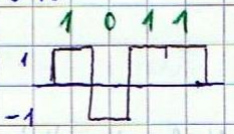
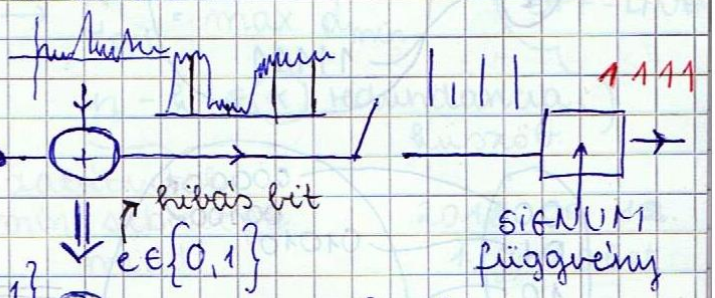
Hibajavító kódolás

- Alapkérdés: hogyan lehet egy megbízhatatlan csatornán, megbízhatóan kommunikálni?
- Csatornamodell: AWGN
  - feladóoldal: 1011 → 
  - vevőoldal: 

- Ha $e = 1 \rightarrow v = u \oplus e = 0 + 1 = 1$
  $\hookrightarrow v = 1 + 1 = 0$

$u \in \{0,1\}$, $e \in \{0,1\}$, $v \in \{0,1\}$

$$P_b = P(v=1 \mid u=0) = P(v=0 \mid u=1) = P(e=1)$$

BSC kódolás

- Vektoriális csatornamodell

$\bar{c} = (01010)$ → hibavektor

$\bar{u} = (10101) \rightarrow \bar{v} = \bar{u} + \bar{e} = (11111)$

$$P(\bar{e}) = P_b^2 (1-P_b)^3$$

Hamming-távolság

$$d(\bar{u}, \bar{v}) = 2$$

$$d(\bar{u}, \bar{v}) = w(\bar{u} \oplus \bar{v}) = 2 = w(\bar{e})$$

$$\bar{u} + \bar{e} = \bar{v}$$
$$\bar{e} = \bar{u} + \bar{v}$$

$w(\bar{e})$: hibavektor súlya

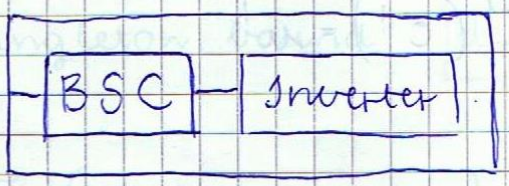
n-hosszúságú üzenetek

$$P(\bar{e}) = P_b^{w(\bar{e})} (1-P_b)^{n - w(\bar{e})}$$

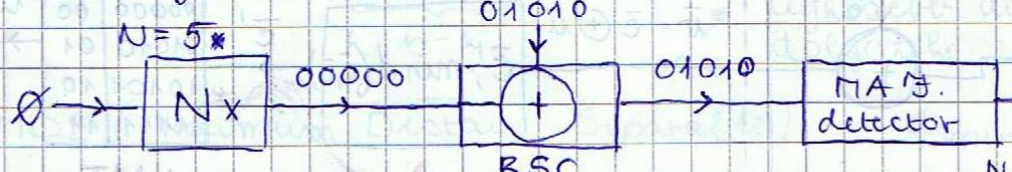
$0 \le P_b \le 0.5$

$$P(\bar{e}) = \left(\frac{P_b}{1-P_b}\right)^{w(\bar{e})} (1-P_b)^n \sim \exp(-w(\bar{e}))$$

1 db hiba
2 db hiba
⋮



- Hibajavítás: ismétléses kódolás → bármilyen jó minőségű csatorna!



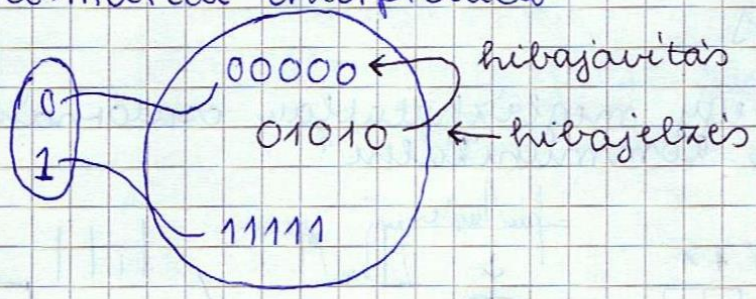
BSC
$P_b \sim 0,1$
0,1 a valószínűsége, hogy 1-es lesz

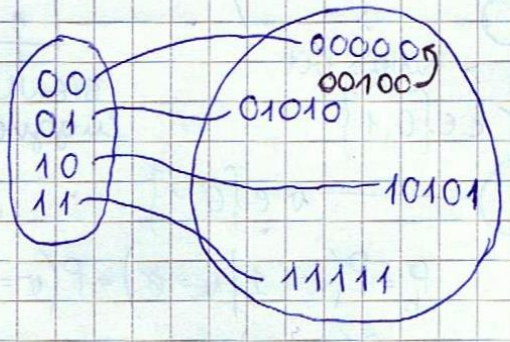
$$P_b' = \sum_{i=\lceil N/2 \rceil}^{N} \binom{N}{i} P_b^i (1-P_b)^{N-i}$$

N: $P_b' \le 10^{-8}$

Hátrány: lassú

- Geometriai interpretáció

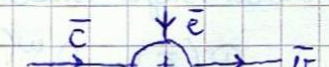




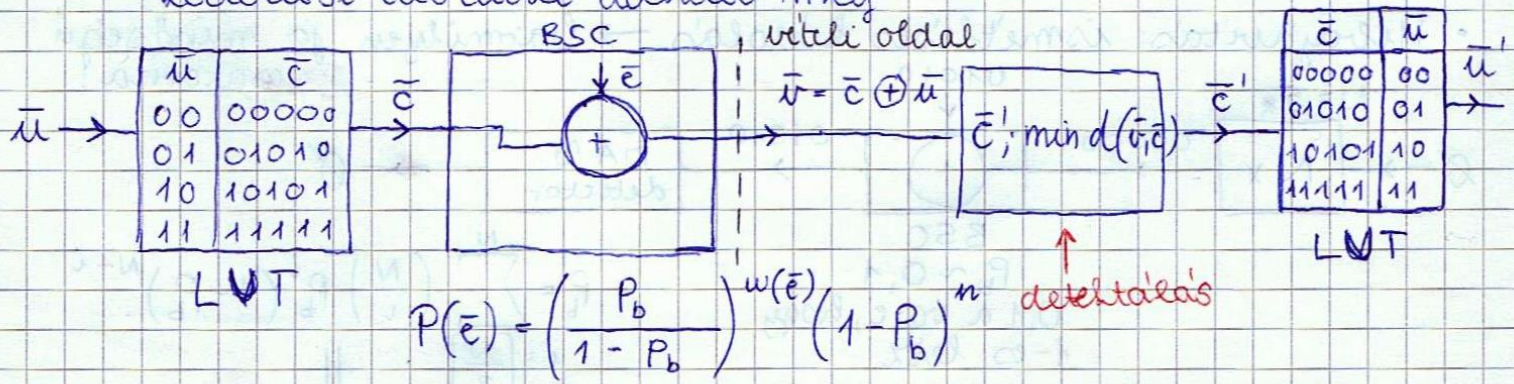
$\Longrightarrow$ Hibajavító kódolás "kiterjesztése" hibajelzés, hibajavítás

↳ d_{min} (hibajelzés/javításhoz fontos)

↳ redundancia ≤ hiszöb (lényeges szempont az ~~sebesse~~ átviteli sebesség szempontjából)

- Formális modell
  - üzenetek $\bar{u} \in \{0,1\}^k \rightarrow \bar{u} = \{\underbrace{0,1,0\ldots}_{k}\}$ 2^k db
  - kód: $C = \{\bar{c}_1, \bar{c}_2 \ldots \bar{c}_M\}$ $M = 2^k$ $\dim(\bar{c}) = n > k$
    redundancia $\frac{k}{n}$; $n-k$
  - kódolás: $\Psi: \{0,1\}^k \rightarrow C$; $\Psi(\bar{u}) = \bar{c}$ 
  - Vett vektor: $\bar{v} \in \{0,1\}^n$
  - detekció: $\Psi\{0,1\}^n \rightarrow C$ $\Psi(\bar{v}) = \bar{c}$
  - dekódolás: $\Psi^{-1}: C \rightarrow \{0,1\}$ $\Psi^{-1}(\bar{c}') = \bar{u}'$

- Általános kódolási séma
  - kódolási táblával adható meg



ū	c̄
00	00000
01	01010
10	10101
11	11111

c̄	ū
00000	00
01010	01
10101	10
11111	11

$$P(\bar{e}) = \left(\frac{P_b}{1-P_b}\right)^{w(\bar{e})} (1-P_b)^n$$

Probléma: a táblázat ~~xxx~~ nagyon gyorsan (exponenciálisan) nő → drága hardver

Komplexitás: 3 $O(2^k)$ NP (Nem Polinomiális) } KERESŐALGORITMUS

2 LUT + SEARCH ↵ / ↳ kódszavak száma (lookup table mérete)

Hátrány még a táblázat kódolása → $C_{opt} = \max d_{min}$ OFF-LINE

↓ ON-LINE komplexitás (futási idejű)

$n - k \leq (\alpha)$ redundancia küszöb

adatátvitel min. sebessége miatt

$C(5, 2)$

↳ kódszavak hossza

↳ kódolt szóvektor hossza (kódszóvektor)

2018. 09. 12.
1. gyakorlat

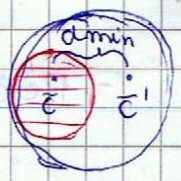
Hibajavító kódolás → nem minden hiba javítása, hanem a nagyobb valószínűségű hibakódok felismerése, javítása

- Kódok teljesítőképessége
  - d_{min}: minimum Hamming-távolság a kódszavak között

$$\min_{\bar{c}, \bar{c}' \in G, \bar{c} \neq \bar{c}'} d(\bar{c}, \bar{c}')$$

hibajelző képesség: $d_{min} - 1$

hibajavító képesség: $t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$



$\bar{c} \rightarrow$ [BSC] $\rightarrow \bar{v}$

$d(\bar{c}, \bar{v}) < d(\bar{c}', \bar{v})$

$d(\bar{c}, \bar{v})$

minél nagyobb a d_{min}, annál jobb a kód

↳ lassul az adatátviteli sebesség

- Singleton bound: $d_{min} \leq n - k + 1$

kódszóhossz, üzenethossz

$\bar{c} = (u_1, \dots u_k \; p_{k+1} \dots p_n)$

$\bar{c}' = (u_1' \dots u_k' \; \underbrace{p_{k+1}' \dots p_n'}_{n-k})$

legkisebb adatátviteli sebességgel dolgozik

MDS (Maximum Distance Separable) $d_{min} = n - k + 1$ → opt.

- Hamming bound: $\sum_{i=0}^{t} \binom{n}{i} \leq 2^{(n-k)}$ redundancia $\rightarrow \frac{n!}{i!\,(n-i)!}$

$\sum_{i=0}^{t} \binom{n}{i} = 2^{n-k}$ → perfect kód

MDS kódok

- polinomiális komplexitás
- REAL TIME opt teljesítőképesség

Lineáris bináris $C(n,k)$ konstrukciója

- $G = \{\bar{g}^{(1)}, \bar{g}^{(2)}, \dots, \bar{g}^{(k)}\}$ $\quad \dim(\bar{g}^{(i)}) = n$

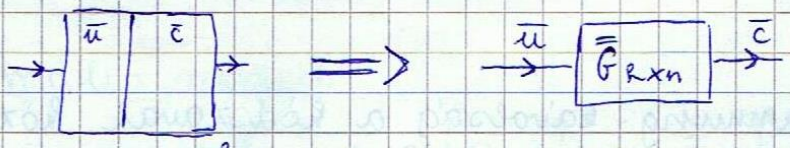
$$G = \mathcal{L}_c\{g\}$$

$$\bar{c} = \sum_{i=1}^{k} u_i \bar{g}^{(i)}$$

($\bar{c}$: n hosszú; u_i: k db; $\bar{g}^{(i)}$: n db)

$$\bar{\bar{G}}_{k\times n} = \begin{pmatrix} \bar{g}^{(1)} \\ \bar{g}^{(2)} \\ \vdots \\ \bar{g}^{(k)} \end{pmatrix} \qquad \bar{c} = \bar{u}\,\bar{\bar{G}}$$

- Technológiai jelentőség: LUT helyett mátrix szorzás



$$2^k(k+n) \gg k \times n$$

- Példa: $C(5,2) \rightarrow G = \{(10110), (01111)\}$ (n, k)

$$\bar{\bar{G}}_{2\times 5} \begin{pmatrix} 10110 \\ 01111 \end{pmatrix} \rightarrow \bar{\bar{B}}$$

$\rightarrow$ identitás (egység) mátrix

$(00)\ \begin{pmatrix} 10110 \\ 01111 \end{pmatrix} = (00000) = \bar{c}^{(0)}$

$(01) \quad = (01111) = \bar{c}^{(1)}$ $\qquad \bar{\bar{G}}_{k\times n} = \left(\bar{\bar{I}}_{k\times k} \mid \bar{\bar{B}}_{k\times(n-k)}\right)$

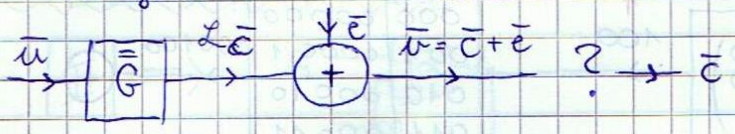
$(10) \quad = (10110) = \bar{c}^{(2)}$ $\qquad d_{min} = 3 \rightarrow \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 1$ javítás

$(11) \quad = (11001) = \bar{c}^{(3)}$ $\qquad d_{min} - 1 = 2$ jelzés

$$\min_{\substack{\bar{c},\bar{c}' \in G \\ \bar{c} \neq \bar{c}'}} d(\bar{c},\bar{c}') \rightsquigarrow \min w(\underbrace{\bar{c}+\bar{c}'}_{\bar{c}''}) \rightsquigarrow \min w(\bar{c}'')$$

- nagy súlyú hibavektor $\rightarrow$ kis vg

• Hibajavítás a vételi oldalon



- Paritásellenőrző mátrix: $\bar{\bar{H}}_{(n-k)\times n} \cdot \bar{\bar{H}}_{(n-k)\times n}\ \bar{c}^T = \bar{0}^T$

$$\bar{\bar{H}}\,\bar{c}^T = \bar{\bar{H}}\,(\bar{u}\,\bar{\bar{G}})^T = \bar{\bar{H}}\,\bar{\bar{G}}^T\bar{u}^T = \bar{0}^T \quad \forall \bar{u} \in \{0,1\}^k$$

$$\Downarrow$$

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

$$\underbrace{\left(\bar{\bar{A}}_{(n-k)\times k} \,/\, \bar{\bar{I}}_{(n-k)\times(n-k)}\right)}_{\bar{\bar{H}}_{(n-k)\times n}} \begin{pmatrix} \bar{\bar{I}}_{k\times k} \\ \bar{\bar{B}}^T_{(n-k)\times k} \end{pmatrix} = \bar{\bar{0}} \Longrightarrow \bar{\bar{A}}_{(n-k)\times k} + \bar{\bar{B}}^T_{(n-k)\times k} = \bar{\bar{0}}$$

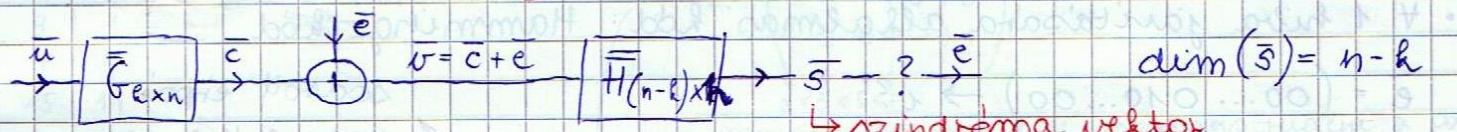
$$\Downarrow$$

$$\bar{\bar{A}} = \bar{\bar{B}}^T$$

- Példa:

$$\bar{\bar{H}}_{3\times 5} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix}$$

$\bar{\bar{B}}^T$ $\bar{\bar{I}}$



↳ szindróma vektor

$\bar{\bar{H}} \cdot \bar{v}^T = s^T \rightarrow$ kiszámolható $\Longrightarrow \bar{\bar{H}}\,(\bar{c}+\bar{e})^T = \bar{s}^T \Longrightarrow \underbrace{\bar{\bar{H}}\,\bar{c}^T}_{\bar{0}^T} + \bar{\bar{H}}\,\bar{e}^T = \bar{s}^T$

ismert — megfigyelhető

~~$\bar{e}^T = \bar{\bar{H}}^{-1}\,\bar{s}^T$~~ ILYEN NINCS!

$$\left(\bar{\bar{H}}\right)\left(\bar{e}^T\right) = \left(\bar{s}^T\right) \Big\} \; n-k \text{ db egyenlet}$$

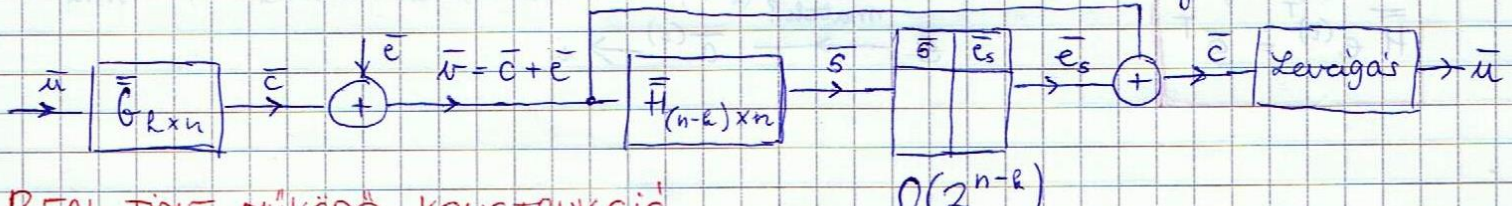
n db ismeretlen

Alulhatározott rendszer.

group leader ↗

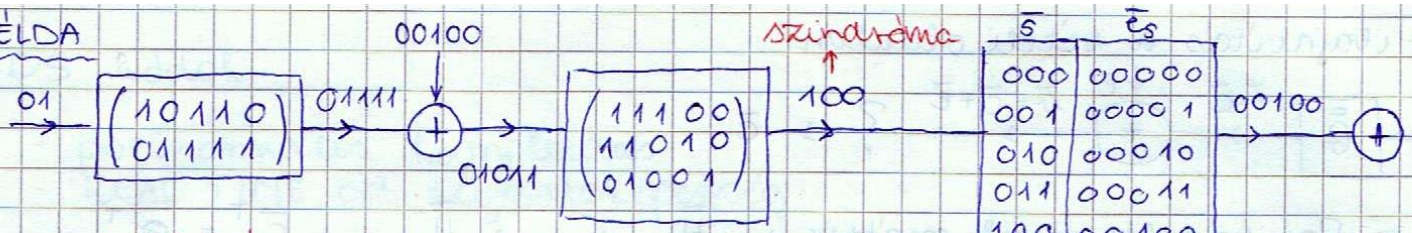
$$E_{\bar{s}} = \left\{ \bar{e} : \bar{\bar{H}}\,\bar{e}^T = \bar{s}^T \right\} \rightarrow \bar{e}_s : \min w(\bar{e})$$

legalacsonyabb súlyú hibavektor ← legnagyobb vg



REAL TIME MŰKÖDŐ KONSTRUKCIÓ

PÉLDA



$E_{s_{001}} = \{$ (00001); (01110); (10111); (11000) $\}$

1 súlyú — GROUP LEADER; 3 súlyú; 4 súlyú; 2 súlyú

2013.09.19.

Szisztematikus kód: első bitek hiadják az egységmátrix

1) $\overline{\overline{G}}$ - ből felírom a paritásellenőrző mátrixot.
2) Megfelelő bittel megcímzem a mátrix sorait

$$\overline{\overline{H}} \begin{pmatrix} 1&1&1&0&0 \\ 1&1&0&1&0 \\ 0&1&0&0&1 \end{pmatrix} \overline{v}^T \begin{pmatrix} 0\\0\\0\\0\\1 \end{pmatrix} = \overline{s}^T \begin{pmatrix} 0\\0\\1 \end{pmatrix}$$

(11 - nél mod2-ben carry nélkül a generátormátrix sorait)

Előírt teljesítőképességű lin. bin. kód tervezése

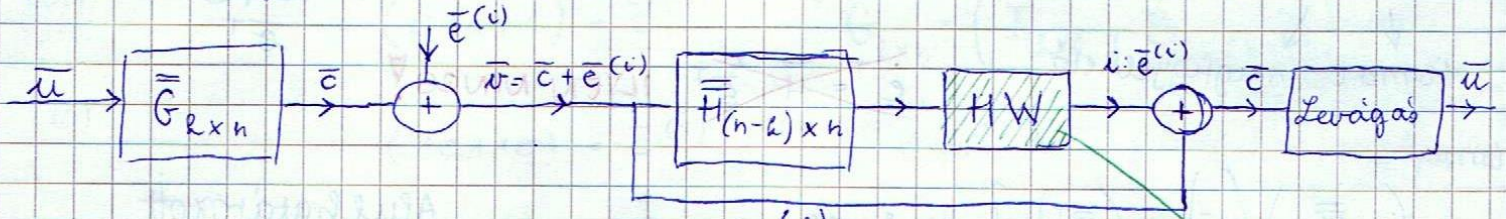
- $\forall$ 1 hiba javítására alkalmas kód: Hamming - kód

$\overline{e} = (00\ldots010\ldots00) \rightarrow i$?

↑ i. pozíció (a többi mind 0)

sodrott érpár KOAX - kábel pl.

Jó minőségű csatornát feltételezünk - wired communication



detektálja a hiba helyét

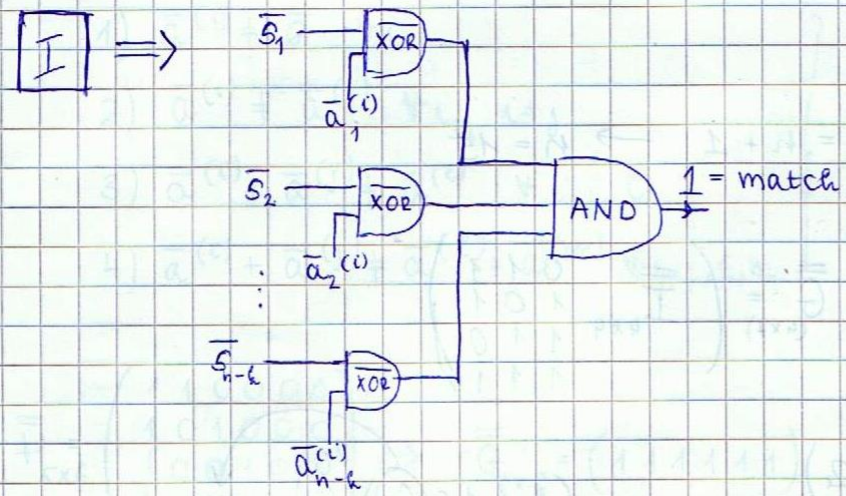
$$\overline{\overline{H}}_{(n-k)\times n} \cdot \overline{e}^{(i)T} = \left(\overline{a}^{(1)T} \ldots \overline{a}^{(i)T} \ldots \overline{a}^{(n)T} \right) \begin{pmatrix} 0\\ \vdots \\ 1 \leftarrow i \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} \cdot \\ \overline{s}^T \\ \cdot \end{pmatrix} = \left(\overline{a}^{(i)T} \right)$$

$$\overline{\overline{H}}\,\overline{v}^T = \overline{s}^T \longrightarrow \overline{\overline{H}} \left(\overline{c} + \overline{e}^{(i)} \right)^T = \overline{\overline{H}}\,\overline{c}^T + \overline{\overline{H}}\,\overline{e}^{(i)T}$$

$$\boxed{\overline{\overline{H}}\,\overline{e}^{(i)T} = \overline{s}^T}$$

$\overline{s} \xrightarrow{\text{match?}} \overline{a}^{(i)} \rightarrow i$

Hardware felépítése



Kritériumok a modellhez

1) $\bar{a}^{(i)} \neq \bar{a}^{(j)} \quad \forall i,j \; ; \; i \neq j$

2) $\bar{a}^{(i)} \neq \bar{0} \quad \forall i$

$$n = 2^{n-k} - 1$$

$$2^{n-k} = n + 1$$

$$2^{n-k} = \sum_{i=0}^{1} \binom{n}{i} \Rightarrow \text{perfect kód}$$

Példa

n	k
3	1
7	4
15	11
⋮	⋮

$C_H(7;4)$:

$$\bar{\bar{H}}_{3\times 7} = \left(\begin{array}{ccc|c|ccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 1 \end{array}\right) \quad \bar{\bar{I}}$$

3 < 5 < 6 < 7

monoton növekvő kell megkonstruálni a paritásellenőrző mátrixot

$$\bar{\bar{G}}_{4\times 7} = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

$\bar{\bar{I}}$

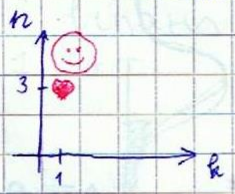
$\bar{\bar{H}}$ első 3 sorának nem identitás mátrixba tartozó invertálása

Singleton bound miatt

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

$$3 \leq d_{min} \leq 3$$

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



$$\bar{\bar{G}}_{k\times n} = \left(\bar{\bar{I}}_{k\times n} ; \bar{\bar{B}}_{k\times(n-k)}\right) \; ; \quad \bar{\bar{H}}_{(n-k)\times n}\left(\bar{\bar{A}}_{(n-k)\times k} ; \bar{\bar{I}}_{(n-k)\times(n-k)}\right)$$

4. előadás — többszörös hibák javítása; galois testek — 2013. 09. 24

Lehetséges ZH példa

1) $k = 11 \rightarrow n = ?$ $\quad 2^{n-k} = n+1 \rightarrow n = 15$

2) $\overline{\overline{H}} = \begin{pmatrix} 0&1&1&1&0&0\\ 1&0&1&0&1&0\\ 1&1&0&0&0&1 \end{pmatrix} \Rightarrow \overline{\overline{G}}_{(4\times7)} = \begin{pmatrix} \overline{\overline{I}}_{4\times4} \\ \begin{matrix} 0&1&1\\ 1&0&1\\ 1&1&0\\ 1&1&1 \end{matrix} \end{pmatrix}$

3) $\overline{\overline{G}} = \begin{pmatrix} 1&0&1&1&0\\ 0&1&1&1&1 \end{pmatrix} \rightarrow C(5;2)$

$\overline{e} = (00001) \quad \overline{e}' (11000)$

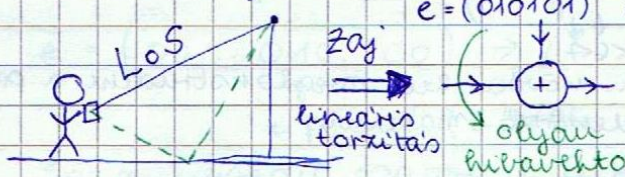
$$\begin{pmatrix} 1&1&1&0&0\\ 1&1&0&1&0\\ 0&1&0&0&1 \end{pmatrix} \begin{pmatrix} 0\\0\\0\\0\\1 \end{pmatrix} = \begin{pmatrix} 0\\0\\1 \end{pmatrix}$$

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

modulo 2 carry nélkül

Többszörös hibák javítása

- technológiai motiváció: vezeték nélküli hálózati technológiák – $\overline{e} = (0101101)$ ban a „probléma" a rádiócsatorna.



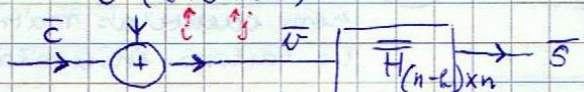
olyan hibavektorokat kapacitunk melyek súlya ≥ 2 → Hamming-kód nem képes elbánni „vele"

$\overline{\overline{H}}\,\overline{v}^T = \overline{s}^T \rightarrow \overline{\overline{H}}\,\overline{e}^{(i,j)T} = \overline{s}^T$ (tervezés?)

adott — megfigy. — kiszámítható — adott

- Hogyan lehet $\forall$ 2 hibát javítani?

$\overline{e} = (0101100)$



$\overline{e}^{(i,j)}$

$$\left(\overline{a}^{(1)T} \ldots \overline{a}^{(i)T} \ldots \overline{a}^{(j)T} \ldots \overline{a}^{(n)T}\right) \begin{pmatrix} 0\\ \vdots\\ 1 \leftarrow i\\ \vdots\\ 1 \leftarrow j\\ \vdots\\ 0 \end{pmatrix} = \left(\overline{s}^T\right) = \left(\overline{a}^{(i)T}\right) + \left(\overline{a}^{(j)T}\right)$$

• Egyértelmű dekódolás feltétele:

1) $\bar{a}^{(i)} \neq \bar{0} \quad \forall i$
2) $\bar{a}^{(i)} \neq \bar{a}^{(j)} \quad \forall i,j \; i \neq j$
3) $\bar{a}^{(i)} + \bar{a}^{(j)} \neq \bar{a}^{(e)} \quad \forall i,j,e$
4) $\bar{a}^{(i)} + \bar{a}^{(j)} \neq \bar{a}^{(e)} + \bar{a}^{(m)} \quad \forall i,j,e,m$

$\alpha_1 \bar{a}^{(i)} + \alpha_2 \bar{a}^{(j)} + \alpha_3 \bar{a}^{(e)} + \alpha_4 \bar{a}^{(m)} \neq \bar{0}$

$\Downarrow$

2 hiba javításhoz $\forall$ 4 különböző oszlopvektor $\bar{\bar{H}}$-ban lineárisan független.

$$\bar{\bar{H}}_{5\times6} = \begin{pmatrix} 1&1&0&0&0&0 \\ 1&0&1&0&0&0 \\ 1&0&0&1&0&0 \\ 1&0&0&0&1&0 \\ 1&0&0&0&0&1 \end{pmatrix} \rightarrow \bar{\bar{G}}_{1\times6} = (1\,1\,1\,1\,1\,1)$$

$\frac{k}{n} = \frac{1}{6}$ (hatodára lassul az adatátviteli sebességet)

$C(6,1)$

Bináris $\{0,1\} \rightarrow$ "q"-áris $\{0,1,\dots q-1\}$

$$\bar{\bar{H}}_{5\times8} = \begin{pmatrix} 4&3&2&1&0&0&0&0 \\ 4&3&2&0&1&0&0&0 \\ 4&3&2&0&0&1&0&0 \\ 4&3&2&0&0&0&1&0 \\ 4&3&2&0&0&0&0&1 \end{pmatrix}$$

$\frac{k}{n} = \frac{3}{8}$-ára lassul az adatátvitel

$C(8,3)$

• Egy kód t hiba javítására képes → legalább 2t lin. fgtlen oszlopvektor van

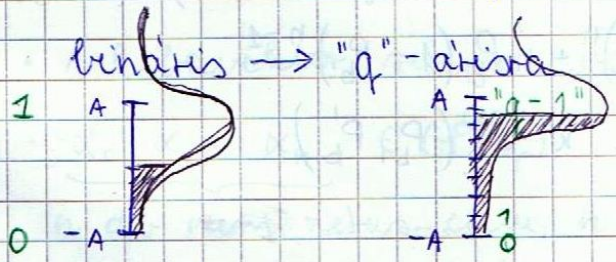
Biz.: $w_{min} = d_{min} = 2t+1$

$w(\bar{b}) = 2t \qquad \bar{\bar{H}}\,\bar{b}^T \neq \bar{0}^T$

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

$$\left(\bar{a}_{i_1}^T \; \bar{a}_{i_2}^T \dots \bar{a}_{i_{2t}}^T\right) \cdot \begin{pmatrix} 0 \\ \vdots \\ \alpha_{i_1} \\ \vdots \\ 0 \\ \alpha_{i_2} \\ \vdots \\ 0 \\ \alpha_{i_{2t}} \\ \vdots \\ 0 \end{pmatrix} = \sum_{j=1}^{2t} \alpha_{i_j} \cdot \bar{a}^{(i_j)T} \neq \bar{0}^T$$

bináris → "q"-áris



- a csatorna elemeik
- $\log_2$"q" adatátviteli sebesség

- Matematikai konklúzió: véges testek feletti algebra GF(q)

Galois field

Galois testek $GF(q) = \{0; 1; 2 \dots q-1\}$

- összeadásra zárt: $\alpha, \beta \in GF(q) \rightarrow \alpha + \beta \in GF(q)$
  - $\alpha + \beta = \beta + \alpha$; $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
  - $\exists \emptyset : \alpha + \emptyset = \alpha \quad \forall \alpha \in GF(q)$
  - $\exists \beta \in GF(q) \; \forall \alpha : \alpha + \beta = \emptyset \qquad \beta = (\alpha)^{-1} = -\alpha$
- szórzás $(*)$
  - $\alpha, \beta \in GF(q) \setminus \{\emptyset\} \rightarrow \alpha \cdot \beta \in GF(q) \setminus \{\emptyset\}$
  - $\alpha \cdot \beta = \beta \cdot \alpha$; $(\alpha \cdot \beta) \cdot \gamma = \alpha (\beta \cdot \gamma)$
  - $\exists 1 : \alpha \cdot 1 = \alpha \quad \forall \alpha \in GF(q) \setminus \{\emptyset\}$
  - $\forall \alpha \in GF(q) \setminus \{0\} \; \exists \beta : \alpha \cdot \beta = 1 \qquad \beta = (\alpha)^{-1} = \frac{1}{\alpha}$

$\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$

- Példa: mod q algebra → csak, ha q prím

$\alpha + \beta = \gamma \mod q \qquad \alpha + \beta = u \cdot q + \gamma$

$\alpha \cdot \beta = \gamma' \mod q \qquad \alpha \cdot \beta = u' \cdot q + \gamma'$

$GF(7) \qquad 5 + 2 = 1 \cdot 7 + \emptyset \qquad 5 + 2 = 0 \mod 7$

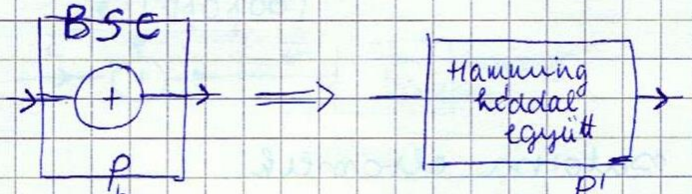
$6 \cdot 6 = 5 \cdot 7 + 1 \qquad 6 \cdot 6 = 1 \mod 7$

5. előadás

határváltozás, polinomok $GF(q)$-ban, Reed-Salomon kódok

2013. 09. 26.

- Kódtervezés kérdése, "kommunikációs mérnökség"
  - Adott P_b (fizikai) $\gg P_b'$ (QoS) $\sim 10^{-8}$



$P(k\text{-bites üzenet helyes átvitele}) = (1 - P_b')^k =$

$= (1 - P_b)^n + n P_b (1 - P_b)^{n-1}$

$n, k = \Psi(P_b, P_b')$

$n = 2^{n-k} - 1 \leftarrow n \leq 2^{n-k} - 1 \leftarrow$ többszörös hibajavítás $\leftarrow$ "q^n-adikus"

$GF(q) \rightarrow$ mod q feletti aritmetika, q - prím

$\alpha \in GF(q) \setminus \{\emptyset\} \rightarrow \alpha^{q-1} = 1$

$\alpha \cdot \alpha_1 \cdot \alpha \cdot \alpha_2 \cdot \ldots \alpha \cdot \alpha_{q-1} = \alpha_{i_1} \cdot \alpha_{i_2} \cdot \ldots \cdot \alpha_{i_{q-1}}$

$\alpha^{q-1} (\alpha_1 \cdot \alpha_2 \cdot \ldots \alpha_{q-1}) = \alpha_{i_1} \cdot \alpha_{i_2} \cdot \ldots \alpha_{i_{q-1}}$

Hatványtábla a GF(7) felett

	1	2	3	4	5	6	rend
1	1	.	.	.	.	.	1
2	2	4	1	2	4	1	3
3	3	2	6	4	5	1	6
4	4	2	1	4	2	1	3
5	5	4	6	2	3	1	6
6	6	1	6	1	6	1	2

primitív elem

$3^3 = 27 = 3 \cdot 7 + 6$

$3^3 = 3^1 \cdot 3^2 = 6$

$3^4 = 3^2 \cdot 3^2 = 2 \cdot 2 = 4$

Polinomok a GF(q) felett

- $a(x) = a_0 + a_1 x + \ldots + a_n x^n$; $dy(a(x)) = n$; $a_0, a_1 \ldots a_n, x \in GF(q)$
- Gyökkeresés sokkal gyorsabb! ~~nisk~~
- $b(x) = b_0 + b_1 x + \ldots + b_n x^n$
- $c(x) = a(x) + b(x) = a_0 + b_0 + (a_1 + b_1) x + \ldots + (a_i + b_i) x^i$
- $c(x) = a(x) b(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + (a_0 b_2 + a_1 b_1 + a_2 b_0) x^2 + \ldots + \sum a_j b_{i-j} x^i$
- Polinom osztás

$a(x) = q(x) d(x) + r(x)$

$dy(r(x)) < dej(d(x))$

$dej(a(x)) > dej(d(x))$

Többszörös hibák javítása Reed-Salomon (RS) kódokkal

- A hibavektor súlya nagy
- $\alpha_0, \alpha_1 \ldots \alpha_{n-1} \in GF(q)$

  n db nem zérus elem, $n = q - 1$

$\overline{u} = (u_0, u_1 \ldots u_{k-1}) \xrightarrow{X} u(x) = u_0 + u_1 x + u_2 x^2 + \ldots + u_{k-1} x^{k-1}$

$\overline{c} = (c_0 c_1 \ldots c_{k-1}) \xrightarrow{X} c(x) = c_0 + c_1 x + \ldots + c_{k-1} x^{k-1}$

$$C_0 = u(x)\big|_{x=\alpha_0} = u_0 + u_1\alpha_0 + u_2\alpha_0^2 + \dots + u_{k-1}\alpha_0^{k-1}$$
$$C_1 = u(x)\big|_{x=\alpha_1} = u_0 + u_1\alpha_1 + u_2\alpha_1^2 + \dots + u_{k-1}\alpha_1^{k-1}$$
$$\vdots$$
$$C_{n-1} = u(x)\big|_{x=\alpha_{n-1}} = u_0 + u_1\alpha_{n-1} + \dots + u_{k-1}\alpha_{n-1}^{k-1}$$

$$\overline{C} = \overline{u} \cdot \overline{\overline{G}}$$

$$\overline{\overline{G}}_{k\times n} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ \alpha_0 & \alpha_1 & & & \alpha_{n-1} \\ \alpha_0^2 & \alpha_1^2 & & & \alpha_{n-1}^2 \\ \vdots & \vdots & & & \vdots \\ \alpha_0^{k-1} & \alpha_1^{k-1} & & & \alpha_{n-1}^{k-1} \end{pmatrix}$$

Miért ezekhet az együtthatókat választotta?

$$t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor \qquad d_{min} = w_{min} \nearrow \min_{\overline{C}\in G} w(\overline{C})$$

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

MDS kód

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

$$t = \left\lfloor \frac{n-k}{2} \right\rfloor$$

adott: $q-1$ akárhány hiba kiszámítható

MDS!!!

- Generátormátrix

$\alpha \in GF(q)$ ↑ primitív elem

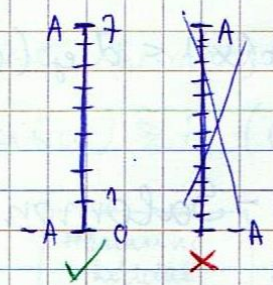
$\alpha_0 = \alpha^0 = 1$
$\alpha_1 = \alpha^1$
$\alpha_2 = \alpha^2$
$\vdots$
$\alpha_{n-1} = \alpha^{n-1}$

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

$\forall$ 2 hibát javító RS kód

$$t = 2 = \left\lfloor \frac{n-k}{2} \right\rfloor \qquad n = q-1$$

q	n	k
1	0	…
2	1	…
3	2	
7	6	2
11	10	6



minél kisebb Galois test választása a célra

$GF(7)$ ↑ 3

$$\overline{\overline{G}}_{2\times 6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}$$

- Paritás ellenőrző mátrix

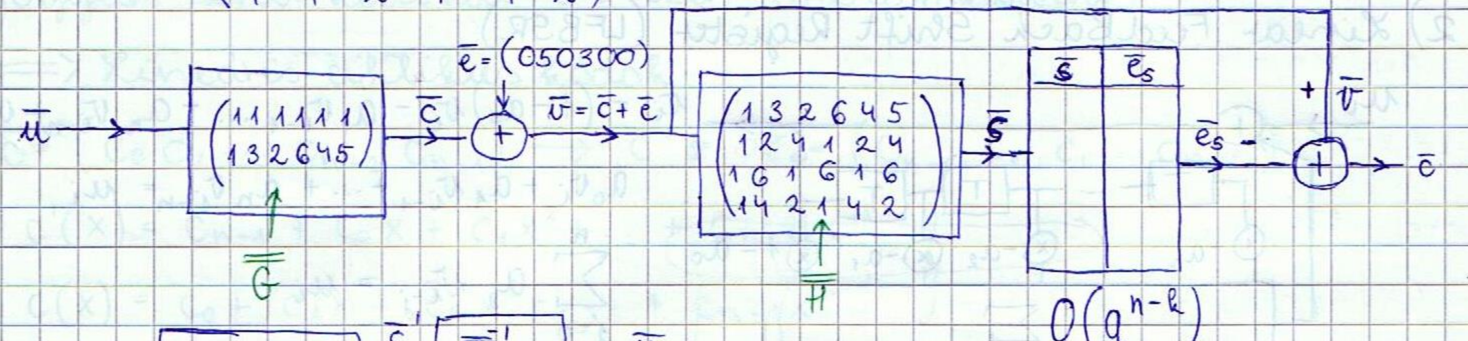
$$c(x) = c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1}x^{n-1} = \emptyset$$

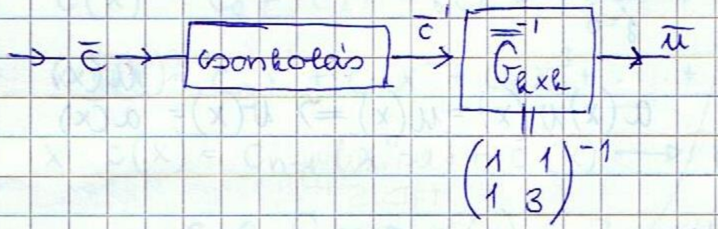
$$\overline{\overline{H}}\,\overline{C}^T = \overline{O}^T$$

$$\overline{\overline{H}}_{(n-k)\times n} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & & & & \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \dots & \alpha^{(n-k)(n-1)} \end{pmatrix}$$

GF(7) -nél maradva

$$\overline{\overline{H}}_{4\times 6} = \begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{pmatrix}$$





6. előadás

2013.10.01.

Gyakorlati kódtervezés

- Service provider megadja a javítandó hibák számát (t)

$$t = \left\lfloor \frac{n-k}{2} \right\rfloor ; \quad n = q-1 \xrightarrow{\text{iteráció}} C(n,k);\ GF(q) \rightsquigarrow \alpha \rightarrow \text{kódolási séma implementáló}$$

ZH PÉLDA

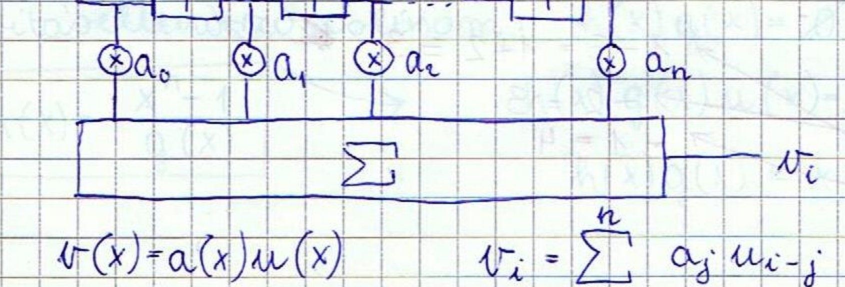
Adja meg azt a RS kódot, mely t = 3 hiba javítására alkalmas!

q	n	k
1		
2		
3		
5		
7	6	0
11	10	4

$C(10, 4) \quad GF(11)$

Shift Register

1) Linear FeedForward Shift Register (LFFSR)

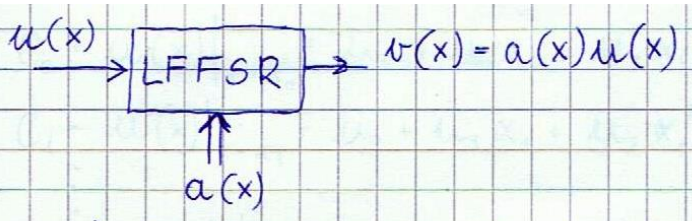


$v_0 = a_0 u_0 \qquad i = 0$

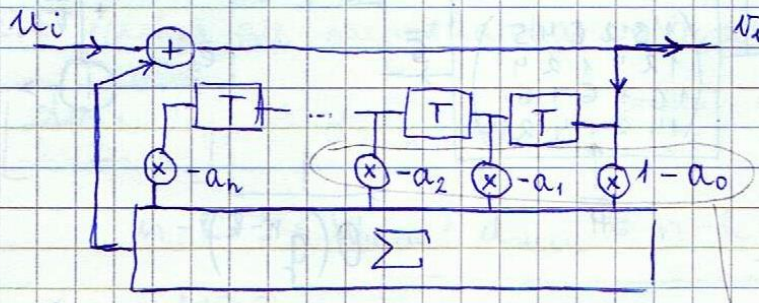
$v_1 = a_0 u_1 + a_1 u_0 \qquad i = 1$

$v_2 = a_0 u_2 + a_1 u_1 + a_2 u_0 \qquad i = 2$

$v(x) = a(x) u(x) \qquad v_i = \sum_{j=0}^{n} a_j u_{i-j}$



2) Linear FeedBack Shift Register (LFBSR)



$$v_i = (1-a_0)v_i - a_1 v_{i-1} \dots - a_n v_{i-n} + u_i$$

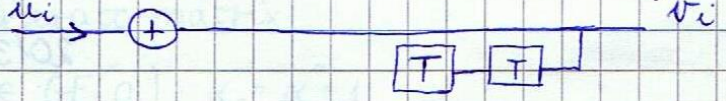
$$a_0 v_i + a_1 v_{i-1} + \dots + a_n v_{i-n} = u_i$$

$$\sum_{j=0}^{n} a_j \cdot v_{i-j} = u_i$$

$$a(x)v(x) = u(x) \Rightarrow v(x) = \frac{u(x)}{a(x)}$$

ez az egész maradék nélkül osztó

LFBSR w R ← euklideszi-algoritmus

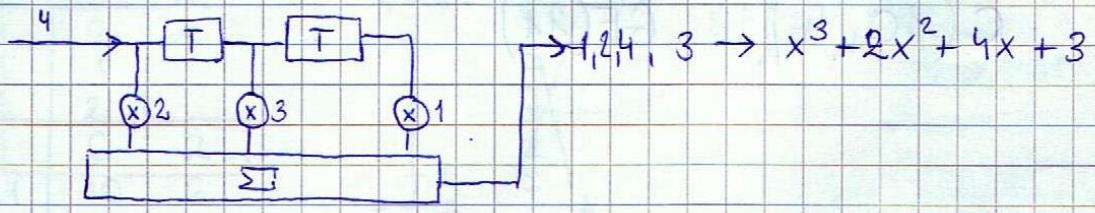


Példák

$$= x^3 + 2x^2 + 4x + 3$$

1. $(x^2 + 3x + 2)\cdot(x+4)$ szorzás elvégzése GF(5) fölött.

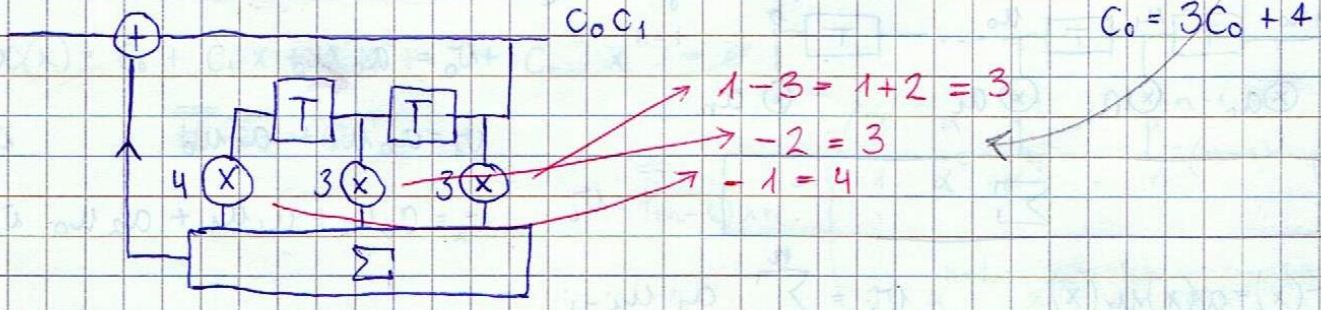
2 db késleltető → 3-adfokú polinom



2. $\frac{x^3 + 4x + 4}{x^2 + 2x + 3} = x + 3$ GF(5)

a_2 a_1 a_0 → másodfokú polinom → 2 késleltető

visszacsatolt



$c_1 = 3c_1 + 4 + 4$ $\qquad$ $c_2 = 3c_2 + 3 + 2$

$2 = 2c_1$ $\qquad$ $0 = 2c_2 \rightarrow c_2 = 0$

$c_1 = 1$

—o—

Hogyan lehet kódokat SR-eken implementálni?

$\Longrightarrow$ Lineáris ciklikus kódok

$\overline{c} = (c_0\, c_1 \cdots c_{n-2}\, c_{n-1}) \longrightarrow \overline{c}' = S\overline{c} = (c_{n-1}, c_0, c_1 \cdots c_{n-2})$

$c'(x) = c_{n-1} + c_0 x + c_1 x^2 + \ldots + c_{n-2} x^{n-1}$

$c(x) = c_0 + c_1 x + c_2 x^2 + \ldots + c_{n-1} x^{n-1}$

$x \cdot c(x) = c_0 x + c_1 x^2 + c_2 x^3 + \ldots + c_{n-1} x^n$

$x \cdot c(x) = c_{n-1}(x^n - 1) + c'(x) \longrightarrow c'(x) = x \cdot c(x) \mod x^n - 1$

$c \in G \longrightarrow c(x) \in G$

Ciklikus ha $c(x) \in G \rightarrow c'(x) = x \cdot c(x) \mod (x^n - 1) \in G$

Lineáris ha $c(x), c'(x) \in G \rightarrow \alpha \cdot c(x) + \beta \cdot c'(x) \in G$

$\forall\, c(n,k)$ lineáris ciklikus kódnál $\exists\, g(x) \rightarrow dy(g(x)) = n - k$

$\rightarrow \boxed{\forall c(x) = u(x) g(x)}$

$\rightarrow g_{n-k} = 1$

$\rightarrow g(x) \mid x^n - 1 \mod (x^n - 1)$

a kódolás REAL-TIME $\Longleftarrow$ (polinom szorzás miatt)

$\Downarrow$

SHR-en tudunk kódolni

Bizonyítás:

$a(x) \in G,\ dy(a(x)) \leq dy(c(x))\ \ \forall\, c(x) \in G;\ c(x) \neq a(x)$

$\qquad\qquad\quad \| \; r$

$(a_0 + a_1 x + \ldots + a_r x^r) \cdot a_r^{-1} \in G$

$g(x) = a_0 a_r^{-1} + a_1 a_r^{-1} x + \ldots$

$\vdots$

$\forall\, c(x) = u(x) g(x)$

Ezt a bizonyítást nem kell tudni, csak hasznos!

—o—

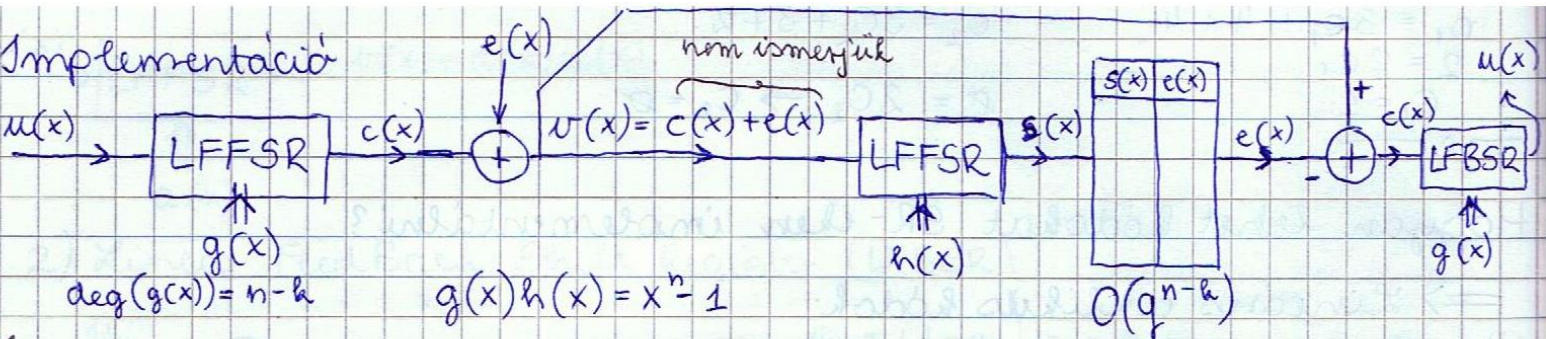
Paritásellenőrző polinom: $h(x) g(x) = 0 \mod (x^n - 1)$

$h(x) g(x) u(x) = 0$ —"—

$h(x) g(x) = x^n - 1$

$\boxed{\exists\, h(x) = \frac{x^n - 1}{g(x)}}$

Implementáció



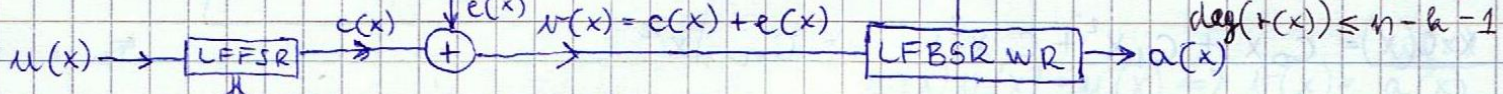
$\deg(g(x)) = n-k$ $\quad g(x)h(x) = x^n - 1$ $\quad O(q^{n-k})$

7. előadás

2013.10.08.

Error Trapping Algorithm (ETA)

- táblázat $\xrightarrow{??}$ SHR-es architektúra



maradék polinom (kisebb fokszám mint $n-k-1$)

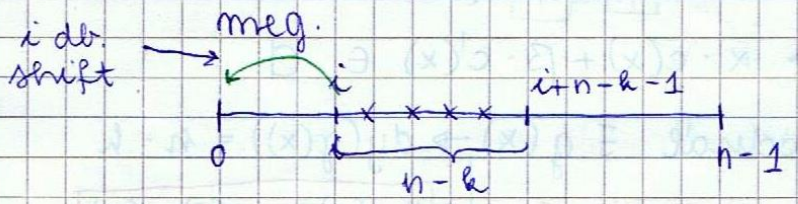
$\deg(r(x)) \leq n-k-1$

$v(x) = u(x)g(x) + e(x)$

$v(x) = a(x)g(x) + r(x)$

$\Big\} \; e(x) = r(x) \Longrightarrow$ első hiba konf.

Feltétel: a hibák a hibavektorban $n-k$ hosszúságban jelennek



az eltolás feltétele: $x^i \cdot e(x)$

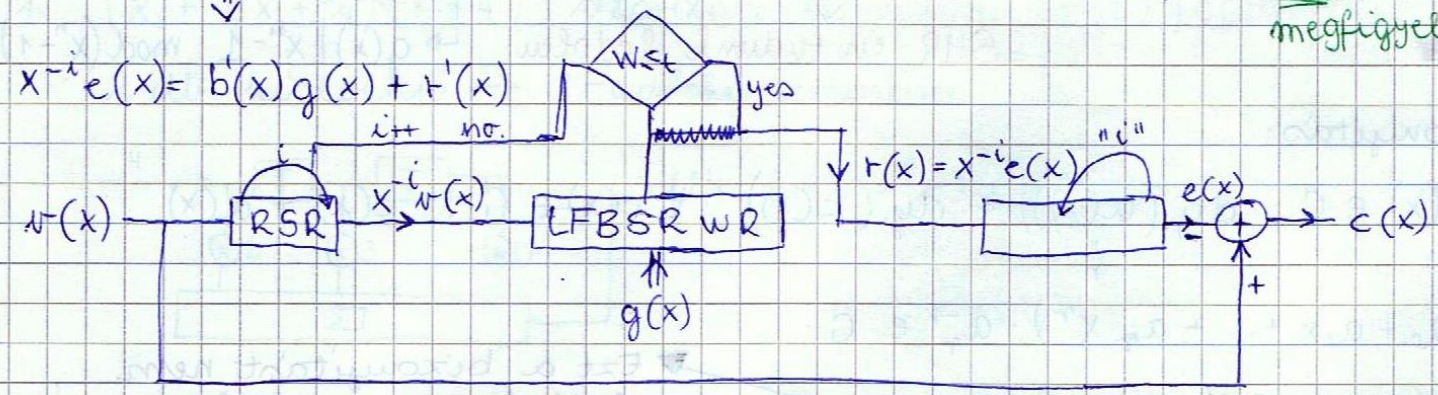
$$\begin{cases} v(x) = u(x)g(x) + e(x) \\ e(x) = b(x)g(x) + r(x) \end{cases} \quad \text{key equation}$$

$$v(x) = \big(u(x) + b(x)\big)g(x) + r(x)$$

megfigyelhető

$x^{-i} v(x) = a'(x)g(x) + r'(x)$

$x^{-i} e(x) = b'(x)g(x) + r'(x)$

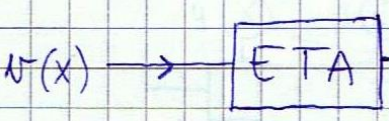


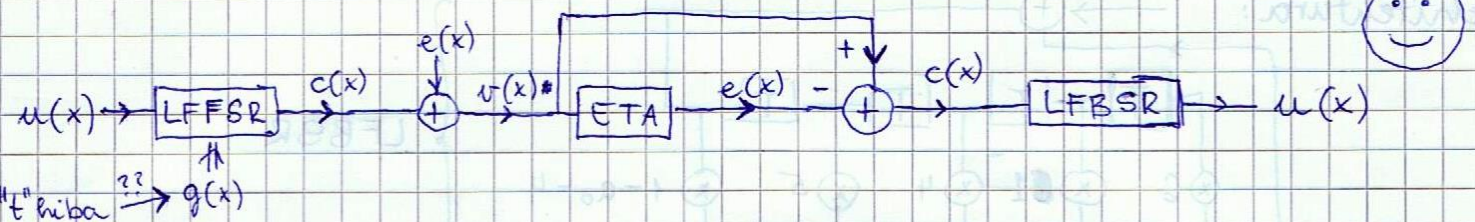
$$\underbrace{x^{-i} e(x)}_{t} - \underbrace{r'(x)}_{t+1} = \underbrace{b'(x)g(x)}_{} \in G$$

$d_{min} = w_{min} = 2t+1$

$w\big(r'(x)\big) \leq t \Longrightarrow x^{-i} e(x) - r'(x) = 0$

$r'(x) = x^{-i} e(x)$





Az RS kódok ciklikusan is implementálhatók!!!

⇓ Optimális kódok
MDS $d_{min} = n - k + 1$

$$t = \left\lfloor \frac{n-k}{2} \right\rfloor$$

⇘ Real Time és egyszerű HW platformon implementálhatók

$$c(x)\Big|_{x=\alpha^i,\ i=1\dots n-k} = c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1} = 0 \Longrightarrow c(x) = \prod_{i=1}^{n-k} (x-\alpha^i) \cdot u(x) = g(x)u(x)$$

$$g(x) = \prod_{i=1}^{n-k} (x-\alpha^i)$$

→ $\deg(g(x)) = n-k$
→ $g_{n-k} = 1$
→ $c(x) = u(x)g(x)$
→ $g(x) \mid x^n - 1$

$$x^n - 1 = \prod_{i=1}^{n} (x-\alpha^i) = \underbrace{\prod_{i=1}^{n-k} (x-\alpha^i)}_{g(x)} \underbrace{\prod_{i=n-k+1}^{n} (x-\alpha^i)}_{h(x)}$$

Példa

$t = 2$ hiba javítása $\xrightarrow[\text{ciklikus kód}]{RS}$

q	n	k
1	-	-
2	-	-
3	-	-
5	-	-
7	6	2

$C(6,2)$; $GF(7)$ felett

$3 \in GF(7)$

⇓

$g(x) = ?$

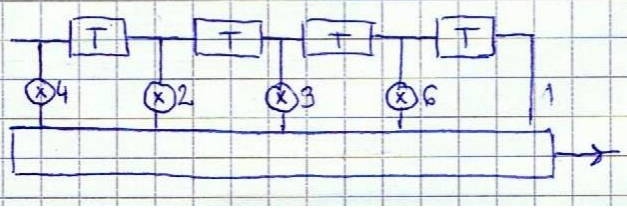
$$t = 2 = \left\lfloor \frac{n-k}{2} \right\rfloor$$

$n = q - 1$

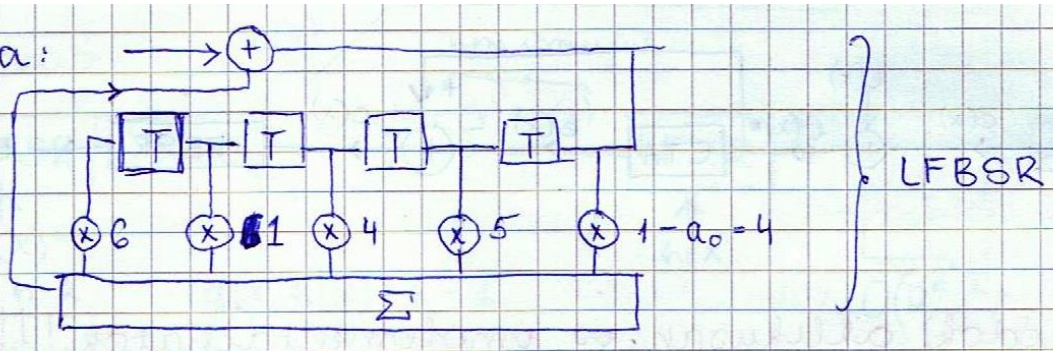
$$g(x) = \prod_{i=1}^{n-k} (x-\alpha^i) = \prod_{i=1}^{4} (x-3^1)(x-3^2)(x-3^3)(x-4) = \prod_{i=1}^{4} (x+4)(x+5)(x+1)(x+3)$$

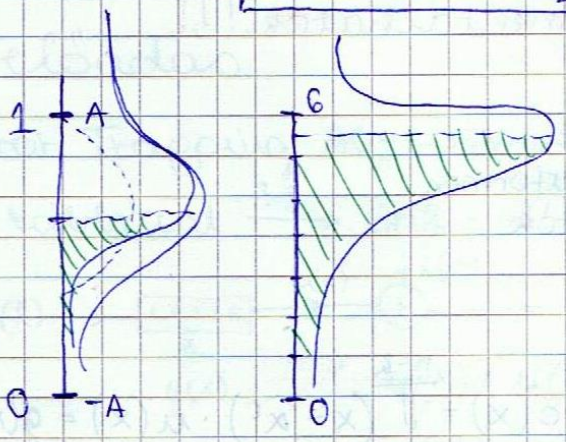
$$g(x) = (x^2 + 2x + 6)\cdot(x^2 + 4x + 3) = x^4 + 2x^3 + 6x^2 + 4x^3 + x^2 + 3x + 3x^2 + 6x + 4$$

$$= x^4 + 6x^3 + 3x^2 + 2x + 4$$ ← ez a generátorpolinom, ezt letöltve a modellre ∀ 1, 2 hiba javítására alkalmas.



Architektura:





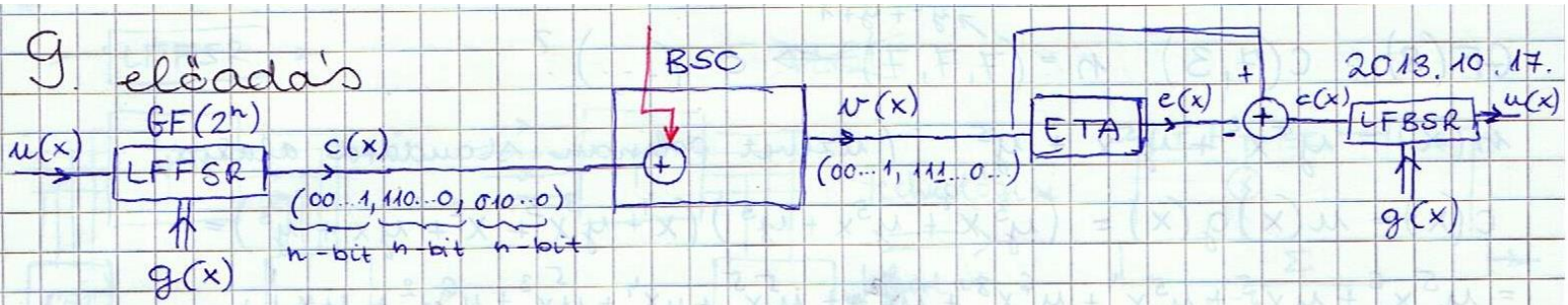
$GF(q) \wedge q$ prím

$\Downarrow$

$GF(2^n)$

9. előadás

2013. 10. 17.



Konklúzió: { Ciklikus → opt. HW
RS kód → opt. teljesítőképesség
BSC-vel történő adatátvitel → átv. tulajdonság jó
csökkenő adatátviteli sebesség

előnyök

Példa: minden 2 hibát javító kód; $\forall 2 \to t = 2$. RS ciklikus inspe.

→ $n, k, 2^m$ →

m	q	n	k
1	2^1	-	-
2	2^2	3	-
3	2^3	7	3
4	2^4	15	11

$n - k = 4$
$n = 2^m - 1$

→ azért nem ezt használjuk, mert tovább csökkentenénk az adatátviteli sebességet

→ $C(7, 3)$, $GF(8) = y$

$p(y) = y^3 + y + 1$

0	0
1	1
2	y
3	$y + 1$
4	y^2
5	$y^2 + 1$
6	$y^2 + y$
7	$y^2 + y + 1$

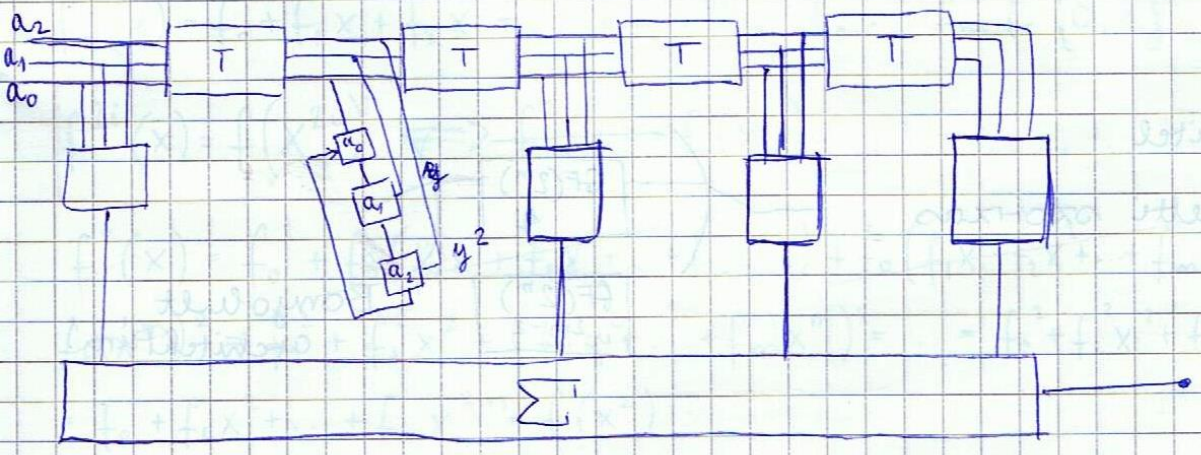
$*$	"+"
$y^{-\infty}$	0
y^0	1
y^1	y
y^2	y^2
y^3	$y + 1$
y^4	$y^2 + y$
y^5	$y^2 + y + 1$
y^6	$y^2 + 1$
y^7	1
y^8	y

$$g(x) = \prod_{i=1}^{n-k} (x - y)^i = (x+y)(x+y^2)(x+y^3)(x+y^4)$$

$$= (x^2 + y^4 x + y^3)(x^2 + y^6 x + 1) =$$

$$= x^4 + y^4 x^3 + y^3 x^2 + y^6 x^3 + y^{10} x^2 + y^2 x + x^2 + y^4 x + y^3 =$$

$$= x^4 + y^3 x^3 + x^2 + yx + y^3$$



$GF(8)$; $C(7,3)$ $\overline{n} = (7,7,7) \longrightarrow \overline{c} = (\ldots)$?

$n(x) = y^5x^2 + y^5x + y^5$ (üzenet polinom standard alakja)

$c(x) = u(x)g(x) = (y^5x^2 + y^5x + y^5)(x^4 + y^3x^3 + x^2 + yx + y^3) =$

$= y^5x^6 + yx^5 + y^5x^4 + y^6x^3 + yx^2 + y^5x^5 + yx^4 + y^5x^3 + y^6x^2 + yx +$

$+ y^5x^4 + yx^3 + y^5x^2 + y^6x + y =$

$= y^5x^6 + y^6x^5 + yx^4 + 0\cdot x^3 + 0\cdot x^2 + y^5x + y$

$\overline{c}(2,7,0,0,2,5,7) \rightarrow 010, 111, 000, 000, 010, 101, 111$

10. előadás

2013.10.17.

Hibajavító kódolás „csúcsa": adott „t" $\longrightarrow$ n, k, m

„t" ↑ Q05

m ↑ milyen $GF(2^m)$ felett kell konstruálnunk?

$n - k = 2t$ $\quad$ $n = 2^m - 1$

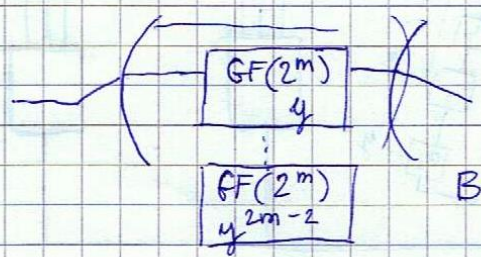
m	n	k
2		
2		
⋮		
2^m	2^m-1	k

$\longrightarrow C_{RS}(n,k)$; $GF(2^m) \ni y$

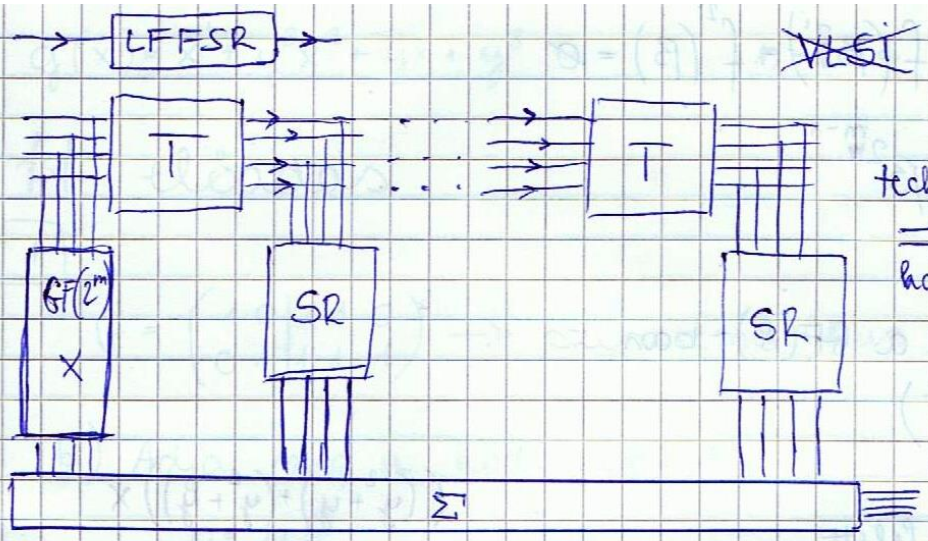
$g(x) = \prod_{i=1}^{n-k} (x - y^i) \Longrightarrow g(x) = y^{i_0} + y^{i_1}x + y^{i_2}x^2 + \ldots + 1\cdot x^{n-k}$

- Opt. kód
- Opt. HW
- Bináris átvitel

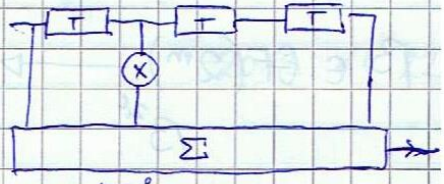
- A $GF(2^m)$ feletti szorzás



Bonyolult architektúra.



technológiai határ



$$g(x) = \sum_{i=0}^{n-k} g_i x^i$$

$$g_i \in \{0, 1\}$$

- „t" hiba javítása → $\overline{H}$-ban $2t$ lin. fgtlu oszlopvektor kiválasztható

$$c(x) = g(x)\,u(x) \rightarrow c(x)\Big|_{x=y^i,\, i=1,2\ldots t} = 0$$

$$g(x)\Big|_{x=y^i} = 0$$

$$c_0 + c_1 y + c_2 y^2 + \ldots + c_{n-1} y^{n-1} = 0$$

$$c_0 + c_1 y^2 + c_2 y^4 + \ldots + c_{n-1} y^{2(n-1)} = 0$$

$$\vdots$$

$$c_0 + c_1 y^{2t} + c_2 y^{4t} + \ldots + c_{n-1} y^{2t(n-1)} = 0$$

$$\Longrightarrow \quad \overline{H} = \begin{pmatrix} 1 & y & y^2 & \ldots & y^{n-1} \\ 1 & y^2 & y^4 & \ldots & y^{2(n-1)} \\ \vdots & & & & \vdots \\ 1 & y^{2t} & y^{4t} & \ldots & y^{2t(n-1)} \end{pmatrix}$$

VLSI implementáció „t" hiba javítására alkalmas

$g(x)$ → „szegény" együtthatók $g_i \in \{0,1\}$ $\forall i = 0 \ldots n-k$

→ „gazdag" gyökök $GF(2^m)$-ben konjugált gyökcsoportok

Minimálpolynomok $GF(2)$ felett

$$f_*(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_m x^m \quad ; \quad f_0, \ldots f_m \in \{0,1\}$$

$$\boxed{f^{2i}(x) = f(x^{2i})} \Longrightarrow f^2(x) = f(x^2)$$

$$f^2(x) = f_0^2 + f_0(f_1 x + f_2 x^2 + \ldots + f_m x^m) + f_0(f_1 x + f_2 x^2 + \ldots + f_m x^m) + (f_1 x + f_1 x^2 + \ldots + f_m x^m)^2 = f_0^2 + f_1^2 x^2 + (f_2 x^2 + \ldots + f_m x^m)^2 = \ldots = f_0^2 + f_1^2 x^2 + f_2^2 x^4 \ldots + f_m^2 x^{2m} =$$

$$= f_0 + f_1 x^2 + \ldots + f_m x^{2m} = f(x^2)$$

$f(\beta) = 0 \quad f(\beta^{2^i}) = 0 \longrightarrow f(\beta^{2^i}) = f^{2^i}(\beta) = 0$

$\beta \in GF(2^m) \longrightarrow \beta^{2^m} = \beta\beta^{2^{m-1}}$

β^{2^i}

Konjugált gyökcsaládok a GF(8)-ban

$(y; y^2; y^4), \quad (y^3; y^6; y^5)$

$((y^2+y)+(y^2+y))x$

Minimál polinom GF(2) felett

$\Phi_i(x)$ min. deg $f(x)$ $\qquad (y^i, y^{2i}, y^{4i} \ldots)$

$$\Phi_1(x) = (x+y)(x+y^2)(x+y^4) = (x^2+y^4x+y^3)(x+y^4) =$$
$$= x^3 + y^4x^2 + y^3x + y^4x^2 + yx + y^7 = x^3 + x + 1 = 1\cdot x^3 + 0\cdot x^2 + 1\cdot x + 1$$

$$\Phi_3(x) = (x+y^3)(x+y^5)(x+y^6) = (x^2+y^2x+y)(x+y^6) =$$
$$= x^3 + y^2x^2 + yx + y^6x^2 + yx + 1 = x^3 + x^2 + 1 = 1\cdot x^3 + 1\cdot x^2 + 0\cdot x + 1$$

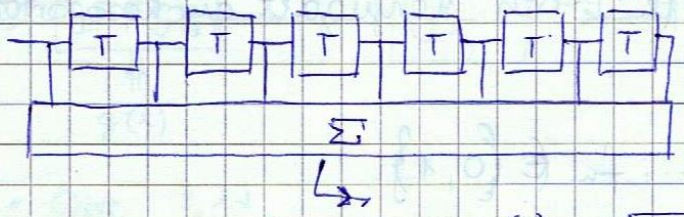
Bose - Chaudhari - Hocquenghem (BCH) kódok

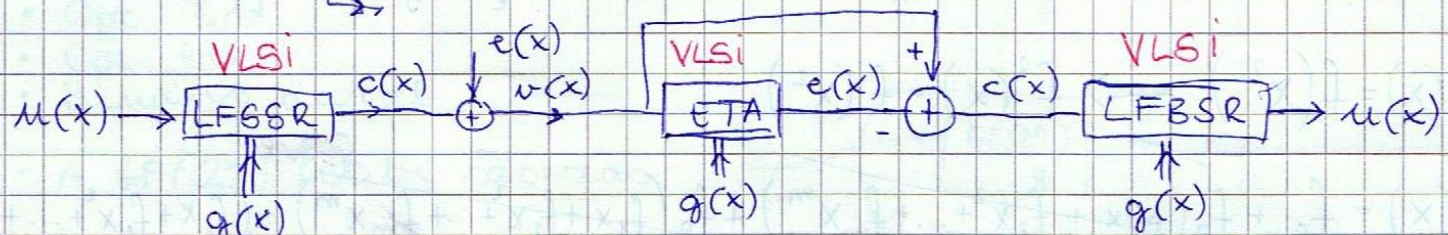
adott „t" $\longrightarrow g(x) = \Phi_1(x)\,\Phi_3(x) \ldots \Phi_{2t-1}(x) \longrightarrow g_j \in \{0,1\}\ \forall j$

$\forall$ 2 hiba javítása $2t-1 = 3 \longrightarrow g(x) = \Phi_1(x)\,\Phi_3(x) = (x^3+x+1)(x^3+x^2+1) =$

$$= x^6 + x^4 + x^3 + x^5 + x^3 + x^2 + x^3 + x + 1 = x^6 + x^5 + x^3 + x^4 + x^2 + x + 1$$

(generátorpolinom)





$\deg(g(x)) = n - k$

$n = 2^3 - 1 = 7$

$C_{BCH}(7;1)$

adatátviteli sebesség csökken

$g(x) = x^4 + y^3x^3 + yx + y^3$ $\quad n-k=4$ $\quad C_{RS}(7,3)$

11. előadás

2013. 11. 22

1

$$G = \left(\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{array}\right) \rightarrow \text{szisztematikus kód}$$

b) Adja meg a kódszavakat!

$c = uG$

u	$c = uG$	w
0 0	0 0 0 0 0	–
0 1	0 1 1 1 1	4
1 0	1 0 1 1 0	3
1 1	1 1 0 0 1	3

c) Hány hibát tud javítani a kód?

Lineáris kód $\rightarrow$ $d_{min} = w_{min} = 3$

$t = ?$ $\quad t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 1$ hiba javítására alkalmas

d) Adja meg a paritásellenőrző mátrixot!

$H G^T = 0$ $\quad G(I_{k\times k}; B) \rightarrow H = (A, I)$

$A = B^T$

$$H = \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{array}\right)$$

e) $e = (1\,1\,1\,1\,1)$

$s^T = He^T$ $\quad (s = eH^T)$

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

→ Eleinegelben mod2-zem a sorokat

$E_{(110)} = \{e, e+c^{(1)}, e+c^{(2)}, e+c^{(3)}\} =$

$= \{(11111), (10000), (01001), (00110)\}$

2 $G = \begin{pmatrix} 1 0 1 1 1 \\ 0 1 1 1 0 \end{pmatrix}$ $\quad e = (0\,1\,1\,0\,0)$

a) $S = eH^T$

$H = \left(\begin{array}{cc|ccc} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 1 \end{array}\right)$

$S = (0\,1\,1\,0\,0)\,(H^T)\,(0\,1\,0)$

u	$c = uG$
00	00000
01	01110
10	10111
11	11001

$E_{(010)} = \{ e,\ e + c^{(1)} \ldots \} =$

$= \{ 01100,\ 00010 \rightarrow e' \text{ mert } w_{min},\ 11011,\ 10101 \}$

3 $G = \left(\begin{array}{ccc|cc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right)$

a) Különböző hibacsoportban van-e $e_1 = (10000)$ $e_2 = (00001)$

$S = eH^T$

$S_1 = e_1 H^T = (10000)\,(01)$

$H = \left(\begin{array}{ccc|cc} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{array}\right)$

$\begin{pmatrix} 01 \\ 10 \\ 11 \\ 10 \\ 01 \end{pmatrix}$ $S_1 = S_2$

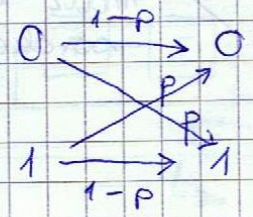
$S_2 = e_2 H^T = (01)$

b) Lehetnek-e csoportvezetők?

Igen lehetnek mert $\emptyset$ súly nem értelmezett és a kör. legkisebb súly az 1!

c) $p = 0{,}2$

$p(e_2) = (1-p)^4 \cdot p = 0{,}2 \cdot 0{,}8^4 = 0{,}0819$



4 Szorzatkód

$G = \left(\begin{array}{ccccc} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{array}\right)$

a) Szorzatkód típusa

$C_{eredeti}$: $\{ c(5, 3) \}$ $\quad C_{szorzat}$: $C \times C = c(25, 9)$

$n = n_1 \cdot n_2$

$k = k_1 \cdot k_2$

$d_{min} = d_{min1} \cdot d_{min2} = w_{min}^2$

u	c = uG	w
000	00000	
001	00110	2
010		
011		
100		
101		
111	11100	

$$d_{min} = 2^2 = 4$$

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

c)

$$u = \begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix} \qquad C = \left(\begin{array}{ccc|cc} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 \\ \hline 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

6

a) Hatvány 3×4 a $GF(8)$-ban?

$GF(8) = GF(2^3)$

$P(y) = y^3 + y + 1$

Hatványtáblából ↑

$3 = (011) = y + 1 = y^3$

$4 = (100) = y^2$

$(y+1)y^2 = y^3 + y^2 =$

$= 1 \cdot (y^3 + y + 1) + \underbrace{y^2 - y - 1}_{(111) = 7}$

Hatványtábla mod $P(y)$

y^0	1
y^1	y
y^2	y^2
y^3	$y + 1$
y^4	$y^2 + y$

$\frac{y^4}{y^3} = y_1 \quad y^4 - y\,P(y) = y^2 + y$

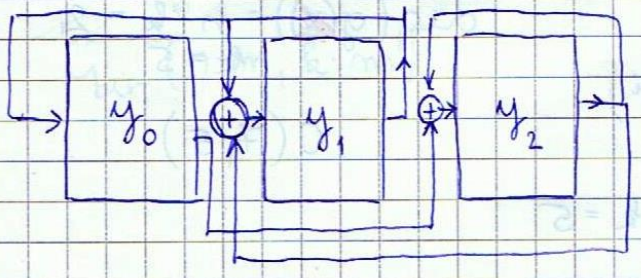
$3 \times 4 = y^3 y^2 = y^5 = y^2 + y + 1$

$(111) = 7$

b) Rajzold le az SHR-t!

$4 \times \frac{}{} = y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 y^3 + a_2 y^4 =$

$= a_0 y^2 + a_1(y+1) + a_2(y^2 + y) = a_1 y^0 + (a_1 + a_2) y^1 + (a_0 + a_2) y^4$



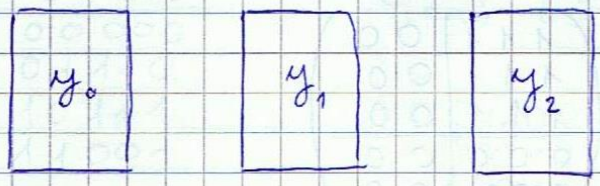
6 a) Mennyi 5×2 $GF(8)$ felett?

$5 = (101) = y^2 + 1 = y^6$

$2 = (010) = y$

$5 \times 2 = y^6 y = y^7 = 1$

b) $2x = y(a_0 + a_1 y + a_2 y^2) = a_2 y^0 + (a_0 + a_2) y^1 + a_1 y^2$ ← elatolgatótábla!!



7 $GF(8) = GF(2^3)$ $\quad t = 2$ $\quad$ MDS: $d_{min} = n - k + 1$

q

$n = q - 1 = 7$ $\quad t = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor \Rightarrow \underline{\underline{k = 3}}$

$$h(x) = \prod_{i=n-k+1}^{n} (x - y^i) = (x - y^5)(x - y^6)(x - y^7) =$$

$$= x^2 + y^6 x + y^5 x + y^{11})(x + 1) =$$

$$= (x^2 + yx + y^2 + y)(x + 1) = x^3 + x^2 y + x y^2 + \cancel{xy} + x^2 + \cancel{xy} + y^2 + y =$$

$$= x^3 + \underbrace{(y+1)}_{y^3} x^2 + y^2 x + \underbrace{(y^2 + y)}_{y^4}.$$

8 $g(x) = \prod_{i=1}^{n-k} (x - y^i) = (x - y)(x - y^2) = x^2 + x\underbrace{(y^2 + y)}_{y^4} + y^3$

$h(x) = \prod_{i=n-k+1}^{n} (x - y^i) \quad \deg(h(x)) = k = 5$

$1 = t = \left\lfloor \frac{n-k}{2} \right\rfloor \Rightarrow k = 5$

9 $n = q - 1 = 7$ $\quad \deg(g(x)) = n - k = 2$

$g(x) = x^2 + x y^4 + y^3 = \prod_{i=1}^{n-k} (x - y^i)$ $\quad k = 5$

$C(7, 5)$

$t = \left\lfloor \frac{n-k}{2} \right\rfloor = 1$ $\quad \deg(h(x)) = k = 5$

12. előadás

2013.10.29.

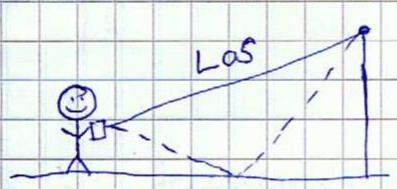
„Burstay" hibák javítása

000,110110010011,000

be

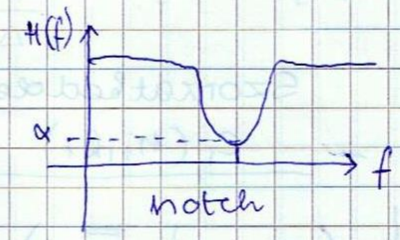
Anyaghibák javítására használják főleg → adattároló eszközök

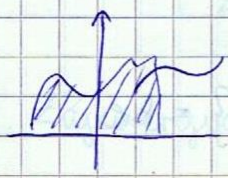
Wireless kommunikáció



Multipath propagation

$H(f) = 1 - \rho e^{-j2\pi f\tau}$





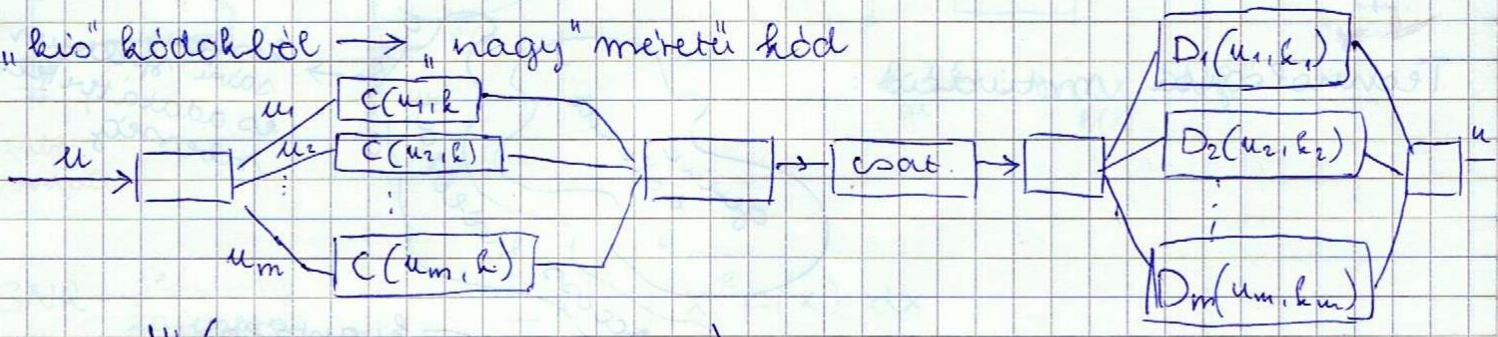
$C(n,k) \rightarrow \left\lfloor \frac{n-k}{2} \right\rfloor$

$C(n,k) \rightarrow be \leq \left\lfloor \frac{n-k}{2} \right\rfloor$

→ nagy „n-k" → $GF(2^m)$

Kódkombinációk

„kis" kódokból → „nagy" méretű kód



$d_{min} = \Psi(d_{min_1}, d_{min_2} \dots d_{min_m})$

1.) Bináris képkód

$C(n,k)$ a $GF(2^m)$ felett

↓

$C_{bin}(n \cdot m, k \cdot m)$

$m \cdot t = be$ ← javítható hibák száma

λ" paraméterű interleaving

$C(n,k)$ szint

$$\bar{\bar{C}} = \left(\begin{array}{c|c} \bar{\bar{u}}_{\lambda\times k} & \bar{\bar{P}}_{\lambda\times(n-k)} \end{array}\right) \begin{matrix}1\\2\\\vdots\\\lambda\end{matrix}$$

$bl = \lambda \cdot t$ → oszloponként átvitel → sorankénti detektálás

Szorzatkódolás

$c_1(n_1,k_1)$ →

$c_2(n_2,k_2)$ ↓

$$\left(\begin{array}{c|c} \bar{\bar{u}}_{\lambda\times k} & \bar{\bar{P}}_1 \\ \hline \bar{\bar{P}}_2 & \bar{\bar{P}}_{12} \end{array}\right) = \bar{\bar{C}}$$

$k = k_1 \cdot k_2$

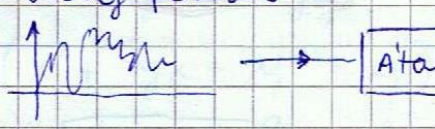
$n = n_1 \cdot n_2$

$\max\{n_2 \cdot t_1 + t_2 \,;\, n_1 \cdot t_2 + t_1\} = be$

függ az átv. műv. del

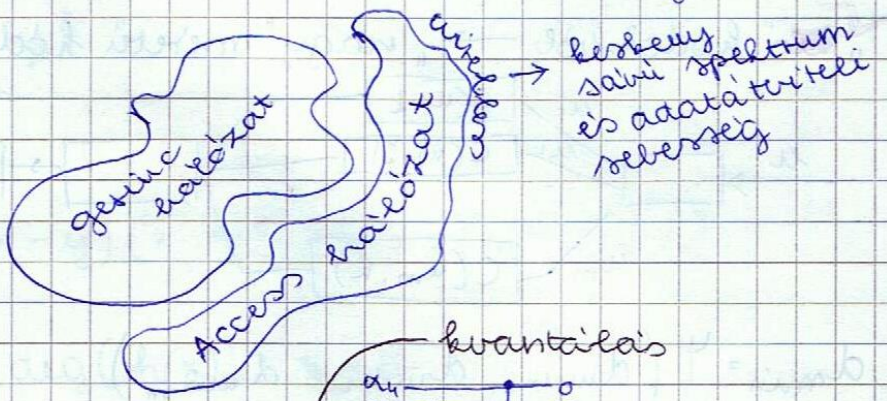
FORRÁSKÓDOLÁS - ADATTÖMÖRÍTÉS

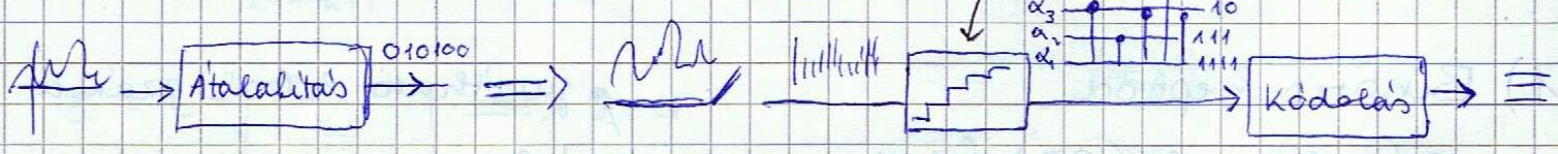
Analóg forrás

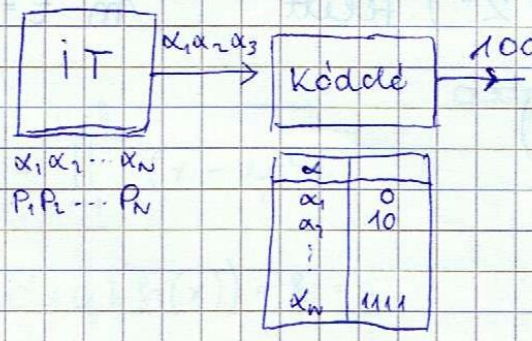


→ időegység alatt min. számú átlagos bit

Technológiai motiváció:







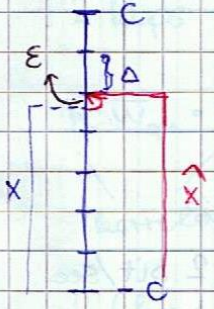
min. adatátv. sebesség

$$P(X_t = x_i \mid X_{t-1} = x_j \;\; X_{t-2} = x_n \dots) = P(X_t = x_i)$$

Kvantálás 13. előadás

2013. 10. 31.

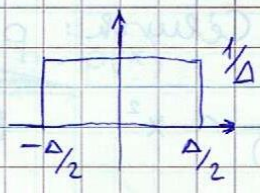
I. Egyenletes kvantálás



$$N = \frac{2C}{\Delta} = 2^n \qquad \varepsilon \in \left[-\frac{\Delta}{2}, \frac{\Delta}{2}\right]$$

kvantálási zaj

$$f_\varepsilon(u) = \frac{1}{\Delta}$$

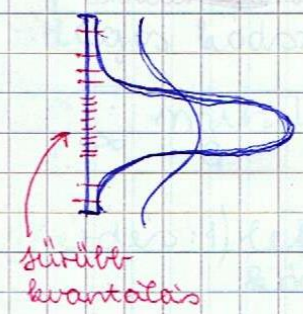


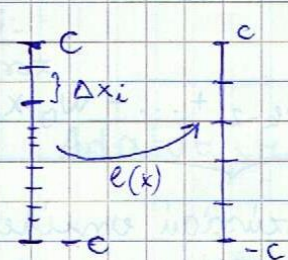
$$SNR = \frac{\text{Jelenergia}}{\text{Zajenergia}} \qquad \text{Jelenergia: } \frac{C^2}{2}$$

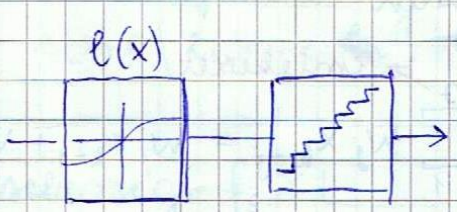
$$\text{Zajenergia: } \mathbb{E}(\varepsilon^2) = \int_{-\frac{\Delta}{2}}^{\Delta/2} u^2 f_\varepsilon(u)\,du = \int_{-\frac{\Delta}{2}}^{\Delta/2} u^2 \frac{1}{\Delta}\,du = \frac{\Delta^2}{12}$$

$$SNR = \frac{C^2/2}{\Delta^2/2} = 6\frac{C^2}{\Delta^2} = \frac{3}{2}\left(\frac{2C}{\Delta}\right)^2 = \frac{3}{2}N^2 \Longrightarrow \boxed{SNR = \frac{3}{2}2^{2n}}$$

PL.:







$$\ell_{opt}(x): \max_{\ell(x)} SNR$$

$$SNR = \frac{\text{jelenerg}}{\text{zajenerg}} \qquad \mathbb{E}x^2 = \int_{-C}^{C} x^2 p(x)\,dx$$

↑ beszédminta sűrűségfüggvénye

$$\text{Zajenergia: } \frac{\Delta y}{\Delta x_i} = \ell'(x_i) \longrightarrow \Delta x_i = \frac{\Delta y}{\ell'(x_i)} = \frac{2C}{N \cdot \ell'(x_i)}$$

$$\sum_i \underbrace{\mathbb{E}(\text{zajenergia} \mid x \in \Delta x_i)}_{\frac{\Delta x_i^2}{12}} p(x_i)\Delta x_i = \sum_i \frac{\Delta x_i^2}{12} p(x_i)\Delta x_i =$$

$$= \sum \frac{N^2}{24C^2} \cdot \frac{1}{\ell'^2(x_i)} p(x_i)\Delta x_i = \text{const} \int_{-C}^{C} \frac{1}{\ell'^2(x)}\,dx$$

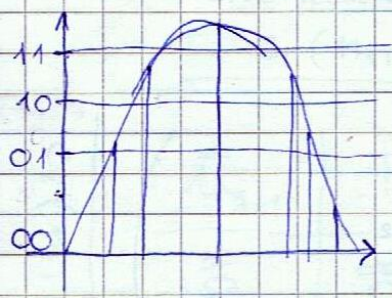
$$\ell_{opt}(x): \max_{\ell(x)} \frac{\int_{-c}^{c} x^2 p(x)\,dx}{\text{const} \int_{-c}^{c} \frac{1}{\ell'^2(x)} p(x)\,dx}$$

$p(x)$ időben folyamatosan változik

$\Longrightarrow$ Célunk: $p(x)$-től független

$$\frac{1}{\ell'^2(x)} \sim x^2 \qquad \ell'(x) \sim \frac{1}{x} \rightarrow \ell(x) \sim \log(x)$$

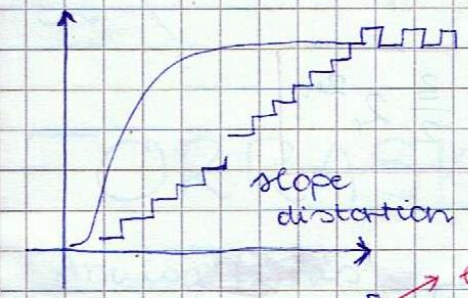
Delta modulátor



00 01 10 11 10 01 00 = 14 bit f_s: 2 bit/sec

00 1 1 1 1 0 0 = 8 bit f_s: bit/sec

$f_s' > f_s \Longrightarrow f_s' \ll f_s n$



Kétek egy palack sö → ht - nagy vgű → rövid kódszó

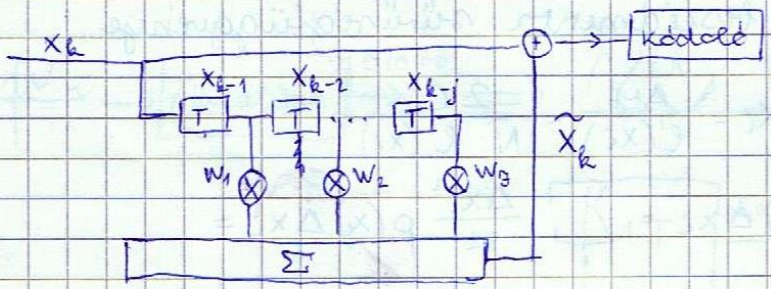
→ tét gépolajat. - kis vgű → hosszú kódszó

emlékezet

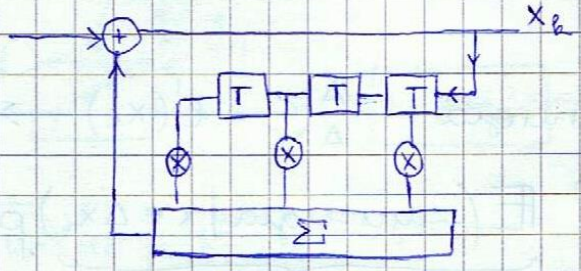
$$x_i \rightarrow \tilde{x}_k = \sum_{j=1}^{J} w_j x_{k-j} = \underbrace{w_1 x_{k-1} + w_2 x_{k-2} + \ldots + w_J x_{k-J}}_{\text{"J" hosszúságú emlékezet}}$$

$$\overline{w}_{opt}: \min_{\overline{w}} \mathbb{E}\left(\underbrace{x_k - \tilde{x}_k}_{\varepsilon_k}\right)^2 \sim \min_{\overline{w}} \mathbb{E}\left(x_k - \sum_{j=1}^{J} w_j x_{k-j}\right)^2$$

ADÓ



VEVŐ



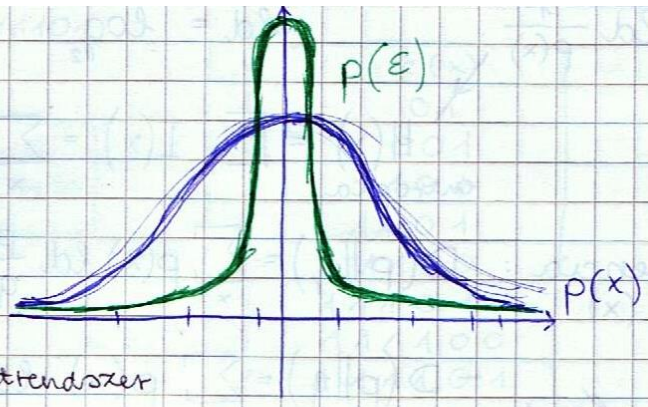
$$\varepsilon_i = x_i - \sum_{j=1}^{J} w_j x_{k-j} \qquad x_k = \varepsilon_k + \sum_{j=1}^{J} w_j x_{k-j}$$

$$\overline{w}_{opt} = \overline{\overline{R}}\,\overline{w} = \overline{r}$$

$W_{opt}: \min_{\overline{w}} E(\varepsilon_k^2)$

$L' << L = \sum_i p_i l_i$

5.2 kbps 6.4 kbps



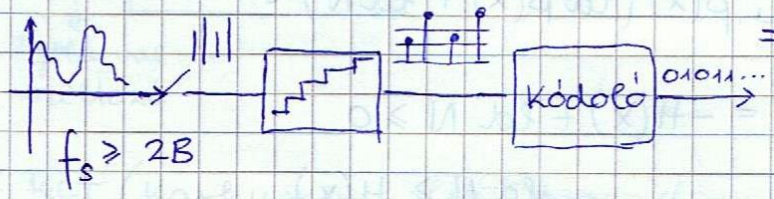
$\overline{R}\,\overline{w}_{opt} = \overline{r}$ → lineáris egyenletrendszer

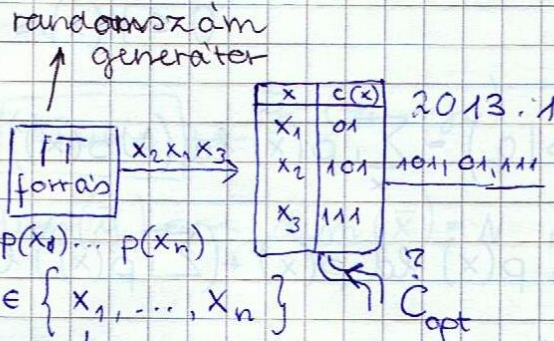
korrelációs

$w_e(k+1) = w_e(k) - \Delta \left\{ x_e - \sum_{j=1}^{7} \right.$

14. előadás

2013. 11. 05.





$c(x) \in \{\overline{c}_1 \dots \overline{c}_n\}$ → kódszó

$l(x) \in \{l_1, \dots l_n\}$ → kódszóhossz

$$L = \sum_x p(x)\, l(x)$$

átlagos kódszóhossz

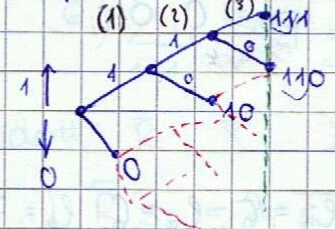
$C_{opt}: \min_C L$ Adatátviteli sebesség: $f_s \cdot L$

Kérdés: 1) Lehet-e egyértelműen dekódolni változó hosszúságú kódszavakat?

2) Hogyan kell úgy megválasztani a kódszavakat, hogy L minimális legyen?

Prefix mentes kód: $\overline{c}_i \not\prec \overline{c}_j$ $\overline{c}_i(01)$, $\overline{c}_j(01111)$

Prefix kódot bináris fával növeszthetek:



„M" növesztésű fa

$2^{M-l(x)}$ pl.: $2^{3-?} = 2$

$$\sum_x 2^{M-l(x)} \leq 2^M \Rightarrow 2^M \sum_x 2^{-l(x)} \leq 2^M$$

Kraft egyenlőtlenség

$$\sum_x 2^{-l(x)} \leq 1$$

$I(x) = \operatorname{ld} \frac{1}{p(x)}$ $\qquad \operatorname{ld} := \log_2$

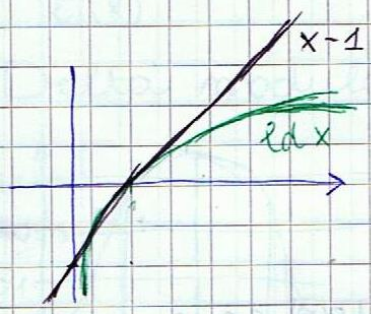
$H(x) = \mathbb{E}_x I(x) = \sum_x p(x) \operatorname{ld} \frac{1}{p(x)} = -\sum_x p(x) \operatorname{ld} p(x)$

entrópia

I-divergencia: $D(p\|q) = \sum_x p(x) \operatorname{ld} \frac{p(x)}{q(x)} \geq 0$

$p(x)$, $q(x)$

$$-D(p\|q) = \sum_x p(x) \operatorname{ld} \frac{q(x)}{p(x)} \leq \sum_x p(x) \left(\frac{q(x)}{p(x)} - 1 \right) =$$



$$= \sum_x \left(q(x) - p(x) \right) = \sum_x q(x) - \sum_x p(x) = 1 - 1 = \emptyset$$

$$0 \leq H(x) \leq \operatorname{ld} N$$

$$D(p\|q) = \sum_x p(x) \operatorname{ld} (N p(x)) = \sum p(x) \left(\operatorname{ld} p(x) + \operatorname{ld} N \right) =$$

$$= \sum p(x) \operatorname{ld} p(x) + \left(\sum p(x) \right) \operatorname{ld} N = -H(x) + \operatorname{ld} N \geq 0$$

$$\operatorname{ld} N \geq H(x)$$

Shannon-Fano kódd (SF)

$l(x) = \left\lceil \operatorname{ld} \frac{1}{p(x)} \right\rceil$ $\qquad \lceil 3{,}1 \rceil = 4$ $\qquad a \leq \lceil a \rceil \leq a + 1$

$$\hookrightarrow \sum 2^{-l(x)} = \sum 2^{-\left\lceil \operatorname{ld} \frac{1}{p(x)} \right\rceil} \leq \sum_x 2^{-\operatorname{ld} \frac{1}{p(x)}} = \sum 2^{\operatorname{ld} p(x)} = \sum p(x) =$$

$= 1$

$$L = \sum_x p(x) \, l(x) = \sum_x p(x) \cdot \left\lceil \operatorname{ld} \frac{1}{p(x)} \right\rceil \geq \sum_x p(x) \operatorname{ld} \frac{1}{p(x)}$$

$$\leq \sum_x p(x) \left(\operatorname{ld} \frac{1}{p(x)} + 1 \right) = \sum p(x) \operatorname{ld} \frac{1}{p(x)} = \ldots =$$

$$= H(x) + 1$$

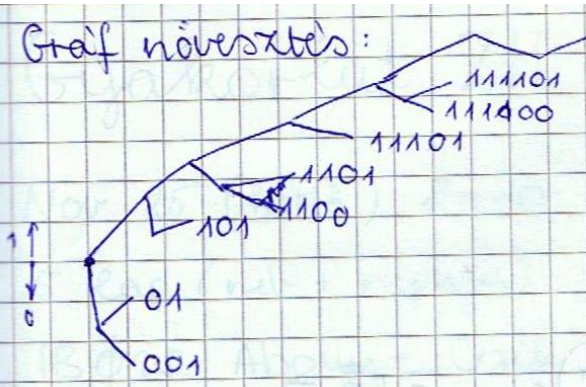
Numerikus példa

$p_1 = 0{,}49$; $p_2 = 0{,}14$; $p_3 = 0{,}14$; $p_4 = 0{,}07$; $p_5 = 0{,}07$; $p_6 = 0{,}04$;

$p_7 = 0{,}02$; $p_8 = 0{,}02$; $p_9 = 0{,}01$

$l_1 = \left\lceil \operatorname{ld} \frac{1}{p_1} \right\rceil = 2$; $l_2 = 3$; $l_3 = 3$; $l_4 = 4$; $l_5 = 4$; $l_6 = 5$, $l_7 = 6$, $l_8 = 6$, $l_9 = 7$

Gráf növesztés:



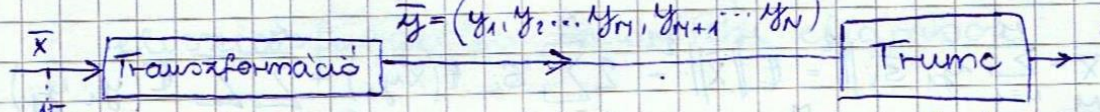
1T forrás

x	c(x)
1	01
2	001
3	101
4	1101
5	1100
6	111101
7	111100
8	111101
9	1111101

X. előadás

2013.11.19.

Veszteséges adattömörítés algoritmusa



fgtlen val. változó

$M = \dim(\bar{y}) \ll \dim(\bar{x}) = N$

KLT (Karhunen - Loéve transzform.)

$R_{ij} = \mathbb{E}(x_i, x_j) \longrightarrow \bar{\bar{R}} = \mathbb{E}(\bar{x}\,\bar{x}^T)$

$\bar{\bar{R}}$ tulajdonságai

1) $R_{ij} = R_{ji} \longrightarrow \bar{\bar{R}} = \bar{\bar{R}}^T$

2) $\forall \bar{a}, \bar{b} \in \mathbb{R}^N \longrightarrow \bar{a}^T \bar{\bar{R}} \bar{b} = \bar{b}^T \bar{\bar{R}} \bar{a}$

3) $\forall \bar{a} \in \mathbb{R}^N \rightarrow \bar{a}^T \bar{\bar{R}} \bar{a} \geq \phi \longrightarrow \sum_i \sum_j a_i a_j R_{ij} = \sum_i \sum_j a_i a_j \mathbb{E}(x_i x_j) =$

$= \mathbb{E}\left(\left(\sum_i a_i x_i\right)\left(\sum_j a_j x_j\right)\right) = \mathbb{E}\left(\sum_i x_i a_i\right)^2 \geq 0$

4) $\bar{\bar{R}}\,\bar{s}_i = \lambda_i \bar{s}_i \quad i = 1 \ldots N \rightarrow \bar{s}_i^T \bar{s}_j = s_{ij} = \begin{cases} 0 & \text{ha } i \neq j \\ 1 & \text{ha } i = j \end{cases}$

5) $\lambda_i \geq \phi$

6) $\sum_{i=1}^{N} R_{ii} = \sum_{i=1}^{N} \lambda_i$

Adott: $\bar{\bar{R}}$; $\bar{x}$

1) $\bar{\bar{R}}\,\bar{s}_i = \lambda_i \bar{s}_i \longrightarrow \lambda_1 > \lambda_2 \ldots > \lambda_M > \lambda_{M+1} \ldots > \lambda_N$

2) $\bar{x} = \sum_{i=1}^{N} y_i \bar{s}_i \; ; \; y_i = \bar{s}_i^T \bar{x} \quad i = 1 \ldots N$

$\bar{x} \longrightarrow \hat{\bar{y}} = (y_1, y_2 \ldots y_M, \cancel{y_{M+1} \ldots y_N})$

3) Tömörítés $\bar{y} = (y_1 \dots y_M)$

4) $\frac{1}{x} = \sum_{i=1}^{M} y_i \bar{s_i}$

Optimalitás

$$\mathbb{E}(y_i y_j) = \mathbb{E}(\bar{s_i}^T \bar{x} \bar{x}^T \bar{s_j}) = \bar{s_i}^T \overbrace{\mathbb{E}(\bar{x} \bar{x}^T)}^{\bar{\bar{R}}} \bar{s_j} = \bar{s_i}^T \bar{\bar{R}} \bar{s_j} =$$

$$= \lambda_j \bar{s_i}^T \bar{s_j} = \lambda_i s_{ij}$$

$$\mathbb{E}(\bar{x} y_i) = \mathbb{E}(\bar{x} \bar{x}^T \bar{s_i}) = \mathbb{E}(\bar{x} \bar{x}^T) \bar{s_i} = \bar{\bar{R}} \bar{s_i} = \lambda_i \bar{s_i}$$

———o———

$$\mathbb{E} \| \bar{x}^* - \hat{\bar{x}} \|^2 = \mathbb{E} \| \bar{x} - \sum_{i=1}^{M} y_i \bar{s_i} \|^2 = \mathbb{E} \|\bar{x}\|^2 - 2 \sum_{i=1}^{M} \bar{s_i}^T \mathbb{E}(\bar{x} y_i) + \sum_{i=1}^{M} \sum_{j=1}^{M} \mathbb{E}(y_i y_j)$$

$$\bar{s_i} \bar{s_j}^T = \sum_{i=1}^{N} \lambda_i - 2 \sum_{i=1}^{M} \bar{s_i}^T \lambda_i \bar{s_i} + \sum_{i=1}^{M} \lambda_i \bar{s_i}^T \bar{s_i} = \sum_{i=1}^{N} \lambda_i - 2 \sum_{i=1}^{M} \lambda_i + \sum_{j=1}^{M} \lambda_i =$$

$$= \sum_{i=1}^{N} \lambda_i - \sum_{i=1}^{M} \lambda_i = \sum_{i=M+1}^{N} \lambda_i = \varepsilon$$

minimalitás

Gyakorlati PCA

Adott $\bar{\bar{R}}, \bar{x}$ $\quad \lambda_1 > \lambda_2 > \dots \lambda_N$

Offline: $\bar{\bar{R}} \bar{s_i} = \lambda_i \bar{s_i}$ $\quad M: \sum_{i=M+1}^{N} \lambda_i < \varepsilon$

$\bar{s_1}, \bar{s_2} \dots \bar{s_M}$

$$\bar{\bar{S}} = \begin{pmatrix} \bar{s_1} \\ \bar{s_2} \\ \vdots \\ \bar{s_M} \end{pmatrix} = (\,|\,)$$

Gyakorlat ZH előtt

2013. 11. 21.

Nov. 25 (hétfő) 8-10

5 lap (név + neptun) - 2-es alapú log. számológép

IB Φ25 Abony - Csík ← ide menj

1) - $C(n,k)$ paritásellenőrző osztja x^{n-1}-et.

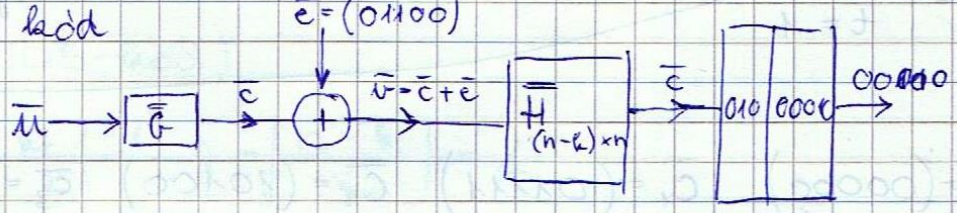
- 2 függ. v.v $H(X,Y) = H(X) + H(Y)$

  $H(X) =$ ~~[illegible]~~ ld 2 = 1

- eloszlásfüggetlen tömörítési eljárások

2) Bináris lineáris kód

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



$C(n,k) = C(5,2)$

$\overline{s} = ?$

$$\overline{\overline{H}}\,\overline{v}^T = \overline{\overline{H}}\,(\overline{c}+\overline{e})^T = \underbrace{\overline{\overline{H}}\,\overline{c}^T}_{0} + \overline{\overline{H}}\,\overline{e}^T = \overline{s}^T$$

$$\overline{\overline{H}}_{3\times5} = \begin{pmatrix} 1&1&1&0&0 \\ 1&1&0&1&0 \\ 1&0&0&0&1 \end{pmatrix} \begin{pmatrix} 0 \\ 1 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

mod2 összeadás

$$\overline{e} \cdot \overline{\overline{H}}\,\overline{e}^T = \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$\overline{s} = \{(01100), (00010), (11011), (10101)\}$

↑ hibavektorok

↑ ez fordul elő a legnagyobb vg-gel

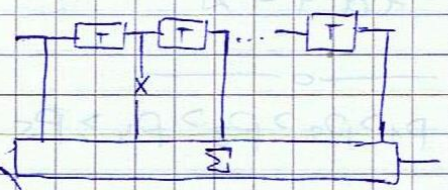
Group leader: a legkisebb súlyú hibavektor

$\overline{c}^{I} = (01110) = (01)(\overline{\overline{G}})$

$\overline{c}^{II} = (10111) = (10)(\overline{\overline{G}})$

$\overline{c}^{III} = (11001) = (11)(\overline{\overline{G}})$

3) BCH $\quad g(x) = \sum_{i=1}^{n-k} a_i x_i \quad \forall a_i \in \{0,1\}$



$f(x^i) = f^{2^i}(x) \rightarrow f(\beta^i) = f^{2^i}(\beta) = \phi$

β, β^{2^i} konjugált gyökcsoportok

$GF(4) = GF(2^2)$ $\quad p(y) = y^2 + y + 1$

$y^{-\infty} = 0$	0	
y^0	1	1
y^1	y	2
y^2	$y+1$	3
y^3	1	
y^4	y	

$$y^2 = 1(y^2 + y + 1) + y + 1$$

$$Cg^{(1)} = \{y, y^2\}$$

$$\Phi(x) = (x+y)(x+y^2) = x^2 + yx + y^2x + y^3 =$$

$$= x^2 + (y + y^2)x + 1 = x^2 + x + 1$$

t - hiba $\quad g(x) = \Phi_1(x) \cdot \Phi_3(x) \cdots \Phi_{2t-1}(x) \Rightarrow$ jelen esetben

$2t - 1 = 1$

$t = 1$

$$g(x) = \Phi_1(x)$$

4)

$C_0 = (00000)$ $\quad \overline{C_1} = (01111)$ $\quad \overline{C_2} = (10100)$ $\quad \overline{C_3} = (11011)$

$C(n, k) \rightarrow C(5, 2)$

n: kódszóhossz $\quad$ ~~k: hány bitet tudok megcímezni~~

$$\overline{\overline{G}}_{2\times 5} = \begin{pmatrix} 10100 \\ 01111 \end{pmatrix}$$

$$\overline{\overline{H}}_{3\times 5} = \begin{pmatrix} 11100 \\ 01010 \\ 01001 \end{pmatrix}$$

$$H(x_k, x_{k-1}, x_{k-2}, x_{k-3}) = \sum_{i=1}^{4} 4\,H(x_k) = 4 \cdot H(x_k) = 4 \cdot 2 = 8$$

ld 4 = 2

$p_1 > p_2 > p_3 > p_4 > p_5 \;\Big|\; l_1, l_2, l_3, l_4 ; l_5 = l_4$

$2^{n-k} = n+1 \quad 2^4 = 15+1 \quad \lambda = 12$

Milyen hosszúságú BURST hiba?

Hamming-kód: 1 hibát tud javítani

↳ 12 · 1 Burst hiba javítása ???

$C(n,k)$

12 { ( ) } = $\bar{C}$

Entrópia mindig ≥ 0!

—o—

t-hibát javít, ciklikus kód, hibaszapda algoritmus.

Hamis

—o—

$C(7,5)$ RS kód (MDS-kód)

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