Zkouška z předmětu TIK

Jméno a příjmení:

Příklad	1	2	3	4	Σ
Body					

Odpovídejte celou větou a každé své tvrzení řádně zdůvodněte.

1. [25 BODŮ] Uvažujme binární symetrické kanály $\mathcal{K}_1, \mathcal{K}_2$ zapojené do série, přičemž kódování probíhá pouze na vstupu $\mathcal{K}_1$ a kanál $\mathcal{K}_2$ tedy pouze přeposílá informaci z výstupu kanálu $\mathcal{K}_1$. Označme pravděpodobnost chybného přenosu bitu v kanálu $\mathcal{K}_1$ jako p a v kanálu $\mathcal{K}_2$ jako q.

   (a) [5 BODY] Je výsledný kanál $\mathcal{K}$ slabě symetrický? Odpověď zdůvodněte výpočtem jeho matice přechodu.

   (b) [5 BODY] Určete kapacitu kanálu $\mathcal{K}$.

   (c) [5 BODY] Stanovte parametry p, q tak, aby byla kapacita kanálu $\mathcal{K}$ maximální, resp. minimální.

   (d) [10 BODŮ] Nechť X_1 a X_2 značí vstup kanálu $\mathcal{K}_1$, resp. vstup kanálu $\mathcal{K}_2$, a Y je výstup $\mathcal{K}_2$. Ověřte, že podmíněná vzájemná informace $I(Y; X_1|X_2)$ je nulová.

   $$I(Y; X_1|X_2) = H(Y|X_2) - H(Y|X_1, X_2)$$

2. [25 BODŮ]

   (a) [8 BODŮ] Může vektor $(1, 2, 2)$ vyjadřovat délky slov binárního Huffmanova kódu? A co vektor $(2, 2, 3, 3, 3)$?

   (b) [5 BODY] Mějme informační zdroj X a uvažujme nesingulární binární kód C, který není jednoznačně dekódovatelný. Jaký je vztah mezi $H(X)$ a $H(C(X))$? Pokud $X_1, \ldots, X_n$ označují kopie veličiny X, jaký je vztah mezi $H(X_1, \ldots, X_n)$ a $H(C(X_1, \ldots, X_n))$?

   (c) [12 BODŮ] Mějme informační zdroj X popsaný vektorem pravděpodobností

   $$(0.12, 0.2, 0.11, 0.2, 0.09, 0.09, 0.19).$$

   Nalezněte binární *Fanův kód* pro X, který je popsán tímto algoritmem: 1) pravděpodobnosti seřadíme do nerostoucí posloupnosti $p_1 \geq \ldots \geq p_7$; 2) vybereme i tak, aby byl rozdíl $|\sum_{j=1}^{i} p_j - \sum_{k=i+1}^{7} p_k|$ minimální a prvkům $\{1, \ldots, i\}$ připíšeme bit 0, ostatním bit 1; 3) rekurzivně provádíme rozdělení z bodu 2) na každé vzniklé podskupině až do okamžiku, kdy existují pouze jednoprvkové podskupiny. Jedná se o optimální kódování zdroje X?

3. [25 BODŮ] Cyklický kód K délky 6 nad $\mathbb{Z}_5$ má generující polynom $g(z) = z^3 + 3z^2 + 2z + 4$.

   (a) [6 BODŮ] Zakódujte systematicky informaci $\bar{a} = (1\,3\,3)$.

   (b) [6 BODŮ] Spočtěte kontrolní polynom $h(z)$ a kontrolní matici $\mathbb{H}$ kódu K.

   (c) [6 BODŮ] Zkontrolujte slovo $\bar{w} = (2\,2\,0\,0\,4\,0)$ a případně opravte chybu (předpokládáme, že chyba je nejvýše jedna).

   (d) [7 BODŮ] Kolik (maximálně) chyb kód K objevuje a kolik chyb opravuje?

4. [25 BODŮ] Je dán okruh komplexních čísel nad $\mathbb{Z}_7$, $A = \mathbb{Z}_7[x]/x^2 + 1 = \{ai + b,\, a, b \in \mathbb{Z}_7,\, i^2 = -1\}$.

   (a) [6 BODŮ] Ověřte, že okruh A tvoří těleso a že prvek $(i + 2)$ je jeho primitivním prvkem.

   (b) [13 BODŮ] Použijte těleso A k vytvoření BCH-kódu nad $\mathbb{Z}_7$ délky $n = 12$, který opravuje aspoň jednu chybu. (Najděte kořeny tohoto kódu v tělese A, spočtěte generující polynom a kontrolní matici kódu - obojí dopočítejte do tvaru polynomu, respektive matice nad $\mathbb{Z}_7$.)

   (c) [6 BODŮ] V jakém tělese byste hledali kořeny BCH-kódu nad $\mathbb{Z}_7$ délky $n = 25$? Najděte co nejmenší použitelné těleso.

Hlavní kroky řešení:

1. (a) Kanál je slabě symetrický, neboť jeho matice přechodu má tvar

$$\begin{pmatrix} 2pq-p-q+1 & -2pq+p+q \\ -2pq+p+q & 2pq-p-q+1 \end{pmatrix}.$$

   (b) Kapacita kanálu je tudíž $1 - H(2pq-p-q+1, -2pq+p+q)$.

   (c) Max. kapacita je pro $p, q \in \{0, 1\}$, min. kapacita pro $p = q = \frac{1}{2}$.

   (d) Platí $I(Y; X_1|X_2) = 0$, jelikož $H(Y|X_1, X_2) = H(Y|X_2)$. To snadno plyne z podmíněné nezávislosti Y a X_1 při X_2, neboli $p_{Y|X_1X_2} = p_{Y|X_2}$.

2. (a) Snadno nalezneme informační zdroj generující délky slov 1, 2, 2: to je např. zdroj popsaný pravděpodobnostmi $(\frac{1}{2}, \frac{1}{4}, \frac{1}{4})$. Druhý vektor nepřísluší délce slov žádného Huffmanova kódu, nebot existují tři nejdelší slova.

   (b) Platí $H(X) = H(C(X))$, protože C je prosté zobrazení. Ovšem bezpamětové rozšíření kódu C není prosté, a tudíž máme pouze $H(X_1, \ldots, X_n) \geq H(C(X_1, \ldots, X_n))$.

   (c) Fanův kód vypadá takto:

Znak	Kód
1	100
2	00
3	101
4	010
5	110
6	111
7	011

   Platí $H(X) = 2.73$. Fanův kód má střední délku kódu 2.8. Není optimální, Huffmanův kód má střední délku 2.78.

3. (a) $v(z) = 1z^5 + 3z^4 + 3z^3 + az^2 + bz + c$, kde $a, b, c \in \mathbb{Z}_5$ dopočítáme tak, aby dělení $v(z) : g(z)$ vyšlo v $\mathbb{Z}_5[x]$ beze zbytku (tehdy je $\bar{v}$ kódové slovo kódu K). Vyjde $\bar{v} = (1\,3\,3\,2\,2\,4)$.

   (b) Protože délka kódu $n = 6$, musí $g(x)$ dělit $x^6 - 1$ v $\mathbb{Z}_5[x]$, vyjde $(x^6 - 1) : g(x) = x^3 + 2x^2 + 2x + 1$. Pak $h(z) = z^3 + 2z^2 + 2z + 1$ a z něj vyrobíme $\mathbb{H}$ takto:

$$\mathbb{H} = \begin{pmatrix} z^2 \cdot h(z)^{op} \\ z \cdot h(z)^{op} \\ h(z)^{op} \end{pmatrix} \leftrightarrow \mathbb{H} = \begin{pmatrix} 0 & 0 & 1 & 2 & 2 & 1 \\ 0 & 1 & 2 & 2 & 1 & 0 \\ 1 & 2 & 2 & 1 & 0 & 0 \end{pmatrix}$$

   (c) Syndrom $\bar{s} = \mathbb{H} \cdot \bar{w}^T = \begin{pmatrix} 3 \\ 1 \\ 1 \end{pmatrix} = 3 \cdot S_3$, což je jediná možnost, jak napsat syndrom slova $\bar{w}$ coby násobek nějakého sloupce matice $\mathbb{H}$. Slovo $\bar{w}$ je chybné a chybu lze opravit: $\bar{v} = \bar{w} - (0\,0\,3\,0\,0\,0) = (2\,2\,2\,0\,4\,0)$.

   (d) Každé tři sloupce v kontrolní matici $\mathbb{H}$ jsou lineárně nezávislé (ověřte si!) ale některé čtveřice sloupců (zde dokonce všechny) už jsou lineárně závislé. Kód K tedy objevuje tři chyb a opravuje jednu chybu.

4. (a) Polynom $x^2 + 1$ nemá kořen v $\mathbb{Z}_7$ (ověřte si dosazením) a je stupně 2, tudíž je ireducibilní nad $\mathbb{Z}_7$. Okruh A tedy tvoří těleso o $7^2 = 49$ prvcích. Multiplikativní grupa A^* má 48 prvků a řády prvků v ní dělí $48 = 2^4 \cdot 3$. Musíme spočítat $(i + 2)^{16} = 4$ a $(i + 2)^{24} = -1$, a vidíme, že $\mathrm{r}(i + 2) = 48$. Tudíž $(i + 2)$ je primitivním prvkem tělesa A.

   (b) Kód má opravovat aspoň jednu chybu, tudíž jeho plánovaná vzdálenost musí být 3 a kód bude mít dva generující kořeny β a β^2 v tělese A. Přitom řád prvku β je roven délce kódových slov, tj. $\mathrm{r}(\beta) = 12$. Už víme, že primitivním prvkem tělesa A je prvek $(i+2)$, jeho řád $\mathrm{r}(i+2) = 48$. Pak $\mathrm{r}((i+2)^4) = 12$, volíme tedy $\beta = (i + 2)^4 = 3i$ a $\beta^2 = 5$.

Nyní můžeme dopočítat generující polynom jako součin (různých) minimálních polynomů pro generující kořeny, $g(z) = m_\beta(z) \cdot m_{\beta^2}(z)$. Přitom minimální polynom pro kořen $\beta = 3i$ musí mít též kořen $\beta^7 = -3i$ (a $\beta^{49} = \beta$), takže $m_\beta(z) = (z - 3i)(z + 3i) = z^2 + 2$ (počítáme nad tělesem A charakteristiky 7). Minimální polynom pro kořen $\beta^2 = 5$ další kořen mít nemusí, $m_{\beta^2}(z) = z - 5 = z + 2$ je už celočíselný polynom (zde $(\beta^2)^7 = 5^7 = 5$). Generující polynom $g(z) = (z^2{+}2)(z{+}2) = z^3{+}2z^2{+}2z{+}4$. Kontrolní matice $\mathbb{H} = \begin{pmatrix} \beta^{11} & \beta^{10} & \dots & \beta^2 & \beta & 1 \\ (\beta^2)^{11} & (\beta^2)^{10} & \dots & (\beta^2)^2 & \beta^2 & 1 \end{pmatrix}$ nad tělesem A a odpovídá následující kontrolní matici nad $\mathbb{Z}_7$:

$$\mathbb{H} = \begin{pmatrix} 2 & 0 & 6 & 0 & 4 & 0 & 5 & 0 & 1 & 0 & 3 & 0 \\ 0 & 3 & 0 & 2 & 0 & 6 & 0 & 4 & 0 & 5 & 0 & 1 \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 3 & 2 & 6 & 4 & 5 & 1 & 3 & 2 & 6 & 4 & 5 & 1 \end{pmatrix} \sim \begin{pmatrix} 2 & 0 & 6 & 0 & 4 & 0 & 5 & 0 & 1 & 0 & 3 & 0 \\ 0 & 3 & 0 & 2 & 0 & 6 & 0 & 4 & 0 & 5 & 0 & 1 \\ 3 & 2 & 6 & 4 & 5 & 1 & 3 & 2 & 6 & 4 & 5 & 1 \end{pmatrix}$$

(c) Potřebujeme těleso $GF(7^k)$ tak, aby v něm byl prvek řádu $n = 25$. To lze jen, když $25 \mid (7^k - 1)$, aneb když $7^k = 1$ v $\mathbb{Z}_{25}$. Protože $7 \nmid 25$, tak takové k existuje, např. $k = \varphi(25) = 20$. Nejmenší k je rovno řádu prvku 7 v grupě $\mathbb{Z}_{25}^*$. Řády prvků v této grupě dělí počet prvků grupy, zde $|\mathbb{Z}_{25}^*| = \varphi(25) = 20$, a vychází $7^2 = -1$, $7^4 = 1$ v $\mathbb{Z}_{25}^*$, tedy $k = \mathrm{r}(7) = 4$. Kořeny BCH-kódu nad $\mathbb{Z}_7$ délky 25 je možné najít v libovolném tělese $GF(7^4) = GF(2401)$.