Varnostno kodiranje - linearni bločni kodi

Naloga 1
Ponavljajoči varnostni kod je sestavljen iz enega podatkovnega in štirih varnostnih bitov. Kolikšna je verjetnost, da bo, navkljub popravljanju napak, sporočilo na drugi strani kanala narobe dekodirano? Verjetnost za napako kanala je 0,05. Pri računanju verjetnosti uporabite binomsko porazdelitev.

Rešitev
Ponavljajoči varnostni kod z enim podatkovnim bitom ima samo dve kodni zamenjavi: same enice in same ničle. Minimalna Hammingova razdalja takega koda je enaka dolžini kodne zamenjave - v našem primeru je to 5, torej $d_H = 5$. Iz tega sledi, da lahko tak kod popravi $f_{\max} = \lfloor \frac{5-1}{2} \rfloor = 2$ napaki. Če se v kanalu zgodijo 3 napake (ali več), bo sporočilo na sprejemni strani narobe dekodirano. Verjetnost, da se to zgodi, je:

$$P = \binom{5}{3} \cdot (1-p_e)^2 \cdot p_e^3 + \binom{5}{4} \cdot (1-p_e)^1 \cdot p_e^4 + \binom{5}{5} \cdot (1-p_e)^0 \cdot p_e^5 = \binom{5}{3} \cdot 0{,}95^2 \cdot 0{,}05^3 + \ldots = 0{,}0012.$$

Naloga 2
S strani FRI ste bili najeti, da vzpostavite novo brezžično povezavo med učilnico PR05 in laboratorijem LASPP. Povezavo modeliramo kot binarni komunikacijski kanal z verjetnostjo napake $p_e = 10^{-5}$. Paketi poslani po kanalu so veliki $n = 1000$ bitov, vključujoč varnostne bite. Predpostavite, da je število varnostnih bitov potrebnih za popravljanje t napak enako $10t$ za $t \leq 10$. Standardi fakultete zahtevajo, da je verjetnost prejema napačnega podatkovnega bita v paketu po opravljenem dekodiranju manjša od 10^{-9}. Najmanj koliko bitov v paketu mora biti varnostnih, da bo izpolnjena zgornja zahteva?

Namigi: Uporabite Poissonov približek za verjetnost x napak v kanalu: $P(x) = \frac{(np_e)^x}{x!} e^{-np_e}$. Predpostavite najslabšo možno situacijo – dekodirnik pokvari dodatnih t podatkovnih bitov, če napačno dekodira.

Rešitev

$P_e = 10^{-5}$

$n = 1000$

$P_N < 10^{-9}$

$$P(k) = \frac{(n \cdot P_e)^k}{k!} \cdot e^{-nP_e} = \frac{(0{,}01)^k}{k!} e^{-0{,}01}$$

toliko napak, da je paket napačen

koliko jih znamo popraviti

dekodirnik pokvari še t bitov in dobimo k napak

t	t_m	X	P_N
1	2	3	$\frac{0{,}01^2}{2!} \cdot e^{-0{,}01} \cdot \frac{3}{990} = 1{,}5 \cdot 10^{-7}$
2	3	5	$\frac{0{,}01^3}{3!} \cdot e^{-0{,}01} \cdot \frac{5}{980} = 8{,}4 \cdot 10^{-10} < 10^{-9}$ ✓

→ toliko napak dekodirnika

→ toliko podatkovnih bitov $(1000 - 10 \cdot t)$

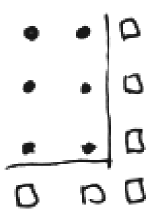
varnostnih bitov je $10 \cdot t = \underline{\underline{20}}$

Naloga 3

S pravokotnim kodom varnostno zakodiramo 6 podatkovnih bitov. Kolikšna je najvišja hitrost pravokotnega koda?

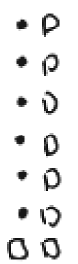
Rešitev

$k = 6$



$n = 6$

Izrojeno:



$n = 8$

$$\text{hitrost} = r = \frac{k}{n} = \frac{6}{12}$$

Najvišja hitrost koda je $R = \frac{1}{2}$.

Naloga 4
Po nezanesljivem kanalu moramo v paketih prenašati podatke, zapisane s tremi biti. Koliko varnostnih bitov moramo dodati, da bomo s primernim kodom lahko vedno popravili vsaj dve napaki na podatkovnih bitih?

Rešitev

Hammingov pogoj: $\boxed{2^k \le \dfrac{2^n}{\sum_{i=0}^{e} \binom{n}{i}}}$ e - število napak

$k=3,\ e=2$

$$2^3 \le \frac{2^n}{\binom{n}{0}+\binom{n}{1}+\binom{n}{2}} = \frac{2^n}{1+n+\frac{n(n-1)}{2}}$$

$n=8 \Rightarrow 8 \le \frac{256}{37} \doteq 6{,}9$

$n=9 \Rightarrow 8 \le \frac{512}{46} \doteq 11{,}1$ ✓

$\boxed{m = n-k = 6}$

Dodati moramo vsaj $m = 6$ varnostnih bitov.

Naloga 5
Določite Hammingovo razdaljo koda L(4, 3), pri katerem je varnostni bit določen tako, da je v kodni zamenjavi vedno sodo število enic.

Rešitev
Imamo $k = 3$ podatkovne bite, kar pomeni, da je vseh kodnih zamenjav $2^3 = 8$. Podatkovnim bitom dodamo varnostni bit, ki zagotavlja sodost enic in dobimo naslednje kodne zamenjave: {000|0, 001|1, 010|1, 011|0, 100|1, 101|0, 110|0, 111|1}. Najmanjši Hammingovi razdalji med pari kodnih zamenjav pravimo Hammingova razdalja koda in je $d_H = 2$.

Naloga 6
Študentska pisarna potrebuje nov varnostni kod za kodiranje letnika, ki ga obiskuje študent. Vrednosti, ki se kodirajo so: 1. letnik, 2. letnik, 3. letnik in absolvent. Definirajte 5-bitni kod (kodne zamenjave), s katerimi bo študentska pisarna lahko kodirala letnik študija in bo omogočal popravljanje enojnih napak.

Rešitev
Želimo popravljati enojne napake, torej je $f_{\max} = 1 = \lfloor \frac{d_H - 1}{2} \rfloor$. Iz tega sledi, da mora biti Hammingova razdalja koda d_H vsaj 3. Primer štirih kodnih zamenjav, s katerimi kodiramo v nalogi podane vrednosti in med katerimi je Hammingova razdalja vsaj 3: {00000, 00111, 11011, 11100}.

Naloga 7
Koliko napak lahko odpravi kod C = {00000000, 11111000, 01100111, 10010110}?

Rešitev
Za podan kod C izračunamo Hammingovo razdaljo med vsemi pari kodnih zamenjav: 5, 5, 4, 6, 5, 5. Hamingova razdalja koda je najmanjša med njimi, torej je $d_H = 4$. Iz tega sledi, da lahko kod popravi $f_{\max} = \lfloor \frac{d_H - 1}{2} \rfloor = \lfloor \frac{3}{2} \rfloor = 1$ napako.

Naloga 8
Linearni bločni kod $L(4, 2)$ je podan z generatorsko matriko

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

Kolikšna je Hammingova razdalja omenjenega koda?

Rešitev

$L(4,2)$

$\downarrow$ 2 podatkovna bita $\Rightarrow z = \{00, 01, 10, 11\}$ $\qquad G = \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix}$

$X = z \cdot G = z \cdot \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \end{pmatrix} = \left\{ \begin{matrix} 0000, \\ 0101, \\ 1010, \\ 1111 \end{matrix} \right\}$ $\qquad d_h = (2, 2, 4, 4, 2, 2)$

$\boxed{\min(d_h) = 2}$

Naloga 9
Sistematični linearni bločni kod L(6,3) je definiran z enačbami:

$$
\begin{aligned}
x_1 &= z_1,\\
x_2 &= z_2,\\
x_3 &= z_3,\\
x_4 &= z_1 + z_2,\\
x_5 &= z_2 + z_3,\\
x_6 &= z_3 + z_1.
\end{aligned}
$$

Kaj se je najverjetneje zgodilo pri prenosu, če smo pri dekodiranju dobili sindrom s=(0,1,0)?

Rešitev

$L(6,3)$ $\qquad x = z \cdot G, \quad s = x \cdot H^T$

$$\left.\begin{aligned} x_1 &= z_1\\ x_2 &= z_2\\ x_3 &= z_3 \end{aligned}\right\}\ \text{podatkovni}$$

$$\left.\begin{aligned} x_4 &= z_1 + z_2\\ x_5 &= z_2 + z_3\\ x_6 &= z_3 + z_1 \end{aligned}\right\}\ \text{varnostni}$$

$$\Rightarrow G = \left[\begin{array}{ccc|ccc} 1 & 0 & 0 & 1 & 0 & 1\\ 0 & 1 & 0 & 1 & 1 & 0\\ 0 & 0 & 1 & 0 & 1 & 1 \end{array}\right], \quad B = \begin{bmatrix} 1 & 0 & 1\\ 1 & 1 & 0\\ 0 & 1 & 1 \end{bmatrix}$$

$$\Rightarrow H = \begin{array}{c} \begin{array}{cccccc} & & & & \boxed{x_5} & \end{array}\\ \begin{bmatrix} 1 & 1 & 0 & 1 & 0 & 0\\ 0 & 1 & 1 & 0 & 1 & 0\\ 1 & 0 & 1 & 0 & 0 & 1 \end{bmatrix} \end{array}$$

$s = (0,1,0)$

Najverjetneje se je torej pokvaril 5. bit.

Naloga 10

Določite informacijski blok z, ki je bil varnostno zakodiran z linearnim bločnim kodom $L(7,4)$, ki ga podaja matrika za preverjanje sodosti

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

če je bila sprejeta kodna zamenjava $y = (0,0,1,0,0,1,0)$.

Rešitev

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

$$S = y \cdot H^T =$$

$$= (0,0,1,0,0,1,0) \cdot \begin{bmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{bmatrix} = \overbrace{[1,0,1]}^{\text{napaka na 5. bitu}}$$

$$\begin{array}{cccccccc} & x_1 & x_2 & z_1 & x_4 & z_2 & z_3 & z_4 \\ \hat{y} = (& 0, & 0, & 1, & 0, & 1, & 1, & 0 \,) \end{array}$$

$$\boxed{\hat{z} = (1,1,1,0)}$$

Najverjetneje je bil poslan blok $\hat{z} = [1, 1, 1, 0]$.

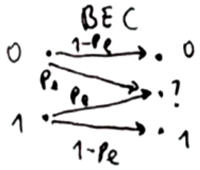
Naloga 11
Podatke pošiljamo po binarnem kanalu z brisanjem (BEC), kjer z verjetnostjo p_e pride do izgube simbola. Podatke, ki jih pošiljamo po omenjenem kanalu kodiramo s Hammingovim kodom

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

V primeru kanala z brisanjem zmore Hammingov kod popraviti kar dve napaki. Dekodirajte kodno zamenjavo $y = (1, ?, 0, 1, 0, 1, ?)$.

Rešitev

$$H = \begin{bmatrix} 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{bmatrix} = [B|I]$$



$$s = y \cdot H^T = [0\ 0\ 0]$$

$$\left(1, \overset{b_1}{?}, 0, 1, 0, 1, \overset{b_2}{?}\right) \cdot \begin{bmatrix} 1 & 1 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} = [0, 0, 0]$$

Sindrom mora biti 0, da ni napake

$$\left.\begin{array}{l} 1 + b_1 = 0 \\ 1 + b_1 + 1 + 1 = 0 \end{array}\right\} \boxed{b_1 = 1}$$

$$1 + 1 + b_2 = 0 \Rightarrow \boxed{b_2 = 0}$$

$$\hat{y} = (\underbrace{1, 1, 0, 1}_{\hat{z}}, \underbrace{0, 1, 0}_{\text{varnostni biti}})$$