Cyklické kódy

V tíhle kapitole, $\mathbb{F} = \mathbb{Z}_2$

Př.: paritní kód délky 4

$$n = 4$$

$$000|0$$
$$001|1$$
$$010|1$$
$$011|0$$
$$100|1$$
$$101|0$$
$$110|0$$
$$111|1$$

$v \in \mathbb{Z}_2^4$ $\quad \sum_{i=1}^{4} v_i = 0$

0110, 1100, 1001, 0011

$H = (1\,1\,1\,1)$

Př.: Hammingův kód (chiba kode / DCV)

Def. lineární kod $\mathcal{C}$ délky n je cyklický

$\forall w \in \mathcal{C}$ platí že $w_1 w_2 \dots w_{n-1} w_0 \in \mathcal{C}$

$w_0 w_1 \dots w_{n-1}$

Věta: $\forall w \in \mathcal{C}$ platí: $\forall i \in \{0, \dots, n-1\}$

$w_i w_{i+1} \dots w_{n-1} w_0 \dots w_{i-1} \in \mathcal{C}$

$w_0 w_1 \dots w_{n-1}$

kódové slova $\equiv$ polynom nad $\mathbb{Z}_2$

$$\sum_{i=0}^{n-1} w_i x^i \in \mathbb{Z}_2[x]$$

$w \longrightarrow p(w)$

Př.: $0110 \equiv x + x^2$

cyklický posun doprava o 1

$$w_0 x^0 \mid w_1 x^1 \mid w_2 x^2 \mid \dots$$
$$w_{n-1} x^n \mid w_0 x^1 \mid w_1 x^2 \mid w_2 x^3 \dots$$

$x \odot p(w) \mod (x^n - 1)$

$x^n \equiv x^0$

násobení v okruhu polynomů $\mathbb{Z}_2[x]/x^n - 1$

x^0 x^1 x^2 x^3	
0 0 0 | 0	$\longrightarrow 0$
0 0 1 | 1	$\longrightarrow x^2 + x^3$
0 1 0 | 1	$\longrightarrow x + x^3$
0 1 1 | 0	$\longrightarrow x + x^2$
1 0 0 | 1	$\longrightarrow 1 + x^3$
1 0 1 | 0	$\longrightarrow 1 + x^2$
1 1 0 | 0	$\longrightarrow 1 + x$
1 1 1 | 1	$\longrightarrow 1 + x + x^2 + x^3$

$\forall p(w)$ násobek $(x+1) \mod x^4 - 1$

$p(w) = (x+1) q(w)$

kde stupeň ≤ 2

$\mathbb{Z}_2[x]$

- $0 \cdot (x+1) = 0$
- $1 \cdot (x+1) = x+1$
- $x(x+1) = x^2+x$
- $x^2(x+1) = x^3+x^2$
- $(x+1)(x+1) = x^2+2x+1 = x^2+1$
- $(x^2+1)(x+1) = x^3+x^2+x+1$
- $(x^2+x+1)(x+1) = x^3+1$
- $(x+x^2)(x+1) = x^3+1$

Úmluva: $\mathbb{Z}_2[x]$ polynomy v x

avšak polynomy v $\mathbb{Z}_2[x]/q(x)$

uvažujme v proměnné Z

Stupeň $p \in \mathbb{C}$ $\leq n-1$

$p(x) \bmod x^n - 1 = p(x)$

Věta: Buď $\mathcal{C}$ cyklický kód délky n a dimenze k. $\exists g \in \mathcal{C}$ polynom stupně $n-k$

$\uparrow$

$\exists w \in \mathcal{C}: g(w) = g$

t.č.:

1) $\mathcal{C} = \{a(z) \cdot g(z) \quad a(z) \in \mathbb{Z}_2[x]/\langle x^n - 1 \rangle\}$

2) $g(z), z \cdot g(z), z^2 \cdot g(z), \dots z^{k-1} \cdot g(z)$

$\uparrow$ tvoří bázi $\mathcal{C}$

3) $g(x)$ dělí $x^n - 1$ (v $\mathbb{Z}_2[x]$)

Dk:

$0 \neq g(z) :=$ polynom v $\mathbb{C}$ s nejmenším stupněm

$\boxed{s} :=$ stupeň $g(z)$, $s \leq n-1$

vezměme si $v(z) \in \mathbb{C}$ libovolně

$r(x)$, dělíme $g(x)$ v $\mathbb{Z}_2[x]$:

$$v(x) = q(x) \cdot g(x) + r(x)$$

1) $r(x) = n \cdot (x^n - 1)$, ARA $r(z) \equiv 0$ — chceme

2) $r(z) \not\equiv 0$ st $r < s$ — nechceme

$$r(z) = v(z) - \boxed{q(z) \cdot g(z)}$$

$v(z) \in \mathbb{C}$, pokud

potom $\in \mathbb{C}$

↑ spor s tím že $g(z)$ má nejmenší stupeň v $\mathbb{C}$

Proč je $a(z) \cdot g(z) \in C$?

Víme $g(z) \in C$

$$a(z) = \sum_{i \in J} x^i$$

J ... lineární $\in C$

$$a(z) \cdot g(z) = \left[\sum_{i \in J} x^i\right] \cdot g(z)$$

i-tý posun $g(z)$

$\in C$ cyklický

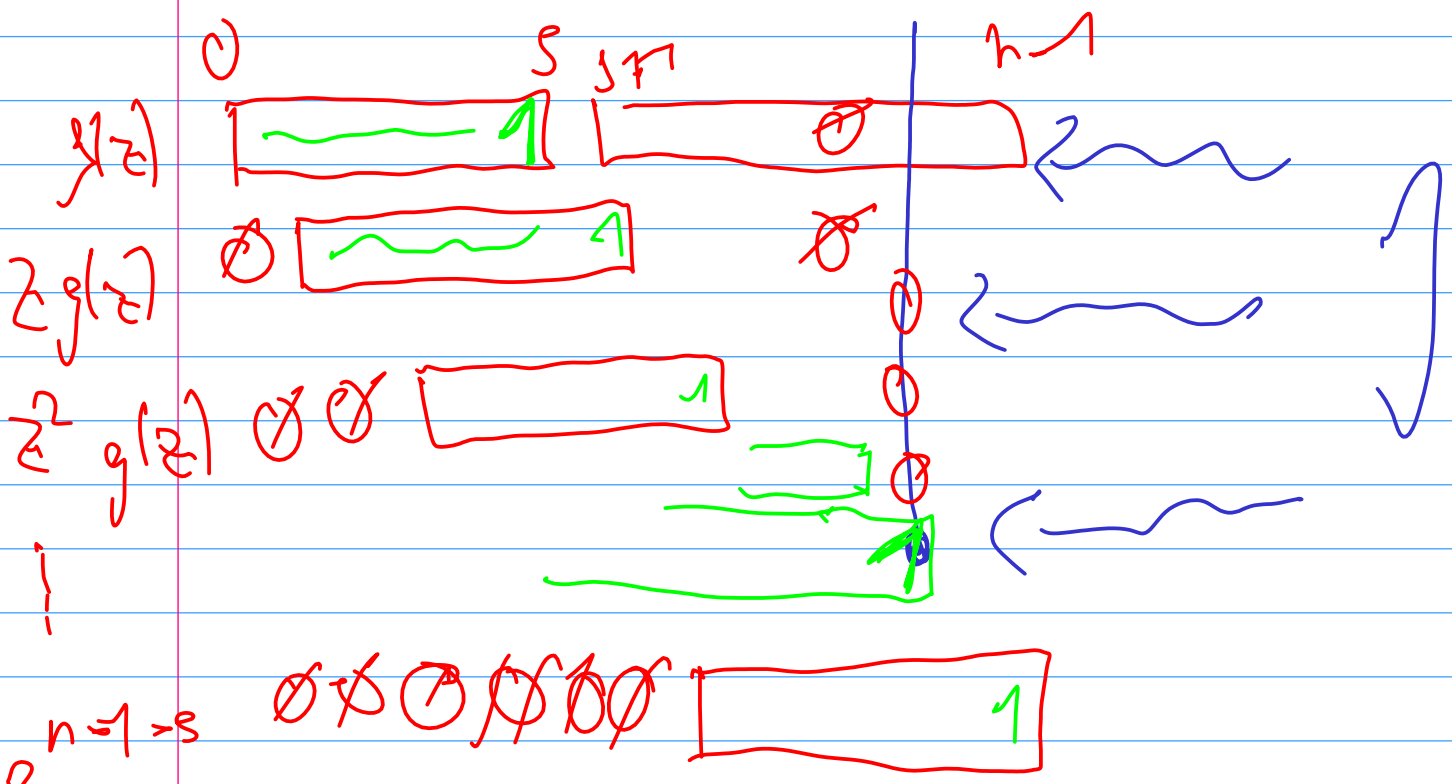
$\forall v \in C \; \exists a(z) : \; v(z) = a(z) \cdot g(z)$

stupeň $v \leq n-1$ ↑ stupeň g

$\Rightarrow$ st $a(z) \leq n-1-s$

$B = \{ g(z), z \cdot g(z), z^2 \cdot g(z), \dots, z^{n-1-s} \cdot g(z) \}$ $s \neq 0$, $s \neq 1$, $s \neq 2$

B generuje celý prostor C



pred jsou $b_0 \dots b_{n-1-s}$ jsou LN

jinak $\sum_{i \in I} \alpha_i b_i = (0, 0, \dots, 0)$

max index I s $\alpha_i \neq 1$

ale pak na pozici $s+I$ je v kombinaci

$\sum \alpha_i b_i$ jednička ↯

D je báze C

$\dim C = k$

$n - s = k \Leftrightarrow \boxed{s = n - k}$

(Př3) $g(x)$ dělí $x^n - 1$

Vydělíme

$x^n - 1 = a(x) \cdot g(x) + r(x)$

$\boxed{st\ r < s}$

v $\mathbb{Z}_2[x]$

rovnost v $\mathbb{Z}_2[x]/x^n - 1$

$0 \equiv a(z) \cdot g(z) + r(z)$

$r(z) = -a(z) \cdot g(z) \in C$

$r(z) \in C$ menší stupeň než s

$$h(x) := \frac{x^n - 1}{g(x)}$$

polynomium se zvlášť
$g(x)$ generující } polynom C
$h(x)$ kontrolní