Kódoláselmélet 2020 november 25.

Bizonyítás (BCH-kódok tétele)

(3) dimenzió $n-\deg(g)$ minden ciklikus kódban

$$G=\begin{pmatrix} g \\ xg \\ x^2g \\ \vdots \\ x^{k-1}g \end{pmatrix} = \underbrace{\begin{pmatrix} \boxed{\quad g \quad} & 0\dots0 & \\ 0 & \boxed{\quad g \quad} & 0\dots0 \\ 00 & \boxed{\quad g \quad} & \\ & & \\ 0\dots\dots0 & & \boxed{\quad g \quad} \end{pmatrix}}_{n \text{ hosszú}}$$

k = kód dimenziója

Példa $n=4$ $g=1+2x\in\mathbb{Z}_3[x]$

$$G=\begin{pmatrix} \boxed{1\ 2} & 0 & 0 \\ 0 & \boxed{1\ 2} & 0 \\ 0 & 0 & \boxed{1\ 2} \end{pmatrix} \qquad \dim = 4-\deg(g).$$

kérdés $n-\deg(g) \overset{?}{\geq} n-r(d-1)$

$$\deg(g) \leq r(d-1)$$

$$\deg(g_i) \overset{?}{\leq} r \qquad g_i \text{ az } \alpha^i \text{ min polinomja.}$$

tetszőleges elem min polinomja $K[x]$-ben
$\beta\in K[x]/\langle f\rangle$
legfeljebb r-ed fokú lehet

$\underbrace{\beta^0, \beta^1, \beta^2, \dots, \beta^r}$ $r+1$ vektor a $K[x]/\langle f\rangle$ K-feletti vektorterében, r-dim.

ezek nemtriv lin komb. már 0 akkor $\deg(\min_\beta)\leq r$

∎

(4) elég megmutatni, hogy $g \mid x^n - 1$-et

x^n-1 polinomnak az α gyöke
mert $o(\alpha) = n$ $\alpha^n = 1$
ugyan így $\alpha^2, \alpha^3, \dots, \alpha^{d-1}$ is
gyöke.

x^n-1 többszöröse $g_1, g_2, \dots, g_{d-1}$
minimál polinomoknak

x^n-1 többszöröse ezek lkkt-jének.

Lemma: Ha $g \mid x^n - 1 \in K[x]$, akkor a

$$G = \begin{pmatrix} g \\ xg \\ \vdots \\ x^{k-1}g \end{pmatrix} \in K^{k \times n} \quad \text{ahol } k = n - \deg(g)$$

generátormátrixú lineáris kód ciklikus.

Biz: Elég a ciklikusság tulajdonságot a generátor vektorokra leellenőrizni!

Elég $x^{k-1} \cdot g$-t eggyel eltolva mint kapunk.

$$x^{k-1} \cdot g = (0 \dots 0 \boxed{a_0 \quad g \quad a_t}) \qquad g = a_0 + a_1 x + \dots + a_t x^t$$

$$= (\boxed{a_t} 0 \dots 0\, 0 \boxed{a_0 \dots a_{t-1}}) \qquad t = n-k.$$

$$h = a_t + x^k \cdot a_0 + x^{k+1} \cdot a_1 + \dots + x^{k+t-1} \cdot a_{t-1} \overset{?}{\in} C$$

$$\Updownarrow$$

$$g \mid h \quad ?$$

$$g \mid h + a_t(x^n - 1) = x^k a_0 + x^{k+1} a_1 + \dots + x^n a_t$$

$$= x^k \cdot g \quad \checkmark$$

Példa BCH-kód keresésére:

$K = \mathbb{Z}_3$ $\quad f = x^3 + 2x + 1 \in K[x]$ irred

$r = 3$

mert $f(0) = 1$

$f(1) = 1$

$f(2) = 1$

$\alpha \in K[x]/\langle f \rangle$ 27-elemű

$o(\alpha) \mid 26$

$\overline{x^3 + 2x + 1} = \overline{0}$

$\overline{x^3} = \overline{x+2}$

$\overline{x^4} = \overline{x^2 + 2x}$

$\alpha = \overline{x}$

$\alpha^2 = \overline{x^2}$

$\alpha^4 = \overline{x^4} = \overline{x^2 + 2x}$

$\alpha^8 = \overline{(x^2+2x)^2} = \overline{x^4 + x^3 + x^2}$

$= \overline{x^2 + 2x + x + 2 + x^2}$

$= \overline{2x^2 + 2}$

$\alpha^{12} = \alpha^8 \cdot \alpha^4 = \overline{(x^2+2x)(2x^2+2)} = \overline{2x^4 + 4x^3 + 2x^2 + 4x} = \overline{2x^2 + x + x + 2 + 2x^2 + x} = \overline{x^2 + 2}$

$\alpha^9 = \alpha^8 \cdot \alpha = \overline{2x^2+2} \cdot \overline{x} = \overline{2x^3 + 2x}$

$= \overline{2x + 1 + 2x} = \overline{x+1}$

$\alpha^{13} = \alpha^9 \cdot \alpha^4 = \overline{x+1} \cdot \overline{x^2 + 2x} = \overline{x^3 + 3x^2 + 2x}$

$= \overline{x + 2 + 2x} = \overline{2}$

$\alpha^{26} = \overline{2}^2 = \overline{1}$ $\quad o(\alpha) = 26.$

$\boxed{\beta = \alpha^2}$

Válasszuk $\beta = \overline{x^2}$ akkor $o(\beta) = 13.$

Keressünk 2-hibajavító kódot.

$\underline{n = 13}$

$d = 5$ a minimális távolság.

β minimálpolinomja

$$\beta^0 = 1 = (1,0,0)$$
$$\beta^1 = \overline{x^2} = (0,0,1)$$
$$\beta^2 = \overline{x^4} = \overline{x^2+2x} = (0,2,1)$$
$$\beta^3 = \overline{x^6} = \overline{x^2(x^2+2x)} = \overline{x^4+2x^3} = \overline{x^2+2x+2x+1}$$
$$= \overline{x^2+x+1} = (1,1,1)$$

$$\beta^3+\beta^2+\beta+2 = (0,0,0)$$

min polinom $\underline{g_1} = \underbrace{x^3+x^2+x+2}$

β^2 min polinomja

$$(\beta^2)^0 = 1 = (1,0,0)$$
$$(\beta^2)^1 = \overline{x^2+2x} = (0,2,1)$$
$$(\beta^2)^2 = \alpha^8 = \overline{2x^2+2} = (2,0,2)$$
$$(\beta^2)^3 = \alpha^{12} = \overline{x^2+2} = (2,0,1)$$

$$(\beta^2)^3+(\beta^2)^2+2 = 0 \qquad g_2 = \underbrace{x^3+x^2+2}$$

β^3 min polinomija

$$(\beta^3)^0 = 1 = (1,0,0)$$

$$\beta^3 = \alpha^6 = \overline{x^2(x^2+2x)} = \overline{x^4+2x^3} = \overline{x^2+2x+2x+1}$$

$$= \overline{x^2+x+1} = (1,1,1)$$

$$(\beta^3)^2 = \alpha^{12} = \overline{x^2+2} = (2,0,1)$$

$$(\beta^3)^3 = \alpha^{18} = 2\cdot\alpha^5 = \overline{2x\cdot(x^2+2x)} = \overline{2x^3+x^2}$$

$$= \overline{2x+1+x^2} = (1,2,1)$$

$$(\beta^3)^3 + (\beta^3)^2 + \beta^3 + 2 = 0$$

$$\boxed{g_3 = x^3+x^2+x+2}$$

β^4 min polinomija

$$(\beta^4)^0 = 1 = (1,0,0)$$

$$(\beta^4)^1 = (2,0,2)$$

$$(\beta^4)^2 = \alpha^{16} = 2\cdot\alpha^3 = \overline{2\cdot x^3} = \overline{2x+1} = (1,2,0)$$

$$(\beta^4)^3 = \beta^{12} = \alpha^{24} = 2\cdot\alpha^{11} = 2\cdot\underbrace{\overline{x+1}}_{\alpha^9}\cdot\underbrace{\overline{x^2}}_{\alpha^2} =$$

$$\overline{2x^3+2x^2} = \overline{2x+1+2x^2} = (1,2,2)$$

$$(\beta^4)^3 + 2(\beta^4)^2 + 2(\beta^4)^1 + 2$$

$$g_4 = \boxed{x^3+2x^2+2x+2}$$

$$g = \text{lkkt}(g_1, g_2, g_3, g_4) = g_1 \cdot g_2 \cdot g_4$$

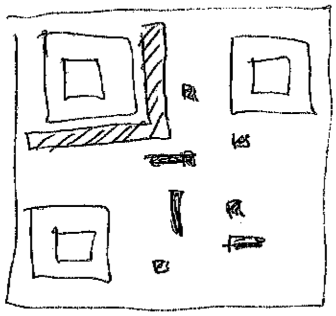
$$\underbrace{(x^3+x^2+x+2)(x^3+x^2+2)}(x^3+2x^2+2x+2)$$

$$(x^6+2x^5+2x^4+2x^3+1x^2+2x+1)(x^3+2x^2+2x+2)$$

$$g = x^9+x^8+2x^7+0\cdot x^6+x^5+0\cdot x^4+2x^3+2x^2+0\cdot x+2$$

$$G = \begin{pmatrix} 2&0&2&2&0&1&0&2&1&1&0&0&0 \\ 0&2&0&2&2&0&1&0&2&1&1&0&0 \\ 0&0&2&0&2&2&0&1&0&2&1&1&0 \\ 0&0&0&2&0&2&2&0&1&0&2&1&1 \end{pmatrix} \in \mathbb{Z}_3^{4\times 13}$$

<u>Példa</u>: QR-kódnál használt



$K = \mathbb{Z}_2$ $\qquad f = x^4+x+1$

$\qquad\qquad \alpha = \overline{x}$

min távolság

15-hosszú 3-hibajavító bináris kód $\quad d = 7$

$$g = 1+x+x^2+x^4+x^5+x^8+x^{10}$$

$\dim = 5$

5-bitnyi információt kódol be 15 bitnyibe

info ráta $\frac{1}{3}$

$\mathbb{Z}_2[x]/\langle f\rangle$ testben

Megj: $(x+y)^2 = x^2 + y^2$ mert $1+1=0$

$$[g(\alpha)]^2 = g(\alpha^2)$$

2-karakterisztikájú testben $\alpha, \alpha^2, \alpha^4, \dots$ minimálpolinomjai megegyeznek.

$\alpha^3, \alpha^6, \alpha^{12}$ minimálpolinomjai is megegyeznek.

QR-példában elég $\alpha, \alpha^3, \alpha^5$ minimálpolinomjait kiszámolni.

Köv: $K=\mathbb{Z}_2$ $d=3$ minimális távolságú BCH kód keresésekor egy ciklikus Hamming-kódot kapunk.

Példa: $K=\mathbb{Z}_2$ $f = x^3+x+1$

$\alpha = \overline{x}$ $o(\alpha)=7$

$\alpha^2 = \overline{x^2}$

$\alpha^3 = \overline{x+1}$

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

α min polinomja

$$\boxed{x^3+x+1}$$

$$P = \begin{array}{cl} \begin{pmatrix} 1&0&0 \\ 0&1&0 \\ 0&0&1 \\ 1&1&0 \\ 0&1&1 \\ 1&1&1 \\ 1&0&1 \end{pmatrix} & \begin{array}{l} \alpha^0 \\ \alpha^1 \\ \alpha^2 \\ \\ \\ \alpha^5 \\ \alpha^6 \end{array} \end{array}$$