infoCode ELŐADÁS 10.05.

$(0, 1, \dots, q-1) \in GF(q)$ $\left\{ \text{"}*\text{"}, \text{"}+\text{"} \right\}$ mod q (q prím)

(T): $\forall \alpha \in GF(q) \setminus \{0\}$ $\alpha^{q-1} = 1$

(D): min m: $\alpha^m = 1 \longrightarrow \text{ord}(\alpha) = m$

(D): $\text{ord}(\alpha) = q-1 \rightarrow \alpha$ primitív elem

q-áris Hamming kódok t = 1 javítóak

$\underline{e}^{(i)} = (0 \dots 0\ \alpha\ 0 \dots 0)$ $\alpha \in GF(q) \setminus \{\emptyset\}$ i, α identifikálni

$\boxed{\underline{\underline{H}}\, \underline{e}^{\omega^T} = \underline{s}^T} \longleftarrow \underline{\underline{H}}\, \underline{v}^T = \underline{s}^T$

$$\begin{pmatrix} \vdots & & \vdots & & \vdots \\ a^{(1)T} & \dots & a^{(i)T} & \dots & a^{(n)T} \\ \vdots & & \vdots & & \vdots \end{pmatrix} \begin{pmatrix} 0 \\ \vdots \\ 0 \\ \alpha \\ 0 \\ \vdots \\ 0 \end{pmatrix}_{e^i} = \alpha\, \underline{a}^{\omega^T} = \underline{s}^T$$

Feltételek: 1.) $\underline{a}^{(i)} = \underline{a}^{(j)}$ $\forall i, j = 1 \dots k$ $i \neq j$

2.) $\underline{a}^{(i)} \neq \underline{0}$

3.) $\underline{a}^{(i)}$ első nem zéró eleme 1

pl: $\begin{pmatrix} 0 \\ 1 \\ 2 \\ 3 \end{pmatrix} \longrightarrow \begin{pmatrix} 0 \\ \alpha \\ \vdots \end{pmatrix}$

$\beta \in GF(q)$

$\xrightarrow{} \boxed{\beta \cdot \underline{s}} \longrightarrow a^{(i)} \dots \longrightarrow i$ $\alpha = \beta_m^{-1}$

Hamming korlát feléje!

$$\frac{q^{n-k} - 1}{q-1} = n \qquad q^{n-k} = n(q-1) + 1 = \sum_{i=0}^{t} \binom{n}{i} (q-1)^i$$

$\boxed{\text{PERFECT KÓD}}$

pl.: $t = 1$ javítóak $C_H(n, k)$ $GF(7)$ felett

$C_H(8, 6)$ $\underline{\underline{H}}_{2\times 8} = \left(\begin{array}{cccccc:cc} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 & 1 \end{array} \right)$

$\underline{\underline{H}} \cdot \underline{\underline{G}}^T = \underline{\underline{0}} \rightarrow \underline{\underline{A}} = -\underline{\underline{B}}^T$

$\downarrow$

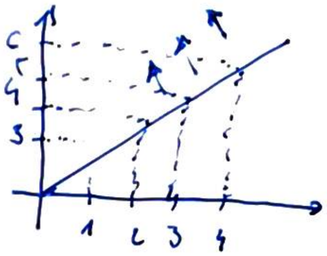
$\underline{\underline{G}}$

Megjegyzés: $C_H(n, n-2)$ $\quad t=1 = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$

$$3 \le d_{min} \le n-k+1 = 3$$

$$\Downarrow$$

$$d_{min} = n-k+1 \quad \text{MDS} \heartsuit$$



n-k

t = 1

t ≥ 2 MDS kód?

tömb[10]

10[tömb] -> (

polinomok GF(q)-ban

$(a_0, a_1, \dots, a_n) \in GF(q)$ $\quad a(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n \cdot x^n$

$(b_0, b_1, \dots, b_n)$ $\quad a_0, a_1, \dots, a_n, x \in GF(q)$

$\deg(a(x)) = n$

$$b(x) = b_0 + b_1 x + b_2 x^2 + \dots b_n x^k$$

$$c(x) = a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1)x + (a_2 + b_2)x^2 + \dots + (a_n + b_n)x^n$$

$$c(x) = a(x) \cdot b(x) = a_0 b_0 + (a_1 b_0 + a_0 b_1)x + (a_2 b_0 + a_1 b_1 + a_0 b_2)x^2 + \dots + \left(\sum_{j=0}^{\min(i, \deg\{a(x)\})} a_j b_{i-j}\right) x^i + \dots$$

polinom r.	vektor r.
$c(x) = a(x) + b(x)$	$c_i = a_i + b_i \rightarrow \underline{c} = \underline{a} + \underline{b}$
$c(x) = a(x) b(x)$	$c_i = \sum_{j=0}^{\min(i, \deg(a(x)))} a_j \cdot b_{i-j} \rightarrow \underline{c} = \underline{a} * \underline{b}$ konvolúció

polinom osztás

Adott $a(x), b(x)$ $\quad \deg(a(x)) = n > \deg(b(x)) = k$

$$a(x) = q(x) b(x) + r(x) \quad \deg(r(x)) < k$$

n-k lépésben

(T): $a(x)\big|_{x=x_1}=0 \longrightarrow a(x)=b(x)(x-x_1)$

$\deg(a(x)) > \deg(b(x))$

(B): $a(x)\big|_{x=x_1} \quad b(x)(x-x_1)\big|_{x=x_1} + r = 0$

köv $\quad a(x)=\prod_{i=1}^{\deg(a(x))}(x-x_i) \qquad \#\text{ gyökök} \le \deg(a(x))$

Algebra alaptétele

Reed-Solomon kódok

RS kódok

$\underline{u}=(u_0,u_1,\dots,u_{n-1}) \in GF(q) \qquad \alpha_0,\alpha_1,\dots,\alpha_{n-1} \in GF(q)$

$\alpha_i \neq \alpha_j$

$\downarrow$

$u(x)=u_0+u_1x+u_2x^2+\dots+u_{k-1}x^{k-1}$

q prím

$\boxed{n=q-1}$

$\underline{c}=(c_0,c_1,\dots,c_{n-1})$

$c_0 = u(x)\big|_{x=\alpha_0} = u_0+u_1\alpha_0+u_2\alpha_0^2+\dots+u_k\alpha_0^{k-1}$

$c_1 = u(x)\big|_{x=\alpha_1} = u_0+u_1\alpha_1+u_2\alpha_1^2+\dots+u_k\alpha_1^{k-1}$

$\vdots$

$c_{n-1} = u(x)\big|_{x=\alpha_{n-1}} = \dots$

$\underline{c}^T = \underline{u}^T \cdot \underline{\underline{G}}_{k\times n}$

$$(c_0,c_1,\dots,c_{n-1})^T=(u_0,u_1,\dots,u_{k-1})\cdot\begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_0 & \alpha_1 & \alpha_2 & \dots & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & \alpha_2^2 & \dots & \alpha_{n-1}^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \alpha_0^{k-1} & \alpha_1^{k-1} & \alpha_2^{k-1} & \dots & \alpha_{n-1}^{k-1} \end{pmatrix}$$

1. $d_{min} = w_{min} = n - \#\text{zérus elem} \ge n-(k-1) = n-k+1$
2. $d_{min} \le n-k+1$

$\boxed{d_{min} = n-k+1}$ MDS kód

RS kódok konstrukciója

α primitív elem $GF(q)$

$\alpha_0 = \alpha^0 = 1 \quad \alpha_1 = \alpha^1 = \alpha \quad \alpha_2 = \alpha^2, \ \dots, \ \alpha_{n-1} = \alpha^{n-1}$

$$\underline{\underline{G}}_{RS} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2k-2} & \dots & \alpha^{(k-1)(n-1)} \end{pmatrix}$$

$\underline{\underline{H}} \cdot \underline{c}^T = \underline{0}$

$\underline{\underline{H}}\,\underline{\underline{G}}^T = 0$

$$\underline{\underline{H}} = \begin{pmatrix} 1 & 1 & 1 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2n-1} \\ 1 & \alpha^3 & \alpha^6 & \dots & \alpha^{3(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k} & \alpha^{(n-k)2} & \dots & \alpha^{(n-k)(n-1)} \end{pmatrix}$$

példa $t = 2 \quad C_{RS}(n, k)$

$2 = t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor \rightarrow n-k = 4$

$d_{min} = n-k+1$

q prím $\quad n = q-1$

q	n	k
2	1	–
3	2	–
5	4	0
7	6	2
11	10	6
13	12	8

$C_{RS}(6, 2)$

kódtervezés

q prím

itt elengedtem : C