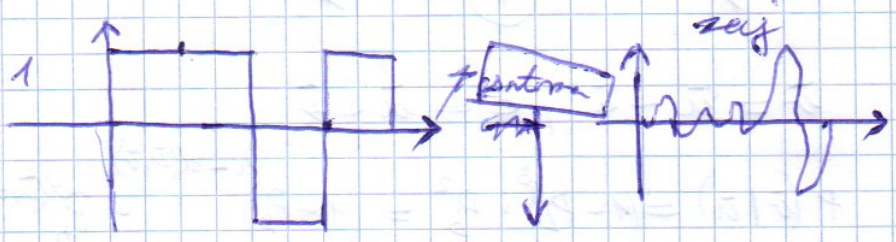
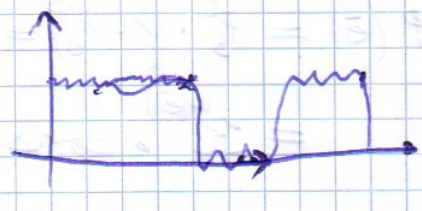
I. Hibajavító kódolás

1101 → 11-11



- zaj adódik a jelhez
- fogadó oldalon egy fv.-el megbecsüljük az eredeti jelet.



sávszél! adóteljesítmény!

$P_b \sim \Psi(SNR)$

P_b ← bit hiba valószínűség

SNR ← jel-zaj viszony

Modell: Binary Simetric Channel

$u_i \in \{0,1\} \rightarrow$ [BSC] $\rightarrow v_i \in \{0,1\}$

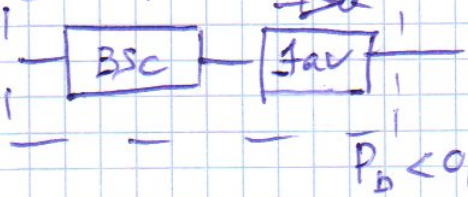
$P_b = P(v_i = 1 \mid u_i = 0) = P(v_i = 0 \mid u_i = 1)$

BSC: $v_i = u_i \oplus e_i$

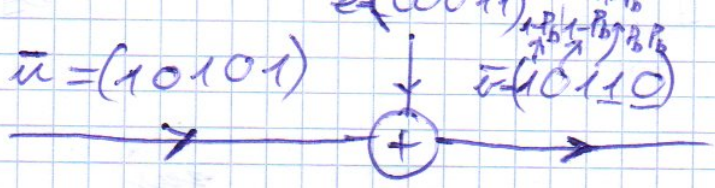
u_i	e_i	v_i	
0	0	0	correct $1-P_b$
0	1	1	hiba P_b
1	0	1	correct $1-P_b$
1	1	0	hiba P_b

$0 \le P_b < 0{,}5$

$P_b > 0{,}5$



$P_b < 0{,}5$



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

n – bitek száma

$d(\bar{u},\bar{v})$ – átfordult bitek száma

$w(\bar{e})$ = 1-esek száma

$$P(\bar{v}|\bar{u}) = (1-P_b)^{n-d(\bar{u},\bar{v})} \cdot P_b^{d(\bar{u},\bar{v})}$$

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

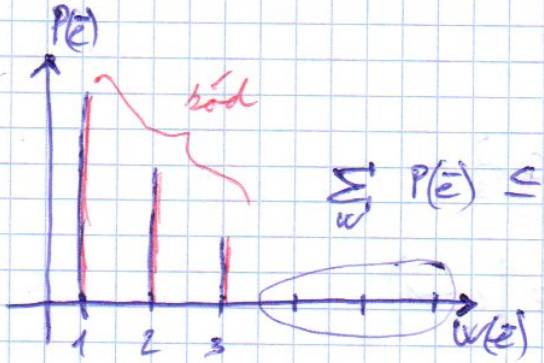
$$= K^{w(\bar{e})} \cdot \text{const} \sim \exp(w(\bar{e}))$$

$$K = \frac{P_b}{1-P_b} < 1$$

Az, hogy sok hiba van bizonyos valószínűsége.

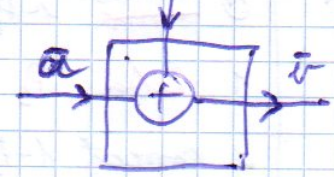
Az, hogy kevés hiba van sok a valószínűsége.

Hibajavító kódolás



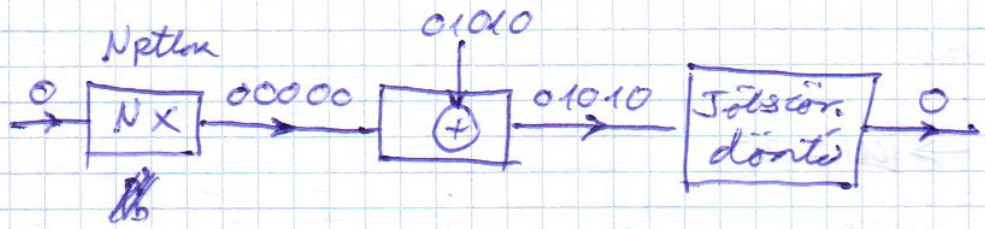
$$\sum_{w} P(\bar{e}) \le 10^{-r}$$ r QOS

BSC



RNG

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



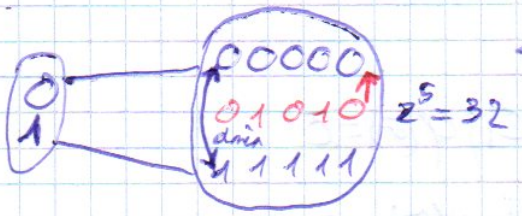
P_b

$10^{-9} \geq P_b' = \sum_{i=\lceil \frac{N}{2} \rceil}^{N} \binom{N}{i} \cdot P_b^i (1-P_b)^{N-i} \ll P_b \sim 0{,}1$

QoS

adatátviteli sebesség csökkenés $\frac{1}{N}$

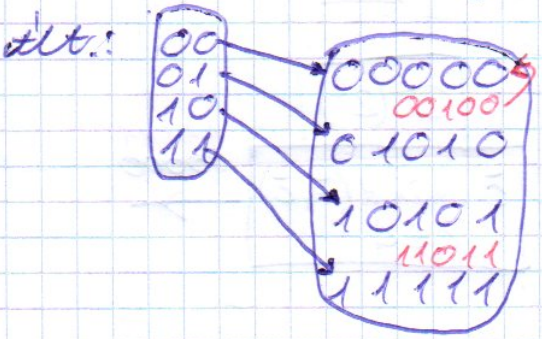
Geometriai interpretáció



2/32 ~~erényes~~ kódszó

d_{min} - Hátvolság

- kibogyelcés
- kibogyavítás



Formális leírás

$\bar{u} \in \{0,1\}^k \rightarrow |u| = 2^k$

$C_1 = \{\bar{c}_1, \bar{c}_2, \dots c_M\}$; $M = 2^k$

$dim(\bar{c}) = n \rightarrow dim(\bar{u}) = k$

$C(n,k)$; $\frac{k}{n}$; $n-k$ redundancia

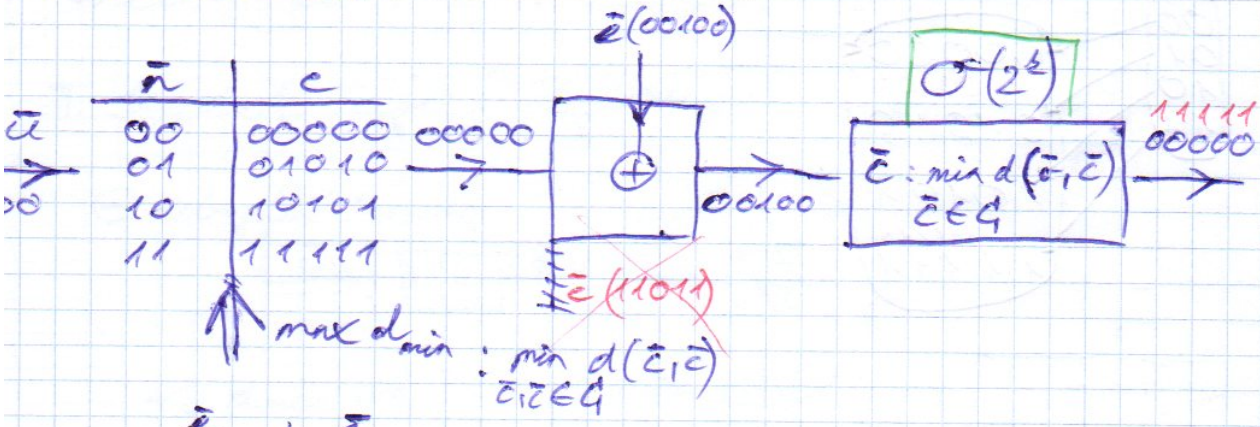
Kódolás $\varphi: \{0,1\}^k \rightarrow C_1$

tetszőleges vektorok $\bar{v} \in \{0,1\}^n$

Dekódolás $\varphi: \{0,1\}^n \rightarrow C_1$; $\varphi(\bar{v}) = \bar{c}$

Dekódolás $\varphi^{-1}: C_1 \rightarrow \{0,1\}^k$; $\varphi(\bar{c}) = \bar{u}$

Implementáció



ē	ū
00000	00
01010	01
10101	10
11111	11

00000 → 00

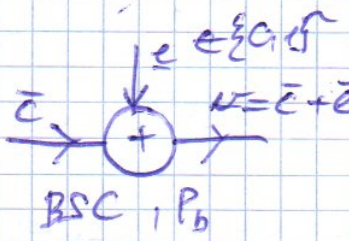
11

$\frac{k}{n} \leq \alpha$

A táblázatokat mire lehet használni? ē

compl ~ $3 \cdot O(2^k)$

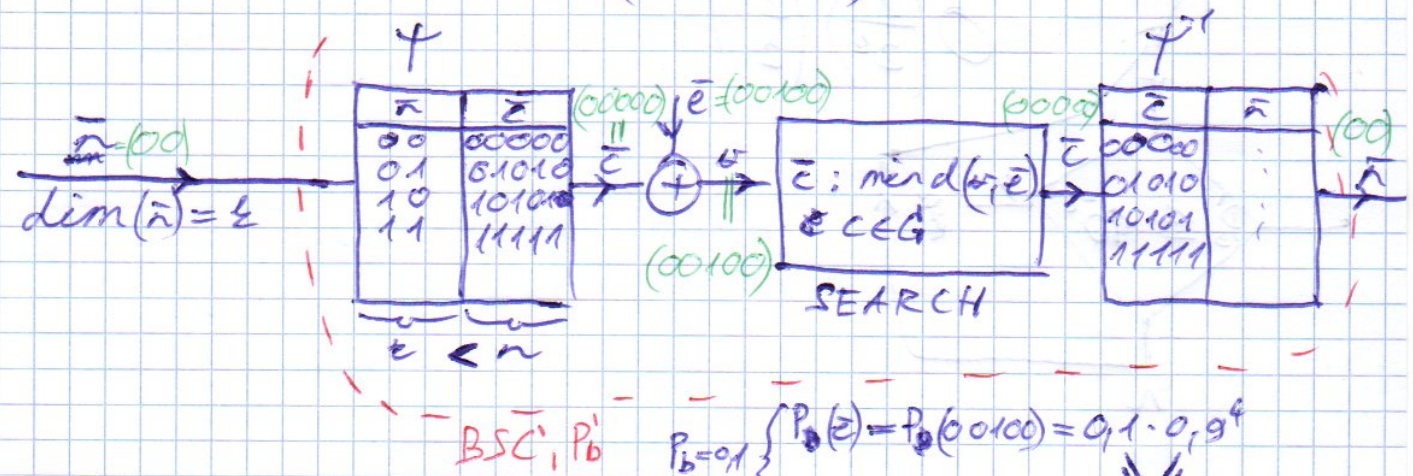
Kódolástechnika II. Ea. 09.11.

Jm.: 

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

$$\sim \text{const} \cdot \mathcal{O}(\exp(w(\bar{e})))$$

Vételi oldalon a v (vett-vektor) és $\bar{e}$ ismeretlen.



$$p_b = 0{,}1 \begin{cases} P_b(\bar{e}) = P_b(00100) = 0{,}1 \cdot 0{,}9^4 \\ P_b(\bar{e}') = P_b(11100) = 0{,}1^3 \cdot 0{,}9^2 \end{cases}$$

3. $\mathcal{O}(2^t)$ → non real-time

max H-távolság
extra

cél: tévesztés ~~valós~~ valószínűsége $\leq 10^{-\gamma}$

"t": # javítható hibák

$$BSC' \rightarrow 1-(1-p_b')^n = \sum_{i=t+1}^{n} \binom{n}{i} p_b^i (1-p_b)^{n-i}$$

blokkhiba valószínűség — blokk hiba valószínűség

$$10^{-\gamma} \geq p_b' = \Psi(p_b)$$

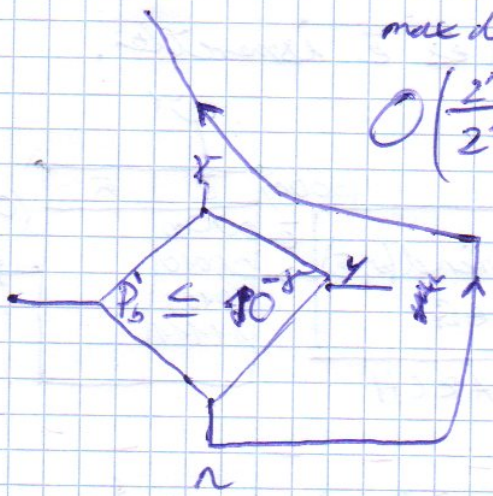
Kérdési tervezés

adott: $P_b, \gamma \xrightarrow[\text{kód}]{\text{hibajav.}} P_b' \leq 10^{-\gamma}$

$n, k \longrightarrow$ kód választás $\longrightarrow t \rightarrow P_b' = \Psi(P_b) \longrightarrow$

max d_{min}

$O\left(\frac{2^n}{2^k}\right)\binom{2^k}{2}$



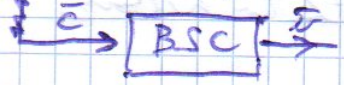
Offline complexity $\longrightarrow$ csillagászati

Online complexity $\longrightarrow$ exp

II. Kódok "teljesítőképessége"

⊖ d_{min}: $\min_{\substack{\bar{c},\bar{c}' \in C \\ \bar{c} \neq \bar{c}'}} d(\bar{c},\bar{c}')$

⊖ hibajelző képesség



$\gamma = d_{min} - 1$

⊖ hibajavító képesség $\quad d(\bar{v},\bar{c}) < d(\bar{v},\bar{c}') \quad \forall \bar{c}' \in C, \bar{c} \neq \bar{c}'$

Δ-egyenlőség: $d(\bar{c},\bar{c}') \leq d(\bar{v},\bar{c}) + d(\bar{v},\bar{c}')$ $\quad \nearrow \searrow \; d(\bar{v},\bar{c}) < d(\bar{c},\bar{c}') - d(\bar{v},\bar{c})$

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

$2 \cdot d(\bar{v},\bar{c}) < d(\bar{c},\bar{c}') \leq d_{min}$

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

09.11.

Singleton bound

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

$\vec{c} = (\underbrace{u_1 \dots u_k}_{\text{üzenet}} \mid \underbrace{p_{k+1} \dots p_n}_{\text{paritás}})$

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

MDS kódok ✓

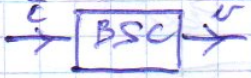
00...0 $p_{k+1} \dots p_n$
00...1
⋮
111...1 $p_{k+1} \dots p_n$

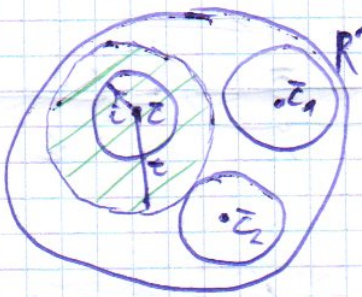
C_{opt} : max d_{min}
↑
MDS

redundancia ?! ⟷ kód minősége

Hamming korlát: $\sum_{i=1}^{t} \binom{n}{i} \leq 2^{n-k}$

Biz:





$\sum_{i=0}^{t} \binom{n}{i} \cdot 2^k \leq 2^n$

t dimenziós gömbök kiadják az R^n-t.

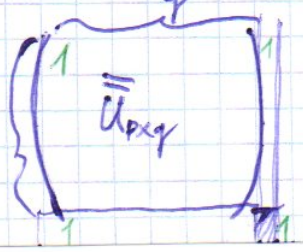
Perfekt kód: $\sum_{i=1}^{t} \binom{n}{i} = 2^{n-k}$

Példák régről:

Paritás bittel kiegészített kód — ARQ: - gyors
hibajav.: 0 - olcsó áruval
hibafelv.: 1

2D paritás

$k = p \times q$ $\quad \vec{\vec{O}}_{(p+1)\times(q+1)}$



$d_{min} = 4 \rightarrow \begin{matrix} r=3 \\ t=1 \end{matrix}$

$\vec{c} + \vec{c}' \in C \quad \forall \vec{c}, \vec{c}' \in C$

$\vec{c}$ 0 0 1 0 1 1
$\vec{c}'$ 0 0 1 1 1 0
$w(0\,0\,0\,1\,0\,1) = 2 \cdot d(\vec{c}, \vec{c}')$

d_{min} : $\min_{\substack{\bar{c},\bar{c}' \in C \\ \bar{c} \neq \bar{c}'}} d(\bar{c},\bar{c}') \sim \min_{\bar{c}' \in C} w(\underbrace{\bar{c}+\bar{c}'}_{\bar{c}''}) \sim \min_{\substack{\bar{c}'' \in C \\ \bar{c}'' \neq \bar{0}}} w(\bar{c}'')$

$O(2^k)$ $O(2^k)$

lin. kód : $d_{min} = w_{min}$

Lineáris bináris kódok (cél: a 2^k komplex "dobozok" kiválasztása)

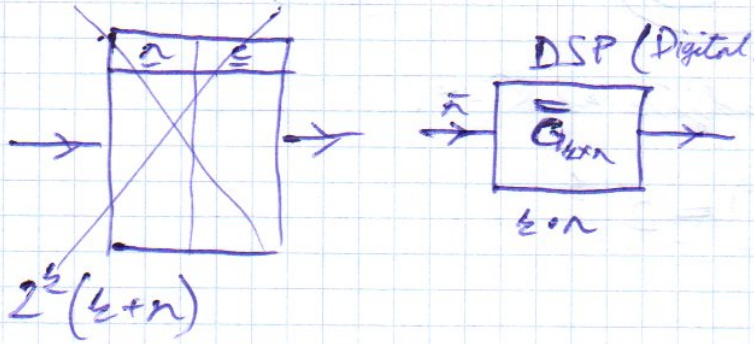
$\bar{g}^{(i)} \in C$ $i = 1, \dots, k$ $\dim(\bar{g}^{(i)}) = n \Rightarrow C = L\{G\}$

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

$$\underbrace{\bar{c}}_{n} = u_1 \underbrace{\bar{g}^{(1)}}_{n} + \dots + u_k \underbrace{\bar{g}^{k}}_{n}$$

Generátor mátrix

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



Szisztematikus kód

$\bar{\bar{G}}_{k \times n} \longrightarrow \bar{c} = (\bar{u}, \bar{p})$

$G = \{(10110), (01111)\}$

$C(5,2)$ — $\underline{G}_{2\times5} \begin{pmatrix} 10|110 \\ 01|111 \end{pmatrix}$

$\uparrow$ $\uparrow$

$\dim(C)$, vektorszám

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

$\underline{c}^{(1)} = (0,1)$ — " — $= (01111)$

$\underline{c}^{(2)} = (1,0)$ — " — $= (10110)$

$\underline{c}^{(3)} = (1,1)$ — " — $= (11001)$

$w_{min} = d_{min} = 3$

$t = \text{javítók}: 1$

$r = \text{det}: 2$

Szisztematikus kódok esetén

$$\underline{\underline{G}}_{k\times n} \left(\underline{\underline{I}}_{k\times k} \mid \underline{\underline{B}}_{k\times(n-k)} \right)$$

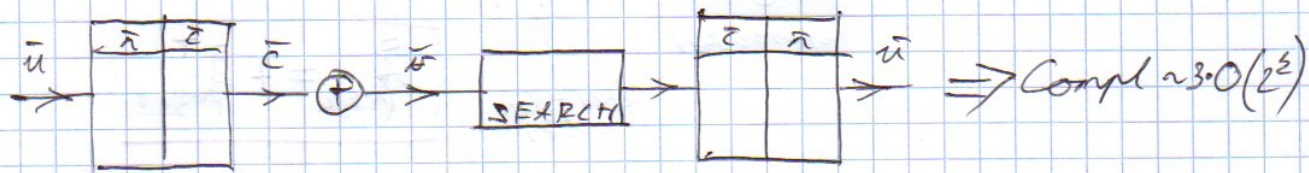
Dekódolás

→ [kivágás] →

Ism

$\bar{e} \in \{0,1\}^n$; $P(\bar{e}) = \varrho^{w(\bar{e})}(1-P_b)^n$; $\varrho = \frac{P_b}{1-P_b}$; $w(\bar{e})$ number of bits

$\bar{u} \in \{0,1\}^k$



$\bar{\bar{G}}_{k\times n}\left(\bar{\bar{I}}_{k\times k} \mid \bar{\bar{B}}_{k\times(n-\xi)}\right)$

Célkitűzés: MDS kódok +
$d_{min} = n-\xi+1$
real-time Hardware

I. Detekció ?! → Paritás ellenőrző mátrix

$\bar{\bar{H}}_{(n-\xi)\times n}$: $\bar{\bar{H}}\,\bar{c}^T = \bar{0}^T \quad \forall \bar{c} \in C$

$\left(\bar{\bar{H}}_{(n-\xi)\times n}\right)\left(\bar{c}^T\right) = \begin{pmatrix}0\\ \vdots \\ 0\end{pmatrix}$ $\quad \bar{\bar{H}}\,\bar{c}^T = \bar{\bar{H}}\left(\bar{u}\,\bar{\bar{G}}\right)^T = \bar{\bar{H}}\,\bar{\bar{G}}^T\,\bar{u}^T \quad \forall \bar{u} \in \{0,1\}^k$

$\Downarrow$

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

$\begin{pmatrix}\bar{h}^{(1)}\\ \bar{h}^{(2)}\\ \vdots \\ \bar{h}^{(n-\xi)}\end{pmatrix}\left(\bar{g}^{(1)T}\ \bar{g}^{(2)T}\ \dots\ \bar{g}^{(k)T}\right) = \bar{\bar{0}} \rightarrow \bar{h}^{(i)}\,\bar{g}^{(k)T} = (\dots)\begin{pmatrix}\vdots\\ \vdots\end{pmatrix} = 0$

$\forall i = 1,\dots,n-\xi$
$j = 1,\dots,\xi$

Szisztematikus kódok:

$$\bar{\bar{G}}_{k\times n} = \left(\bar{\bar{I}}_{k\times k} \,|\, \bar{\bar{B}}_{k\times(n-k)}\right) \overset{??}{\Longrightarrow} \bar{\bar{H}}_{(n-k)\times k} = \left(\bar{\bar{A}}_{(n-k)\times k} \,|\, \bar{\bar{I}}_{(n-k)\times(n-k)}\right)$$

$$\bar{\bar{H}}\,\bar{\bar{G}}^T = \bar{\bar{0}} \longrightarrow \underbrace{\left(\bar{\bar{A}}_{(n-k)\times k} \,|\, \bar{\bar{I}}_{(n-k)(n-k)}\right)}_{\text{hipervektor}} \begin{pmatrix} \bar{\bar{I}}_{k\times k} \\ \bar{\bar{B}}_{(n-k)k} \end{pmatrix} = \bar{\bar{A}}_{(n-k)k} + \bar{\bar{B}}^T_{(n-k)\times k} = \bar{\bar{0}}$$

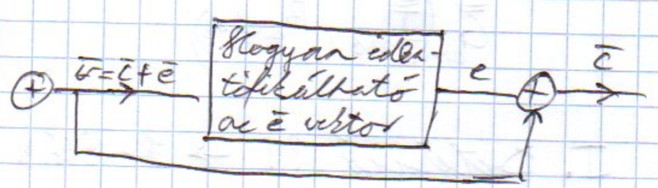
hiperoszlop vektor

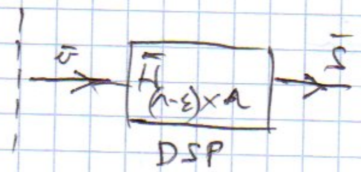
$$\boxed{\bar{\bar{A}}_{(n-k)k} = +\,\bar{\bar{B}}^T_{(n-k)\times k}}$$

modulo 2-nél ~~nincs~~ nem számít a negatív

$$\bar{\bar{G}}_{2\times5} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{pmatrix} \quad \bar{\bar{H}}_{3\times5} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

Detekció – „kulcs” egyenlet





$\bar{\bar{H}}\,\bar{v}^T = \bar{s}^T$; $\dim(\bar{s}) = n-k$.

adott, megf., kiszámolható

$$\bar{\bar{H}}(\bar{c}+\bar{e})^T = \underbrace{\bar{\bar{H}}\bar{c}^T}_{0} + \bar{\bar{H}}\bar{e}^T = \bar{s}^T \qquad \boxed{\bar{\bar{H}}\,\bar{e}^T = \bar{s}^T}$$

adott, ??, kiszámolható

$\bar{\bar{H}}$ nem invertálható

$$\left(\bar{\bar{H}}_{(n-k)\times n}\right)\left(\bar{e}^T\right) = \bar{s}^T$$

$\}$ k db — ismeretlen

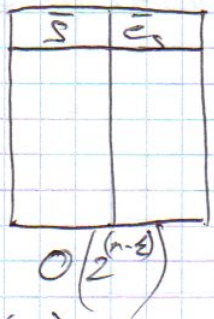
„n − k” db egyenlet
„n” db ismeretlen

alulhatározott lin. egyr.

⇓

rögzítenünk kell k db ismeretlent, tehát egy $\bar{s}$-hoz 2^k $\bar{e}$ vektor létezik.

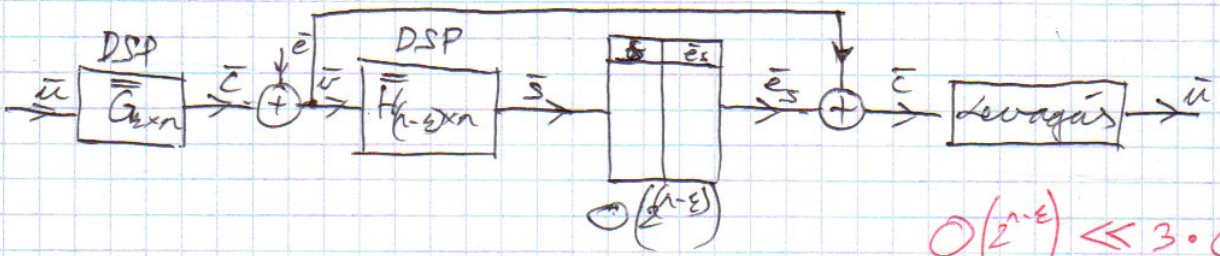
$\bar{\bar{H}}\bar{e}^T = \bar{s}^T \Rightarrow E_s = \{\bar{e} : \bar{\bar{H}}\bar{e}^T = \bar{s}^T\} \rightarrow \bar{e}_s : \min_{\bar{e}\in E_s} w(\bar{e})$



$\rightarrow P(\bar{e}) = \exp(w(\bar{e}))$

LIKELIHOOD

méret: $2^{(n-k)}(n-k)\cdot 2$



$O(2^{n-k}) \ll 3\cdot O(2^k)$

$C(5,2)$ lin. bin. kód $\bar{\bar{G}}_{2\times 5} = \begin{pmatrix}1&0&1&1&0\\0&1&1&1&1\end{pmatrix}$ $\bar{\bar{H}}\begin{pmatrix}1&1&1&0&0\\1&1&0&1&0\\0&1&0&0&1\end{pmatrix}$

$\bar{c}^{(0)} = (0\,0\,0\,0\,0)$
$\bar{c}^{(1)} = (0\,1\,1\,1\,1)$
$\bar{c}^{(2)} = (1\,0\,1\,1\,0)$
$\bar{c}^{(3)} = (1\,1\,0\,0\,1)$

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

$\begin{pmatrix}1&1&1&0&0\\1&1&0&1&0\\0&1&0&0&1\end{pmatrix}\begin{pmatrix}0\\0\\0\\0\\1\end{pmatrix} = \begin{pmatrix}0\\0\\1\end{pmatrix}$ (E_1)

P: $0{,}1\cdot 0{,}9^4 \gg 0{,}1^2\cdot 0{,}9^3 \gg$

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

$\gg 0{,}1^3\cdot 0{,}9^2 \gg$ $0{,}1^4\cdot 0{,}9$

ha $P_b = 0{,}1$

$\bar{s}$	$\bar{e}_s$
001	00001 → P
⋮	
100	00100

$E_{100} = \{(00100), (01011), (10010), (11101)\}$

$\bar{c}\in E_s$; $\bar{e}' = \bar{e} + \bar{c} \subset E_s$

$H\bar{e}^T = \bar{s}^T$ $H\bar{e}'^T = \bar{\bar{H}}(\bar{e}+\bar{c})^T = \underbrace{\bar{\bar{H}}\bar{c}^T}_{\bar{0}^T} + \bar{\bar{H}}\bar{e}^T = \bar{s}^T$

$F_5 = \{\bar{e}, \bar{e}+\bar{c}^{(1)}, \bar{e}+\bar{c}^{(2)}, \ldots \bar{e}+\bar{c}^{(2^k-1)}\}$

$\bar{e}$ $\quad \bar{e}+\bar{c}^{(1)} \quad \bar{e}+\bar{c}^{(2)} \quad \bar{e}+\bar{c}^{(3)}$

Bl.: $F_{001} = (00001), (01110), (10111), (11000)$

itlg VV

Zeitformen

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

$\underline{\underline{G}}_{k\times n} = \underline{\underline{I}}_{k\times k} \mid \underline{\underline{B}}_{k\times(n-k)}$ generátor mátrix

$\underline{\underline{H}}_{(n-k)\times n} = \underline{\underline{A}}_{(n-k)\times k} \mid \underline{\underline{I}}_{(n-k)(n-k)}$

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

<u>új BSC</u> (P_b')

$$\boxed{(1-P_b')^2 = (1-P_b)^5 + (1-P_b)^4 P_b + \dots}$$

II. Szabvány elrendezés (Standard array)

$\bar{c}^{(0)}, \bar{c}^{(1)}, \dots, \bar{c}^{(2^k-1)}$

$\bar{e}_1 \neq \bar{0}: \bar{e}_1+\bar{c}^{(1)}, \dots, \bar{e}_1+\bar{c}^{(2^k-1)}$ → lineáris csoport $C(n,k)$

$\bar{e}_2: \bar{e}_2+\bar{c}^{(1)}, \dots, \bar{e}_2+\bar{c}^{(2^k-1)}$

$\vdots$

$\bar{e}_{2^{n-k}}: \bar{e}_{2^{n-k}}+\bar{c}^{(1)}, \dots, \bar{e}_{2^{n-k}}+\bar{c}^{(2^k-1)}$

2^{n-k}

2^k

$2^k \cdot 2^{n-k} = 2^n$

$\bar{s}$	$\bar{e}_s$
000	00000
001	00001

Student elmond a lin. bin kódról.

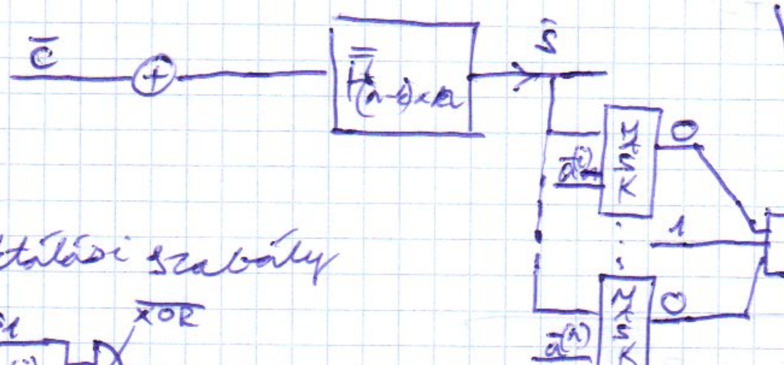
$10^{-r} \geq P_b' = \Psi(P_b)$

$\forall$ 1-hibajavítására alk. kód

Hamming kód (technológiailag releváns) P_b kicsi

elegendő $\forall$ 1 bit hibajavítás

$$\underline{e}^{(i)} = (00\ldots010\ldots00) \rightarrow \text{"}i\text{" ismeretlen} \rightarrow \text{"}i\text{" identifikálni}$$



$$\overline{\overline{H}}\,\underline{v}^T = \underline{s}^T$$

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

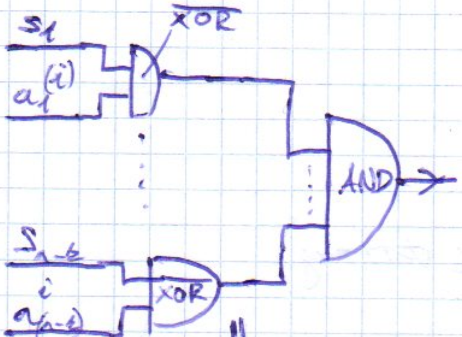
$$\overline{\overline{H}}\,\underline{e}^{(i)T} = \underline{s}^T$$

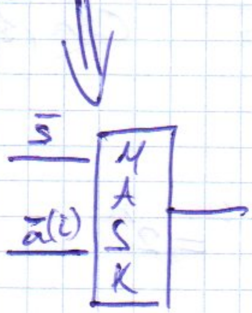
($\overline{\overline{H}}$: adott, $\underline{s}$: adott)

$$\left(\underline{a}^{(1)T} \cdots \underline{a}^{(i)T} \cdots \underline{a}^{(n)T}\right)\begin{pmatrix}0\\ \vdots\\ 0\\ 1\\ 0\\ \vdots\\ 0\end{pmatrix} = \begin{pmatrix}s_1\\ \vdots\\ s_{n-k}\end{pmatrix} = \begin{pmatrix}a_1^{(i)}\\ a_2^{(i)}\\ \vdots\\ a_{n-k}^{(i)}\end{pmatrix}$$

$$\underline{s}^T = \underline{a}^{(i)T}$$

Detektálási szabály





Feltételek:

- $\forall\ \underline{a}^{(i)} \neq \underline{a}^{(j)}$ $\quad \forall\ i,j = 1,\ldots,n;\ i \neq j$
- $\underline{a}^{(i)} \neq 0$

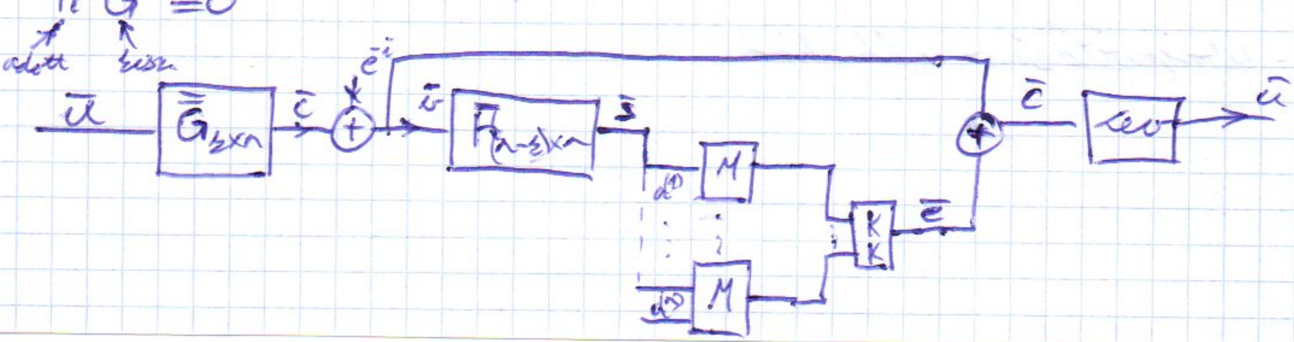
k	n
1	3
4	7
11	15

Teljesül: $n \leq 2^{n-k} - 1$ oszlopvektorra

$$\boxed{n + 1 = 2^{n-k}} \Rightarrow \sum_{i=0}^{t=1} \binom{n}{i} = 2^{n-k} \rightarrow \text{perfekt kód}$$

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

($\overline{\overline{H}}$: adott, $\overline{\overline{G}}$: keres)



$$\underset{3\times 7}{H} \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \Longrightarrow \underset{4\times 7}{G} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$3 < 5 < 6 < 7$

Jeweils

adott: P_b ; γ : $P_b' < 10^{-\gamma}$ $\quad$ k, n : $2^{n-k} = n+1$

~~$P_b' = \Psi(P_b) \cdot (1-P_b')^{\frac{n}{2}} = (1-P_b)^n$~~

$$\boxed{P_b' = \Psi(P_b) : (1-P_b')^{\frac{n}{2}} = (1-P_b)^n + n \cdot P_b (1-P_b)^{n-1}}$$

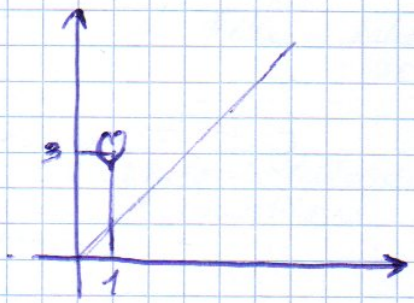
QOS: $P_b' < 10^{-\gamma}$

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

$n-k+1$

$C(3,1)\ 3 \leq d_{min} \leq 3$

$d_{min} = 0$



Kódolástechnika · EA

09.23.

Ismétlés

Inkódionális: 1 db paritásbit $\bar{c}(a_1, \dots, a_5 | p)$ $p = a_1 + \dots + a_5$

① $C(6,5)$ $\quad \bar{\bar{G}}_{5\times6}\begin{pmatrix}1&0&0&0&0&1\\0&1&0&0&0&1\\0&0&1&0&0&1\\0&0&0&1&0&1\\0&0&0&0&1&1\end{pmatrix} \rightarrow \bar{\bar{H}}_{1\times6} = (1\,1\,1\,1\,1\,1)$

$\bar{\bar{H}}(\bar{c}^T) = 0 \quad 1$

↑ páros ↑ fura vna

② $C(5,3)$

$\bar{\bar{G}}_{3\times5}\begin{pmatrix}1&0&0&0&1\\0&1&0&1&0\\0&0&1&1&1\end{pmatrix}$ $\quad \bar{e}(1,0000)$ $\quad \bar{e}'(00001)$

Megkülönböztethető e két hibavektor?

$\bar{\bar{H}}_{2\times5}\begin{pmatrix}0&1&1&1&0\\1&0&1&0&1\end{pmatrix}$ $\quad \bar{\bar{H}}\cdot\bar{e}^T = \begin{pmatrix}0\\1\end{pmatrix}$ $\quad \bar{\bar{H}}\bar{e}'^T = \begin{pmatrix}0\\1\end{pmatrix}$

③

$C(7,4)$ Hamming-kód → Szindróma-dekódolási táblázat

$(2^{r-k} = n+1)$ ✓

$2^3 = 8$

Minden egy hibát javítani tud

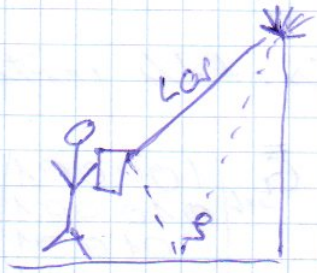
$\bar{\bar{H}}_{3\times7}\begin{pmatrix}0&1&1&1&1&0&0\\1&0&1&1&0&1&0\\1&1&0&1&0&0&1\end{pmatrix}$

$\bar{s}$	$\bar{e}_s$
000	0000000
001	0000001
010	0000010
011	1000000
100	0000100
101	0100000
110	0010000
111	0001000

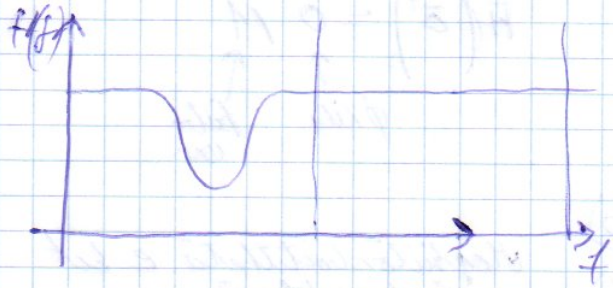
Hogyan lehet többszörös hibákat javítani?

Technológiai motiváció:

reflexiós tényező



$$H(f) = 1 + s e^{j 2\pi f \tau}$$



$\bar{e} = (0 \ldots 0\,1\,0 \ldots 0\,1\,0 \ldots 0\,1\,0 \ldots 0)$

egy megoldás: - duplázni a sávszélet,
hiba esetén átlépni a másikra

H 2 hiba javítása?

$\bar{e}^{ij} = (0 \ldots 0\,\overset{i}{1}\,0 \ldots 0\,\overset{j}{1}\,0 \ldots 0) \rightarrow i, j$

Szindróm egyenlet

$$\bar{\bar{H}}\,\bar{v}^T = \bar{s}^T \longrightarrow \bar{\bar{H}}\left(\bar{c} + \bar{e}^{(ij)}\right)^T = \underbrace{\bar{\bar{H}}\,\bar{c}^T}_{0} + \bar{\bar{H}}\,\bar{e}^{(ij)T} \longrightarrow$$

$$\bar{\bar{H}}\,\bar{e}^{(ij)T} = \bar{s}^T$$

↑ adott ↑ adott

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

Detekció: $\forall \bar{a}^{(i)} \neq \bar{0}$

$\forall \bar{a}^{(i)} \neq \bar{a}^{(j)}$

$\forall \bar{a}^{(i)} + \bar{a}^{(j)} \neq \bar{a}^{(k)}$

$\forall \bar{a}^{(i)} + \bar{a}^{(j)} \neq \bar{a}^{(k)} + \bar{a}^{(l)}$

lin. ftlen. 09.23.

$\alpha_1 \bar{a}^{(i)} + \alpha_2 \bar{a}^{(j)} + \alpha_3 \bar{a}^{(e)} + \alpha_4 \bar{a}^{(m)} \neq \bar{0}$ $\quad \alpha_i \in \{0,1\}$

4db ftlen vektor H-ban

$\bar{\bar{H}}_{4\times5}\begin{pmatrix}1&1&0&0&0\\1&0&1&0&0\\1&0&0&1&0\\1&0&0&0&1\end{pmatrix}$ $\quad C(5,1)$

<u>Lemma:</u> "t" db hiba jav. $\rightarrow$ $\bar{\bar{H}}$-nak "2t" db lin. független oszlopvektora van.

<u>Biz:</u> $\left\lfloor \frac{d_{min}-1}{2} \right\rfloor = t \rightarrow 2t+1 = d_{min} \rightarrow d_{min}-1$ db

$d_{min} = w_{min}$; $w(\bar{r}) = d_{min}-1$ $\quad \bar{r} \notin C$

$\Downarrow$

$\bar{\bar{H}}\,\bar{r}^T \neq \bar{0}^T$

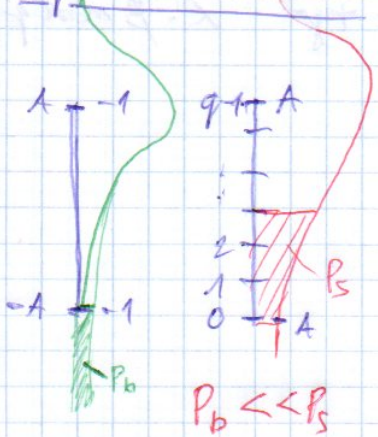
Tehát $w_{min}-1 = d_{min}-1$ ftlen oszlorrak kell lenni.

$\bar{\bar{H}}\begin{pmatrix}0\\1\\0\\\vdots\\0\\1\\0\\\vdots\end{pmatrix} = \sum_{j=1}^{w_{min}-1} r_j \bar{a}^{(ij)^T} \neq \bar{0}^T$

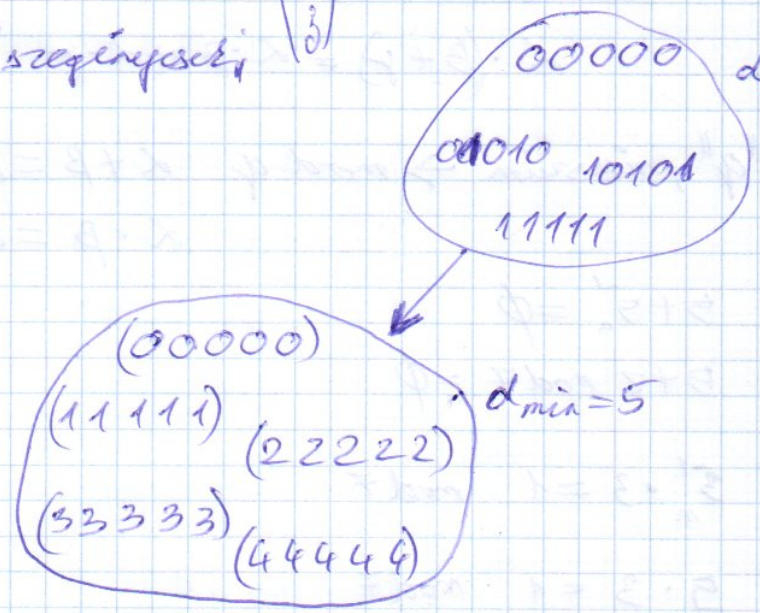
bináris vektorok "szegényesek"

$\Downarrow$ átírjuk

q-áris kódok



$P_b << P_s$



Zárt műveletek (semmilyen művelet sem vezethet ki az $-t, t$ adottságrészből)

$GF(q)$

Galois Field

$GF(q) = \{0, 1, \dots, q-1\}$ "+" "*"

művelet "+" $\forall \alpha, \beta \in GF(q) \to \alpha + \beta \in GF(q)$

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

$\exists \phi : \alpha + 0 = \alpha \quad \forall \alpha \in GF(q)$

$\forall \alpha \in GF(q) \Rightarrow \exists \beta : \alpha + \beta = 0$

$\beta = \alpha_a^{-1} = -\beta$

"*" $\forall \alpha, \beta \in GF(q) \setminus \{0\} \to \alpha \cdot \beta \in GF(q) \setminus \{0\}$

$\alpha \cdot \beta = \beta \cdot \alpha$; $\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$

$\exists 1 : \alpha \cdot 1 = \alpha \quad \forall \alpha \in GF(q) \setminus \{0\}$

$\forall \alpha \in GF(q) \setminus \{0\} \to \exists \beta$

$\alpha \cdot \beta = 1 \to \beta = \alpha_m^{-1}$

disztributivitás

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

"q" prímszám $\to$ mod q $\quad \alpha + \beta = d \cdot q + r \quad \alpha + \beta \bmod q = r$

$\alpha \cdot \beta = d' \cdot q + r' \quad \alpha \cdot \beta \bmod q = r'$

$5 + 5_a^{-1} = \phi$

$5 + 2 \bmod 7 = \phi$

$5_m^{-1} \cdot 3 = 1 \mod 7$

$5 \cdot 3 = 1 \mod 7$

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

Bsp.: $\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_{q-1} = \underbrace{\alpha \cdot \alpha_1}_{\alpha_{i_1}} \cdot \underbrace{\alpha \cdot \alpha_2}_{\alpha_{i_2}} \cdot \ldots \cdot \alpha \cdot \alpha_{q-1}$

$\alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_{q-1} = \alpha^{q-1} \cdot \alpha_1 \cdot \alpha_2 \cdot \ldots \cdot \alpha_{q-1}$

$\alpha^{q-1} = 1$

rang

$m = ord(\alpha)$ min $\alpha^m = 1$

elem	1	2	3	4	5	6	ord	
1	1	1	1	1	1	1	1	
2	2	4	1	2	4	1	3	
3	3	2	6	4	5	1	6	→ primitiv elem
4	4	2	1	4	2	1	3	
5	5	4	6	2	3	1	6	
6	6	1	6	1	6	1	2	

Ism

$GF(q) = \langle \{0, 1, \dots q-1\}, \underset{\text{mod } q}{+}, * \rangle$ - q prím

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

(I) Polynomok a $GF(q)$ felett

$a(x) = a_0 + a_1 x + \dots a_n x^n \rightarrow a_0 \dots a_n, x \in GF(q)$

$deg(a(x)) = n$

Együtthatók: $x \Rightarrow 0, 1, \dots q-1$

$b(x) = b_0 + b_1 x + b_2 x^2 + \dots + b_m x^m \quad \| \; m \leq n$

a) Műveletek

$c(x) = a(x) + b(x) = (a_0 + b_0) + (a_1 + b_1) x + \dots + (a_m + b_m) x^m + a_{m+1} x^{m+1} + \dots + a_n x^n$

$c(x) = a(x) \cdot b(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0) x + \dots +$ [hatch] stb.

$+ \sum_{j=0}^{\min\{i, deg(a(x))^2\}} a_j b_{i-j} x^i + \dots$

$\bar{c} = (c_0 \dots c_n) \Rightarrow c(x) = c_0 + c_1 x + \dots + c_n x^n$

polynom	vektor
$c(x) = a(x) + b(x)$	$\bar{c} = \bar{a} + \bar{b}$
$c(x) = a(x) \cdot b(x)$	$\bar{c} = \bar{a} * \bar{b}$ konvolúció

$c_i = \sum_{j=0}^{\min\{i, deg(a(x))^2\}} a_j b_{i-j}$

$a(x)\Big|_{x=n} = \phi \qquad a(x) \neq \phi$

$a(x) = b(x)(x-n) \longleftarrow a(x)\Big|_{x=n} = b(x)\underbrace{(x-n)}_{\phi} + \underbrace{r}_{\phi} = \phi$

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

↓ relaxáljuk tovább

$m \leq \deg(a(x))$

$a(x) = \text{const} \prod_{i=1}^{m} (x - u_i)$

$\forall a(x), d(x)$

$\deg(a(x)) = n > \deg(d(x)) = k \rightarrow \exists\, q(x), r(x) : a(x) = q(x)d(x) + r(x)$

$\deg(r(x)) < \deg(d(x)) = k$

Euklidész

Input: $a(x), d(x)$
Output: $q(x), r(x)$
$\Big\} a(x) = q(x)d(x) + r(x)$

Lépésszám: $n-k$

(II.) Reed-Solomon kódok (RS) a GF(q) felett

$\lambda_0, \lambda_1, \dots, \lambda_{n-1} \in GF(q) \setminus \{0\} \qquad n = q-1$

$\bar{u} \xrightarrow{x} u(x) = u_0 + u_1 x + u_2 x^2 + \dots + u_{k-1} x^{k-1} \qquad \deg(u(x)) = k-1$

$$\left.\begin{aligned} c_0 &= u(x)\Big|_{x=\lambda_0} = u_0 + u_1\lambda_0 + \dots + u_{k-1}\lambda_0^{k-1} \\ c_1 &= u(x)\Big|_{x=\lambda_1} = u_0 + u_1\lambda_1 + \dots + u_{k-1}\lambda_1^{k-1} \\ &\vdots \\ c_{n-1} &= u(x)\Big|_{x=\lambda_{n-1}} = u_0 + u_1\lambda_{n-1} + \dots + u_{k-1}\lambda_{n-1}^{k-1} \end{aligned}\right\} \quad \bar{c} = \bar{u}\,\bar{\bar{G}}_{k\times n} \quad \text{DSP based}$$

$$\bar{\bar{G}}_{k\times n} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ \lambda_0 & \lambda_1 & & \lambda_{n-1} \\ \vdots & \vdots & & \vdots \\ \lambda_0^{k-1} & \lambda_1^{k-1} & & \lambda_{n-1}^{k-1} \end{pmatrix}$$

RS kódok bináris MDS kódok!!! $\rightarrow d_{min} = n-k+1$

$d_{min} = w_{min}$

$w(\bar{c}) = n - \#\text{of zeros} \geq n-(k-1)$

$\|$

$n-k-1$

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

$\alpha \in GF(q)$ primitív elem

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

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

RS tervezés $GF(q)$ feletti α primitív elemből generálható $\bar{\bar{G}}$

$\forall$ 2 hiba javítására alkalmas RS kódot

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

$n = q-1$
"q" – prím

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

$k = q-1$

$-k$

$C_{RS}(6,2)$ a $GF(7)$ felett 3 primitív

sitr.	0	1	2	3	4	5
$\bar{\bar{G}}$	1	1	1	1	1	1
	1	3	2	6	4	5

Paritás ellenőrző mátrix

$$C(x)\Big|_{\alpha_i} = \phi \quad i = 1, \dots, n-k$$

$$\left.\begin{aligned} &c_0 + c_1\alpha + c_2\alpha^2 + \dots + c_{n-1}\alpha^{n-1} = \phi \\ &c_0 + c_1\alpha^2 + c_2\alpha^4 + \dots + c_{n-1}\alpha^{2(n-1)} = \phi \\ &\vdots \\ &c_0 + c_1\alpha^{n-k} + c_2\alpha^{2(n-k)} + \dots + c_{n-1}\alpha^{(n-k)(n-1)} \end{aligned}\right\} \quad \underset{(n-k)\times n}{\bar{\bar{H}}}\,\bar{c}^T = \bar{0}^T$$

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

$$\left(\bar{\bar{H}}\bar{c}^T\right)_l = \phi \qquad \forall l = 0, \dots, n-k$$

$$\sum_{i=0}^{n-1} \alpha^{li} c_i = \sum_{i=0}^{n-1} \alpha^{li} \sum_{j=0}^{k-1} \alpha^{ij} u_j =$$

$$= \sum_{j=0}^{k-1} \left(\sum_{i=0}^{n-1} \alpha^{i(l+j)} \right) u_j = \sum_{j=0}^{k-1} \frac{\alpha^{(l+j)n} - 1}{\alpha^{(l+j)} - 1} u_j = 0$$

$$\alpha^{(l+j)n} = \left(\alpha^n\right)^{(l+j)} = \left(\alpha^{(q-1)}\right)^{l+j} = 1^{l+j} = 1$$

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

09.25.

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

$\uparrow i_1 \quad \uparrow i_2 \quad \cdots \quad \uparrow i_{n-k}$

lin. független oszlopvektorok száma $d_{min} - 1$

$n-k$ db $\rightarrow$ MDS

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

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

$$\bar{\bar{H}}_{(n-k)\times(n-k)} \begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \cdots & \alpha^{i_{n-k}} \\ \alpha^{2i_1} & \alpha^{2i_2} & \cdots & \alpha^{2i_{n-k}} \\ \vdots & \vdots & & \vdots \\ \alpha^{(n-k)i_1} & \alpha^{(n-k)i_2} & \cdots & \alpha^{(n-k)i_{n-k}} \end{pmatrix} \rightarrow \det \bar{\bar{H}}_{(n-k)\times(n-k)} \neq 0$$

Vander-Monde

$\bar{u}\ \bar{\bar{G}}_{k\times n} = \bar{c}$

$\uparrow$ ismeretlen $\quad \uparrow$ adott $\quad \uparrow$ adott

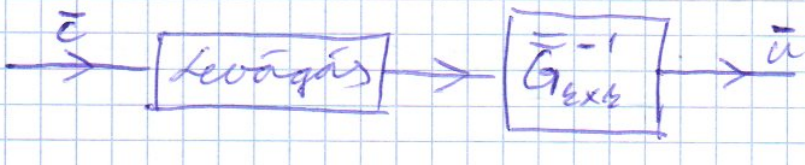
k db ismeretlen

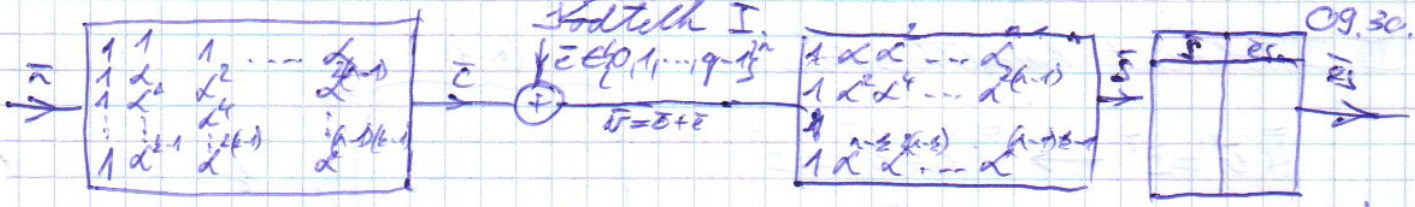
"n" db egyenlet

túlhatározott

$\Downarrow$

$\bar{\bar{G}}^{-1}_{k\times k}(\bar{c})_k = \bar{u}$





09.30.

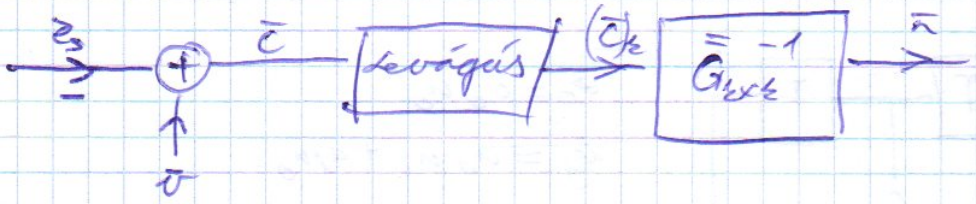
$t = \left[\frac{n-k}{2}\right]$ $n = q-1$ "q" prímszám

! $O(q^{n-k})$!

$p(\bar{e})$ nem csak súly, lehet eltérő

$E_s = \{\bar{e};\ \bar{\bar{H}}\bar{e}^T = \bar{s}^T\}$ } offline

$\bar{e}_s$ = max $p(\bar{e})$
$e \in E_s$



II. Numerikus példa

$GF(7)$ $G\begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}$ $H\begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{pmatrix}$

$\bar{s}$	$\bar{e}_s$
0000	000000
0001	546210
⋮	⋮
6565	200300
⋮	⋮

$\bar{\bar{G}}^{-1}\begin{pmatrix} 3 & 5 \\ 5 & 3 \\ 3 & 4 \end{pmatrix}$

$\begin{vmatrix} 1 & 1 \\ 1 & 3 \end{vmatrix} = 2$

$\begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix} 12 =$

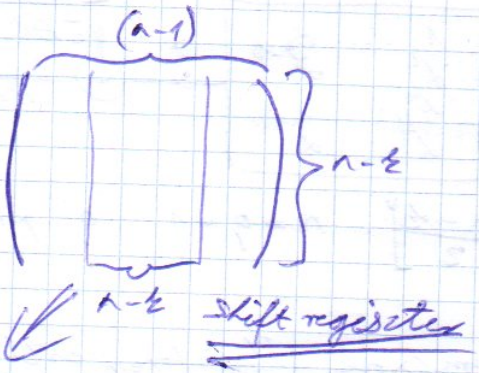
$\bar{r}(0,1) \to \bar{c}(132645) \xrightarrow{+\bar{e}(200300)} \bar{v}(332245) \xrightarrow{\bar{\bar{H}}} \bar{s}(6565) \leftrightarrow e_s(200300) \to$

$\to \bar{v} - \bar{e}_s^T(132645) \to (\bar{c})_k(1,3) \xrightarrow{\bar{\bar{G}}^{-1}} \bar{r}(0,1)$

III. Tábicat helyettesítés

$$\bar{\bar{H}}\,\bar{v}^T = \bar{s}^T \rightarrow \bar{\bar{H}}(\bar{c}+\bar{e})^T = \bar{s}^T$$

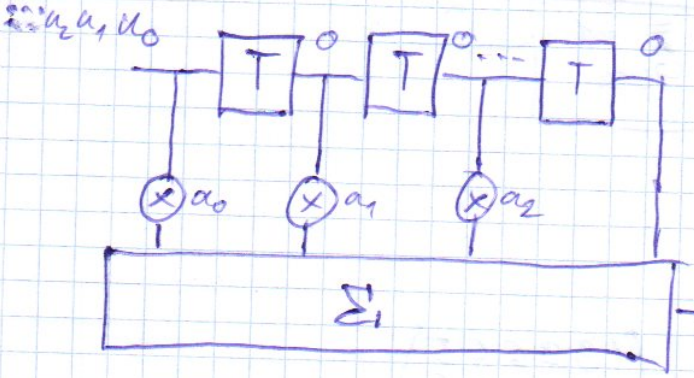
$$\bar{\bar{H}}\,\bar{e}^T = \bar{s}^T$$



$$\bar{\bar{H}}'_{(n-k)\times(n-k)}\,\bar{e}^T = \bar{s}^T$$

IV SHR

LFSR (Linear ~~Feed Forward~~ Shift Register)



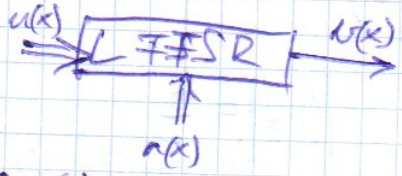
$$v_0 = a_0 u_0$$

$$v_1 = a_0 u_1 + a_1 u_0$$

$$v_2 = a_0 u_2 + a_1 u_1 + a_2 u_0$$

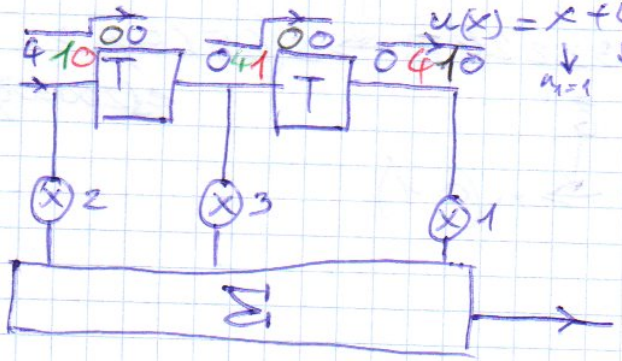
$$v_i \quad v_i = \sum_j a_j u_{i-j}$$

$$v(x) = u(x) \cdot a(x)$$



GF(5)

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



$v_0 = 3$ $\quad i = 0$

$v_1 = 4$ $\quad i = 1$

$v_2 = 2$ $\quad i = 2$

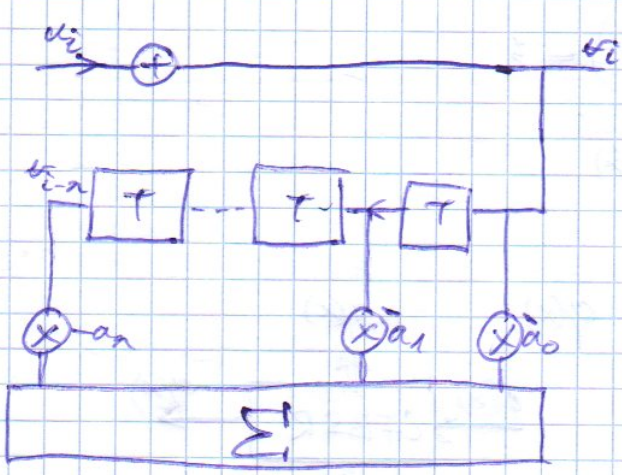
$v_3 = 1$ $\quad i = 3$

$v_4 = 0$ $\quad i = 4$

$$(x^3+2x^2+4x+3)$$

09.30.

IV. LFBSR (Linear Feedback Shift Register)

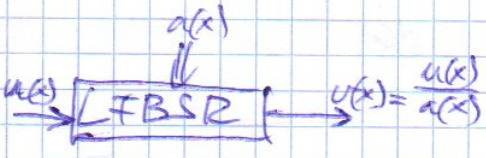


$$v_i = u_i + (1-a_0)v_i - a_1 v_{i-1} - \dots - a_n v_{i-n}$$

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

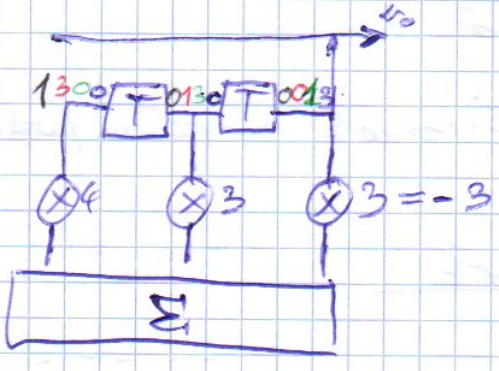
$$\sum_{i=0}^{n} a_i v_{i-i} = u_i$$

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



GTÉ

$$(x^3+4x+4) : (x^2+2x+3) = x+3$$



$3 \times v_0 + 4 = v_0 \qquad i = 0$

$4 = 3v_0$

$v_0 = 3_m \cdot 4 = 2 \cdot 4 = 3$

$i = 1$

$3 \times v_1 + 3 \cdot 3 + 4 = v_1$

$2v_1 + 3 = 0$

$2v_1 = 2$

$v_1 = 1$

$i = 2$

$2 + 3 + 3v_2 = v_2$

$0 \qquad v_2 = 0$

$i = 3$

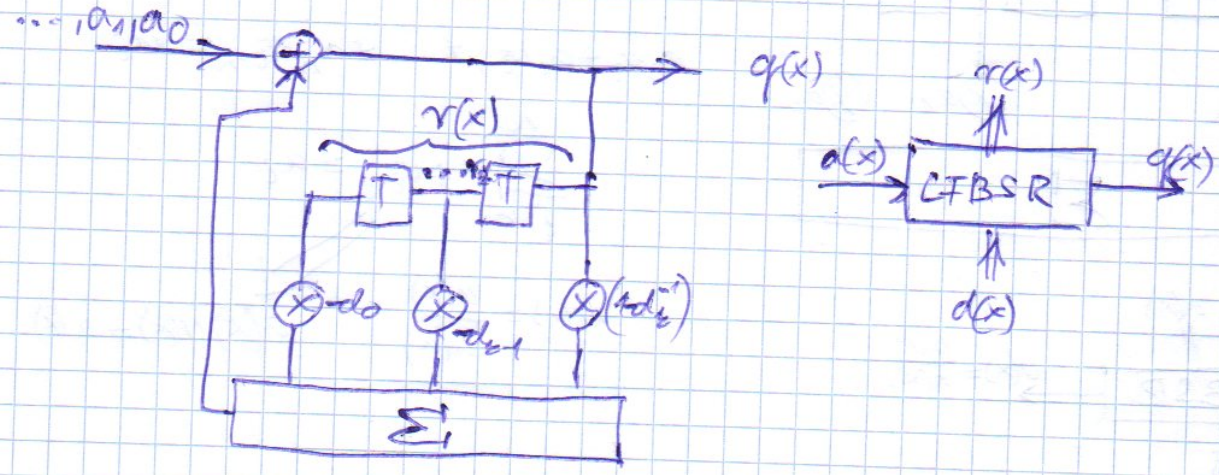
$4 + 3v_3 = v_3$

$v_3 = 0$

V. Maradékos osztás

$$\deg(a(x)) = n \;>\; \deg(d(x)) = k$$

$$\exists\, q(x), r(x) \qquad a(x) = q(x)\,d(x) + r(x)$$



VI. Technológiai motiváció

algebrai kódok : polinomok szorzása/osztása

Lineáris ciklikus kódok

Def Ciklikus eltolás:

$$c = (c_0\, c_1 \dots c_{n-2}\, c_{n-1}) \qquad c' = Sc = (c_{n-1}, c_0, c_1, \dots c_{n-2})$$

Tétel

$$c'(x) = x \cdot c(x) \mod x^n - 1 \quad \checkmark$$

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

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

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

Q.e.d.

09.30.

$c \in C_1 \quad \Rightarrow \lambda c = c' \in C_1 \leftarrow$ cik

$c, c' \in C_1 \quad \lambda c + \beta c' \in C_1 \leftarrow$ Lin

Tétel

$C(n, \ell)$ lin. abl. kód $\rightarrow \exists\, g(x)$ –
- a) $\deg(g(x)) = n - \ell$
- b) $g_{n-\ell} = 1$
- c) $\forall\, c(x) \in C_1$: $g(x)\, u(x) = c(x)$
- d) $g(x) \mid x^n - 1$

Bic.: $a(x) \in C_1$; $\deg(a(x)) \leq \deg(c(x))$

$\deg(a(x)) = m$; $g(x) = a_m^{-1}\, a(x)$

$\Downarrow$ $g_m = 1$

$(a_m^{-1} \cdot a_m x^m + \dots)$

Technológiai jelentőség

$u(x) \rightarrow$ [LFTS R] $\rightarrow c(x)$

$g(x)$

$\deg(g(x) - g'(x)) < m$

$\Downarrow$

$g(x)$ – ből csak 1 létezhet

$g(x)\,;\ x\,g(x)\,;\ \dots\,;\ x^{n-1-m}\,g(x)$

$u_0\, g(x) + u_1 x g(x) + \dots + u_{n-1-m} x^{n-1-m} g(x) \in C_1$

$g(x)\,(u_0 + u_1 x + \dots + u_{k-m-1} x^{n-1-m}) \in C_1$

$g(x) \cdot u(x) = c(x)$

$\exists\, c'(x) : c'(x) + u(x)\, g(x) + r(x)$

$c'(x) - u(x)\, g(x) = r(x)$

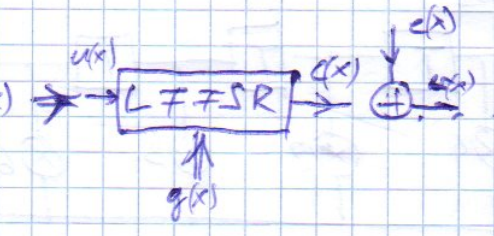
$n - m - 1 = \ell - 1 \rightarrow m = n - \ell$ a) ✓

ciklikus kódok

$C(n,k)$ $\quad c(x) \in C \Rightarrow x\,c(x) \bmod (x^n - 1) \in C$

$c(x), c'(x) \in C \quad \alpha c(x) + \beta c'(x) \in C$

$\exists\, g(x)$:
- $\deg g(x) = n - k$
- $g_{n-k} = 1$
- $\forall c(x) \in C \quad c(x) = u(x)\, g(x)$
- $g(x) \mid x^n - 1$



$h(x)$ paritásellenőrző

$\deg h(x) = k$

$h(x)$: $\forall c(x) \in C \quad h(x)\,c(x) = 0 \bmod x^n - 1 \Rightarrow h(x)\,g(x)\,u(x) = 0 \bmod x^n - 1$

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

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

RS kódok ciklikusak is!

$x^n - 1 \big|_{x = \alpha^i,\ i = 1, \dots, n} = 0 \qquad (\alpha^i)^n = (\alpha^n)^i = (\alpha^{q-1})^i = 1^i = 1$

győzött rem zérus elemei $GF(q)$-nak

$c(x) \big|_{x = \alpha^i,\ i = 1, \dots, n} = 0 \qquad c(x) = \prod_{i=1}^{n-k} (x - \alpha^i)\, u(x) = g(x)\, u(x)$

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

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

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

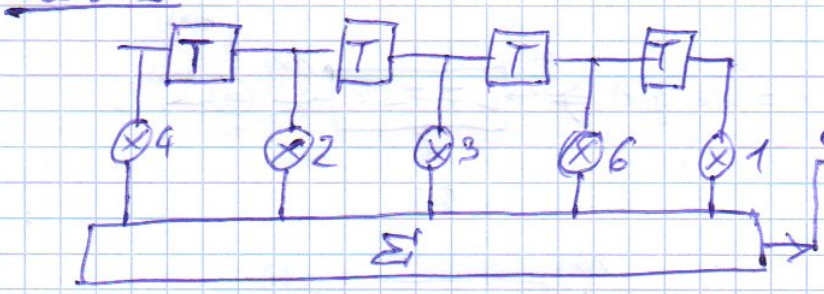
$h(x) = \prod_{i=n-k+1}^{n} (x - \alpha^i)$

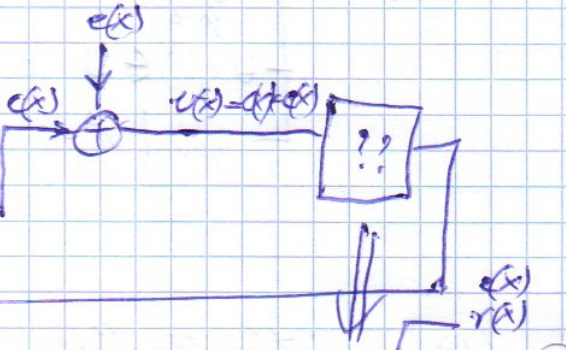
$C(6,2) \Rightarrow$ $g(x) = (x-3)(x-2)(x-6)(x-4) = (x^2+2x+6)(x^2+4x+3) =$

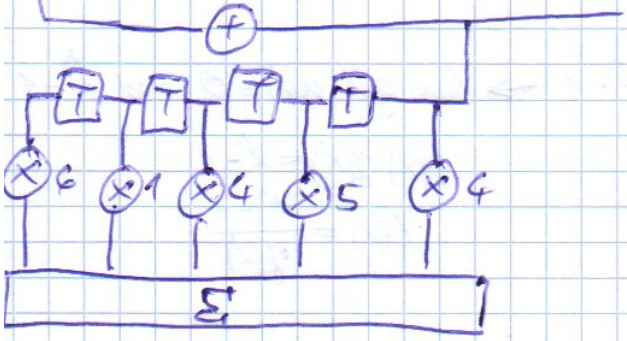
$GF(7) \ni 3$ $= x^4+2x^3+6x^2+4x^3+x^2+3x+3x^2+6x+6 =$

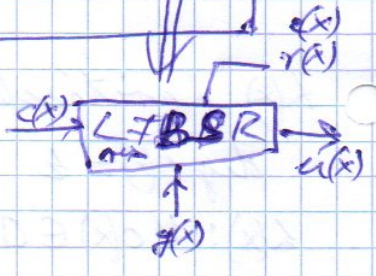
$= x^4+6x^3+3x^2+2x+6$

Kódolás









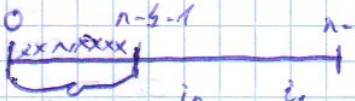
Error Trapping Algorithm (ETA)

$e(x) = c(x) + e(x)$

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

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

→ csak akkor igaz, ha "alsó hiba"



$e(x) = e_{i_0}x^{i_0} + e_{i_1}x^{i_1} + \dots + e_{i_{t-1}}x^{i_{t-1}}$

$i_{t-1} \leq n-k-1$

$e(x) = e_{i_0}x^{i_0} + e_{i_1}x^{i_1} + \dots + e_{i_0+n-k-1}x^{i_0+n-k-1}$

i_0 ismeretlen

$v(x) = c(x) + e(x) = u(x)g(x) + e(x) = a(x)g(x) + r(x)$

nem minden i

$r(x) \neq e(x)$

$e(x) = b(x)g(x) + s(x)$

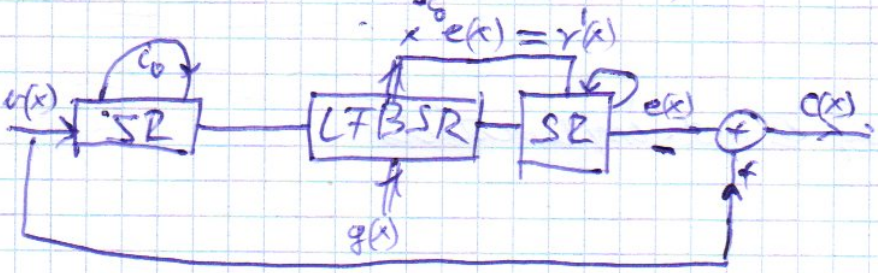
$v(x) = u(x)g(x)s + b(x)g(x) + s(x) \longrightarrow s(x) = r(x)$

$v(x) = a(x)\ g(x) + r(x) \rightarrow e(x) = b(x)g(x) + r(x)$

(a $v(x)$-et osztva a $g(x)$-el megfigy. az $r(x)$-et)

$x^{-i_0} v(x) = x^{-i_0} u(x)g(x) + x^{-i_0} e(x)$

$\deg\left(x^{-i_0} e(x)\right) \leq n - k - 1$



"i_0" ?

$x^{-i_0} e(x) = b'(x)\ g(x) + r'(x) \rightarrow x^{-i_0} e(x) - r'(x) = b'(x)\ g(x) \in C$

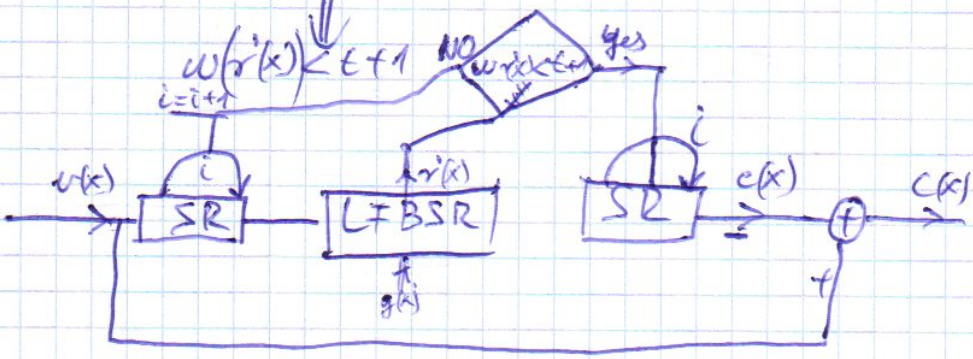
$w\left(x^{-i_0} e(x)\right) \leq t$

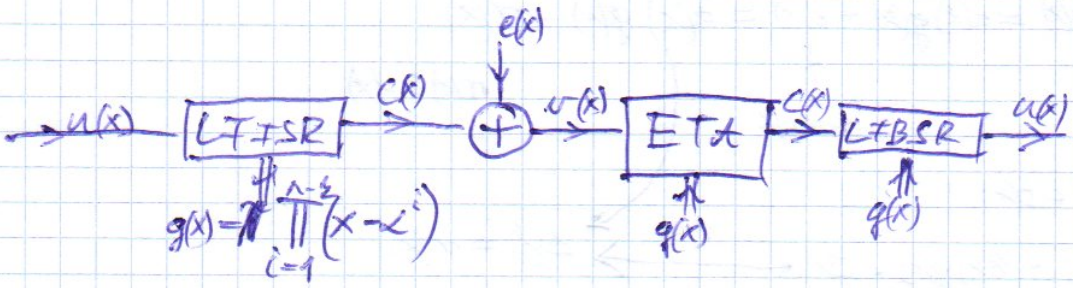
$d_{min} = w_{min} = 2t+1$

$w\left(r'(x)\right) \geq t+1$

$w\left(b'(x)g(x)\right) \geq 2t+1$

pl. $w(b'(x)g(x)) = 0$





∀ SR alapú

Peterson – Gorenstein – Zierler (a hibák nem kell sorozatos egymás t")
lassú

de RS kód ciklikus.

⇓ NDS

⇓ SHR alapú

Optimális teljesítő képesség és opt. implementációi

q prím ⇒ q^m

q prím $\neq 2^n$

Kibővítés: $GF(2^m)$

Algebra a p^m felett "p" prímszám $p=2$

Irreducibilis polinom

$P(y) \neq P_1(y)\,P_2(y)$; $\deg(P_i(y)) < \deg(P(y))$ $i=1,2$

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

y^3+y+1

y^4+y+1

elemek	p-áris szám	polynom repr.
0	0 ... 0	$0y^{m-1}+\dots+0\cdot y^{m-2}+\dots+0=0$
1	0 ... 1	$0y^{m-1}+\dots+1\cdot y^0=1$
α	$a_{m-1}\,a_{m-2}\dots a_0$	$a_{m-1}y^{m-1}+a_{m-2}y^{m-2}+\dots a_0y^0=a(y)$
β	$b_{m-1}\,b_{m-2}\dots b_0$	$b_{m-1}y^{m-1}+b_{m-1}y^{m-1}+\dots+b_0y^0=b(y)$
γ		
p^m-1	$p-1\,p-1\dots p-1$	$(p-1)y^{m-1}+(p-1)y^{m-2}+\dots+(p-1)y^0=$

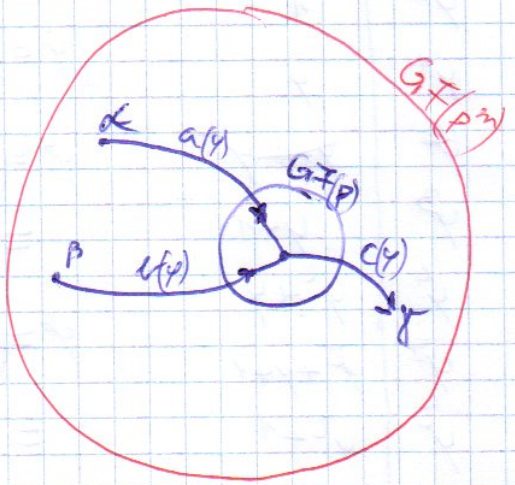
$\alpha \circ_p \beta = \gamma$

$a(y)+b(y) = u(y)P(y)+c(y)$

$\deg(c(y)) \leq m-1$

$a(y)\cdot b(y) = u'(y)P(y)+c'(y)$

$\alpha \cdot \beta = \gamma'$



Algebra a $GF(2^m)$ felett $p=2, m=2$ $\quad p(y)=y^2+y+1$

dec	bináris	
0	0 0	0
1	0 1	1
2	1 0	y
3	1 1	y^2+1

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

2db Looku Table

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

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

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

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

Antilogtábla

y^{∞}	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

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

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

$y^5 = (y^2+1)(y^3+y+1)+y^2+y+1 =$

$= y^5+y^3+y^2+y^3+y+1$

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

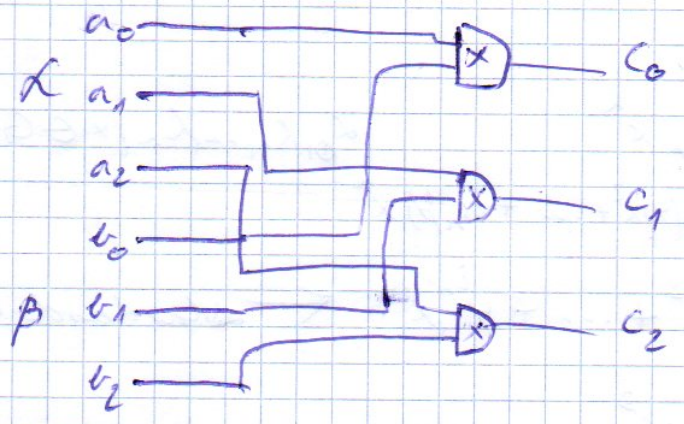
$= y^6+y^4+y^3+y^4+y^2+y+y^3+y+1$

y^{∞}	0	000	0
y^0	1	001	1
y^1	2	010	y
y^2	3	011	$y+1$
y^3	4	100	y^2
y^4	5	101	y^2+1
y^5	6	110	y^2+y
y^6	7	111	y^2+y+1

$4 \cdot 3 = y^3 \cdot y^3 = y^5 \to 7$

$5+6 = y^2+1+y^2+y = y+1 \to 3$

Összeadás



γ

Szorzás

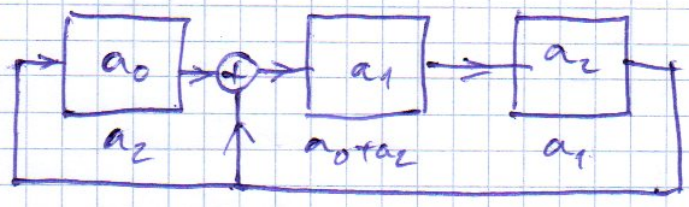
$GF(2^m)$ – ben

$2 \cdot \alpha \rightarrow y(a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 =$

y^3

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

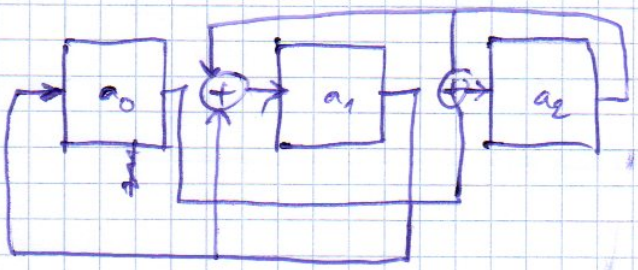
$= a_2 + (a_0 + a_2) y + a_1 y^2$



$2 \cdot 5 = y \cdot y^5 = y^7 = 1$

$4 \cdot \alpha \rightarrow y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 (y+1) + a_2 (y^2 + y) =$

$= a_1 + (a_1 + a_2) y + (a_0 + a_2) y^2$



ULSI y^e

$\alpha \cdot \beta \rightarrow (a_0 + a_1 y + a_2 y^2) y^e$

Polynomok a $GF(p^m)$ felett:

$$a(x) = a_0 + a_2 x^2 + \dots + a_n x^n \qquad a_0, a_1, \dots, a_{n-1}, x \in GF(p)$$

$$a(x) = a_0(y) + a_1(y)x + a_2(y)x^2 + \dots + a_n(y)x^n$$

$$a(x) = y^{i_0} + y^{i_1}x + y^{i_2}x^2 + \dots + y^{i_n}x^n \leftarrow \text{standard alak}$$

$$a(x) = 5 + 6x + 7x^2 + 4 \cdot x^3$$

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

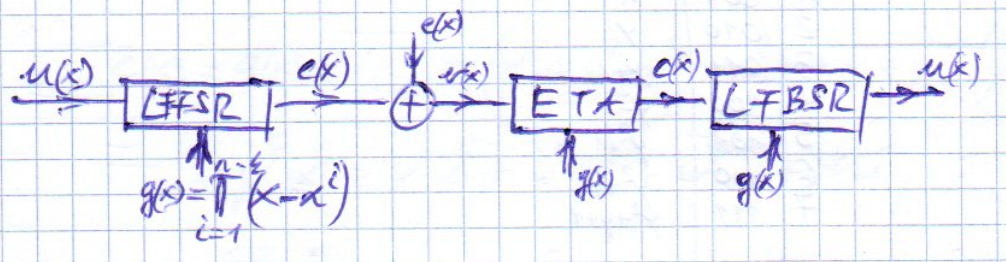
$$a(x) = y^6 + y^4 x + y^5 x^2 + y^2 x^3$$

Ism.

RS kódok ciklikusok

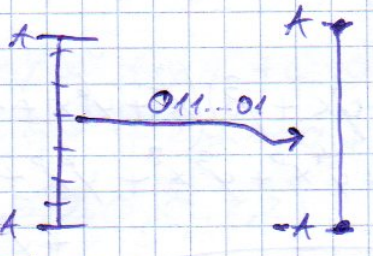
↓

opt ∧ HW



GF(q) – ~~Ezen~~ nem jól használjuk ne adatátvitelt

GF(2^m)



Kódtervezés:

adott "t" → 2t = n − k

$n = 2^m - 1$

m		n	k
1	2^1		
2	2^2		
4	2^3		
8	2^4		
16	2^5		

$\Rightarrow$ GF(2^m), C(n, k); $\gamma \in$ GF(2^m)

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

opt ∧ HW ∧ Bin. Szimm.

(MDS) (SHR)

Schritt: $t=2 \Rightarrow \left.\begin{array}{l} d=n-k \\ n=2^m-1 \end{array}\right\}$

m	2^m	n	k
1	2	1	*
2	4	3	*
3	8	7	3
4	16	15	11

$C_R(7,3)$, $\gamma \in GF(8)$

0	000	0
1	001	1
2	010	γ
3	011	$\gamma+1$
4	100	γ^2
5	101	γ^2+1
6	110	$\gamma^2+\gamma$
7	111	$\gamma^2+\gamma+1$

$P(\gamma) = \gamma^3+\gamma+1$

$\gamma^{-\infty}$	0	γ^7	1
γ^0	1	γ^8	γ
γ^1	γ	γ^9	γ^2
γ^2	γ^2	γ^{10}	$\gamma+1$
γ^3	$\gamma+1$	γ^{11}	$\gamma^2+\gamma$
γ^4	$\gamma^2+\gamma$	γ^{12}	$\gamma^2+\gamma+1$
γ^5	$\gamma^2+\gamma+1$	γ^{13}	γ^2+1
γ^6	γ^2+1		

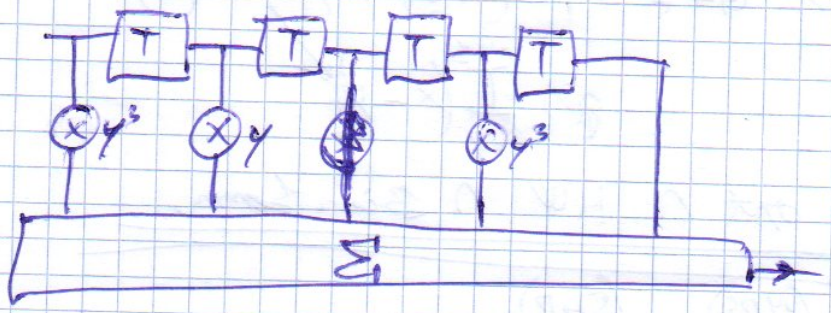
$$g(x) = \prod_{i=1}^{4}(x-\gamma^i) = (x+\gamma)(x+\gamma^2)(x+\gamma^3)(x+\gamma^4) =$$

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

$$= x^4+\gamma^4x^3+\gamma^3x^2+\gamma^6x^3+\gamma^3x^2+\gamma^2x+$$

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

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



$\bar{u} = (7,7,7) \longrightarrow \bar{c}$ $\qquad 7 \to 111 \to y^2+y+1 = y^5$

$a(x) = 7x^2 + 7x + 7 = y^5x^2 + y^5x + y^5$

$c(x) = g(x) \cdot a(x) = \left(x^4 + y^3x^3 + x^2 + yx + y^3\right)\left(y^5x^2 + y^5x + y^5\right)$

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

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

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

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

$= 7x^6 + 5x^5 + 2x^4 + 0 + 0 + 7x + 2$

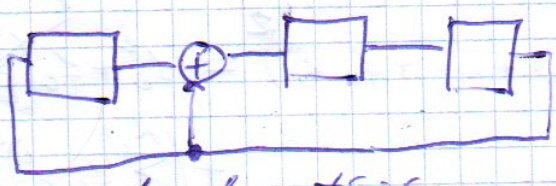
$\bar{c} = (7,5,2,0,0,7,2)$

$y^3 + y^6 + y =$

$= y^7 + y + 1 + y^7 + 1 + y = 0$

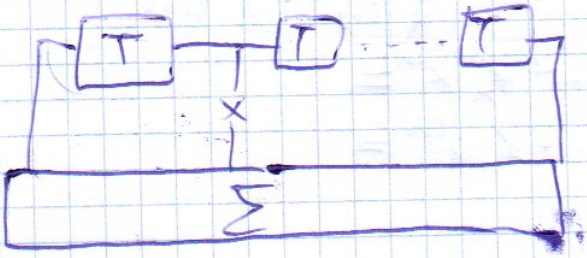
De!

(X) y ~



Implementációs problema

VLSI



$g(x) : g_i \in \{0,1\} = GF(2)$

"t" hiba javítása a $g(x)$ gyökei $2t$ db

$g(x)\Big|_{y^{i_1}, y^{i_2}, \ldots, y^{i_{2t}}} \to c(x) = a(x)\cdot g(x)\Big|_{y^{i_1}, y^{i_2}, \ldots, y^{i_{2t}}} = \phi$

$c_0 + c_1 y^{i_1} + c_2 y^{2i_1} + \ldots + c_{n-1} y^{i_1(n-1)} = \phi$

$\vdots$

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

$$\overline{H}\begin{pmatrix} 1 & y^{i_1} & y^{2i_1} & \dots & y^{(n-1)i_1} \\ 1 & y^{i_2} & y^{2i_2} & \dots & y^{(n-1)i_2} \\ \vdots & & & & \\ 1 & y^{i_{2t}} & y^{2i_{2t}} & \dots & y^{(n-1)i_{2t}} \end{pmatrix} \qquad \det\left(\overline{H}_{2t\times 2t}\right)\neq 0$$

$2t$ db lin. ftlen

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

$g(x)$ —
- $g_i \in GF(2) \rightarrow$ VLSI implementálható (szegényes egyh.)
- ("gazdag" gyökök) $\rightarrow$ Első telj. képesség "t" hiba jav. alkalmas legyen

algebrai kibővítés: $GF(2)$ feletti polinomok

$$f(x) = f_0 + f_1 x + f_2 x^2 + \dots + f_n x^n ; \quad f_0, f_1, \dots, f_n \in GF(2)$$

$$f^{2^l}(x) = f(x^{2^l}) \rightarrow f^2(x) = f(x^2)$$

$$f^2(x) = \left(f_0 + f_1 x + \dots + f_n x^n\right)^2 = f_0^2 + f_0\left(\sum_{i=1}^{n} f_i x^i\right) + f_0\left(\sum_{i=1}^{n} f_i x^i\right) + \left(\sum_{i=1}^{n} f_i x^i\right)^2 =$$

$$= f_0^2 + f_1^2 x^2 + f_1 x\left(\sum_{i=2}^{n} f_i x^{i-1}\right) + f_1 x\left(\sum_{i=2}^{n} f_i x^{i-1}\right) + \left(\sum_{i=3}^{n} f_i x^i\right)^2 =$$

$$= f_0^2 + f_1^2 x^2 + f_2^2 x^4 + \dots + f_n^2 x^{2n} =$$

$$= f_0 + f_1 x^2 + f_1 x^4 + \dots + f_n x^{2n} =$$

$f(\beta) = 0 \quad f(\beta^2) = 0$

$f(\beta^{2^l}) = 0 \quad l = 1, 2, \dots \qquad f(\beta^{2^l}) = f^{2^l}(\beta) = \left(f(\beta)\right)^{2^l} = 0$

$G \neq (8)$ feletti konjugált gyökcsoport:

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

$$\Phi_1(x) = (x+y)(x+y^2)(x+y^4) = (x^2 + y^4x + y^3)(x+y^4) =$$

$$= x^3 + y^4x^2 + y^3x + y^4x^2 + yx + 1 = 1x^3 + 0x^2 + 1x + 1$$

$$\Phi_2(x) = (x+y^3)(x+y^5)(x+y^6) = (x^2 + y^2x + y)(x+y^6) =$$

$$= x^3 + y^2x^2 + yx + x^2y^6 + yx + 1 =$$

$$= 1x^3 + 1x^2 + 0x + 1$$

$\Phi_1(x)$, $\Phi_2(x)$

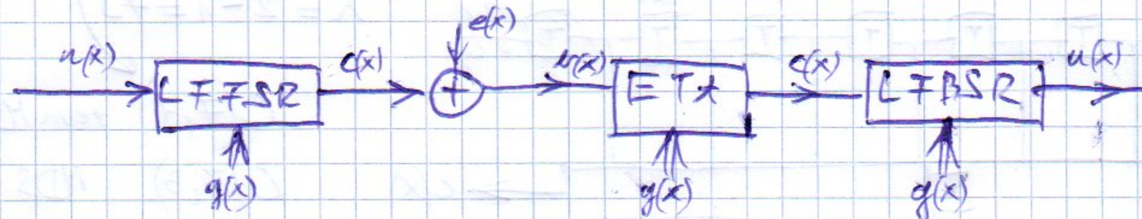
Ism.

Blokk kódolás "csúcsa":

adott "t" —RS→ m, n, k ; $n-k=2t$; $n=2^m-1$

m	2^m	n	k
min		+	+

→ $g(x)=\prod_{i=1}^{n-k}(x-\gamma^i)=\sum_{i=0}^{n-k}\gamma^{l_i}x^i$ → SR



Σ {
- Opt. kód (teljesítőképesség) ⇐ RS
- Real time impl. (SR archit.) ⇐ ciklikus kódok
- Bináris adatátvitel ("leggyobb" kivezérelhetőség) ⇐ $GF(2^m)$

Probléma:

$g(x)$: $g_i \in GF(2^m)$ → szorzás

Kihívás:

$g(x)$: $g_i \in \{0,1\} \in GF(2)$ de gazdag gyökök $GF(2^m)$-ben

$f(x) \in GF(2)$, $f(\beta)=\phi$, $f(\beta^{2^l})=\phi$

(↑ gyöktényezős alak — gazdag gyökök)

$GF(2^m)$-ben I. $(\gamma, \gamma^2, \gamma^4, \dots)$ → $\Phi_1(x)=(x-\gamma)(x-\gamma^2)(x-\gamma^4)$

II. $(\gamma^3, \gamma^6, \gamma^{12}, \dots)$ → $\Phi_3(x)=(x-\gamma^3)(x-\gamma^6)(x-\gamma^{12})$

⋮

BCH (Bose – Chaudhuri – Hocquenghem):

adott "t" $g(x) = \Phi_1(x) \cdot \Phi_3(x) \cdot \ldots \cdot \Phi_{2t-1}(x) \rightarrow \deg(g(x)) \leq m \cdot t$

↓

SL-es egyl.

∀ 2 hiba jav. alkalmas BCH kód "t" = 2

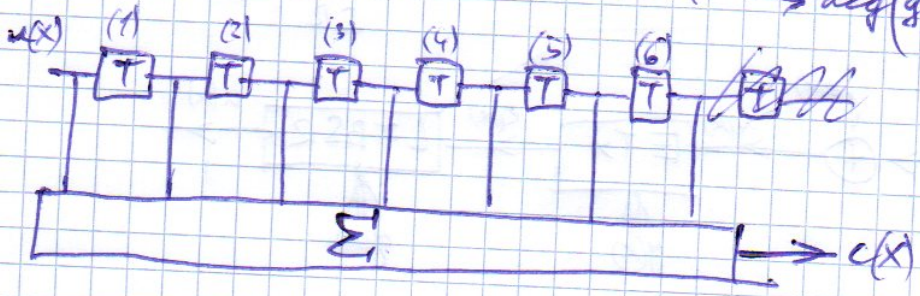
$\Rightarrow g(x) = \Phi_1(x) \cdot \Phi_3(x) = (x^3+x+1)(x^3+x^2+1) = x^6+x^5+x^3+x^5+x^3+x^2+x^3+x+1$

$= x^6+x^5+x^4+x^3+x^2+x+1 \rightarrow \deg(g(x)) = n-k = 6$

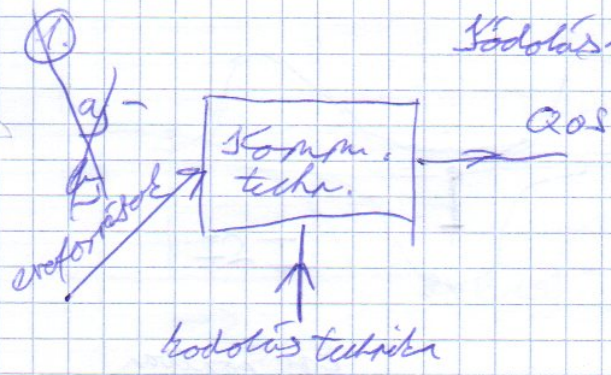
$n = 2^3-1 = 7$

$C(7,1)$ rep MDS

$C(7,3)$ MDS



Kódolástechnika 10.21.



Erőforrások:

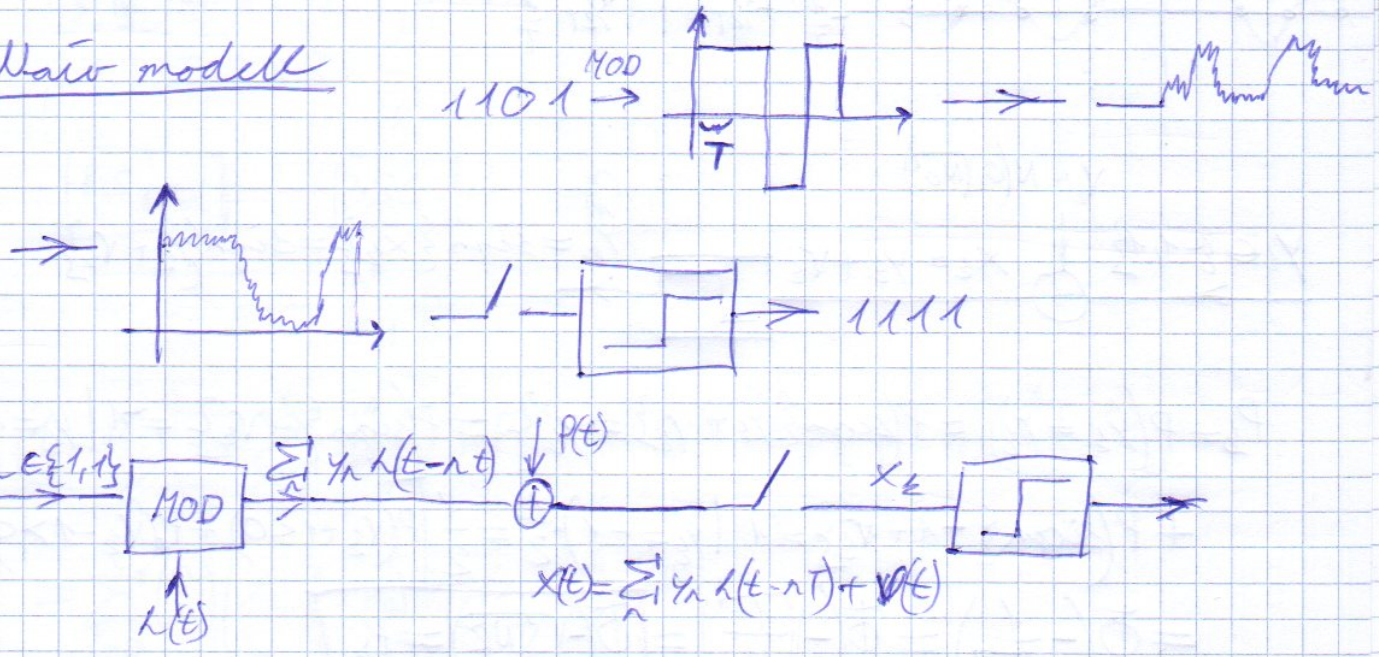
- Sávszélesség
- $SNR = \frac{P_{jel}}{\text{zajenergia}} = \frac{A^2}{N_0}$

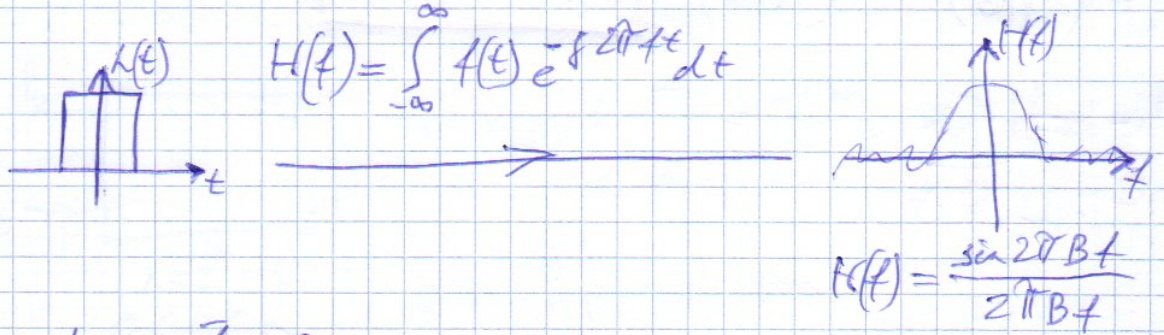
$N_0 = \xi T B$ (Boltz., hőm., felbontóképesség)

QoS paraméterek:

1. $\frac{1}{T}$
2. $P_b \leq 10^{-x}$

Naiv modell





Sávszél $= \infty$

$$x(t) = \sum_i \gamma_n h(t - nT) + \nu(t)$$

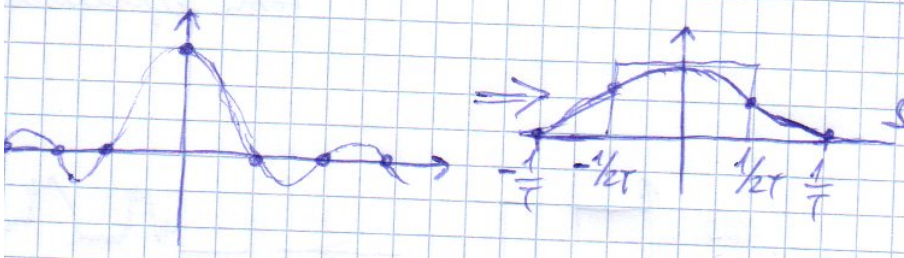
$$x(t + \xi T) = \sum_i \gamma_n h(t_0 + \xi T - nT) + P(t_0 + \xi T)$$

$$x_\xi = \sum_{n}^{i} h_{\xi - n}\, \gamma_n + \nu_\xi$$

$$x_\xi = h_0 \gamma_\xi + \underbrace{\sum_{n \neq \xi}^{i} h_{\xi - n}\, \gamma_n}_{\text{ISI}} + \nu_\xi$$

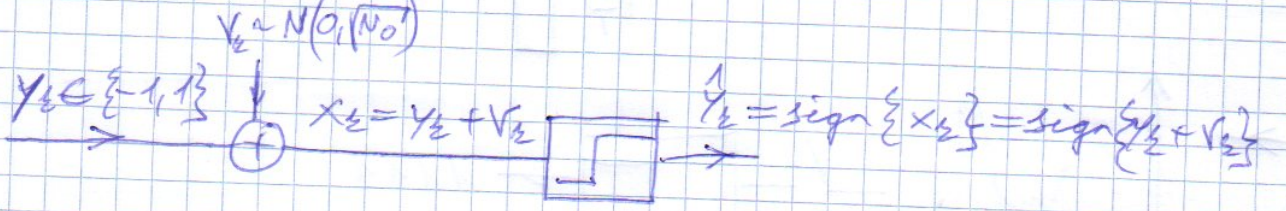
Egy pontban összeadódnak az eddig leadott bitek.

A csatorna a memóriája ennek



$$B \sim \frac{1}{T}$$

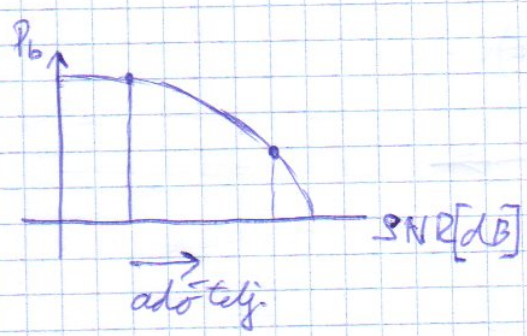
Sávszél ~ adatátviteli sebesség



$$P_b = P(\hat{\gamma}_\xi \neq \gamma_\xi) = P(\text{sign}\{\gamma_\xi + \nu_\xi\} \neq \gamma_\xi) = P(\text{sign}\{1 + \nu_\xi\} = -1 \mid \gamma_\xi = 1) \cdot \frac{1}{2} +$$

$$+ P(\text{sign}\{-1 + \nu_\xi\} = 1 \mid \gamma_\xi = -1) \cdot \frac{1}{2} = \frac{1}{2}\left[P(\nu_\xi + 1 < 0) + P(\nu_\xi - 1 > 0)\right] =$$

$$= \Phi\left(-\frac{1}{\sqrt{N_0}}\right) = \Phi\left(-\sqrt{\frac{1^2}{N_0}}\right) = \boxed{\Phi\left(-\sqrt{SNR}\right) = P_b}$$



mérték korlátozzák a hiba valószínűségét

$P_b = \Phi(-\sqrt{SNR})$

QOS ~ erőforrások

Kódtervezés:

adott SNR erőforrás $\rightarrow P_b = \Phi(-\sqrt{SNR})$

QOS $\rightarrow P_b' < 10^{-r}$

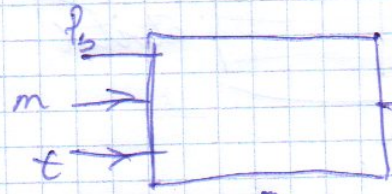
$\frac{1}{T}$ adatátviteli sebesség $\rightarrow B$

$GF(2^m)$

$\hookrightarrow P_{sz} = 1-(1-P_b)^m$

$$(1-P_{sz}')^k = \sum_{i=1}^{t} \binom{n}{i} P_{sz}^{\,i} \cdot (1-P_{sz})^{n-i} \Rightarrow (1-P_b')^{m\cdot k} =$$

$$= \sum_{i=0}^{t} \binom{n}{i} \left[1-(1-P_b)^m\right]^i (1-P_b)^{(n-i)m}$$



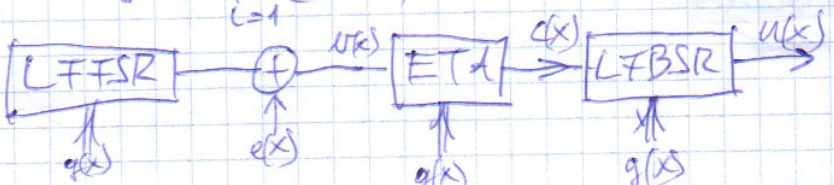
P_b': $n, m, t \rightarrow GF(2^m)$ $\Rightarrow P_b \leq 10^{-r}$

$C(n,k)$ $\frac{1}{T}\frac{k}{n}$ $B' = \frac{n}{k} B$

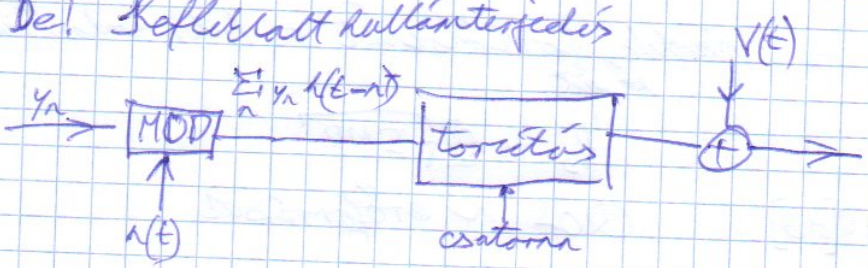
$n = 2^m - 1$

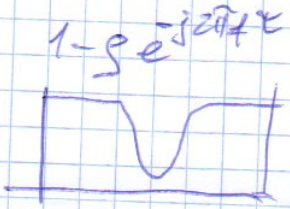
$0 < k < n$

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



Del. Reflektált hullámterjedés





ISI → burst hiba

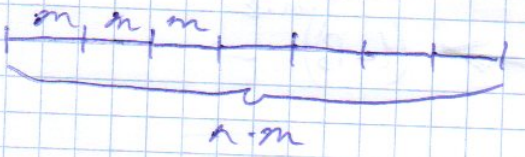
Burst hibák elleni védelem kell!

$n-k \geq bl(\bar{c}) \geq 2l \qquad \bar{e} + \bar{e}' \neq \bar{c}$

$l \leq \left\lfloor \frac{n-k}{2} \right\rfloor$ Reiger-bound

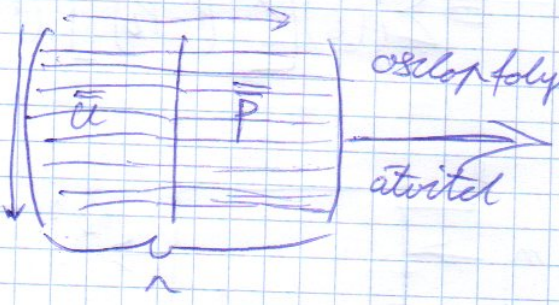
Burst hiba javító kódolás?

Bináris kétkód $C(n,k)$ a $GF(2^m)$ felett "t" hibajavítás



$C(n \cdot m, k \cdot m) \quad bl = m \cdot t$

λ-interleaving kód $C(n,k,t$



$\bar{u}_{\lambda k} \mid \bar{p}_{\lambda(n-k)} \qquad C(\lambda n, \lambda k)$

Ha λ nagy → rem real-time

vételi oldalon sorfolytonos detekció

$\Sigma = \Sigma_1 \cdot \Sigma_2$

$n = n_1 \cdot n_2$

y C(n,2)

$\ast \cdot C(n_1, \Sigma_1), t_1$ →

C(n₂, Σ₂), t_2 ↓

$\bar{\bar{v}}_{\pi_1 \cdot \Sigma_1}$	$\bar{\bar{P}}_1$
$\bar{\bar{P}}_2$	$P_{12} = P_{21}$

⊖ Oszlop folyt. átvitel, vízszintes jav.

$t_1 \cdot n_2 + t_2$

⊖ Sor folyt. átvitel, függ. jav.

$n_1 \cdot t_2 + t_1$

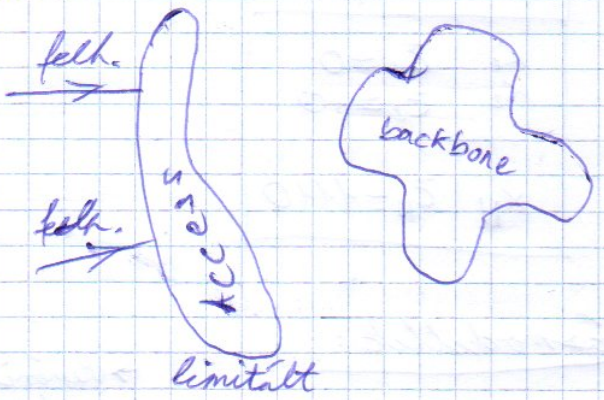
Online detekció rem működik!

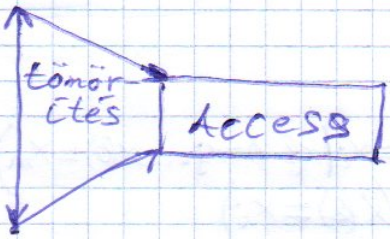
$bl = \max\{t_1 n_2 + t_2, n_1 \cdot t_2 + t_1\}$

Adattömörítés – forráskódolás

Tech. mot.

Kis adatátviteli sebességű csat. Hogyan lehet „szélessávú" szolg. megvalósítása!

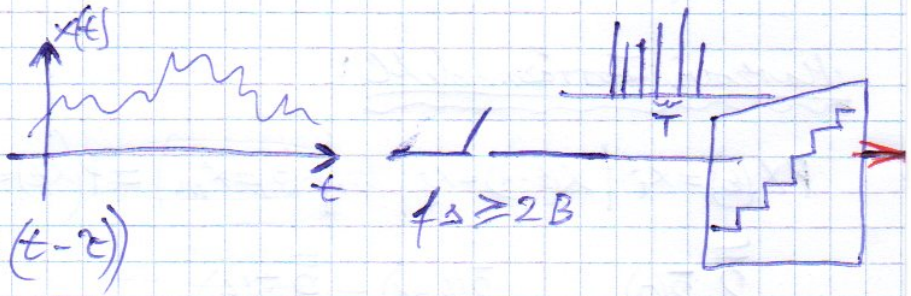




IT: van-e elvi alsó határ

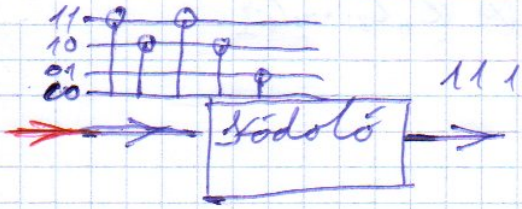
Gyakorlati: JPEG/MPEG, APC, Entrópia alapú alg.

Intuitív modell



$$R(\tau) = E\left(x(t) \times (t-\tau)\right)$$

$$F(f) = \int_{-\infty}^{\infty} R(\tau)\, e^{-j4\pi\tau}\, d\tau$$



adatátviteli seb.: f_s on

- 8 kHz · 8 bit = 64 kbps
- 44,1 kHz · 16 bit = 84 Mbps

?!?

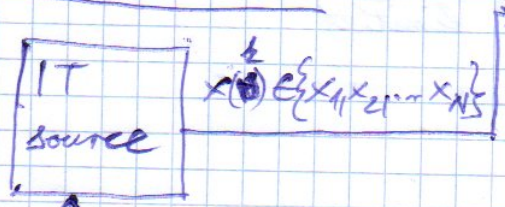
A közcsatlakozási csatorna nem támogatja ezeket az adatátviteli sebességeket

Ötlet:

LUT

X	$\bar{c}_i$
x_1	$\bar{c}_1 = 0$
x_2	$\bar{c}_2 = 10$
⋮	
x_N	$\bar{c}_N = 1110$

Forrásmodellek:



Memória mentes forrás

~~$P(x(k)) = P(x(k-1))$~~

$P(x(k) = x_i \mid x(k-1) = x_j, \dots, x(0) = x_m) = P(x(k) = x_i)$

$p_i = P(x(k) = x_i), \; i = 1, \dots, N$

$\bar{p}$

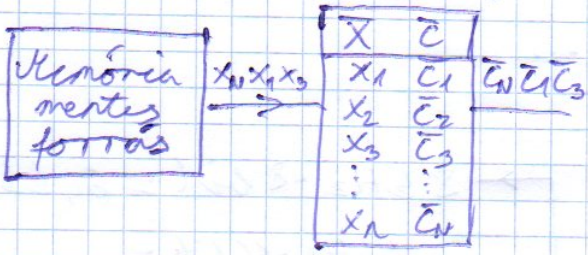
Markovi Forrásmodell:

$$P(x(k) = x_i \mid x(k-1) = x_j \mid \dots \mid x(0) = x_m) = P(x(k) = x_i \mid x(k-1) = x_j) \rightarrow p_{ij}$$

$$\bar{\bar{P}} \; \bar{p}(0) \qquad \bar{p}(k+1) = \bar{\bar{P}} \, \bar{p}(k)$$

Forráskódolás: $P(x) \; \{p_1, p_2, \dots, p_n\}$ $\quad \bar{c}(x) \; \{\bar{c}_1, \bar{c}_2, \dots, \bar{c}_n\}$

$x \in \{x_1, x_2, \dots, x_n\}$ $\quad l(x) \; \{l_1, l_2, \dots, l_n\}$



Átlagos kódszóhossz: $L = E(l(x)) = \sum_x p(x) \, l(x)$

Adatátviteli sebesség: $f_s \cdot L$

C_{opt}: $\min_{C} L$

Kérdések:

- Lehet-e változó szóhosszúságú kódokat egyértelműen dekódolható
- $\ell(x) = ?$ elvi alsó határa?

Egyértelműen dekódolható kódok

prefix-mentes kódok

↓

bináris fa

Kraft-egyenlőtlenség

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

$$\sum_x z^{L-\ell(x)} \leq z^L$$

Információ: $I(x) = \underset{(\log_2)}{ld} \frac{1}{p(x)} \geq 0 \rightarrow H(x) = E(I(x)) = \sum_x p(x) ld \frac{1}{p(x)}$ (entrópia)

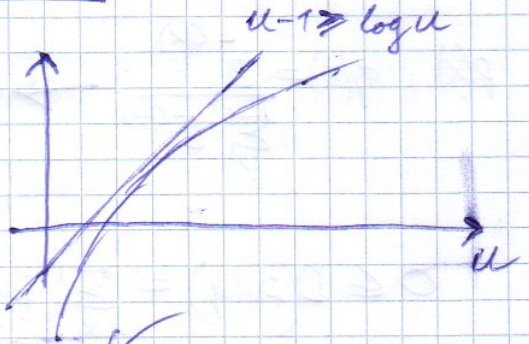
I-divergencia (távolság): $p(x)$ és $q(x)$ $\quad D(p\|q) = \sum_x p(x) ld \frac{p(x)}{q(x)} \geq 0$

- $D(p\|q) \leq 0$

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

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

$$= \sum_x q(x) - \sum_x p(x) = 1 - 1 = 0$$



$\boxed{0 \le H(x) \le \ld N}$

$p(x)$, $q(x) = \frac{1}{N}$, $0 \le D(p\|q) = \sum_x p(x) \ld \frac{p(x)}{1/N} = \sum_x p(x) \ld (N \cdot p(x)) =$

$= \sum_x p(x) \{\ld p(x) + \ld N\} =$

$= \sum_x p(x) \ld p(x) + \ld N \sum_x p(x)$

$0 \le -H(x) + \ld N \rightarrow H(x) \le \ld N$

$H(x) = \sum_x p(x) \ld \frac{1}{p(x)} \ge 0$

Forráskódolási tétel:

$H(x) \le L$

$\sum_x p(x) \ld \frac{1}{p(x)} \le \sum_x p(x) l(x)$

$p(x)$, $q(x) = \frac{2^{-l(x)}}{\sum_y 2^{-l(y)}} \rightarrow 0 \le q(x) \le 1$, $\sum_x q(x) = \frac{\sum_x 2^{-l(x)}}{\sum_y 2^{-l(y)}} = 1$

$0 \le D(p\|q) = \sum_x p(x) \ld \frac{p(x)}{2^{-l(x)} / \sum_y 2^{-l(y)}} = \sum_x p(x) \ld \{p(x) 2^{l(x)} \cdot \sum_y 2^{-l(y)}\}$ (≥ 1)

$\le \sum_x p(x) \ld \{p(x) 2^{l(x)}\} = \sum_x p(x) \{\ld p(x) + l(x)\} =$

$= \sum_x p(x) \ld p(x) + \sum_x p(x) l(x) = -H(x) + L$

$\Downarrow$

$0 \le -H(x) + L$

$H(x) \le L$

Entrópia alapú tömörítési algoritmusok – Shannon–Fano (57)

$$\sum_x p(x) \operatorname{ld}\frac{1}{p(x)} \le \sum_x l(x)\, p(x) \qquad l(x) = \lceil \operatorname{ld}\frac{1}{p(x)} \rceil$$

↑ racionális szám

$$a \le \lceil a \rceil \le a+1$$

adott $p(x) \longrightarrow l(x) \longrightarrow$ bináris fa ✓ $\Rightarrow$ kódszavak

↓ LookUpTable

$$\sum_x 2^{-l(x)} \le 1 \; ; \quad \sum_x 2^{-\lceil \operatorname{ld}\frac{1}{p(x)} \rceil} \le$$

$$\le \sum_x 2^{-\operatorname{ld}\frac{1}{p(x)}} = \sum_x 2^{\operatorname{ld} p(x)} = \sum_x p(x) = 1$$

Kraft-egyenlőség ✓

Teljesítőképesség $L = \sum_x p(x)\, l(x) = \sum_x p(x) \lceil \operatorname{ld} \frac{1}{p(x)} \rceil \ge$

$$\ge \sum p(x) \operatorname{ld}\frac{1}{p(x)} = H(x)$$

$$L = \sum_x p(x) \lceil \operatorname{ld}\frac{1}{p(x)} \rceil \le \sum_x p(x)\left(\operatorname{ld}\frac{1}{p(x)} + 1\right) = \sum_x p(x) \operatorname{ld}\frac{1}{p(x)} + \sum_x p(x) =$$

$$= H(x) + 1$$

$$H(x) \le L_{sf} \le H(x) + 1 \longrightarrow \text{fa?}$$

adatátv. sebesség $f_s(H(x)+1) = f_s H(x) + f_s$ $\quad f_s$ egy nagy szám is lehet

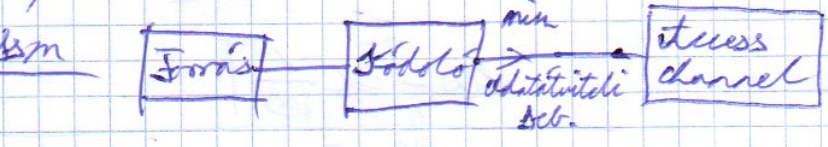
Sűrűségtorzsetés

$E = \frac{U}{d}$

$\Phi = EA$

Kódolástechnika E1 10.30.

Kihívások:
- agresszió tömörítés ??
- kis alg. komplex ..

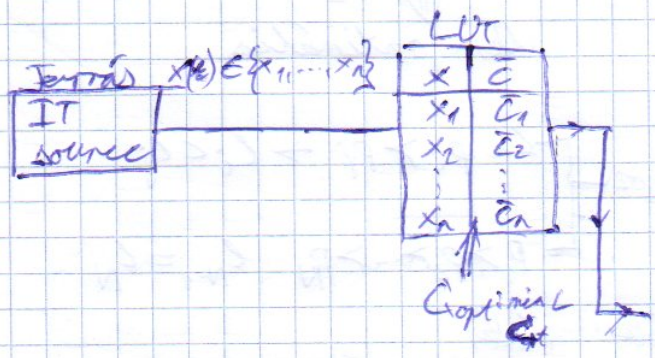


$P_1\ P_2 \quad P(x) \to P(x)$

$x_1, x_2, \dots, x_n \to X$

$c_1\ c_2 \dots c_n \to c(x)$

$l_1\ l_2 \dots l_n \to l(x)$



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

$f_s \cdot L \quad , f_s \geq 2B$

$H(x) = \sum_x p(x) \operatorname{ld} \frac{1}{p(x)}$

$H(x) \leq L$

Shannon-Fano kód:

$$l(x) = \left\lceil \operatorname{ld} \frac{1}{p(x)} \right\rceil$$

adott: $p(x) \to l(x) \to$ cim fa $\to$ LUT

$H(x) \leq L_{SF} \leq H(x) + 1$

Num. példa

$p_1 = 0{,}49 \quad p_2 = 0{,}14 \quad p_3 = 0{,}\overset{14}{0}7 \quad p_4 = 0{,}0\cancel{7} \quad p_5 = 0{,}07 \quad p_6 = 0{,}04$

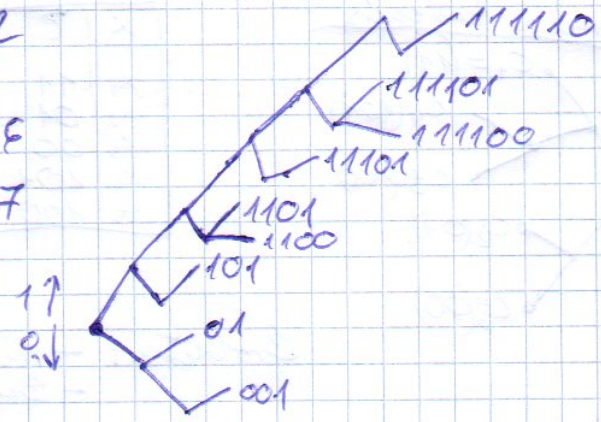
$p_7 = 0{,}02 \quad p_8 = 0{,}02 \quad p_9 = 0{,}01$

$l_1 = \operatorname{ld} \frac{1}{0{,}49} = \lceil 1{,}029 \rceil = 2$

$l_2 = 3 \quad l_5 = 4 \quad l_4 = 5$

$l_3 = 3 \quad l_6 = 5 \quad l_9 = 7$

$l_4 = 4 \quad l_7 = 6$



$x \rightarrow$

x	c(x)
x_1	01
x_2	001
x_3	101
x_4	1100
x_5	1101
x_6	11101
x_7	111100
x_8	111101
x_9	1111101

$\rightarrow c(x)$

$L = 2{,}89 \qquad H(x) = 2{,}314$

$\xi = \frac{H(x)}{L} \approx 80\%$

$l(x) = \left\lceil \mathrm{ld}\,\frac{1}{p(x)} \right\rceil$

$\Downarrow$

Nem optimális

Huffman-kód

opt. kritériumok:
- ha $p_i > p_j \rightarrow l_i < l_j$
- $p_1 > p_2 > \dots > p_N \quad l_{N-1} = l_N$

opt. kódnövesztés

"k": $\bar{p}(k) = p_1(k)\, p_2(k) \dots p_N(k)\,,\; l_1(k), l_2(k), \dots, l_n(k)$

"k+1" $\bar{p}(k+1) = p_1(k)\, p_2(k) \dots p'_N(k+1)\, p'_{N+1}(k+1)\,,$

$l_1(k), l_2(k), \dots, l_N(k+1), l_{N+1}(k+1)$

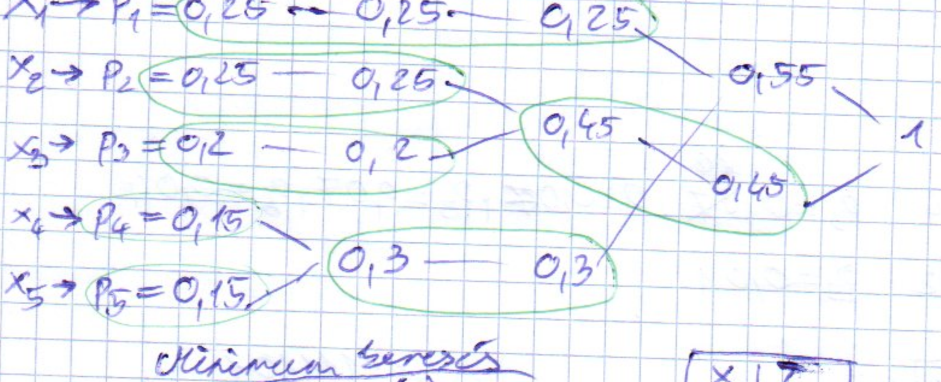
$\| \; p'_N(k+1) + p'_{N+1}(k+1) = p_N(k)$

$l_n(k) + 1$

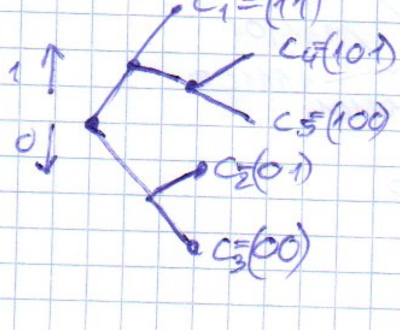
$L(k+1) = \sum_{i=1}^{N+1} p_i(k+1)\, l_i(k+1) =$

$= \sum_{i=1}^{N-1} p_i(k)\, l_i(k) + p'_N(l_n(k)+1) + p'_{N+1}(l_n(k)+1) =$

$= \sum_{i=1}^{N-1} p_i(k)\, l_i(k) + p_N(k)\, l_N(k) + p_N(k) = L(k) + p_N(k) \Rightarrow$ min. növekedés



Minimum keresés



x	c
x_1	11
x_2	01
x_3	00
x_4	101
x_5	100

$L = 2{,}3$ bit

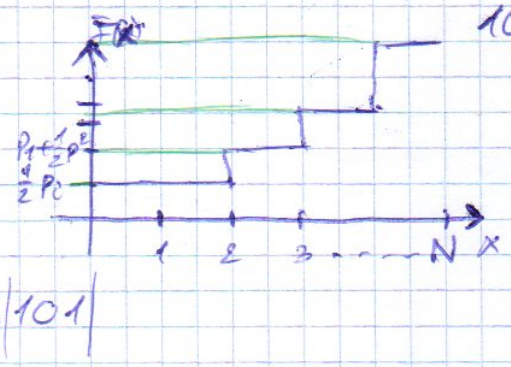
Probléma:
- minimum keresés
- bináris fa

$\Rightarrow$ kompl. nagy.

De: $-\bar{p}(k)$, k időben inhomogén

~~Huffman~~ 10.30.

Shannon-Fano-Elias kód SFE



$$\bar{F}(x) = \sum_{a<x} p(a) + \frac{1}{2} p(x)$$

kumulatív eloszlásfv.

$0.5 \rightarrow 0.|101|$

$$l(x) = \left\lceil ld \frac{1}{p(x)} \right\rceil + 1$$

adott: $p(x) \rightarrow \bar{F}(x) \rightarrow$ Bin conv. $\rightarrow$ Truncate (levágás) $\rightarrow$ kód $\rightarrow$ LUT

$p(x) \rightarrow l(x) = \left\lceil ld \frac{1}{p(x)} \right\rceil + 1 \rightarrow$ Truncate

előny: - nincs sorbarendezés
- nincs bin. fa

$$L(x) = \sum_x p(x) l(x) = \sum_x p(x) \left(\left\lceil ld \frac{1}{p(x)} \right\rceil + 1 \right) < \sum_x p(x) \left(ld \frac{1}{p(x)} + 1 + 1 \right) =$$

$$= \sum_x p(x) ld \frac{1}{p(x)} + 2 \sum_x p(x) = H(x) + 2$$

Num. példa

		$\bar{F}(x)$		$l(x)$	$z(x)$
x_1	$p_1 = 0,25$	$0,125$	$0,001$	3	001
x_2	$p_2 = 0,25$	$0,375$	$0,011$	3	011
x_3	$p_3 = 0,2$	$0,6$	$0,10011$	4	1001
x_4	$p_4 = 0,15$	$0,775$	$0,11000111$	4	1100
x_5	$p_5 = 0,15$	$0,925$	$0,11110110$	4	1110

$L_{SFE} = 3,5 > L_H = 2,3$

	Opt	tlg komplex
H	☺	min. keresés + bin fa
SF	$L < H(x)+1$	bin fa
SFE	$L < H(x)+2$	bin ~~fa~~ dec. konv.

alg. komplex ↓ tlg. képesség ↑

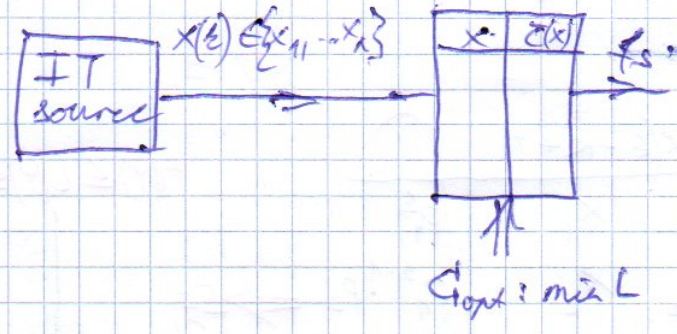
cél: $H(x) \leq L \leq H(x) + \varepsilon$??

Kódolástechnika

11.04.
8. hét

~~1000 kHz~~
~~$20 \cdot 10^{-9}$~~ s

Ismétlés



$$\bar{l}(x) = \sum_x p(x) l(x) = \sum_x p(x) \cdot \bar{l}(l(x))$$

$$H(x) \le L$$

$$\sum_x p(x) \operatorname{ld} \frac{1}{p(x)}$$

$$\begin{cases} p_1\ p_2\ \dots\ p_N \leftarrow p(x) \\ x_1\ x_2\ \dots\ x_N \leftarrow x \\ \bar{c}_1\ \bar{c}_2\ \dots\ \bar{c}_N \leftarrow \bar{c}(x) \\ l_1\ l_2\ \dots\ l_N \leftarrow l(x) \end{cases}$$

Shannon	L_{opt}	komplex. vagy
ST	$L_{ST} \le H(x)+1$	közepes
STE	$L_{STE} \le H(x)+2$	real-time

$$H(x) \le L \le H(x) + \varepsilon \quad ??$$

Együttes entrópia

$$H(x,y) =$$

$$P(x,y) = P(x) \cdot P(y)$$

$$= \sum_x \sum_y P(x,y) \operatorname{ld} \frac{1}{P(x,y)} = \sum_x \sum_y P(x) \cdot P(y) \cdot \left(\operatorname{ld} \frac{1}{P(x)} + \operatorname{ld} \frac{1}{P(y)} \right) =$$

$$= \sum_x P(x) \operatorname{ld} \frac{1}{P(x)} \underbrace{\left(\sum_y P(y) \right)}_{=1} + \sum_y P(y) \operatorname{ld} \frac{1}{P(y)} \underbrace{\left(\sum_x P(x) \right)}_{=1}$$

$$H(x,y) = \sum_x P(x) \operatorname{ld} \frac{1}{P(x)} + \sum_y P(y) \operatorname{ld} \frac{1}{P(y)}$$

$$H(x_1, x_2, \dots x_k) = \sum_{i=0}^{k} H(x_i) \rightarrow \text{i.i.d.r.v.} \rightarrow k \cdot H(x)$$

Blokk kódolás:

$\bar{X} = \{X(k), X(k-1), \dots, X(k-K+1)\} \longrightarrow H_1(\bar{X}) = K \cdot H_1(X)$

- azonos eloszlású v. v. (i.i.d. val. v.)

Y	$X(k)$	$X(k-1)$	$\dots$	$X(k-K+1)$	
y_1	x_1	x_1	$\dots$	x_1	p_1^k
y_2	x_1	x_1	$\dots$	x_2	$p_1^{k-1} \cdot p_2$
$\vdots$	$\vdots$	$\vdots$		$\vdots$	
y_{M^K}	x_M	x_M		x_M	p_M^k

$\Rightarrow$ SI kód

$H(Y) \le L(Y) \le H(Y)+1$

$H(Y) \le L_Y \le K \cdot H(X) + 1$

$H(X) \le L_Y \le H_1(X) + 1$

$K H(X) \le L_Y \le K H_1(X) + 1$

$\gamma^{(K)} = \frac{L_Y}{K}$

$H(X) \le \gamma^{(K)} \le H_1(X) + \frac{1}{K}$

$K = \left\lceil \frac{1}{\varepsilon} \right\rceil$

$O\left(\frac{1}{K}\right) \Longleftrightarrow O(K^M)$

$p(x)$ eloszlás kell! $\Leftarrow$ 1 döbeni változás

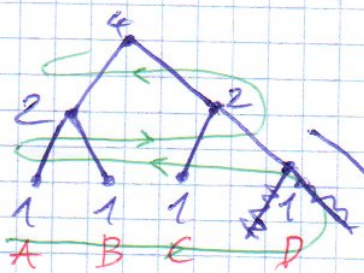
de becsülés

Distributiv free

1104
9.167

adaptív Huffman $p(x)$ ismeretlen (Pl.: JPEG, MPEG)

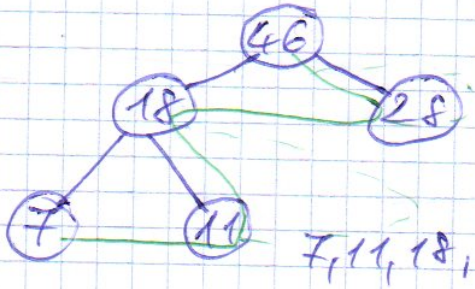
Sibling pair property



- gyerekek összege = szülő

⊖ 18+28=46

⊖ 7+11=18

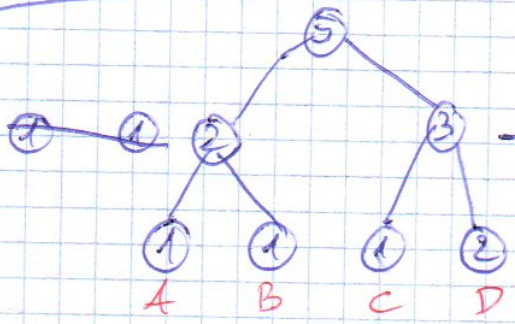


7, 11, 18, 28, 46

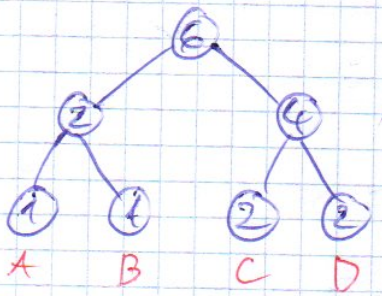
- szig. mon. rem csökkenő

ABCD → DCD4

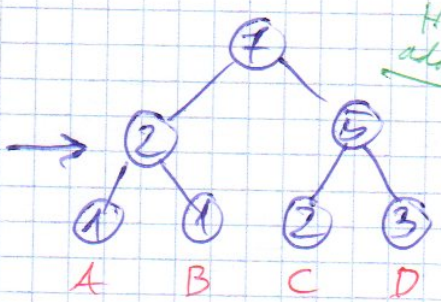
be: D



be: C



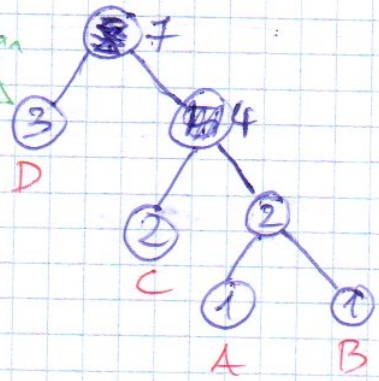
be: D



1, 1, 2, 3, 2, 5, 7

⇔

Huffman adaptív



1, 1, 2, 2, 3, 4, 7 ✓

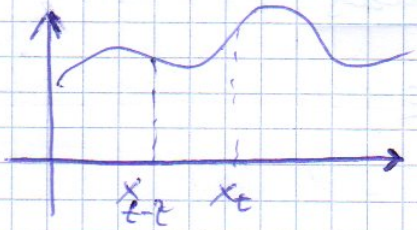
LEFT algorithm

LEFT algorithm

Kódolástechnika 11. 06.
9. ea

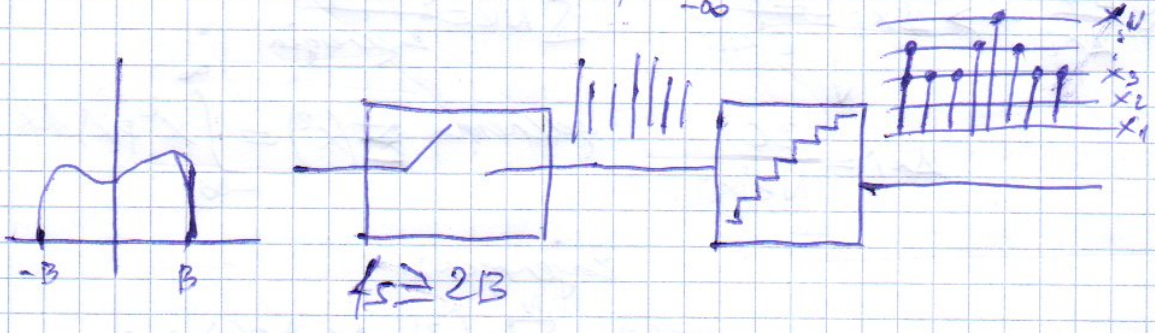
Autokorrelációs függvény

$$R(\tau) = E(x(t)\,x(t-\tau))$$

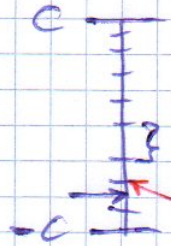


Energiaspektrum:

$$F(f) = \int_{-\infty}^{\infty} R(\tau)\, e^{-j2\pi f t}\, d\tau$$



Egyenletes lépésközű kvantálás



$$\Delta = \frac{2C}{N} \; ; \; N = 2^n \; , \; \varepsilon = x - \hat{x} \; , \; SNR = \frac{\text{átlagos jelenergia}}{\text{kvantálási zaj}}$$

jel-zaj viszony

$$\varepsilon \in [-\Delta/2, \Delta/2]$$

átlagos jelenergia: $\frac{C^2}{2}$

$$P_\varepsilon(x) = \frac{1}{\Delta}$$

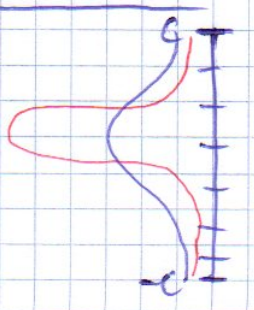
Kvantálási zajenergia:

$$E(\varepsilon^2) = \int_{-\Delta/2}^{\Delta/2} x^2 \cdot \frac{1}{\Delta}\, dx = \frac{\Delta^2}{12}$$

$$SNR = \frac{C^2/2}{\Delta^2/12} = 6\frac{C^2}{\Delta^2} = \frac{3}{2}\frac{4C^2}{\Delta^2} =$$

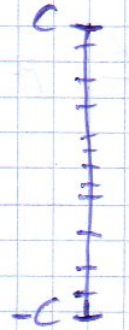
$$= \frac{3}{2}N^2 = \boxed{\frac{3}{2}2^{2n}} \Rightarrow SNR$$

Problémák:

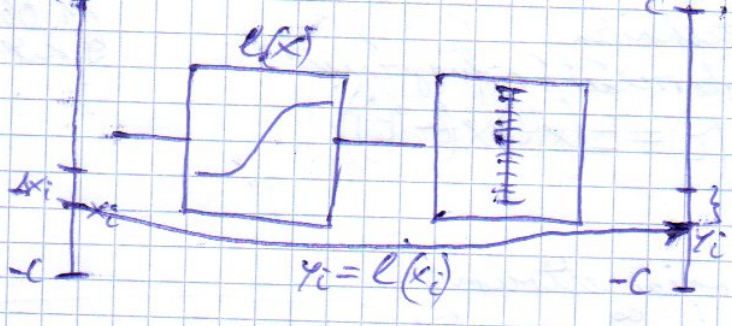


$$C' = \frac{C}{2}$$

$$SNR' = \frac{SNR}{4} \Rightarrow$$



Jobb egyenletes



Nem egyenletes lépésközű kvantálás

$$\ell'(x_i) \approx \frac{\Delta y}{\Delta x_i} \rightarrow \Delta x_i = \frac{\Delta y}{\ell'(x_i)}$$

$$\Delta x_i = \frac{2C}{N \ell'(x_i)}$$

$$SNR = \frac{\text{jelenergia}}{\text{zajenergia}}$$

$$\text{jelenergia } E(x^2) = \int_{-\infty}^{\infty} x^2 p(x)\,dx$$

zajenergia:

$$E(\varepsilon^2) = \sum_{i=1}^{N} E(\varepsilon^2 | x \in \Delta x_i)\, p(x_i)\, \Delta x_i =$$

$$= \sum_{i=1}^{N} \frac{\Delta x_i^2}{12} p(x_i) \Delta x_i = *$$

$$\frac{d\ell(x)}{dx}$$

$$* = \sum_{i=1}^{N} \frac{4C^2}{N^2 12} \frac{1}{\ell'^2(x_i)} p(x_i) \Delta x_i = \frac{C^2}{3N^2} \int_{-C}^{C} \frac{1}{\ell'^2(x)} p(x)\,dx$$

$$SNR = \text{const} \cdot \frac{\int_{-C}^{C} x^2 p(x)\,dx}{\int_{-C}^{C} \frac{1}{\ell'^2(x)} p(x)\,dx}$$

$\ell_{opt}(x)$ max $SNR(\ell(x))$

$p(x)$-től független állandó lesz.

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

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

"A-law" $\frac{1 + \lg(Ax)}{1 + \lg(A)}$ $A = 87{,}6$

"μ-law" $\frac{1 + \lg \mu x}{1 + \lg \mu}$ $\mu = 1000$

Lloyd-Max kvantálás

$\Delta = \{\Delta_1, \Delta_2, \dots, \Delta_N\}$ $\quad Q = \{q_1, \dots q_N\}$

$$\alpha(Q,\Delta) = E(x-\hat{x})^2$$

$$E(x-\hat{x})^2 = \sum_{i=1}^{N} \int_{\Delta_i} (x-q_i)^2 p(x|x\in\Delta_i)\,dx\, P_i$$

$$P_i = \int_{\Delta_i} p(x)\,dx$$

$$Q_{opt}, \Delta_{opt} : \min_{\Delta, Q} \alpha(Q,\Delta)$$

ekkor $Q: \Delta_{opt} \to \Delta_{iopt} := \{x : (x-q_i)^2 < (x-q_j)^2;\ \forall j = 1,\dots,N | j \neq i\}$

ekkor $\Delta: Q_{opt} \to \dfrac{\partial \alpha(\Delta,Q)}{\partial q_e} = 2\int_{\Delta_i} (x-q_e)\, p(x|x\in\Delta_e)\,dx\, P_e = 0$

$$\Downarrow$$

$$q_e = E(x | x\in\Delta_e)$$

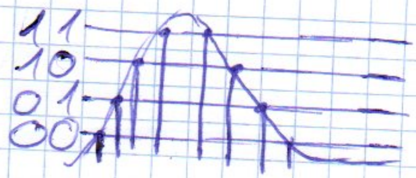
$\Delta(0), Q(0)$ — egyenletes kvantálás

$$\xrightarrow{\Delta_{opt}} \Delta(1), Q(0) \xrightarrow[Q_{opt}]{} \Delta(1), Q(1) \xrightarrow[\Delta_{opt}]{} \Delta(2), Q(1) \xrightarrow[Q_{opt}]{} \dots \to Q_{opt}, \Delta_{opt}$$

$$\alpha(Q,\Delta) \geq 0$$

$\|$ LVQ

A memória kihasználása



00 01 10 11 11 10 01

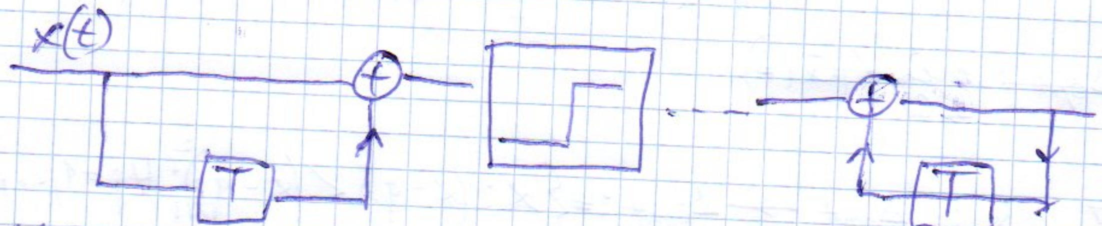
00 1 1 1 "1" 0 0 0 00

16 bit

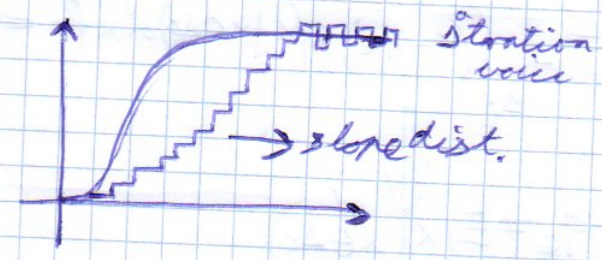
9 bit

Legyen inkább változás alapú kódolás

Diff. kvantáló $f_s \cdot n \gg f_s$



Probléma



Megoldás:

$f_s' > f_s$

Adaptív prediktív kódolás

Kérek egy üveg sö — rt 0,999
— tét gépolajat 0,001

x_t → beszéd minta a "t"-ik időpillanatban

$$\tilde{x}_t = \sum_{j=1}^{J} w_j x_{t-j}, \quad \text{"J" memória}$$

$$\varepsilon_t := x_t - \tilde{x}_t; \quad E(x_t x_{t-i}) = R(i); \quad E(x_{t-i} x_{t-j}) = R(i-j)$$

$$\underline{w}_{opt}: \min_{\underline{w}} E(\varepsilon_t^2) \sim \min_{\underline{w}} E\left(x_t - \sum_{j=1}^{J} w_j x_{t-j}\right)^2 \sim \min_{\underline{w}} E(x_t^2) \ldots$$

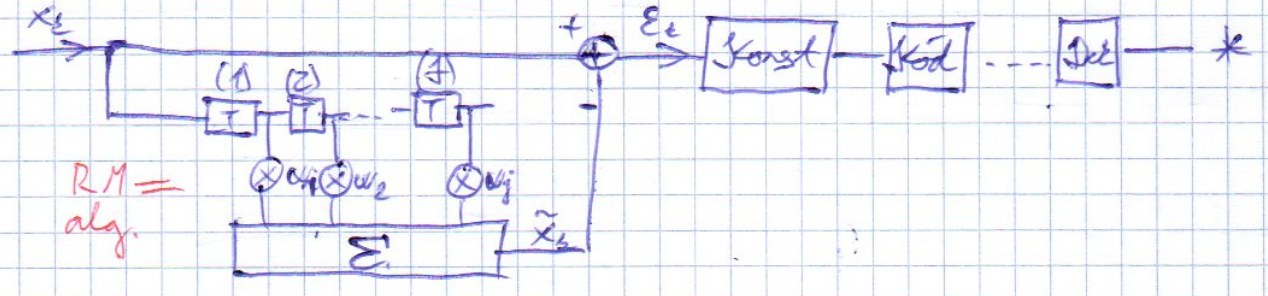
$$\sim \min_{\bar{w}} E(x_k^2) - 2\sum_{i=1}^{N_1} w_i E(x_k x_{k-i}) + \sum_{i=1}^{N_1}\sum_{j=1}^{N_1} w_i w_j E(x_{k-i} x_{k-j}) \sim$$

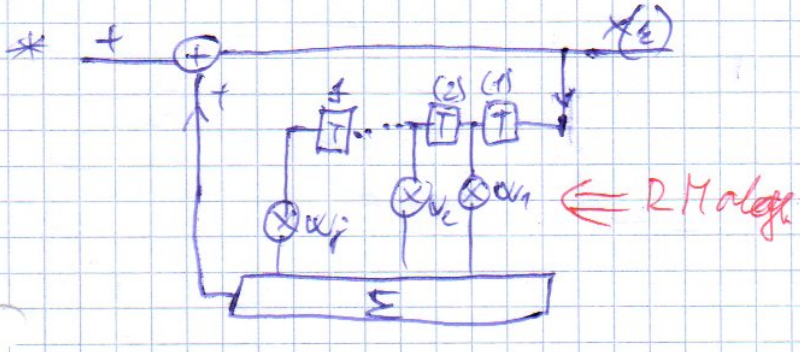
$$\sim \min_{\bar{w}} R(0) - 2\sum_{j=1}^{N_1} R(j) w_j + \sum_{i=1}^{N_1}\sum_{j=1}^{N_1} w_i w_j R(i-j) \sim \quad \bar{r}: r_i = R(j)$$

$$\bar{\bar{R}}: R_{ij} = R(i-j)$$

$$\sim \min_{\bar{w}} \bar{w}^T \cdot \bar{\bar{R}} \bar{w} - 2\bar{r}^T \bar{w} + R(0) \Rightarrow \bar{w}_{opt} \boxed{\bar{\bar{R}} \bar{w} = \bar{r}} \Rightarrow$$

$$\Rightarrow x(t) \rightarrow R(\tau) \rightarrow \bar{r}\ \bar{\bar{R}} \rightarrow \bar{w}_{opt}: \bar{\bar{R}}\bar{w} = \bar{r}$$



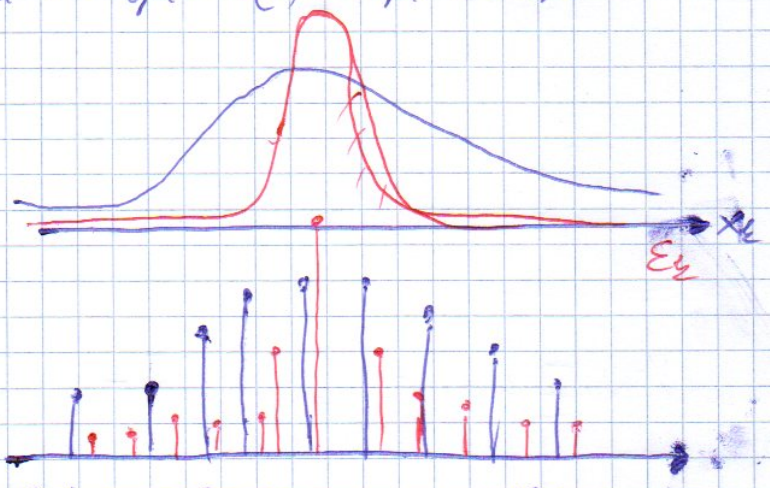


$$E(\varepsilon_k^2) = R(0) - 2\bar{r}^T \bar{w}_{opt} + \bar{w}_{opt}^T \bar{\bar{R}} \bar{w}_{opt} = R(0) - \bar{w}_{opt}^T \bar{\bar{R}} \bar{w}_{opt} =$$

$$= E(x_k^2) - \text{pozitív}$$

$$E(\varepsilon_k^2) \ll E(x_k^2)$$

predikciós szórás $\ll$ jel változásának szórása



$p(\varepsilon_k)$ → több az egyenlőtől

$p(x_k)$ kövül az egyenletesre

$$H(\varepsilon_k) < H(x_k)$$

Kell a korrelációs függvényt

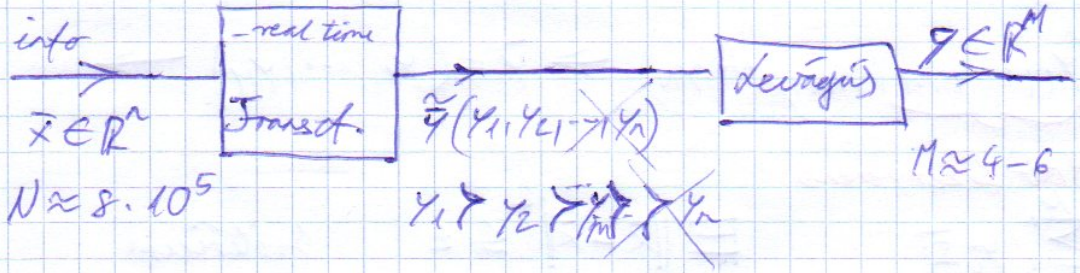
rekurzió megold:

$$w_c(k+1) = w_c(k+1) - \Delta\left\{x_k - \sum_{j=1}^{J} w_j(k) x_{k-j}\right\} x_{k-c}$$

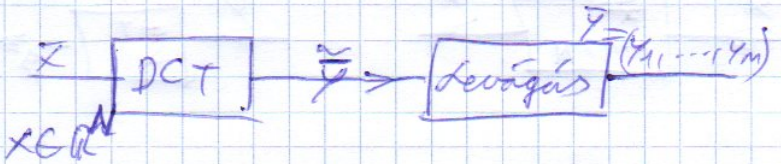
Kódolástechnika EA 11. 18.
11. hét

- 60 perc - számológép - 5db üres lap - QII

Adattömörítés transzformációs kódolással



info. veszteség $\leq \varepsilon$ JPEG/MPEG ~ pixelek csak minden második átvitel



$M \ll N$ | Nem elég agresszív

PCA (főtérelemzés) alapú tömörítés KLT transzformációval

$\bar{x} = (x_1, \dots, x_i, \dots, x_j, \dots, x_N) \rightarrow \bar{\bar{R}}: R_{ij} = E(x_i x_j)$

$\bar{\bar{R}} = E(\bar{x}\bar{x}^T)$

Tulajdonságok:

1) $R_{ij} = R_{ji}$; $\bar{\bar{R}} = \bar{\bar{R}}^T$ 2) $\forall \bar{a}, \bar{b} \in \mathbb{R}^N : \bar{a}^T \bar{\bar{R}} \bar{b} = \bar{b}^T \bar{\bar{R}} \bar{a}$

3) $\forall \bar{a} \in \mathbb{R}^N : \bar{a}^T \bar{\bar{R}} \bar{a} \geq 0$ | $\sum_i \sum_j a_i R_{ij} a_j = \sum_i \sum_j a_i E(x_i x_j) a_j =$
$= E\left(\sum_i \sum_j a_i a_j x_i x_j\right) = E\left(\sum_i \lambda_i x_i\right)^2 \geq 0$

4) $\bar{\bar{R}} \bar{s}_i = \lambda \bar{s}_i$; $\forall i = 1, \dots, N$; $\bar{s}_i^T \bar{s}_j = s_{ij} = \begin{cases} 1 & \text{if } i = j \\ 0 & \text{if } i \neq j \end{cases}$ | $\bar{s}_i^T \bar{\bar{R}} \bar{s}_j = \lambda_j (\bar{s}_i^T \bar{s}_j)$
$\bar{s}_j^T \bar{\bar{R}} \bar{s}_i = \lambda_i (\bar{s}_i^T \bar{s}_j)$

5) $\lambda_i \geq 0 \quad \forall i = 1, \dots, N$

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

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

$\bar{s}_1 \quad \bar{s}_1 \qquad \bar{s}_M \quad \bar{s}_{M+1} \qquad \bar{s}_N$

$\bar{x} = \sum_{i=1}^{N} y_i \cdot \bar{s}_i \quad$ ahol $y_i = \bar{s}_i^T \cdot \bar{x} \quad i = 1, \dots, N$

$\bar{x} \to \tilde{\bar{y}} = (y_1, \dots, y_M, y_{M+1}, \dots, y_N) \Rightarrow \bar{y} = (y_1, \dots, y_M) \longrightarrow$

M db főkomponens

$\Rightarrow \hat{\bar{x}} = \sum_{i=1}^{M} y_i \bar{s}_i \qquad \mathbb{E}\left\|\bar{x} - \hat{\bar{x}}\right\|^2 \le \varepsilon$ kritérium

– veszteséges tömörítés

$\bar{\bar{S}}_{M \times M} = \begin{pmatrix} \bar{s}_1 \\ \bar{s}_2 \\ \vdots \\ \bar{s}_M \end{pmatrix}$

$\mathbb{E}(y_i y_j) = \mathbb{E}\left(\bar{s}_i^T \bar{x}\, \bar{x}^T \bar{s}_j\right) = \bar{s}_i^T \mathbb{E}(\bar{x}\bar{x}^T)\, \bar{s}_j = \bar{s}_i^T \bar{\bar{R}} \bar{s}_i = \bar{s}_i^T \lambda_j \bar{s}_j = \lambda_i \delta_{ij}$

$\mathbb{E}(\bar{x} y_i) = \mathbb{E}\left(\bar{x}\bar{x}^T \bar{s}_i\right) = \mathbb{E}(\bar{x}\bar{x})\, \bar{s}_i = \bar{\bar{R}}\, \bar{s}_i = \lambda_i \bar{s}_i$

$\mathbb{E}\|\bar{x}\|^2 = \sum_{i=1}^{N} \mathbb{E}(x_i)^2 = \sum_{i=1}^{N} R_{ii} = \sum_{i=1}^{N} \lambda_i$

$\mathbb{E}\left\|\bar{x} - \hat{\bar{x}}\right\|^2 = \mathbb{E}\left\|\bar{x} - \sum_{i=1}^{M} y_i \bar{s}_i\right\|^2 = \mathbb{E}\|\bar{x}\|^2 - 2\sum_{i=1}^{M} \mathbb{E}(y_i \bar{x})\, \bar{s}_i^T +$

$+ \sum_{i=1}^{M} \sum_{j=1}^{M} \mathbb{E}(y_i y_j)\, \bar{s}_i^T \bar{s}_j =$

$= \sum_{i=1}^{N} \lambda_i - 2\sum_{i=1}^{M} \lambda_i + \sum_{i=1}^{M} \lambda_i = \boxed{\sum_{i=M+1}^{N} \lambda_i} \Rightarrow \min$

sajátértékek

$\boxed{\lambda_n \sim O\left(\exp(-n^2)\right)}$ ← természet ajándéka

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

Pareto eloszlás

11.18

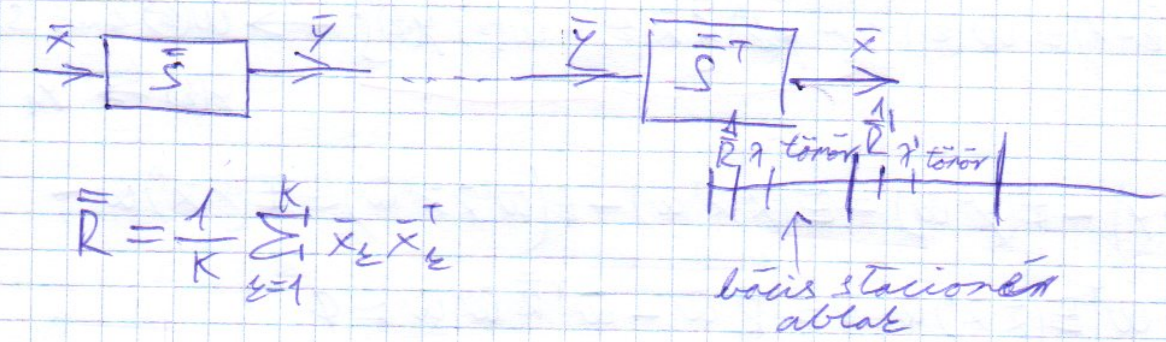
11.hét

Adott: $\bar{\bar{R}} \longrightarrow \bar{\bar{R}}\,\bar{s}_i = \lambda_i \bar{s}_i \rightarrow$

$\lambda_1 > \lambda_2 > \dots > \lambda_M > \lambda_{M+1} > \dots > \lambda_N \Rightarrow$

$\Rightarrow M: E\|\bar{x}-\hat{\bar{x}}\|^2 = \sum_{i=M+1}^{N} \lambda_i \le \varepsilon$

$\bar{\bar{S}}_{M\times N} = \begin{pmatrix} \bar{s}_1 \\ \bar{s}_2 \\ \vdots \\ \bar{s}_M \end{pmatrix}$ Offline



$\bar{\bar{R}} = \frac{1}{K}\sum_{k=1}^{K} \bar{x}_k \bar{x}_k^T$

Sajátérték számítás:

$\det(\bar{\bar{R}} - \lambda \bar{\bar{I}}) = 0$

Gyors sajátérték keresés

$\lambda_1, \bar{s}_1 \rightarrow \max_{\bar{w}} f(\bar{w}) \sim \max_{\bar{w}} \frac{\bar{w}^T \bar{\bar{R}}\bar{w}}{\bar{w}^T \cdot \bar{w}} \sim \max_{\bar{w}} \bar{w}^T \bar{\bar{R}}\bar{w} \quad \|\bar{w}\|=1$

$\sum_{i=1}^{N} \kappa_i \bar{s}_i = \bar{w} \qquad \bar{w}^T \bar{s}_i = \kappa_i \qquad \|\bar{\kappa}\|^2 = \sum_{i=1}^{N} \kappa_i^2 = 1$

$\sum_{i=1}^{N}\sum_{j=1}^{N} \kappa_i \kappa_j \bar{s}_i^T \bar{\bar{R}}\bar{s}_j = \sum_{i=1}^{N}\sum_{j=1}^{N} \kappa_i \kappa_j \lambda_i \delta_{ij} = \sum_{i=1}^{N} \lambda_i \kappa_i^2 \le$

$\le \lambda_1 \sum_{i=1}^{N} \kappa_i^2 = \lambda_1$

$\bar{w}_{opt} = \bar{s}_1$

Elegendő optimalizálásként felfogni

$\rightarrow \operatorname{grad}_{\bar{w}} f(\bar{w}) = \bar{\bar{R}}\bar{w} - (\bar{w}^T \bar{\bar{R}}\bar{w})\,\bar{w}$

$$\bar{w}(k+1) = \bar{w}(k) + \gamma \left\{ \bar{\bar{R}}\, \bar{w}(k) - \bar{w}^T(k)\, \bar{\bar{R}}\, \bar{w}(k)\, \bar{w}(k) \right\} \longrightarrow \bar{w}(k) \to \bar{s}_1$$

$\bar{\bar{R}}$ ismeretlen ; kell olyan alg. ami $\bar{\bar{R}}$ ismerete nélkül megadja a legnagyobb sajátértéket

$\bar{x}(k)$, $y(k) = \bar{w}^T(k)\, \bar{x}(k)$

$$\bar{w}(k+1) = \bar{w}(k) + \gamma\, y(k) \left\{ \bar{x}(k) - \bar{w}(k)\, y(k) \right\} \longrightarrow \bar{w}(k) \text{ konv. } \bar{s}_1$$

$y(k) \xrightarrow{\text{konv}} y_1$

$$\mathbb{E}(\bar{x} \cdot y) - \mathbb{E}(y^2 \bar{w}) = \mathbb{E}(\bar{x}\bar{x}^T\bar{w}) - \mathbb{E}(\bar{w}^T\bar{x}\bar{x}^T\bar{w}) = \mathbb{E}(\bar{x}\bar{x}^T)\bar{w} -$$

$$- \bar{w}^T \mathbb{E}(\bar{x}\bar{x}^T)\bar{w}\,\bar{w} = \bar{\bar{R}}\,\bar{w} - \bar{w}^T\bar{\bar{R}}\,\bar{w}\,\bar{w} = \phi$$

Megadja az első főkomponenst

↳ Ebből az első n főkomponens megkapható

(lin. művelet, $\bar{\bar{R}}$, csak a fonek megfigyelésével)