Tutorial 2 SK

22 September 2021 18:02

LINEÁRNE KÓDY

$C \subseteq \{0,1\}^n$

(n, M, d)

minimálna vzdialenosť

→ porovnať všetky dvojice slov

$O(M^2)$

KÓDOVAŤ

$m_0 \longrightarrow c_0$

$m_1 \longrightarrow c_1$

$\vdots$

$m_{M-1} \longrightarrow c_{M-1}$

DEKÓDOVAŤ

Pri prijatí w

$\min_{c \in C} H(w, c)$

LINEÁRNE KÓDY - DEFINÍCIA

Kód $C \subseteq \{0, \dots, q-1\}^n$ (q je mocnina prvočísla)

je lineárny, ak má nasledujúce dve vlastnosti:

I. $x, y \in C \Rightarrow x + y \in C$

$x = (x_0, \dots, x_{n-1})$

$y = (y_0, \dots, y_{n-1})$

$x + y = (x_0 + y_0, \dots, x_{n-1} + y_{n-1})$

II. $\forall k \in \{0, \dots, q-1\} \quad \forall c \in C, k \cdot c = (k \cdot c_0, \dots, k \cdot c_{n-1}) \in C$

$(+, \cdot)$ sú operácie konečného poľa $\mathbb{F}_q$ (mod q až q je

$(+, \cdot)$ sú operácie konečného poľa $\mathbb{F}_q$ $\left(\text{mod } q \text{ až } q \text{ je } \underset{\text{prvočíslo}}{p}\right)$

Ex 2.1 $C = \{00000, 00110, 10010, 10001, 00101, 10100, 00011, 10111\}$

10100 — 10100 — 00110

II. $k \in \{0,1\}$ ✓

I.

Lineárny kód je podpriestor $(\{0,1\}^n, +, \cdot)$ (Skalárny súčin)

n-dimenzionálny priestor s 2^n vektormi

k-dimenzionálny podpriestor má 2^k vektorov. $(k=3$ pre $C)$

NOTÁCIA → $(n, 2^k, d) \simeq (n, k, d)$

Pretože C je lineárny podpriestor, existuje k vektorov, ktoré sú lineárne nezávislé. Tieto vektory tvoria bázu.

$\{b_0, \dots, b_{k-1}\} \subseteq C$ L.N. ⇝ žiadny vektor nieje lineárnou kombináciou iných

$\forall c \in C$ $\boxed{c = a_0 b_0 + a_1 b_1 + \dots + a_{k-1} b_{k-1}}$

$C = \{ a_0 b_0 + \dots + a_{k-1} b_{k-1} \}$

$a_i \in \{0, \dots, q-1\}$

$(a_0 + a_0') b_0 \dots (a_{k-1} + a_{k-1}') b_{k-1}$

$C = \{00000, 00110, 10010, 10001, 00101, 10100, 00011, 10111\}$

$b_0 = 00110$
$b_1 = 10010$ $\Big\}$ 10100
$b_2 = 10001$ $\Big\}$ 00011 $\Big\}$ 10111 $\Big\}$ 00101

$0 \cdot b_0 + 0 \cdot b_1 + 0 \cdot b_2 = 00000$ ✗

Lineárny kód vždy obsahuje nulové slovo

Ako počítať d lineárneho kódu?

- $H(c_1, c_2) = H(c_1 + w, c_2 + w)$ $\quad w \in \{0,1\}^n$
  $\Big\|$ $\quad c_1, c_2 \in C$
  $H(c_1 + c_1, c_2 + c_1)$ $\quad c \in C$
  $\Big\|$
  $H(\vec{0}, c_2 + c_1)$
  $\Big\|$

→ $H(\vec{0}, c) \Rightarrow$ Na nájdenie d stačí nájsť kódové slovo s najmenším počtom jedničiek

$O(n)$

... najmenším počtom jednotiek

$O(M)$

$C = \{00000, 00110, 10010, 10001, 00101, 10100, 00011, 10111\}$

$(5, 3, 2)$-kód

KÓDOVANIE

Generujúca matica $G = \begin{bmatrix} b_0 \\ \vdots \\ b_{k-1} \end{bmatrix}$ kde matica ktorá má na riadkoch bázové vektory

$M = 2^k \Rightarrow m_i \sim$ binárna expanzia i $\quad i \in \{0, \dots 2^k - 1\}$

$m_1 = 001$
$\vdots$
$m_5 = 101$ $\quad m_i \in \{0,1\}^k$

na zakódovanie m_i spočítam

$m_i \cdot G$ ⬅

$C = \{00000, 00110, 10010, 10001, 00101, 10100, 00011, 10111\}$

$G = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{pmatrix}$

$m_1 = 001$ $\quad a_0 a_1 a_2$ $\qquad m_1 \cdot G = (001) \cdot G = (0\cdot 0 + 1\cdot 0 + 1\cdot 1 \mid 0\,0\,0\,1)$

$m_5 = 101 \Rightarrow m_5 = a_0 \cdot b_0 + a_1 b_1 + a_2 \cdot b_2$

$m_5 = 101 \Rightarrow m_5 = a_0 \cdot b_0 + a_1 b_1 + a_2 \cdot b_2$

Nepotrebujeme kódovaciu tabuľku, stačí matica G.

Štandardná forma $G = (I_k \mid A)$

$k \times k$ identita

$k \times (n-k)$ matica (checksum matica)

Kód so štandardnou generujúcou maticou sa nazýva systematický.

$m \cdot G = [m_1 \overbrace{\quad}^{n-k}]$

Algoritmus na získanie normálnej formy:

1) Začneme s ľubovoľnou maticou G.

2) Povolené operácie:

a.) permutácia riadkov
b.) násobenie riadkov nenulovým skalárom
c.) súčet riadkov

} Zmena bázy alebo nie bázy

d.) permutácia stĺpcov
e.) násobenie stĺpcov nenulovým skalárom

} Zmena kódu na ekvivalentný

$$G = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 \end{pmatrix} \simeq \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} G_1$$

$$G = \begin{pmatrix} 0&0&1&1&0 \\ 1&0&0&1&0 \\ 1&0&0&0&1 \end{pmatrix} \simeq \begin{pmatrix} 1&0&0&1&0 \\ 0&0&1&1&0 \\ 0&0&1&0&1 \end{pmatrix} \simeq \begin{pmatrix} 1&0&0&1&0 \\ 0&0&1&1&1 \\ 0&0&1&0&1 \end{pmatrix} G_1$$

$$\simeq \begin{pmatrix} 1&0&0&0&1 \\ 0&0&1&1&1 \\ 0&0&1&0&1 \end{pmatrix} \simeq \left(\begin{array}{ccc|cc} 1&0&0&0&1 \\ 0&1&0&1&1 \\ 0&0&1&1&1 \end{array}\right) = (\pi_3 | A) = G'$$

$(abc) \cdot G' = abc\,0\,(a+b+c)$ $\qquad$ $\begin{matrix}1\\0\\1\end{matrix} \rightarrow a+c$

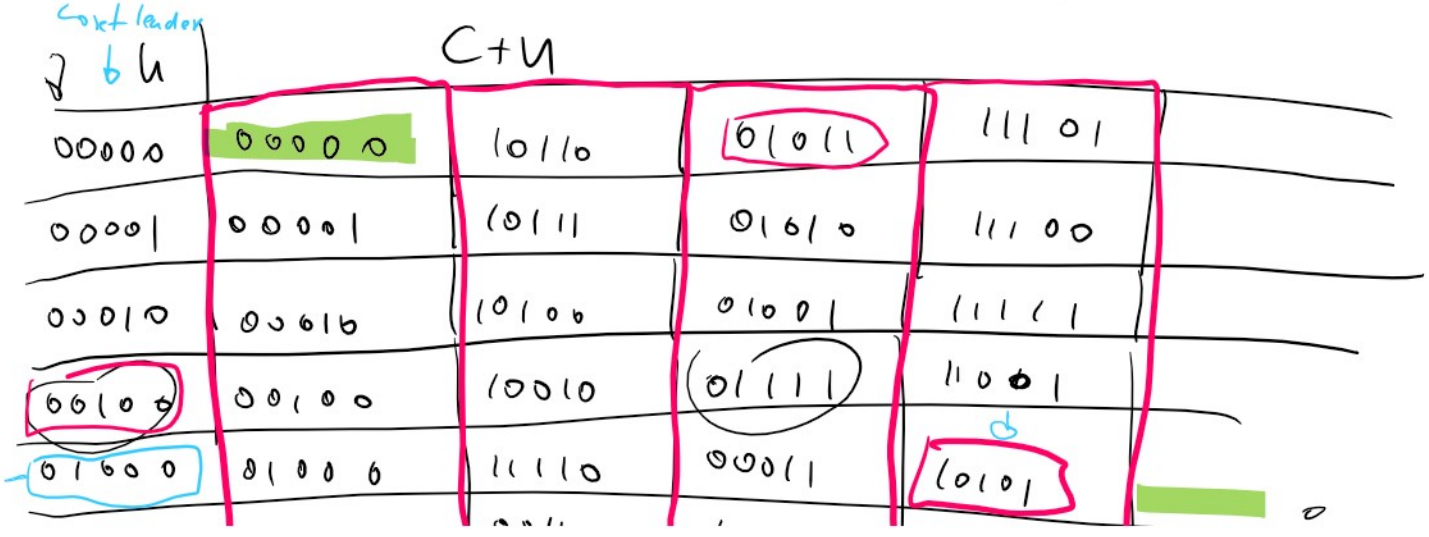
DEKÓDOVANIE

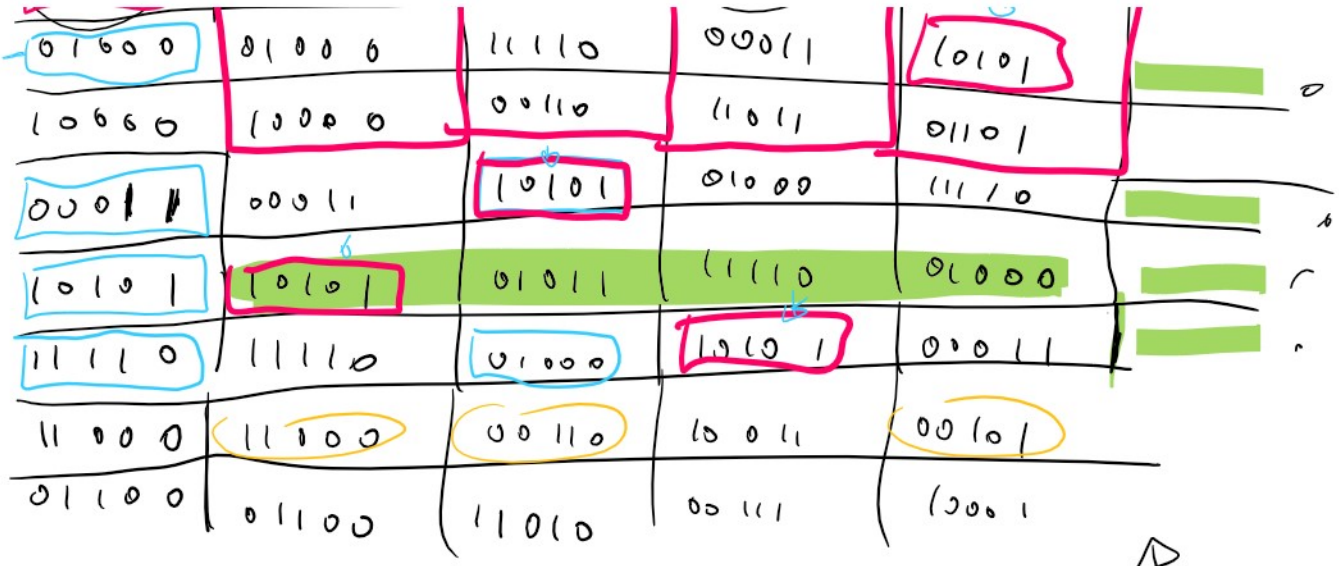
$\text{Coset } u = \{u + c \mid c \in C\}$ $\qquad u \in \{0,1\}^5$

$\forall u, v \in \{0,1\}^n$ | Coset u a coset v sú buď rovnaké, alebo disjunktné.

Coset leader → vektor s najmenšou váhou patriaci do balíka

EX 2.7 $\qquad C = \{01000, 10110, 01011, 11101\}$ $\qquad (5,2,3)$-kód





1.) prijaté slovo označíme w

2.) nájdeme w v štandardnej tabuľke

3.) nájdeme coset leadera lw zodpovedajúceho kosetu

4.) dešifrujeme ako $w + lw$

$w = 11110 \Rightarrow 11010$

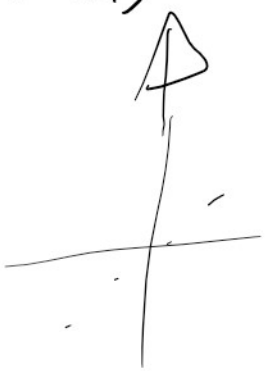
Dešifrovanie pomocou syndrómov

Duálny kód $C^\perp$ of C

Skalárny súčin $\vec{x} \cdot \vec{y} = (x_0 \cdot y_0 + x_1 \cdot y_1 + \dots + x_{n-1} \cdot y_{n-1})$

$\vec{x}$ a $\vec{y}$ sú kolmé ak $\vec{x} \cdot \vec{y} = 0$

$$C^\perp = \{ w \mid w \in \{0,1\}^n : w \cdot c = 0, \forall c \in C \}$$



ak C má dimenziu k, tak $C^\perp$ má dimenziu $n-k$

$G = (I_2 \mid A)$ = generátorová matica C

$H = (-A^T \mid I_{n-2})$ = generátorová matica $C^\perp$

$$\left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \end{array}\right) = G$$

$$H = \left(\begin{array}{ccc|cc} 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{array}\right)$$

$\forall c \in C$

$c \cdot H^T = \underbrace{000}_{n-2}$ ✓

$$(01001) \cdot \begin{pmatrix} 0 & 0 \\ 1 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \end{pmatrix} = \left[\underbrace{(01001)\cdot(00010)}_{0},\ \underbrace{(01001)\cdot(11101)}_{0} \right]$$

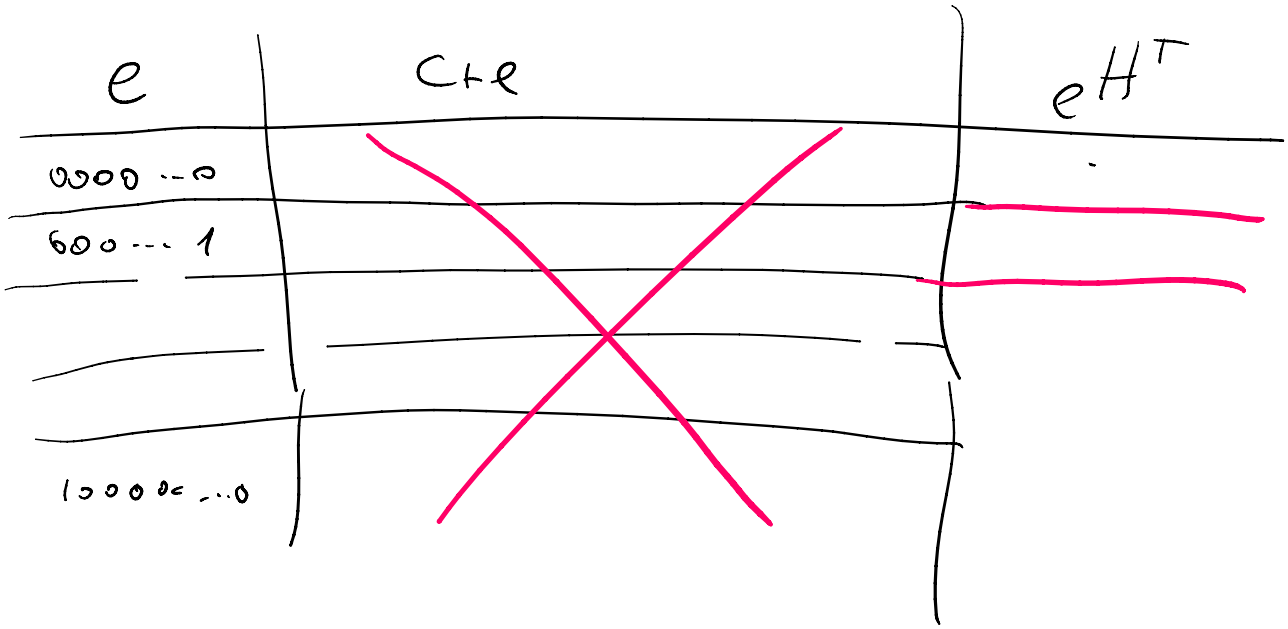
chyba v správe je definovaná vektorom e

$w = (c+e)$

$$w \cdot H^T = (c+e)\cdot H^T = c \cdot H^T + e \cdot H^T = \underbrace{e \cdot H^T}_{\text{Syndróm}}$$

$\forall e_1, e_2$ v rovnakom kosete $\quad e_1 \cdot H^T = e_2 \cdot H^T$

Existuje korespondencia jedna z jednej medzi kosetmi a syndrómami



1.) Označíme prijaté slovo ako w

2.) Spočítame $w \cdot H^T \sim s$

3.) Zistíme lead. w z koseta ktorý má syndróm s

4.) Dekódujem ako $w+l_w$