Příklady k předmětu AVT

Lineární a cyklické kódy

1. Lineární kód K nad $\mathbb{Z}_3$ délky 5 má generující matici $\mathbb{G} = \begin{pmatrix} 2 & 2 & 0 & 1 & 2 \\ 2 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 0 & 0 \end{pmatrix}$.

   a) Zakódujte informaci $\bar{a} = (102)$ pomocí matice $\mathbb{G}$. Spočtěte systematickou generující matici $\mathbb{G}_S$ kódu K a opět zakódujte informaci $\bar{a} = (102)$ pomocí systematické matice $\mathbb{G}_S$.

   b) Spočtěte kontrolní matici $\mathbb{H}$ kódu K a zkontrolujte, zda je slovo $\bar{v} = (12201)$ kódové.

   c) Dekódujte $\bar{v}$ za předpokladu, že bylo použito systematické kódování, a potom za předpokladu, že bylo použito kódování pomocí matice $\mathbb{G}$.

   Výsledek: a) $\bar{w} = (20112)$, $\mathbb{G}_S = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 2 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix}$, $\bar{w}_s = (10221)$. b) $\mathbb{H} = \begin{pmatrix} 0 & 1 & 2 & 1 & 0 \\ 2 & 0 & 0 & 0 & 1 \end{pmatrix}$, $\mathbb{H}\ \bar{v}^T = \bar{o}$. c) $\bar{a}_s = (122)$, $\bar{a} = (110)$.

2. Je dána kontrolní matice lineárního kódu K nad $\mathbb{Z}_7$, $\mathbb{H} = \begin{pmatrix} 1 & 2 & 2 & 0 & 4 \\ 0 & 2 & 3 & 6 & 1 \end{pmatrix}$.

   a) Kolik informačních znaků a kolik kontrolních znaků má kód K? Kolik je kódových slov v K?

   b) Spočtěte systematickou generující matici a zakódujte pomocí ní informaci $\bar{a} = (a_1 \dots a_k)$, kde $a_i = 2$ pro všechna $i = 1, \dots, k$.

   c) Slovo $\bar{v} = (13360)$ bylo zakódováno systematicky. Ověřte, zda je bez chyby, případnou chybu opravte a dekódujte. (Předpokládáme, že chyba je nejvýše jedna.)

   Výsledek: a) 3 info-znaky, 2 kontrolní znaky, 7^3 kódových slov. b) $\mathbb{G}_S = \begin{pmatrix} 1 & 0 & 0 & 5 & 5 \\ 0 & 1 & 0 & 5 & 3 \\ 0 & 0 & 1 & 6 & 3 \end{pmatrix}$, $\bar{u} = (22241)$. c) $\mathbb{H}\ \bar{v}^T = \begin{pmatrix} 6 \\ 2 \end{pmatrix}$, $\bar{e} = (00300)$, $\bar{w} = (13060)$, informace $\bar{a} = (130)$.

3. Lineární kód nad $\mathbb{Z}_3$ má generující matici $\mathbb{G} = \begin{pmatrix} 1 & 0 & 1 & 2 \\ 2 & 1 & 0 & 2 \end{pmatrix}$. Najděte jeho kontrolní matici.

   a) Opravte slovo $\bar{v} = (1020)$ za předpokladu, že obsahuje nejvýše jednu chybu.

   b) Jak by se dalo slovo $\bar{v} = (1020)$ opravit, kdyby v něm byly právě dvě chyby? Najděte všechna kódová slova, jejichž Hammingova vzdálenost od $\bar{v}$ je 2.

   c) Dokažte, že kód (vždy) opravuje jednu chybu.

   Výsledek: $\mathbb{H} = \begin{pmatrix} 2 & 2 & 1 & 0 \\ 1 & 2 & 0 & 1 \end{pmatrix}$. a) $\bar{w} = (1120)$, b) $\bar{w}_1 = (0000)$, $\bar{w}_2 = (2021)$, $\bar{w}_3 = (1012)$. c) Stačí ukázat, že žádný sloupec matice $\mathbb{H}$ není násobkem jiného sloupce.

4. ISBN (International Standard Book Number) je lineární kód délky 10 nad $\mathbb{Z}_{11}$, jehož kódová slova splňují rovnici $\sum_{i=1}^{10} i \cdot v_i = 0$ v $\mathbb{Z}_{11}$. (Pozn. Číslo 10 se v tomto kódu značí jedním znakem X, tedy jako římská desítka.)

   a) Doplňte kontrolní znak tak, aby vzniklo kódové slovo: $80 - 7113 - 175 - v_{10}$

   b) Napište kontrolní matici ISBN kódu. Kolik chyb kód objevuje a kolik opravuje?

   c) Najděte systematickou generující matici ISBN kódu.

   Výsledek: a) $v_{10} = X$. b) $\mathbb{H} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \end{pmatrix}$, kód objevuje jednu chybu a neopravuje žádnou chybu. c) $\mathbb{G}_S = (E_9|B)$, kde $B = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{pmatrix}$.

5. Ověřte, zda množina slov tvoří binární lineární kód. Pokud ano, nalezněte jeho generující matici.

   a) $A = \{(11111), (11110), (11101), (11100), (00011), (00010), (00001), (00000)\}$

   b) $B = \{(1111), (1110), (1101), (0011), (0010), (0001), (0000)\}$

Výsledek: a) A je lineární kód, $\mathbb{G} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix}$, ostatní slova jsou právě všechny lineární kombinace slov v řádcích matice $\mathbb{G}$ (je jich 8). b) B není lineární kód, protože nemá 2^k slov (zkuste najít dvě kódová slova, jejichž součet není kódové slovo).

6. Lineární kód délky 4 nad nad $\mathbb{Z}_3$ má generující matici $\mathbb{G} = \begin{pmatrix} 2 & 2 & 1 & 1 \\ 2 & 0 & 1 & 0 \end{pmatrix}$.

   a) Vypište všechna kódová slova a ověřte, že se jedná o cyklický kód.

   b) Najděte generující polynom a pomocí něj zakódujte informaci $\bar{a} = (12)$.

   c) Najděte generující matici, která určuje stejné kódování jako generující polynom. Ověřte to zakódováním informace $\bar{a} = (12)$ pomocí této matice.

   Výsledek: a) $K = \{a_1\bar{b}_1 + a_2\bar{b}_2,\ a_i \in \mathbb{Z}_3\}$, kde $\bar{b}_1, \bar{b}_2$ jsou řádky matice $\mathbb{G}$. Bude devět kódových slov a s každým je v K i cyklicky posunuté slovo. b) $g(z) = 2 + z^2$, $v(z) = 2 + z + z^2 + 2z^3$. c) $\mathbb{G}_1 = \begin{pmatrix} 2 & 0 & 1 & 0 \\ 0 & 2 & 0 & 1 \end{pmatrix}$, $\bar{v} = (2112)$.

7. Cyklický kód K délky 6 nad nad $\mathbb{Z}_3$ má generující polynom $g(z) = z^2 + z + 1$.

   a) Kolik informačních znaků a kolik kontrolních znaků má kód K? Kolik je kódových slov v K?

   b) Zakódujte pomocí $g(z)$ informaci ze samých 1, tj. $\bar{a} = (a_1 \dots a_k)$, kde $a_i = 1$ pro všechna $i = 1, \dots, k$.

   c) Najděte kontrolní polynom a ověřte pomocí něj, zda je slovo $\bar{v} = (100200)$ bez chyb. Pokud ano, dekódujte.

   Výsledek: a) 4 info-znaky, 2 kontrolní znaky, 3^4 kódových slov. b) $w(z) = 1 + 2z + 2z^4 + z^5$, aneb $\bar{w} = (120021)$. c) $h(z) = z^4 + 2z^3 + z + 2$, $h(z) \cdot (1 + 2z^3) = 0$ v $\mathbb{Z}_3^{(6)}$, kde $z^6 = 1$. Informace je $a(z) = 1 + 2z$, aneb $\bar{a} = (1200)$.

8. Ověřte, že polynom $g(z) = 1 + 2z + 2z^2 + z^3$ může generovat cyklický kód délky 6 nad $\mathbb{Z}_3$.

   a) Zakódujte systematicky zprávu $\bar{a} = (122)$ pomocí $g(z)$.

   b) Najděte kontrolní polynom $h(z)$ a ověřte, že váš polynom je kódový.

   c) Nalezněte systematickou generující matici daného kódu a pomocí ní opět systematicky zakódujte zprávu $\bar{a} = (122)$.

   Výsledek: $g(x)$ dělí $x^6 - 1$ beze zbytku v $\mathbb{Z}_3[x]$. a) $w(z) = z^5 + 2z^4 + 2z^3 + z^2$. b) $h(z) = z^3 + z^2 + 2z + 2$, $h(z) \cdot w(z) = 0$ v $\mathbb{Z}_3^{(6)}$. c) $\mathbb{G}_S = \begin{pmatrix} 1 & 0 & 0 & 1 & 2 & 2 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 2 & 2 & 1 \end{pmatrix}$, $\bar{w} = (122100)$.

9. Najděte generující polynomy všech cyklických kódů délky 5 nad $\mathbb{Z}_5$.

   a) Vyberte nějaký generující polynom cyklického kódu délky 5 nad $\mathbb{Z}_5$ se 3 informačními znaky. Najděte některou jeho generující matici a některou jeho kontrolní matici.

   b) Zjistěte, zda je $\bar{v} = (12221)$ kódové slovo vámi vybraného kódu. Pokud ne, opravte chybu, je-li to možné.

   Výsledek: $g(z) = (z - 1)^i$ pro $i \in \{1, 2, 3, 4\}$. a) $g(z) = z^2 - 2z + 1$, $h(z) = z^3 - 3z^2 + 3z - 1$, $\mathbb{G} = \begin{pmatrix} 1 & 3 & 1 & 0 & 0 \\ 0 & 1 & 3 & 1 & 0 \\ 0 & 0 & 1 & 3 & 1 \end{pmatrix}$, $\mathbb{H} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 & 0 \end{pmatrix}$. b) $\mathbb{H}\ \bar{v}^T = \begin{pmatrix} 1 \\ 4 \end{pmatrix}$, $\bar{e} = (00300)$, $\bar{w} = (12421)$.

10. Najděte generující polynomy všech binárních cyklických kódů délky 5 a napište jejich systematické generující matice.

    Výsledek: Jsou dva binární cyklické kódy délky 5. $g_1(z) = 1 + z$, $\mathbb{G}_1 = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix}$, kód parity. $g_2(z) = 1 + z + z^2 + z^3 + z^4$, $\mathbb{G}_2 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 \end{pmatrix}$, opakovací kód.

11. Najděte cyklický kód nad $\mathbb{Z}_3$, jehož kontrolní matice má ve sloupcích všechna nenulová slova délky 2 nad $\mathbb{Z}_3$. Najděte generující polynom tohoto kódu. Návod: Využijte těleso GF(9) a jeho primitivní prvek.

Výsledek: $\mathbb{H} = \begin{pmatrix} 0 & 1 & 2 & 2 & 0 & 2 & 1 & 1 \\ 1 & 1 & 0 & 1 & 2 & 2 & 0 & 2 \end{pmatrix} = \begin{pmatrix} 1 & \beta & \beta^2 & \dots & \beta^7 \end{pmatrix}$, kde $\beta = i + 1$ je primitivní prvek v $GF(9) = \mathbb{Z}_3[x]/x^2 + 1$. $g(z) = z^2 + z + 2$=nenulový polynom nad $\mathbb{Z}_3$ s kořenem $\beta = i + 1$ nejmenšího stupně (viz př. 12 v kapitole o polynomech nad Z_p).