Zkouška 1. termín – MIN401 – jaro 2021 – 17. 6. 2021

Veškeré odpovědi musí být zdůvodněny a výpočty musí být doprovozeny komentářem. (Řešení sestávající pouze z odpovědí budou považována za opsaná a hodnocena 0 body.)

1. (4 body) Rozložte polynom

$$p(x) = x^4 + 2x^3 + 2x + 2$$

na ireducibilní faktory nad $\mathbb{Z}_3$.

2. (8 bodů) Uvažme grupy $(\mathbb{Z}, +)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z} \times \mathbb{Z}, +)$ a grupy permutací $(\mathbb{S}_n, \circ)$, $n \geq 2$.

(a) Uvažme podmnožinu

$$M = \{\sigma \in \mathbb{S}_5 | \sigma(2) = 2 \text{ nebo } \sigma(2) = 5\} \subseteq \mathbb{S}_5.$$

Rozhodněte, zda je M podgrupa v $\mathbb{S}_5$.

(b1) Určete nejmenší podgrupu H_1 v $\mathbb{Z}_{18}$ obsahující prvky 6 a 9.

(b2) Najděte nějakou netriviální podgrupu H_2 v $\mathbb{Z}_{18}$ neobsahující prvek 6.

(b3) Existuje v $\mathbb{Z}_{18}$ netriviální podgrupa, která neobsahuje ani jeden z prvků 6 a 9?

(c1) Uvažme zobrazení $\varphi : \mathbb{Z}_6 \to \mathbb{S}_6$ takové, že

$$\varphi(0) = \mathrm{id} \quad \text{a} \quad \varphi(k) = (1, 2, \ldots, k+1)$$

kde $k \in \{1, \ldots 5\}$. Rozhodněte, zda φ je homomorpfismus grup.

(c2) Uvažme homomorpfismus grup $\psi : \mathbb{Z} \to \mathbb{S}_8$ určený podmínkou

$$\psi(1) = (1, 4, 2, 6)(2, 5, 7).$$

Určete jádro $\ker \psi$. Dále určete $\psi(23)$.

(c3) Uvažme homomorpfismus grup $\psi' : \mathbb{Z} \times \mathbb{Z} \to \mathbb{S}_{10}$ určený podmínkami

$$\psi'(1, 0) = (3, 5)(2, 4) \quad \text{a} \quad \psi'(0, 1) = (1, 7)(6, 10, 8, 9).$$

Určete jádro $\ker \psi'$. Dále určete $\psi'(10, 10)$.

3. (8 bodů) Mějme lineární $(6, 3)$-kód nad $\mathbb{Z}_2$ zadaný maticí

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

Tedy délka zprávy před zakódováním je 3 a po zakódování 6. Byla přijata zpráva

(a) 100001,

(b) 110011,

(c) 111001.

Ve všech těchto případech určete syndrom a zprávu dekódujte (tj. určete odeslanou zprávu) za předpokladu, že při přenosu došlo k nejmenšímu možnému počtu chyb. Je dekodódování za tohoto předpokladu vždy možné jednoznačně? Jestliže nikoliv, určete všechny možnosti s minimem chyb.

Řešení a bodování:

1. **[4 body]** Vyzkoušením 0, 1 a 2 přímo vidíme, že polynom $p(x)$ nemá kořeny nad $\mathbb{Z}_3$. Ještě je ale možné, že $p(x)$ je součinem dvou kvadratických faktorů, tj. že

$$x^4 + 2x^3 + 2x + 2 = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd,$$

kde $a, b, c, d \in \{0, 1, 2\}$. Tedy $bd = 2$, což dává dvě možnosti: $b = 2$, $d = 1$ a přehozené pořadí (které by ale jen znamenalo přehození pořadí kvadratických faktorů). Pro tyto hodnoty b a d dostáváme zbývající rovnice

$$a + c = 2, \quad b + ac + d = ac = 0 \quad \text{a} \quad ad + bc = a + 2c = 2.$$

Případ $a = 0$ nemá řešení a v případš $c = 0$ dostaneme $a = 2$, tj.

$$p(x) = x^4 + 2x^3 + 2x + 2 = (x^2 + 2x + 2)(x^2 + 1).$$

2. **[8 bodů]**

(a) Například $(125) \in M$, ale inverze tohoto cyklu do M nepatří, tj. $(152) \notin M$. Tedy M není podgrupa.

(b) H_1 je generována největším společným dělitelem 6 a 9, tj. $H_1 = \{0, 3, 6, 9, 12, 15\}$. Dále $H_2 = \{0, 9\}$ a podgrupa v (b3) neexistuje – rozmyslete si, jaký by musel být nejmenší nenulový prvek v takové podgrupě.

(c1) φ není homomorpfismus – například $\varphi(1) \circ \varphi(5)$ není identita v $\mathbb{S}_6$.

(c2) Jelikož $\omega := (1, 4, 2, 6)(2, 5, 7) = (1, 4, 2, 5, 7, 6)$ je cyklus délky 6, je

$$\ker \psi = 6\mathbb{Z} = \{6k \in \mathbb{Z} | k \in \mathbb{Z}\}.$$

Dále $\psi(24) = id$ a tedy $\psi(23) = \omega^{-1} = (1, 6, 7, 5, 2, 4)$.

(c3) Zjevně $\psi'(1, 0)$ má řád 2 a $\psi'(0, 1)$ má řád 4 (řády jsou v $\mathbb{S}_{10}$). Tedy

$$\ker \psi' = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} \,|\, 2|a \vee 4|b\}.$$

Dále $\psi'(10, 10) = (6, 8)(10, 9)$.

3. **[8 bodů]** Matice kódu G a matice kontroly parity H jsou

$$G = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{a} \quad H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 \end{pmatrix}.$$

Platná kódová slova (při přenosu bez chyb) jsou

$$110100, \quad 101010, \quad 011001, \quad 011110, \quad 101101, \quad 110011, \quad 000000, \quad 000111.$$

(a) Dostáváme syndrom $H \cdot (100001)^T = (111)^T$, přičemž slova s tímto syndromem jsou

$$010101, \quad 001011, \quad 111000, \quad 111111, \quad 001100, \quad 010010, \quad 100001, \quad 100110.$$

Minimální počet jsou tedy dvě chyby (jedničky), což nastane u třech slov 001100, 010010 a 100001. Po odečtení slova 100001 dostaneme 101101, 110011 a 000000, tj. původně byla zaslána některá ze zpráv 101, 011 nebo 000. Dekódování tedy není jednoznačné.

(b) Dostáváme syndrom $H \cdot (110011)^T = (000)^T$, tj. 110011 je platné kódové slovo a poslaná zpráva byla 011.

(c) Dostáváme syndrom $H \cdot (111001)^T = (100)^T$, přičemž slova s tímto syndromem jsou

$$001101, \quad 010011, \quad 100000, \quad 100111, \quad 010100, \quad 001010, \quad 111001, \quad 111110.$$

Minimální počet je tedy jedna chyba (jednička), což nastane u slova 100000. Po odečtení slova 111001 dostaneme 011001, tj. původně byla zaslána zpráva 001.