

KG 1: Cvičení č.12

Irena Penev

9.1.2026

Samoopravné kódy

Připomenutí: (n, k, d) kód je podmnožina C množiny $\mathbb{Z}_2^n = \{0, 1\}^n$ binárních stringů délky n taková, že $|C| = 2^k$ a $d = \min\{d(x, y) \mid x, y \in C, x \neq y\}$, kde $d(x, y)$ je *Hammingova vzdálenost* stringů x, y , tj. počet pozic, kde se liší. Platí, že (n, k, d) -kód umí detekovat $d - 1$ chyb a opravit až $\lfloor \frac{d-1}{2} \rfloor$ chyb.

Kombinatorická koule se středem x a poloměrem r je $B(x, r) = \{y \in \mathbb{Z}_2^n \mid d(x, y) \leq r\}$. Pro její objem platí $V(r) = |B(x, r)| = \sum_{i=0}^r \binom{n}{i}$.

Věta (Hammingův odhad). Pro $(n, k, d = 2t + 1)$ -kód platí $2^k = |C| \leq \frac{2^n}{V(t)}$.

Věta (Gilbert-Varshamov odhad). Pro $n, d \geq 1$ existuje (n, k, d) -kód C , že $2^k = |C| \geq \frac{2^n}{V(d-1)}$.

Příklad 1 (Parametry). Určete parametry (n, k, d) následujících kódů:

(a) $C_1 = \{0000, 1111\}$ (b) $C_2 = \{100, 010, 001, 111\}$ (c) $C_3 = \{00, 11, 01\}$.

Příklad 2 (Kódy v $\mathbb{Z}_2^5$). (a) Napište nějaký $(n, k, d) = (5, 2, 2)$ -kód C .

(b) Existuje $(5, 3, 3)$ -kód?

Příklad 3 (Přidání bitu). Ať $C \subseteq \mathbb{Z}_2^n$ je kód, pro který je minimální vzdálenost lichá, tj. $d = 2t + 1$.

(a) Kolik chyb C opraví?

(b) Z C vyrobíme nový kód $C' \subseteq \mathbb{Z}_2^{n+1}$ tak, že každé slovo prodloužíme o jeden bit, aby celkový počet jedniček byl sudý. Určete parametry (n', k', d') kódu C' . Kolik chyb opraví?

Příklad 4 (Hadamardův kód). Pro $k \geq 1$ a $n = 2^k$ definujme $n \times n$ matici S_n induktivně jako

$$S_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad a \quad S_{2n} = \begin{pmatrix} S_n & S_n \\ S_n & -S_n \end{pmatrix}.$$

(a) Dokažte, že každé dva řádky matice S_n se liší na přesně $n/2$ pozicích.

(b) Hadamardův kód H_n vznikne tak, že vezmeme řádky matice S_n spolu s řádky matice $-S_n$ (kde místo -1 píšeme vždy 0). Dokažte, že H_n je $(2^k, k + 1, 2^{k-1})$ -kód.

(Btw. První fotky Marsu přišly na Zemi zakódované pomocí H_{32} .)

Lineární kódy

Řekneme, že (n, k, d) -kód C je *lineární*, ak je to podprostor $\mathbb{Z}_2^n$, tj. $00\dots 0 \in C$ a $x, y \in C \Rightarrow x \text{ XOR } y \in C$. Lineární (n, k, d) -kód značíme $[n, k, d]$.

Generující matice $[n, k, d]$ -kódu C je matice $G(C)$ o k řádcích a n sloupcích, jejíž řádky tvoří bázi příslušného podprostoru. *Kontrolní matice* $[n, k, d]$ -kódu C je matice $K(C)$ o $n - k$ řádcích a n sloupcích, jejíž řádky tvoří bázi ortogonálního doplňku. Např. pro paritní $[4, 3, 1]$ -kód $C_4 = \{0000, 0011, \dots, 1111\}$ je

$$G(C_4) = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 1 \end{pmatrix} \quad \text{a} \quad K(C_4) = (1 \quad 1 \quad 1 \quad 1).$$

Příklad 5. *Které z kódů v Příkladu 1 jsou lineární?*

Příklad 6. *Napište kód, který má generující matici $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix}$ a sestrojte jeho kontrolní matici.*