Osnove kodova za ispravljanje grešaka

Milan M.Milosavljević

Ciljevi

- Šta su blok kodovi
- Kako se meri rastojanje izmedju kodnih reči
- Šta je težina kodne reči
- Šta je minimalno rastojanje i minimalna težina jednog koda
- Kako se odnose ove veličine prema broju grešaka koje kodovi mogu da detektuju ili isprave

Uvod

- Kada se jedna kodna reč z_i prenosi po nekom kanalu sa šumovima i na izlazu kanala primi $\hat{z}$, tada se odgovarajuća greška u prenosu dobija kao razlika $e = \hat{z}$- z_i.
- Ključna ideja algebarskog kodovanja je dodavanje algebarske strukture u skupu kodnih reči tako da se greška može lako izraziti pomoću operacija koje definišu tu algebarsku strukturu.

Primer 6.1 *Razlike binarnih sekvenci*

Prirodno je razlike binarnih sekvenci definisati preko XOR operacije. Dakle važi npr

11011-01101=10110

Uvod

- Tehnički govoreći operacija oduzimanja iz primera 6.1 odgovara aritimetici po modulu 2, odnosno odgovarajuća algebarska struktura je polje Galoa GF(2). Kodne reči dužine n u tom slučaju pripadaju vektorskom prostoru $GF(2)^n$. Ovaj koncept se direktno proširuje na D-arne kodove korišćenjem aritimetike po modulu D.

Definicija 6.1 *Blok kod*

D-arni blok kod dužine n je neprazan podskup vektorskog prostora n-torki $GF(D)^n$. Jednostavnije rečeno to su D-arne reči dužine n posmatrane kao vektori kolone.

Uvod

Primer 6.2 *Blok kod*

Skup {1101, 0110, 1110} je jedan primer binarnog blok koda.

Drugi primer blok koda je ternarni kod sa simbolima 0, 1, 2, takav da je 1+2=0, 1+1=2, 1+0=1, 2+2=1, 2+0=2 (aritmetika u GF(3)), čije su kodne reči {120, 201, 222, 010}.

Skup {011, 110, 10} nije blok kod, budući da kodne reči nisu iste dužine.

Hemingovo rastojanje i težine kodnih reči

Definicija 6.2 *Hemingovo rastojanje*

Hamingovo rastojanje $d(z_i, z_j)$, izmedju dve reči z_i i z_j iste dužine, odnosno dva niza dužine n, je broj simbola (pozicija) u kojima se te dve kodne reči razlikuju.

Primer 6.3 *Heminigovo rastojanje*

Hemingovo rastojanje izmedju 101010 i 111010 je 1, pošto se ove dve reči razlikuju samo na 2. poziciji.

Hemingovo rastojanje izmedju 1010 i 0101 je 4, pošto se ove dve reči razlikuju u svim pozicijama.

Hemingovo rastojanje izmedju 1010 i 111010 nije definisano, budući da su reči različite dužine.

Hemingovo rastojanje i težine kodnih reči

Hemingovo rastojanje je zaista rastojanje u strogom matematičkom smislu (zadovoljava tri aksioma metričkog rastojanja – simetrija, nulto rastojanje i nejednakost trougla)

Definicija 6.3 *Težine kodnih reči*

Težina jedne reči jednaka je broju nenultih simbola u toj reči.

Primer 6.4 *Težine kodnih reči*

Težina reči 10110 je 3, dok je težina reči 00000000 jednaka 0. Težina reči 0001000 je jednaka 1.

Osobina 6.1

Hemingovo rastojanje dve kodne reči jednako je težini njihove razlike, odnosno

$$d(z_i, z_j) = \mathrm{w}(z_i - z_j),$$

gde d( ) označava Hemingovo rastojanje, a w( ) težinu reči.

Hemingovo rastojanje i težine kodnih reči

Primer 6.5

Ovaj primer pokazuje ekvivalentnost Hemingovog rastojanja i težine razlike:

$$d(10110,11010)=2$$

$$w(10110-11010)=w(01100)=2.$$

Osobina 6.2

Težina kodnih reči je uvek pozitivna ili jednaka nuli.

Definicija 6.4

Nula kodna reč je kodna reč sastavljena samo od nula. Označava se sa 0.

Hemingovo rastojanje i težine kodnih reči

Osobina 6.3

Težina jedne kodne reči je nula, ako i samo ako je kodna reč nula kodna reč.

Osobina 6.4

Težine su simetrična funkcija, odnosno $w(z_i) = \mathrm{w}(-z_i)$, gde se pod $-z_i$ podrazumeva reč u kojoj je svaki simbol zamenjen suprotnim simbolom.

Primer 6.6 *Simetrija težina*

Razmotrimo ternarni kod sa simbolima 0,1,2 u GF(3). Tada je

w(-1202102)=w(2101201)=5=w(1202102).

Primetimo da je u binarnom slučaju $-z_i$=z_i (-1=1, -0=0).

Hemingovo rastojanje i težine kodnih reči

Osobina 6.5

Za svaku kodnu reč z_i i z_j važi

$w(z_i)$ +w(z_j)$\geq$ $w(z_i + z_j)$.

Primer 6.7

U binarnom slučaju imamo

w(110101)+w(010101)=4+3=7 $\geq$ 1=w(100000)=w(110101+010101).

Razmotrimo ternarni kod sa simbolima 0,1,2

w(01221021)+w(21002010)=6+4=10$\geq$ 5=w(01221021+21002010).

Hemingovo rastojanje i težine kodnih reči

- Zašto su Hemingova rastojanja i težine reči važna za algebarske kodove za ispravljanje grešaka?
- Greška e koja nastaje pri prenosu jednaka je $e = \hat{z}$- z_i, gde je z_i emitovana a $\hat{z}$primljena kodna reč. Broj grešaka pri prenosu jednostavno je jednak težini reči e, odnosno w($\hat{z}$- z_i).
- Ova vrednost je ujedno jednaka Hemingovom rastojanju d($\hat{z}$, z_i) izmedju emitovane i primljene kodne reči.
- Stoga je detektovanje greške ekvivalentno sa detektovanjem ne nulte težine.
- Ispravljanje grešaka svodi se na izračunavanje razlike e, bez poznavanja z_i, budući da je na prijemu poznato samo $\hat{z}$.

Hemingovo rastojanje i težine kodnih reči

Control Question 52

1. What is the weight of 11101101?
2. What is the weight of 0?
3. What is the weight of 1?
4. What is the weight of 2?
5. What is the weight of 1221032?
6. What is the Hamming distance between 11 and 00?
7. What is the Hamming distance between 101 and 001?
8. What is the Hamming distance between 1234 and 3214?

Dekodavanje minimalnog rastojanja i maksimalne verodostojnosti

- Na koji način se dekoduju blok kodovi?
- Prirodan intuitivan kriterijum za dekodovanje je minimizacija greške dekodovanja, odnosno w(e).
- S druge strane videli smo da je ta minimizacija ekvivalentna nalaženju najbliže kodne reči u odnosu na primljenu, odnosno minimizacija d($\hat{z}$, z_i).
- Npr. ako su moguće kodne reči 000 i 111, a primljena reč je 010, tada je ako nemamo nikakvu dodatnu informaciju, dekodovana reč 000, jer je d(000,010)=1, d(111,010)=2, dakle 010 je najbliža kodna reč.

Dekodavanje minimalnog rastojanja i maksimalne verodostojnosti

Definicija 6.5 *Dekodovanje po principu minimalnog rastojanja*

Kaže se da kod *C* koristi dekodovanje minimalnog rastojanja ako je odluka D prilikom dekodovanja za svaku primljenu reč $\hat{z}$ najbliža kodna reč, tj.

$$D(\hat{z}) = \underset{z \in C}{\operatorname{Argmin}}\, \mathrm{d}(\mathrm{z}, \hat{z}) \ .$$

Posmatrajmo sada proces dekodovanja sa stanovišta Bajesovske verovatnosne postavke problema.

Kada je primljena reč $\hat{z}$, najverovatnija emitovana kodna reč z je ona koja maksimizuje verovatnoću $P(X = z|Y = \hat{z})$, gde je X ulaz, a Y izlaz iz kanala.

Dekodavanje minimalnog rastojanja i maksimalne verodostojnosti

- Ova verovatnoća se ne može izračunati bez poznavanja apriorne verovatnoće emitovanja kodnih reči $P(X = z_i)$.
- Stoga se obično uvode neke pretpostavke, od kojih je razumna ona po kojoj se sve kodne reči emituju sa jednakim verovatnoćama (tzv. pretpostavka maksimalne entropije).
- Tada važi

$$\underset{z\in C}{\mathrm{Argmax}}\ \mathrm{P}(\mathrm{X}=\mathrm{z}|Y=\hat{z}) = \underset{z\in C}{\mathrm{Argmax}}\ \frac{P(Y=\hat{z}|X=z)P(X=z)}{P(Y=\hat{z})}$$

$$= \underset{z\in C}{\mathrm{Argmax}} P(Y=\hat{z}|\mathrm{X}=\mathrm{z})\mathrm{P}(\mathrm{X}=\mathrm{z}) =$$

$$\underset{z\in C}{\mathrm{Argmax}} P(Y=\hat{z}|\mathrm{X}=\mathrm{z}) \qquad (6.3)$$

Dekodavanje minimalnog rastojanja i maksimalne verodostojnosti

Član $P(Y = \hat{z}|\mathrm{X} = \mathrm{z})$ je lakši za izračunavanje nego početni izraz $\mathrm{P}(\mathrm{X} = \mathrm{z}|Y = \hat{z})$. Na primer u slučaju BSC ovaj član se svodi na proizvode transmisionih verovatnoća za svaki simbol.

Ako je BSC takav da svi simboli imaju jednaku verovatnoću greške p, ovaj član postaje

$$\mathrm{P}(\mathrm{X} = \mathrm{z}|Y = \hat{z}) = p^{d(z,\hat{z})}(1-p)^{n-d(z,\hat{z})}, \quad (6.4)$$

budući da je $d(z, \hat{z})$ simbola preneseno sa greškom i

n-$d(z, \hat{z})$ simbola tačno preneto.

Lako je videti da kodna reč koja maksimizira $P(Y = \hat{z}|\mathrm{X} = \mathrm{z})$ je ona koja minimizira rastojanje d($\hat{z}$, z_i).

Ovim je ujedno pokazano da je dekodovanje po metodu minimalnog rastojanja i maksimalne verodostojnosti ekvivalentno u slučaju BSC.

Detekcija i ispravljanje grešaka

- Da li postoji način da se unapred za zadati kod može reći koliko grešaka može detektovati, a koliko ispraviti?
- Odgovor je pozitivan i zasniva se na važnom svojstvu blok kodova: njihovom minimalnom rastojanju.

Definicija 6.6 *Minimalno rastojanje koda*

Minimalno rastojanje koda $C = \{z_1, z_2, \dots, z_M\}$ je minimalno Hemingovo rastojanje $d_{min}(C)$ izmedju bilo koje dve različite kodne reči

$$d_{min}(C) = \min_{i \neq j} d(z_i, z_j).$$

Naredna teorema pokazuje zašto je minimalno rastojanje jednog koda od centralnog značaja u teoriji kodova za ispravljanje grešaka

Detekcija i ispravljanje grešaka

Teorema 6.1 *Kapacitet detekcije i ispravljanja grešaka*

Blok kod dužine n i sa dekodovanjem na osnovu minimalnog rastojanja, može za bilo koja dva broja t i s, takva da je $0 \leq t \leq n$, i $0 \leq s \leq n - t$, da ispravi sve oblike nizova grešaka sa ukupno t ili manje grešaka i da detektuje sve oblike nizova grešaka sa $t + 1, \dots, t + s$ grešaka, ako i samo ako je minimalno rastojanje koda striktno veće od $2t + s$.

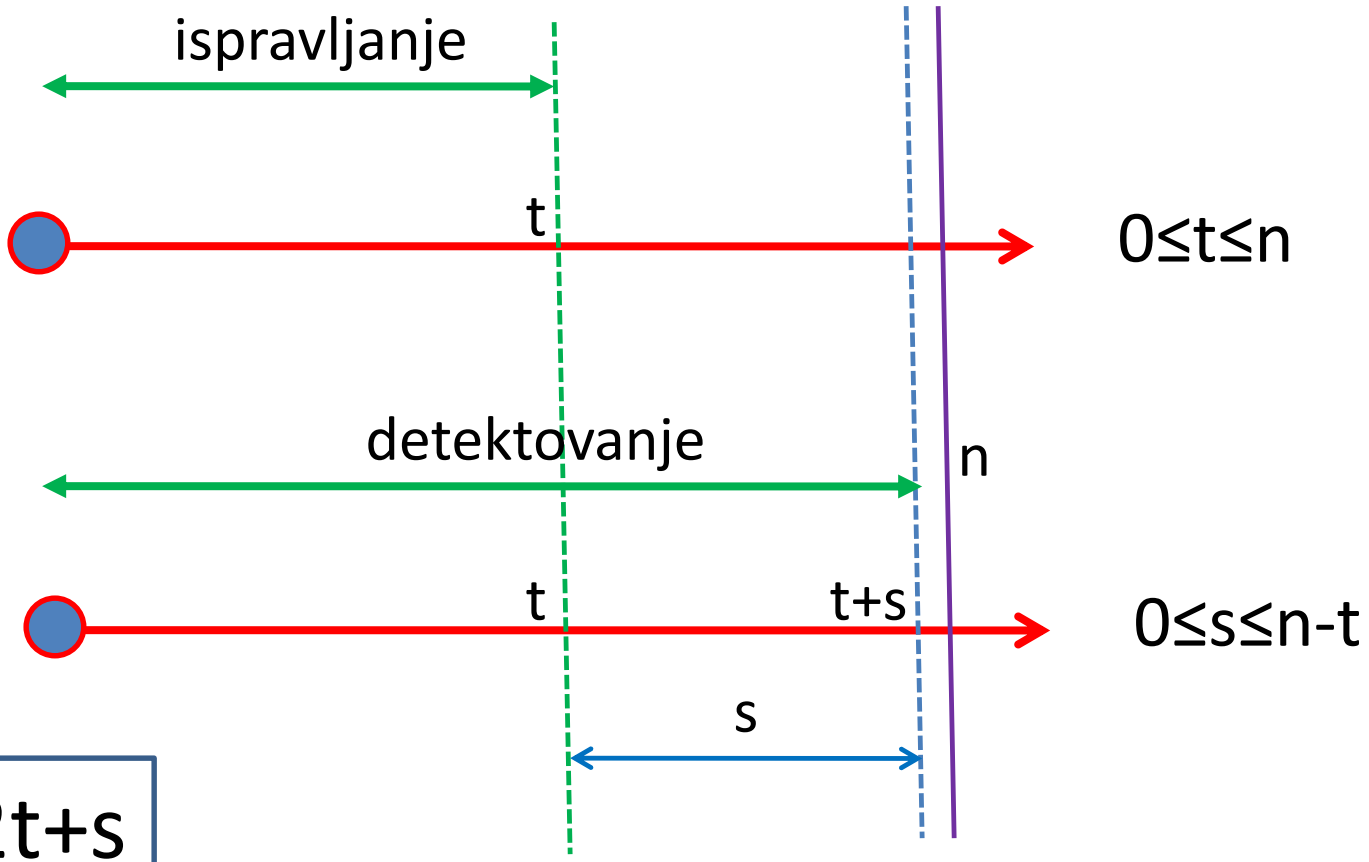
Osobina 6.6 *Maksimalni kapacitet detekcije grešaka*

Blok kod C koji koristi detekciju zasnovanu na minimalnom rastojanju, može se upotrebiti za detekciju svih oblika nizova grešaka sa ukupno manje od $d_{min}(C) - 1$ grešaka.

Dokaz

U teoremi 6.1 treba staviti $t = 0, \quad s = d_{min}(C) - 1.$

Detekcija i ispravljanje grešaka



$D_{min}(C)>2t+s$

Detekcija i ispravljanje grešaka

Osobina 6.7 *Maksimalni kapacitet ispravljanja grešaka*

Blok kod C koji koristi dekodovanje zasnovano na principu minimalnog rastojanja, može da se upotrebi za ispravljanje svih oblika nizova grešaka sa ukupno $(d_{min}(C) - 1)/2$ ili manje grešaka i ne može da ispravi sve oblike nizova grešaka sa ukupno$1 + (d_{min}(C) - 1)/2$grešaka.

Napomenimo da je deljenje sa 2 u gornjim izrazima tzv euklidsko odnosno celobrojno deljenje (u oznaci $\lfloor x/2 \rfloor$,tjcelobrojnideodeljenja).

Dokaz

U teoremi 6.1 treba staviti $t = (d_{min}(C) - 1)/2$, s=0.

Ujedno veličina $(d_{min}(C) - 1)/2$ je maksimalno t koje se može upotrebiti u ovoj teoremi.

Detekcija i ispravljanje grešaka

Primer 6.8

Blok kod sa minimalnim rastojanjem 8 može se upotrebiti za sledeće zadatke:

- Ispravljanje svih oblika grešaka sa manje ili jednako 3 greške i detektovanje svih oblika sa 4 greške (t=3, s=1)
- Ispravljanje svih oblika grešaka sa manje ili jednake 2 greške i detektovanje svih oblika grešaka sa 3 do 5 grešaka (t=2,s=3)
- Ispravljanje svih oblika grešaka sa 1 greškom i detektovanje svih oblika grešaka sa 2 do 6 grešaka (t=1, s=5)
- Detektovanje svih oblika grešaka sa manje ili jednako 7 grešaka (t=0, s=7)

Detekcija i ispravljanje grešaka

Primer 6.8 Nastavak

Blok kod sa minimalnim rastojanjem 7 može se upotrebiti za sledeće zadatke:

- Ispravljanje svih oblika grešaka sa 3 ili manje grešaka (t=3, s=0)
- Ispravljanje svih oblika grešaka manje sa manje ili jednako 2 greške i detektovanje svih oblika grešaka sa 3 i 4 grešake (t=2,s=2)
- Ispravljanje svih oblika grešaka sa 1 greškom i detektovanje svih oblika grešaka sa 2 do 5 grešaka (t=1, s=4)
- Detektovanje svih oblika grešaka sa manje ili jednako 6 grešaka (t=0, s=6)

Primer 6.9

Da bi blok kod mogao da ispravlja 1 grešku, njegovo minimalno rastojanje mora biti barem 3.

Detekcija i ispravljanje grešaka

Control Question 53

1. A communication engineer want to have a channel where all patterns of 3 or less errors are corrected. Can he use a block code with a minimum distance of 5?

2. How many errors can be corrected at most with a block code with a minimum distance of 6?

3. Can such a code furthermore detect errors? If yes, how many?