

Samoopravné kódy

Připomenutí: Označme $S_n = \{0, 1\}^n$ množinu binárních stringů délky n . (*Samo*)*opravný kód* je podmnožina $C \subseteq S_n$. Prvky C se nazývají *kódová slova*. *Hammingova vzdálenost* dvou stringů $x, y \in S_n$ je počet bitů, které musíme v x změnit, abychom dostali y . Značí se $d(x, y)$. *Minimální vzdálenost kódu* C je $d = \min\{d(x, y) \mid x, y \in C, x \neq y\}$. Kód *opraví až c chyb*, pokud pro každý string $y \in S_n$ existuje nejvýše jedno kódové slovo $x \in C$, že $d(x, y) \leq c$.

Řekneme, že C (nad binární abecedou) je (n, k, d) -kód, pokud $C \subseteq S_n$, $|C| = 2^k$ a má minimální vzdálenost d . Nechť $A(n, d)$ označuje maximální velikost kódu $C \subseteq S_n$ s minimální vzdáleností d . Kombinatorickou kouli se středem $x \in S_n$ a poloměrem $r \geq \mathbb{N}_0$ definujeme jako $B_n(x, r) = \{y \in S_n : d(x, y) \leq r\}$.

Hammingův odhad: $A(n, d) \cdot |B(\mathbf{0}, t)| \leq 2^n$, kde $t = \lfloor \frac{d-1}{2} \rfloor$.

Kód $C \subseteq S_n$ (nad binární abecedou) je *lineární*, pokud tvoří vektorový podprostor S_n . Lineární (n, k, d) -kód se též označuje jako $[n, k, d]$ -kód. Matice, jejíž řádky tvoří bázi lineárního kódu C , se nazývá *generující matice* C . Matice, jejíž řádky tvoří bázi ortogonálního doplňku $C^\perp$ prostoru C , se nazývá *kontrolní matice* C .

Věta: Minimální vzdálenost C lze spočítat jako $\min\{d(\mathbf{0}, y) \mid y \in C, y \neq \mathbf{0}\}$.

Lineárně-algebraický fakt: Nechť $M \in \mathbb{Z}_2^{k \times n}$ je matice plného ranku, potom řádkový prostor M je $[n, k, d]$ -kód C pro nějaké vhodné d . (A M je generující matice kódu C .)

Příklad 1. Dokažte, že Hammingova vzdálenost $d(\cdot, \cdot) : S_n^2 \rightarrow \mathbb{N}_0$ je metrika. Tedy že splňuje

- (a) $\forall x \in S_n : d(x, x) = 0$,
- (b) $\forall x, y \in S_n : d(x, y) = d(y, x)$ (Symetrie),
- (c) $\forall x, y, z \in S_n : d(x, y) + d(y, z) \geq d(x, z)$ (Trojúhelníková nerovnost).

Příklad 2. Dokažte, že kód s minimální vzdáleností C opraví až $\lfloor \frac{d-1}{2} \rfloor$ chyb.

Příklad 3. Uvažme $n = 3$ a kódy $C_1 = \{000, 111\}$, $C_2 = \{001, 010, 110\}$, $C_3 = \{000, 011, 101, 110\}$. Jaká je minimální vzdálenost kódů C_1 , C_2 , C_3 ? Kolik chyb opraví?

Příklad 4. Spočítejte objem koule $B_n(x, r)$, $0 \leq r \leq n$. To jest, spočítejte $|B_n(x, r)|$.

Příklad 5. Hledáme kód $C \subseteq S_7$ s $d = 3$ a co nejvíce stringy.

- (a) Vzpomeňte si, jak vyrobit takový kód o 16 slovech, tj. $(7, 4, 3)$ -kód. *Hint: použijte Fanovu rovinu.*
- (b) Dokažte, že jakýkoliv kód $C \subseteq S_7$ s $d = 3$ musí splňovat $|C| \leq 16$.

Příklad 6. Uvažme $n = 3$ a kódy $C_1 = \{000, 111\}$, $C_2 = \{001, 010, 110\}$, $C_3 = \{000, 011, 101, 110\}$. Rozhodněte, které z těchto kódů jsou lineární a najděte jejich generující a kontrolní matice.

Příklad 7. Napište kód, který odpovídá generující matici $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$ a sestrojte jeho kontrolní matici.

Příklad 8. Nechť je G_1 generující matice (n_1, k, d_1) -kódu a G_2 generující matice (n_2, k, d_2) -kódu. Určete parametry kódu, jehož generující matice má tvar

- (a) $\begin{pmatrix} G_1 & G_2 \end{pmatrix}$,
- (b) $\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$.

Příklad 9 (Předtermín 17.12.). (a) Definujte (n, k, d) -kód (nad abecedou $\{0, 1\}$).

- (b) Uveďte příklad $(4, 2, 2)$ -kódu.
- (c) Existuje $(4, 2, 3)$ -kód?

Samoopravné kódy

Připomenutí: Označme $S_n = \{0, 1\}^n$ množinu binárních stringů délky n . (*Samo*)opravný kód je podmnožina $C \subseteq S_n$. Prvky C se nazývají *kódová slova*. *Hammingova vzdálenost* dvou stringů $x, y \in S_n$ je počet bitů, které musíme v x změnit, abychom dostali y . Značí se $d(x, y)$. *Minimální vzdálenost kódu* C je $d = \min\{d(x, y) \mid x, y \in C, x \neq y\}$. Kód *opraví až c chyb*, pokud pro každý string $y \in S_n$ existuje nejvýše jedno kódové slovo $x \in C$, že $d(x, y) \leq c$.

Řekneme, že C (nad binární abecedou) je (n, k, d) -kód, pokud $C \subseteq S_n$, $|C| = 2^k$ a má minimální vzdálenost d . Nechť $A(n, d)$ označuje maximální velikost kódu $C \subseteq S_n$ s minimální vzdáleností d . Kombinatorickou kouli se středem $x \in S_n$ a poloměrem $r \geq \mathbb{N}_0$ definujeme jako $B_n(x, r) = \{y \in S_n : d(x, y) \leq r\}$.

Hammingův odhad: $A(n, d) \cdot |B(\mathbf{0}, t)| \leq 2^n$, kde $t = \lfloor \frac{d-1}{2} \rfloor$.

Kód $C \subseteq S_n$ (nad binární abecedou) je *lineární*, pokud tvoří vektorový podprostor S_n . Lineární (n, k, d) -kód se též označuje jako $[n, k, d]$ -kód. Matice, jejíž řádky tvoří bázi lineárního kódu C , se nazývá *generující matice* C . Matice, jejíž řádky tvoří bázi ortogonálního doplňku $C^\perp$ prostoru C , se nazývá *kontrolní matice* C .

Věta: Minimální vzdálenost C lze spočítat jako $\min\{d(\mathbf{0}, y) \mid y \in C, y \neq \mathbf{0}\}$.

Lineárně-algebraický fakt: Nechť $M \in \mathbb{Z}_2^{k \times n}$ je matice plného ranku, potom řádkový prostor M je $[n, k, d]$ -kód C pro nějaké vhodné d . (A M je generující matice kódu C .)

Příklad 1. Dokažte, že Hammingova vzdálenost $d(\cdot, \cdot) : S_n^2 \rightarrow \mathbb{N}_0$ je metrika. Tedy že splňuje

- (a) $\forall x \in S_n : d(x, x) = 0$,
- (b) $\forall x, y \in S_n : d(x, y) = d(y, x)$ (Symetrie),
- (c) $\forall x, y, z \in S_n : d(x, y) + d(y, z) \geq d(x, z)$ (Trojúhelníková nerovnost).

Příklad 2. Dokažte, že kód s minimální vzdáleností C opraví až $\lfloor \frac{d-1}{2} \rfloor$ chyb.

Příklad 3. Uvažme $n = 3$ a kódy $C_1 = \{000, 111\}$, $C_2 = \{001, 010, 110\}$, $C_3 = \{000, 011, 101, 110\}$. Jaká je minimální vzdálenost kódů C_1 , C_2 , C_3 ? Kolik chyb opraví?

Příklad 4. Spočítejte objem koule $B_n(x, r)$, $0 \leq r \leq n$. To jest, spočítejte $|B_n(x, r)|$.

Příklad 5. Hledáme kód $C \subseteq S_7$ s $d = 3$ a co nejvíce stringy.

- (a) Vzpomeňte si, jak vyrobit takový kód o 16 slovech, tj. $(7, 4, 3)$ -kód. *Hint: použijte Fanovu rovinu.*
- (b) Dokažte, že jakýkoliv kód $C \subseteq S_7$ s $d = 3$ musí splňovat $|C| \leq 16$.

Příklad 6. Uvažme $n = 3$ a kódy $C_1 = \{000, 111\}$, $C_2 = \{001, 010, 110\}$, $C_3 = \{000, 011, 101, 110\}$. Rozhodněte, které z těchto kódů jsou lineární a najděte jejich generující a kontrolní matice.

Příklad 7. Napište kód, který odpovídá generující matici $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix}$ a sestrojte jeho kontrolní matici.

Příklad 8. Nechť je G_1 generující matice (n_1, k, d_1) -kódu a G_2 generující matice (n_2, k, d_2) -kódu. Určete parametry kódu, jehož generující matice má tvar

- (a) $\begin{pmatrix} G_1 & G_2 \end{pmatrix}$,
- (b) $\begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$.

Příklad 9 (Předtermín 17.12.). (a) Definujte (n, k, d) -kód (nad abecedou $\{0, 1\}$).

- (b) Uveďte příklad $(4, 2, 2)$ -kódu.
- (c) Existuje $(4, 2, 3)$ -kód?