Teorie kódování

LS 2022/23, FJFI ČVUT

3. domací úlohy

1a) Mějme binární BCH kód délky n opravující 2 chyby s generujícími kořeny α a α^3. Uvažme, že jsme místo kódového slova $w \in \{0,1\}^n$ přijali slovo $x \in \{0,1\}^n$ a spočetli jsme syndrom $(s_1, s_3) = \left(x(\alpha), x\left(\alpha^3\right)\right)$. Dokažte, že pokud $s_1 = 0$ a $s_3 \neq 0$, tak potom muselo dojít při přenosu $w \to x$ k alespoň 3 chybám.

1b) Mějme binární BCH kód délky n opravující t chyb s generujícími kořeny $\alpha, \alpha^3, \dots, \alpha^{2t-1}$. Uvažme chybový vektor $e \in \{0,1\}^n$ a nechť $i_1, i_2, \dots, i_\tau$ jsou indexy jeho nenulových pozic, tzn. pozic, na kterých došlo k chybě. Spočtěme si nyní $2t$-složkový syndrom:

$$
\begin{aligned}
s_1 = \ & e(\alpha) \ = \ \alpha^{i_1} + \alpha^{i_2} + \cdots + \alpha^{i_\tau} \\
s_2 = \ & e(\alpha^2) = \ (\alpha^{i_1})^2 + (\alpha^{i_2})^2 + \cdots + (\alpha^{i_\tau})^2 \\
s_3 = \ & e(\alpha^3) = \ (\alpha^{i_1})^3 + (\alpha^{i_2})^3 + \cdots + (\alpha^{i_\tau})^3 \\
\vdots \\
s_{2t} = \ & e(\alpha^{2t}) = \ (\alpha^{i_1})^{2t} + (\alpha^{i_2})^{2t} + \cdots + (\alpha^{i_\tau})^{2t}.
\end{aligned}
$$

Dokažte, že pro každé $j \in \{1, 2, \dots, t\}$ platí, že $s_{2j} = s_j^2$.

Mějme binární BCH kód délky n opravující t chyb s generujícími kořeny $\alpha, \alpha^3, \dots, \alpha^{2t-1}$, nechť $e \in \{0,1\}^n$ je (chybový) vektor váhy $\tau \leq t$ s nenulovými pozicemi $i_1, i_2, \dots, i_\tau$, a nechť $(s_1, s_2, \dots, s_{2t})$ je odpovídající $2t$-složkový syndrom e. Dále, nechť p je přirozené číslo splňující podmínku $\tau \leq p \leq t+1$, a označme M_p následující matici s rozměry $p \times p$:

$$
M_p = \begin{pmatrix}
1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\
s_2 & s_1 & 1 & 0 & 0 & & 0 & 0 \\
s_4 & s_3 & s_2 & s_1 & 1 & & 0 & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & & & \\
s_{2p-2} & s_{2p-3} & s_{2p-4} & s_{2p-5} & s_{2p-6} & & s_p & s_{p-1}
\end{pmatrix}
$$

2a) Dokažte, že v tělese charakteristiky 2 platí vztah

$$
\det M_\tau = \prod_{1 \leq a < b \leq \tau} \left(\alpha^{i_a} - \alpha^{i_b}\right) \neq 0.
$$

2b) Dokažte, že v tělese charakteristiky 2 platí vztah $\det M_{\tau+1} \neq 0$.

2c) Pro každé $p > \tau + 1$ dokažte, že M_p je singulární matice. Jinými slovy, $\det M_p = 0$.
Hint — vypozorujte následující identitu:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 & \dots & 0 & 0 \\ s_2 & s_1 & 1 & 0 & 0 & \dots & 0 & 0 \\ s_4 & s_3 & s_2 & s_1 & 1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & & \vdots & \vdots \\ s_{2p-2} & s_{2p-3} & s_{2p-4} & s_{2p-5} & s_{2p-6} & \dots & s_p & s_{p-1} \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ f_1 \\ f_2 \\ \vdots \\ f_\tau \\ 0 \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

kde $f_1, f_2, \dots, f_\tau$ jsou koeficienty lokátoru $f(x) = \prod_{a=1}^{\tau} (1 - \alpha^{i_a} \cdot x) = 1 + \sum_{a=1}^{\tau} f_a \cdot x^a$.

Antisymetrická Hadamardova matice velikosti n je $n \times n$ matice H_n s hodnotami $+1$ na diagonále a ± 1 jinde taková, že každé dva různé řádky jsou na sebe kolmé a $a_{ij} = -a_{ji}$ pro všechny různé dvojice $i, j \in \{1, 2, \dots, n\}$. Jinými slovy, H_n je matice ± 1 splňující

$$H_n \cdot H_n^T = n \times I_n \quad \text{a} \quad H_n + H_n^T = 2 \times I_n, \text{ kde } I_n \text{ je jednotková } n \times n \text{ matice.}$$

3) Pro nekonecně mnoho hodnot n, zkonstruujte (nějakou) antisymetrickou Hadamardovu matici velikosti n.