Kódoláselmélet 2020 december 2. (1)

Df.: Ha a BCH-kód definíciójában az α elemet konstanspolinomnak választjuk, azaz $0 \neq \alpha \in K$, akkor

α^k min polinomja $x-\alpha^k$

azaz a generátor polinom $g=(x-\alpha)(x-\alpha^2)\dots(x-\alpha^{d-1})$.

A kapott kódot Reed-Solomon kódnak nevezzük.

Példa: $K = GF(2^3) \cong \mathbb{Z}_2[x]/\langle x^3+x^2+1\rangle$

$\beta \in K\setminus\{0\}$ primitív elem $\beta = \overline{x}$

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

$\beta^4 = \overline{x^2+x+1}$, $\beta^5 = \overline{x+1}$, $\beta^6 = \overline{x^2+x}$, $\beta^7 = \overline{1}$

$o(\beta) = 7$

Legyen $\alpha = \overline{x+1} = \beta^5$ $\quad o(\alpha) = 7$

Legyen $n=7$, $d=5$ (2-hibajavító)

$g = (x-\alpha)(x-\alpha^2)(x-\alpha^3)(x-\alpha^4) =$

$x^4 - (\alpha+\alpha^2+\alpha^3+\alpha^4)x^3 + (\alpha\cdot\alpha^2+\alpha\cdot\alpha^3+\alpha\cdot\alpha^4$

$+\alpha^2\alpha^3+\alpha^2\alpha^4+\alpha^3\alpha^4)x^2 \cancel{-(\alpha+\alpha^2+\alpha^3+\alpha^4)x}$ $+ \alpha\alpha^2\alpha^3\alpha^4$

$-(\alpha\alpha^2\alpha^3+\alpha\alpha^2\alpha^4+\alpha\alpha^3\alpha^4+\alpha^2\alpha^3\alpha^4)x$

$= x^4 - (\quad\quad)x^3 + (\alpha^3+\alpha^4+\cancel{2\alpha^5}+\alpha^6+1)x^2$

$-(\alpha^6+1+\alpha+\alpha^2)x + \alpha^3$

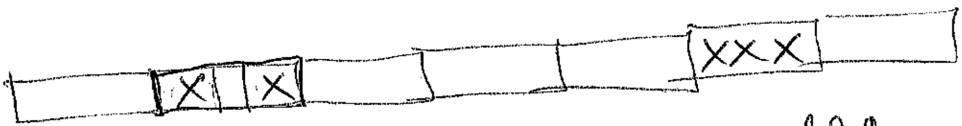
$$= x^4 + (\beta^5 + \beta^3 + \beta + \beta^6)x^3 +$$
$$(\beta + \beta^6 + \beta^2 + 1)x^2 + (\beta^2 + 1 + \beta^5 + \beta^3)x + \beta$$
$$= x^4 + \beta x^3 + 1 x^2 + \beta x + \beta$$

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

üzenet K^3 ~~vektortér~~ kódnó K^7

$\Vert 2$ $\qquad$ $\Vert 2$ ~~mint halmaz~~

$\mathbb{Z}_2^9$ $\qquad$ $\mathbb{Z}_2^{21}$ mint ~~Abel-csop~~ $\mathbb{Z}_2$ feletti vektortér



K felett 2-hibajavító, de $\mathbb{Z}_2$ felett akár többet is ki tud javítani (csomós hibákat)

$\mathbb{Z}_2$ feletti gen. mátrix

$$\left(\begin{array}{c|c|c|c|c|c|c}
\begin{matrix}0&1&0\\0&0&1\\1&0&1\end{matrix} & \begin{matrix}0&1&0\\0&0&1\\1&0&1\end{matrix} & \begin{matrix}1&0&0\\0&1&0\\0&0&1\end{matrix} & \begin{matrix}0&1&0\\0&0&1\\1&0&1\end{matrix} & \begin{matrix}1&0&0\\0&1&0\\0&0&1\end{matrix} & \begin{matrix}0&0&0\\0&0&0\\0&0&0\end{matrix} & \begin{matrix}0&0&0\\0&0&0\\0&0&0\end{matrix} \\
\hline
\begin{matrix}0&0&0\\0&0&0\\0&0&0\end{matrix} & & & & & & \begin{matrix}0&0&0\\0&0&0\\0&0&0\end{matrix} \\
\hline
\begin{matrix}0&0&0\\0&0&0\\0&0&0\end{matrix} & \begin{matrix}0&0&0\\0&0&0\\0&0&0\end{matrix} & & & & &
\end{array}\right)$$

Kód összefűzés

$C_1 \le K^{n_1}$ lineáris kód, d_1-dim, ~~r_1 hibajavító~~ r_1 - min távolság

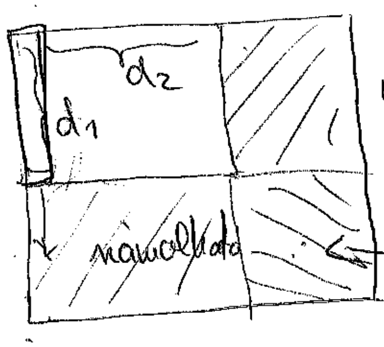
$C_2 \le K^{n_2}$ —//— d_2-dim, ~~r_2 hibajavító~~ r_2 - min táv

$\Downarrow$

$C_3 \le K^{n_1 n_2}$ lineáris, $d_1 \cdot d_2$-dim, ~~$r_1 r_2$-hibajavító~~ $r_1 r_2$ min táv.

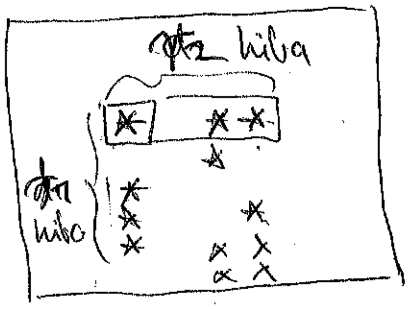
kódszavak n_2 oszlop úgy, hogy a számolható sorok C_2 elemei, oszlopok C_1 elemei

n_1 sor



kétféleképpen számolható

$$C_3 = \{ A \in K^{n_1 \times n_2} \mid \forall i \; A_{i,*} \in C_2, \; \forall j \; A_{*,j} \in C_1 \}$$

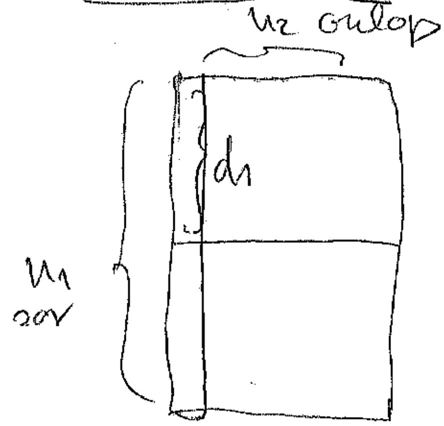


mi a legkisebb súlyú nem 0 mátrix kódszó

min távolság $r_1 \cdot r_2$

info ráta $\frac{d_1 \cdot d_2}{n_1 \cdot n_2}$

Kód ismétlés



$C_1 \subseteq K^{n_1}$ lin kód

d_1-dim r_1-min táv

n_2 tetszőlege

oszlopok a C_1 elemei

ez speciális esete a kód összefűzésnek

$C_2 = K^{n_2}$, $d_2 = n_2$, $r_2 = 1$

info ráta $\frac{d_1}{n_1}$ min távolság r_1

relatív hibajavító képesség $\frac{r_1}{n_1 \cdot n_2}$ az

rosszabbodik.

Konvolúciós kódok

$g \in K[x]$ polinom generátor fix

$h \in K[x]$ üzenet tetszőleges méretű

$gh \in K[x]$ kódszó

min távolság $\leq \deg(g) + 1$ -

h mérete $\deg(h)+1$

gh mérete $\underbrace{\deg(g)} + \deg(h) + 1$

$\deg(g)$-vel megnöveli az üzenet méretét.

Áll: minimális súlyú ~~bitek~~ kódszavakban néhány helyen tömörülnek a hibák

Low density parity Check kódók

LDPC kódok

$P \in K^{n \times d}$ n hossz, d dimenzió

nagyon sok helyen P-ben 0 van.

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

pl. $\mathbb{Z}_2$ felett minden oszlopban 3 db 1-es

$$C = \left\{ (x_1, x_2, x_3, x_4, x_5, x_6, x_7) \in \mathbb{Z}_2^7 \;\middle|\; \begin{array}{l} x_2 + x_5 + x_7 = 0 \\ x_1 + x_4 + \cancel{x_5} = 0 \\ x_3 + x_6 + \cancel{x_7} = 0 \end{array} \right\}$$

1001101

1000101