2. kolokvij iz TEORIJE KODIRANJA IN KRIPTOGRAFIJE

3. junij 2014

Priimek in ime: ____________________

Vpisna št.: __________ Vrsta: __________ Kolona: __________

1. (5 + 5 = 10 točk) Linearen dvojiški $[n, k, d]$-kod $\mathcal{C}_1$ je podan z nadzorno matriko

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

   (a) Poiščite parametre $[n, k, d]$ za kod $\mathcal{C}_1$. Koliko napak lahko popravi kod $\mathcal{C}_1$?

   (b) S pomočjo sindromov dekodirajte prejeto besedo $y = 101011$.

$n = 6$ (št. stolpcev H - bločna dolžina)

$k = 6 - 3$ dimenzija

$d = 3$: poljubna dva stolpca H sta lin. neodv.

$\Rightarrow d \geq 3$

stolpec 1 + stolpec 3 = stolpec 2 $\Rightarrow d \leq 3$

$$H y^T = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} = H \cdot 001000^T$$

$\rightsquigarrow$ prišlo je do napake na 3. mestu!

$$x = y + 001000 = 100011$$

Vse naloge je treba ustrezno utemeljiti, samo odgovori ne štejejo nič.
Vseeno pa ne pozabite napisati odgovorov!

2. $(5+3+3=11$ točk) Pokažite, da velja

(a) $A_2(n,d) \leq 2A_2(n-1,d)$,

(b) $A_2(4,3) = 2$,

(c) $A_2(5,3) = 4$.

a) Naj bo $\mathcal{C}$ dvojiški (n, M, d)-kod z lastnostjo $M = A_2(n,d)$

Naj bo $\mathcal{C}_0 = \{ x_1 \dots x_{n-1} ; \; x_1 \dots x_{n-1} 0 \in \mathcal{C} \}$

$\mathcal{C}_1 = \{ x_1 \dots x_{n-1} ; \; x_1 \dots x_{n-1} 1 \in \mathcal{C} \}$

Kode $\mathcal{C}_0$ in $\mathcal{C}_1$ sta $(n-1, M, d)$-kode.

Ker je $\mathcal{C}_0 \cup \mathcal{C}_1 = \mathcal{C}$: za vsaj enega od $\mathcal{C}_0, \mathcal{C}_1$ velja, da ima najmanj $|\mathcal{C}|/2$ elementov, naj bo to $\mathcal{C}_i$:

$$A_2(n,d) = |\mathcal{C}| \leq 2 |\mathcal{C}_i| \leq 2 A_2(n-1, d)$$

b) $\mathcal{C} = \{0000, 1110\}$ je $(4, 2, 3)$-dvojiški kod

$\Rightarrow A_2(4,3) \geq 2$

Vendar ne obstaja $(4,3,3)$ dvojiški kod $\mathcal{C}'$;

BŠS: $0000 \in \mathcal{C}'$; vsaka druga beseda iz $\mathcal{C}'$ mora imeti težo vsaj 3. Poljubni dve besedi s težo vsaj 3 pa se razlikujejo na največ dveh mestih.

$\Rightarrow \quad A_2(4,3) = 2$

c) $A_2(5,3) \leq 2 \cdot A_2(4,3) = 4$ po točki (a)

$\mathcal{C} = \{00000, 11100, 00111, 11011\}$

je $(5,4,3)$-dvojiški kod: $A_2(5,3) \geq 4$

$\Rightarrow \quad A_2(5,3) = 4$

3. (9 točk) Fotografije so shranjene v formatu, pri katerem je vsaka pika predstavljena s petimi biti (32 barv). Te slike bi radi poslali po dvojiškem simetričnem kanalu z verjetnostjo napake (posameznega bita) 0.01. Da slike ne bi bile popačene, je zaželeno, da se poljubna pika pokvari z verjetnostjo največ 0.01. Zato je pri prenosu potrebno uporabiti kode za popravljanje napak; vsako piko bomo predstavili z eno kodno besedo. Predlagajte linearen $[n, k, d]$-kod s čim večjo informacijsko zmogljivostjo, s katerim se da doseči dovolj zanesljiv prenos: ocenite n in d ter nato kod predstavite z nadzorno matriko. Predpostavimo, da pri dekodiranju popravimo $\lfloor (d-1)/2 \rfloor$ napak po pravilu najbližjega soseda; če je napak več, izberemo naključno vrednost (verjetno napačno).

$k = 5$ (sporočila – 5 bitov) : $0.99^5 = 0.95$: Pika se pokvari z verjetnostjo 0.05; potrebujemo kod za popravljanje napak

Kod popravi 1 napako: $d \geq 3$

Hammingova meja: $2^k \leq \frac{2^n}{1+n} \Rightarrow 2^{n-5} \geq 1+n$

$n = 8: \quad 8 \geq 9$ //

$n = 9: \quad 16 \geq 10$ ✓

$[9, 5, 3]$ – kod obstaja:

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

vsi stolpci različni $\Rightarrow d \geq 3$, (morda $d = 4$)

kod popravi 1 napako

Zanesljivost prenosa: verjetnost, da pri prenosu kodne besede ni napake:

$$\underbrace{0.99^9}_{0 \text{ napak}} + 9 \cdot \underbrace{0.99^8 \cdot 0.01}_{\substack{1 \text{ napaka} \\ (1 \text{ bit pokvarjen})}} = 0.99656$$ ✓

4. $(5+5=10$ točk) Dan je polinom $g(t)=t^4+t^3+t^2+1$ s koeficienti iz obsega $\mathbb{Z}_2$ in naj bo $\mathcal{C}=\langle g(t)\rangle$ dvojiški kod z bločno dolžino 7.

(a) Pokažite, da je $\mathcal{C}$ cikličen kod z generatorskim polinomom $g(t)$.

(b) Določite dimenzijo in razmaknjenost koda $\mathcal{C}$.

a) $t^7+1 : t^4+t^3+t^2+1 = t^3+t^2+1$

V $\mathbb{Z}_2$: $t^7+1 = t^7-1$

$$
\begin{array}{l}
t^7+t^6+t^5+t^3 \\
\hline
t^6+t^5+t^3+1 \\
t^6+t^5+t^4+t^2 \\
\hline
t^4+t^3+t^2+1 \\
t^4+t^3+t^2+1 \\
\hline
0
\end{array}
$$

$t^4+t^3+t^2+1 \mid t^7+1$

$\Rightarrow$ g je generatorski polinom za ciklični kod dolžine 7:

$\mathcal{C}=\langle g(t)\rangle$ je cikličen kod.

b) $k = n - \deg(g) = 7-4 = 3$

$\Rightarrow$ $\mathcal{C}$ vsebuje $2^3=8$ besed,

to so 0000000 in 7 cikličnih pomikov 1011100

(vsi so različni). Vsak od njih ima

težo 4. Ker $\mathcal{C}$ linearen:

$$d(\mathcal{C}) = \min_{\substack{x\in\mathcal{C} \\ x\neq 0}} t(x) = 4$$

Alternativno: sestavimo generatorsko in nadzorno matriko in razmaknjenost odčitamo iz nadzorne matrike (poljubni 3 stolpci lin. neodv., poljubni 4 pa ne)