Věta $H(u,v)$ ... vzd. slov u, v

ad 1. $H(u,v) \geq r+1$ pro kódová slova

došlo k $\leq r$ chybám $\Rightarrow$ slovo v, které se liší od kódového slova nejvýše na r místech

$\Rightarrow$ v není kódové.

$H(u,v) \leq r$ pro kódová $\Rightarrow$ chybu nemusíme odhalit, při přijetí u nevíme, jestli bylo vysláno u nebo v.

ad 2. $\exists u, v$ kódová : $H(u,v) \leq 2r \Rightarrow$ $\exists w : H(u,w) \leq r \wedge H(w,v) \leq r$)

při přijetí w nevíme, jestli bylo vysláno u nebo v.

„$\Leftarrow$" analogicky

4 6-14:08

Úvod do kódování — Pár slov o šifrách

Jak konstruovat kódová slova, abychom je snadno rozpoznali? Kontrolu parity jsme už viděli, další triviální možnost je prosté opakování bitů – např. $(3,1)$–kód bere jednotlivé bity a posílá je třikrát po sobě.
Systematickou cestou je pak využití dělitelnosti polynomů. Zpráva $b_0 b_1 \dots b_{k-1}$ je reprezentována jako polynom $m(x) = b_0 + b_1 x + \cdots + b_{k-1} x^{k-1}$. k

Definice

Nechť $p(x) = a_0 + a_1 x + \cdots + a_{n-k} x^{n-k} \in \mathbb{Z}_2[x]$ je polynom s $a_0 = 1$, $a_{n-k} = 1$. **Polynomiální kód generovaný polynomem** $p(x)$ je (n,k)–kód jehož slova jsou polynomy stupně menšího než n dělitelné $p(x)$.

$c_0 + c_1 x + \dots + c_{n-1} x^{n-1}$, n

4 6-14:21

Př. 1: $v(x) = q(x) \cdot p(x) = q(x)(1+x)$

$v(x)$ má kořen 1 $\Leftarrow$ kořen 1

$v(1) = 0$

Př. 2: $p(x) = 1 + x + x^2$ $(3,1)$

kódujeme: $1 \cdot x^2 = 1 \cdot p(x) + (x+1)$

$[\ x^2 \equiv x+1 \quad (\text{mod } p(x))]$

$1 \longrightarrow \underset{1\ \ 1}{1+x} : \underset{1}{1}$ $\quad 0 \to 0\ 0\ 0$

4 6-14:25

Primitivní $p(x)$ stupně m: [nad $\mathbb{Z}_2$]

$p(x) \mid x^{2^m - 1} - 1 = x^{2^m-1} + 1$

$p(x) \nmid x^k - 1$ pro $k < 2^m - 1$

4 6-14:31

Věta st $p(x) = m$

kód $(n, n-m)$

detekuje jednoduché a dvojité chyby

Dk. $v(x) = u(x) + e(x)$ ... přenesený kód

chybu detekujeme $\Leftrightarrow p(x) \nmid e(x)$

Jedna chyba $\Leftrightarrow e(x) = x^i$, $i \in \{0, \dots, n-1\}$

zřejmě $p(x) \nmid x^i$ [neboť $p(0) \neq 0$]

2 chyby $\Leftrightarrow e(x) = x^i + x^j$, $i, j \in \{0, \dots, n-1\}$, $i < j$

$p(x) \mid x^i + x^j \Leftrightarrow p(x) \mid x^i(1 + x^{j-i}) \wedge p(x) \nmid x^i$

$\Leftrightarrow p(x) \mid (1 + x^{j-i}) \overset{\text{prim}}{\Leftrightarrow} j - i \geq 2^m - 1$

Přitom $p(x) \nmid (1 + x^{j-i})$ pro $n \leq 2^m - 1$

4 6-14:39

Máme $\frac{\varphi(2^n - 1)}{n}$ primitivních polynomů stupně n nad $\mathbb{Z}$.

$n = 2$: $\frac{\varphi(3)}{2} = 1$

$n = 3$: $\frac{\varphi(7)}{3} = 2$

$n = 5$: $\frac{\varphi(2^5 - 1)}{5} = 6$

4 6-14:51

Věta

Každý polynomiální (n, k)–kód je lineární kód.

Stačí dokázat, že zobrazení $g: \mathbb{Z}_2^k \to \mathbb{Z}_2^n$ (mezi v.p.) daného polynomem $p(x)$ je lineární.

(i) $a \in \mathbb{Z}_2$, $u \in \mathbb{Z}_2^k$: $g(a\cdot u) = a \cdot g(u)$

(ii) $u, v \in \mathbb{Z}_2^k$: $g(u+v) = g(u) + g(v)$

$g(u) = r_1(x) + x^{n-k}\cdot u(x)$

$g(v) = r_2(x) + x^{n-k}\cdot v(x)$

$g(u+v) = r_3(x) + x^{n-k}[u(x)+v(x)]$

$r_3(x) \equiv r_1(x) + r_2(x)$ [mod $p(x)$]

4 6-14:56

Úvod do kódování — Pár slov o šifrách

Věta

Každý polynomiální (n, k)–kód je lineární kód.

Generující matice (7, 4) kódu příslušná k polynomu $p(x) = 1 + x^2 + x^3$ je

(1) $x^3 \equiv 1 + x^2$ (1 0 1)

$x \cdot x^3$

$x^2 \cdot x^3$

$x^3 \cdot x^3$

$\mathbb{Z}_2^4$

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

$1 \quad x \quad x^2 \quad x^3$

P $(n-k)/k$

E_k

4 6-15:02

$$\mathbb{Z}_2^k \underset{h}{\overset{g}{\rightleftarrows}} \mathbb{Z}_2^n \qquad G = \begin{pmatrix} P \\ E_k \end{pmatrix} \qquad H = (E_{n-k} \ P)$$

$(h \circ g)(u) \overset{(?)}{=} 0$

(1) ⇒ (3) $h(u) = H \cdot u = 0 \iff u \in \operatorname{Ker} h$

(2) $u \in \operatorname{Im} g \iff u$ je kódové slovo

(1) $(h\circ g)(u) = H(G\cdot u) = (H\cdot G)\cdot u =$

$= (E_{n-k} | P)\begin{pmatrix} P \\ E_k \end{pmatrix} = (E_{n-k}P + PE_k) =$

$= P + P = 0$

4 6-15:05

Máme tedy $h \circ g = 0$ tj. $\operatorname{Im} g \subseteq \operatorname{Ker} h$

Obrácení: prvních $(n-k)$ sloupců H tvoří bázi $\mathbb{Z}_2^{n-k}$ ($h: \mathbb{Z}_2^n \to \mathbb{Z}_2^k$)

Obraz $\operatorname{Im} h$ generuje celý $\mathbb{Z}_2^{n-k}$ ⇒ obsahuje 2^{n-k} prvků.

$$f: G \to K \qquad G/_{\ker f} \cong f(G) \qquad |\ker f| = \frac{|G|}{|\operatorname{Im} f|}$$

$$|\operatorname{Ker} h| = \frac{|\mathbb{Z}_2^n|}{|\operatorname{Im} h|} = \frac{2^n}{2^{n-k}} = 2^k$$

Přitom $|\operatorname{Im} g| = 2^k$ prvků

4 6-15:13

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

$H \cdot G = 0$ nulová matice 3/4

4 6-15:10

DRSA: $d \cdot e \equiv 1 \pmod{\varphi(n)}$

Euler: $(M, n) = 1$: $M^{\varphi(n)} \equiv 1 \pmod n$

$OT \equiv C^d \equiv (M^e)^d = M^{e\cdot d} = M^{1+k\cdot\varphi(n)} \equiv$

$e \cdot d = 1 + k\cdot\varphi(n)$

$\equiv M\cdot (M^{\varphi(n)})^k \equiv$

$\equiv M \cdot 1^k = M \pmod n$

4 6-15:10