

Samoopravné kódy

Alexandr Kazda

Univerzita Karlova

12. května 2020

- $\mathcal{R}(r, m)$ je $[2^m, 1 + \binom{m}{1} + \dots + \binom{m}{r}, 2^{m-r}]$ -kód ($m \geq r$)
- Kódová slova hodnoty polynomů stupně $\leq r$ v proměnných x_1, \dots, x_m nad \mathbb{Z}_2
- Příklad: $x_1x_2 + x_3 + 1$ má stupeň 2
- Značení: Jednočlen x_I je součin všech x_i pro $i \in I$, tj. $x_{\{2,5,7\}} = x_2x_5x_7$
- Chceme ukázat, že polynomy stupně $\leq r$ mají málo nul = mají hodně hodnot 1

Lemma

Bud' f nenulový polynom stupně $\leq r$ v $\mathbb{Z}_2[x_1, \dots, x_m]$. Pak f má hodnotu 1 (nenulu) v aspoň 2^{m-r} bodech (z 2^m).

- $m = 1$: $f(x_1) = ax_1 + b$ má aspoň 1 hodnotu 1
- Indukční krok

$$f(x_1, \dots, x_m) = x_1 g(x_2, \dots, x_m) + h(x_2, \dots, x_m)$$

- Pro $g = 0$ má $f = h$ aspoň $2^{m-1-r} \cdot 2$ hodnot 1
- Jinak g má stupeň $\leq r - 1$, tedy $g = 1$ pro aspoň $2^{m-1-(r-1)} = 2^{m-r}$ bodů
- Dopočteme x_1 , aby $f(x_1 \dots) = x_1 g + h = 1$ a máme 2^{m-r} hodnot 1 pro f

Parametry $\mathcal{R}(r, m)$

- Každé nenulové kódové slovo má aspoň 2^{m-r} nenul, tedy $\Delta(\mathcal{R}(r, m)) \geq 2^{m-r}$.
- Cvičení: Existuje polynom stupně r , který má nuly všude krom 2^{m-r} bodů.

Parametry $\mathcal{R}(r, m)$

- Pokud $f \neq g$ jsou polynomy stupně $\leq r$, tak $f - g$ má nenulové hodnoty,
- tedy kódová slova určená f a g se liší,
- tedy velikost kódu je počet polynomů stupně $\leq r$
- $f = \sum_{I \in \mathcal{J}} x_I$ pro \mathcal{J} systém nejvýše r -prvkových podmnožin $\{1, 2, \dots, m\}$
- Možných voleb \mathcal{J} je přesně $2^{1 + \binom{m}{1} + \dots + \binom{m}{r}}$
- Proto $k = 1 + \binom{m}{1} + \dots + \binom{m}{r}$.

- Generující – viz cvičení (hint na předchozím slajdu)
- Paritní: $\mathcal{R}(r, m)$ a $\mathcal{R}(m - r - 1, m)$ jsou navzájem duální kódy.
- Důkaz: Dimenze sedí $[2^m, 1 + \binom{m}{1} + \dots + \binom{m}{r}]$ vs. $[2^m, 1 + \binom{m}{1} + \dots + \binom{m}{m-r-1}]$.

$$1 + \binom{m}{1} + \dots + \binom{m}{r} + 1 + \binom{m}{1} + \dots + \binom{m}{m-r-1} = 2^m$$

- Stačí ukázat, že generátory jsou navzájem „ortogonální“ (nad \mathbb{Z}_2)

Stupně $|I| = a \leq r$ a $|J| = b \leq m - r - 1$

$$\langle x_I, x_J \rangle = \sum_{(x_1, \dots, x_m) \in 2^m} x_{i_1} x_{i_2} \cdots x_{i_a} \cdot x_{j_1} \cdots x_{j_b}$$

Aspoň jeden index ℓ není ani v I ani v J . Proto na x_ℓ součin $x_I x_J$ nezávisí a součet výše je proto sudý ($= 0$ v \mathbb{Z}_2).

- Šlo by to dělat systematicky; my to uděláme algebraicky...
- Zdrojové slovo má $1 + \binom{m}{1} + \dots + \binom{m}{r}$ bitů
- Bity=koeficienty polynomu f
- Odešleme tabulku hodnot f

- Proč nepočítat syndromy a reprezentanty? Protože možných syndromů je $2^{1+\binom{m}{1}+\dots+\binom{m}{m-r-1}}$ (pro $\mathcal{R}(1,5)$ je to $2^{2^5-5-1} = 2^{26}$, tj. asi 67 milionů)
- Přejde nám tabulka 2^m hodnot, chceme interpolovat polynomem f s.t. $\leq r$ (s chybami)
- Idea: Určíme koeficienty f postupně jeden po druhém,
- O každém koeficientu necháme „hlasovat“ různé části přijatého slova
- Příklad ze skript
- Jak je to obecně?

- Bud' $\{i_1, \dots, i_\ell\} = I \subset \{1, \dots, m\}$ velikosti $\leq r$. Zafixujme každou hodnotu x_j pro $j \notin I$ na 0 nebo 1 libovolně.
- Pozorování: Bud' J množina velikosti $\leq r$, že $\exists i \in I \setminus J$. Pak

$$\sum_{x_{i_1}, \dots, x_{i_\ell} = 0}^1 x_J$$

je sudé (tj. 0 v \mathbb{Z}_2).

- Naopak $\sum_{x_{i_1}, \dots, x_{i_\ell} = 0}^1 x_I = 1$.
- Přijde nám tabulka 2^m hodnot y , chceme zjistit, zda koeficient a_I je 1 nebo 0 (ignorujme na chvíli chyby)
- Zafixuji si hodnoty s indexy z $J = \{1, \dots, m\} \setminus I$ na nějaké hodnoty c a sčítám hodnoty y .