

# Samoopravné kódy

Alexandr Kazda

Univerzita Karlova

12. května 2020

# Cyklické kódy – co bylo

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- V okruhu  $R = \mathbb{F}_q[x]/(x^n - 1)$  jsou to hlavní ideály
- Kódová slova  $\equiv$  polynomy; konstantní člen vlevo
- Generující polynom  $\beta$  je NSD všech kódových slov v  $\mathbb{F}_q[x]$
- $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- V okruhu  $R = \mathbb{F}_q[x]/(x^n - 1)$  jsou to hlavní ideály
- Kódová slova  $\equiv$  polynomy; konstantní člen vlevo
- Generující polynom  $\beta$  je NSD všech kódových slov v  $\mathbb{F}_q[x]$
- $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- V okruhu  $R = \mathbb{F}_q[x]/(x^n - 1)$  jsou to hlavní ideály
- Kódová slova  $\equiv$  polynomy; konstantní člen vlevo
- Generující polynom  $\beta$  je NSD všech kódových slov v  $\mathbb{F}_q[x]$
- $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- V okruhu  $R = \mathbb{F}_q[x]/(x^n - 1)$  jsou to hlavní ideály
- Kódová slova  $\equiv$  polynomy; konstantní člen vlevo
- Generující polynom  $\beta$  je NSD všech kódových slov v  $\mathbb{F}_q[x]$
- $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- V okruhu  $R = \mathbb{F}_q[x]/(x^n - 1)$  jsou to hlavní ideály
- Kódová slova  $\equiv$  polynomy; konstantní člen vlevo
- Generující polynom  $\beta$  je NSD všech kódových slov v  $\mathbb{F}_q[x]$
- $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód

- Lineární kódy nad  $\mathbb{F}_q$  uzavřené na cyklické posuny
- V okruhu  $R = \mathbb{F}_q[x]/(x^n - 1)$  jsou to hlavní ideály
- Kódová slova  $\equiv$  polynomy; konstantní člen vlevo
- Generující polynom  $\beta$  je NSD všech kódových slov v  $\mathbb{F}_q[x]$
- $\beta \mid x^n - 1$  v  $\mathbb{F}_q[x]$  pro nenulový kód

# Generující matice

- Buď  $\beta = b_0 + b_1x + \dots + b_kx^k$  pro  $k < n$ .
- Víme  $C = \{\beta \cdot r : r \in \mathbb{F}_q[x], \deg r \leq n - k - 1\}$
- Volme

$$M = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{k-2} & b_{k-1} & b_k & 0 & \cdots & 0 \\ & & & \ddots & & & & & & \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k \end{pmatrix}$$

- Řádky jsou kódová slova  $\beta, x\beta, x^2\beta, \dots, x^{n-k-1}\beta$
- Řádky lineárně generují  $C$
- Řádky jsou LN (je jich  $n - k$ )



# Generující matice

- Buď  $\beta = b_0 + b_1x + \dots + b_kx^k$  pro  $k < n$ .
- Víme  $C = \{\beta \cdot r : r \in \mathbb{F}_q[x], \deg r \leq n - k - 1\}$
- Volme

$$M = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{k-2} & b_{k-1} & b_k & 0 & \cdots & 0 \\ & & & \ddots & & & & & & \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k \end{pmatrix}$$

- Řádky jsou kódová slova  $\beta, x\beta, x^2\beta, \dots, x^{n-k-1}\beta$
- Řádky lineárně generují  $C$
- Řádky jsou LN (je jich  $n - k$ )

# Generující matice

- Bud'  $\beta = b_0 + b_1x + \dots + b_kx^k$  pro  $k < n$ .
- Víme  $C = \{\beta \cdot r : r \in \mathbb{F}_q[x], \deg r \leq n - k - 1\}$
- Volme

$$M = \begin{pmatrix} b_0 & b_1 & b_2 & \dots & b_{k-1} & b_k & 0 & 0 & \dots & 0 \\ 0 & b_0 & b_1 & \dots & b_{k-2} & b_{k-1} & b_k & 0 & \dots & 0 \\ & & & \ddots & & & & & & \\ 0 & 0 & \dots & 0 & b_0 & b_1 & b_2 & \dots & b_{k-1} & b_k \end{pmatrix}$$

- Řádky jsou kódová slova  $\beta, x\beta, x^2\beta, \dots, x^{n-k-1}\beta$
- Řádky lineárně generují  $C$
- Řádky jsou LN (je jich  $n - k$ )

# Generující matice

- Buď  $\beta = b_0 + b_1x + \dots + b_kx^k$  pro  $k < n$ .
- Víme  $C = \{\beta \cdot r : r \in \mathbb{F}_q[x], \deg r \leq n - k - 1\}$
- Volme

$$M = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{k-2} & b_{k-1} & b_k & 0 & \cdots & 0 \\ & & & \ddots & & & & & & \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k \end{pmatrix}$$

- Řádky jsou kódová slova  $\beta, x\beta, x^2\beta, \dots, x^{n-k-1}\beta$
- Řádky lineárně generují  $C$
- Řádky jsou LN (je jich  $n - k$ )

# Generující matice

- Buď  $\beta = b_0 + b_1x + \dots + b_kx^k$  pro  $k < n$ .
- Víme  $C = \{\beta \cdot r : r \in \mathbb{F}_q[x], \deg r \leq n - k - 1\}$
- Volme

$$M = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{k-2} & b_{k-1} & b_k & 0 & \cdots & 0 \\ & & & \ddots & & & & & & \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k \end{pmatrix}$$

- Řádky jsou kódová slova  $\beta, x\beta, x^2\beta, \dots, x^{n-k-1}\beta$
- Řádky lineárně generují  $C$
- Řádky jsou LN (je jich  $n - k$ )

# Generující matice

- Buď  $\beta = b_0 + b_1x + \dots + b_kx^k$  pro  $k < n$ .
- Víme  $C = \{\beta \cdot r : r \in \mathbb{F}_q[x], \deg r \leq n - k - 1\}$
- Volme

$$M = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{k-2} & b_{k-1} & b_k & 0 & \cdots & 0 \\ & & & \ddots & & & & & & \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k \end{pmatrix}$$

- Řádky jsou kódová slova  $\beta, x\beta, x^2\beta, \dots, x^{n-k-1}\beta$
- Řádky lineárně generují  $C$
- Řádky jsou LN (je jich  $n - k$ )

# Generující matice

- Buď  $\beta = b_0 + b_1x + \dots + b_kx^k$  pro  $k < n$ .
- Víme  $C = \{\beta \cdot r : r \in \mathbb{F}_q[x], \deg r \leq n - k - 1\}$
- Volme

$$M = \begin{pmatrix} b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k & 0 & 0 & \cdots & 0 \\ 0 & b_0 & b_1 & \cdots & b_{k-2} & b_{k-1} & b_k & 0 & \cdots & 0 \\ & & & \ddots & & & & & & \\ 0 & 0 & \cdots & 0 & b_0 & b_1 & b_2 & \cdots & b_{k-1} & b_k \end{pmatrix}$$

- Řádky jsou kódová slova  $\beta, x\beta, x^2\beta, \dots, x^{n-k-1}\beta$
- Řádky lineárně generují  $C$
- Řádky jsou LN (je jich  $n - k$ )

# Paritní matice

- Předpoklad  $1 \leq k \leq n - 1$
- Volme  $\delta = (x^n - 1)/\beta$ ;

$$\delta = d_{n-k}x^{n-k} + d_{n-k-1}x^{n-k-1} + \dots + d_0$$

- Víme, že  $\sum_{i=0}^c d_{c-i}b_i$  je koeficient u  $x^c$  v  $\delta\beta = x^n - 1$  (tj. typicky 0)
- Návrh paritní matice

$$P = \begin{pmatrix} d_{n-k} & d_{n-k-1} & \cdots & d_1 & d_0 & 0 & 0 & \cdots & 0 \\ 0 & d_{n-k} & \cdots & d_2 & d_1 & d_0 & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_1 & d_0 \end{pmatrix}$$

- Dimenze řádkového prostoru  $k$  sedí ( $k + (n - k) = n$ ).

# Paritní matice

- Předpoklad  $1 \leq k \leq n - 1$
- Volme  $\delta = (x^n - 1)/\beta$ ;

$$\delta = d_{n-k}x^{n-k} + d_{n-k-1}x^{n-k-1} + \dots + d_0$$

- Víme, že  $\sum_{i=0}^c d_{c-i}b_i$  je koeficient u  $x^c$  v  $\delta\beta = x^n - 1$  (tj. typicky 0)
- Návrh paritní matice

$$P = \begin{pmatrix} d_{n-k} & d_{n-k-1} & \cdots & d_1 & d_0 & 0 & 0 & \cdots & 0 \\ 0 & d_{n-k} & \cdots & d_2 & d_1 & d_0 & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_1 & d_0 \end{pmatrix}$$

- Dimenze řádkového prostoru  $k$  sedí ( $k + (n - k) = n$ ).



# Paritní matice

- Předpoklad  $1 \leq k \leq n - 1$
- Volme  $\delta = (x^n - 1)/\beta$ ;

$$\delta = d_{n-k}x^{n-k} + d_{n-k-1}x^{n-k-1} + \dots + d_0$$

- Víme, že  $\sum_{i=0}^c d_{c-i}b_i$  je koeficient u  $x^c$  v  $\delta\beta = x^n - 1$  (tj. typicky 0)
- Návrh paritní matice

$$P = \begin{pmatrix} d_{n-k} & d_{n-k-1} & \cdots & d_1 & d_0 & 0 & 0 & \cdots & 0 \\ 0 & d_{n-k} & \cdots & d_2 & d_1 & d_0 & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_1 & d_0 \end{pmatrix}$$

- Dimenze řádkového prostoru  $k$  sedí ( $k + (n - k) = n$ ).

# Paritní matice

- Předpoklad  $1 \leq k \leq n - 1$
- Volme  $\delta = (x^n - 1)/\beta$ ;

$$\delta = d_{n-k}x^{n-k} + d_{n-k-1}x^{n-k-1} + \dots + d_0$$

- Víme, že  $\sum_{i=0}^c d_{c-i}b_i$  je koeficient u  $x^c$  v  $\delta\beta = x^n - 1$  (tj. typicky 0)
- Návrh paritní matice

$$P = \begin{pmatrix} d_{n-k} & d_{n-k-1} & \cdots & d_1 & d_0 & 0 & 0 & \cdots & 0 \\ 0 & d_{n-k} & \cdots & d_2 & d_1 & d_0 & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_1 & d_0 \end{pmatrix}$$

- Dimenze řádkového prostoru  $k$  sedí ( $k + (n - k) = n$ ).

# Paritní matice

- Předpoklad  $1 \leq k \leq n - 1$
- Volme  $\delta = (x^n - 1)/\beta$ ;

$$\delta = d_{n-k}x^{n-k} + d_{n-k-1}x^{n-k-1} + \dots + d_0$$

- Víme, že  $\sum_{i=0}^c d_{c-i}b_i$  je koeficient u  $x^c$  v  $\delta\beta = x^n - 1$  (tj. typicky 0)
- Návrh paritní matice

$$P = \begin{pmatrix} d_{n-k} & d_{n-k-1} & \cdots & d_1 & d_0 & 0 & 0 & \cdots & 0 \\ 0 & d_{n-k} & \cdots & d_2 & d_1 & d_0 & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_1 & d_0 \end{pmatrix}$$

- Dimenze řádkového prostoru  $k$  sedí ( $k + (n - k) = n$ ).

# Paritní matice

- Předpoklad  $1 \leq k \leq n - 1$
- Volme  $\delta = (x^n - 1)/\beta$ ;

$$\delta = d_{n-k}x^{n-k} + d_{n-k-1}x^{n-k-1} + \dots + d_0$$

- Víme, že  $\sum_{i=0}^c d_{c-i}b_i$  je koeficient u  $x^c$  v  $\delta\beta = x^n - 1$  (tj. typicky 0)
- Návrh paritní matice

$$P = \begin{pmatrix} d_{n-k} & d_{n-k-1} & \cdots & d_1 & d_0 & 0 & 0 & \cdots & 0 \\ 0 & d_{n-k} & \cdots & d_2 & d_1 & d_0 & 0 & \cdots & 0 \\ & & & \ddots & & & & & \\ 0 & \cdots & 0 & d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_1 & d_0 \end{pmatrix}$$

- Dimenze řádkového prostoru  $k$  sedí ( $k + (n - k) = n$ ).

- Bereme první řádek  $M$  a nějaký cyklický posun slova  $d_{n-k}d_{n-k-1}\cdots d_1d_00\cdots 0$ .
- Příklad 1: Posun o  $c \in \{0, 1, \dots, k-1\}$  doprava

$$\begin{array}{ccccccc} b_c & b_{c+1} & b_{c+2} & \cdots & b_{k-1} & & b_k \\ d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_{n-2k+c+1} & & d_{n-2k+c} \end{array}$$

- $\sum_{i=0}^{k-c} d_{n-k-i}b_{c+i}$  je koeficient u  $x^{n-k+c}$  v  $x^n - 1$ , tj. nula.

- Bereme první řádek  $M$  a nějaký cyklický posun slova  $d_{n-k}d_{n-k-1}\cdots d_1d_00\cdots 0$ .
- Příklad 1: Posun o  $c \in \{0, 1, \dots, k-1\}$  doprava

$$\begin{array}{ccccccc} b_c & b_{c+1} & b_{c+2} & \cdots & b_{k-1} & b_k \\ d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_{n-2k+c+1} & d_{n-2k+c} \end{array}$$

- $\sum_{i=0}^{k-c} d_{n-k-i}b_{c+i}$  je koeficient u  $x^{n-k+c}$  v  $x^n - 1$ , tj. nula.

- Bereme první řádek  $M$  a nějaký cyklický posun slova  $d_{n-k}d_{n-k-1}\cdots d_1d_00\cdots 0$ .
- Příklad 1: Posun o  $c \in \{0, 1, \dots, k-1\}$  doprava

$$\begin{array}{cccccc} b_c & b_{c+1} & b_{c+2} & \cdots & b_{k-1} & b_k \\ d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_{n-2k+c+1} & d_{n-2k+c} \end{array}$$

- $\sum_{i=0}^{k-c} d_{n-k-i}b_{c+i}$  je koeficient u  $x^{n-k+c}$  v  $x^n - 1$ , tj. nula.

- Bereme první řádek  $M$  a nějaký cyklický posun slova  $d_{n-k}d_{n-k-1}\cdots d_1d_00\cdots 0$ .
- Příklad 1: Posun o  $c \in \{0, 1, \dots, k-1\}$  doprava

$$\begin{array}{ccccccc} b_c & b_{c+1} & b_{c+2} & \cdots & b_{k-1} & b_k \\ d_{n-k} & d_{n-k-1} & d_{n-k-2} & \cdots & d_{n-2k+c+1} & d_{n-2k+c} \end{array}$$

- $\sum_{i=0}^{k-c} d_{n-k-i}b_{c+i}$  je koeficient u  $x^{n-k+c}$  v  $x^n - 1$ , tj. nula.



- Příklad 2: Posun o  $k$  doprava (cyklicky)

$$\begin{array}{cccccccc} b_0 & b_1 & \dots & b_{k-1} & b_k & 0 & 0 & \dots & 0 \\ d_0 & 0 & \dots & 0 & d_{n-k} & d_{n-k-1} & d_{n-k-2} & \dots & d_1 \end{array}$$

- $b_0 d_0 + b_k d_{n-k} = -1 + 1 = 0$

- Příklad 2: Posun o  $k$  doprava (cyklicky)

$$\begin{array}{cccccccc} b_0 & b_1 & \dots & b_{k-1} & b_k & 0 & 0 & \dots & 0 \\ d_0 & 0 & \dots & 0 & d_{n-k} & d_{n-k-1} & d_{n-k-2} & \dots & d_1 \end{array}$$

- $b_0 d_0 + b_k d_{n-k} = -1 + 1 = 0$

- Příklad 2: Posun o  $k$  doprava (cyklicky)

$$\begin{array}{cccccccccc} b_0 & b_1 & \dots & b_{k-1} & b_k & 0 & 0 & \dots & 0 \\ d_0 & 0 & \dots & 0 & d_{n-k} & d_{n-k-1} & d_{n-k-2} & \dots & d_1 \end{array}$$

- $b_0 d_0 + b_k d_{n-k} = -1 + 1 = 0$

- Příklad 3: Posun o  $c \in \{k+1, k+2, \dots, n-1\}$  doprava (cyklicky)

$$\begin{array}{cccccccccc} b_0 & b_1 & \dots & b_{c-k} & b_{c-k+1} & \dots & b_k & 0 & \dots \\ d_{c-k} & d_{c-k-1} & \dots & d_0 & 0 & \dots & 0 & \dots & d_{n-k} & \dots \end{array}$$

- $\sum_{i=0}^{k-c} d_{c-k-i} b_i$  je koeficient u  $x^{c-k}$  v  $x^n - 1$ , tj. nula.
- Tím jsme probrali všechny možná posunutí
- **Pozor**, slovo  $d_n, d_{n-1}, \dots, d_0$  je  $\delta$  **pozpátku**.

- Příklad 3: Posun o  $c \in \{k+1, k+2, \dots, n-1\}$  doprava (cyklicky)

$$\begin{array}{cccccccccc} b_0 & b_1 & \dots & b_{c-k} & b_{c-k+1} & \dots & b_k & 0 & \dots \\ d_{c-k} & d_{c-k-1} & \dots & d_0 & 0 & \dots & 0 & \dots & d_{n-k} & \dots \end{array}$$

- $\sum_{i=0}^{k-c} d_{c-k-i} b_i$  je koeficient u  $x^{c-k}$  v  $x^n - 1$ , tj. nula.
- Tím jsme probrali všechny možná posunutí
- **Pozor**, slovo  $d_n, d_{n-1}, \dots, d_0$  je  $\delta$  **pozpátku**.

- Příklad 3: Posun o  $c \in \{k+1, k+2, \dots, n-1\}$  doprava (cyklicky)

$$\begin{array}{cccccccccc} b_0 & b_1 & \dots & b_{c-k} & b_{c-k+1} & \dots & b_k & 0 & \dots \\ d_{c-k} & d_{c-k-1} & \dots & d_0 & 0 & \dots & 0 & \dots & d_{n-k} & \dots \end{array}$$

- $\sum_{i=0}^{k-c} d_{c-k-i} b_i$  je koeficient u  $x^{c-k}$  v  $x^n - 1$ , tj. nula.
- Tím jsme probrali všechny možná posunutí
- **Pozor**, slovo  $d_n, d_{n-1}, \dots, d_0$  je  $\delta$  **pozpátku**.

- Příklad 3: Posun o  $c \in \{k+1, k+2, \dots, n-1\}$  doprava (cyklicky)

$$\begin{array}{cccccccccc} b_0 & b_1 & \dots & b_{c-k} & b_{c-k+1} & \dots & b_k & 0 & \dots \\ d_{c-k} & d_{c-k-1} & \dots & d_0 & 0 & \dots & 0 & \dots & d_{n-k} & \dots \end{array}$$

- $\sum_{i=0}^{k-c} d_{c-k-i} b_i$  je koeficient u  $x^{c-k}$  v  $x^n - 1$ , tj. nula.
- Tím jsme probrali všechny možná posunutí
- Pozor, slovo  $d_n, d_{n-1}, \dots, d_0$  je  $\delta$  pozpátku.

- Příklad 3: Posun o  $c \in \{k+1, k+2, \dots, n-1\}$  doprava (cyklicky)

$$\begin{array}{cccccccccc} b_0 & b_1 & \dots & b_{c-k} & b_{c-k+1} & \dots & b_k & 0 & \dots \\ d_{c-k} & d_{c-k-1} & \dots & d_0 & 0 & \dots & 0 & \dots & d_{n-k} & \dots \end{array}$$

- $\sum_{i=0}^{k-c} d_{c-k-i} b_i$  je koeficient u  $x^{c-k}$  v  $x^n - 1$ , tj. nula.
- Tím jsme probrali všechny možná posunutí
- **Pozor**, slovo  $d_n, d_{n-1}, \dots, d_0$  je  $\delta$  **pozpátku**.



# Příklad: Paritní kód

- $n = 3$ , nad  $\mathbb{F}_2$ ,  $C = \{000, 011, 101, 110\}$ .
- Ze středy víme, že  $\beta = 1 + x$ , (stupeň)  $k = 1$
- Generující matice

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

- $\delta = (x^3 - 1)/(1 + x) = x^2 + x + 1$ , tedy

$$P = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

# Příklad: Paritní kód

- $n = 3$ , nad  $\mathbb{F}_2$ ,  $C = \{000, 011, 101, 110\}$ .
- Ze středy víme, že  $\beta = 1 + x$ , (stupeň)  $k = 1$
- Generující matice

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

- $\delta = (x^3 - 1)/(1 + x) = x^2 + x + 1$ , tedy

$$P = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

# Příklad: Paritní kód

- $n = 3$ , nad  $\mathbb{F}_2$ ,  $C = \{000, 011, 101, 110\}$ .
- Ze středy víme, že  $\beta = 1 + x$ , (stupeň)  $k = 1$
- Generující matice

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

- $\delta = (x^3 - 1)/(1 + x) = x^2 + x + 1$ , tedy

$$P = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

# Příklad: Paritní kód

- $n = 3$ , nad  $\mathbb{F}_2$ ,  $C = \{000, 011, 101, 110\}$ .
- Ze středy víme, že  $\beta = 1 + x$ , (stupeň)  $k = 1$
- Generující matice

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

- $\delta = (x^3 - 1)/(1 + x) = x^2 + x + 1$ , tedy

$$P = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

# Příklad: Paritní kód

- $n = 3$ , nad  $\mathbb{F}_2$ ,  $C = \{000, 011, 101, 110\}$ .
- Ze středy víme, že  $\beta = 1 + x$ , (stupeň)  $k = 1$
- Generující matice

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

- $\delta = (x^3 - 1)/(1 + x) = x^2 + x + 1$ , tedy

$$P = \begin{pmatrix} 1 & 1 & 1 \end{pmatrix}$$

# $H_3$ jako cyklický kód

- $n = 7$  nad  $\mathbb{F}_2$
- Je třeba přerovnat pořadí písmen
- Půjdeme na to přes paritní matici:

# $H_3$ jako cyklický kód

- $n = 7$  nad  $\mathbb{F}_2$
- Je třeba přerovnat pořadí písmen
- Půjdem na to přes paritní matici:

# $H_3$ jako cyklický kód

- $n = 7$  nad  $\mathbb{F}_2$
- Je třeba přerovnat pořadí písmen
- Půjdeme na to přes paritní matici:



# $H_3$ jako cyklický kód

- $n = 7$  nad  $\mathbb{F}_2$
- Je třeba přerovnat pořadí písmen
- Půjdeme na to přes paritní matici:

$$P = \begin{pmatrix} ? & ? & ? & ? & ? & 0 & 0 \\ 0 & ? & ? & ? & ? & ? & 0 \\ 0 & 0 & ? & ? & ? & ? & ? \end{pmatrix}$$

# $H_3$ jako cyklický kód

- $n = 7$  nad  $\mathbb{F}_2$
- Je třeba přerovnat pořadí písmen
- Půjdeme na to přes paritní matici:

$$P = \begin{pmatrix} 1 & ? & ? & ? & 1 & 0 & 0 \\ 0 & 1 & ? & ? & ? & 1 & 0 \\ 0 & 0 & 1 & ? & ? & ? & 1 \end{pmatrix}$$

# $H_3$ jako cyklický kód

- $n = 7$  nad  $\mathbb{F}_2$
- Je třeba přerovnat pořadí písmen
- Půjdeme na to přes paritní matici:

$$P = \begin{pmatrix} 1 & 0 & ? & ? & 1 & 0 & 0 \\ 0 & 1 & 0 & ? & ? & 1 & 0 \\ 0 & 0 & 1 & 0 & ? & ? & 1 \end{pmatrix}$$

# $H_3$ jako cyklický kód

- $n = 7$  nad  $\mathbb{F}_2$
- Je třeba přerovnat pořadí písmen
- Půjdeme na to přes paritní matici:

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

# $H_3$ jako cyklický kód

- $n = 7$  nad  $\mathbb{F}_2$
- Je třeba přerovnat pořadí písmen
- Půjdeme na to přes paritní matici:

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

- Vypadá to, že  $\delta = x^4 + x^2 + x + 1$

# $H_3$ jako cyklický kód

- $n = 7$  nad  $\mathbb{F}_2$
- Je třeba přerovnat pořadí písmen
- Půjdeme na to přes paritní matici:

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

- Vypadá to, že  $\delta = x^4 + x^2 + x + 1$
- Dopočteme  $\beta = (x^7 - 1)/(x^4 + x^2 + x + 1) = x^3 + x + 1$

# $H_3$ jako cyklický kód II

- Alternativní odvození: Projdeme všechny cyklické kódy s  $n = 7$  nad  $\mathbb{F}_2$
- Numerologie:  $\dim C = 4$ , tedy stupeň  $\beta = 7 - 4 = 3$
- Chceme  $\beta$  dělitele  $x^7 - 1$  stupně 3 v  $\mathbb{F}_2[x]$
- $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$ , tedy dvě možné  $\beta$
- $\beta = 1 + x + x^3$  i  $\beta = 1 + x^2 + x^3$  jsou ekvivalentní  $H_3$

# $H_3$ jako cyklický kód II

- Alternativní odvození: Projdeme všechny cyklické kódy s  $n = 7$  nad  $\mathbb{F}_2$
- Numerologie:  $\dim C = 4$ , tedy stupeň  $\beta = 7 - 4 = 3$
- Chceme  $\beta$  dělitele  $x^7 - 1$  stupně 3 v  $\mathbb{F}_2[x]$
- $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$ , tedy dvě možné  $\beta$
- $\beta = 1 + x + x^3$  i  $\beta = 1 + x^2 + x^3$  jsou ekvivalentní  $H_3$



# $H_3$ jako cyklický kód II

- Alternativní odvození: Projdeme všechny cyklické kódy s  $n = 7$  nad  $\mathbb{F}_2$
- Numerologie:  $\dim C = 4$ , tedy stupeň  $\beta = 7 - 4 = 3$
- Chceme  $\beta$  dělitele  $x^7 - 1$  stupně 3 v  $\mathbb{F}_2[x]$
- $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$ , tedy dvě možné  $\beta$
- $\beta = 1 + x + x^3$  i  $\beta = 1 + x^2 + x^3$  jsou ekvivalentní  $H_3$

# $H_3$ jako cyklický kód II

- Alternativní odvození: Projdeme všechny cyklické kódy s  $n = 7$  nad  $\mathbb{F}_2$
- Numerologie:  $\dim C = 4$ , tedy stupeň  $\beta = 7 - 4 = 3$
- Chceme  $\beta$  dělitele  $x^7 - 1$  stupně 3 v  $\mathbb{F}_2[x]$
- $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$ , tedy dvě možné  $\beta$
- $\beta = 1 + x + x^3$  i  $\beta = 1 + x^2 + x^3$  jsou ekvivalentní  $H_3$

# $H_3$ jako cyklický kód II

- Alternativní odvození: Projdeme všechny cyklické kódy s  $n = 7$  nad  $\mathbb{F}_2$
- Numerologie:  $\dim C = 4$ , tedy stupeň  $\beta = 7 - 4 = 3$
- Chceme  $\beta$  dělitele  $x^7 - 1$  stupně 3 v  $\mathbb{F}_2[x]$
- $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$ , tedy dvě možné  $\beta$
- $\beta = 1 + x + x^3$  i  $\beta = 1 + x^2 + x^3$  jsou ekvivalentní  $H_3$

# $H_3$ jako cyklický kód II

- Alternativní odvození: Projdeme všechny cyklické kódy s  $n = 7$  nad  $\mathbb{F}_2$
- Numerologie:  $\dim C = 4$ , tedy stupeň  $\beta = 7 - 4 = 3$
- Chceme  $\beta$  dělitele  $x^7 - 1$  stupně 3 v  $\mathbb{F}_2[x]$
- $x^7 - 1 = (1 + x)(1 + x + x^3)(1 + x^2 + x^3)$ , tedy dvě možné  $\beta$
- $\beta = 1 + x + x^3$  i  $\beta = 1 + x^2 + x^3$  jsou ekvivalentní  $H_3$

## Bonus: Kolik je cyklických kódů délky 3 nad $\mathbb{F}_2$ ?

- Str. 52 v učebnici
- Dělitelé  $x^3 - 1$  stupně  $< 3$  v  $\mathbb{F}_2$  nám dají různé kódy (mohou být ekvivalentní)
- $x^3 - 1 = (x + 1)(x^2 + x + 1)$ , tedy dělitelé  $\beta = 1$ ,  $\beta = x + 1$ ,  
 $\beta = x^2 + x + 1$
- Totální kód, paritní kód, opakovací kód
- Nesmíme zapomenout kód  $\{000\}$