BCH kódy pro $\leq t$ chyb

d = min vzdálenost mezi slovy v $\mathcal{C}$

$d = 2t+1$

def:
BCH bin. kód délky n (liché) s plánovanou vzdáleností d

$\Leftrightarrow$

- cyklický kód nad $\mathbb{Z}_2[x]/q(x)$ q ireducibilní

s generujícími kořeny $\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{d-1}, \alpha^d$

kde α je generátor cyklické grupy $(\mathbb{Z}_2[x]/q(x)) \setminus \{0\}$

Pozn: 1) když α^i je kořen $\rightsquigarrow$ α^{2i} je kořen

stačí uvažovat jen liché mocniny α

2) BCH(d) pro d sudé a BCH(d+1) mají stejný generující polynom

BÚNO d liché

Věta: Pro BCH(d) kód platí, že min vzdálenost mezi kód. slovy je $\geq d$

Stačí ukázat, pro kontrolní matici H platí že liboli $(d-1)$ sloupců je LN

$$\widetilde{H} = \begin{pmatrix} 1 & \alpha^1 & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^3 & \alpha^6 & \cdots & \alpha^{3(n-1)} \\ 1 & \alpha^5 & \alpha^{10} & \cdots & \alpha^{5(n-1)} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \alpha^{d-2} & \alpha^{2(d-2)} & \cdots & \alpha^{(d-2)(n-1)} \end{pmatrix}$$

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & & \alpha^{2(n-1)} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & & \alpha^{3(n-1)} \\ 1 & \vdots & & & & \\ 1 & & & & & \\ 1 & & & & & \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & & & \alpha^{(d-1)(n-1)} \end{pmatrix}$$

$w \in C \iff Hw = \emptyset$

PŘ.: každých $(d-1)$ sloupců je LN $\iff$ $\det[\text{sloupce}] \neq 0$

Nejme $\rho = \{i_1, i_2, \dots, i_{d-1}\}$

$$H_\rho := \left[H_{i_1} \mid H_{i_2} \mid \cdots \mid H_{i_{d-1}} \right]$$

$$= \begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{d-1}} \\ (\alpha^{i_1})^2 & \alpha^{2i_2} & & \alpha^{2i_{d-1}} \\ (\alpha^{i_1})^3 & \alpha^{3i_2} & & \vdots \\ \vdots & \vdots & & \\ (\alpha^{i_1})^{d-1} & \alpha^{(d-1)i_2} & & \alpha^{(d-1)i_{d-1}} \end{pmatrix}$$

Vandermondova matice $a_1 \dots a_d$

$$V(a_1 \dots a_d) := \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & a_4 & \dots & a_d \\ a_1^2 & a_2^2 & a_3^2 & a_4^2 & \dots & a_d^2 \\ \vdots & & & & & \\ a_1^{d-1} & a_2^{d-1} & a_3^{d-1} & a_4^{d-1} & \dots & a_d^{d-1} \end{pmatrix}$$

$$v(a_1 \dots a_d) := \det V(a_1 \dots a_d)$$

Tvrzení: $v(a_1 \dots a_d) = \prod_{d \geq j > i \geq 1} (a_j - a_i)$

Chceme Tvrzení na

$$\begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & & & & & \\ 1 & & & & & \\ 1 & & & H_p & & \\ 1 & & & & & \end{pmatrix}$$

$v(1, \alpha^{i_1}, \alpha^{i_2}, \alpha^{i_3} \dots \alpha^{i_{d-1}})$ — navzájem různé

protože α je generátor cyklické grupy

Tvrzení $\rightsquigarrow 0 \neq \det \begin{bmatrix} 1 & 1 & \dots & 1 \\ 1 & & & \\ \vdots & & H_p & \\ 1 & & & \end{bmatrix} = \det[H_p]$

Dk (Torzen'): ihned z (d-1)-kvalit následující lemma

Lemma: $v(a_1, \dots, a_d) = v(a_1, \dots, a_{d-1}) \cdot \prod_{i=1}^{d-1} (a_d - a_i)$

Dk (Lemma): uvažme $v(a_1, a_2, \dots a_{d-1}, t) =: f(t)$

t proměnná

$a_1 \dots a_{d-1}$ pevné parametry

$$f(t) = \det \begin{pmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ a_1 & a_2 & a_3 & & a_{d-1} & t \\ a_1^2 & a_2^2 & a_3^2 & & (a_{d-1})^2 & t^2 \\ \vdots & & & & & t^3 \\ a_1^{d-1} & & & & & t^{d-1} \end{pmatrix}$$

rozvoj dle d-tého sloupce

"poly(t)" $= \sum_{i=0}^{d-1} t^i \cdot \det$ — nezávisí na t

1) $\deg f(t) = d-1$

2) $f(t) = \sum_{i=0}^{d-1} c_i t^i$ $\quad c_{d-1} = v(a_1, \dots, a_{d-1})$

3) $t \to a_i \quad \forall i \in \{1, \dots d-1\} \quad f(a_i) = 0$

$$f(t) = M \times \prod_{i=1}^{d-1} (t - a_i) = v(a_1, \dots a_{d-1}) \cdot \prod_{i=1}^{d-1} (t - a_i)$$

$$f(a_d) = v(a_1, \dots a_{d-1}) \prod_{i=1}^{d-1} (a_d - a_i)$$

ZÁVĚR: $BCH(d)$ ~> kód s vzdál. mezi kód. slovy $\geq d$

Jak v praxi dekódovat $BCH(d)$?

mějme $d = 2t+1$.

$v \in \mathbb{C}$ —(e chyba)→ w

NASTALO $p \leq t$ chyb

$e = (\emptyset \; e_{i_1} \; \emptyset \; e_{i_2} \; \emptyset \; e_{i_p} \; \emptyset)$

$e_{i_1} = 1, \; e_{i_2} = 1, \; e_{i_p} = 1$

$$e(z) = \sum_{j=1}^{p} z^{i_j}$$

~> $w(z) = v(z) + e(z)$

$H \cdot w(x) = H \cdot e(x) = \text{syndrom}$

$\| \qquad \| \qquad \|$

$0 \qquad \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_{d-1} \end{pmatrix}$

$$\begin{pmatrix} 1 & \alpha & \alpha^2 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \alpha^{2n-2} \\ \vdots & & & & \\ 1 & \alpha^{d-1} & \alpha^{2(d-1)} & \cdots & \alpha^{(d-1)(n-1)} \end{pmatrix} \begin{pmatrix} \vdots \\ 1 \\ \vdots \\ 1 \\ \vdots \\ 1 \\ \vdots \end{matrix} \begin{matrix} i_1 \\ i_2 \\ \\ \\ i_p \end{matrix} = \begin{pmatrix} S_1 \\ S_2 \\ \\ S_{d-1} \end{pmatrix}$$

$$S_1 = \alpha^{i_1} + \alpha^{i_2} + \alpha^{i_3} + \cdots + \alpha^{i_p}$$

$$S_2 = \alpha^{2i_1} + \alpha^{2i_2} + \cdots + \alpha^{2i_p}$$

$$S_k = \sum_{j=1}^{p} (\alpha^{i_j})^k = \sum \alpha^{k \cdot i_j}$$

Def: $\alpha^{j} =: \boxed{a_j}$ $\quad j \in \{1, \dots, p\}$

Ciel: $\exists$ $s_1 \dots s_{d-1}$ unerit $a_1 \dots a_p$

Def: $f(x) = (1 - \boxed{a_1} x)(1 - \boxed{a_2} x) \cdots (1 - \boxed{a_p} x)$

Lokation ... e

Probl: having $f(x)$ = inverse a_j

$$s_k = \sum_{j=1}^{p} a_j^{k}$$

$$f(x) = 1 + f_1 x + f_2 x^2 + \dots + f_p x^p$$

$$f_1 =: -\sum_{j=1}^{p} a_j = \sum a_j$$

Obecně

$$f'(x) = \underbrace{f_1 + 2f_2 x + 3f_3 x^2 + \cdots + p f_p x^{p-1}}$$

$$= -\frac{q_1}{(1-q_1 x)} f(x) - \frac{q_2}{(1-q_2 x)} \cdot f(x) - \cdots$$

$$\rightsquigarrow$$

$$\frac{f'(x)}{f(x)} = -\sum_{j=1}^{p} \boxed{\frac{q_j}{1-q_j x}}$$

$$\| \quad \infty$$

$$\frac{1}{x} \sum_{y=1} (q_1 x)^y + \frac{1}{x} \sum_{y=1}^{\infty} (q_2 x)^y + \cdots$$

$$\| \quad \infty$$

$$\frac{1}{x} \sum_{y=1} q_1^y x^y + q_2^y x^y + \cdots q_p^y x^y$$

$$= \sum_{y=1} \left(q_1^y + \cdots q_p^y\right) x^{y-1}$$

$y=1 : s_1$

$y=2 : s_2$

$y=d-1 : s_{d-1}$

$$\left(\sum_{\text{all } a_1^{y_1}\cdots a_p^{y_p}} x^{y-1}\right) \cdot \left(1+\sum_{i=1}^{p} f_i \cdot x^i\right)$$

$$f_1 x^0 + f_2 x^2 + f_3 x^4 + \cdots$$

$$f_1 = \sum a_j = s_1$$

$$f_3 = s_3 + s_2 \cdot f_1 + s_1 \cdot f_2$$

$$f_4 = s_4 + s_3 f_1 + s_2 f_2 + s_1 f_3 + s_1 f_1$$

$$\begin{pmatrix} s_1 \\ \\ s_{p-1} \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ s_2 & 1 & & & & & \\ s_3 & s_2 & 1 & & & & \\ s_4 & s_3 & s_2 & 1 & & & \\ & \ddots & & & & & \\ s_{2p-1} & \cdots & & & & & s_{p-1} \end{pmatrix} \begin{pmatrix} f_1 \\ \\ f_p \end{pmatrix}$$

M_p

Věta: $\forall r \in \{1, \dots, t+1\}$ a nastelý počet chyb $\leq r$

$\det M_p = 0 \quad p \geq r+2$

$\det M_{r+1} \neq \emptyset$

$\det M_r \neq \emptyset$

$\rightsquigarrow$ Pokud $\det M_{t+2} \neq 0 \rightsquigarrow t+1$ chyb

jinak najdi r větší, spočítej M_p

a vrať $(f_1, \dots, f_r) \rightsquigarrow$ koeficienty $f(x)$

nejsou inverze k $q_1, \dots, q_r$