1) Naj bo $C = \{000, 101\}$ dvojiški kod in $p = \frac{1}{3}$ verjetnost napake pri prenosu enega simbola. Kodno besedo 000 pošljemo z verjetnostjo $\frac{3}{4}$, kodno besedo 111 pa z verjetnostjo $\frac{1}{4}$. Prejeta beseda je $s = 101$.
Kaj je poslana kodna beseda po:

a) Pravilu največje verjetnosti?

b) Pravilu najmanjše napake?

c) Pravilu najbližjega soseda?

a) Pravilo največje verjetnosti: $P(\text{prejeli } y \mid \text{poslali } x)$, $x \in C$, maksimalna

$x = 000$: $P(\text{prejeli } 101 \mid \text{poslali } 000) = p(1-p)p = \left(\frac{1}{3}\right)^2 \cdot \frac{2}{3} = \frac{2}{27}$

$x = 111$: $P(\text{prejeli } 101 \mid \text{poslali } 111) = (1-p)p(1-p) = \left(\frac{2}{3}\right)^2 \cdot \frac{1}{3} = \frac{4}{27}$

$\Rightarrow x = 111$

b) Pravilo najmanjše napake: $P(\text{poslali } x \mid \text{prejeli } y)$, $x \in C$, maksimalna

$$P(\text{poslali } x \mid \text{prejeli } y) = \frac{P(\text{prejeli } y \mid \text{poslali } x) \cdot P(\text{poslali } x)}{P(\text{prejeli } y)}$$

$$P(\text{prejeli } 101) = P(\text{prejeli } 101 \mid \text{poslali } 000) \cdot P(\text{poslali } 000) + P(\text{prejeli } 101 \mid \text{poslali } 111) \cdot P(\text{poslali } 111)$$

$$= \frac{2}{27} \cdot \frac{3}{4} + \frac{4}{27} \cdot \frac{1}{4} = \frac{1}{18} + \frac{1}{27} = \frac{5}{54}$$

$x = 000$: $P(\text{poslali } 000 \mid \text{prejeli } 101) = \frac{\frac{2}{27} \cdot \frac{3}{4}}{\frac{5}{54}} = \frac{3}{5}$

$x = 111$: $P(\text{poslali } 111 \mid \text{prejeli } 101) = \frac{\frac{4}{27} \cdot \frac{1}{4}}{\frac{5}{54}} = \frac{2}{5}$

$\Rightarrow x = 000$

c) $d(000, 101) = 2$

$d(111, 101) = 1$

$\Rightarrow x = 111$

---

2) Pokažite, da stari 10-mestni ISBN kod odkrije vse napake na enem mestu in vse transpozicije dveh različnih znakov.

ISBN: International Standard Book Number

$a_1 a_2 \cdots a_{10}$, $a_i \in \{1, 2, \ldots, 10\}$

$w_i := 11 - i$, $i = 1, 2, \ldots, 10$, utežni

Pravilen ISBN kod: $N = \sum_{i=1}^{10} w_i a_i \equiv 0 \mod 11$

10 v zapisu označimo z X

Napaka na enem mestu:

Pravilna vrednost a_j, napačna vrednost a_j'

$N = 10a_1 + \ldots + (11-j)a_j + \ldots + a_{10} \mod 11$

$N' = 10a_1 + \dots + (11-j)a_j' + \dots + a_{10} \mod 11$

$N' - N = (11-j)a_j' - (11-j)a_j \mod 11$

$= (11-j)\cdot(a_j' - a_j) \mod 11$

$\Rightarrow N' = (11-j)\cdot(a_j' - a_j) \mod 11$

$w_j = 11-j \in \{1,2,\dots,10\} \Rightarrow w_j \neq 0 \mod 11$

$a_j \neq a_j' \Rightarrow a_j' - a_j \neq 0 \mod 11$

$\Rightarrow N' \neq 0 \mod 11$

Transpozicija:

$\dots a_i \dots a_j \dots$
$\dots a_j \dots a_i \dots$

$a_i \neq a_j$

$N = 10a_1 + w_i a_i + \dots + w_j a_j + \dots + a_{10} \mod 11$

$N' = 10a_1 + w_i a_j + \dots + w_j a_i + \dots + a_{10} \mod 11$

$N' - N = w_i(a_j - a_i) + w_j(a_i - a_j) \mod 11$

$\Rightarrow N' = (w_i - w_j)(a_i - a_j) \mod 11$

$w_i - w_j = 11 - i - (11-j) = j - i$

$\Rightarrow N' = (j-i)(a_j - a_i) \mod 11$

$j-i \neq 0$, $a_j - a_i \neq 0$

$\Rightarrow N' \neq 0 \mod 11$

---

3) Prejeli smo napačen ISBN kod 0-669-03925-4 zaradi napake dveh zaporednih mest, ki ne vključujeta prve ali zadnje številke. Izračunajte pravilen ISBN kod.

$a_1 a_2 \cdots a_{10} = 0669039254$

$S = 10 \cdot 0 + 9 \cdot 6 + 8 \cdot 6 + 7 \cdot 9 + \ldots + 1 \cdot 4 = 236 \equiv 5 \mod 11$

$S_N \equiv 0 \mod 11$?

$S_N - S = w_k a_{k+1} + w_{k+1} a_k - w_k a_k - w_{k+1} a_{k+1} \mod 11$

$= w_k (a_{k+1} - a_k) - w_{k+1} (a_{k+1} - a_k)$

$= (w_k - w_{k+1})(a_{k+1} - a_k)$

$w_k - w_{k+1} = 1$

$= a_{k+1} - a_k \mod 11$

$\Rightarrow S_N = a_{k+1} - a_k + 5 \mod 11$

$\Rightarrow S_N = (a_{k+1} - a_k) + 5 \mod 11$

$\Rightarrow a_{k+1} - a_k = 6 \mod 11$

Za vse pare preverimo, kateri ustrezajo tej razliki ...

$\Rightarrow (a_6, a_7) = (3, 9)$

$\Rightarrow$ Pravilen ISBN: 0-669093925-4

4) Pokažite, da EMŠO kod odkrije vse napake na enem mestu. Ali odkrije tudi transpozicije?

EMŠO: $a_1 a_2 \cdots a_{13}$

1-7: Rojstni dan
8-9: Številka registra (SLO 50-59)
10-12: Zaporedna številka (moški 000-499, ženske 500-999)
13: Kontrolna števka

$$\sum_{i=1}^{6} (8-i)\, a_i + \sum_{i=7}^{12} (14-i)\, a_i + a_{13} \equiv 0 \mod 11$$

Napaka na enem mestu:

$$S - S' = w_i \cdot (a_i - a_i') \mod 11 \qquad (i = 1, \ldots, 6)$$

- $S - S' = \underset{\neq 0}{(8-i)} \underset{\neq 0}{(a_i - a_i')} \mod 11$

  $\Rightarrow S' \neq 0$

- $S - S' = \underset{\neq 0}{(14-i)} \underset{\neq 0}{(a_i - a_i')} \mod 11 \qquad (i = 7, \ldots, 12)$

  $\Rightarrow S' \neq 0$

- $S - S' = \underset{\neq 0}{a_i - a_i'} \mod 11 \qquad (i = 13)$

  $\Rightarrow S' \neq 0$

Transpozicija:

Ne odkrije transpozicije, če se zgodi med prvim in drugim delom

$w = \{7,6,5,4,3,2,7,6,5,4,3,2,1\}$

$S' = (w_j - w_i)(a_j - a_i)$

Če je $w_j - w_i = 0$, napake ne odkrije

---

5) Alenka želi Borisu poslati sporočilo JA ali NE prek binarnega simetričnega kanala z verjetnostjo napake pri prenosu enega simbola p.

Ima na voljo 2 shemi:

i) Uporaba binarnega koda dolžine 3, ki lahko popravi 1 napako:

JA → 111
NE → 000

ii) Uporaba binarnega koda dolžine 2, ki lahko odkrije 1 napako:

JA → 11
NE → 00

Predpostavimo, da Alenka pošlje Borisu sporočilo JA.

a) Pokažite, da bo pri uporabi (i) sheme Boris dekodiral Alenkino sporočilo kot NE natanko tedaj, ko prejme 100, 010, 001 ali 000. Poiščite verjetnost tega dogodka.

b) Alenka uporabi (ii) shemo. Poiščite verjetnost, da Boris odkrije napako, ki se je zgodila.

c) Če Alenka uporabi (ii) shemo in predpostavimo, da ko Boris odkrije napako, zahteva ponovno pošiljanje, dokler ne prejme kodne besede 00 ali 11, poiščite verjetnost, da bo Boris dekodiral Alenkino sporočilo kot NE.

a) $P(\text{dekodira kot NE}) = P(\text{dobi } 100) + P(\text{dobi } 010) + P(\text{dobi } 001) + P(\text{dobi } 000)$

$= 3 \cdot p^2(1-p) + p^3$

b) $P(\text{odkrije napako}) = \frac{P(\text{dobi } 01) + P(\text{dobi } 10)}{P(\text{ena ali dve napaki})} = \frac{2p(1-p)}{p^2 + 2p(1-p)} = \frac{2p-2p^2}{p^2+2p-2p^2}$

$= \frac{2p(1-p)}{2p-p^2} = \frac{2(1-p)}{2-p}$

c) DN

19.5.

LINEARNI KODI

Kod je linearen natanko tedaj, ko je podprostor vektorskega prostora.

Minimalna razdalja pri linearnem kodu je Hammingova teža
$d = \min\{ wt(c);\ c \in C, c \neq 0\}$.

Kod lahko popravi $t = \lfloor \frac{d-1}{2} \rfloor$ napak.

---

1) Pokažite, da je kod $C = \{000000, 101010, 010101, 111111\}$ linearen? Koliko napak popravi? Poiščite generatorsko in nadzorno matriko za kod C. Z dobljeno generatorsko matriko zakodirajte sporočilo 11.

$GF(2)^6: \forall x, y \in C: x+y \in C$ ✓

$\Rightarrow C$ linearen

$d = 3$

$\Rightarrow t = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$

$\Rightarrow$ Lahko popravi 1 napako

$$G = \left[\begin{array}{cc:cccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right] = \left[\begin{array}{c:c} I_2 & A_4 \end{array}\right]^{\begin{matrix} k & n-k \end{matrix}}_{k}$$ generatorska matrika

$\Rightarrow H = [-A^T \vdots I_{n-k}]$ nadzorna matrika

$GF(2): -A^T = A^T$

$$\Rightarrow H = \left[\begin{array}{cc:cccc} 1 & 0 & 1 & & & \\ 0 & 1 & & 1 & & \\ 1 & 0 & & & 1 & \\ 0 & 1 & & & & 1 \end{array}\right]$$

$$c = [1\ 1]\left[\begin{array}{cccccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \end{array}\right] = 111111$$

---

2) Kodirajmo besedilo $(b_1, b_2, b_3) \in \{0,1\}^3$ kot $(b_1, b_2, b_3, b_2 + b_3, b_1 + b_3, b_1 + b_2)$.

a) Določite parametre (n, M, d).

b) Koliko napak lahko popravi?

c) Kako dekodiramo po pravilu najbližjega soseda?

a) n = dolžina kodne besede = 6

M = število možnih kodnih besed $= 2^3 = 8$

0	0	0	000000	
0	0	1	001110	3
0	1	0	010101	3
0	1	1	011011	4
1	0	0	100011	3
1	0	1	101101	4
1	1	0	110110	4
1	1	1	111000	3

$\Rightarrow d$ = minimalna razmaknjenost $= 3$

b) Popravi lahko $t = \left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{3-1}{2} \right\rfloor = 1$ napako.

c) $G = \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 \end{array}\right]$

Iz definicije koda dobimo:

$$c_1 + c_2 + c_6 = 0$$
$$c_2 + c_3 + c_4 = 0$$
$$c_1 + c_3 + c_5 = 0$$

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

(ker $Hc^T = 0$)

Če sprejmemo $y = (y_1, y_2, y_3, y_4, y_5, y_6)$ in zapišemo $y = c + e$, dobimo:

$$Hy^T = H(c+e)^T = \underbrace{Hc^T}_{=0} + He^T = He^T$$

sindrom	stanje
000	ni napake
101	napaka na 1. mestu
110	napaka na 2. mestu
⋮	⋮
100	napaka na 6. mestu

(Gledamo po stolpcih matrike H)

Kaj pa, če dobimo 111?

$111 = 101 + 010 = 110 + 001$

To je sindrom teže 2, ki ga ne znamo popraviti.

Če H izračunamo kot $H = [-A^T \,|\, I]$, dobimo:

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

Dobimo podobno, ampak malo drugače.

Torej je dekodiranje odvisno od izbora matrike H.

---

3) Kod C je podan z generatorsko matriko $G = \left[\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right]$.

a) Koliko napak popravi?

b) S pomočjo sindromov dekodirajte sprejeto sporočilo
011101100100010011010000.

a) $c' = 10001$, $w(c') = 2 \Rightarrow d \leq 2$

$\begin{bmatrix}1\\0\\0\end{bmatrix}, \begin{bmatrix}0\\1\\0\end{bmatrix}, \begin{bmatrix}0\\0\\1\end{bmatrix}$ neodvisni $\Rightarrow d \geq 2$

$\Rightarrow d = 2$

$\left\lfloor \frac{d-1}{2} \right\rfloor = \left\lfloor \frac{1}{2} \right\rfloor = 0$

$\Rightarrow$ Ne popravi napak

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

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

0 1	ne zazna napake
1 1	napaka na 1. mestu
1 0	napaka na 2. mestu
0 0	ni napake

Razdelimo sporočilo v bloke po 5

$H \cdot [01110]^T = \begin{bmatrix}0\\0\end{bmatrix}$

⇒ Ni napake

$$H \cdot [1\,1\,0\,0\,1]^T = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

⇒ Napaka na 2. mestu

⇒ Pravilno: $[1\,0\,0\,0\,1]$

$$H \cdot [0\,0\,0\,1\,0]^T = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

⇒ Napaka na 4. mestu

⇒ Pravilno: $[0\,0\,0\,0\,0]$

$$H \cdot [0\,0\,1\,1\,0\,0]^T = \begin{bmatrix} 1 \\ 1 \end{bmatrix}$$

⇒ Napaka na 2. mestu

⇒ Pravilno: $[0\,1\,1\,1\,0]$

$$H \cdot [1\,0\,0\,0\,0]^T = \begin{bmatrix} 0 \\ 1 \end{bmatrix}$$

⇒ Ne zazna napake

⇒ Ne moremo dekodirati

Pri dekodiranju upoštevamo prve 3 znake vsakega bloka:

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

HAMMINGOV KOD

Hammingov kod reda r nad $GF(q)$ je linearen $[n,k,d]$-kod dolžine $n = \frac{q^r-1}{q-1}$ in dimenzije $k = n-r$, podan z nadzorno matriko H, v kateri sta vsaka dva stolpca linearno neodvisna.

---

4) Konstruirajte nadzorno matriko za Hammingov kod reda 3 nad končnim obsegom $GF(3)$.

$$n = \frac{3^3-1}{3-1} = \frac{26}{2} = 13$$

$$k = n-r = 13-3 = 10$$

$$H = \underbrace{\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 2 & 2 & 2 \\ 1 & 1 & 1 & 2 & 0 & 0 & 1 & 2 & 0 & 2 & 0 & 1 & 2 \end{bmatrix}}_{n} \Big\} n-k$$

---

5) Kasanijev kod K_ℓ, kjer je $\ell \geq 2$, je definiran kot

$$K_\ell = \{ x \in \mathbb{Z}_2^{|F|} ; \sum_{\alpha \in F} x_\alpha = 0, \sum_{\alpha \in F} \alpha x_\alpha = 0, \sum_{\alpha \in F} \alpha^3 x_\alpha = 0 \},$$

kjer je $F = GF(2^{2\ell+1})$.

Kodna beseda $x = (x_\alpha)_{\alpha \in F}$ je dvojiški vektor, katere koordinate so indeksirane z elementi obsega F.

a) Pokažite, da je koda K_ℓ linearen.

b) Pokažite, da je minimalna razdalja koda K_ℓ vsaj 6.

a) $\forall x, y \in K_\alpha : x+y \in K_\alpha$

$$\sum_{\alpha \in F} (x_\alpha + y_\alpha) = \sum_{\alpha \in F} x_\alpha + \sum_{\alpha \in F} y_\alpha = 0 + 0 = 0$$

$$\sum_{\alpha \in F} \alpha (x_\alpha + y_\alpha) = \sum_{\alpha \in F} \alpha x_\alpha + \sum_{\alpha \in F} \alpha y_\alpha = 0 + 0 = 0$$

$$\sum_{\alpha \in F} \alpha^3 (x_\alpha + y_\alpha) = \sum_{\alpha \in F} \alpha^3 x_\alpha + \sum_{\alpha \in F} \alpha^3 y_\alpha = 0 + 0 = 0$$

b) $d = \min\{ wt(x) \; ; \; x \in K_\alpha, x \neq 0 \}$

$\sum_{\alpha \in F} x_\alpha = 0 \Rightarrow$ x ima sodo število enic

$\Rightarrow$ Teža ne more biti 1,3,5,...

Dokažimo, da ne more biti 2 ali 4.

Ni kodne besede s težo 2

Predpostavimo, da imamo kodno besedo s težo 2:

$\alpha_1, \alpha_2, \; \alpha_1 \neq \alpha_2$

$$\sum_{\alpha \in F} \alpha x_\alpha = 0 \Rightarrow \alpha_1 + \alpha_2 = 0 \Rightarrow \alpha_1 = \alpha_2$$

Ni kodne besede s težo 4

Predpostavimo, da imamo kodno besedo s težo 4:

$\alpha_1, \alpha_2, \alpha_3, \alpha_4$, α_i paroma različni

$$\sum_{\alpha \in F} \alpha \chi_\alpha = 0 \Rightarrow \alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0 \Rightarrow \alpha_4 = \alpha_1 + \alpha_2 + \alpha_3$$

$$\sum_{\alpha \in F} \alpha^3 \chi_\alpha = 0 \Rightarrow \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + \alpha_4^3 = 0$$

$$\Rightarrow \alpha_1^3 + \alpha_2^3 + \alpha_3^3 + (\alpha_1 + \alpha_2 + \alpha_3)^3 = 0$$

$$\Rightarrow (\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_3) = 0$$

$$\Rightarrow \alpha_1 = \alpha_2 \vee \alpha_1 = \alpha_3 \vee \alpha_2 = \alpha_3$$

26.5.

1) Naj bo C_1 linearen $[n, k_1, d_1]$-kod in C_2 linearen $[n, k_2 - d_2]$-kod.

Sestavimo nov kod C na naslednji način:

$$C = \{ a \| a + b \; ; \; a \in C_1, b \in C_2 \}$$

a) Ali je tudi C linearen?

b) Kakšni so njegovi parametri?

c) Sestavite njegovo generatorsko in nadzorno matriko iz generatorskih in nadzornih matrik kodov C_1 in C_2.

a) $c_1 = a_1 \| (a_1 + b_1)$
$c_2 = a_2 \| (a_2 + b_2)$

$$c_1 + c_2 = a_1 \| (a_1 + b_1) + a_2 \| (a_2 + b_2)$$

$$= (\underbrace{a_1 + a_2}_{\in C_1}) \| (\underbrace{a_1 + a_2}_{\in C_1} + \underbrace{b_1 + b_2}_{\in C_2})$$

$\Rightarrow C$ linearen

b) $n' = 2n$

$$C_1 \times C_2 \longrightarrow C$$
$$(a, b) \longmapsto (a \| a + b)$$

$$|C| = |C_1| \times |C_2| = q^{k_1} \cdot q^{k_2} = q^{k_1 + k_2}$$

$$\Rightarrow \dim C = k_1 + k_2 = k'$$

$a \| a + b \in C$

i) $b = 0$:

$$wt(a \| a) = \underbrace{wt(a)}_{\geq d_1} + \underbrace{wt(a)}_{\geq d_1} \geq 2d_1$$

ii) $b \neq 0$:

$$wt(a \| a+b) = wt(a) + wt(a+b) \geq *$$

$$wt(x+y) \leq wt(x) + wt(y)$$

$$x = a$$
$$y = a + b$$

$$\Rightarrow wt(b) \leq wt(a) + wt(a+b)$$

$\Rightarrow * \geq wt(b) \geq d_2$

$\Rightarrow d' = \min\{2d_1, d_2\}$

$\Rightarrow C : [2n, k_1+k_2, \min\{2d_1, d_2\}]$

c) $G = \begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}$

$GH^T = 0$

$H = \begin{bmatrix} H_1 & 0 \\ -H_2 & H_2 \end{bmatrix}$

$$\begin{bmatrix} G_1 & G_1 \\ 0 & G_2 \end{bmatrix}\begin{bmatrix} H_1^T & -H_2^T \\ 0 & H_2^T \end{bmatrix} = \begin{bmatrix} G_1H_1^T & -G_1H_2^T+G_1H_2^T \\ 0 & G_2H_2^T \end{bmatrix} = 0 \quad \checkmark$$

Hammingova zgornja meja:

$$A_q(n,d) \leq \frac{q^n}{\sum_{s=0}^{\lfloor (d-1)/2 \rfloor}\binom{n}{s}(q-1)^s}$$

Gilbert-Varshamova spodnja meja:

$$A_q(n,d) \geq \frac{q^n}{\sum_{s=0}^{d-1}\binom{n}{s}(q-1)^s}$$

---

2) Koliko največ besed ima dvojiški $[8,k,3]$-kod? Poiščite še njegovo generatorsko matriko.

$n = 8$
$q = 2$
$d = 3$

$$A_2(8,3) \leq \frac{2^8}{\sum_{s=0}^{1} \binom{8}{s}(2-1)^s} = 28,44$$

$$\Rightarrow 2^k \leq 28,44$$

$$\Rightarrow k \leq 4$$

$$A_2(8,3) \geq \frac{2^8}{\sum_{s=0}^{1} \binom{8}{s}(2-1)^s} = 6,9$$

$$\Rightarrow 2^k \geq 6,9$$

$$\Rightarrow k \geq 3$$

Torej: $3 \leq k \leq 4$

Preverimo, ali lahko konstruiramo $[8,4,3]$-kod:

Najprej konstruirajmo nadzorno matriko:

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

H mora imeti $d-1 = 2$ poljubna linearno neodvisna stolpca.

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

CIKLIČNI KODI

3) Ali so naslednji kodi ciklični?

a) $C_1 = \{ x \in \mathbb{Z}_3^5 ; wt(x) \equiv 0 \mod 3 \}$

b) $C_2 = \{ x \in \mathbb{Z}_3^5 ; \sum_{i=0}^{5} x_i \equiv 0 \mod 3 \}$

c) $C_3 = \{ x \in \mathbb{Z}_3^5 ; \sum_{i=0}^{5} i x_i \equiv 0 \mod 7 \}$

a) $x = 11100$
$y = 10011$

$\Rightarrow x+y = 21111$

$\Rightarrow wt(x+y) = 5 \neq 0 \mod 3$

$\Rightarrow C_1$ ni linearen

$\Rightarrow C_1$ ni ciklični

b) $x, y \in C_2$

$\Rightarrow x+y \in C_2$

$\Rightarrow C_2$ linearen

$x = (x_1, x_2, x_3, x_4, x_5) \in C_2$

$\Rightarrow \hat{x} = (x_5, x_1, x_2, x_3, x_4) \in C_2$

$\Rightarrow C_2$ ciklični

c) $x, y \in C_3$

$\Rightarrow \sum_{i=1}^{5} i(x_i + y_i) = \sum_{i=1}^{5} i x_i + \sum_{i=1}^{5} i y_i \equiv 0 \mod 7$

$\Rightarrow C_3$ linearen

$x = (1,3,0,0,0)$

$\Rightarrow \hat{x} = (0,1,3,0,0)$

$\Rightarrow 1 \cdot 2 + 3 \cdot 3 = 11 \neq 0 \mod 7$

$\Rightarrow \hat{x} \notin C_3$

$\Rightarrow C_3$ ni ciklični

---

4) Nad obsegom $GF(13)$ je dan kod:

$C = \{(c_0, c_1, \ldots, c_{12}) ; \sum_{i=0}^{12} c_i \equiv 0 \mod 13, \sum_{i=0}^{12} i c_i \equiv 0 \mod 13\}$

a) Ali je kod C ciklični?

b) Dekodirajte besedo $y = (1,3,8,2,1,0,1,9,11,4,12,8,12)$.

a) $c, d \in C$

$\Rightarrow c + d \in C$

$\Rightarrow C$ linearen

$c = (c_0, c_1, \ldots, c_{12}) \in C$

$\hat{c} = (c_{12}, c_0, c_1, \dots, c_{11}) \in C$

$\sum_{i=0}^{12} \hat{c}_i \equiv 0 \mod 13$

$\sum_{i=0}^{12} i\,\hat{c}_i \equiv \sum_{i=0}^{12} (i+1)\,c_i$

$\equiv \sum_{i=0}^{12} i\,c_i + \sum_{i=0}^{12} c_i$

$\equiv 0 \mod 13$

$\Rightarrow C$ ciklicen

b) $H = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \end{bmatrix}$

$Hy^T = Hc^T + He^T$

$Hy^T = \begin{bmatrix} 7 \\ 2 \end{bmatrix}$

$\Rightarrow j \cdot 7 \equiv 2 \mod 13$

$\Rightarrow j \equiv 7^{-1} \cdot 2 \mod 13$

$\equiv 2 \cdot 2 \mod 13$

$\equiv 4 \mod 13$

$\Rightarrow$ Napaka na 4. mestu

0 1 2 3 4 5 ...

$y = (1,3,8,2,\underset{4}{1},0,1,9,11,4,12,8,12)$

$\Rightarrow 1 - 7 = -6 \equiv 7 \mod 13$

---

5) Poiščite najmanjši dvojiški ciklični kod, ki vsebuje besedo 011011.

$(c_0, c_1, c_2, c_3, c_4, c_5) \longmapsto c(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + c_4 x^4 + c_5 x^5$

$011011 \longmapsto c(x) = x + x^2 + x^4 + x^5 = x(1 + x + x^3 + x^4)$

Iščemo $\gcd(c(x), x^6 - 1)$

$\Rightarrow \gcd(1 + x + x^3 + x^4, x^6 + 1) = ?$

$(x^6 + 1) : \underbrace{(x^4 + x^3 + x + 1)}_{g(x)} = x^2 + x + 1$

$k = n - \deg g = 6 - 4 = 2$

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

2.6.

REED-SOLOMONOVI KODI

$g(t) = (t - \beta)(t - \beta^2) \cdots (t - \beta^{d-1})$

β primitivni element $GF(q)$

---

1) Dan je vektor $v = (0, 5, 3, 4, 1, 0)$ s koeficienti iz $GF(7)$. Naj bo C najmanjši ciklični $[n, k, d]$ kod nad $GF(7)$, ki vsebuje v.

a) Poiščite generatorski polinom za dani kod.

b) Ali je C Reed-Solomonov kod?

c) Določite razdaljo d za dani kod. Ali C doseže Hammingovo mejo?

a) $c(x) = 5x + 3x^2 + 4x^3 + x^4 = x(5 + 3x + 4x^2 + x^3)$

$\gcd(5 + 3x + 4x^2 + x^3, x^6 - 1) = ?$ v $\mathbb{Z}_7$

$$(x^6 - 1) : (x^3 + 4x^2 + 3x + 5) = x^3 - 4x^2 + 6x + 4$$
$$-(x^6 + 4x^5 + 3x^4 + 5x^3)$$
$$-4x^5 - 3x^4 - 5x^3 - 1$$
$$\vdots$$
$$0$$

$\Rightarrow \gcd(5 + 3x + 4x^2 + x^3, x^6 - 1) = 5 + 3x + 4x^2 + x^3 =: g(x)$

b) $g(0) = 5$
$g(1) = 1 + 4 + 3 + 5 = 6$
$g(2) = 2^3 + 4 \cdot 2^2 + 3 \cdot 2 + 5 = 1 + 2 + 6 + 5 = 0$
$g(3) = 3^3 + 4 \cdot 3^2 + 3 \cdot 2 + 5 = 0$
$g(4) = 4$
$g(5) = 0$
$g(6) = 5$

$\Rightarrow g(x) = (x-2)(x-3)(x-5)$

Ali je $g(x) = (x-\beta)(x-\beta^2)\cdots(x-\beta^{d-1})$ za nek primitivni β?

Edine potencialne možnosti za β so ničle.

i) $\beta = 2$:

$\beta^2 \equiv 4$

ii) $\beta = 3$:

$\beta^2 \equiv 9 \equiv 2$

$\beta^3 \equiv 2 \cdot 3 \equiv 6$

iii) $\beta = 5$:

$\beta^2 \equiv 25 \equiv 4$

$\Rightarrow$ C ni R-S kod.

c) $G = \begin{bmatrix} 5 & 3 & 4 & 1 & 0 & 0 \\ 0 & 5 & 3 & 4 & 1 & 0 \\ 0 & 0 & 5 & 3 & 4 & 1 \end{bmatrix}$

$\cdot 5^{-1} \equiv 3$

$\sim \begin{bmatrix} 1 & 2 & 5 & 3 & 0 & 0 \\ 0 & 1 & 2 & 5 & 3 & 0 \\ 0 & 0 & 1 & 2 & 5 & 3 \end{bmatrix}$ $-2\times$

$$\sim \left[\begin{array}{cccccc} 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 2 & 5 & 3 & 0 \\ 0 & 0 & 1 & 2 & 5 & 3 \end{array}\right] \begin{array}{l} \leftarrow \\ \leftarrow -2x \\ \leftarrow -x \end{array}$$

$$\sim \left[\begin{array}{ccc:ccc} 1 & 0 & 0 & 5 & 3 & 4 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 & 5 & 3 \end{array}\right]$$

$$H = \left[\begin{array}{ccc:ccc} -5 & -1 & -2 & 1 & 0 & 0 \\ -3 & 0 & -5 & 0 & 1 & 0 \\ -4 & -1 & -3 & 0 & 0 & 1 \end{array}\right]$$

$$= \left[\begin{array}{ccc:ccc} 2 & 6 & 5 & 1 & 0 & 0 \\ 4 & 0 & 2 & 0 & 1 & 0 \\ 3 & 6 & 4 & 0 & 0 & 1 \end{array}\right]$$

Nobena dva stolpca nista lin. odvisna.

$\Rightarrow d \geq 3$

$$\begin{bmatrix} 6 \\ 0 \\ 6 \end{bmatrix} = 6\begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} + 6\begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$\Rightarrow d \leq 3$

Torej: $d = 3$

Hammingova meja: $A_q(n, d) \leq \frac{q^n}{\sum_{i=0}^{\lfloor \frac{d-1}{2} \rfloor} \binom{n}{i}(q-1)^i}$

$q = 7, n = 6, d = 3$

$\Rightarrow A_7(6,3) \leq \frac{7^6}{\binom{6}{0}\cdot 6^0 + \binom{6}{1}\cdot 6^1} = \frac{7^6}{1+36} \approx 3179,7$

$\vee$

Vseh kodnih besed je $7^3 = 343$.

$\Rightarrow$ Koda ne doseže Hammingove meje.

---

2) Poiščite generatorski polinom za R-S kod nad $GF(11)$ dolžine 10, ki odpravi 2 napaki.

$n = 10$

$\left\lfloor \frac{d-1}{2} \right\rfloor = 2 \Rightarrow d = 5$ ali $d = 6$

Izberemo $d = 5$ ...

Ker je to R-S kod, velja $k = 10 - 5 + 1 = 6$.

$st(g) = n - k = 4$

$g(x) = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + a_4 x^4$

$= (x-\beta)(x-\beta^2)(x-\beta^3)(x-\beta^4)$ ($d-1$)

$\beta = 2$

$gcd(2,11) = 1$ ✓

$\beta^2 = 4$
$\beta^3 = 8$
$\beta^4 = 5$
$\beta^5 = 10$
$\beta^6 = 9$
$\beta^7 = 7$
$\beta^8 = 3$
$\beta^9 = 6$
$\beta^{10} = 1$

$\Rightarrow \beta = 2$ primitivni element ✓

$\Rightarrow g(x) = (x-2)(x-4)(x-8)(x-5)$

$= (x^2-6x+8)(x^2-13x+40)$

$= x^4+3x^2+5x^2+8x+1$

---

3) Na nekem komunikacijskem kanalu se lahko zgodijo napake na 20 zaporednih bitih. Predlagajte R-S kod, ki zna popraviti takšne napake.

Če izberemo $GF(2^r)$, bo kodna beseda $(c_0, c_1, \ldots, c_n)$, kjer so $c_i \in GF(2^r)$.

$r := 5$

$\Rightarrow GF(2^5) = GF(32)$

$n = 2^5 - 1 = 31$

20 zaporednih napak lahko sestavlja največ 5 pokvarjenih blokov po 5 bitov.

Torej moramo biti sposobni popraviti 5 bločnih napak.

$\Rightarrow d = 11$

$\Rightarrow k = 21$

$\Rightarrow [31, 21, 11]$ R-S kod (ena možna rešitev)