Linerani kodovi

Milan M.Milosavljević

Linearni kodovi

Linearni kodovi predstavljaju jednu od najznačajnijih klasa kodova zbog njihove jednostavnosti i lake implementacije.

- Šta ćemo naučiti:
- Šta su (n,m) D-arni linearni kodovi
- U ovoj klasi kodova je minimalno rastojanje ekvivalentno sa minimalnim težinama
- Kako se vrši kodovanje pomoću generator matrica
- Šta je sistematska forma generator matrica ovih kodova
- Kako se vrši dekodovanje na osnovu verifikacionih matrica i sindrom tabela
- Kako se izračunava minimalno rastojanje linearnih kodova
- Šta su binarni Hemingovi kodovi i kako se koriste

Linearni kodovi

Definicija 6.7 *Linearni kod*

(n,m) D-arni linearni kod $(1 \leq m \leq n)$ je m-dimenzioni podprostor vektorskog prostora $GF(D)^n$ n-dimenzionih vektora u GF(D).

Dakle, linearni kodovi su blok kodovi koji su vektorski prostor.

Primer 6.10 *Linearni kod*

Kod {1101,0110,1110} dat u primeru 6.2 nije linearni kod, pošto 0000 nije kodna reč ovog koda, i stoga nije vektorski prostor.

Binarni kod {0000,1101, 0110, 1011} je linearni kod pošto je bilo koja linearna kombinacija kodnih reči takodje kodna reč. Dalje, to je (4,2) binarni linearni kod pošto je dimenzija vektorskog podprostora 2, a njegova dužina 4.

Minimalno rastojanje ovog koda je 2, pa se može koristiti za ispravljanje samo jedne greške (prema teoremi 6.1).

Linearni kodovi

Control Question 54

For each of the following binary codes, say whether or not this is a linear code. If yes, give the two numbers n and m of the definition:

1. $\mathcal{C} = \{0000, 1000, 0001, 1001\}$
2. $\mathcal{C} = \{1000, 0001, 1001\}$
3. $\mathcal{C} = \{00, 01, 11\}$
4. $\mathcal{C} = \{0000, 1000, 1100, 0100, 1101, 0001, 0101, 1001\}$
5. $\mathcal{C} = \{0, 1, 10, 11\}$
6. $\mathcal{C} = \{00, 11, 10, 01\}$
7. $\mathcal{C} = \{0000, 0001, 0010, 0100\}$

Linearni kodovi

Osobina 6.8

Svaki linearni kod sadrži nula kodnu reč.

Ovo svojstvo direktno sledi iz činjenice da je linearni kod vektorski (pod)prostor.

Koliko kodnih reči sadrži jedan (n,m) D-arni linearni kod?

Osobina 6.9

(n,m) D-arni linearni kod sadrži D^m različitih kodnih reči, uključujući i nula kodnu reč.

Ova osobina je zgodna za brzu proveru da li je jedan kod sa pogrešnim brojem kodnih reči (nije stepen od D) linearni kod. Takodje se na osnovu ovog svojstva lako pogadja m – dimenzija bazisa koda.

Linearni kodovi

Dokaz

Pošto je linearni kod vektorski prostor dimenzije m, svaka kodna reč se dobija kao linearna kombinacija m bazisnih kodnih reči (to je ujedno jedna baza ovog vektorskog prostora). Za (n,m) D-arni kod, ima ukupno D^m različitih kodnih reči, zapravo svih D^m mogućih linearnih kombinacija.

Osobina 6.10 Brzina linearnog koda

Brzina prenosa linearnog (n,m) koda je

$$R = \frac{m}{n}.$$

Dokaz

Podsetimo se da je brzina D-arnog koda izvora sa M različitih poruka sa kodnim rečima dužine n data sa $R = \frac{\log_D M}{n}$.

Linearni kodovi

Koliko se različitih poruka može kodovati (m,n) linearnim kodom? Onoliko koliko ima kodnih reči, a to je D^m . Stoga je

$$R = \frac{\log_D D^m}{n} = \frac{m}{n}.$$

Teorema *6.2* *Ekvivalentnost minimalnog rastojanja i minimalne težine*

Za svaki linearni kod C

$$d_{min}(C) = w_{min}(C),$$

gde je $w_{min}(C)$ minimalna težina koda, odnosno najmanja težina nenultih kodnih reči

$$w_{min}(C) = \min_{\substack{z \in C \\ z \neq 0}} w(z).$$

Ovaj rezultat je značajan zato što je daleko lakše izračunati u praksi $w_{min}(C)$ nego $d_{min}(C)$.

Linearni kodovi

Primer 6.11

(11,3) binarni kod {00000000000, 10011110000, 01000111100, 00111001111, 11011001100, 10100111111, 01111110011, 11100000011} ima minimalnu težinu 5, a samim tim i minimalno rastojanje 5.

Stoga ovaj kod može da ispravi sve oblike nizova grešaka sa ukupno 1 i 2 greške (videti osobinu 6.7). Proveriti da li je ovaj kod linearan.

Linearni kodovi

Control Question 55

What is the minimum distance of the following codes?

1. $\mathcal{C} = \{0000, 1000, 0001, 1001\}$
2. $\mathcal{C} = \{0000, 1000, 1100, 0100, 1101, 0001, 0101, 1001\}$
3. $\mathcal{C} = \{00000000, 00001011, 00110000, 00111011, 11000000, 11001011, 11110000, 11111011\}$
4. $\mathcal{C} = \{1000, 0001, 0010, 0100\}$

Answer

1. $d_{\min}(\mathcal{C}) = w_{\min}(\mathcal{C}) = 1$
2. $d_{\min}(\mathcal{C}) = w_{\min}(\mathcal{C}) = 1$
3. $d_{\min}(\mathcal{C}) = w_{\min}(\mathcal{C}) = 2$ (e.g. third codeword)
4. $d_{\min}(\mathcal{C}) = 2$!! Although $w_{\min}(\mathcal{C}) = 1$! This is a pitfall! This code not a linear code. Thus the minimum weight theorem cannot be applied. Her the minimum distance is simply computed using its definition. It is easy to see that the distance between any two codewords is 2.

Linearni kodovi

Control Question 56

How many errors can (at most) correct the following linear codes:

1.

2. $\mathcal{C} = \{0000, 1000, 1100, 0100, 1101, 0001, 0101, 1001\}$

3. $\mathcal{C} = \{000000000, 000000111, 000111000, 000111111, 111000000, 111000111, 111111000, 111111111$

Answer

1. $d_{\min}(\mathcal{C}) = w_{\min}(\mathcal{C}) = 1$ thus this code can correct $(1-1)/2 = 0$ errors!! This is not a very useful code!

2. $d_{\min}(\mathcal{C}) = w_{\min}(\mathcal{C}) = 3$ thus this code can correct $(2-1)/2 = 1$ error.

Kodovanje linearnim kodom

Sada ćemo pokazati kako se poruke transformišu u kodne reči linearnog koda.

Ako se m kodnih reči izabere za bazu (n,m) linearnog koda označe sa $z_1, z_2, \dots, z_m$, tada se bilo koja kodna reč z_i može zapisati u obliki

$$z_i = \sum_{k=1}^{k=m} u_{i,k} z_k$$

gde su $u_{i,k}$ komponente z_i za bazisnih vektora z_k. U kompaktnom obliku, koristeći linearnu algebru imamo:

$$z_i = \left(u_{i,1,}, \dots, u_{i,m}\right) \cdot G = u_i \cdot G \ ,$$

gde je u_i vektor red $\left(u_{i,1,}, \dots, u_{i,m}\right)$ a G matrica čiji su redovi $z_1, z_2, \dots, z_m$.

Kodovanje linearnim kodom

Prema tome, poruka u_i dužine m simbola se koduje kodnom rečju z_i množenjem sa matricom G. Stoga se matrica G naziva generator matrica datog koda.

Definicija 6.8 *Generator matrica*

m x n matrica G je generator matrica (n,m) linearnog koda C ako i samo ako su njenih m vektora redova bazisi vektorskog prostora C. Kodovanje poruke u dužine m se svodi na množenje $z = u \cdot G$.

Primer 6.12 *Generator matrica*

Neka je dat (4,2) binarni linearni kod iz primera 6.10 {0000, 1101, 0110, 1011}. Ovaj kod ima četiri kodne reči i može da koduje četiri poruke: četiri binarne reči od po dva bita $u_0 = 00, u_1 = 10, u_2 = 01, u_3 = 11$. Izvršimo kodovanje pomoću generator matrice.

Kodovanje linearnim kodom

Jedna moguća baza ovog koda je $z_1 = 1101, z_2 = 0110$, što daje generator matricu

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

Tada se u_1 koduje u

$$u_1 \cdot G = (1\ 0) \cdot \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} = (1\ 1\ 0\ 1) = z_1.$$

Slično postupamo za transformisanje u_2 u z_2, u_3 u 1011 i u_0 u 0000.

Primetimo da linearni kod uvek koduje nula poruku u nula kodnu reč. Ovo je posledica linearnosti koda, odnosno činjenice da je linearni kod vektorski prostor.

Sistematska forma linearnih kodova

Od svih mogućih generator matrica, jedna ima poseban oblik, ako postoji. To je sistematska forma.

Definicija 6.9 *Sistematska forma*

Generator Matrica G (n,m) linearnog koda je sistematske forme ako se može zapisati u obliku

$$G = [I_m \; P] = \begin{bmatrix} 1\,0\,\ldots 0\; p_{1,1}\; \ldots p_{1,n-m} \\ 0\,1\,\ldots 0\; p_{2,1}\; \ldots\; p_{2,n-m} \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ 0\,0\,\ldots 1\; p_{m,1}\; \ldots p_{m,n-m} \end{bmatrix},$$

gde je I_m jedinična matrica dimenzije m, dok je P m x (n-m) matrica koja se često naziva matrica parnosti (*Parity Matrix*).

Sistematski forma linearnih kodova

Primetimo, da ukoliko postoji sistematska forma generator matrice linearnog koda, ona je jedinstvena.

Definicija 6.10 *Sistematski linearni kod*

Linearni kod koji koristi generator matricu u sistematskoj formi se naziva sistematski (linearni) kod.

Kada (n,m) linearni kod koristi sistematsku formu generator matrice, tada je prvih m simbola od ukupno n simbola kodne reči egzaktno jednak simbolima poruke:

$$z_i = (u_{i,1}, u_{i,2}, \dots, u_{i,m}, z_{i,m+1}, \dots, z_{i,n}) .$$

Drugim rečima, sistematski kod prvo šalje nekodovanu poruku, a zatim (n-m) kodnih simbola za potrebe detekcije i ispravljanja grešaka.

Sistematski forma linearnih kodova

Primer 6.13

Vratimo se na primer 6.12. Drugi mogući izbor bazisa je $z_1 = 1011, z_2 = 0110$, što daje

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

Što je ujedno sistematska forma generator matrice ovog koda.

Primer 6.14 *Biti provere parnosti*

Za binarne poruke bit provere parnosti je bit koji odgovara parnosti bita poruke, tj. binarna suma bita poruke. Npr. bit provere parnosti za poruku 01101 je 1+1+1=1, dok je za poruku 00101 jednak 1+1=0.

Sistematski forma linearnih kodova

Kodovanje sa bitom provere parnosti se sastoji jednostavno u slanju nekodovane poruke iza koje sledi bit parnosti. U terminima teorije kodovanja ovo odgovara (m+1,m) binarnom linearnom kodu, čija je generator matrica

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

Koja je u sistematskoj formi. Primetimo da je minimalno rastojanje ovog koda 2 (prema teoremi 6.2), što znači da ovaj kod može da detektuje samo jednu grešku (videti teoremu 6.1).

Sistematska forma linearnih kodova

Control Question 57

For the following matrices

1. say if it could be a generator matrix.
2. if yes, say if it is in systematic form.
3. if the matrix is not in systematic form, give the systematic form matrix for the corresponding code.
4. (when it is a generator matrix) how will the message `1011` be encoded using the systematic form?

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

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

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

Dekodovanje: verifikaciona matrica

Na koji način linearni kodovi detektuju i ispravljaju greške?

Pretpostavimo da smo našli matricu F, takvu da za svaku kodnu reč z važi da je $z \cdot F = 0$.

Tada, ako se prilikom prenosa z desi greška e, što znači da je na prijemu $\hat{z} = \mathrm{z} + \mathrm{e}$, imamo

$$\hat{z} \cdot F = (z + e) \cdot F = z \cdot F + e \cdot F = 0 + e \cdot F = e \cdot F.$$

Ovaj rezultat je od velike koristi, pošto proizvod $\hat{z} \cdot F$ je nezavisan od emitovane kodne reči z i zavisi samo od greške e. Prema gornjim izrazima sledi da greška u prenosu rezultuje u linearnim kombinacijama redova matrice F. U cilju ispravljanja i/ili detektovanja grešaka, potrebno je jednostavno vektore iz vektorskog prostora generisanog redovima matrice F preslikati u odgovarajuće korigovane (ili detektovane) poruke. Iz matematičkih razloga jednačina $z \cdot F = 0$ se uvek daje u obliku

$$z \cdot H^T = 0.$$

(uslov ortogonalnosti $G \cdot H^T = 0$)

Dekodovanje: verifikaciona matrica

Definicija 6.11 *Verifikaciona matrica*

Matrica H dimenzije (n-m) x n je verifikaciona matrica za (n,m) D-arni linearni kod C, ako i samo ako važi

$$\forall z \in GF(D)^n \qquad z \cdot H^T = 0 \Leftrightarrow z \in C.$$

Drugim rečima, verifikaciona matrica koda C je jezgro (kernel) koda C.

Primetimo da jedan kod može imati više različitih verifikacionih matrica. Svaka matrica čiji su redovi bazis vektorskog prostora koji je ortogonalan na linearni kod je verifikaciona matrica toga koda.

Kako naći verifikacionu matricu?

U slučaju sistematskog koda verifikaciona matrica se nalazi lako.

Dekodovanje: verifikaciona matrica

Teorema 6.3

Za sistematski linearni (n,m) kod C, čija je sistematska forma generator matrice data sa

$$G = [I_m \;\; P],$$

matrica oblika

$$H = [-P^T \;\; I_{n-m}]$$

je verifikaciona matrica.

Dekodovanje: verifikaciona matrica

Dokaz Teoreme 6.3

Za bilo koju poruku u_i , odgovarajuća kodna reč je data sa

$$z_i = u_i \cdot G = u_i \cdot [I_m \; P]$$

Odnosno

$$\begin{cases} (z_{i,1}, \dots, z_{i,m}) = u_i \\ (z_{i,m+1}, \dots, z_{i,n}) = u_i \cdot P \end{cases}$$

Stoga je

$$(z_{i,m+1}, \dots, z_{i,n}) = (z_{i,1}, \dots, z_{i,m}) \cdot P,$$

odnosno

$$-(z_{i,1}, \dots, z_{i,m}) \cdot P + (z_{i,m+1}, \dots, z_{i,n}) = 0,$$

Dekodovanje: verifikaciona matrica

Ili u matričnoj formi

$$z_i \cdot \begin{bmatrix} -P \\ I_{n-m} \end{bmatrix} = 0.$$

Prema tome pronašli smo matricu $[-P^T \quad I_{n-m}]^T$, takvu da je njen proizvod sa bilo kojom kodnom reči jednak nuli.

Drugi deo dokaza se svodi na pokazivanje da svaka reč x koja zadovoljava $x \cdot [-P^T \; I_{n-m}]^T = 0$, zadovoljava i

$$x = (x_1, \dots, x_m) \cdot G,$$

I kao takva predstavlja kodnu reč. ■

Primetimo da je u slučaju polja GF(2), $-P = P$.

Dekodovanje: verifikaciona matrica

Primer 6.15

Razmotrimo sistematski kod čija je generator matrica data sa

$$G = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 1 \end{bmatrix} = \begin{bmatrix} I_2 & \begin{matrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{matrix} \end{bmatrix}.$$

Tada je (n=5, m=2)

$$H = \begin{bmatrix} \begin{bmatrix} 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}^T & I_3 \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 \end{bmatrix}$$

je jedna moguća verifikaciona matrica koda C.

- Kako se dobija verifikaciona matrica u opštem slučaju, kada generator matrica nije u sistematskoj formi?
- Neka je H verifikaciona matrica (n,m) D-arnog linearnog koda sa generator matricom G, čiji su redovi $z_1, z_2, \dots, z_m$. H možemo naći na osnovu sledećeg algoritma:

Dekodovanje: verifikaciona matrica

1. Za i=m+1,...,n, izabrati z_i kao proizvoljan vektor u $GF(D)^n$ linearno nezavisan od $z_1, z_2, \dots, z_{i-1}$,
2. Izračunati inverznu matricu M^{-1} matrice M čiji su redovi $z_1, z_2, \dots, z_n$,
3. Izdvojiti H^T kao poslednjih n-m kolona matrice M^{-1}.

Primer 6.16

Vratimo se na primer 6.12 i (4,2) kod, čiji je jedan generator dat sa

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

Nadjimo prvo dva vektora nezavisna u odnosu na prethodno odabrane. Izaberimo npr. 1000 i 0100.

Dekodovanje: verifikaciona matrica

Tada je

$$M = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, M^{-1} = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 \end{bmatrix}$$

Odakle sledi

$$H^T = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 1 & 1 \end{bmatrix}, \text{tj. } H = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{bmatrix}.$$

Dekodovanje: verifikaciona matrica

Control Question 58

Give one verification matrix for the linear code the systematic form encoding matrix is

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

Answer

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

Dekodovanje: verifikaciona matrica

Control Question 59

Is the word z =1001101 a codeword of the code, one verification matrix of which is

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

Answer

yes: $z \cdot H^T = 0$ thus z is a codeword.

Dualni kodovi

- Verifikaciona matrica (n,m) D-arnog linearnog koda C je (n-m) x n matrica H takva da je njeno jezgro ker(H) jednako C: ker(H)=C.
- Na osnovu fundamentalne teoreme o dimenzijama vektorskog prostora dim(ker(H))+rank(H)=n, dim(C)+rank(H)=n ili rank(H)=n-m.
- Prema tome n-m redova matrice H generiše n-m dimenzionalni podprostor $G(D^n$, tj. (n,n-m) linearni kod. Ovaj kod se naziva dualni kod koda C (i obrnuto).

Osobina 6.11

Dualni kod dualnog koda C je sam kod C.

Osobina 6.12

Generator matrica jednog koda je verifikaciona matrica njegovog dualnog koda i obrnuto.

Sindromi

Ponovimo još jednom ključne ideje linearnih kodova.

Ako je z kodna reč koja se prenosi, a e greška prilikom prenosa, primljena reč je $\hat{z} = z + e$. Ako je H verifikaciona matrica korišćenog koda za ispravljanje grešaka, tada je

$$\hat{z} \cdot H^T = (z + e) \cdot H^T = z \cdot H^T + e \cdot H^T = \mathbf{0} + e \cdot H^T = e \cdot H^T$$

Ovo ilustruje važnu činjenicu da je $\hat{z} \cdot H^T$ zavisi samo od vektora greške e, a ne i od prenesene kodne reči $\hat{z}$. Stoga je veličina $\hat{z} \cdot H^T$ od posebne važnosti u dekodovanju i naziva se sindrom ($\hat{z}$ u odnosu na H).

Sindromi

Definicija 6.12 *Sindromi*

Sindrom reči $\hat{z}$ u odnosu na verifikacionu matricu H je proizvod $\hat{z} \cdot H^T$.

Osobina 6.13

Sindrom $s = \hat{z} \cdot H^T$ primljene reči $\hat{z}$ u odnosu na verifikacionu matricu H koda C zavisi samo od greške u prenosu $e = \hat{z} - z_i$, a ne i od prenošene kodne reči z_i, $z_i \in C$.

Greška e se može dekomponovati u elementarne greške e_k (greške na nivo svakog simbola), odnosno vektor greške ima svoje komponente $e = (e_1, \dots, e_n)$, koje se mogu izraziti sa

$$s(\hat{z}) = \hat{z} \cdot H^T = e \cdot H^T = \sum_k e_k h_k$$

gde je h_k k-ta kolona matrice H, $H = [h_1, \dots, h_n]$.

Sindromi

Da bi se našao korektor (suprotno od greške) dovoljno je naći korektore koji odgovaraju pojedinačnim greškama. Ispravljanje više grešaka se vrši sumiranjem odgovarajućih korektora za pojedinačne greške.

Korigovanje se dakle vrši u dva koraka: mapiranjem kolona matrice H u korektore (koji se pamte u memoriji), dodavanjem jedinice na odgovarajuće nenulte pozicije sidroma.

Primer 6.17 *Korekcione tablice zasnovane na sindromima*

Neka je

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

verifikaciona matrica zadatog binarnog koda.

Sindromi

Tada se na osnovu kolona matrice H izvode sledeći korektori

Syndrome	Corrector
101	10000
111	01000
100	00100
010	00010
001	00001

a)

Syndrome	Corrector
000	00000
001	00001
010	00010
011	?
100	00100
101	10000
110	?
111	01000

b)

jednostavno rednim isčitavanjem kolona matrice H, tabela a). Ako izvršimo uredjenje prema sindromima, kako se to u praksi i koristi dobijamo tabelu b).

Sindromi

Primetimo sledeće:

- Nula sindrom se uvek mapira u nema korigovanja, na osnovu definicije 6.11
- Za 011 i 110 korektor nije jedinstven u ovom primeru. Npr.

  011=010+001, što daje 00011 (00001+00010),

  011=111+100, što daje 01100.
- Razlog za to leži u činjenici da ovaj kod ima minimalno rastojanje 3 i može da koriguje samo 1 grešku i ne sve oblike vektora greške sa ukupno 2 ili više grašaka. Ova dva sindroma zaista odgovaraju dvema greškama u prenosu.

Opšti postupak dekodovanja sa sindromima

U praksi, pamti se tabela sindroma i odgovarajućih korektora.
Opšta procedura dekodovanja primljene poruke $\hat{z}$ je sledeća:

1. Izračunati sindrom $s(\hat{z}) = \hat{z} \cdot H^T$
2. Izračunati korektor $c = -e$, na osnovu linearnih kombinacija memorisanih korektora
3. Izvršiti dekodovanje $z = \hat{z} + c$.

Primer 6.18 *Dekodovanje linearnih kodova*

Nastavimo sa primerom 6.17, u kome je generator matrica data sa

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

Opšti postupak dekodovanja sa sindromima

Pretpostavimo da se prenosi u=10. Ova poruka se koduje u reč z=10101, sa datim linearnim (5,2) kodom.

Pretpostavimo da je $\hat{z} = 00101$, odnosno da je prilikom prenosa prvi bit pogrešno prenet.

Računamo sindrom $s(\hat{z}) = \hat{z} \cdot H^T = 101$, što vodi ka korektoru $c = 10000$, videti tabelu a) iz primera 6.17.

Dekodovanje se vrši po formuli $\hat{z} + c = 00101 + 10000 = 10101$, što daje u prva dva bita dekodovanu poruku 10, pošto je korišćen sistematski binarni kod, i kao što vidimo ona odgovara originalnoj poruci na ulazu u kanal.

Opšti postupak dekodovanja sa sindromima

Kontrolno pitanje 60

Šta je originalna poruka, ako je primljena poruka 101011001, a verifikaciona matrica upotrebljenog koda je data sa

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

Odgovor

Originalna poruka je 10001.

$s(\hat{z}) = \hat{z} \cdot H^T = 0101$, što odgovara trećoj koloni u H, što znači da se greška desila na trećoj poziciji. Stoga je emitovana kodna reč 100011001 (promenjen je treći bit), a budući da je kod sistematičan (videti H), originalna poruka je 10001 (uzeti prvih m=9-4=5 bita).

Minimalno rastojanje i verifikaciona matrica

Kod linearnih kodova moguće je izračunati minimalno rastojanje na osnovu verifikacione matrice.

Teorema 6.4 *Verifikaciona matrica i minimalno rastojanje*

Ako je H verifikaciona matrica (n,m) D-arnog linearnog koda C $(0 \leq m \leq n)$, tada je minimalno rastojanje koda $d_{min}(C)$ jednako najmanjem broju linearno zavisnih kolona u H.

Za binarne linearne kodove C sa verifikacionom matricom H, ovaj rezultat znači sledeće:

- H nema nula kolone, odnosno $d_{min}(C) > 1$.
- Ako H nema dva puta istu kolonu, $d_{min}(C) > 2$.

Minimalno rastojanje i verifikaciona matrica

Primer 6.19

Binarni linearni kod sa verifikacionom matricom

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

Ima rastojanje 3. Zaista, H nema nula kolonu niti dva puta istu kolonu, pa je stoga $d_{min}(C) > 2$. U H postoje tri linearno zavisne kolone $h_1, h_3 \; i \; h_5$.

Osonine 6.14

Za (n,m) linearni kod C, važi

$$d_{min}(C) \leq n - m + 1.$$

Minimalno rastojanje i verifikaciona matrica

Control Question 61

What is the minimum distance of a code, the verification matrix of which is

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

How many errors can this code correct?

Binarni Hemingovi kodovi

- Sada ćemo izučavati dobre binarne kodove koji mogu da koriguju jednu grešku.
- Pošto želimo da ispravimo samo jednu grešku, dovoljno je da sindrom daje indikaciju gde se ta greška nalazi. Dakle ideja je da sindrom direktno daje poziciju, npr. 00..01 za prvu poziciju, 00...10 za drugu, 00...11 za treću, i td.
- Podsetimo se da jedna greška na poziciji k odgovara sindromu koji je k-ta kolona matrice H. Ova činjenica vodi ka ideji da se konstruiše verifikaciona matrica čije su kolone binarne reperezentacije njihovih pozicija
- Šta nam još uvek nije jasno:

1. Koju dimenziju treba da ima ova verifikaciona matrica?
2. Da li ova konstrukcija zaista daje verifikacionu matricu koda?
3. Da li ovako konstruisan kod može zaista da koriguje sve vektore grešaka sa ukupno jednom greškom?

Binarni Hemingovi kodovi

- Što se tiče prvog pitanja, podsetimo se da je sindrom linearnog (n,m) koda dužine n-m. Ako sindrom direktno koduje poziciju greške, trebalo bi da reprezentuje 2^{n-m}-1 pozicija. Prema tome, ako se izabere da je dužina kodne reči n= 2^{n-m}-1, sve pozicije jedne greške će biti zastupljene u verifikacionoj matrici.
- U donjoj tabeli su date moguće vrednosti dimenzije ove klase kodova

n	m	$r = n - m$
7	4	3
15	11	4
31	26	5
63	57	6
⋮	⋮	⋮

Binarni Hemingovi kodovi

- Navedimo dva primera verifikacionih matrica za dužine koda n=7 i n=15.

$$H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

$$H_4 = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Binarni Hemingovi kodovi

- Drugo pitanje ima pozitivan odgovor, dakle ova konstrukcija daje jedan linearan kod, budući da su matrice koje rezultuju u ovoj konstrukciji punog ranga, odnosno rank(H)=n-m. Ovo se može pokazati tako što se lako može konstruisati jedinična matrica I_{n-m} od kolona datih matrica (uzimanjem 1., 2., 4., 8. ..... kolone). Odavde sledi da je dimenzija kernela ove matrice m, što daje (n,m) linearni kod.
- Da bi smo odgovorili na poslednje pitanje: da li ovaj kod može da ispravi sve oblike vektora grešaka sa ukupno jednom greškom, dovoljno je izračunati minimalno rastojanje. Verifikaciona matrica dobijena ovom konstrukcijom nikad neće imati nula kolonu niti dve iste kolone , tako da je u važnosti$d_{min}(C) \geq 3$. S druge strane prve tri kolone ove matrice predstavljaju binarnu reperezentaciju brojeva 1,2 i 3 i kao takve su uvek linearno zavisne. Odavde sledi da je minimalno rastojanje ovog koda uvek 3 i da može da ispravi sve oblike vektora grešaka sa ukupno jednom greškom.
- Ovaj kod se naziva binarni Hemingov kod.

Binarni Hemingovi kodovi

Definicija 6.13 *Hemingov kod*

Hemingov kod je $(2^r - 1, 2^r - r - 1)$ binarni linearni kod, $(r \geq 2)$, čija je verifikaciona matrica data sa

$$H_r = [b_r(1)^T \; b_r(2)^T \; \cdots \; b_r(n)^t] = \begin{bmatrix} 0 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 1 & \cdots & 1 \\ 1 & 1 & \cdots & 1 \end{bmatrix}$$

gde je $b_n(i)$ binarna reprezentacija broja i pomoću n-bitne reči (npr. $b_4(5) = 0101$).

Binarni Hemingovi kodovi

Osobina 6.15

Svaki binarni Hemingov kod može da koriguje sve oblike vektora greške sa ukupno jednom greškom.

Primer 6.20 *Hemingov kod*

Uzmimo da je r=3 i konstruišimo Hemingov binarni kod (7,4). Tada imamo

$$H_3 = \begin{bmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

Da bi smo našli generator matricu, potrebno je da pronadjemo 4 vektora z, takvih da je $z \cdot H^T = 0$.

Binarni Hemingovi kodovi

Nastavak primera 6.20

To su npr. vektori (ima više mogućih rešenja)

$$\begin{aligned} z_1 &= 1110000 \\ z_2 &= 1101001 \\ z_3 &= 1000011 \\ z_4 &= 1111111 \end{aligned}$$

što daje generator matricu

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

Binarni Hemingovi kodovi

Nastavak primera 6.20

Pretpostavimo da je poslata poruka u=1001. Ona se koduje u kodnu reč $z = u \cdot G = 0001111$. Neka se u toku prenosa desi greška na trećem bitu, tako da je primljena kodna reč sada $\hat{z}$=0011111. Kako se ona dekoduje?

Sindrom $s(0011111) = \hat{z} \cdot H^T = 011$, odnosno binarna reprezentacija za 3, što znači da se desila jedna greška na 3. bitu. Stoga je rezultat dekodovanja $\hat{z}$-0010000=0001111, dakle kodna reč koja je stvarno i poslata.