Teorie kódování

Lineární kódy

Grupa

$G = \langle \mathbb{M}; \cdot \rangle$ – multiplikativní grupa

- $\forall x, y \in \mathbb{M} : x \cdot y \in \mathbb{M}$
- $\forall x, y, z \in \mathbb{M} : (x \cdot y) \cdot z = x \cdot (y \cdot z)$
- $\exists e \in \mathbb{M} : \forall x \in \mathbb{M} : x \cdot e = e \cdot x = x$
- $\forall x \in \mathbb{M} : \exists x^{-1} \in \mathbb{M} : x \cdot x^{-1} = x^{-1} \cdot x = e$

$G = \langle \mathbb{M}; + \rangle$ – aditivní grupa

- $\forall x, y \in \mathbb{M} : x + y \in \mathbb{M}$
- $\forall x, y, z \in \mathbb{M} : (x + y) + z = x + (y + z)$
- $\exists e \in \mathbb{M} : \forall x \in \mathbb{M} : x + e = e + x = x$
- $\forall x \in \mathbb{M} : \exists (-x) \in \mathbb{M} : x + (-x) = (-x) + x = e$

Komutativní (Abelova) grupa

- $G = \langle \mathbb{M}; \cdot \rangle : \quad \forall x, y \in \mathbb{M} : x \cdot y = y \cdot x$
- $G = \langle \mathbb{M}; + \rangle : \quad \forall x, y \in \mathbb{M} : x + y = y + x$

Těleso

$T = \langle \mathbb{M}; +, \cdot \rangle$ – těleso

1. $\langle \mathbb{M}; + \rangle$ – komutativní grupa
2. $\langle \mathbb{M} \setminus \{0\}; \cdot \rangle$ – komutativní grupa
3. $\forall x, y, z \in \mathbb{M} : x \cdot (y + z) = x \cdot y + x \cdot z$
   $(x + y) \cdot z = x \cdot z + y \cdot z$

$Z_p = \langle \mathbb{Z}_p; \oplus, \otimes \rangle$ – konečné těleso

- $Z_p = \langle \mathbb{Z}_p; \oplus \rangle : \quad x \oplus y = (x + y) \bmod p$
- $Z_p = \langle \mathbb{Z}_p; \otimes \rangle : \quad x \otimes y = (x \cdot y) \bmod p$

Okruh – těleso oslabené o podmínku existence x^{-1}

Těleso (okruh) Z_p

Věta: Je-li $\mathrm{nsd}(x, p) = 1$, pak existuje x^{-1} v $\mathbb{Z}_p$.

Věta: Je-li $p \in \mathbb{P}$, pak $\langle \mathbb{Z}_p; \oplus, \otimes \rangle$ je konečné těleso.

Poznámka: Je-li $p \in \mathbb{P}$, pak $\forall x \in \mathbb{Z}_p \setminus \{0\}\ \exists x^{-1}$.

Věta: Je-li $p \notin \mathbb{P}$, pak $\langle \mathbb{Z}_p; \oplus, \otimes \rangle$ je pouze okruh.

Poznámka: $x \ominus y = x \oplus (-y)$
$x \oslash y = x \otimes y^{-1}$

Poznámka: $-x = (p - x) \bmod p$

Lineární prostor

$L = \langle \mathbb{T}^n; +, \cdot \rangle$ – lineární prostor nad tělesem $\mathbb{T}$

1. $\langle \mathbb{T}^n; + \rangle$ – komutativní grupa
2. $\forall \overline{x} \in \mathbb{T}^n, \forall t \in \mathbb{T} : t \cdot \overline{x} \in \mathbb{T}^n$
3. $\forall \overline{x}, \overline{y} \in \mathbb{T}^n, \forall s, t \in \mathbb{T} : t \cdot (\overline{x} + \overline{y}) = t \cdot \overline{x} + t \cdot \overline{y}$
   $(s \cdot t) \cdot \overline{x} = s \cdot (t \cdot \overline{x})$
   $(s + t) \cdot \overline{x} = s \cdot \overline{x} + t \cdot \overline{x}$
   $1 \cdot \overline{x} = \overline{x}$
   $0 \cdot \overline{x} = \overline{0}$

Lineární kód

Definice: Lineárním kódem rozumíme libovolný podprostor prostoru $\mathbb{A}^n$.

Věta: Každý lineární (n, k)-kód má k informačních a $(n - k)$ kontrolních znaků.

Pokud bude $\alpha_1, \alpha_2, \ldots, \alpha_k$ báze kódu K, potom libovolné slovo vyjádříme jako

$$\beta = a_1\alpha_1 + a_2\alpha_2 + \cdots + a_k\alpha_k$$

pro právě jednu k-tici $\alpha = a_1 a_2 \ldots a_k$.
Předpis pro kódování informačních znaků je tedy

$$\varphi(\alpha) = a_1\alpha_1 + \cdots + a_k\alpha_k = \sum_{i=1}^{k} a_i\alpha_i \quad (\alpha = a_1 \ldots a_k)$$

Generující a kontrolní matice

Definice: Kontrolní matice **H** lineárního (n, k)-kódu K je libovolná matice soustavy homogenních lineárních rovnic, jejichž řešením je K.

Tedy $\alpha \in K \Leftrightarrow \mathbf{H}\alpha = \theta \quad (\theta = 00\ldots0)$

Definice: Generující matice **G** lineárního (n, k)-kódu K je matice typu $k \times n$, kde řádky jsou tvořeny bázovými slovy $\alpha_1, \alpha_2, \ldots, \alpha_k$.

$$\mathbf{G} = \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_k \end{pmatrix}$$

Vlastnosti G:

- každý řádek je kódovým slovem
- řádky jsou LNZ $\Rightarrow h(\mathbf{G}) = k$
- každé kódové slovo je lineární kombinací řádků

Systematický kód

Věta: Lineární (n, k)-kód je systematický $\Leftrightarrow$ má generující matici ve tvaru $\mathbf{G} = (\mathbf{E}|\mathbf{B})$, kde $\mathbf{E}$ je jednotková matice a $\mathbf{B}$ je typu $k \times (n-k)$.

Potom platí:

$$\begin{aligned}
\varphi(\alpha) &= \alpha\mathbf{G} = \alpha(\mathbf{E}|\mathbf{B}) = \\
&= a_1 \dots a_k \begin{pmatrix} 1 & \dots & 0 & b_{11} & \dots & b_{1,n-k} \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & 1 & b_{k1} & \dots & b_{k,n-k} \end{pmatrix} = \\
&= \underbrace{a_1 \dots a_k}_{\alpha} \underbrace{a_{k+1} \dots a_n}_{\alpha'} = \alpha\alpha'
\end{aligned}$$

Ekvivalentní kódy

Věta: Říkáme, že dva blokové kódy K_1, K_2 (délky n) jsou ekvivalentní, existuje-li permutace Π čísel $1, \ldots, n$ taková, že platí $a_1 \ldots a_n \in K_1 \Leftrightarrow a_{\Pi(1)} \ldots a_{\Pi(n)} \in K_2$.

Věta: Každý lineární kód je ekvivalentní se systematickým lineárním kódem.

Věta: Lineární kód s generující maticí $\mathbf{G} = (\mathbf{E}_k|\mathbf{B})$ má kontrolní matici $\mathbf{H} = (-\mathbf{B}^T|\mathbf{E}_{n-k})$.

Duální kód

Skalární součin slov $\alpha, \beta \in \mathbb{A}^n$: $\alpha \odot \beta = \sum_{i=1}^{n} a_i b_i$.

Definice: Řekneme, že slova α, β jsou ortogonální, $\alpha \perp \beta$, je-li $\alpha \odot \beta = 0$.

Definice: Duálním kódem $K^\perp$ k lineárnímu kódu K rozumíme množinu všech slov α, která mají s každým slovem z K skalární součin roven 0.

$$K^\perp = \{\alpha \in \mathbb{A}^n | \forall \beta \in K : \alpha \perp \beta\}$$

Věta: Duální kód $K^\perp$ lineárního (n, k)-kódu K má $(n - k)$ informačních znaků a je tedy $(n, n - k)$-kódem. Generující matice kódu K je kontrolní maticí duálního kódu $K^\perp$ a naopak.

Objevování chybových slov

Definice: Řekneme, že lineární kód K objevuje chybové slovo ϵ, platí-li $\forall \alpha \in K : \alpha + \epsilon \notin K$.

Poznámka: Kód K může objevit jen $\epsilon \notin K$.

Definice: Hammingova váha slova $\alpha \in \mathbb{A}^n$, $\alpha = a_1 \dots a_n$ je

$$\|\alpha\| = |\{i \in \hat{n} | a_i \neq 0\}|$$

Lemma: Lineární kód K objevuje t-chyby $\Leftrightarrow$ objevuje všechna chybová slova váhy nejvýše t.

Poznámka: $\mu(K) = \min\{\|\alpha\| | \alpha \in K, \alpha \neq \theta\}$

Věta: Lineární kód K objevuje t-chyby $\Leftrightarrow$ každých t sloupců jeho kontrolní matice je LN.

Věta: Lineární kód K opravuje t-chyby $\Leftrightarrow$ každých $2t$ sloupců jeho kontrolní matice je LN.

Opravování chybových slov

Definice: Řekneme, že dekódování $\delta : \mathbb{A}^n \to K$ opravuje (dekóduje) chybové slovo $\epsilon \Leftrightarrow \forall \alpha \in K : \delta(\alpha + \epsilon) = \alpha$.

Definice: Třída slova $\epsilon = e_1 \dots e_n$ podle kódu K je množina

$$\epsilon + K = \{\epsilon + \alpha | \alpha \in K\}$$

Věta: Libovolné dekódování opraví nejvýše po jednom chybovém slově z každé třídy podle K.

Poznámka: Lineární (n, k)-kód $\Rightarrow$ existuje s^{n-k} tříd.

Standardní dekódování

Z každé třídy vybereme jedno slovo – **pivot (reprezentant)** – tak, aby měl nejmenší váhu v dané třídě. Pro $\beta \in \mathbb{A}^n$ označme π_β pivota vybraného ve třídě obsahující β.

$\delta(\beta) = \beta - \pi_\beta \qquad \beta - \pi_\beta \in K; \beta \in K \Rightarrow \pi_\beta = \theta$

Tabulková metoda standardního dekódování

Tabulka má s^{n-k} řádků, s^k sloupců.

Syndromová metoda standardního dekódování

Syndromem slova α rozumíme slovo

$$\sigma_\alpha = \mathbf{H}\alpha, \quad \sigma_\alpha \in \mathbb{A}^{n-k}$$

$\alpha \in K \Leftrightarrow \mathbf{H}\alpha = \theta \Leftrightarrow \sigma_\alpha = \theta$

Vlastnost syndromu: přijaté slovo má stejný syndrom, jako chybové slovo

$\beta = \alpha + \epsilon \quad \Rightarrow \quad \sigma_\beta = \sigma_\alpha + \sigma_\epsilon = \sigma_\epsilon$

Slova ze stejné třídy mají stejný syndrom.