Kombinatorika a grafy I — 13. cvičení*

24. května 2019

1 Samoopravné kódy

Abeceda Σ je konečná množina q *symbolů. Slovo* délky n je uspořádaná n-tice symbolů. Jako Σ^n označíme množinu slov délky n. *Hammingova vzdálenost* slov $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \Sigma^n$ je definována jako $d(x, y) = |\{i \in \{1, \ldots, n\} \colon x_i \neq y_i\}|$. *(Blokový) kód* je množina $C \subseteq \Sigma^n$ takzvaných *kódových slov*. Řekneme, že s kódem C je možné *opravit nanejvýš* t *chyb*, pokud pro každé $y \in \Sigma^n$ existuje nanejvýš jedno $x \in C$ takové, že $d(x, y) \leq t$. *Parametry* kódu C jsou $(n, k, d)_q$, kde $k = \log_q |C|$ a $d = \min_{x \neq y \in C}\{d(x, y)\}$.

Lineární kód C je podprostorem vektorového prostoru $\mathbb{F}_q^n$, kde $\Sigma = \mathbb{F}_q$ je konečné těleso velikosti q. Nechť C je lineární kód s parametry $[n, k, d]_q$. *Duálním kódem* k C je kód $C^\perp = \{y \in \mathbb{F}_q^n \colon \langle x, y\rangle = 0 \text{ pro každé } x \in C\}$, kde pro $x = (x_1, \ldots, x_n), y = (y_1, \ldots, y_n) \in \mathbb{F}_q^n$ je $\langle x, y\rangle = \sum_{i=1}^n x_i y_i$. *Generující maticí* kódu C je matice $M \in \mathbb{F}_q^{k \times n}$, která má za řádky vektory báze kódu C. *Kontrolní maticí* kódu C je matice $M^\perp \in \mathbb{F}_q^{(n-k) \times n}$, která je generující maticí kódu $C^\perp$.

Příklad 1. *Dokažte, že Hammingova vzdálenost je na množině* Σ^n *metrikou.*

Příklad 2. *Nechť* C *je lineární kód s parametry* $[n, k, d]_q$. *Dokažte následující tvrzení.*

(a) Platí $C^\perp = \{y \in \mathbb{F}_q^n \colon My = 0\}$, *kde* M *je generující maticí kódu* C.

(b) Duální kód $C^\perp$ *je lineárním kódem s délkou slov* n *a s dimenzí* $n - k$. *Speciálně platí* $\dim(C) + \dim(C^\perp) = n$.

(c) Platí $(C^\perp)^\perp = C$.

(d) Platí $C = \{x \in \mathbb{F}_q^n \colon M^\perp x = 0\}$, *kde* $M^\perp$ *je kontrolní maticí kódu* C.

Příklad 3. *Nechť* C *je kód s parametry* $(n, k, 2t + 1)_2$ *nad abecedou* $\{0, 1\}$. *Rozhodněte, jaké jsou parametry kódu* C', *který z* C *vznikne prodloužením každého kódového slova o jeden symbol určující paritu počtu jedniček v daném slově.*

Příklad 4. *Dokažte, že Hadamardovy kódy (nad tělesem* $\mathbb{F}_2$*) vzniklé Sylvesterovou konstrukcí jsou lineární.*

Příklad 5. *Uvažme kód obsahující všechna slova délky* $n \geq 2$ *nad* $\{0, 1\}$ *sudé váhy, neboli* $C = \{x = (x_1, \ldots, x_n) \in \mathbb{F}_2^n \colon \sum_{i=1}^n x_i \equiv 0 \pmod 2\}$. *Určete parametry tohoto kódu, ověřte, že je lineární a určete jeho duální kód* $C^\perp$.

*Informace o cvičení naleznete na http://kam.mff.cuni.cz/~balko/