UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Lucija Palibrk

Teorija kodiranja i konačna polja

SPECIJALISTIČKI RAD

Podgorica, 2017.

UNIVERZITET CRNE GORE

Prirodno-matematički fakultet Podgorica

Teorija kodiranja i konačna polja

SPECIJALISTIČKI RAD

Matematika

Mentor: Vladimir Božović

Lucija Palibrk

Studijski program Matematika

Podgorica, Oktobar 2017.

Apstrakt

Ono što me je navelo da odaberem ovu temu za svoj specijalistički rad jeste mogućnost sagledavanja jasne koristi strogo teorijskih matematičkih dostignuća. Naime, u ovom radu otkrićemo zanimljivu i konkretnu primjenu onih zaključaka donijetih na časovima algebre, koji su se, možda, nekima na prvi pogled, činili sasvim apstraktni i potpuno beskorisni.

U ovom radu, vidjećemo kako se teorija kodiranja oslanja na algebru. Osim što ćemo obnoviti neka saznanja iz teorije konačnih polja, upoznaćemo se sa osnovnim pojmovima teorije kodiranja i proučiti neke vrste kodova.

U prvoj glavi dali smo osnovne informacije o teoriji kodiranja i pokušali da objasnimo čime se to ona bavi. Naveli smo razliku između izvornog i kanalnog kodiranja i jednostavnim primjerima pokušali da zainteresujemo čitaoce ovog rada. U drugoj glavi dali smo osnovne definicije teorije kodiranja i dali primjer kodiranja dodavanjem bita parnosti. Naveli smo osnovna dva pravila dekodiranja, uveli smo pojam distance koda, zatim smo objasnili svojstva detekcije i korekcije greške nekog koda. U trećoj glavi dali smo rezime algebarkih tvrđenja iz teorije konačnih polja koja su potrebna za proučavanje linearnih kodova, a zatim smo u četvrtoj, govorili uopšteno o linearnim kodovima.

Abstract

The reason I chose this subject to my thesis is the possibility to observe clear benefits of strictly theoretical achievements in mathematics. Particularly, in this thesis we will unveil an interesting and concrete implementation of conclusions made during algebra classes, which for some people seemed completely abstract and entirely useless.

In this thesis, we will see how coding theory relies on algebra. Besides recalling some facts from the theory of finite fields we will also be introduced to the basic terms in coding theory and observe some types of codes.

In the opening chapter we provided basic information about Coding theory and tried to explain what the Theory is about. We pointed out the difference between source and channel coding and with simple examples we attempted to keep our readers interested. In the second chapter there are basic definitions of coding theory and example of coding by adding a parity bit. We listed two basic rules of decoding, introduced concept of code distance, then we explained detection and failure correction features of a code. In the third chapter we provided summary of algebraic claims from theory of final fields which are necessary for studying linear codes, and the final, fourth chapter, is about liner codes in general.

Sadržaj

Glava 1

Uvod

U današnje digitalno i informacijsko doba učinkovit i pouzdan prenos informacija vrlo je bitan, a oslanja se na metode grane matematike poznate kao *Teorija kodiranja*.

Ova relativno mlada nauka potiče od Kloda Šenona (*Claude E. Shannon*), američkog matematičara, koji je poznat kao začetnik teorije informacija, i njegovog djela „*A Mathematical Theory of Communication* ". Teorija informacija i teorija kodiranja su srodne teorije koje za glavni cilj imaju učinkovitu i pouzdanu komunikaciju u često neprijateljskom okruženju, pri čemu prenos mora zahtjevati što manju količinu vremena i napora.

Teorija kodiranja je bazirana na analizi podataka koji se prenose kroz kanale sa šumom i na ispravljanje eventualnih grešaka koje pri tom nastaju. Naime, fizički medijum preko kojeg se poruke šalju naziva se kanal. (Na primjer: telefonska linija, satelitska veza, bežični kanal koji se koristi za mobilne komunikacije itd.) Ti kanali preko kojih se poruke prenose često su nesavršeni. Različite vrste kanala sklone su različitim vrstama šumova odnosno smetnji pri prenosu podataka. Šum može biti izazvan svjetlošću, bukom, ljudskom greškom, kvarom opreme koja se koristi, naponom i sl. Teorija kodiranja, dakle, pokušava da prevaziđe štetne efekte šumova

na kanalima. Ako posmatramo primjer čuvanja podataka i njihovog čitanja sa CD-a, do greške može doći zbog fizičkih oštećenja na površini CD-a. Vidjećemo da je osnovna ideja u kodiranju poruka dodavanje redundancije tj. određene suvišnosti u formi dodatog simbola na izvornu poruku prije njenog prenosa kroz kanal sa šumom.

Razlika izmedju kriptografije i kodiranja je u tome što je glavni zadatak kriptografije da napravi poruke koje su teške za razumijevanje bez šifre (ključa), što sa kodiranjem nije slučaj. Ako imamo riječ koju prenosimo a koja je u binarnom zapisu, kodiranjem se dodaju neki pomoćni bitovi koji pomažu pronalaženju i ispravljanju eventualne greške nastale pri prenosu riječi od pošiljaoca do primaoca (pomenuta redundancija). Najprostiji način kodiranja je pomoću bitova parnosti što će biti objašnjeno kasnije. Posle više pokušaja, prvi kod pomoću kojeg se pronalazi i ispravlja nastala greška, predstavio je Ričard Heming (*Richard Hamming*).

Razlikujemo izvorno kodiranje (*source coding*) i kodiranje kanala (*channel coding*). Izvorno kodiranje podrazumijeva promjenu izvora poruke u odgovarajući kod koji se prenosi preko kanala. Preciznije, izvorno kodiranje predstavlja proces koji se koristi za šifrovanje informacija, uklanjajući nepotrebne podatke, tako da propusni opseg signala bude prilagođen efikasnom prenosu. Primjer izvornog kodiranja je ASCII kod koji pretvara svaki karakter u bajt od 8 bita.

Primjer 1.1. *Razmotrimo izvorno kodiranje četiri vrste voća (jabuka, kruška, šljiva, višnja) na sledeći način:*

jabuka $\rightarrow$ *00*

kruška $\rightarrow$ *01*

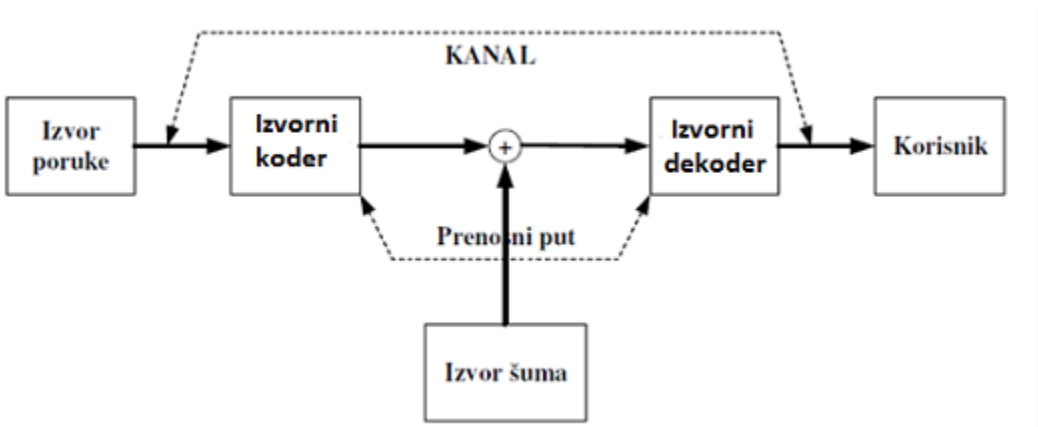
šljiva $\rightarrow$ *10*

višnja $\rightarrow$ *11*

Pretpostavimo da je poruka „jabuka ", koja je kodirana kao 00, prenijeta kroz kanal

sa šumom. Poruka može biti oštećena pri prenosu kroz kanal zbog šuma a zatim i primljena pogrešno, kao 01 na primjer. Primalac, međutim ne zna da je poruka oštećena i pomisliće da je izvorna poruka „kruška". Ovakva komunikacija očigledno ne uspijeva.

Jednostavni komunikacijski model može biti predstavljen na sledeći način:



Slika 1.1: Izvorno kodiranje

Ideja o kodiranju kanala podrazumijeva ponovno kodiranje poruke nakon izvornog kodiranja uvođenjem neke vrste suvišnosti tj. redundancije, tako da se greške mogu otkriti ili čak ispraviti.

Na prethodnom primjeru možemo prikazati kodiranje kanala uvođenjem suvišnosti od jednog bita na sledeći način:

$00 \rightarrow 000$

$01 \rightarrow 011$

$10 \rightarrow 101$

$11 \rightarrow 110$

Pretpostavimo da je poruka „jabuka” (koja je kodirana sa 000 posle izvornog i kanalnog kodiranja) prenijeta kroz kanal sa smetnjama i da postoji samo jedna greška na poruci. Tada primljena riječ mora biti jedna od sledeće tri: 100, 010, 001. U ovom slučaju možemo uočiti grešku jer nijedna od poruka 001,100,010, nije među našim kodiranim porukama.

Moramo imati na umu da gornja šema kodiranja dozvoljava otkrivanje grešaka po cijeni smanjenja brzine prenosa jer moramo prenositi tri bita za poruku od dva bita. Gornja šema kodiranja kanala nam ne dozvoljava da ispravljamo greške. Na primjer, ako je primljeno 100 onda mi ne znamo da li ono potiče od poruke 000 ili 110 ili 101. Međutim ako se uvede više suvišnosti, tj. ukoliko vršimo kanalno kodiranje tako da poruku od dva bita kodiramo porukom sa četiri ili više bita, bićemo u mogućnosti da ispravimo greške nastale pri prenosu. Na primjer, možemo dizajnirati sledeću šemu kodiranja kanala:

$00 \rightarrow 00000$

$01 \rightarrow 01111$

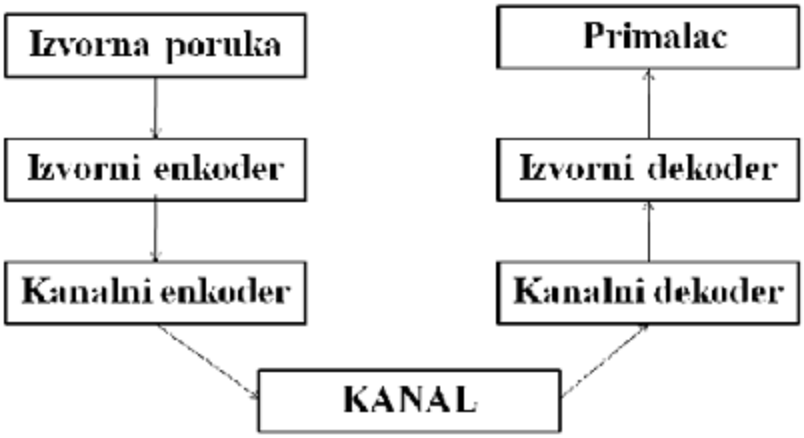
$10 \rightarrow 10110$

$11 \rightarrow 11001$

Pretpostavimo da je poruka „jabuka ” prenijeta preko kanala sa smetnjama i to tako da je nanijeta samo jedna greška. Tada primljena poruka mora biti jedna od sledećih: 10000, 01000, 00100, 00010, 00001. Pretpostavimo da je primljena 10000. Tada smo sigurni da 10000 dolazi od 00000 jer postoje najmanje dvije greške između 10000 i svake druge kodirane poruke 01111, 10110, 11001.

Još treba imati na umu da u ovom slučaju gubimo više u smislu brzine prenosa informacija.

Da bismo lakše razumijeli kanalno kodiranje pogledajmo sliku 1.2.



Slika 1.2: Kanalno kodiranje

Cilj kodiranja kanala je da se postigne:

1. brzo kodiranje poruka
2. jednostavan prenos kodiranih poruka
3. brzo dekodiranje primljenih poruka
4. maksimalan prenos podataka po jedinici vremena
5. maksimalna sposobnost detekcije i korekcije greške

Generalno 5. uopšte nije kompatibilno sa 4. Prema tome svako rešenje je nužno, kompromis između svih pet ciljeva. Kodiranje kanala se još naziva algebarsko kodiranje, jer su algebarski alati obimno uključeni u teoriju kodiranja kanala. Tu dolazimo do osnovnog cilja ovog specijalističkog rada, a to je, ukazati na značaj algebre na razvoj teorije kodiranja.

Glava 2

Teorija kodiranja

2.1 Kodiranje kanala

Počnimo sa osnovnim definicijama.

Definicija 2.1. *Neka su dati skupovi: A - skup svih mogućih simbola izvorne poruke i B - skup svih mogućih simbola koda. Kodiranje je pravilo koje svakom simbolu izvorne poruke pridružuje tačno jednu riječ sastavljenu od simbola koda. Drugim riječima, kodiranje možemo opisati kao funkciju koja elementima skupa A pridružuje jedan ili više elemenata skupa B. Ono što dobijemo tim preslikavanjem kodirana je poruka, odnosno kod koji šaljemo kroz komunikacijski kanal.*

U uvodu smo napomenuli da je svrha kodiranja kanala uvođenje redundantnosti u informativne poruke tako da se greške koje se javljaju pri prenosu mogu otkriti ili čak ispraviti.
Sledeći primjer pokazuje jednu od najjednostvnijih metoda za otkrivanje grešaka.

Primjer 2.1. *(**Dodavanje bita parnosti**) Pretpostavimo da želimo poslati poruku u binarnom sistemu koja se sastoji od 7 bitova. Dodavanje bita parnosti znači da na kraj dodamo osmi bit čiju vrijednost odaberemo tako da ukupan broj nenultih bitova*

bude paran. Na primjer 0110010 → 01100101, 1100110 → 11001100. Ukoliko dođe do greške tokom prenosa poruke, možemo je uočiti jer će broj nenultih bitova biti neparan. Nedostatak ovog načina otkrivanja greške je to što ne možemo sa sigurnošću reći koji bit je pogrešan, niti možemo u slučaju više grešaka, prepoznati da je do greške uopšte i došlo.

Definicija 2.2. *Neka je $A = \{a_1, a_2, \dots a_q\}$ skup od q elemenata koga ćemo nazivati alfabet i čije elemente ćemo nazivati simbolima.*

1. *q-arna riječ dužine n nad skupom A je niz $w = w_1 w_2 \dots w_n$ gdje je svaki $w_i \in A$ za $\forall i = 1, 2, \dots n$. Takođe w možemo posmatrati i kao vektor $(w_1, w_2, \dots w_n)$.*

2. *q-arni blok-kod dužine n nad skupom A je neprazni skup C q-arnih riječi nad A koje imaju istu dužinu n.*

3. *Element skupa C nazivamo riječ u C.*

4. *Broj riječi u C, u oznaci $|C|$, nazivamo veličinom skupa C.*

5. *Kod dužine n i veličine M zovemo (n, M) kod.*

Vidjećemo da se za alfabet najčešće uzima konačno polje F_q, reda q.
Kod nad alfabetom $F_2 = \{0, 1\}$ nazivamo binarnim kodom. Simboli za binarni kod su: 0 i 1. Evo nekih primjera za binarne kodove:

1. $C_1 = \{00, 01, 10, 11\}$ - ovo je (2,4) kod.

2. $C_2 = \{000, 011, 101, 110\}$ - ovo je (3,4) kod.

3. $C_3 = \{0011, 0101, 1010, 1100, 1001, 0110\}$- ovo je (4,6) kod.

Kod nad alfabetom $F_3 = \{0, 1, 2\}$ nazivamo ternarni kod.

Definicija 2.3. *Komunikacijski kanal se sastoji od konačnog kodnog alfabeta* $A = \{a_1, a_2, \dots a_q\}$ *kao i skupa tekućih kanalnih vjerovatnoća:* $P(a_j - primljen|a_i - poslat)$ *koje zadovoljavaju:*

$$\sum_{j=1}^{q} P(a_j - primljen|a_i - poslat) = 1$$

za sve $i = 1, \dots q$. *Ovde smo sa* $P(a_j - primljen|a_i - poslat)$ *označili uslovnu vjerovatnoću da je* a_j *primljen znajući da je poslat* a_i.

Definicija 2.4. *Za komunikacijski kanal se kaže da je bez memorije ako je ishod bilo kog prenosa nezavisan od ishoda prethodnog prenosa.*

Ako su $c = c_1c_2 \dots c_n$ i $x = x_1x_2 \dots x_n$ riječi dužine n, onda u kanalu bez memorije važi

$$P(x - primljen|c - poslat) = \prod_{i=1}^{n} P(x_i - primljen|c_i - poslat). \tag{2.1.1}$$

Definicija 2.5. *q-arno simetrični kanal je kanal bez memorije koji ima kodni alfabet veličine q takav da važi :*

- *Svaki poslati simbol ima istu vjerovatnoću* $p < 1/2$ *da bude primljen sa greškom.*
- *Ako je simbol primljen sa greškom, onda je svaka od* $q - 1$ *mogućih grešaka jednako vjerovatna.*

Konkretno, binarno-simetrični kanal (BSC) je kanal bez memorije koji ima kodni alfabet $\{0, 1\}$ i kanalne vjerovatnoće:

$$P(1 - primljeno|0 - poslato) = P(0 - primljeno|1 - poslato) = p, \tag{2.1.2}$$

$$P(0 - primljeno|0 - poslato) = P(1 - primljeno|1 - poslato) = 1 - p. \tag{2.1.3}$$

Dakle, vjerovatnoća greške u BSC je p. Nazivamo je prelazna (*crossover*) vjerovatnoća.

Primjer 2.2. *Pretpostvimo da su riječi iz koda* $\{000, 111\}$ *poslate preko* BSC *- binarnog simetričnog kanala sa prelaznom vjerovatnom* $p = 0.05$. *Pretpostavimo da je primljena riječ 110. Probaćemo da nađemo najvjerovatnije poslatu riječ računanjem tekućih kanalnih vjerovatnoća:*

$$P(110 - primljeno|000 - poslato) =$$
$$(P(1 - primljeno|0 - poslato))^2 * P(0 - primljeno|0 - poslato) =$$
$$(0.05)^2 * (1 - 0.05) = 0.02375$$

$$P(110 - primljeno|111 - poslato) =$$
$$(P(1 - primljeno|1 - poslato))^2 * P(0 - primljeno|1 - poslato) =$$
$$(0.95)^2 * (0.05) = 0.04512$$

Kako je druga vjerovatnoća veća nego prva, možemo zaključiti da je vjerovatnije da je poslata riječ 111.

2.2 Pravila dekodiranja

Postupak pronalaženja originalne poruke x iz primljene poruke y naziva se dekodiranje.[3] Pretpostavimo da je primljena riječ x. Ako je x riječ koja pripada kodu onda možemo zaključiti da nije bilo greške pri transmisiji. Inače znamo da su se neke greške pojavile. Tada trebamo pravilo za nalaženje najvjerovatnije poslate riječi. Takvo pravilo

je poznato kao pravilo dekodiranja. Mi ćemo razmatrati u nastavku dva pravila dekodiranja: dekodiranje po pravilu maksimalne vjerovatnoće i dekodiranje po pravilu najbližeg susjeda.

2.2.1 Dekodiranje po pravilu maksimalne vjerovatnoće

Pretpostavimo da su riječi iz koda C prenijete preko komunikacionog kanala. Ako je primljena riječ x, mi možemo računati tekuće kanalne vjerovatnoće:
$P(x - primljeno|c - poslato)$ za sve riječi $c \in C$. Po pravilu maksimalne vjerovatnoće, riječ x ćemo dekodirati u riječ $c_x \in C$, takvu da ona maksimizira tekuće kanalne vjerovatnoće tj.

$$P(x - primljen|c_x - poslat) = max\{P(x - primljen|c - poslat)|c \in C\}$$

. Postoje dvije vrste ovakvog dekodiranja:

1. **Potpuno pravilo** Ako je riječ x primljena, treba naći najvjerovatnije poslatu riječ. Ako postoji više od jedne takve riječi, izaberemo jednu od njih proizvoljno.

2. **Nepotpuno pravilo** Ako je x primljena, treba naći najvjerovatnije poslatu riječ. Ako postoji više od jedne takve riječi, zahtjevamo retransmisiju, tj. ponovno slanje poruke.

2.2.2 Dekodiranje po pravilu najbližeg susjeda

Prije nego objasnimo ovo pravilo uvedimo pojam Hamingove udaljenosti.
Pretpostavimo da je neka riječ iz koda C poslata preko BSC sa prelaznom vjerovatnoćom: $p < 1/2$. Ako je riječ x primljena, onda je za bilo koju riječ $c \in C$ tekuća

kanalna vjerovatnoća data sa:

$$P(x - primljen \,|\, c - poslat) = p^l * (1-p)^{n-l},$$

gdje je n dužina riječi x, a l je broj mjesta na kojima se x i c razlikuju. Kako je $p < 1/2$ to onda $1 - p > p$ pa je tražena vjerovatnoća veća za veće vrijednosti $n - l$ tj. za manje vrijednosti veličine l. Stoga je pomenuta vjerovatnoća najveća za onu riječ $c \in C$ za koju je l najmanje. Veličinu l nazivamo Hemingovom udaljenošću ili Hemingovim rastojanjem riječi x i c. Evo i precizne definicije.

Definicija 2.6. *Neka su x i y riječi dužine n nad alfabetom A. Hemingovo rastojanje od x do y, u oznaci $d(x, y)$, se definiše kao broj mjesta na kojima se x i y razlikuju. Ako je $x = x_1x_2 \dots x_n$ i $y = y_1y_2 \dots y_n$ onda*

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

gdje su x_i, y_i posmatrani kao riječi dužine 1 i

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

Primjer 2.3. *Neka je $A = \{0, 1\}$ i $x = 01010$, $y = 01101$, $z = 11101$. Tada $d(x, y) = 3$, $d(y, z) = 1$, $d(z, x) = 4$.*

Teorema 2.1. *Neka su x, y, z riječi dužine n nad alfabetom A. Tada važi:*

1. $0 \leq d(x, y) \leq n$
2. $d(x, y) = 0 \Leftrightarrow x = y$
3. $d(x, y) = d(y, x)$

4. $d(x,z) \leq d(x,y) + d(y,z)$

Dokaz. Svojstva 1, 2 i 3 su očigledna iz definicije Hemingove udaljenosti. Zbog svojstva

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

dovoljno je dokazati nejednakost trougla tj. 4. za $n = 1$.

Ako $x = z$ onda $d(x,z) = 0$ pa nejednakost važi.

Ako $x \neq z$ onda mora biti da je $x \neq y$ ili $y \neq z$ jer ne mogu istovremeno biti $d(x,y) = 0$ i $d(y,z) = 0$ zbog svojstava 1 i 2, pa je $x \neq y$ ili $y \neq z$. Dakle, 4 očigledno važi. □

Vratimo se sada pravilu najbližeg susjeda. Pretpostavimo da je riječ iz koda C poslata preko komunikacionog kanala. Ako je riječ x primljena, onda po pravilu najbližeg susjeda dekodiramo je u onu riječ c_x iz C za koju je $d(x,c_x)$ minimalno tj.

$$d(x,c_x) = min\{d(x,c), c \in C\}. \tag{2.2.1}$$

Ovaj način dekodiranja još zovemo i dekodiranje po minimalnoj udaljenosti. Razlikujemo potpuno i nepotpuno dekodiranje i u ovom slučaju. Ako postoje dvije ili više riječi $c_x \in C$ za primljenu riječ x, koje zadovoljavaju (2.1.1) onda potpuno pravilo podrazumijeva proizvoljno biranje neke od tih riječi c_x, dok nepotpuno pravilo zahtjeva ponovno slanje.

Teorema 2.2. *Za binarno simetrični kanal sa prelaznom vjerovatnoćom* $p < 1/2$*, pravilo dekodiranja po maksimumu vjerovatnoće je isto kao dekodiranje po pravilu najbližeg susjeda.*

Dokaz. Neka je sa C označen kod koji se koristi i neka je x primljena riječ dužine n.

Za bilo koju riječ c dužine n i za bilo koje $0 \leq i \leq n$ važi:

$$d(x,c) = i \Leftrightarrow P(x - primljeno \,|\, c - poslat) = p^i * (1-p)^{(n-i)}.$$

Kako $p < 1/2$, to slijedi da je

$$p^0 * (1-p)^n > p^1 * (1-p)^{n-1} > p^2 * (1-p)^{n-2} > \cdots > p^n * (1-p)^0$$

Po definiciji, pravilo dekodiranja po maksimumu vjerovatnoće nam daje da se x dekodira u $c \in C$ ako je $P(x - primljen|c - poslat)$ najveća vjerovatnoća. Ona je najveća za $i = 0$ tj. za $d(x,c)$ najmanje. Stoga je pravilo dekodiranja po maksimumu vjerovatnoće, u ovom slučaju, isto kao i pravilo najbližeg susjeda. □

Primjer 2.4. *Binarni kod* $C = \{0000, 0011, 1000, 1100, 0001, 1001\}$ *se šalje preko binarnog simetričnog kanala. Neka je* $x = 0111$ *primljeno. Tada:*

$d(x, 0000) = 3$

$d(x, 0011) = 1$

$d(x, 1000) = 4$

$d(x, 1100) = 3$

$d(x, 0001) = 2$

$d(x, 1001) = 3$

Koristeći pravilo najbližeg susjeda (tj. pravilo maksimalne vjerovatnoće) mi x dekodiramo u 0011.

Primjer 2.5. *Neka je* $C = \{000, 011\}$ *binarni kod. Tabela dekodiranja po nepotpunom pravilu najbližeg susjeda za C izgleda ovako:*

Oznaka $*$ *u tabeli označava zahtjevanu retransmisiju.*

$primljeno : x$	$d(x, 000)$	$d(x, 011)$	$dekodiramo :$
000	0	2	000
100	1	3	000
010	1	1	*
001	1	1	*
110	2	2	*
101	2	2	*
011	2	0	011
111	3	1	011

Pored dužine i veličine koda, još jedna važna i korisna karakteristika koda je njegova distanca.

Definicija 2.7. *Neka je kod C takav da sadrži najmanje dvije riječi. Udaljenost ili distanca koda C, u oznaci $d(C)$ je $min\{d(x, y)|x, y \in C, x \neq y\}$.*

Kod dužine n, veličine M i distance d, se označava kao $[n, M, d]$ kod. Brojevi n, M,d se nazivaju parametri koda. Ispostavlja se da je distanca koda usko povezana sa mogućnostima uviđanja i ispravljanja grešaka.

2.3 Detekcija i korekcija greške

Definicija 2.8. *Neka je u pozitivan cio broj. Kod C ima m-mogućnosti detektovanja greške ako kad god riječ iz C uključuje najmanje jednu ali najviše m grešaka, rezultujuća riječ nije riječ u C. Kod C ima tačno m-mogućnosti detektovanja greške ako ima m- mogućnosti uočavanja greške ali nema $m + 1$- tih mogućnosti.*

Primjer 2.6. *Binarni kod $C = \{00000, 00111, 11111\}$ ima jednostruku mogućnost spoznaje greške pošto mijenjanjem bilo koje riječi koda u jednoj poziciji ne dobijamo neku drugu riječ u C. Drugim rječima:*
$00000 \rightarrow 00111$ *zahtjeva promjenu tri bita,*

$00000 \to 11111$ *zahtjeva pet grešaka,*

$00111 \to 11111$ *zahtjeva dvije promjene,*

Tačnije kod C *ima tačno jednu mogućnost uočavanja greške jer pri promjeni prve dvije pozicije riječi* 00111 *dobijamo drugu kodnu riječ* 11111*, pa* C *nema dvostruku mogućnost spoznaje greške.*

Teorema 2.3. *Neka je* u *pozitivan cio broj. Kod* C *ima* u*- mogućnosti detektovanja greške ako i samo ako je* $d(C) \geq u+1$*, ili drugim riječima kod sa distancom* d *je kod sa tačno* $d-1$ *mogućnosti detektovanja greške.*

Dokaz. Pretpostavimo da je $d(C) \geq u+1$.Dokažimo da C ima u-mogućnosti detektovanja greške. Ako $c \in C$ i x je takvo da je

$$1 \leq d(c,x) \leq u \leq < d(C)$$

onda $x \notin C$ pošto je distanca za C ili $u+1$ ili više, pa kako je c proizvoljno, jasno C ima u-mogućnosti detektovanja.

Obratno, ako je C posjeduje u- mogućnosti detektovanja, dokažimo da je onda $d(C) \geq u+1$. Ako pretpostavimo suprotno, tj. da je $d(C) < u+1$ tj. da $d(C) \leq u$, tada postoje c_1, c_2 iz C da je

$$1 \leq d(c_1, c_2) = d(C) \leq u$$

. Sada ako počnemo od riječi $c_1 \in C$ i primjenimo $d(c)$ grešaka, pošto je $1 \leq d(C) \leq u$ dobijemo riječ c_2 koja je u C, međutim to nije saglasno sa pretpostavkom da C ima u-mogućnosti detektovanja greške. □

Definicija 2.9. *Neka je* v *pozitivan cio broj. Kažemo da kod* C *ima* v*-mogućnosti ispravke greške ako je pri dekodiranju (po pravilu minimalne udaljenosti) moguće*

ispraviti v ili manje grešaka, pod pretpostavkom da se koristi nepotpuno pravilo dekodiranja. Kod C ima strogo v-mogućnosti ispravke ako on ima v, ali nema $v+1$-mogućnosti ispravke greške.

Primjer 2.7. *Posmatrajmo binarni kod $C = \{000, 111\}$. Koristeći pravilo dekodiranja po minimalnoj udaljenosti, dobijamo :*

- *Ako je* 000 *poslato onda, ako postoji jedna greška u prenosu, primljena riječ (*100, 010, 001*) će biti dekodirana u* 000.
- *Ako je* 111 *poslato i jedna greška postoji u prenosu onda će primljena riječ (*110, 101, 011*) biti dekodirana u* 111.

U oba slučaja, jedna greška je ispravljena. Dakle, C ima jednostruku mogućnost ispravke.
Ako postoje najmanje dvije greške u prenosu, onda pravilo dekodiranja po minimalnoj udaljenosti daje pogrešnu riječ. Na primjer ako je 000 *poslato i postoje dvije greške i primljeno je na primjer* 011 *onda će* 011 *biti dekodirano u* 111. *Dakle, C ima strogo jednu mogućnost ispravke.*

Teorema 2.4. *Kod C ima v-mogućnosti korekcije greške ako i samo ako je $d(C) \geq 2v+1$ tj. kod sa distancom d ima tačno $\lfloor (d-1)/2 \rfloor$-mogućnosti ispravke, pri čemu je $\lfloor x \rfloor$ najveći cio broj manji ili jednak od x.*

Dokaz. Pretpostavimo da je $d(c) \geq 2v+1$. Neka je c poslata riječ i neka je x primljena riječ. Ukoliko postoji v ili manje grešaka u transmisiji onda $d(x, c) \leq v$. Dalje, za bilo koju riječ $y \in C$ da je $y \neq c$ imamo

$$d(c, y) \leq d(c, x) + d(x, y)$$

tj.

$$d(x, y) \geq d(c, y) - d(x, c)$$

.

Dakle,

$$d(c, y) \geq 2v + 1 - v = v + 1 > d(x, c)$$

. Ovo važi za bilo koje $y \in C$. To bi onda x bilo korektno dekodirano u c ako se koristi pravilo najbližeg susjeda. Ovo pokazuje da C ima v-mogućnosti ispravke greške. Obratno, pretpostavimo da C ima v-mogućnosti ispravke greške. Ako $d(C) < 2v + 1$ onda postoje dvije riječi $c_1, c_2 \in C$ takve da je

$$d(c_1, c_2) = d(C) < 2v + 1$$

tj.

$$d(c_1, c_2) = d(C) \leq 2v$$

.

Zapazimo da ako je $d(c_1, c_2) < v + 1 \leq 2v$ tj. $d(c_1, c_2) \leq v$ onda c_1 može biti poslato i primljeno kao c_2 uključujući najviše v grešaka, a onda ove greške neće biti ispravljene (u suštini biće neprimjećene) pošto je $c_2 \in C$. Ovo je međutim u kontradikciji sa tim da C ima v mogućnosti ispravljanja greške. Dakle,mora biti da je

$$d(c_1, c_2) \geq v + 1$$

. Sada bez gubljenja opštosti, možemo pretpostaviti da se c_1 i c_2 razlikuju u tačno

$d = d(C)$ prvih pozicija, pri čemu je

$$v + 1 \leq d \leq 2v$$

. Ako je riječ $x = x_1 x_2 \dots x_v x_{v+1} \dots x_d x_{d+1} \dots x_n$ takva da se u prvih v slova slaže sa c_2, zatim se u sledećih $d - v$ slova slaže sa c_1 i u zadnjih $n - d$ slova se slaže i sa c_1 i sa c_2 onda imamo

$$d(x, c_2) = d - v \leq v = d(x, c_1)$$

. To imamo dva slučaja:

Prvi: $d(x, c_2) < d(x, c_1)$ kada je x dekodirano nepravilno u c_2 i

drugi: $d(x, c_1) = d(x, c_2)$ u kome će biti zatražen ponovni postupak. Na ovaj način dolazimo do kontradikcije, pa mora biti da je $d(C) \geq 2v + 1$. Dakle važi teorema. $\square$

Glava 3

Konačna polja

3.1 Struktura konačnih polja

Iz prethodnog poglavlja znamo da je kodni alfabet A konačan skup. Mi ćemo skup A opremiti algebarskim strukturama. Ideja je da definišemo dvije operacije na skupu A tako da A postane polje.

Teorija konačnih polja počinje sa eminentnim matematičarima kao što su Pjer de Ferma (*Pierre de Fermat*) i Leonard Ojler (*Leonhard Euler*). Razvija se zahvaljujući radu Karla Fridriha Gausa (*Johann Carl Friedrich Gauss*) i Evarista Galoa(*Évariste Galois*) a postaje interesantna poslednjih decenija zbog svojih brojnih primjena u matematici, računarstvu i teoriji komunikacija. U ovom poglavlju navešćemo neke zaključke iz teorije konačnih polja.[2]

Definicija 3.1. *Polje F je neprazan skup elemenata sa dvije operacije: $''+''$ i $''*''$, koje nazivamo sabiranje i množenje i koje zadovoljavaju sledeće aksiome:*
Za sve $a, b, c \in F$ važi:

1. *F je zatvoren za operacije $+$ i $*$, tj.*
   $a + b \in F$ *i* $a * b \in F$

2. *Zakon komutativnosti za operacije* $+$ *i* $*$*, tj.*

   $a + b = b + a$ *i* $a * b = b * a$

3. *Zakon asocijacije za operacije* $+$ *i* $*$*, tj.*

   $(a + b) + c = a + (b + c)$ *i* $a * (b * c) = (a * b) * c$

4. *Distributivni zakon* $a * (b + c) = a * b + a * c$

   Još važi da moraju postojati dva različita elementa: 0 *i* 1 *u* F *koje nazivamo aditivni i multiplikativni neutralni element i koji zadovoljavaju sledeće:*

5. $a + 0 = a$ *za sve* $a \in F$

6. $s * 1 = a$ *i* $a * 0 = 0$ *za sve* $a \in F$

7. *Za sve* $a \in F$ *postoji aditivni inverzni element* $(-a)$ *u* F *takav da je* $a+(-a) = 0$

8. *Za sve* $a \neq 0$ *iz* F *postoji multiplikativni inverzni element* $a^{-1} \in F$ *takav da je* $a * a^{-1} = 1$.

Obično umjesto $a * b$ pišemo samo ab i sa F^* označavamo skup $F \setminus \{0\}$.

Dakle, struktura $(F, +, *)$ je polje ako važi da je $(F, +)$ Abelova grupa, $(F \setminus \{0\})$ je Abelova grupa i operacija $*$ je distributivna prema $+$.

Primjer 3.1. *Neka polja sa kojima se često susrećemo su:*

$\mathbb{Q}$- *polje racionalnih brojeva, polje* $\mathbb{R}$ *i polje* $\mathbb{C}$.

Sve aksiome iz prethodne definicije su zadovoljene ako posmatramo standardno sabiranje i množenje. Međutim, ova polja su beskonačna.

Označimo sa $\mathbb{Z}_2$ *skup* $\{0, 1\}$. *Definišimo sabiranje i množenje preko sledećih tablica.*

$+$	0	1
0	0	1
1	1	0

$*$	0	1
0	0	0
1	0	1

Jasno se vidi da je $\mathbb{Z}_2$ polje sa samo dva elementa.

Lema 3.1. *Neka su a,b dva bilo koja elementa polja F. Tada:*

- $(-1)a = -a$
- $ab = 0 \Rightarrow a = 0 \vee b = 0$

Dokaz. Važi: $(-1)a + a = (-1)a + 1a = ((-1) + 1)a = 0a = 0$
dakle, $(-1)a = -a$ jer je $(-a)$ jedinstven. Dalje, za $a \neq 0$, ako je $ab = 0$ imamo $0 = a^{-1} * 0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$ pa $b = 0$. □

Polje koje sadrži samo konačan broj elemenata nazivamo konačno polje.
Skup F koji zadovoljava aksiome $1. - 7.$ se naziva komutativni prsten.

Primjer 3.2. *Skup svih cijelih brojeva $\mathbb{Z} = \{0, \pm 1, \pm 2, \dots\}$ formira prsten sa uobičajno definisanim sabiranjem i množenjem. Skup svih polinoma nad poljem F u oznaci:*

$$F[x] := \{a_0 + a_1 x + a_2 x^2 + \dots a_n x^n : a_i \in F, n \geq 0\},$$

formira prsten sa uobičajnim sabiranjem i množenjem polinoma.

Definicija 3.2. *Neka su a,b i $m > 1$ cijeli brojevi. Kažemo da je a kongruentno sa b po modulu m u oznaci $a \equiv b \ (mod\ m)$ ako $m|(a - b)$.*

Za date cijele brojeve a i $m > 1$, pomoću algoritma dijeljenja imamo $a = mq + b$, gdje je b jedinstveno određeno sa a i m, $0 \leq b \leq m - 1$. Dakle, svaki cijeli broj a je kongruentan sa tačno jednim od brojeva $0, 1, 2, \dots m - 1$ po modulu m. Cijeli broj b naziva se ostatak dijeljenja sa m. Ako je $a \equiv b \ (mod\ m)$ i $c \equiv d \ (mod\ m)$ onda imamo da je $a + c \equiv b + d \ (mod\ m)$ i $a - c \equiv b - d \ (mod\ m)$ i $a * c \equiv b * d \ (mod\ m)$. Za cijele brojeve $m > 1$ sa $\mathbb{Z}_m$ ili $\mathbb{Z}|_{(m)}$ označavaćemo skup $\{0, 1, \dots m - 1\}$ i definišimo sabiranje "+" i množenje "*" na $\mathbb{Z}_m$ na sledeći način:

$a + b =$ ostatak pri dijeljenju $a + b$ sa m

$a * b =$ ostatak od $a * b$ pri dijeljenju sa m.

Lako je pokazati da sve aksiome $1. - 7.$ važe tako da $(\mathbb{Z}_m, +, *)$ formira prsten. Za $\mathbb{Z}_2$ znamo da je polje jer važi i osma aksioma. Međutim lako se pokazuje da na primjer $\mathbb{Z}_4$ nije polje. Dakle, $\mathbb{Z}_m$ je za neke m polje a za neke nije.

Definicija 3.3. *Neka je R prsten. Element $a \in R$, $a \neq 0$ naziva se lijevim (desnim) djeliocem nule ukoliko postoji $b \in R$, $b \neq 0$ da je $ab = 0$ ($ba = 0$).*

Definicija 3.4. *Asocijativni, komutativni prsten R sa jedinicom, bez djelitelja nule naziva se integralni domen.*

Zbog leme 3.1. zaključujemo da je svako polje integralni domen.

Teorema 3.1. *$\mathbb{Z}_m$ je polje ako i samo ako je m prost broj.*

Dokaz. Pretpostavimo, prvo, da je $\mathbb{Z}_m$ polje, to je onda ono integralni domen tj. nema djelitelja nule. Dokažimo da je m prost. Pretpostavimo suprotno tj. da je m složen, tj. $m = k * l$, za $k, l < m$ i $k, l \in \mathbb{Z}_m$. Znamo da je u $\mathbb{Z}_m$ $m \equiv 0$ tj. m i nulu poistovjećujemo pa je $k * l = 0$. To onda ili $k = 0$ ili $l = 0$ pa $m|k$ ili $m|l$ tj. $m \leq k$ ili $m \leq l$, a ovo nije tačno, pa dolazimo do kontradikcije. Dakle, m je prost.

Sada neka je m prost. Dokažimo da je $\mathbb{Z}_m$ polje. Neka je a nenulti element iz $\mathbb{Z}_m$, tj. $0 < a < m$. Znamo da je a uzajamno prost sa m. To onda postoje u i v da $0 \leq u \leq m - 1$ i $u * a + v * m = 1$. Pošto je $v * m \equiv 0 \ (mod\ m)$ to onda $u * a \equiv 1 \ (mod\ m)$ tj. $u * a = 1$ u Z_m. Dakle, $u = a^{(-1)}$. Kako je a proizvoljno uzet to je $\mathbb{Z}_m$ polje. □

Za prsten R, cijeli broj $n \geq 1$ i $a \in R$ u oznaci na ili $n * a$ označavaćemo

$$\sum_{i=1}^{n} a = a + a + a + \ldots a.$$

Definicija 3.5. *Neka je F polje. Karakteristika za F je najmanji pozitivan cio broj p takav da je $p * 1 = 0$, gdje je 1 multiplikativni neutral za F. Ako p ne postoji onda kažemo da je karakteristika za F nula. Oznaka: $charF$.*

Karakteristika za $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ je nula. Dok je za bilo koji prost broj p karakteristika polja $\mathbb{Z}_p$ jednaka p.

Teorema 3.2. *Karakteristika bilo kog polja je ili nula ili prost broj.*

Dokaz. Jasno je odmah da 1 ne može biti karakteristika polja jer $1 * 1 = 1 \neq 0$. Pretpostavimo sada suprotno tj.da karakteristika p može biti složen broj. Neka $p = m * n$, za pozitivne cijele brojeve $1 < n, m < p$. Neka su sad $a = m * 1$ i $b = n * 1$ elementi polja. Tada

$$a * b = m * 1 * n * 1 = (\sum_{i=1}^{m} 1) * (\sum_{i=1}^{n} 1) = m * n * 1 = p * 1 = 0.$$

Zaključujemo, $a * b = 0$, pa je $a = 0$ ili $b = 0$. Dakle, $m * 1 = 0$ ili $n * 1 = 0$ za $m, n < p$, što bi značilo da p nije karakteristika polja. Konačno, p mora biti prost. □

Neka su E i F dva polja i neka je F podskup od E. Polje F nazivamo podpolje polja E ako je sabiranje i množenje sa E, restrikovano na F isto kao ono definisano na samom polju F.
Na primjer, polje racionalnih brojeva $\mathbb{Q}$ je podpolje polja realnih brojeva $\mathbb{R}$, ali i polja kompleksnih brojeva $\mathbb{C}$. Takođe, $\mathbb{R}$ je podpolje za $\mathbb{C}$.Evo još jedne ekvivalentne definicije podpolja.

Definicija 3.6. *Neprazan skup S polja $(F, +, *)$ je podpolje polja F ako je $(\forall a, b \in S)$ $a - b \in S$ i $(\forall a, b \in S)$ $ab^{-1} \in S$.*

Takođe, da napomenemo ako je F polje karakteristike p, gdje je p prost broj, onda se $\mathbb{Z}_p$ može posmatrati kao podpolje za F.

Teorema 3.3. *Konačno polje karakteristike p (p prost broj) sadrži p^n elemenata, za neko $n \geq 1$ cijeli broj.*

Dokaz. Konačno polje označimo sa F. Izaberimo jedan element α_1 iz F^*. Tvrdimo da su: $0 * \alpha_1$, $1 * \alpha_1$,...,$(p-1) * \alpha_1$ međusobno različiti. Ukoliko bi $i * \alpha_1 = j * \alpha_1$, za neke $0 \geq i \geq j \geq p-1$ onda: $(j-i) * \alpha_1 = 0$ i $0 \geq j - i \geq p-1$.
Kako je karakteristika za F jednaka p to onda $j - i = 0$ tj. $j = i$. Ako je

$$F = \{0 * \alpha_1, 1 * \alpha_1 \ \ldots, (p-1) * \alpha_1\}$$

onda $|F| = p$ pa je tvrđenje tačno. Inače, izaberimo element α_2 iz skupa $F \setminus \{0 * \alpha_1, 1 * \alpha_1, \ldots, (p-1) * \alpha_1\}$ i tvdrdimo da su $a_1 * \alpha_1 + a_2 * \alpha_2$ međusobno različiti za sve a_1, a_2, $0 \leq a_1, a_2 \leq p-1$.
U suprotnom, kada bi važilo, $a_1 * \alpha_1 + a_2 * \alpha_2 = b_1 * \alpha_1 + b_2 * \alpha_2$ za neke $0 \leq a_1, a_2, b_1, b_2 \leq p-1$ onda bismo imali da je $a_2 = b_2$ jer inače $\alpha_2 = (b_2 - a_2)^{-1} * (a_1 - b_1) * \alpha_1$, a ovo bi značilo kontradikciju sa tim da je α_2 izabrano iz skupa $F \setminus \{0 * \alpha_1, 1 * \alpha_1, \ldots, (p-1) * \alpha_1\}$, jer je Z_p podpolje u F i $(b_2 - a_2)^{-1} * (a_1 - b_1)$ pripada Z_p. Dakle, $a_2 = b_2$, pa je i $a_1 = b_1$, tj. $(a_1, a_2) = (b_1, b_2)$. Zaključujemo da su svi različiti. Kako je F konačan ovako nastavljamo i dobijemo elemente $\alpha_1, \alpha_2, \ldots \alpha_n$ takve da $\alpha_i \in F \setminus \{a_1 * \alpha_1 + \ldots a_{i-1} * \alpha_{i-1} : a_1, \ldots a_{i-1} \in Z_p\}$ za sve $2 \leq i \leq n$ i $F = \{a_1 * \alpha_1 + \cdots + a_n * \alpha_n : a_1, \ldots a_n \in Z_p\}$. Na isti način dokažemo da su svi $a_1 * \alpha_1 + \cdots + a_n * \alpha_n$ međusobno različiti za sve $a_i \in Z_p$. To onda dobijamo $|F| = p^n$. □

Lema 3.2. *Za svaki element b konačnog polja F sa q elemenata važi: $b^q = b$.*

Dokaz. Trivijalno je za slučaj $b = 0$. Ako $b \neq 0$ posmatrajmo sve nenulte elemente iz F, tj. $F^* = \{b_1, b_2, \ldots b_{q-1}\}$. To onda $F^* = \{bb_1, bb_2, \ldots bb_{q-1}\}$. Dalje,

$$b_1 b_2 \ldots b_{q-1} = (bb_1)(bb_2) \ldots (bb_{q-1})$$

tj.

$$b_1 b_2 \dots b_{q-1} = b^{q-1}(b_1 b_2 \dots b_{q-1})$$

. Dakle, $b^{q-1} = 1$, tj. $b^q = b$. □

3.2 Prsten polinoma

Beskonačni nizovi elemenata polja F tj. nizovi $(a_0, a_1, \dots), a_i \in F$ se nazivaju polinomima nad poljem F ako je samo konačno mnogo koeficijenata (komponenata) $a_i \in F$ različito od nule. Pišemo: $P = (a_0, a_1, \dots a_n)$ i $a_j = 0$ za $j > n$. U tom slučaju n nazivamo stepen polinoma P i koristimo oznaku $deg(P)$. Po dogovoru uzimamo $deg(0) = -\infty$. Na skupu svih polinoma nad poljem F definišemo binarne operacije $+$ i $*$ na sledeći način $P = (a_0, a_1, \dots a_n), Q = (b_0, b_1, \dots b_m), P+Q = (d_0, d_1, \dots d_s)$ gdje je $d_j = a_j + b_j$ i s je najveći nenegativni cio broj za koji je $d_s \neq 0$, $P*Q = (c_0, c_1, \dots c_r)$ i $c_k = \sum_{i=0}^{k} a_i b_{k-i}$ i r je najveći nenegativan cio broj za koji $c_r \neq 0$. Polinom $(0, 1)$ nad poljem F sa jediničnim elementom 1, označimo sa x. Tada svaki polinom $P = (a_0, a_1, \dots a_n)$ nad poljem F možemo zapisati u obliku $a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$. Označimo skup svih polinoma nad poljem F sa $F[x]$. Lako se dokazuje da je ova struktura prsten.

Nenulti polinom $f(x) = \sum_{i=0}^{n} a_i x^i$ stepena n se naziva moničnim ako je $a_n = 1$.

Definicija 3.7. *Za polinom $f(x)$ pozitivnog stepena kažemo da je reducibilan nad F ako postoje polinomi $g(x)$ i $h(x)$ nad F takvi da je $deg(g(x)) < deg(f(x))$ i $deg(h(x)) < deg(f(x))$ i $f(x) = g(x) * h(x)$. Inače ako ovi polinomi ne postoje kažemo da je $f(x)$ ireducibilan.*

Primjer 3.3.

1. *Polinom $f(x) = x^4 + 2x^6 \in Z_3[x]$ je stepena 6 i reducibilan je tj. svodljiv nad*

Z_3 jer $f(x) = x^4(1 + 2x^2)$.

2. *Polinom $g(x) = 1 + x + x^2 \in Z_2[x]$ je stepena 2. Nesvodljiv je. Inače bi imao linearni faktor x ili $x - 1$ međutim $g(0) = 1$ i $g(1) = 1$.*

3. *Slično, polinomi $1+x+x^3$ i $1+x^2+x^3$ su nesvodljivi nad Z_2 jer nemaju linearne faktore.*

Važi teorema o dijeljenju polinoma čiji dokaz nećemo navoditi.

Teorema 3.4. *Neka je $f(x) \in F[x]$ polinom stepena $n \geq 1$. Tada za bilo koji polinom $g(x) \in F[x]$ postoji jedinstven par $(s(x), r(x))$ polinoma, da je $deg(r(x)) < deg(f(x))$ ili $r(x) = 0$ i $g(x) = s(x)f(x) + r(x)$. Polinom $r(x)$ naziva se ostatak od $g(x)$ pri dijeljenju sa $f(x)$.*

Definicija 3.8. *Neka su $f(x), g(x) \in F[x]$ dva nenulta polinoma. Najveći zajednički djelilac za ove polinome u oznaci $nzd(f(x), g(x))$ je monični polinom najvećeg stepena koji je djelilac i za $f(x)$ i za $g(x)$. Kažemo da je $f(x)$ uzajamno prost sa $g(x)$ ako je $nzd(f(x), g(x)) = 1$. Najmanji zajednički sadržalac za $f(x)$ i $g(x)$ u oznaci $nzs(f(x), g(x))$ je monični polinom najmanjeg stepena koji sadrži i $f(x)$ i $g(x)$.*

Neka je ϕ funkcija koja svakom polinomu $P = (a_0, a_1, \ldots a_n)$ nad poljem F pridružuje tzv. polinomsku funkciju $\phi(P)$ koja slika polje F u polje F tako da $(\forall x \in F)$ $\phi(P)(x) = a_0 + a_1x + \ldots a_nx^n$. Ispostavlja se da je ϕ epimorfizam. Čak ako je F beskonačno ovo preslikavanje je izomorfizam, međutim to nije slučaj sa konačnim poljima.

Primjer 3.4. *Posmatrajmo $F = \mathbb{Z}_3 = \{0, 1, 2\}$ i polinome $p = (1, 2, 1, 1), q = (1, 0, 1)$ iz $\mathbb{Z}_3$. Ove polinomme pomoću ϕ preslikavamo u polinomske funkcije $\phi(p) = 1 + 2x + 1x^2 + 1x^3$ i $\phi(q) = 1 + x^2$. Pokazaćemo da u ovom slučaju ϕ nije injekcija. Ispostavlja*

se da je $\phi(p)(x) = \phi(q)(x)$ *za sve* $x \in \mathbb{Z}_3$. *Dakle, u pitanju su iste funkcije, ali polinomi* p *i* q *očigledno nisu isti.*

Da napomenemo vrijednost polinoma u nekoj tački je vrijednost odgovarajuće polinomske funkcije u toj tački. Navodimo još jedno jednostavno tvrđenje.

Teorema 3.5. *Polinom drugog ili trećeg stepena iz* $F[x]$ *svodljiv je ako i samo ako ima bar jedan korijen u polju* F.

Pomoću polinoma nad poljem F se konstruišu proširenja polja. Na $F[x]$ takođe možemo definisati relaciju kongruencije slično kao na bilo kom prstenu. Ispostavlja se da je to relacija ekvivalencije i $F[x]$ posiječen po toj relaciji sa standardno definisanim sabiranjem i množenjem čini komutativni asocijativni prsten sa jedinicom.
Sledeća teorema slično se dokazuje kao teorema 3.1. i ukazuje na analogije između prstena cijelih brojeva $\mathbb{Z}$ i prstena polinoma $F[x]$.

Teorema 3.6. *Neka je* $f(x)$ *polinom nad poljem* F *stepena* $deg(f(x)) \geq 1$. *Tada* $F[x]|_{(f(x))}$ *sa sabiranjem i množenjem definisanim na standardan način formira prsten. Štaviše* $F[x]|_{(f(x))}$ *je polje ako i samo ako je* $f(x)$ *nesvodljiv tj. ireducibilan polinom nad* F.

Ako je $f(x)$ linearni polinom onda je polje $F[x]|_{(f(x))}$ samo polje F.

Primjer 3.5. *Posmatrajmo prsten* $R[x]|_{(1+x^2)} = \{a + bx, a, b \in R\}$. *Ovo je polje jer je* $(1 + x^2)$ *nesvodljiv nad* $\mathbb{R}$. *Tačnije ovo je kompleksno polje* $\mathbb{C}$. *To je jasno jer je nula polinoma* $(1 + x^2)$ *imaginarna jedinica* i.

Teorema 3.7. *Neka je* F *podpolje polja* E *takvo da* $|F| = q$. *Tada element* $b \in E$ *leži u* F *ako i samo ako* $b^q = b$.

Dokaz. Direktni smjer je očigledan zbog leme 3.2.. Obratno, neka je $b \in E$ i neka $b^q = b$. Posmatrajmo polinom $x^q - x$. On ima najviše q različitih korijena u E. Svi elementi

iz F su korijeni za ovaj polinom i $|F| = q$, pa je $F = \{svikorijenipolinomax^q - xuE\}$. Dakle za sve $b \in E$, za koje $b_q = b$ slijedi da je $b \in F$. □

Za dva polja E i F kompozicija $E \circ F$ je najmanje polje koje sadrži i E i F.

Teorema 3.8. *Za bilo koji prost broj p i cio broj $n \geq 1$, postoji jedinstveno konačno polje sa p^n elemenata.*

Dokaz. Prvo dokažimo postojanje. Posmatrajmo polje Z_p. Neka je $f(x)$ ireducibilan polinom nad Z_p. Tada je $Z_p[x]|_{(f(x))}$ polje. Slično kao u Teoremi 3.3. dokazujemo da ovo polje ima tačno p^n elemenata. Dokažimo jedinstvenost. Posmatrajmo dva polja E, F koja imaju po p^n elemenata. Posmatrajmo polinom $x^{p^n} - x$ nad kompozicijom $E \circ F$. Biće $E = \{$svi korijeni polinoma $x^{p^n} - x\} = F$. Dakle, jedinstvenost je dokazana. □

Konačno polje sa q elemenata označavaćemo sa F_q. Za ireducibilni polinom $f(x)$ stepena n nad poljem F neka je α neki njegov korijen. Tada polje $F[x]|_{f(x)}$ može biti predstavljeno kao $F[\alpha] = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : a_i \in F\}$.

Definicija 3.9. *Element α u konačnom polju F_q naziva se primitivni element ili generator za F_q ako je $F_q = \{0, \alpha, \alpha^2, \ldots, \alpha^{q-1}\}$.*

Definicija 3.10. *Red nenultog elementa $a \in F_q$, u oznaci $ord(a)$, je najmanji pozitivan cio broj k takav da je $a^k = 1$.*

Primjer 3.6. *Pošto ne postoje nelinearni faktori polinoma $1 + x^2$ nad F_3 to je on ireducibilan nad F_3. Posmatrajmo element a polja $F_9 = F_3[a]$ koji je korijen polinoma $1 + x^2$. Tada $a^2 = -1$, $a_3 = a(a^2) = -a$ i $a^4 = (-1)^2 = 1$, pa je $ord(a) = 4$.*

Lema 3.3. *Red $ord(a)$ dijeli $q - 1$ za sve $a \in F_q^*$. Takođe za svaka dva nenulta elementa $a, b \in F_q^*$ ako je $nzd(ord(a), ord(b)) = 1$ onda $ord(ab) = ord(a)ord(b)$.*

Dokaz. Neka je a proizvoljni nenulti element iz F_q. Neka je m pozitivan cio broj takav da $a^m = 1$. Neka je $m = c * ord(a) + d$, za neke cijele brojeve c i d. Biće $1 = a^m = a^{c*ord(a)+d} = (a^{ord(a)})^c * a^d = a^d$. Dakle, $a^d = 1$ pa $d = 0$ tj.$ord(a)$ dijeli m. Za $a \in F_q^*$ važi $a^{q-1} = 1$ pa na osnovu prethodnog $ord(a)$ dijeli $q - 1$.

Što se tiče drugog dijela teoreme, neka je $r = ord(a)ord(b)$. Jasno $a^r = 1 = b^r$, $(ab)^r = 1$. Dakle, $ord(ab) \leq ord(a)ord(b)$. Sa druge strane ako označimo $t = ord(ab)$ onda $1 = (ab)^{t*ord(a)} = (a^{ord(a)})^t * b^{t*ord(a)} = b^{t*ord(a)}$. Slijedi da $ord(b)$ dijeli $t * ord(a)$, a kako su $ord(a)$ i $ord(b)$ uzajamno prosti to $ord(b)$ dijeli t.

Slično tako dobijemo $ord(a)$ dijeli t, pa i $ord(a) * ord(b)$ dijeli t. Dakle, $t = ord(ab) \geq ord(a)ord(b)$ tj. $t = ord(a)ord(b)$ □

Teorema 3.9. *Nenulti element polja F_q je njegov primitivni element ako i samo ako je njegov red $q - 1$. Svako konačno polje ima najmanje jedan primitivni element.*

Dokaz. Jasno je da je $a \in F_q^*$ element reda $q - 1$ ako i samo ako su elementi $a, a^2, \ldots a^{q-1}$ različiti. To je ekvivalentno sa tim da je $F_q = \{0, a, a^2, \ldots a^{q-1}\}$, tj. a je primitivni element polja F_q.

Sada dokažimo da svako konačno polje F_q ima bar jedan primitivni element.

Neka je m najmanji zajednički sadržalac za redove svih elemenata iz F_q^*. Ako je $m = r_1^{k_1} \ldots r_n^{k_n}$ kanonska faktorizacija za m, gdje su r_i, $i = 1, \ldots n$ različiti prosti brojevi, onda za sve $i = 1, \ldots n$ postoji $b_i \in F_q^*$ da je $ord(b_i) = r_i^{k_i}$. Jer ako je r^k prosti stepen u kanonskoj faktorizaciji od m onda r^k dijeli $ord(a)$ za neko $a \in F_q^*$ pa je red za $a^{\frac{ord(a)}{r^k}}$ je r^k.

Zaključujemo da su svih $q - 1$ elemenata iz F_q^* korijenovi polinoma $x^m - 1$, pa je $m \geq q - 1$. Prema prethodnoj lemi postoji $b \in F_q^*$ da je $ord(b) = m$ i m dijeli $q - 1$. Dakle, $m = ord(b) = q - 1$. □

Ako je α korijen ireducibilnog polinoma stepena m nad poljem F_q i ako je on

primitivni element polja $F_{q^m} = F_q[\alpha]$, onda svaki element u F_{q^m} može biti predstavljen kao polinom od α ili kao stepen od α jer

$$F_{q^m} = \{a_0 + a_1\alpha + \dots a_{m-1}\alpha^{m-1}, a_i \in Fq\} = \{0, \alpha, \alpha^2, \dots \alpha^{q^m-1}\}$$

. Kažemo da je polje F proširenje polja K ako i samo ako je K podpolje polja F.

Definicija 3.11. *Za element $a \in F$ kažemo da je algebarski element polja F nad poljem K ako je on korijen polinoma čiji su koeficijenti elementi polja K. Ako za $a \in F$ ne postoji takav polinom, kažemo da je a transcedentan element polja F.*

Neka je F_q podpolje polja F_r. Za svaki element $a \in F_r$, zanima nas nenulti polinom $f(x) \in F_q[x]$ najmanjeg stepena da je $f(a) = 0$.

Definicija 3.12. *Minimalni polinom elementa $a \in F_q^m$ u odnosu na F_q je nenulti monični polinom $f(x)$ najmanjeg stepena u $F_q[x]$ da je $f(a) = 0$.*

Teorema 3.10. *Minimalni polinom elementa iz F_{q^m} u odnosu na F_q postoji i jedinstven je. On je, također, nesvodljiv nad F_q.*

Dokaz. Neka je $a \in F_{q^m}$. Kako je a korijen polinoma $x^{q^m} - x$ onda je egzistencija minimalnog polinoma jasna. Pretpostavimo da su $M_1(x)$, $M_2(x)$ dva polinoma iz $F_q[x]$ i da su oba minimalna za a. Prema algoritmu dijeljenja biće $M_1(x) = s(x)M_2(x) + r(x)$, za neke $s(x)$ i $r(x)$ takve da je $r(x) = 0$ ili $deg(r(x)) < deg(M_2(x))$.Dalje je, $0 = M_1(a) = s(a)M_2(a) + r(a) = r(a)$. Po definiciji minimalnog polinoma biće $r(x) = 0$, tako da $M_2(x)$ dijeli $M_1(x)$. Slično dobijemo da $M_1(x)$ dijeli $M_2(x)$, pa zaključujemo $M_1(x) = M_2(x)$ jer su oba monična. Jedinstvenost je dokazana. Neka je $M(x)$ minimalni polinom za a. Pretpostavimo da je svodljiv nad F_q. Tada bismo imali dva monična polinoma $f(x), g(x) \in F_q[x]$ da je $deg(f(x)) < deg(M(x))$, $deg(g(x)) <$

$deg(M(x))$ i $M(x) = f(x)g(x)$. Dalje, $0 = M(a) = f(a)g(a)$ pa je $f(a) = 0$ ili $g(a) = 0$, a ovo je kontradiktorno sa tim da je $M(x)$ minimalni polinom za a. □

Teorema 3.11. *Ako je monični ireducibilni polinom $M(x) \in F_q[x]$ takav da ima $a \in F_{q^m}$ kao korijen onda je on minimalni polinom za a u odnosu na F_q.*

Dokaz. Neka je $f(x)$ minimalni polinom za a u odnosu na F_q. Prema algoritmu dijeljenja postoje $h(x), e(x) \in F_q[x]$ da $M(x) = h(x)f(x) + e(x)$ da je $deg(e(x)) < deg(f(x))$ i $0 = M(a) = e(a)$ pa je $e(x) = 0$ i $f(x) = M(x)$, pošto je $M(x)$ monični ireducibilni polinom i $f(x)$ nije nenulta konstanta. □

Neka je $f(x) \in F_q[x]$ monični ireducibilni polinom stepena m. Neka je $a \in F_q^m$ korijen od $f(x)$. Onda je minimalni polinom za a u odnosu na F_q baš polinom $f(x)$.

Glava 4

Linearno kodiranje

Linearni kod dužine n nad konačnim poljem F_q je potprostor vektorskog prostora F_q^n.

Njihova algebarska struktura omogućava nam da ih lakše opišemo nego nelinearne kodove. Navešćemo neka svojstva vektorskih prostora nad konačnim poljima.

4.1 Vektorski prostori

Definicija 4.1. *Neka je F_q konačno polje reda q. Neprazan skup V, zajedno sa vektorskim sabiranjem "+" i skalarnim množenjem elementima iz F_q, "$*$", je vektorski (linearni) prostor nad F_q ako zadovoljava sledeće uslove:*
za sve $u, v, w \in V$ i sve $\lambda, \mu \in F_q$:

1. $u + v \in V$
2. $(u + v) + w = u + (v + w)$
3. *Postoji* $0 \in V$ *sa svojstvom* $0 + v = v + 0 = v$, *za sve* $v \in V$
4. *Za svaki* $v \in V$ *postoji element iz* V *u oznaci* $(-v)$ *takav da je* $v + (-v) = (-v) + v = 0$

5. $u + v = v + u$

6. $\lambda * v \in V$

7. $\lambda * (u + v) = \lambda * u + \lambda * v$, $(\lambda + \mu) * u = \lambda * u + \mu * u$

8. $(\lambda\mu) * u = \lambda * (\mu * u)$

9. *ako je* 1 *multiplikativni neutral za* F_q *onda je* $1 * u = u$.

Neka je F_q^n skup svih vektora dužine n sa komponentama iz F_q tj. $F_q^n = \{(v_1, v_2, \ldots, v_n) : v_i \in F_q\}$. Definišemo vektorsko sabiranje u F_q^n kao sabiranje po komponentama, koristeći sabiranje definisano u polju F_q. Za $u = (u_1, u_2, \ldots, u_n)$, $v = (v_1, v_2, \ldots, v_n)$ iz F_q^n,

$$u + v = (u_1 + v_1, u_2 + v_2, \ldots u_n + v_n)$$

. Skalarno množenje na F_q^n definišemo kao množenje po komponentama. Za proizvoljno $v = (v_1, v_2, \ldots, v_n) \in F_q^n$ i $\lambda \in F_q$,

$$\lambda * v = (\lambda * v_1, \lambda * v_2, \ldots, \lambda * v_n)$$

.

Označimo $0 = (0, 0, \ldots, 0) \in F_q^n$.

Primjer 4.1. *Za* $q = 2$, $F_2 = \{0, 1\}$ *polje,* $C_4 = \{(0,0,0,0), (1,0,1,0), (0,1,0,1), (1,1,1,1)\}$ *jeste prostor nad* F_2.

Definicija 4.2. *Neprazan podskup* C *vektorskog prostora* V *je potprostor od* V *ako je on sam za sebe vektorski prostor sa istim vektorskim sabiranjem i skalarnim množenjem kao i* V.

Sledeća teorema slijedi odmah iz prethodne definicije.

Teorema 4.1. *Neprazan podskup C vektorskog prostora V nad F_q je potprostor ako i samo ako važi sledeće : ako $x, y \in C$ i $\lambda, \mu \in F_q$ onda $\lambda * x + \mu * y \in C$.*

Definicija 4.3. *Neka je V vektorski prostor nad F_q. Linearna kombinacija vektora: $v_1, v_2, \ldots v_r$ iz V je vektor $\lambda_1 * v_1 + \ldots \lambda_r * v_r$ gdje su $\lambda_i \in F_q$ neki skalari.*

Definicija 4.4. *Neka je V vektorski prostor nad poljem F_q. Skup vektora $\{v_1, v_2, \ldots v_r\}$ u V je linearno nezavisan ako $\lambda_1 * v_1 + \ldots \lambda_r * v_r = 0$ povlači da je $\lambda_1 = \lambda_2 = \ldots \lambda_r = 0$. Dati skup je linearno zavisan ako nije linearno nezavisan, tj. ako postoje $\lambda_1, \lambda_2, \ldots \lambda_r$ iz F_q koji nisu istovremeno jednaki nuli, da $\lambda_1 * v_1 + \ldots \lambda_r * v_r = 0$.*

Bilo koji skup koji sadrži 0 je linearno zavisan.

Definicija 4.5. *Neka je V vektorski prostor nad F_q i $S = \{v_1, v_2, \ldots v_k\}$ neprazan podskupod V. Linearni omotač od S se definiše kao skup*

$$< S >= \{\lambda_1 * v_1 + \ldots \lambda_k * v_k, \lambda_i \in F_q\}$$

.

Ako je $S = \emptyset$ definišemo $< S >= 0$. Jasno je da je $< S >$ potprostor od V. Kažemo da je on generisan sa S. Za dati potprostor C od V i njegov podskup S kažemo da S generiše C ako je $C =< S >$. Ako je S već potprostor od V onda $< S >= S$.

Definicija 4.6. *Neka je V vektorski prostor nad F_q. Neprazan skup $B = \{v_1, v_2, \ldots v_k\}$ u V je baza za V ako je $V =< B >$ i B je linearno nezavisan.*

Da napomenemo da ako je $B = \{v_1, v_2, \ldots v_k\}$ baza u V onda bilo koji vektor iz V može biti predstavljen na jedinstven način kao linearna kombinacija vektora iz B. Takođe, može postojati više baza jednog istog prostora V nad F_q, ali sve one imaju isti

broj elemenata i taj broj nazivamo dimenzija prostora V nad F_q. Koristimo oznaku $dim(V)$.

Teorema 4.2. *Neka je V vektorski prostor nad F_q. Ako je $dim(V) = k$ onda V ima q^k elemenata i ima*

$$\frac{1}{k!}\prod_{i=0}^{k-1}(q^k - q^i)$$

različitih baza.

Dokaz. Ako je $\{v_1, v_2, \dots v_k\}$ baza za V onda je

$$V = \{\lambda_1 * v_1 + \dots \lambda_k * v_k : \lambda_i \in F_q, i = 1, \dots k\}$$

. Pošto $|F_q| = q$ onda postoji tačno q izbora za svaki od λ_i pa V ima tačno q^k elemenata. Neka je $B = \{v_1, v_2, \dots v_k\}$ jedna baza za V. Pošto $v_1 \neq 0$ postoji $q^k - 1$ izbora za v_1. Da bi B bila baza nikako ne smije važiti $v_2 \in < v_1 >$ pa postoji $q^k - q$ izbora za v_2. Nastavljajući u ovom maniru zaključujemo da za izbor v_i imamo $q^k - q^{i-1}$ mogućnosti za sve $2 \leq i \leq k$. Za izbor $(v_1, v_2, \dots v_k)$ ima $\prod_{i=0}^{k-1}(q^k - q^i)$ mogućnosti. Međutim pošto poredak vektora nije bitan za bazu to je broj različitih baza za V jednak $\frac{1}{k!}\prod_{i=0}^{k-1}(q^k - q^i)$. □

Definicija 4.7. *Neka su $u = (u_1, u_2, \dots, u_n)$, $v = (v_1, v_2, \dots, v_n)$ iz F_q^n. Skalarni proizvod za u i v se definiše kao $u \circ v = u_1v_1 + u_2v_2 + \dots u_nv_n \in F_q$. Koristimo i oznaku $< u, v >$.*

Za u, v kažemo da su ortogonalni ako $< u, v >= 0$.

Definicija 4.8. *Neka je S neprazan podskup za F_q^n. Ortogonalni komplement $S^\perp$ za S je skup:*

$$S^\perp = \{v \in F_q^n :< v, s >= 0 \text{ za sve } s \in S\}$$

. *Ako je* $S = \emptyset$ *onda definišemo* $S^{\perp} = F_q^n$.

Lako je uočiti da je $S^{\perp}$ uvijek potprostor vektorskog prostora F_q^n za bilo koji skup S iz F_q^n i važi $< S >^{\perp} = S^{\perp}$.

Teorema 4.3. *Neka je* S *podskup od* F_q^n*, tada:*

$$dim(< S >) + dim(S^{\perp}) = n$$

.

Dokaz. Jasno je ako je $S = \emptyset$. Ukoliko je $dim(< S >) = k \leq 1$ pretpostavimo da je baza $\{v_1, v_2, \ldots, v_k\}$. Pokažimo da je $dim(S^{\perp}) = n - k$. Jasno $x \in S^{\perp}$ ako i samo ako $< v_1, x >=< v_2, x >= \cdots < v_k, x >= 0$, tj. $Ax^{\perp} = 0$ gdje je A matrica dimenzije $k \times n$ čije su vrste vektori baze. $Ax^{\perp} = 0$ je linearni sistem sa k jednačina od n nepoznatih. Prostor rješenja ovog sistema je dimenzije $n - k$. □

Obnovili smo osnovno o vektorskim prostorima, vratimo se proučavanju linearnih kodova.

4.2 Linearni kodovi

Definicija 4.9. *Linearni kod dužine* n *nad* F_q *je potprostor prostora* F_q^n.

Definicija 4.10. *Neka je* C *linearni kod u* F_q^n. *Dualni kod za* C *je ortogonalni komplement potprostora* C *u* F_q^n. *Koristimo oznaku* $C^{\perp}$. *Dimenzija linearnog koda* C *je dimenzija vektorskog prostora* C *nad* F_q.

Neka je C linearni kod dužine n nad F_q. Važi:

1. $|C| = q^{dim(C)}$ tj. $dim(C) = log_q|C|$.

2. $C^{\perp}$ je linearni kod i važi $dim(C) + dim(C^{\perp}) = n$.

3. $(C^{\perp})^{\perp} = C$.

Linearni kod C dužine n i dimenzije k nad F_q se obično naziva q-arni $[n, k]$ kod ili $[n, q, k]$ kod. Nekada se i distanca koda naglašava.

Definicija 4.11. *Neka je C linearni kod. Kažemo da je C samoortogonalan ako je $C \subseteq C^{\perp}$. Kažemo da je C samodualan ako je $C = C^{\perp}$.*

Dimenzija samoortogonalnog koda dužine n mora biti manja ili jednaka od $n/2$ a dimenzija samodualnog koda dužine n je $n/2$.
Hemingova udaljenost(distanca) $d(x, y)$ riječi x i y definisana je ranije u drugom poglavlju. Sada ćemo definisati pojam Hemingove težine.

Definicija 4.12. *Neka je x riječ u F_q^n. Hemingova težina riječi x u oznaci $wt(x)$ se definiše kao broj nenultih koordinata u x tj. $wt(x) = d(x, 0)$, gdje je 0-nula riječ.*

Za svaki element $x \in F_q$ Hemingovu težinu definišemo na sledeći način:

$$wt(x) = d(x, 0) = \begin{cases} 1, & x \neq 0 \\ 0, & x = 0 \end{cases}$$

Napišmo $x \in F_q^n$ kao $x = (x_1, x_2, \ldots x_n)$. Hemingova težina riječi x se može ekvivalentno definisati sa :

$$wt(x) = wt(x_1) + wt(x_2) + \cdots + wt(x_n)$$

.

Lema 4.1. *Ako su $x, y \in F_q^n$ onda $d(x, y) = wt(x - y)$.*

Dokaz. Posmatrajmo prvo riječi dužine 1. Neka su $x, y \in F_q$ tada $d(x, y) = 0$ ako i samo ako $x = y$ ako i samo ako $x - y = 0$ tj. $wt(x - y) = 0$. Sada ako imamo riječi $x, y \in F_q^n$ prethodni postupak ponovimo za sve komponente tj. slova riječi x i y. □

Teorema 4.4. *Neka je q parno. Ako $x, y \in F_q^n$ onda $d(x, y) = wt(x + y)$.*

Dokaz. Ovo je jasno ako znamo da za q parno važi: za svako $a \in F_q$ $a = -a$. □

Za $x = (x_1, x_2, \ldots x_n)$ i $y = (y_1, y_2, \ldots y_n)$ iz F_q^n definišimo sledeću operaciju

$$x * y = (x_1 * y_1, x_2 * y_2, \ldots x_n * y_n)$$

. Lako se dokazuje da ako je $x, y \in F_2^n$ onda $wt(x + y) = wt(x) + wt(y) - 2wt(x * y)$. Dakle, $wt(x) + wt(y) \geq wt(x + y)$ za sve $x, y \in F_2^n$.

Definicija 4.13. *Neka je C linearan kod. Minimalna (Hemingova) težina koda C je najmanja od svih težina nenultih riječi u C. Oznaka: $wt(C)$.*

Teorema 4.5. *Neka je C linearan kod nad F_q. Tada $d(C) = wt(C)$.*

Dokaz. Već znamo da je $d(x, y) = wt(x - y)$. Po definiciji postoje $x', y' \in C$ da je $d(x', y') = d(C) = wt(x' - y') \geq wt(C)$ jer važi da $x' - y' \in C$. Suprotno, postoji $z \in C \setminus \{0\}$ da je $wt(C) = wt(z) = d(z, 0) \geq d(C)$ pa $wt(C) = d(C)$. □

Primjer 4.2. *Posmatrajmo binarni linearni kod $C = \{0000, 1000, 0100, 1100\}$. Vidimo $wt(1000) = 1$, $wt(0100) = 1$, $wt(1100) = 2$. Zaključujemo $d(C) = 1$.*

Navedimo neke prednosti linearnih kodova.

1. Linearni kod je vektorski prostor i može biti potpuno opisan pomoću baze.

2. Distanca linearnog koda je jednaka njegovoj težini.

3. Kodiranje i dekodiranje za linearne kodove je brže i jednostavnije nego za proizvoljne nelinearne kodove.

Definicija 4.14. *Neka je A matrica nad F_q. Elementarna transformacija vrsta u A je bilo koja od sledeće tri operacije:*

1. *zamijena dvije vrste,*
2. *množenje vrste nenultim skalarom,*
3. *zamijena vrste njenom sumom sa drugom vrstom pomnoženom skalarom.*

Definicija 4.15. *Dvije matrice su ekvivalentne po vrstama ako jedna može biti dobijena od druge nizom elementarih transformacija vrsta.*

Sada ćemo objasniti dva algoritma za nalaženje baze datog koda.

4.2.1 Algoritmi za nalaženje baze koda

Algoritam 1

Zadajemo neprazan skup S iz F_q^n. Želimo pronaći bazu za linearni kod $C =< S >$ generisan sa S. Metoda podrazumijeva sledeće : od matrice A čije su vrste riječi u S, koristeći elementarne transformacije vrsta, dođemo do trougaonog oblika matrice A. Nenulte vrste dobijene matrice predstavlaju vektore baze za C.

Primjer 4.3. *Neka je $q = 3$, $F_3 = \{0, 1, 2\}$ i neka je $S = \{12101, 20110, 01122, 11010\}$. Nađimo bazu za linearni kod $C =< S >$.*

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

Sabirajući prvu i drugu vrstu, zatim množeći prvu sa 2 *i sabirajući je sa četvrtom vrstom dobijamo sl. matricu:*

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

Stavljajući treću vrstu na drugu poziciju, zatim sabirajući je sa preostale dvije dobijamo trougaoni oblik matrice :

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

Zaključujemo da je baza u C *sledeća* $\{12101, 01122, 00001\}$.

Algoritam 2

Unosimo neprazan skup S iz F_q^n. Želimo pronaći bazu za linearni kod $C =< S >$ generisan sa S. Metoda podrazumijeva formiranje matrice A čije su kolone riječi iz S, zatim korišćenje elementarih transformacija vrsta da A dovedemo do trougaonog oblika. Bazu će činiti vodeće kolone matrice.

Primjer 4.4. *Neka je* $q = 2$, $F_2 = \{0, 1\}$, $S = \{11101, 10110, 01011, 11010\}$. *Nađimo bazu za* $C =< S >$ *po algoritmu 2. Formiramo matricu* A *stavljajući riječi iz* S *kao*

kolone u A.

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

Koristeći elementarne transformacije vrsta svedemo A na trougaoni oblik:

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

Vodeće kolone su prva, druga i četvrta pa one čine bazu za C: $\{11101, 10110, 11010\}$. *Primjetimo da je u drugom algoritmu dobijena baza podskup skupa S, dok to nije obavezno u algoritmu* 1.

4.2.2 Generatorna i kontrolna matrica

Poznavanje baze linearnog koda omogućava nam da eksplicitno opišemo svaku njegovu riječ. U teoriji kodiranja baza za linearni kod se obično predstavlja u vidu matrice, nazvane generatorna matrica, dok se matrica koja predstavlja bazu dualnog koda naziva kontrolna matrica koda C.

Definicija 4.16. *Generatorna matrica linearnog koda C je matrica G čije su vrste bazni vektori za C, dok je kontrolna matrica H koda C generatorna matrica za dualni*

kod $C^{\perp}$.

- Ako je C $[n,k]$ linearni kod onda je G matrica $k \times n$ a H je $(n-k) \times n$ matrica.
- Kako baza vektorskog prostora ima više to onda i generatornih matrica za linearni kod takođe ima više. Čak i kada je baza fiksirana, permutacije redova generatorne matrice takođe daju drugačiju generatornu matricu.
- Vrste tj. redovi generatorne matrice su linearno nezavisne. Isto važi i za matricu H. Da bi pokazali da je neka $k \times n$ matrica G generatorna matrica za dati $[n,k]$ linearni kod, dovoljno je pokazati da su redovi u G kodne riječi za C i da su linearno nezavisni.

Definicija 4.17. *Kažemo da je generatorna matrica u standardnoj formi ako je oblika* $(I_k|X)$. *Kažemo da je kontrolna matrica u standardnoj formi ako je oblika* $(Y|I_{n-k})$.

Lema 4.2. *Neka je* C $[n,k]$ *linearni kod nad* F_q, *sa generatornom matricom* G. *Važi da* $v \in F_q^n$ *pripada* $C^{\perp}$ *ako i samo ako je* v *ortogonalan sa svakom vrstom iz* G, *tj.* $v \in C^{\perp} \Leftrightarrow vG^{\top} = 0$. *Ako je data* $(n-k) \times n$ *matrica* H *onda je* H *kontrolna matrica za* C *ako i samo ako su vrste u* H *linearno nezavisne i važi* $HG^{\top} = 0$.

Dokaz. Sa r_i označimo i-tu vrstu u G, $r_i \in C, \forall i \in \{1,2,\dots k\}$ i svako $c \in C$ može biti predstavljeno: $c = \lambda_1 * r_1 + \cdots + \lambda_k * r_k$, gdje $\lambda_i \in F_q$, $\forall i \in \{1,2,\dots k\}$. Ako $v \in C^{\perp}$ onda $v * c = 0, \forall c \in C$, pa je v ortogonalno na svako r_i, tj. $vG^{\top} = 0$. Suprotno, ako je $v * r_i = 0, \forall i \in \{1,2,\dots k\}$ onda jasno, $\forall c \in C, c = \lambda_1 * r_1 + \cdots + \lambda_k * r_k$ važi $v * c = 0$ tj. $v \in C^{\perp}$. Ako je H kontrolna matrica, onda su vrste za H linearno nezavisne po definiciji. Pošto su vrste za H riječi u $C^{\perp}$ to onda $HG^{\top} = 0$. Obratno, ako $HG^{\top} = 0$, onda vrste iz H, tj. potprostor vrsta iz H je sadržan u $C^{\perp}$. Još važi da su vrste u H linearno nezavisne i dimenzija za H je $n-k$, pa je H kontrolna matrica. □

Alternativna, ekvivalentna formulacija prethodne leme je:
Neka je C $[n, k]$ linearni kod nad F_q sa kontrolnom matricom H. Onda $v \in F_q^n$ pripada C ako i samo ako je v ortogonalno na svaku vrstu iz H, tj. $v \in C \Leftrightarrow vH^\top = 0$. Za datu $k \times n$ matricu G znamo da je ona generatorna za C ako i samo ako su joj vrste linearno nezavisne i $GH^\top = 0$.

Teorema 4.6. *Neka je C linearni kod i H kontrolna matrica za C. Onda važi:*

1. *C ima distancu $\geq d$ ako i samo ako bilo kojih $d-1$ kolona u H je linearno nezavisno i*

2. *C ima distancu $\leq d$ ako i samo ako H ima d kolona koje su linearno zavisne.*

Dokaz. Neka je $v = (v_1, v_2, \ldots v_n) \in C$ riječ težine $l > 0$. Pretpostavimo da su nenulte koordinate na pozicijama $i_1, i_2, \ldots i_l$ pa $v_j = 0$ za sve j izvan $\{i_1, i_2, \ldots i_l\}$. Neka je sa c_i označena i-ta kolona matrice H. Prema alternativnoj formulaciji prethodne leme imamo da C sadrži nenultu riječ $v = (v_1, v_2, \ldots v_n)$ težine l ako i samo ako je $0 = vH^\top = v_{i_1} * c_{i_1}^\top + \cdots + v_{i_l} * c_{i_l}^\top$, što je tačno ako i samo ako su ovih l kolona u H linearno nezavisne. Ako kažemo da je $d(C) \geq d$ to je ekvivalentno sa tim da C ne sadrži nijednu nenultu riječ težine $\leq d-1$, što je opet ekvivalentno tome da je bilo kojih $d-1$ linearno nezavisno u H. Slično ako kažemo da je distanca za C manja ili jednaka od d to je ekvivalentno sa tim da C sadrži nenulte riječi težine $\leq d$, što je opet ekvivalentno sa tim da H ima $\leq d$ koje su linearno zavisne. □

Neposredna posledica ove teoreme je sledeća lema.

Lema 4.3. *Neka je C linearni kod i H njegova kontrolna matrica. Sledeća tvrđenja su ekvivalentna:*

1. *C ima distancu d.*

2. *Bilo kojih $d-1$ kolona u H je linearno nezavisna i H ima d kolona koje su linearno zavisne.*

Primjer 4.5. *Neka je C binarni linearni kod sa kontrolnom matricom*

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

Vidimo da H nema nultih kolona niti bilo koje dvije kolone u sumi daju 0, to su znači bilo koje dvije kolone u H linearno neazvisne. Međutim prva, treća i četvrta u sumi daju nulu tj. linearno su zavisne, pa je $d = 3$.

Teorema 4.7. *Ako je generatorna matrica G linearnog $[n, k]$ koda data u standardnoj formi sa $G = (I_k|X)$ onda je $H = (-X^\top|I_{n-k})$.*

Primjer 4.6. *Nađimo G i H za binarni linearni kod $C =< S >$ gdje je $S = \{11101, 10110, 01011, 11010\}$. Prema prvom algoritmu:*

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

A svedemo na trougaoni oblik:

$$\left[\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right]$$

Uočavamo generatornu matricu:

$$G = \left[\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right] = \left[\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right]$$

Biće,

$$H = \left[\begin{array}{ccc|cc} 0 & 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 \end{array}\right]$$

Važi $GH^\top = 0 = HG^\top$.

Treba napomenuti da ne mora svaki linearni kod da ima generatornu matricu u standardnoj formi. Međutim, nakon pogodnih permutacija koordinata riječi i dozvoljenog množenja odgovarajućih koordinata sa nenultim skalarom, uvijek možemo dobiti novi kod koji ima generatornu matricu u standardnoj formi. Tada govorimo ekvivalentnim kodovima.

Definicija 4.18. *Dva* $[n, M]$ *koda nad* F_q *su ekvivalentni ako jedan može biti dobijen od drugog kombinacijom sledećih operacija:*

- *permutacija n simbola riječi,*
- *množenje nenultim skalarom simbola na fiksnoj poziciji.*

Primjer 4.7. *Neka je* $q = 2$ *i* $n = 4$ *i* $C = \{0000, 0101, 0010, 0111\}$. *Birajući da permutujemo slova u riječi pomoću sledeće premutacije* $(1, 2, 3, 4) \to (2, 4, 1, 3)$, *dobijemo ekvivalentan kod* $C' = \{0000, 1100, 0001, 1101\}$.

Teorema 4.8. *Bilo koji linearni kod* C *je ekvivalentan sa nekim linearnim kodom* C' *koji ima generatornu matricu u standardnoj formi.*

Dokaz. Ako je G generatorna matrica koda C prevedimo je elementarnim transformacijam u dijagonalni oblik. Reorganizujmo kolone u tako dobijenoj dijagonalnoj formi da vodeće kolone budu prve i formiraju identičku matricu. Dobijemo G' matricu u standardnoj formi koja je generatorna matrica koda koga ćemo označiti sa C' i važi da je on ekvivalentan kodu C. □

Sada ćemo objasniti šta podrazumijeva kodiranje linearnim kodovima.
Neka je C $[n, k, d]$ linearni kod nad konačnim poljem Fq. Svaka riječ iz C predstavlja neku vrstu informacije, pa C predstavlja q^k različitih vrsta informacija. Ako je fiksirana baza u C i to $\{r_1, \dots r_k\}$ tada svaka riječ može biti jedinstveno određena sa linearnom kombinacijom $v = u_1 * r_1 * \cdots + u_k * r_k$, gdje su $u1, \dots u_k \in F_q$. Ekvivalentno, možemo posmatrati generatornu matricu G koda C, čija je i-ta vrsta r_i, vektor izabrane baze. Za dati vektor $u = (u_1, u_2, \dots u_k) \in F_q^k$ jasno je da je $v = uG = u_1 * r_1 * \cdots + u_k * r_k$ kodna riječ u C. Obratno, svaki $v \in C$ može se zapisati kao $v = uG$, gdje je $u \in F_q^k$. Dakle svaka riječ $u \in F_q^k$ može biti kodirana kao $v = uG$. Proces predstavljanja elemenata $u \in F_q^k$ kao riječi $v = uG$ je takozvani proces kodiranja.

Primjer 4.8. *Neka je C binarni $[5,3]$ linearni kod sa generatornom matricom*

$$G = \left[\begin{array}{ccc|cc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right]$$

Tada se poruka $u = 101$ kodira na sledeći način: $v = uG = (101)G = 10011$.

Zapazimo da je informaciona stopa jednaka 3/5, tj. samo su 3 bita od 5 korišćena za emitovanje poruke.

Obratimo pažnju na neke prednosti generatorne matrice G u standardnoj formi. Prvo, ako je C dat sa $G = (I|X)$ onda imamo da je $H = (-X^\top|I)$, zatim ako je $[n,k,d]$ linearni kod dat sa $G = (I|X)$ onda je trivijalno naći poruku u iz date kod riječi $v = uG$, jer $v = uG = u(I|X) = (u, uX)$, tj. prvih k cifara u riječi v daje poruku u. Te cifre nazivamo informaciske. Ostalih $n-k$ cifara zovemo kontrolnim. One predstavljaju redundanciju koja je dodata poruci da bi se zaštitila od smetnji pri prenosu.

4.2.3 Dekodiranje linearnih kodova

Najčešće koristimo dekodiranje po pravilu najbližeg susjeda za linearne kodove.

Definicija 4.19. *Neka je C linearni kod dužine n nad F_q i neka je $u \in F_q^n$ bilo koji vektor dužine n. Definišimo suskup (koset) koda C određen sa u na sledeći način: $C + u = \{v + u | v \in C\} = u + C$.*

Teorema 4.9. *Neka je C neki $[n,k,d]$ linearni kod nad konačnim poljem F_q, tada:*

1. *Svaki vektor iz F_q^n je sadržan u nekom suskupu (kosetu) koda C.*

2. *Za sve* $u \in F_q^n$, $|C+u| = |C| = q^k$.

3. *Za sve* $u, v \in F_q^n$, $u \in C+v \to C+u = C+v$.

4. *Dva koseta su ili identična ili nemaju zajednički presjek.*

5. *Postoji* q^{n-k} *različitih koseta koda* C.

6. *Za sve* $u, v \in F_q^n$, $u - v \in C \Leftrightarrow u, v$ *pripadaju istom kosetu koda* C.

Dokaz. 1. Jasno je da za $v \in F_q^n$ važi $v \in C+v$.

2. Po definiciji $C+u$ ima najviše $|C| = q^k$ elemenata. Tačnije $v+u$ i $w+u$ iz $C+u$ su isti ako i samo ako $v = w$ pa $|C+u| = |C|$.

3. Ako $u \in C+v$ onda $C+u \subseteq C+v$ pa zbog 2. $C+u = C+v$.

4. Posmatrajmo $C+u$ i $C+v$. Ako $x \in (C+u) \cap (C+v)$ onda $C+x = C+u$ i $C+x = C+v$ pa $C+u = C+v$.

5. Jasno imajući u vidu da je $|F_q^n| = q^n$ i $|C| = q^k$.

6.$u - v = c \in C \to u = c+v \in C+v \to C+u = C+v \to u, v$ pripadaju istom kosetu. Obratno ako su $u, v \in C+x \to u = c+x, v = c'+x$ za $c, c' \in C \to u - v = c - c' \in C$. □

Definicija 4.20. *Riječ sa najmanjom Hemingovom težinom u kosetu zove se vodeća riječ koseta.*

Neka je C linearni kod. Pretpostavimo da je riječ v prenešena preko komunikacionog kanala a riječ w je primljena sa greškom: $e = w - v \in w + C$. Biće $w - e = v \in C$, pa je zadovoljeno da su e i w u istom kosetu. Inače e nazivamo uzorak greške. Pošto je najbolje da se pojavljuje uzorak greške sa najmanjom težinom, dekodiranje po principu najbližeg susjeda radi za linearne kodove. Nakon primanja riječi w, biramo riječ $e \in w + C$ najmanje težine i zaključujemo da je $v = w - e$ poslata riječ, tj. dekodiramo w u $v = w - e$.

Primjer 4.9. *Neka je* $q = 2$ *i* $C = \{0000, 1011, 0101, 1110\}$.*Dekodirajmo sledeću primljenu riječ* $w = 1101$. *Imamo sledeće kosete:* $C = 0000 + C, 0001 + C, 0010 + C, 1000 + C$. *Posmatrajmo* $w + C = 1000 + C$. *Riječ najmanje težine u ovo kosetu je* 1000 *pa* $1101 - 1000 = 0101$. *Tako da zaključujemo da je najvjerovatnije poslata riječ upravo* 0101.

U slučaju da imamo više mogućnosti za izbor uzorka greške e, zavisno od toga da li koristimo potpunu ili nepotpunu metodu vršimo prroizvoljno biranje ili ponovni prenos. Prethodna šema dekodiranja efikasna je ako je dužina linearnog koda n mala jer potrebna je ušteda vremena pri prepoznavanju koseta kojem primljena riječ pripada. Vrijeme možemo uštedjeti koristeći tzv. sindrom za prepoznavanje koseta kojem primljena riječ pripada.

Definicija 4.21. *Neka je* C *neki* $[n, k, d]$ *linearni kod nad* F_q *i* H *njegova kontrolna matrica. Za proizvoljno* $w \in F_q^n$ *definišemo sindrom za* w *kao riječ* $s(w) = wH^\top \in F_q^{n-k}$.

Teorema 4.10. *Neka je* C *neki* $[n, k, d]$ *linearni kod i* H *odgovarajuća kontrolna matrica za* C. $\forall u, v \in F_q^n$ *važi:*

1. $s(u + v) = s(u) + s(v)$
2. $s(u) = 0 \Leftrightarrow u$ *je riječ u* C
3. $s(u) = s(v) \Leftrightarrow u$ *i* v *pripadaju istom kosetu od* C.

Dokaz ove teoreme jasno slijedi iz definicije sindrom riječi i dijela 6. teoreme 4.10. Vidimo da dio 3. govori o tome da mi možemo prepoznati koset po njegovom sindromu jer sve riječi u datom kosetu imaju isti sindrom. Postoji $''1-1''$ korespodencija između koseta i njegovog sindroma. Pošto su sindromi riječi iz F_q^{n-k}, to ih je najviše q^{n-k}.

Znamo da koseta ima q^{n-k} pa je i odgovarajućih sindroma q^{n-k}. Dakle, svi vektori iz F_q^{n-k} su sindromi.

Koraci pri konstrukciji tabele koja povezuje svaku vodeću riječ koseta sa njenim sindromom, pretpostavljajući potpunu metodu dekodiranja prema najbližem susjedu su:

Korak 1: Izlistati sve kosete za kod i izabrati iz svakog koseta riječ najmanje težine kao vodeću.

Korak 2: Naći kontrolnu matricu H za kod i za svaku vodeću riječ koseta u, izračunati sindrome $s(u) = uH^\top$.

Dekodiranje pomoću sindroma podrazumijeva sledeće korake:

Korak 1: Za primljenu riječ w izračunajmo njen sindrom $s(w)$.

Korak 2: U tabeli nađemo vodeću riječ koseta u sa sindromom $s(u) = s(w)$.

Korak 3: Dekodiramo w kao $v = w - u$.

Posebna vrsta linearnih kodova su Hemingovi kodovi. Tu spadaju kodovi koji omogućavaju otkrivanje jedne greške i kodovi koji omogućavaju ispravljanje jedne greške. Takođe u linearne kodove spadaju Golejevi kodovi (po švajcarsko-američkom matematičaru i fizičaru *Marcel J. E. Golay (1902-1989)*), Rid-Milerovi kodovi (po američkim matematičarima i inženjerima *Irving S. Reed (1923-2012), David E. Muller (1924-2008)*), ciklični linearni kodovi i mnogi drugi koje nećemo proučavati u ovom radu.[1]

Glava 5

Zaključak

Htjeli mi to da prihvatimo ili ne, matematika je nauka koja duboko zalazi u mnoge sfere života. Ona objašnjava suštinu mnogim praktičnim stvarima i pojavama.
Ovaj rad se pozabavio, prije svega, tome da čitaoca uvede u osnove Teorije kodiranja, da ga zaintrigira tom veoma širokom i korisnom granom matematike koja je usko povezana sa Algebrom.
Nadam se da će ovaj rad biti od koristi, bar kao početna literatura, onima koji žele da se detaljnije i opširnije bave linearnim kodovima.

Bibliografija

[1] Bojan Berleković. *Neke klase linearnih kodova*. Univerzitet u Novom Sadu.

[2] Joseph J. Rotman. *Advanced Modern Algebra*. Prentice Hall.

[3] Chaoping Xing San Ling. *Coding Theory, A First Course*. Cambridge University Press, New York, 2004.