BCH kódy

Bose, Chaudhuri, Hocquenghem

$V \overset{BH}{\rightsquigarrow} W \xrightarrow{\text{jum}} \widetilde{W} \overset{Dc}{\rightsquigarrow} W/V$

1) cyklický kód, nad $\underbrace{\mathbb{Z}_2[x]/q(x)}_{2^m\text{-prvkové těleso}}$, $q(x)$ je ivr. polynom stupně m

Př: $n = 15 = 2^4 - 1$, $m = 4 \rightsquigarrow q(x) = x^4 + x + 1$

$$\underbrace{\mathbb{Z}_2[x]/q(x)}_{T_q} = \{a_0 + a_1 z + a_2 z^2 + a_3 z^3 ; a_0, a_1, a_2, a_3 \in \mathbb{Z}_2\}$$

víme, že $T_q \setminus \{0\}$ je cyklická, tudíž $\exists\, \alpha \in T_q \setminus \{0\}$

$$T_q \setminus \{0\} = \{\alpha, \alpha^2, \alpha^3, \ldots, \alpha^{15} = 1\}$$

Pro naši dvojici q, $\alpha = z$

$\alpha^0 = z^0 = z^{15} = 1$ | $z^4 = z + 1$ | $z^8 = 1 + z^2$ | $z^{12} = 1 + z + z^2 + z^3$

$\alpha^1 = z^1 = z$ | $z^5 = z + z^2$ | $z^9 = z + z^3$ | $z^{13} = 1 + z^2 + z^3$

$\alpha^2 = z^2 = z^2$ | $z^6 = z^2 + z^3$ | $z^{10} = 1 + z + z^2$ | $z^{14} = 1 + z^3$

$\alpha^3 = z^3 = z^3$ | $z^7 = 1 + z + z^3$ | $z^{11} = z + z^2 + z^3$

min. polynomy : $P_{z^0}(x) = x+1$

$P_{z^2}(x) = P_{z^4}(x) = x^4+x+1$

$P_{z^3}(x) = x^4+x^3+x^2+x+1$

⋮

Vezmeme kód s generujícími kořeny α_z, α_z^{11}

$\rightsquigarrow$ generující polynom

$$g(x) = (x^4+x+1)(x^4+x^3+x^2+x+1)$$

$\deg g = 8 \iff$ dim kódu je 7

Pozn.: $v(x) = \sum_{i=0}^{14} v_i x^i$ polynom st ≤ 14 odpovídá kód. slovu $v_0 v_1 \dots v_{14} \in \mathbb{Z}_2^{15}$

$\Updownarrow$

$v(\alpha) = \sum v_i \alpha^i = \sum_{i=0}^{14} v_i z^i = 0 \iff$ 4 rovnicím mezi koef. v

$v(\alpha^3) = \sum v_i \alpha^{3i} = \sum_{i=0}^{14} v_i z^{3i} = 0 \iff$ 4 rovnicím mezi koef. v

prvky $T_q \longleftrightarrow$ polynomy st ≤ 3 s koef. z $\mathbb{Z}_2$

$\updownarrow$

$(a_0, a_1, a_2, a_3) \in \mathbb{Z}_2^4$

Kontrolní matice H

$$\alpha^i \rightsquigarrow (e_1, e_2, e_3, e_4) \in \mathbb{Z}_2^4$$

$$H = \begin{pmatrix} H_1 \in \mathbb{Z}_2^{4\times 15} \\ H_2 \in \mathbb{Z}_2^{4\times 15} \end{pmatrix} \in \mathbb{Z}_2^{8\times 15}$$

$$H_1 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{ccccccccc} \alpha^0 & \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 & \alpha^6 & \alpha^7 & \cdots \alpha^{14} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 0 & \cdots \\ 0 & 1 & 0 & 0 & 1 & 1 & 0 & \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 & \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & \end{pmatrix} \end{array}$$

$$H_2 = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ 4 \end{array} \begin{array}{c} \begin{array}{cccc} \alpha^{0\cdot 3} & \alpha^{1\cdot 3} & \alpha^{2\cdot 3} & \alpha^{3\cdot 3} \end{array} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

$v \overset{\text{BCH}}{\rightsquigarrow} w$ ŠUM $\tilde{w}$ LEŤ NEŽ TAD $\rightsquigarrow w$

Předpokládejme nastaly 2 chyby na pozicích $i \neq j$ $\hookrightarrow$ $\tilde{w} = w + \alpha^i + \alpha^j$
$= w + z^i + e^j$

$$H \cdot \tilde{w} = \begin{pmatrix} \tilde{w}(\alpha) \\ \tilde{w}(\alpha^3) \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \end{pmatrix} = \begin{pmatrix} \alpha^i + \alpha^j \\ \alpha^{3i} + \alpha^{3j} \end{pmatrix}$$

$$S_1^3 = \underbrace{\alpha^{3i} + \alpha^{3j}}_{S_2} + \underbrace{\alpha^{2i+j} + \alpha^{2j+i}}_{\alpha^{i+j} S_1}$$

$$\alpha^{i+j} = (S_1)^2 + (S_1)^{-1} S_2$$

kvadratická rovnice $\leftrightarrow$ UMÍME DOBŘE

$$(\lambda + \alpha^i)(\lambda + \alpha^j)$$

$$\lambda^2 + \underbrace{(\alpha^i + \alpha^j)}_{\parallel} \lambda + \alpha^{i+j} = \lambda^2 + S_1 \lambda + S_1^2 + S_2 \cdot S_1^{-1}$$

Obecně, jak dekódovat:

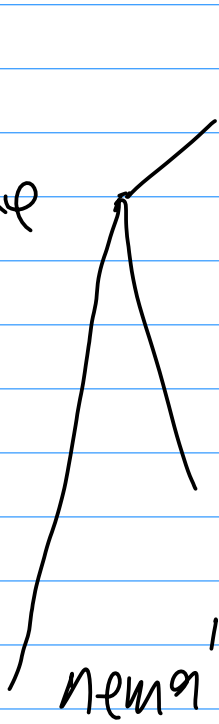
1) spočteme syndrom $\begin{pmatrix} s_1 \\ s_2 \end{pmatrix} = \begin{pmatrix} \widetilde{w}(\alpha) \\ \widetilde{w}(\alpha^3) \end{pmatrix}$

2) pokud $s_1 = s_2 = 0$ $\quad w := \widetilde{w}$

3) jinak a nejsme kodany $\quad \lambda^2 + s_1\lambda + s_1^2 + s_2 s_1$

$s_1 \neq 0$

vyřešíme



nemá řešení $\rightsquigarrow$ >2 chyby

$w := \emptyset$

Věta (Davenport 1968): Těleso $GF(p^m)$

existuje $\beta \in GF(p^m)$ t.ž.

$B := \{\beta^0, \beta^1, \beta^2, \dots \beta^{m-1}\}$ je

báze vektorového prostoru $GF(p^m)$ nad $\mathbb{Z}_p$

Normální báze $GF(p^m)$

Def: Pro $\alpha \in GF(p^m)$ t.ž. $\alpha = \sum_{i=0}^{m-1} \alpha_i \beta^{p^i}$

definujeme stopu

$$tr(\alpha, B) = \sum_{i=0}^{m-1} \alpha_i$$

$\alpha_i \in \mathbb{Z}_p$

Př.: $\mathbb{Z}_2[x]/q(x)$ kde $q = x^4 + x + 1$

$\beta = z^3$ $\beta^2 = z^2 + z^3$ $\beta^4 = z = 1 + z + z^2 + z^3$

$\beta^8 = z + z^3$

B prob 7 D. věty $\rightsquigarrow \begin{pmatrix} 0&0&1&0 \\ 0&0&1&1 \\ 0&1&1&0 \\ 1&1&1&1 \end{pmatrix}$ má hodnost 4

Věta: $GF(2^m)$ s normální bazí $\beta, \beta^2, \beta^{2^2}, \dots, \beta^{2^{m-1}}$.

Potom $\underbrace{\mu^2 + \mu = 0}_{c_0} \leftrightsquigarrow \mu^2 = \mu$

$c_0 = 1$, $c_1 = 1$, $c_{m-1} = 1$

má řešení $\mu = d_1\beta + d_2\beta^2 + d_3\beta^{2^2} + \dots + d_0\beta^{2^{m-1}}$

kde $d = d_0\beta^{2^0} + d_1\beta^{2^1} + d_2\beta^{2^2} + \dots + d_{m-1}\beta^{2^{m-1}}$

$\forall i: d_i \in \{0,1\}$, speciálně $d_i^2 = d_i$

$$\mu^2 = \left(\sum c_i \beta^{2^i}\right)\left(\sum c_j \beta^{2^j}\right)$$

$$\sum_{i=0}^{m-1} c_i^2 \left(\beta^{2^i}\right)^2 = \sum c_i \beta^{2^{i+1}}$$

$$= \sum_{i=0}^{m-2} d_{i+1}\beta^{2^{i+1}} + d_0 \underbrace{\beta^{2^m}}_{=\beta}$$

$$= d$$

Věta: $GF(2^m)$ s normální bazí $B = \beta, \beta^2, \beta^{2^2}, \dots, \beta^{2^{m-1}}$.

Potom $\mu^2 + \mu + \alpha = 0$ má řešení právě tehdy když $Tr(\alpha, B) = 0$. Pokud má řešení:

$$\mu^{(1)} = 1\cdot\beta^{2^0} + (\alpha_1+1)\beta^{2^1} + (\alpha_2+\alpha_1+1)\beta^{2^2} + \dots + \left(\sum_{i=1}^{m-1}\alpha_i + 1\right)\beta^{2^{m-1}}$$

$$\mu^{(0)} = 0\cdot\beta^{2^0} + (\alpha_1+0)\beta^{2^1} + (\alpha_2+\alpha_1+0)\beta^{2^2} + \dots + \left(\sum_{i=1}^{m-1}\alpha_i\right)\beta^{2^{m-1}}$$

$$= \alpha_1\beta^{2^1} + (\alpha_2+\alpha_1)\beta^{2^2} + \dots + \left(\sum_{i=1}^{m-1}\alpha_i\right)\beta^{2^{m-1}}$$

$\Rightarrow$

Dk: nechť $\bar{\mu}$ je řešením

$$\bar{\mu} = \sum_{i=0}^{m-1} c_i \beta^{2^i} \qquad \bar{\mu}^2 = \sum_{i=0}^{m-1} c_i \beta^{2^{i+1}}$$

$$Tr(\bar{\mu} + \bar{\mu}^2) = 2\sum c_i = 0$$

$$Tr(\alpha)$$

$\Leftarrow$

$$Tr(\alpha) = 0 \iff \alpha_0 = \sum_{i=1}^{m-1}\alpha_i$$

	λ^0	λ^1	λ^2	λ^3	...	λ^{n-1}
$[\mu^{(0)}]^2$	$\sum_{i=1}^{m} d_i + d_0$	$\emptyset$	d_1	d_1+d_2	...	$\sum_{i=1}^{m-2} d_i$
$\mu^{(0)}$	$\emptyset$	d_1	d_1+d_2	$d_1+d_2+d_3$	...	$\sum_{i=1}^{m-1} d_i$
d	d_0	d_1	d_2	d_3	...	d_{n-1}
Σ	$=\emptyset$	$\emptyset$	$\emptyset$	$\emptyset$	...	$\emptyset$

$$(\mu^{(0)})^2 + \mu^{(d)} + d = \emptyset$$

$\mu^{(n)}$ analogicky

$$a\lambda^2 + b\lambda + c = 0 \qquad a \neq 0,\ b \neq 0$$

$$\Updownarrow \quad \lambda = (b \cdot a^{-1}) \cdot \mu$$

$$\boxed{\mu^2 + \mu + c(b^{-1})^2 = 0}$$

ZÁVĚR: kvadratické rovnice v $\mathbb{Z}_2[x]/q(x)$ se řeší

snadno