of error-correcting codes*, Proc. IEEE, vol. 68, pp. 564–593, May 1980.

[2] W. Cherowitzo, *Combinatorics in space*, dostupno na `http://www-math.ucdenver.edu/~wcherowi/courses/m7409/mariner9talk.pdf` (travanj 2020.)

[3] W. Cherowitzo, *Reed-Muller codes*, dostupno na `http://www-math.ucdenver.edu/~wcherowi/courses/m7823/reedmuller.pdf` (travanj 2020.)

[4] C. Fragouli, E. Soljanin, *Network Coding Fundamentals*, now Publishers Inc., 2007.

[5] R. Hill, *A First Course in Coding Theory*, Oxford University Press, 1996.

[6] R. Kötter, F.R. Kschischang, *Coding for Errors and Erasures in Random Network Coding*, IEEE Transactions on Information Theory, vol. 54, no. 8, August 2008.

[7] J. H. van Lint, *Introduction to Coding Theory*, Third Revised and Expanded Edition, Springer-Verlag, 1999.

[8] J. H. van Lint and R. M. Wilson, *Course in Combinatorics*, 2nd ed. Cambridge, U.K.: Cambridge Univ. Press, 2001.

[9] J. Šiftar, V. Krčadinac, *Konačne geometrije*, skripta, Sveučilište u Zagrebu, Zagreb, 2012.

Sažetak

U ovom radu obrađene su metode prijenosa informacija kroz komunikacijski kanal. Proučene su metode klasičnog kodiranja i mrežnog kodiranja. U klasičnom kodiranju smo definirali blokovne kodove te njihova svojstva. Također smo definirali linearne kodove i proučili dvije vrste, Hammingove i Reed-Mullerove kodove. Nakon toga smo obradili mrežno kodiranje kod kojeg se paketi linearno kombiniraju na čvorovima. Glavna tvrdnja rada je da se u mrežnom kodiranju jednakom brzinom, kojom u klasičnom kodiranju prenosimo informaciju na jedno odredište, može prenijeti informacija na više odredišta. Tvrdnju iskazujemo i dokazujemo glavnim teoremom mrežnog kodiranja u čijem dokazu se koristi teorem minimalnog reza i maksimalnog toka. Na kraju smo obradili vrstu mrežnog kodiranja u kojem se paketi nasumično linearno kombiniraju na čvorovima, slučajno mrežno kodiranje i odgovarajuće potprostorne kodove.

Summary

In this graduate thesis, methods of information transfer through the communication channel were discussed. Classical coding and network coding methods were studied. In classical coding, we have defined block codes and their properties. We also defined linear codes and studied two types, Hamming and Reed-Muller codes. After that, we discussed network coding in which packets are linearly combined at the nodes. The main claim of the thesis is that in network coding at the same speed, at which in classical coding we transfer information to one destination, information can be transferred to several destinations. We state and prove the claim by the main network coding theorem in the proof of which the theorem of minimum cut and maximum flow is used. Finally, we discussed a type of network coding in which packets are randomly linearly combined at the nodes, random network coding and the correspoding subspace codes.

Životopis

Rođen sam u Zagrebu 27. srpnja 1994. godine gdje sam završio osnovnu školu Malešnicu i prirodoslovno-matematički smjer Gimnazije Lucijana Vranjanina. Nakon završetka srednje škole i položene državne mature 2013. godine upisujem Preddiplomski sveučilišni studij Matematika na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu. Po završetku preddiplomskog studija 2017. godine upisujem Diplomski sveučilišni studij Matematička statistika na istom visokom učilištu. Kao predsjednik Studentskog zbora Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu jedan sam od idejnih začetnika i osnivača znanstveno-sportskog natjecanja studenata STEM područja STEM Games. Trenutno sam zaposlen kao softverski inženjer u Ericssonu Nikoli Tesli te sam koordinator sveučilišnih sportskih natjecanja u organizaciji Zagrebačkog sveučilišnog sportskog saveza. Aktivan sam član futsal sekcije Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu.