10-09-07 Kódolástechnika

Levendovszky János

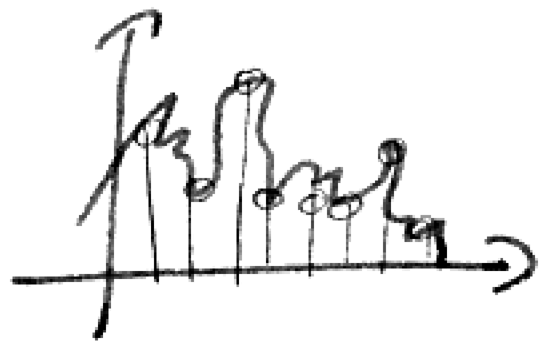
· diák letölthetők
· 1 ZH a félév végén → ld ZH terv
· csak az előadáson elhangzott dolgokat kérdezik

· Forráskódolás, csatornakódolás, adatbiztonság

Csatornakódolás (hibajavító kódolás)

IT forrásmodell: a forrás egy véletlen folyamat

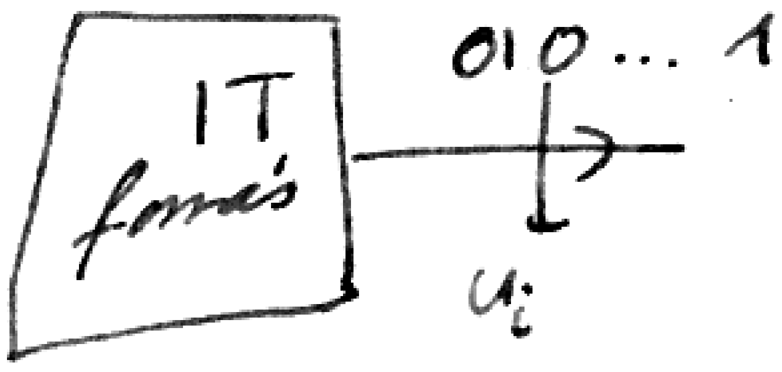
IT → információelméleti



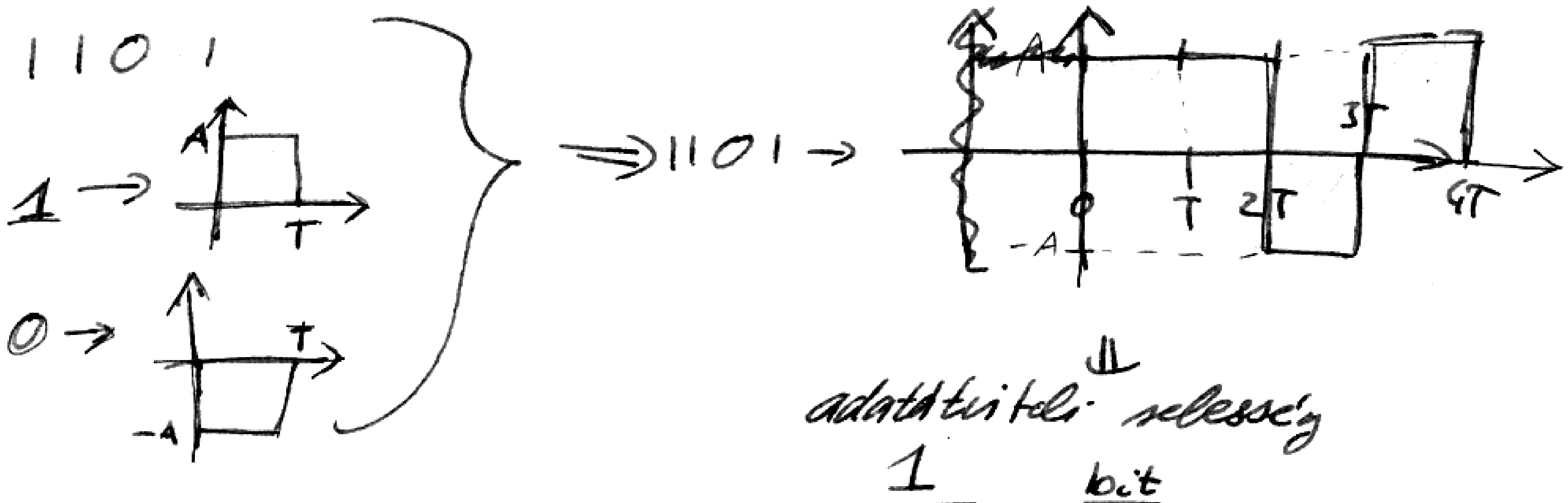
mintavételezzük (diszkretizáljuk) időben és amplitúdóban

· amplitúdóban is, amplitúdónként tekintett szimbólum

szimb.	kódszó
α_1	000
α_2	001
⋮	⋮
α_n	111



$P(u_i=1)=P(u_i=0)=\frac{1}{2}$ (⟺ a sorozatban egyenlő az 1 és 0 valószínűsége)



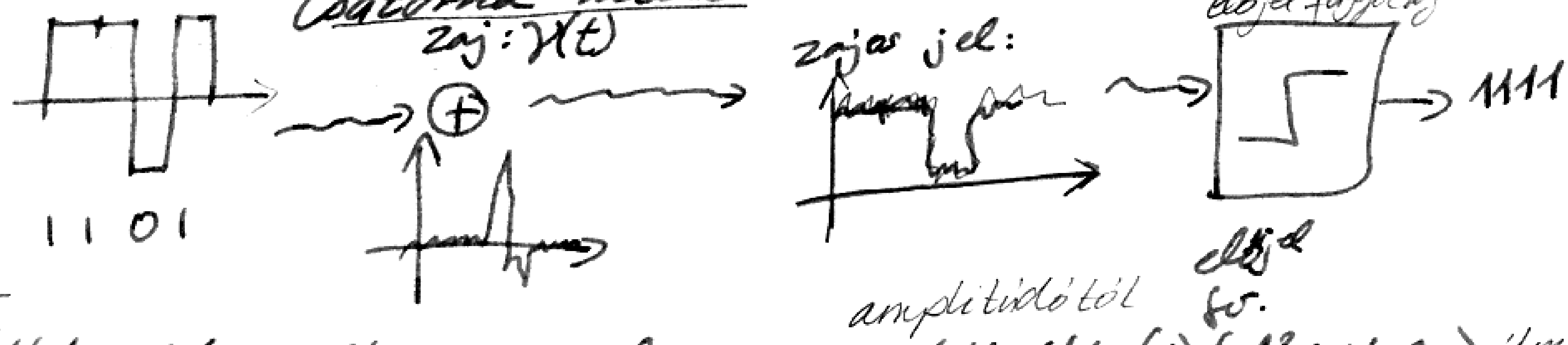
⇓

adatátviteli sebesség

$\frac{1}{T}$ $\frac{\text{bit}}{\text{sec}}$

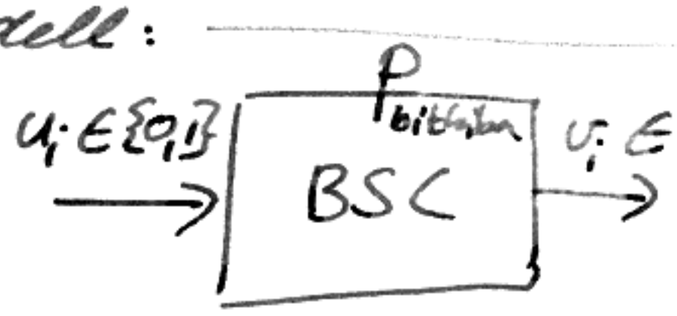
Csatorna modell

· analóg



A bithibázás valószínűsége függ az amplitúdótól (A) (A^2 ~ teljesítmény)

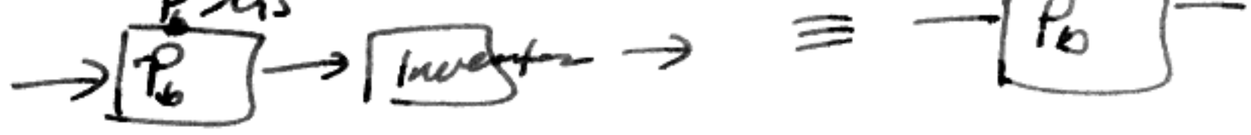
Csatornamodell:



$$P_{bithiba} = P(v_i = 1 \mid u_i = 0) = P(v_i = 0 \mid u_i = 1)$$

Bithiba valószínűsége: 1 volt 0-ra vagy 0 volt 1-re

$0 \le P_b \le 0{,}5$, mert.

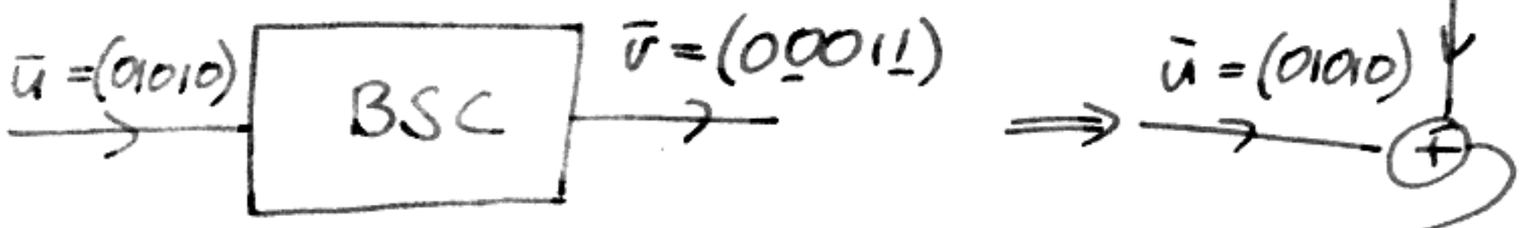


$\bar{u} = (01010) \rightarrow$ BSC $\rightarrow \bar{v} = (00011)$ $\quad P(\bar{v}|\bar{u}) = P_b^2 (1-P_b)^{5-2} \Rightarrow$

$\Rightarrow P(\bar{v}|\bar{u}) = P_b^{d(\bar{u},\bar{v})} (1-P_b)^{n-d(\bar{u},\bar{v})} =$ ($d(\bar{u},\bar{v})$: hibák száma)

$= \left(\frac{P_b}{1-P_b}\right)^{d(\bar{u},\bar{v})} (1-P_b)^n =$

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

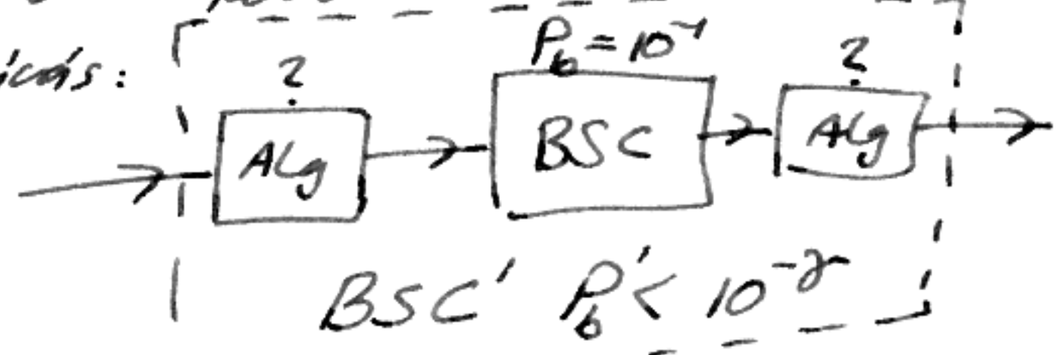


Technológiai kihívások

- Sávkorlátozott
- $P_b \sim 10^{-4}$ (adóteljesítmény-korlát miatt)

10-09-07 Kódoláselmélet

Kikódolás:

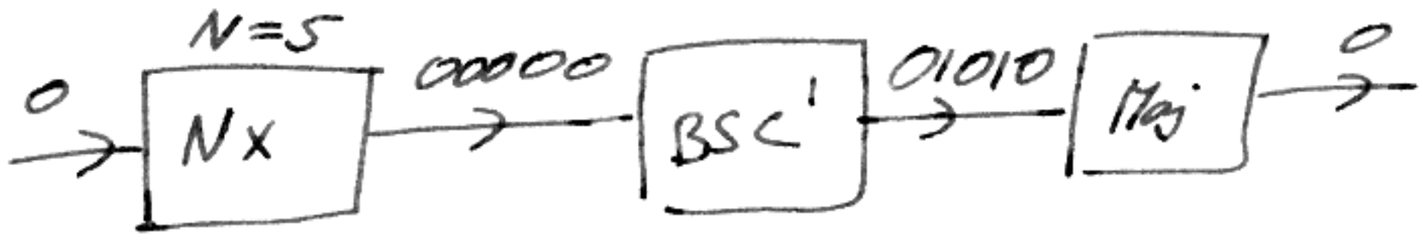


γ: QOS ≈ 6

↓

Quality of Service

pl.

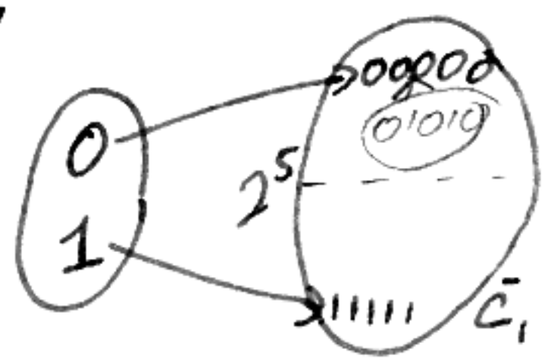


$\sum_{i}^{N} \binom{N}{i} P_b^i (1-P_b)^{n-i} \approx 10^{-6} \ll P_b'$, ha N nagy

$i = \lceil \frac{N}{2} \rceil$

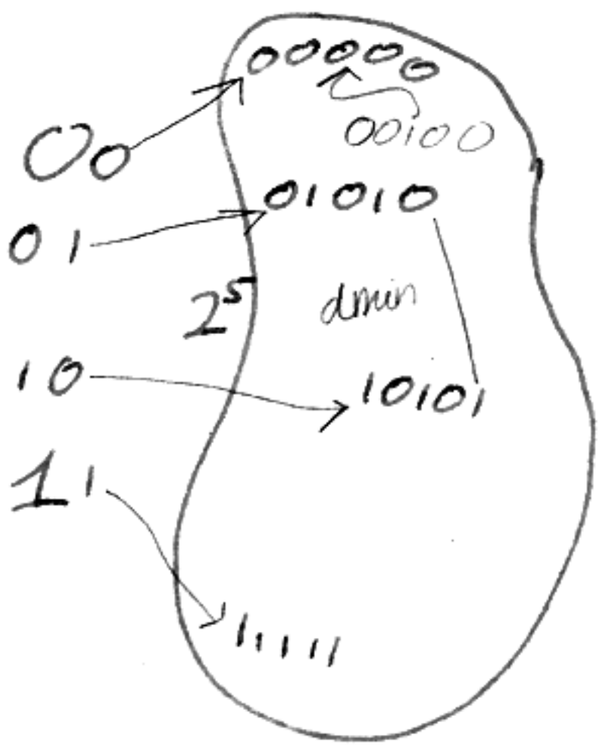
ár:

$\frac{1}{N}$ adatátviteli sebesség



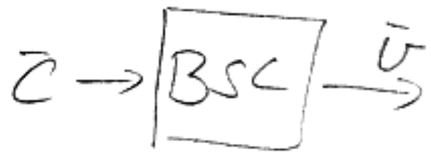
kitejesztett állapottér → hibadetekció, javítás

Hibajavító kódolás, geometriai interpretáció



$d_{min} = \min \bar{c}_i, \bar{c}_j \in C \quad d(\bar{c}_i, \bar{c}_j)$

$i \neq j$



javítható hibák száma: $d_{min} - 1$

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

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

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

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

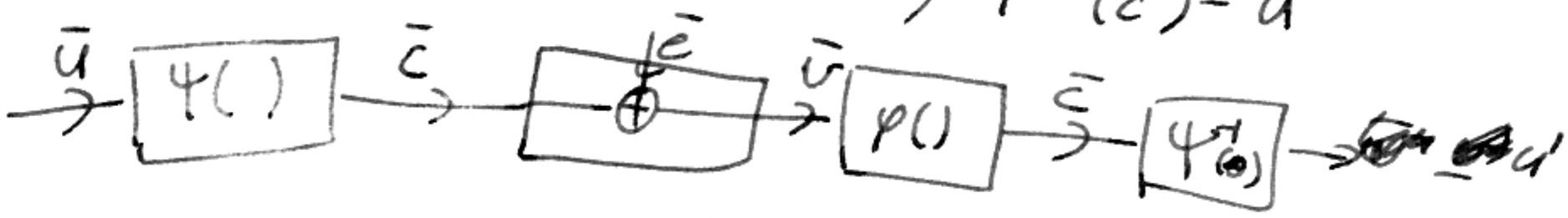
$2\, d(\bar{v}, \bar{c}) < d_{min}$

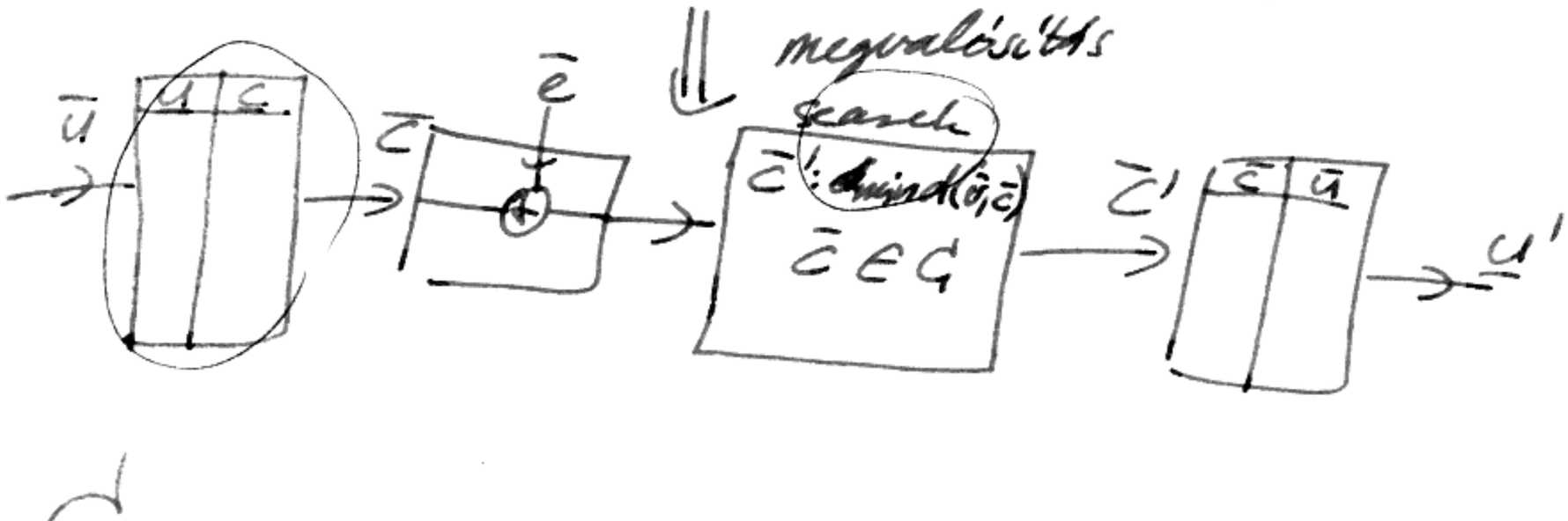
C_{opt} : max d_{min} ; $d_{im}(\bar{c}) \leq \beta$
C ↑ dimenzió

Folytatás

Formális modell

- üzenet: $\bar{u} = (\underbrace{010\ldots0}_{k}) \in \{0,1\}^k$; $\dim(\bar{u}) = k$
- kód: $C = \{\bar{c}^{(1)}, \bar{c}^{(2)} \ldots \bar{c}^{(M)}\}$, $M = 2^k$ $\dim(\bar{c}) = n > k$
- kódolás: $\psi \; \{0,1\}^k \to C$; $\psi(u) = \bar{c}$
- Vett vektor: $\bar{v} \in \{0,1\}^n \supset C$
- detekció: $\varphi(0,1)^n \to C$, $\varphi(\bar{v}) = \bar{c}$, $\bar{c} \min_{\bar{c} \in C} d(\bar{v}, \bar{c})$
- dekódolás: $\psi^{-1} \; C \to \{0,1\}^k$; $\psi^{-1}(\bar{c}') = \bar{u}'$



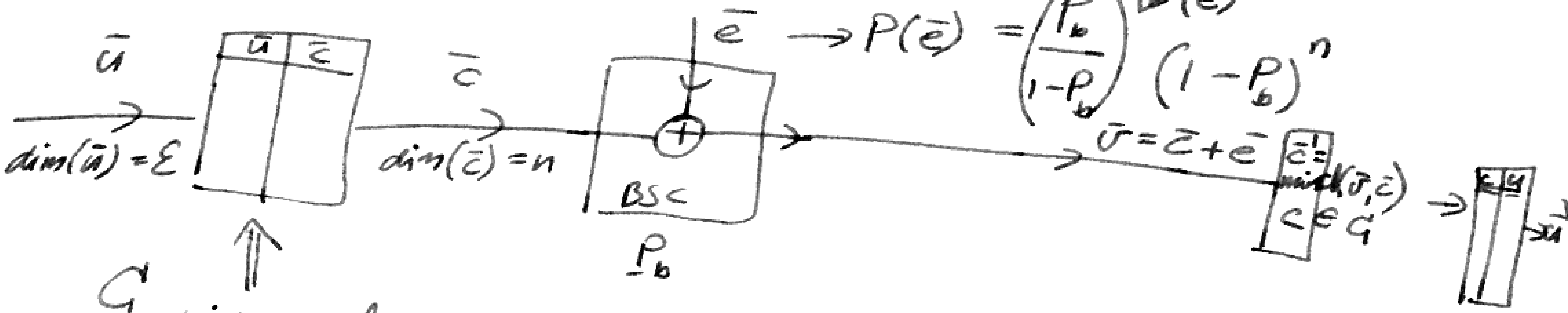


C_{opt} : max dmin ; $h - k \leq \alpha$

Problémák: on-line complexity $3 \cdot O(2^k)$ – nagy a késleltetés
↳ nem késleltethető, nem real-time

off-line complexity $O\binom{2^n}{2^k}\binom{2^k}{2}$ ← túl sokáig tart, késleltethetetlen

10-09-09 Kódtech



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

C_{opt}: max d_{min}; $n-k \leq \varepsilon$

C

$\Longrightarrow 3C(2^k) \Longrightarrow$ nem real-time a cucc, hadiászati és űrtechnológiai célra használják

---

Ma: hogy lehet polinomiális komplexet csinálni?

Kódok teljesítőképessége

$d_{min} \overset{?}{\Longleftrightarrow} n-k$ redundancia mérték

t

hib, jav képesség

· Szisztematikus kód: $\bar c = (\overset{u_1 \dots u_k,}{\text{üzenet}}, \overset{p_{k+1} \dots p_n}{\text{paritás}})$

↓ üzenetszegmens ↓ paritásbitek

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

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

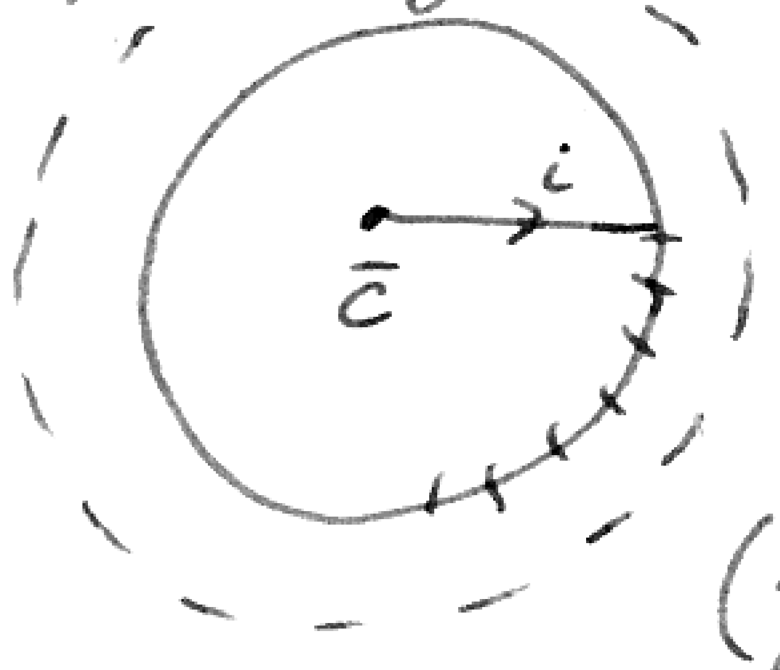
$d_{min} = n-k+1 \rightarrow$ |MDS-kód| EZ A LEGJOBB

max. distance separable

neve: $C(n,k)$

↙ kódhossz ↘ üzenethossz

Hamming-kód



hány vett vektor van, amely épp ilyen távol van?

$\binom{n}{i}(q-1)^i$ van.

t sugarú gömb térfogata $q^k \sum_{i=0}^{t} \binom{n}{i}(q-1)^i \le q^n$

↑ gömbök száma ↑ teljes tér mérete

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

Bináris eset:

$$\sum_{i=0}^{t} \binom{n}{i} \le 2^{n-k} \rightarrow \text{Perfekt eset: } \sum_{i=0}^{t} \binom{n}{i} = 2^{n-k}$$

CÉL:

MDS-kód

polinomiális kódszámával implementálható

⇓

real-time MDS-kód

Lineáris bináris kódok

$$\mathcal{G} = \{\bar{g}_1, \bar{g}_2, \dots, \bar{g}_k\} \quad \dim(\bar{g}_i) = n \quad \forall i = 1, 2, \dots, k$$

$$\downarrow$$

$$C = \mathcal{L}_C\{\mathcal{G}\}$$

lineáris burok, lineárkomb.

$$\bar{c} = \sum_{i=1}^{k} u_i \bar{g}_i \rightarrow \bar{c}, \bar{c}' \in C \rightarrow \bar{c} + \bar{c}' \in C, \quad \bar{0} \in C$$

Generátormátrix: $\bar{\bar{G}}_{k \times n}$ $\begin{pmatrix} \text{—} \bar{g}_1 \text{—} \\ \text{—} \bar{g}_2 \text{—} \\ \vdots \\ \text{—} \bar{g}_k \text{—} \end{pmatrix}$ } k db sor

minden vektor hossza n

$$\bar{c} = \bar{u} \cdot \bar{\bar{G}} = \underbrace{(\text{—} \bar{c} \text{—})}_{n} = \underbrace{(\text{—} \bar{u} \text{—})}_{k} \left(\bar{\bar{G}}\right)$$

⇒ jelentőség: ~~táblázat~~

mátrix-vektor szorzás → olcsó

Példa:

$$\bar{\bar{G}}_{2\times 5} = \left(\begin{array}{cc|ccc} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

$C(5,2)$

Kódszavak: $c_0 = (00)\cdot(G) = (00000)$

$c_1 = (01)\cdot(G) = (01\ 111)$

$c_2 = (10)\cdot(G) = (10\ 110)$

$c_3 = (10)\cdot(G) = (11\ 001)$

$\Big\}\ d_{min} = 3$

$t = \left[\frac{d_{min}-1}{2}\right] = 1$

Lineáris kódra: $d_{min} = w_{min}$

$O\binom{2^k}{2}$ $O(2^k)$

Mert: $\min_{\substack{\bar{c},\bar{c}' \in C \\ \bar{c}\neq\bar{c}'}} d(\bar{c},\bar{c}')$ az ömny súlya épp a távolság.

$\to \min_{\substack{\bar{c},\bar{c}' \in C \\ \bar{c}\neq\bar{c}'}} w(\bar{c}+\bar{c}') \sim \min_{\bar{c}'' \in C,\ \bar{c}''\neq\bar{0}} w(\bar{c}'')$

Szisztematikus kód esetén: $\bar{c} = (\bar{u}, \bar{p})$

$$G_{k\times n} = \left(\bar{\bar{I}}_{k\times k},\ \bar{\bar{B}}_{k\times(n-k)}\right)$$

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

$\forall \bar{c} \in C$ ⇝

→ kibajelzés módszere és jó gyors

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

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

Szisztematikus esetben:

$\bar{\bar{H}}_{(n-k)\times n} = (\bar{\bar{A}}_{(n-k)\times k},\ \bar{\bar{I}}_{(n-k)\times(n-k)})$;

$$(\bar{\bar{A}}_{(n-k)\times k},\ \bar{\bar{I}}_{(n-k)\times(n-k)}) \begin{pmatrix} \bar{\bar{I}}_{k\times k} \\ \bar{\bar{B}}^T_{(n-k)\times k} \end{pmatrix} = \bar{\bar{0}} \Rightarrow \bar{\bar{A}}_{(n-k)\times k} + \bar{B}^T_{(n-k)\times k} = \bar{\bar{0}}$$

$\Downarrow$

$\bar{\bar{A}} = -\bar{\bar{B}}^T$ ($-x$, mert bináris)

$\Downarrow$

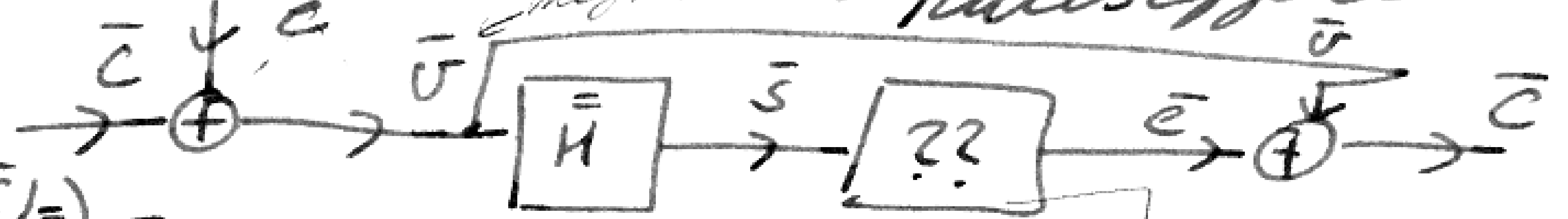
$\bar{\bar{A}} = \bar{\bar{B}}^T$

A példában:

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

$\bar{\bar{A}} = \bar{\bar{B}}^T$ ↗ $\bar{\bar{I}}_{3\times 3}$ ↑

meghívható **Kulcsegyenlet**



$\dim(\bar{S}) = n-k$; $\bar{\bar{H}} \cdot \bar{v}^T = \bar{S}^T$ ← kiszámolható

$$\bar{\bar{H}}(\bar{c}+\bar{e})^T = \bar{s} \Rightarrow \underbrace{\bar{\bar{H}} \bar{c}^T}_{\bar{0}} + \bar{\bar{H}}\bar{e}^T = \bar{S}^T$$

$$\boxed{\bar{\bar{H}}\bar{e}^T = \bar{S}^T}$$

ismert ($\bar{\bar{H}}$), adott ($\bar{S}^T$)

n-k db egyenlet
n db ismeretlen ⇒ alulhatározott

$$E_{\bar{s}} := \{\bar{e} : \bar{\bar{H}}\bar{e}^T = \bar{S}^T\}$$

$$\bar{e}_s \quad \min_{\bar{e} \in E_s} w(\bar{e})$$

→ a legkisebb súlyú hibavektort választjuk, mert az a legvalószínűbb

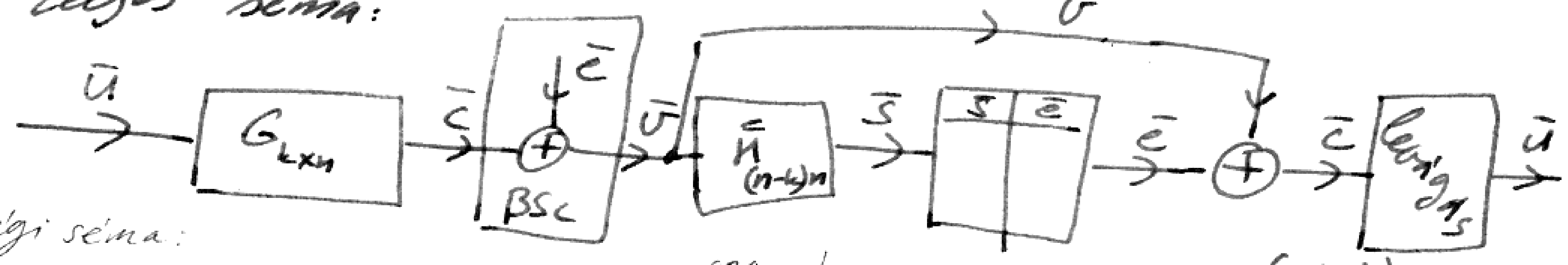
$$p(\bar{e}) = \left(\frac{p_b}{1-p_b}\right)^{w(\bar{e})} (1-p_b)^n$$

?? :

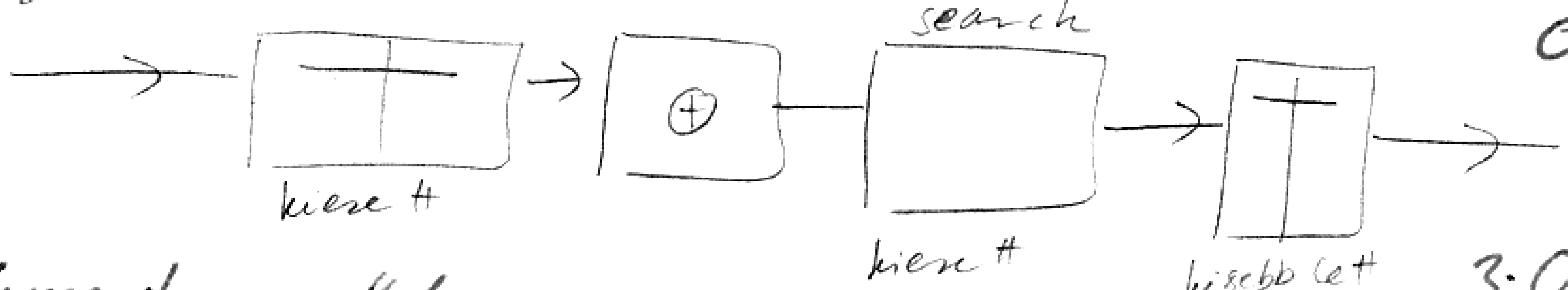
$\bar{s}$	$\bar{e}$

táblázat előregyártott

A teljes séma:



Régi séma:



$O(2^{n-k})$

$\wedge$

$3 \cdot O(3\, 2^k)$

Numerikus példa:

$$\bar{\bar{G}} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \quad \bar{v} = (11000) \quad \bar{\bar{H}}_{2\times5} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

(T)

$C(5,3)$

$(000) \to (00000) = c_0$
$(001) \to (00111) = c_1$
$(010) \to (01010) = c_2$
$(011) \to (01101) = c_3$
$(100) \to (10001) = c_4$
$(101) \to (10110) = c_5$
$(110) \to (11011) = c_6$
$(111) \to (11100) = c_7$

$\bar{C} > \bar{e} + \bar{v} = 11100$

A hibacsoport tulajdonsága

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

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

$$\bar{\bar{H}}\bar{v}^T = \begin{pmatrix} 1 \\ 1 \end{pmatrix} = \bar{s}^T$$

$$\bar{\bar{H}}\bar{e}^T = \begin{pmatrix} 1 \\ 0 \\ 1 \end{pmatrix}$$

pl. $\bar{e} = (00100)$

$E_s := \{\bar{e}, \bar{e}+c_1, e+c_2, \ldots\}$

épp az $\bar{e}$ a legkisebb súlyú

10-09-16 Kodtech

Lineáris kód, duális kód

Általános kódelmélet
- üzenet+vektor, k hosszú
- hibajavító kódolás — kódtáblázat
- n hosszú kódszó

} $n - k \leq E$ ne legyen túl nagy a redundancia

bináris szimmetrikus csatorna — ez egy jó modell
- bináris vektort generál → azt nem tudjuk megfigyelni

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

vett vektor $\underline{v}$ — itt már nem ismerjük a kódszót és a hibát

$\underline{c}'$ detektált kódszó

$\underline{u}'$ üzenet

Lineáris bináris kódok
- táblázat helyett mátrixszorzás
- generátormátrix ←
- paritás-ellenőrző mátrix ←
- szindrómavektor

$\bar{\bar{H}}\,\bar{\bar{G}}^T = \bar{\bar{O}} \Rightarrow \bar{\bar{H}}_{(n-k)\times k} = \left(\bar{\bar{A}}_{(n-k)\times k}, \bar{\bar{I}}_{n-k}\right)$

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

$\bar{\bar{A}} = \bar{\bar{B}}^T$ (szimmetrikus kód esetén)

$E_s = \{\bar{e} : \bar{\bar{H}}\bar{e}^T = \bar{s}^T\}$, $\bar{e}_s$: $\bar{e} \in E_s$ → minimális súlyú

hibacsoport.

Nyitott kérdés: a kód teljesítőképessége

d_{min} t (javítandó hibák száma) → $\bar{\bar{G}}$ vagy $\bar{\bar{H}}$ előállítandó

Lineáris, bináris Hamming-kód

Előtte: szabványos elrendezés, Standard array

kódszavak $\bar{c}^{(0)}$	$\bar{c}^{(1)}$	....	$\bar{c}^{(M=2^k)}$	súly	
$\bar{e}$	$\bar{e}+\bar{c}^{(1)}$	...	$\bar{e}+\bar{c}^{(M)}$	$\bar{s}$	$\bar{e}_s$
⋮					
$\bar{e}'$	$\bar{e}'+\bar{c}^{(1)}$	....	$\bar{e}'+\bar{c}^{(n)}$	$\bar{s}'$	$\bar{e}_{s'}$

→ ez egy hibacsoport

2^{n-k} db → 2^n db vektor összesen

„még ezekkel nem volt"

$M = 2^k$ db —

pl.: $\bar{\bar{G}}_{2\times 4} = \begin{pmatrix} 10 & 11 \\ 01 & 10 \end{pmatrix}$ $\bar{\bar{H}}_{2\times 4} = \begin{pmatrix} 1 1 & 1 0 \\ 1 0 & 0 1 \end{pmatrix}$

$\bar{c}^{(0)} = (0000)$	$\bar{c}^{(1)} = (0110)$	$\bar{c}^{(2)} = (1011)$	$\bar{c}^{(3)} = (1101)$	$\bar{S}$ (00)	min w( ) a sorban (0000)
$\bar{e} = (0001)$	$\bar{e}+\bar{c}^{(1)} = (0111)$	$\bar{e}+\bar{c}^{(2)} = (1010)$	$\bar{e}+\bar{c}^{(3)} = (1100)$	$\bar{\bar{H}}\cdot\bar{e}$ (01)	(0001)
$\bar{e}' = (0010)$	$\bar{e}'+\bar{c}^{(1)} = (0100)$	(1001)	(1111)	(10)	(0010) 2 van az előtt
$\bar{e}'' = (0011)$	(0101)	(1000)	(1110)	(11)	(1000)

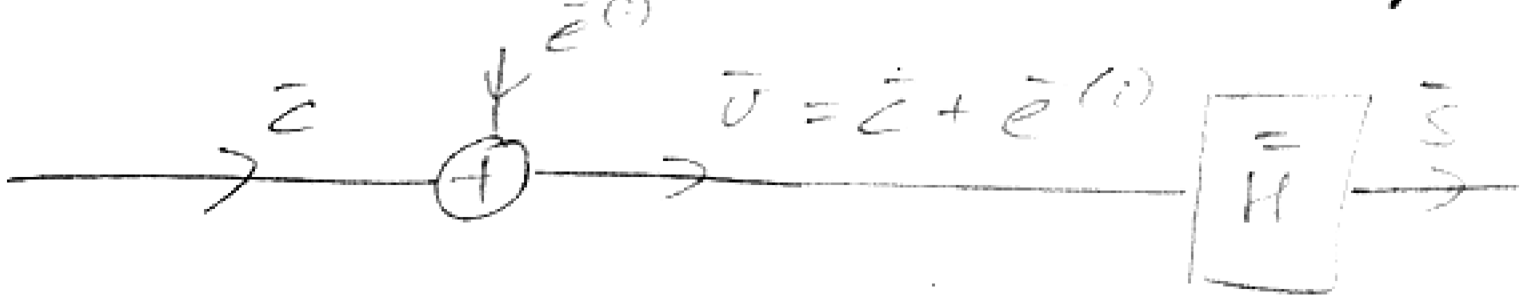
Hamming-kódok: ∀ 1 hiba javítása! $\bar{e} = (00\ldots 0\overset{i.}{1}0\ldots 0)$
i. bázisvektor

feladat: i indexet kitalálni

$$\bar{\bar{H}}_{(n-k)\times n} = \begin{pmatrix} \bar{a}^{(1)T} & \bar{a}^{(2)T} & \ldots & \bar{a}^{(i)T} & \ldots & \bar{a}^{(n)T} \end{pmatrix}$$

Technológiai motiváció:
vezetékes MODEM kommunikáció
ott nincs annyi hiba

$\dim(\bar{a}^{(i)}) = n-k \quad \forall i = 1,\ldots,n$



$\bar{\bar{H}}\cdot\bar{v}^T = \bar{S}^T$
adott — megfigyelhető — kiszámítható

$$\bar{\bar{H}}(\bar{c}+\bar{e}^{(i)})^T = \bar{\bar{H}}\bar{c}^T + \bar{\bar{H}}\bar{e}^{(i)T} = \bar{S}^T$$

$$\bar{\bar{H}}\,\bar{e}^{(i)T} = \bar{S}^T$$
adott — adott

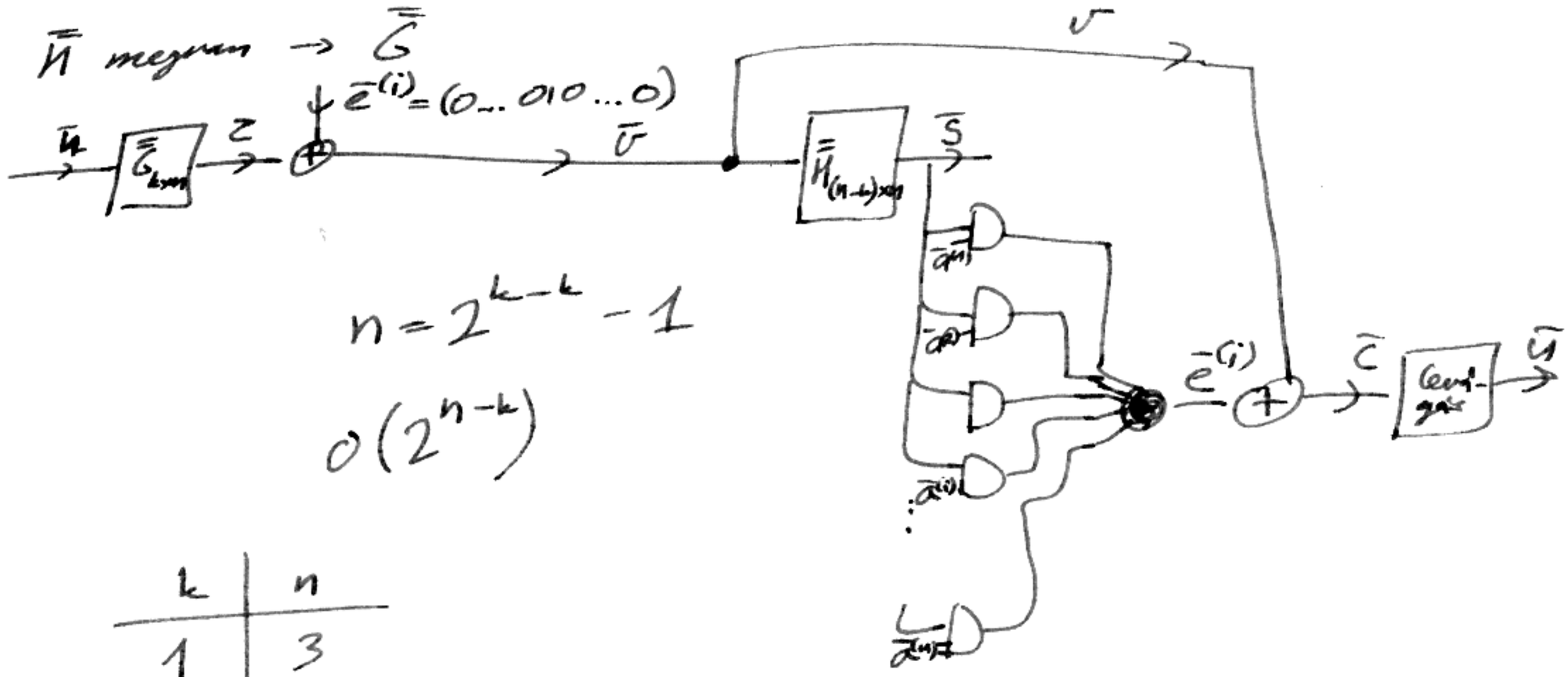
$\bar{S} \times \bar{a}^{(i)} \rightarrow i$

<u>Feltételek:</u>

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

10-09-16 Kodtech

$\bar{\bar{H}}$ megvan → $\bar{\bar{G}}$



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

$$O(2^{n-k})$$

k	n
1	3
4	7
11	15
⋮	⋮

Példa: $C_H(7,4) \xrightarrow{?} \bar{\bar{H}} \to \bar{\bar{G}} \to$ szindrómás dekódolási táblázat

$$\bar{\bar{H}}_{3\times7} = \left(\begin{array}{ccc|cccc} 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 \end{array}\right)$$

$$\bar{\bar{G}}_4 = \left(\begin{array}{cccc|ccc} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{array}\right)$$

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

Gyakorlati kódtervezés $P' \le 10^{-\gamma}$, P_b

$$P_{correct} = (1-P_b)^n + \binom{n}{1} P_b (1-P_b)^{n-1} = (1-P_b)^n + n P_b (1-P_b)^{n-1} \ge 1 - 10^{-\gamma}$$

Tervezés: adott: P_b, γ

keresett: n. 1., Létezik-e n, amellyel kielégíthető az egyenlet?

2., Ha igen; n, k: $2^{n-k} = n+1$

3., $\bar{H} \to \bar{\bar{G}} \to$ szindrómás dekódolási táblázat

---

$C_H(3,1)$

$t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor$ $\quad 3 \le d_{min} \le 3 \to d_{min} = 3$

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

d.e. egy MDS-kód.

Több hiba javítása

Ez kell szindrómás rendszerben.

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

Feltételek:

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

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

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

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

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

} Bináris oszlopvektorok nem elég gazdagok ennek kielégítésére

$\Downarrow$

DUÁLIS KÓD KELL

10-09-21 Kodtech

Több hiba javítására alkalmas kódok

- ez kell a vezeték nélküli kommunikációhoz, mert ott sok a hiba
- ekkor bináris szimbólum helyett → q-áris szimbólumok

  Ehhez 2 dolog kell:
  - cél: minél kisebb q
  - q zárt ⟶ véges testekkel kell foglalkoznunk

LEMMA: d_{min} lineáris kód

$\bar{\bar{H}}$-nak $d_{min}-1$ független oszlopvektora van

$d_{min} = w_{min}$

$$\bar{c} = (0 \ldots 0 c_1 0 \ldots 0 c_2 0 \ldots 0 c_{w_{min}} 0 \ldots 0)$$

$$\bar{\bar{H}}_{(n-k)\times n} \, \bar{c}^T = \bar{0}^T$$

$$\left(\bar{a}^{(i_1)T} \ldots \bar{a}^{(i_2)T} \ldots \bar{a}^{(i_{w_{min}})T} \right) \begin{pmatrix} 0 \\ \vdots \\ 0 \\ c_1 \\ 0 \\ \vdots \end{pmatrix} = \sum_{j=1}^{w_{min}} \bar{a}^{(i_j)T} = \bar{0}$$

ezek az oszlopvektorok választódnak ki

Véges testek

$GF(q) = \{a_0, a_1, \ldots, a_{q-1}\} = \{0, 1, \ldots, q-1\}$

Galois Field

⇒ "+", "*" műveletekre zárt

Axiómák: + : zárt, kommutatív, asszociatív, ∃0, ∃ inverz

· : zárt, ha nem 0-val szorzunk, nem 0-t kapunk, kommutatív, asszociatív, ∃1, ∃ inverz, kivéve 0

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

pl. mod p prím

pl $5x + 2 = 1 \pmod 7$

$5x = 2_a^{-1} + 1$

$5x = 5 + 1$

$5x = 6$

$x = 5_m^{-1} \cdot 6$

$x = 3 \cdot 6 = 4$

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

$\alpha\alpha_1 \cdot \alpha\alpha_2 \cdot \alpha\alpha_3 \cdot \ldots \alpha\alpha_{q-1} = \alpha_1\alpha_2 \ldots \alpha_{q-1}$

$\alpha^{q-1} \cdot \prod \alpha_i = \prod \alpha_i$

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

$\min m : \alpha^m = 1 \rightarrow rend(\alpha) = m$

$m/m' : \alpha^{m'} = 1 \rightarrow m/q-1$

$m' = u \cdot m + r$

$1 = \alpha^{m'} = \alpha^{u \cdot m + r} = \underbrace{(\alpha^m)^u}_{1} \cdot \underbrace{\alpha^r}_{1} = 1$ $\quad r = 0$ $\Rightarrow$ mert m a legkisebb

Hatványtábla $GF(7)$

elem	1	2	3	4	5	6	hatvány	rend
1	1							1
2	2	4	1					3
3	3	2	6	4	5	1		6 → primitív elem, hatványai kifejezik a testet
4	4	2	1					3
5	5	4	6	2	3	1		6
6	6	1						2

q-ális Hamming-kód
(1 hiba javítására alkalmas)

$\bar{e} = (00 \ldots 0 \alpha 0 \ldots 0) \rightarrow\!\!\rightarrow i;\ \alpha$

pl. $\bar{v} = (1\ 2 \ldots 3\ 4 \ldots 6) \rightarrow \bar{c} = (1\ 2 \ldots 6\ 4 \ldots 6)$

i $\quad \alpha = 4$

$\bar{e}^{(i)}$

$\bar{v} = \bar{c} + \bar{e}^{(i)}$ Kuleseggenlő sch

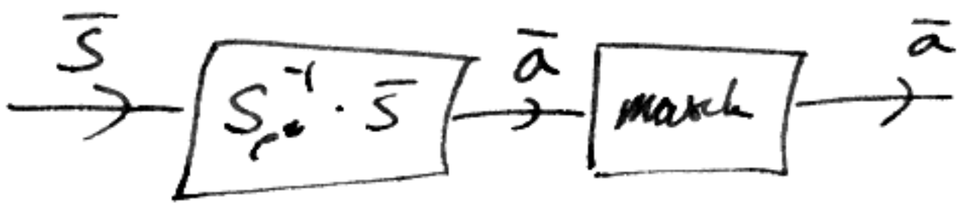
$\bar{\bar{H}}(\bar{c} + \bar{e}^{(i)})^T = \cancel{\bar{\bar{H}}\bar{c}^T}^{0} + \bar{\bar{H}}\,e^{(i)T} = \bar{S}^T$

$\bar{\bar{H}}_{(n-k) \times n}$ $\rightarrow \bar{S}$

10-09-21 Kódtech

$$\left(\bar{a}^{(0)T} \quad \bar{a}^{(1)T} \quad \bar{a}^{(q)T}\right)\begin{pmatrix}0\\0\\\vdots\\0\\\alpha\\0\\\vdots\\0\end{pmatrix}\leftarrow i \;=\; \alpha\cdot\bar{a}^{(i)T} = \bar{s}^{T}$$

α : az első nemnulla komponens



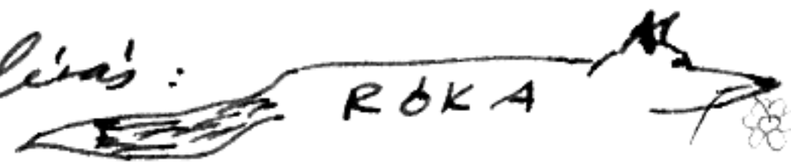
működik, ha $\bar{a}^{(i)} \neq \bar{0} \quad \forall i = 1,\dots,n$

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

$\bar{a}^{(i)}$ első nullától különböző komponense 1-es

$$\frac{q^{n-k}-1}{q-1} = n$$

Racionális felírás:



$q^{n-k} = n(q-1)+1$ ↳ ↳

$q^{n-k} = \sum_{i=0}^{n-1}\binom{n}{i}(q-1)^i \Rightarrow$ ez perfekt kód

$C_H(8,6)$; $GF(7)$; $\bar{\bar{H}}_{2\times 8} = \left(\begin{array}{cccccc|cc} 1&1&1&1&1&1&1&0\\ 1&2&3&4&5&6&0&1\end{array}\right)$

$\bar{\bar{B}}$

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

$\bar{\bar{G}}_{6\times 8} = \left(\begin{array}{cccccc|cc} 1&0&0&0&0&0&6&6\\ 0&1&0&0&0&0&6&5\\ 0&0&1&0&0&0&6&4\\ 0&0&0&1&0&0&6&3\\ 0&0&0&0&1&0&6&2\\ 0&0&0&0&0&1&6&1\end{array}\right)$

↑ bináris kódnál nem kellene −

$C_H(n, n-2)$

EZEK MDS-kódok

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

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

d_{min} egyenes MDS-kódok: 1 kivételével

10-09-23 Kodtech

Többszörös hibák javítása
(vezeték nélküli technológiákhoz kell)

polinomok a G-F(q) felett

$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m,$

$a_0, a_1, \ldots, a_n \in GF(q)$

$\Uparrow$

véges, gyorsan lehet kiszámítható kereséssel gyököt lelni

$deg(a(x)) = m$

↑ fokszám

$b(x) = b_0 + b_1 x + b_2 x^2 + \ldots + b_n x^n;$ $\quad deg(b(x)) = n$

$c(x) = a(x) + b(x) \Rightarrow c_i = a_i \oplus b_i \rightarrow deg(c(x)) = max\{deg(a(x)), deg(b(x))\}$

↑ modulo összeadás

$d(x) = a(x)\,b(x) = a_0 b_0 + (a_0 b_1 + a_1 b_0)x + \ldots$

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

$deg(d(x)) = deg(a(x)) + deg(b(x))$

polinom	vektor
$a(x)+b(x)$	$\bar{a}+\bar{b}$
$a(x)b(x)$	$\bar{a} * \bar{b}$

↑ konvolúció

$a(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_m x^m$

$\downarrow \uparrow \chi$

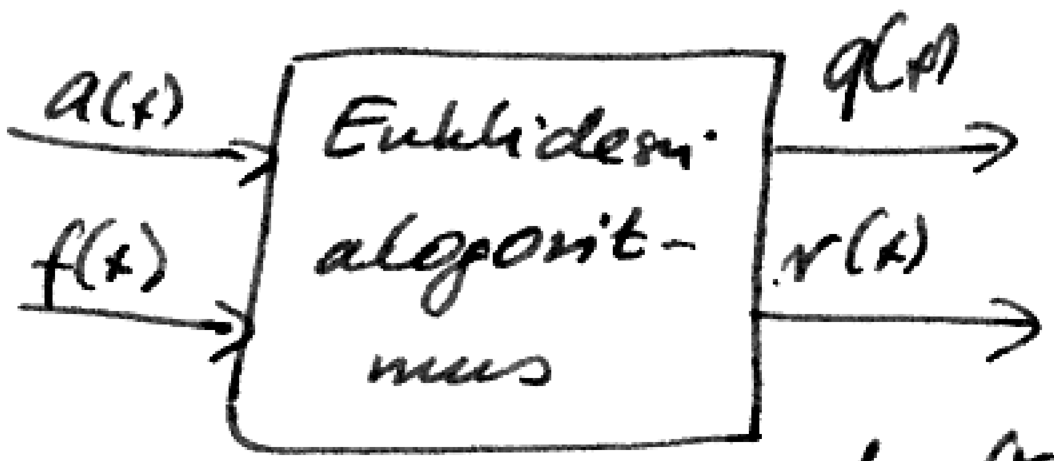
$\bar{a} = (a_0, a_1, \ldots, a_m)$

Osztás:

$a(x) \quad deg(a(x)) = m$

$\quad\quad\quad\quad\quad\quad\quad\quad \vee$

$f(x) \quad deg(f(x)) = k$



$deg(r(x)) < deg(d(x))$

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

$a(x)\Big|_{x=x_i} = \emptyset$ $\quad a(x) = b(x)(x - x_i) \rightarrow$ a gyöktényező kiemelhető;

↓

x_i gyöke $a(x)$-nek

$a(x)\Big|_{x=x_i} = \underbrace{b(x)(x-x_i)\Big|_{x=x_i}}_{\emptyset} + r = \emptyset$

$r \rightarrow 0$

↳ mert az osztási maradéknak 0-nak kell lennie

→ a gyöktényezők kiemelésével csökken a fokszám, nem lehet több gyök mint fok.

Reed - Solomon (RS) kódok → képes több hiba javítására

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

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

$\alpha_0, \alpha_1, \dots \alpha_{n-1} \in GF(q) \setminus \{0\}$

$c_i = u(x)\Big|_{x=\alpha_i}, \; i = 0, \dots, n-1$

pl. $c_0 = u_0 + u_1 \alpha_0 + u_2 \alpha_0^2 + \dots + u_{k-1} \alpha_0^{k-1}$

$c_1 = u_0 + u_1 \alpha_1 + u_2 \alpha_1^2 + \dots + u_{k-1} \alpha_1^{k-1}$

$c_2 = u_0 + u_1 \alpha_2 + u_2 \alpha_2^2 + \dots + u_{k-1} \alpha_2^{k-1}$

$\vdots$

$c_{n-1} = u_0 + u_1 \alpha_{n-1} + u_2 \alpha_{n-1}^2 + \dots + u_{k-1} \alpha_{n-1}^{k-1}$

$\bar{c} = \bar{u} \bar{\bar{G}}$,

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

$\Downarrow$

ez is egy lineáris kód, ezért

Az RS-kódok MDS-kódok (azaz optimális kódok)

- DSP-n implementálható
- $d_{min} = w_{min}$

$d_{min} = w_{min}$ (mert lineáris kód)

$\Downarrow$

n - nem-zérus elemek $\geq n - (k-1)$

($c_i = u(x)\Big|_{x=\alpha_i}$ $i = 0, \dots n-k$ ← ez a gyökök maximális számából jön ki: $\deg(n(x)) = k-1$)

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

Szabványos generálás:

$\alpha \in GF(q)$ primitív; $\alpha_0 = \alpha^0 = 1$

$\alpha_1 = \alpha^1 = \alpha$

$\alpha_2 = \alpha^2$

$\alpha_3 = \alpha^3$

$\vdots$

$\alpha_{n-1} = \alpha^{n-1}$

$n - 1 = q - 2 \rightarrow \boxed{n = q - 1}$

10-09-23 Kodtech

Paritásellenőrző mátrix

$$C(x)\Big|_{x=\alpha^i_6} = c_0 + c_1 x + c_2 x^2 + \dots + c_{n-1} x^{n-1}\Big|_{x=\alpha^i} = \emptyset \qquad i = 1, \dots, n-k$$

Pl.

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

$$\bar{\bar{H}}_{(n-k)\times n} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & & \alpha^{2(n-1)} \\ \vdots & \vdots & & & \vdots \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & & \alpha^{(n-k)(n-1)} \end{pmatrix} \rightarrow \text{"}\ell+1\text{". oszlopvektor}$$

Másik biz., hogy ez MDS-kód:

$$\bar{\bar{H}}_{(n-k)\times(n-k)} = \begin{pmatrix} \alpha^{i_1} & \alpha^{i_2} & \dots & \alpha^{i(n-k)} \\ \alpha^{2i_1} & \alpha^{2\cdot i_2} & & \alpha^{2i(n-k)} \\ \alpha^{3i_1} & \alpha^{3\cdot i_2} & & \alpha^{3i(n-k)} \\ \vdots & \vdots & & \vdots \\ \alpha^{(n-k)i_1} & \alpha^{(n-k)i_2} & & \alpha^{(n-k)i(n-k)} \end{pmatrix} \rightarrow \begin{pmatrix} \alpha^{\ell} \\ \alpha^{2\ell} \\ \alpha^{3\ell} \\ \vdots \\ \alpha^{\ell(n-k)} \end{pmatrix}$$

$i_1, i_2, \dots, i_{n-k}$ oszlopok

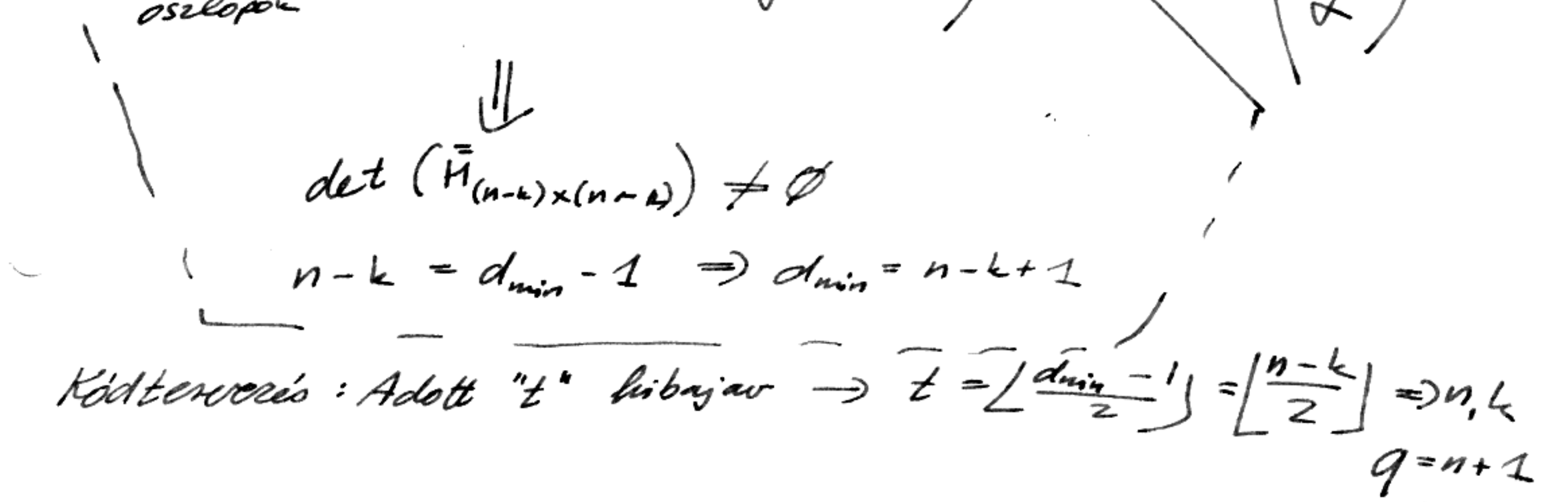
$$\Downarrow$$

$$\det\left(\bar{\bar{H}}_{(n-k)\times(n-k)}\right) \neq \emptyset$$

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

Kódtervezés: Adott "t" hibajavító $\rightarrow$ $t = \left\lfloor \frac{d_{min}-1}{2} \right\rfloor = \left\lfloor \frac{n-k}{2} \right\rfloor \Rightarrow n, k$

$q = n+1$



Pl. (lehet olyan a zh-n)

$\forall$ 2 hiba javítására alkalmas RS kód

$\perp$

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

$q=1 \quad n=\emptyset$
$q=2 \quad n=1$
$q=3 \quad n=2$
$q=5 \quad n=4$
} értelmetlenek

[$q=7 \quad n=6 \quad k=2$] a legkisebb q-t vizsgáljuk, amire már értelmes

$q=11 \quad n=10 \quad k=6$
$q=13 \quad n=12 \quad k=8$
$\vdots$

$q=(7) \rightarrow GF(7) \quad C(6,2)$; a 3 primitív elem

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

Adott "t" számú hiba javítására $\exists$ MDS kód $\rightarrow$ RS kód

$\perp$

implementálható

Ez jó. Baj: táblázat megjegyzendő és nagy, mert már nem bináris elemekből vannak benne. A táblázat mérete: $O(q^{n-k})$

Másik baj: minél több hibát javítunk, annál nagyobb a q. Nagyobb q $\rightarrow$ nagyobb hibavalószínűség.

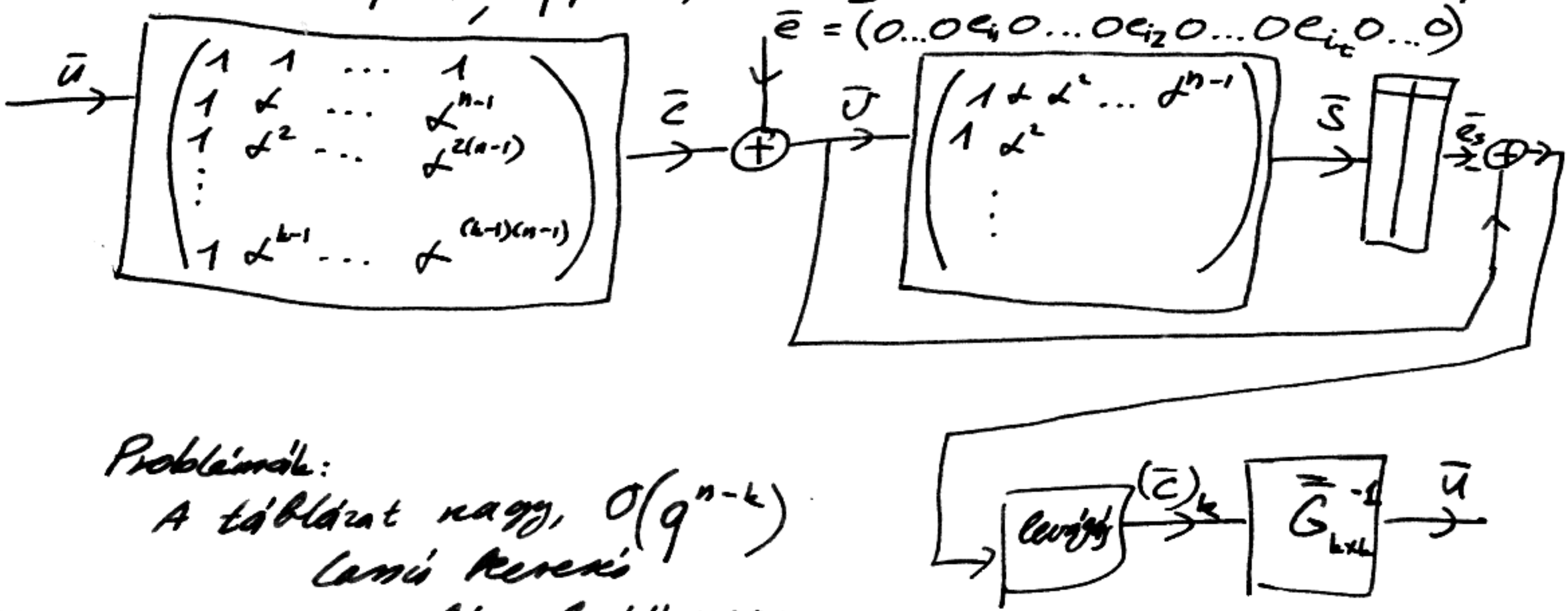
Cél: $GF(2^k)$

10-03-28 Kodtech

- Reed-Solomon kódok

Adott "t" → n, k

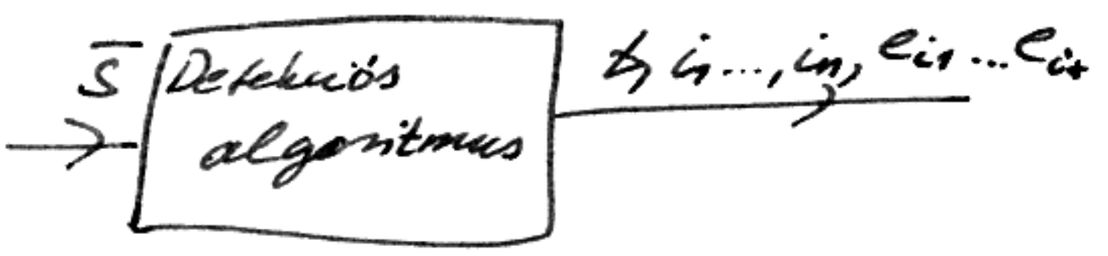
$n = q-1$, q prím, $\left\lfloor \frac{n-k}{2} \right\rfloor = t \Rightarrow n, k, q \Rightarrow \alpha \in GF(q)$



Problémák:
A táblázat nagy, $O(q^{n-k})$
Lassú keresés
nem fér el, túl nagy

- Hogyan lehet polinomiális komplexitású (real-time) detektálási algoritmust gyártani?
- Hogyan lehet a bináris esetre visszatérni?

Peterson-Gerenstein-Zierler detekciós algoritmus
(real-time detekció)



$\bar{e} = (0 \dots 0 e_{i_1} 0 \dots 0 e_{i_2} 0 \dots 0 e_{i_t} 0 \dots 0)$

$t, i_1 \dots i_t, e_{i_1}, \dots, e_{i_t}$

hibák száma — hibahelyek — hibaértékek

implementálás

megismerés

1, Feltesszük, hogy $t, i_1 \dots i_n$ ismert,
keresük $e_{i_1} \dots e_{i_t}$
2, Feltesszük, hogy t ismert,
keresük $i_1 \dots i_n$
3, Feltesszük, hogy semmi nem ismert,
$t = ?$

Jelölés:

$$(\bar{\bar{H}} \bar{e}^T)_e = (\bar{s} S^T)_e$$

$$\sum_{i=0}^{n-1} \alpha^{ij} e_i = S_j \quad \sum_{j=1}^{t} \alpha^{i_j l} e_{i_j} = S_l$$

új jel: $X_j = \alpha^{i_j}, \; j = 1 \dots t$ $\xrightarrow{\text{új forma}}$ $\sum_{j=1}^{t} X_j^l Y_j = S_l$

$Y_j = e_{i_j}, \; j = 1 \dots t$

1, Feltesszük: $t, i_1 \dots i_t$ ismertek $\xrightarrow{??}$ $e_{i_1} \dots e_{i_t}$

$$\sum_{j=1}^{t} X_j^{\ell} \gamma_j = S_\ell, \quad \ell = 1, \dots, t \Rightarrow \begin{pmatrix} X_1 & X_2 & \dots & X_t \\ X_1^2 & X_2^2 & \dots & X_t^2 \\ \vdots & & & \\ X_1^t & X_2^t & \dots & X_t^t \end{pmatrix} \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_t \end{pmatrix} = \begin{pmatrix} S_1 \\ S_2 \\ \vdots \\ S_t \end{pmatrix}$$

$\bar{\bar{V}}_{t\times t}\, \bar{\gamma}_t = \bar{S}_t \rightarrow$ polinomiális

ismert ismert

2, Feltesszük "t" ismert

$i_1 \dots i_t = ?$

$$L(x) = \prod_{j=1}^{t} (1 - x X_j) \rightarrow L\left(X_j^{-1}\right) = 0 \quad \forall j = 1, \dots, t$$

$$L(x) = 1 + L_1 x + L_2 x^2 + \dots + L_t x^t \xrightarrow{?} L_1, L_2, \dots, L_t \longrightarrow \sum_{j=1}^{t} X_j^{\ell+t} \gamma_j L(X_j^{-1}) = 0$$

$\ell = 1, \dots, t$

$$\sum_{j=1}^{t} X_j^{-\ell+t} \gamma_j \left(1 + L_1 X_j^{-1} + L_2 X_j^{-2} + \dots + L_t X_j^{-t}\right) = 0$$

$$\underbrace{\sum_{j=1}^{t} X_j^{\ell+t} \gamma_j}_{S_{\ell+t}} + L_1 \underbrace{\sum_{j=1}^{t} X_j^{\ell+t-1} \gamma_j}_{S_{\ell+t-1}} + L_2 \underbrace{\sum_{j=1}^{t} X_j^{\ell+t-2} \gamma_j}_{S_{\ell+t-2}} + \dots + L_t \underbrace{\sum_{j=1}^{t} X_j^{\ell} \gamma_j}_{S_\ell} = 0$$

$$L_1 S_{\ell+t-1} + L_2 S_{\ell+t-2} + \dots + L_t S_\ell = -S_{\ell+t} \qquad \ell = 1, \dots, t$$

$$\begin{pmatrix} S_1 & S_2 & \dots & S_t \\ S_2 & S_3 & \dots & S_{t+1} \\ \vdots & & & \\ S_t & S_{t+1} & & S_{2t-1} \end{pmatrix} \begin{pmatrix} L_t \\ L_{t-1} \\ \vdots \\ L_1 \end{pmatrix} = \begin{pmatrix} -S_{t+1} \\ -S_{t+2} \\ \vdots \\ -S_{2t} \end{pmatrix}^{\vee} \quad \bar{\bar{U}}_{t\times t}\, \bar{L}_t = \bar{S}_t^{\vee} \Rightarrow L(A) = 1 + L_1 x + \dots + L_t x^t \Rightarrow$$

$\Rightarrow L(X_j^{-1}) = \emptyset^{\vee}$ $\quad X_j = \alpha^{ij\vee} \Rightarrow i_1 \dots i_t \rightarrow$ minden polinomiális, real-time

3, $t = ?$

Tetszőleges mátrix felbontható így: $\bar{\bar{U}}_{t\times t} = \bar{\bar{V}}^{T}_{t\times t}\, \bar{\bar{B}}^{\dagger}_{t\times t}\, \bar{\bar{V}}_{t\times t}$

$$\bar{\bar{V}} = \begin{pmatrix} 1 & 1 & \dots & 1 \\ x_1 & x_2 & \dots & x_t \\ \vdots & & & \\ x_1^{t-1} & x_2^{t-1} & \dots & x_t^{t-1} \end{pmatrix} \qquad \bar{\bar{B}} = \begin{pmatrix} x_1 y_1 & 0 & \dots & 0 \\ 0 & x_2 y_2 & & 0 \\ \vdots & & & \\ 0 & 0 & \dots & x_t y_t \end{pmatrix}$$

$$\det(U) = \det^2(V) \cdot \det(B)$$

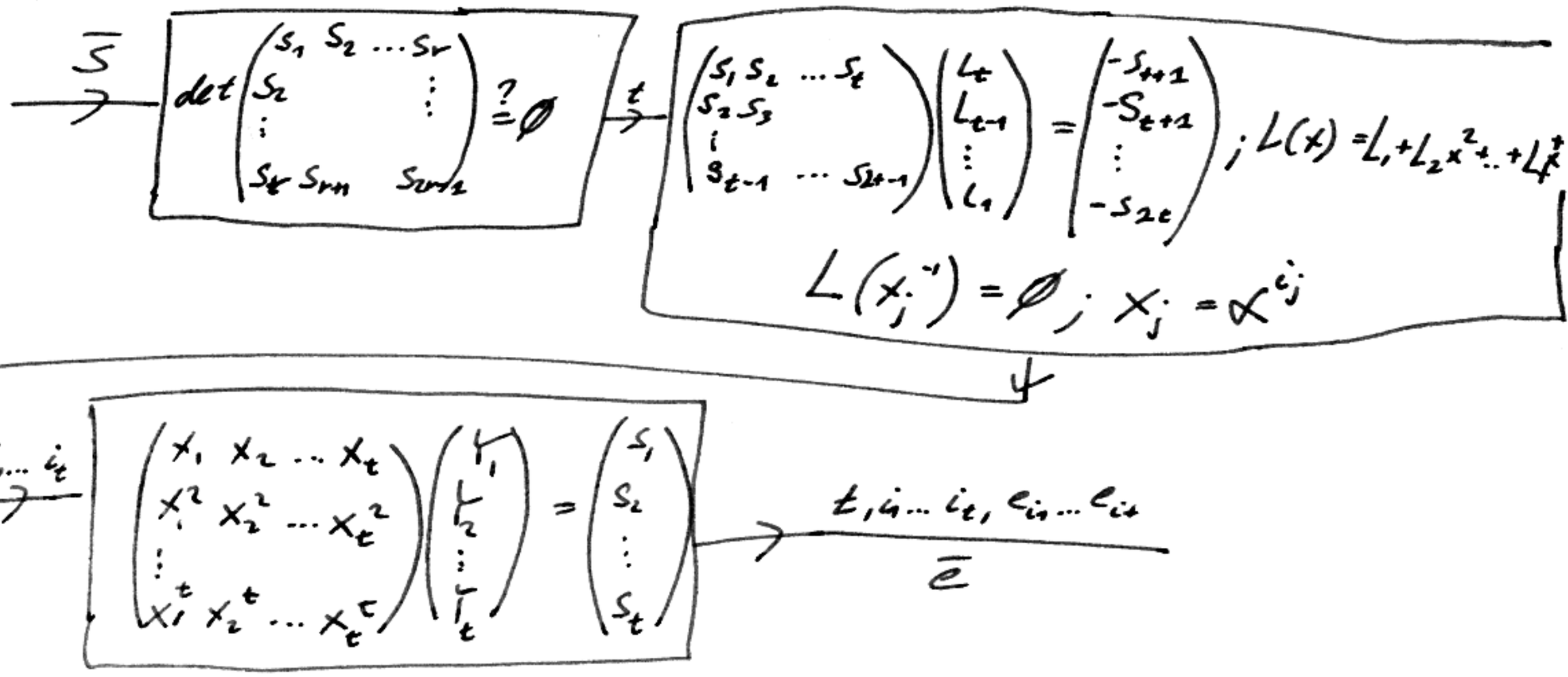
$$\bar{\bar{U}}_{r\times r} = \begin{pmatrix} S_1 & S_2 & \dots & S_r \\ S_2 & S_3 & \dots & S_{r+1} \\ \vdots & & & \\ S_r & S_{r+1} & \dots & S_{2r-1} \end{pmatrix} \quad r > t \qquad \det(\bar{\bar{U}}_{r\times r}) = 0$$

t keresése:

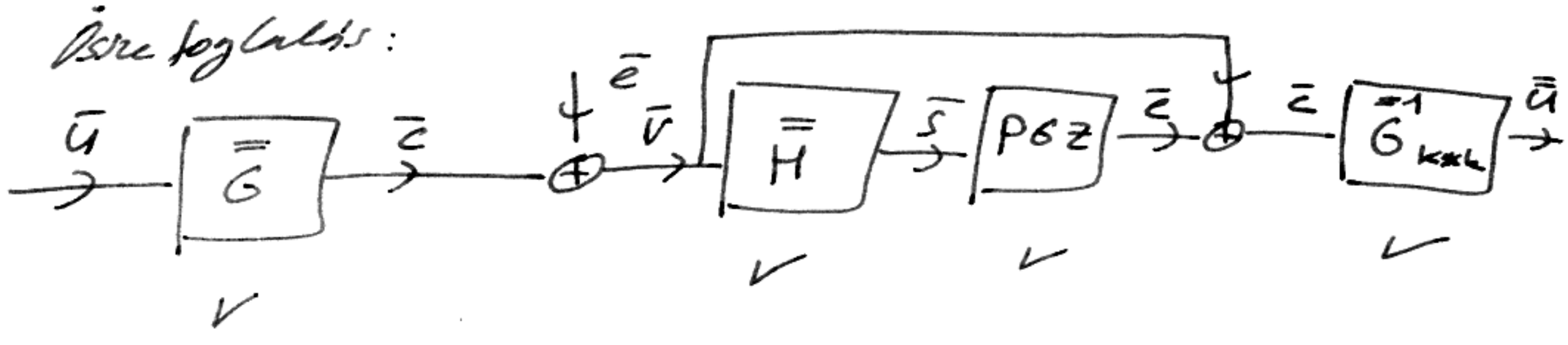
$r = \left\lfloor \frac{n-k}{2} \right\rfloor$; $\det(\bar{\bar{U}}_{r\times r}) \stackrel{?}{=} 0$, $r = r - 1$ $\Longrightarrow$ $\boxed{r = t}$

10-09-28 Kodtech

Implementálás:



Összefoglalás:



MIND POLINOMIÁLIS

- MDS kód (RS optimálisak)
- Akárhány hibát javít
- Real-Time

Numerikus példa PGZ algoritmusra

$GF(11)$; $\bar{s} = (3, 1, 5, 6, 10, 8) \xrightarrow{?} \bar{e}: t, i_1 \dots i_t, e_{i_1} \dots e_{i_t}$

$\alpha = 6 \in GF(11)$

- hány hibát tud javítani?

$\dim(\bar{s}) = n - k$; $n = q - 1$, $n = 10$, $k = 4 \rightarrow t = \left\lfloor \frac{n-k}{2} \right\rfloor = 3 \equiv$ elvileg 3 javítható

1, $r = 3$, $\det\begin{pmatrix} 3 & 1 & 5 \\ 1 & 5 & 6 \\ 5 & 6 & 10 \end{pmatrix} = 3 \cdot 3 + 1 \cdot 9 + 5 \cdot (-8) = 7 - 7 = \emptyset \Rightarrow$ 3-nál kevesebb hiba

$r = 2$

$\det\begin{pmatrix} 3 & 1 \\ 1 & 5 \end{pmatrix} = 3 \neq \emptyset \Rightarrow t = 2 \Rightarrow$ ill most 2 hiba van $\equiv$ ill csak 2 van

$\begin{pmatrix} 3 & 1 \\ 1 & 5 \end{pmatrix} \begin{pmatrix} l_1 \\ l_2 \end{pmatrix} = \begin{pmatrix} 6 \\ 5 \end{pmatrix} \Rightarrow \begin{matrix} 3l_2 + l_1 = 6 \\ l_2 + 5l_1 = 5 \end{matrix} \Rightarrow \begin{matrix} 3l_2 + 4 = 6 \\ 3l_2 + 9l_4 = 4 \end{matrix} \rightarrow \begin{matrix} 3l_2 = 9 \\ l_4 = 3 \end{matrix} \Rightarrow l_2 = 1 \Rightarrow$ gyökkeresés, a gyökök:

$x_1^{-1} = 2 \Rightarrow x_1 = 6$

$x_2^{-1} = 6 \Rightarrow x_2 = 2$

	1	2	3	4	5	6	7	8	9
6	6	3	7	9	10	5	8	3	2

→ kontrollsor

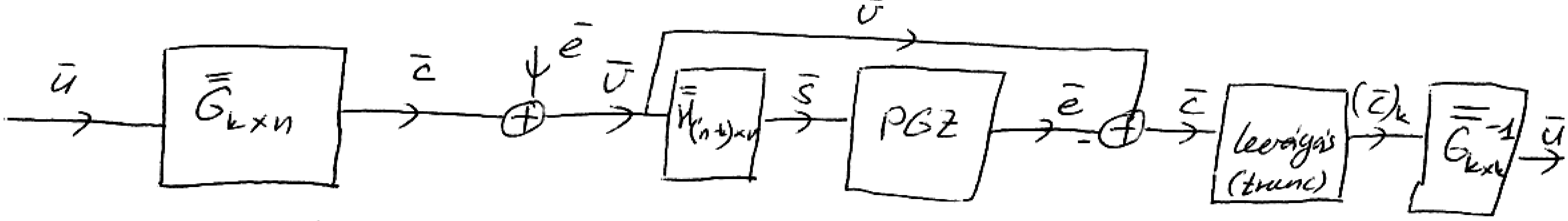
$i_1 = 1$

$i_2 = 9$

$$\begin{pmatrix} 6 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3 \\ 1 \end{pmatrix} \Rightarrow \left.\begin{aligned} 6y_1 + 2y_2 &= 3 \\ 3y_1 + 4y_2 &= 1 \end{aligned}\right\} \begin{aligned} y_1 &= 3 \\ y_2 &= 9 \end{aligned}$$

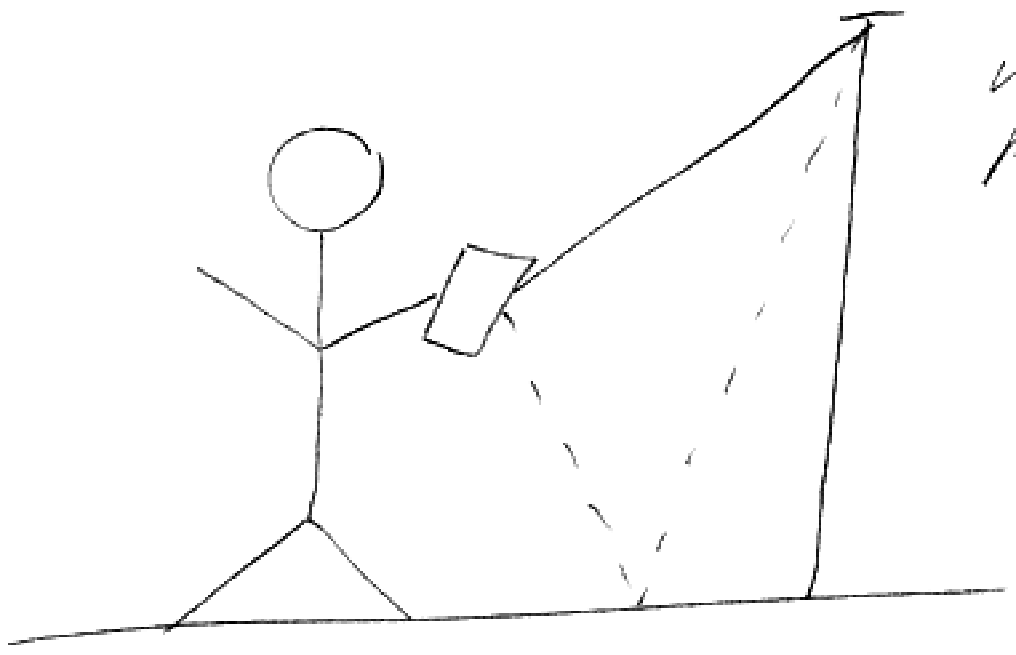
$\bar{e} = (0300000009)$

10-09-30 Kódtech



- optimális kód
- tetszőleges számú hiba javítása
- Real-Time

Probléma: q-áris esetben romlik a csatorna minősége



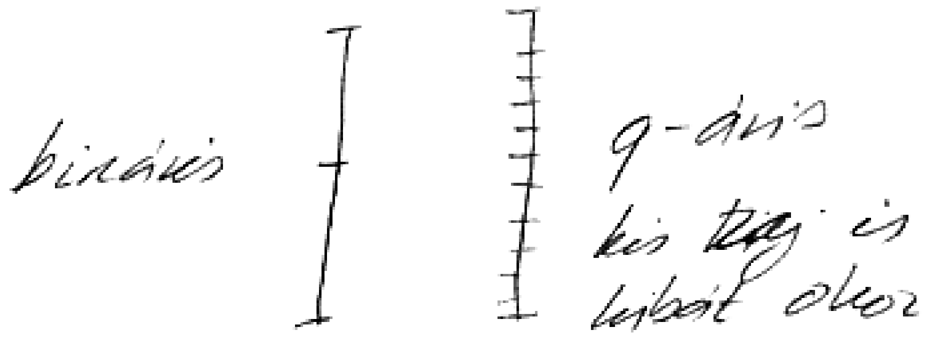
Multipath propagation ⇒ Selective fading ⇒ nagy csatorna-torzítás

⇓

sok hibát kell javítani (t nagy) ⇒ n is nagy ⇒ q is nagy

⇓

sok szimbólumra kell osztani a frekvenciát:



⇒ még több hiba

VISSZA A BINÁRIS TARTOMÁNYBA!

1. lehetőség: ~~q~~ kódoljunk binárisan:

GF(11)

$0 \to 0000$
$1 \to 0001$
$2 \to 0010$
$\vdots \quad \vdots$
$10 \to 1010$

$\frac{11}{16}$ veszteség

↓

akkor tűnik el, ha 2 hatvány alapú testet tudunk használni

↓

KIHÍVÁS: spektrális kihasználtság

↓

algebrai kihívás:

GF-prímhatvány fölött

$GF(p^m)$

p prím, (gyakorlatilag $p=2$)

Algebra a $GF(p^m)$ felett (p prím)

elemek	p-áris vektor	polinom
0	$(00\ldots0)$	$0\cdot y^{m-1}+0y^{m-2}+\ldots+0y^0=\emptyset$
1	$(00\ldots1)$	$0\cdot y^{m-1}+0y^{m-2}+\ldots+1\cdot y^0=1$
$\vdots$	$\vdots$	$\vdots$
α	$(a_{m-1}, a_{m-2}, \ldots a_0)$	$a_{m-1}y^{m-1}+a_{m-2}y^{m-2}+\ldots+a_0y^0=a(y)$
β	$(b_{m-1}, b_{m-2}, \ldots b_0)$	$b_{m-1}y^{m-1}+b_{m-2}y^{m-2}+\ldots+b_0y^0=b(y)$
γ	$(c_{m-1}, c_{m-2}, \ldots c_0)$	$c_{m-1}y^{m-1}+c_{m-2}y^{m-2}+\ldots+c_0y^0=c(y)$
$\vdots$	$\vdots$	
p^m-1		

$\forall a_i \in GF(p)$

Irreducibilis polinom: nem bontható alacsonyabb fokú polinomokra:

$$p(y) \neq p_1(y)p_2(y);\ \deg(p_i(y)) < \deg(P(y))\ i=1,2$$

$$P(y) = 1+y+y^2$$
$$1+y+y^3$$
$$1+y+y^4$$
$$1+y^2+y^5$$

mod $p(y)$ polinommüveletek:

szorzás: $a(y)b(y) = c(y) \mod p(y)$

azaz: $a(y)\,b(y) = u(y)p(y) + c(y) \rightarrow \deg(c(y)) < \deg(p(y))$

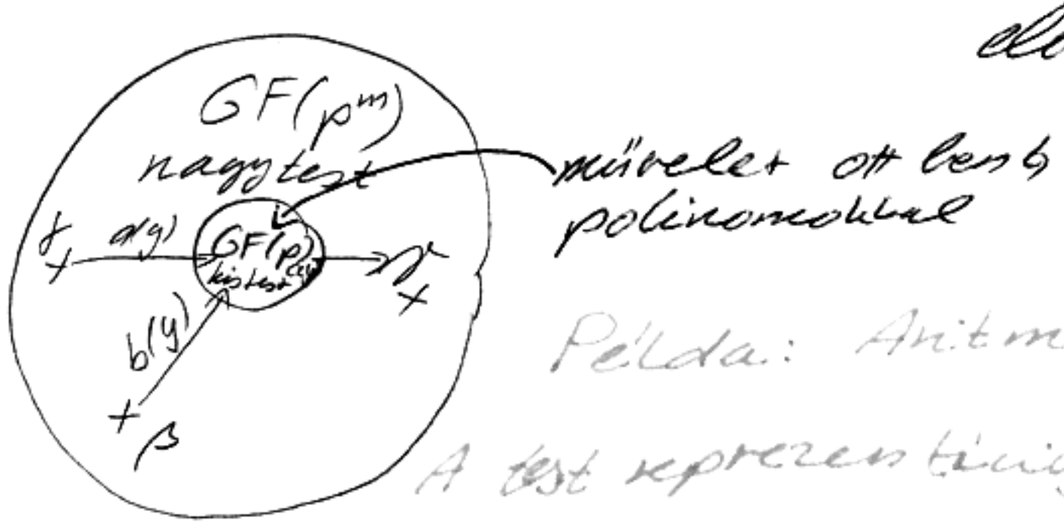
összeadás: $a(y)+b(y) = c'(y) \mod p(y)$

azaz: $a(y)+b(y) = u'(y)\,p(y) + c'(y)$

polinomok közti müveletek $\rightarrow$ polinomok együtthatói közti müveletek

$\Downarrow$

elvégezhető a $GF(p)$ testben.



Példa: Aritmetika a $GF(4)$-ben

$GF(2^2)$

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

↑ az irreducibilis polinom

A test reprezentációja:

ELEMEK	bináris	polinom
0	00	$0\cdot y^1+0\cdot y^0=0$
1	01	$0\cdot y^1+1\cdot y^0=1$
2	10	$1\cdot y^1+0\cdot y^0=y$
3	11	$1\cdot y^1+1\cdot y^0=y+1$

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

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

$1+2 = 1+y = 3$

$1+3 = \underbrace{1+1}_{0}+y = y = 2$

$2+2 = y+y = 0y = 0$

$2+3 = y+1+y = 1$

$3+3 = y+1+y+1 = 0$

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

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

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

($p(y)$)

10-09-30 Kodtech

Példa: Hatványtábla $GF(8)$ fölött

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

$p(y) = y^3 + y + 1$ ↑ az irreducibilis polinom

ELEMEK	bináris	polinom
0	000	0
1	001	1
2	010	y
3	011	y+1
4	100	y^2
5	101	y^2+1
6	110	y^2+y
7	111	y^2+y+1

HATVÁNYOK

y^0	1
y^1	y
y^2	y^2
y^3	$y+1 \leftarrow y^3 = (y^3+y+1)+y+1$
y^4	$y^2+y \leftarrow y^4 = y(y^3+y+1)+y^2+y$
y^5	$y^2+y+1 \leftarrow y^5 = (y^2+1)(y^3+y+1)+y^2+y+1$
y^6	$y^2+1 \leftarrow y^6 = (y^3+y+1)(y^3+y+1)+y^2+1$
(y^7)	(1)

2^0	1
2^1	2
2^2	4
2^3	3
2^4	6
2^5	7
2^6	5
(2^7)	(1)

Hatványtábla alkalmazása:

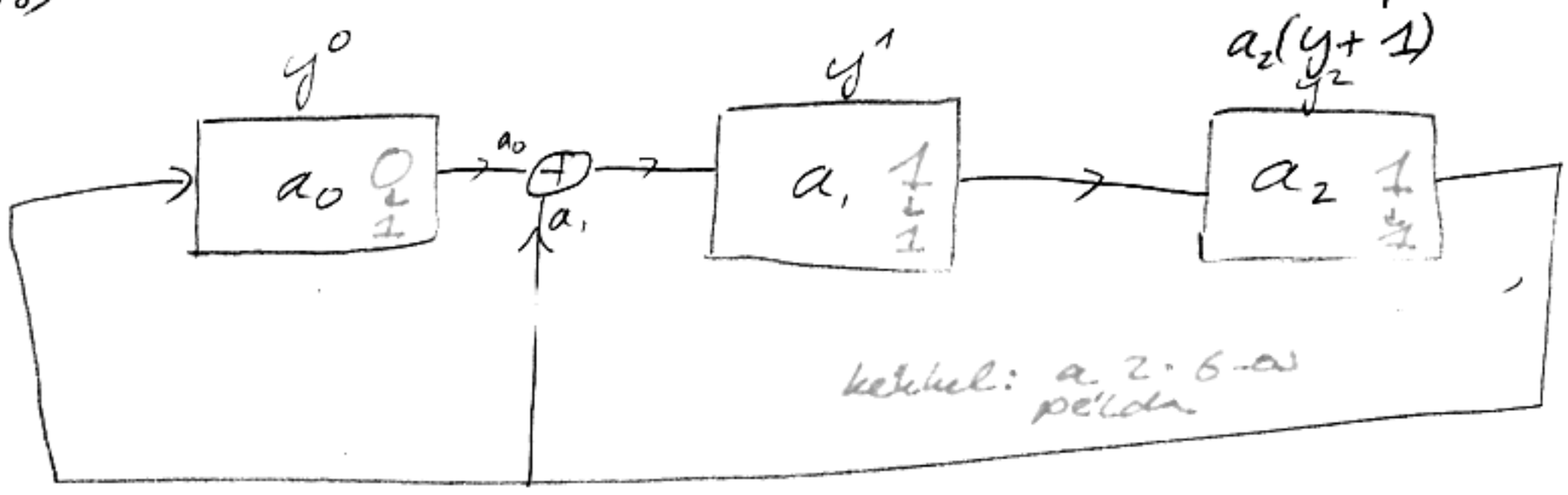
$2 \cdot 6 = ? = y \cdot y^4 = y^5 = y^2+y+1 = 7$

Megvalósítás:

Shiftregiszterekkel

Pl. $y \cdot \alpha = y \cdot (a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 = a_2 + (a_0+a_2) y + a_1 y^2$ ($GF(8)$)

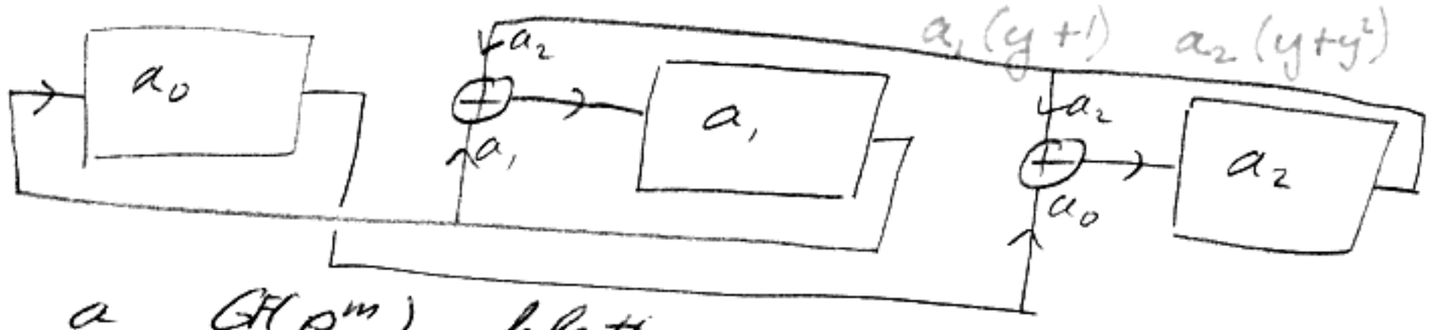
↑ $a_2(y+1)$



Ez egy shiftregiszter, y-nal szorzó.

pl. $y^2 \cdot \alpha = y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 y^3 + a_2 y^4 = a_1 + (a_1+a_2) y + (a_0+a_2) y^2$

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



Polinomok a $GF(p^m)$ felett

$\alpha(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \ldots + \alpha_n x^n$ $\quad \alpha_0, \alpha_1, \ldots, \alpha_n, x \in GF(p^m)$

$\alpha(x) = a_0(y) + a_1(y) x + a_2(y) x^2 + \ldots + a_n(y) x^n$

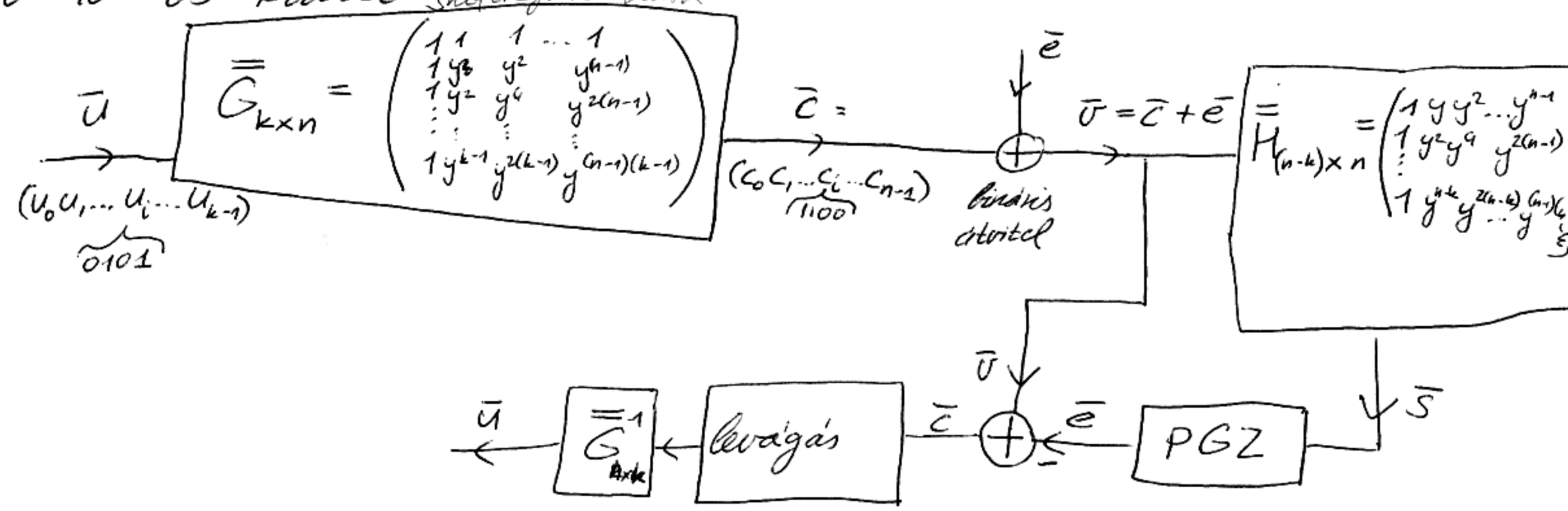
$\alpha(x) = y^{i_0} + y^{i_1} x + y^{i_2} x^2 + \ldots + y^{i_n} x^n$ → standard reprezentáció

pl. $GF(8)$

$\alpha(x) = 7 + 5x + 3x^2 + 4x^3 \rightarrow \alpha(x) = (y^2+y+1) + (y^2+1)x + (y+1)x^2 + y^2 x^3$

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

10-10-05 Kodtech - shiftreg. hálózata



Tulajdonságok:

- tetszőleges számú hiba jav. ✓
- MDS (optimális) ✓
- Bináris adatátvitelű ✓

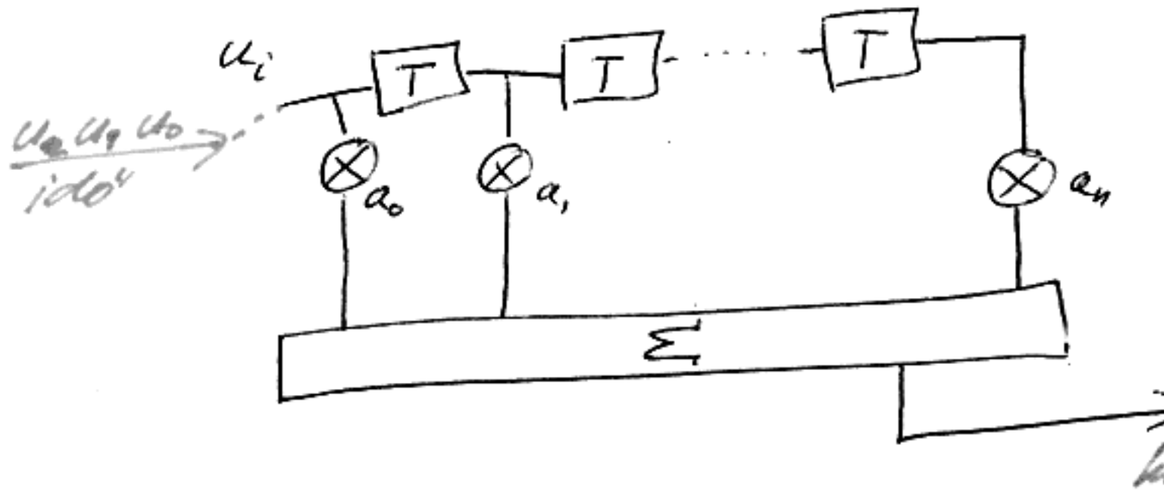
→ egyszerű HW-en implementálni?

↓

1 db SHR

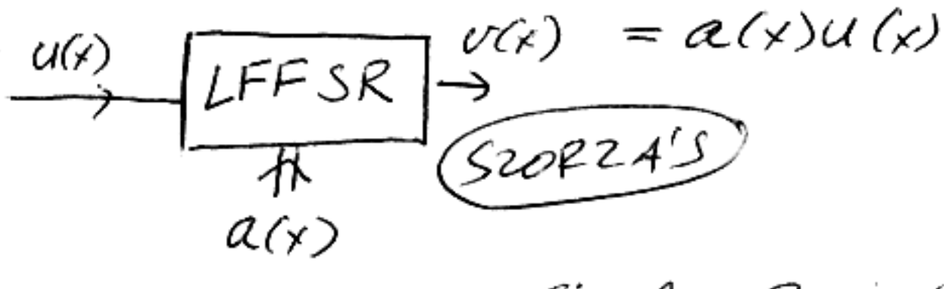
Shiftregiszter - architektúrák

Linear FeedForward Shift Register (LFFSR)

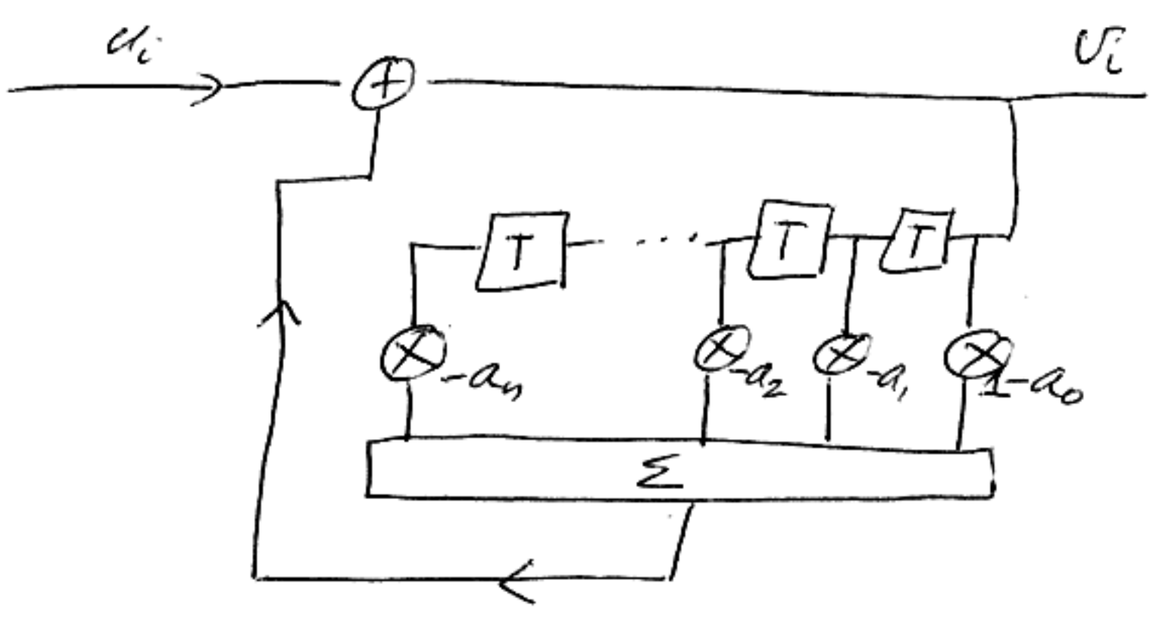


$$v_i = \sum_{j=0}^{n} a_j u_{i-j} \rightarrow$$

$$\rightarrow \bar{v} = \bar{a} * \bar{u} \xrightarrow{\text{pl.}} V(x) = a(x)U(x)$$



Linear FeedBack Shift Register



$$v_i = u_i - \sum_{i=1}^{n} a_i v_{i-j} + (1-a_0) v_i \Rightarrow$$

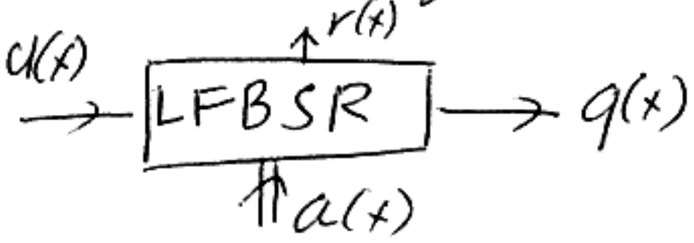
$$\Rightarrow \sum_{j=0}^{n} a_j v_{i-j} = u_i \rightarrow$$

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

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

OSZTÁS

Euklideni algoritmus



$$deg(u(x)) = n > deg a(x) = n$$

$$u(x) = q(x)\,a(x) + r(x)$$

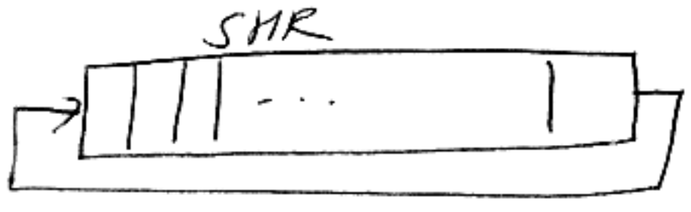
MARADÉKOS OSZTÁS

Technológiai célkitűzés: kódok SR-es implementálása
Algebrai kihívás: mátrix-vektor műveletek helyett polinomok körüli műveletek

Ciklikus eltolás: adott egy kódvektor:

$$\bar{c} = (c_0, c_1 \dots c_{n-2}, c_{n-1});$$

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



$$c'(x) = x \cdot c(x) \mod (x^m - 1)$$

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

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

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

$$x \cdot c(x) = c_{n-1}(x^n - 1) + c'(x)$$ (Ezt láttuk be az előző 4 sorban)

Lineáris ciklikus kódok

$$\bar{c} \in G \Rightarrow \bar{c}' = S\bar{c} \in G$$

$$\bar{c}, \bar{c}' \in G \Rightarrow \alpha\bar{c} + \beta\bar{c}' \in G$$

Főtétel: Minden $C(n,k)$ lineáris ciklikus kódhoz $\exists$ $g(x)$, generátor-polinom

$$g(x) \begin{cases} deg(g(x)) = n - k \\ g_{n-k} = 1 \\ \forall c(x) \in G : c(x) = u(x)\,g(x) \\ g(x) \mid x^n - 1 \end{cases}$$

→ technikai jelentőség:

Bizonyítás (nem kell tudni):

$a(x) \in G$

$deg(a(x)) = m \le deg(c(x))$

$g(x) := a_m^{-1} a(x) \in G$; $g_m = 1$

$g'(x)$ nem létezik, mert $g(x) - g'(x) \in G$,

$deg(g(x) - g'(x)) < m$ ↯

10-10-05 Kodtech

$g(x), x\,g(x), x^2 g(x) \dots x^{n-m-1} g(x) \in G$ a ciklikusság miatt

$u_0 g(x) + u_1 x g(x) + u_2 x^2 g(x) + \dots + u_{n-m-1} x^{n-m-1} g(x) \in G$

$(u_0 + u_1 x + u_2 x^2 + \dots + u_{n-m-1} x^{n-m-1}) g(x) \in G$

$u(x)\, g(x) \in G$

$\forall c(x) : c(x) = u(x) g(x) + r(x)$ $\quad r(x) = c(x) - u(x) g(x) \in G$

$\deg(r(x)) < \deg(g(x))$

$r(x) = \emptyset$

$n - m - 1 = k - 1 \Rightarrow m = n - k$

$x^k g(x) = (x^n - 1) + c(x)$

$c(x)$: osztható $g(x)$-szel

$x^k g(x)$: osztható $g(x)$-szel

osztható $g(x)$-szel

BIZONYÍTÁS VÉGE

paritásellenőrző polinom

$\forall c(x) \in G : h(x)\, c(x) = \emptyset \mod(x^n - 1)$

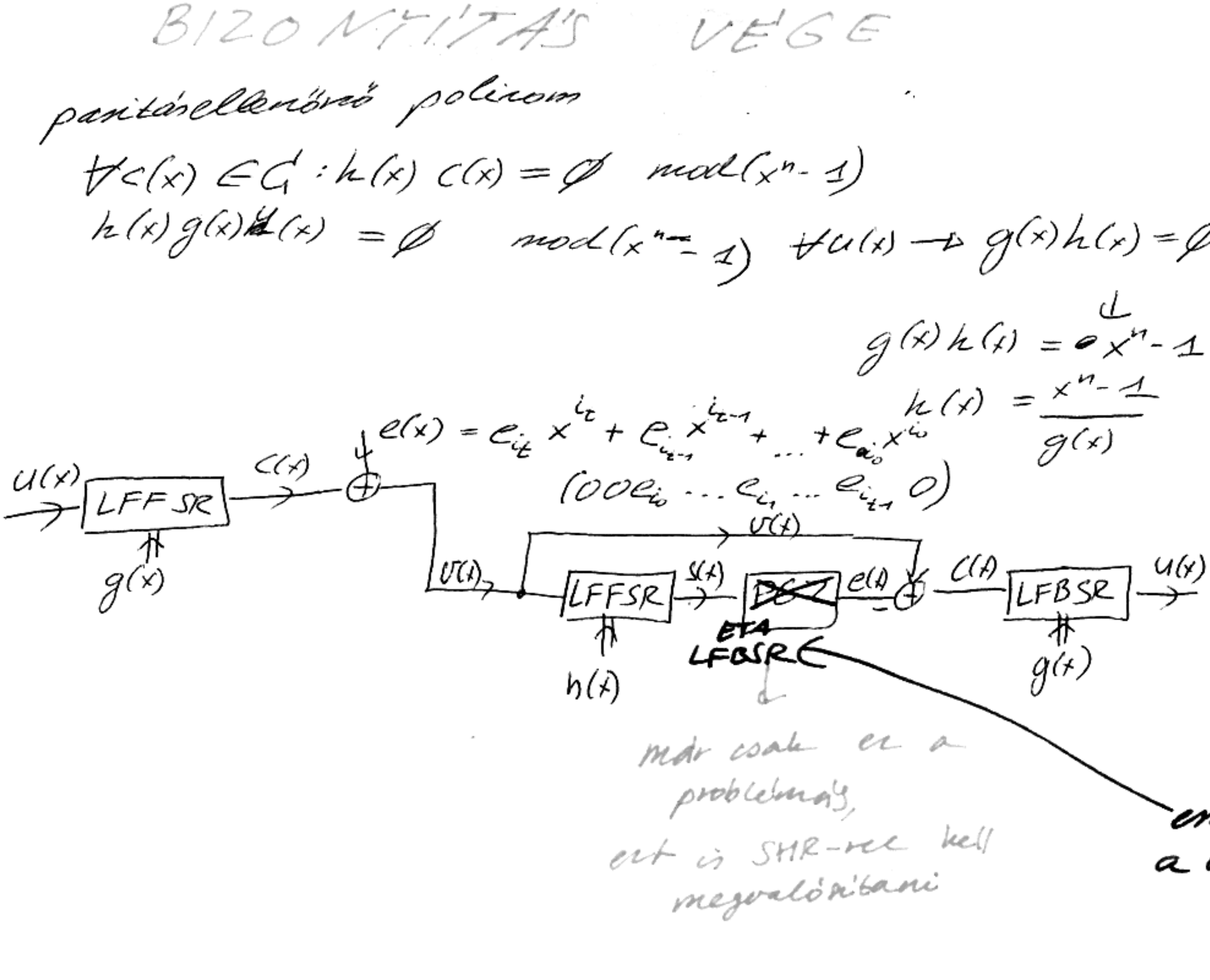
$h(x) g(x) u(x) = \emptyset \mod(x^n - 1)$ $\forall u(x) \to g(x) h(x) = \emptyset \mod(x^n - 1)$

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

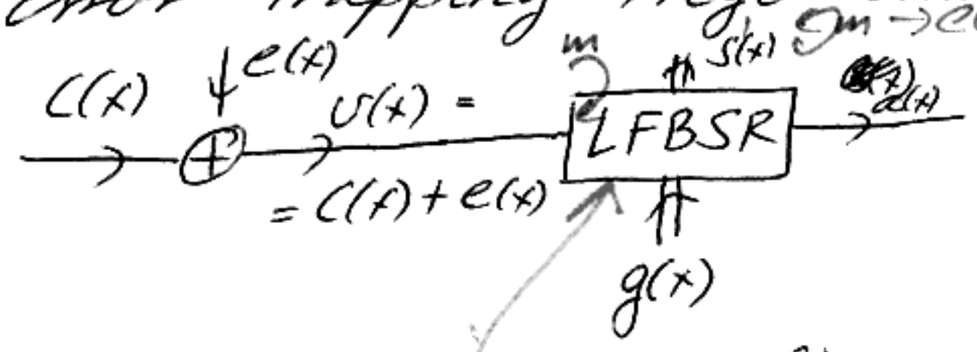
$h(x) = \frac{x^n - 1}{g(x)}$

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

$(0\,0\,e_{i_0} \dots e_{i_1} \dots e_{i_{t-1}}\, 0)$



Error Trapping Algoritkm (hibadetekció ciklikus kódok esetén)



$$U(x) = a(x)g(x) + S(x)$$

kulcsegyenlet: $U(x) = C(x) + e(x)$

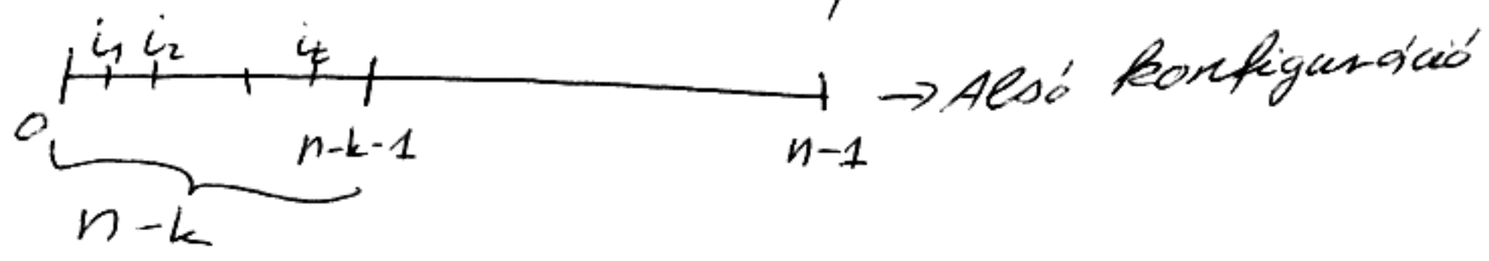
$$U(x) = C(x) + e(x) = a(x)g(x) + b(x)g(x) + S(x)$$

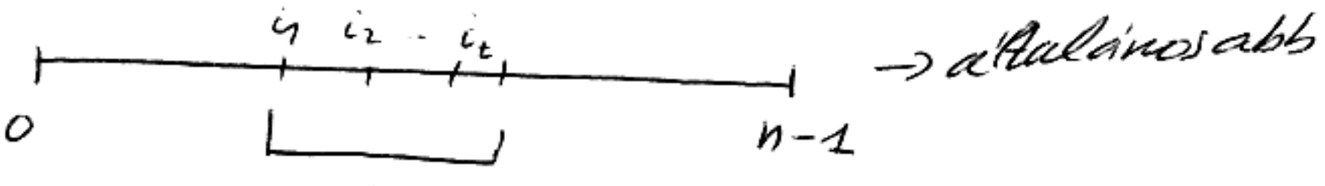
$S(x) = S(x)$, ugyanaz

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

$$\left.\begin{aligned} U(x) &= a(x)g(x) + S(x) \\ U(x) &= a(x)g(x) + e(x) \end{aligned}\right\} \Rightarrow e(x) = S(x)$$ HA elég kicsi a hiba polinom alakban

fokszáma





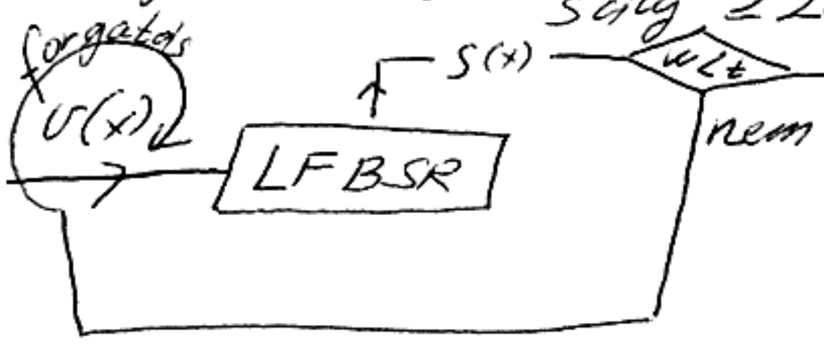
$n-k-1$

$$x^{-m}U(x) = x^{-m}a(x)g(x) + x^{-m}e(x)$$

$$x^{-m}U(x) = a'(x)g(x) + S'(x)$$ → ez van zöddel a fenti ábrán

$$x^{-m}e(x) = b'(x)g(x) + S'(x)$$

$$\underbrace{x^{-m}e(x)}_{súly < t} - \underbrace{S'(x)}_{\leq t} = \underbrace{b'(x)g(x)}_{súly \geq 2t+1} \in C$$



$S(x) = x^{-m}e(x) \ominus x^{+m}S(x) = e(x)$

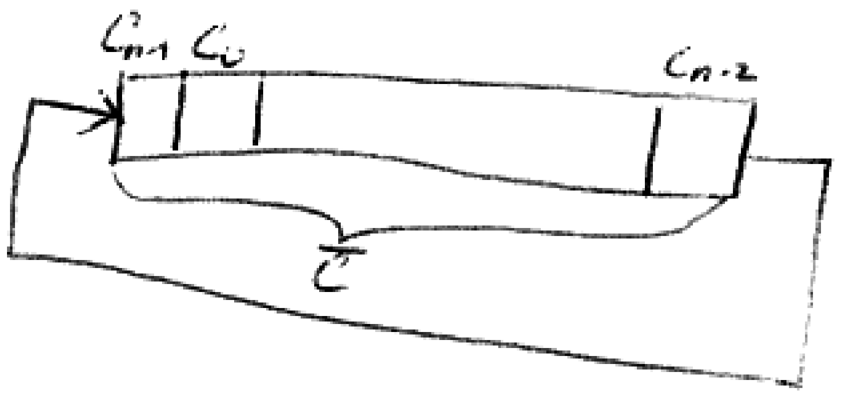
⟸ egyetlen SHR kell hozzá

szuboptimális, mert csak akkor tud javítani, ha a hiba egy $n-k-1$ hosszú regiszterbe esik (való életben az elég való ritka)

10-10-12 Kodtech

Ciklikus kódok (lineáris)

$c(x) \xrightarrow{S} c'(x) = x \cdot c(x) \mod (x^n - 1)$

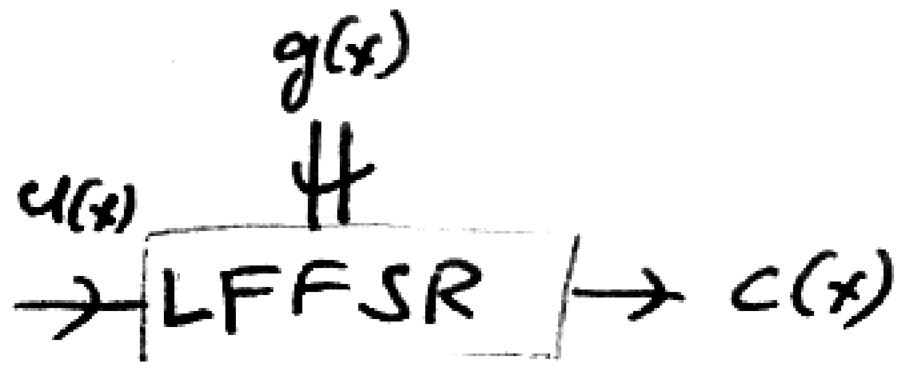


$c(x) \in C \Rightarrow c'(x) \in C$

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

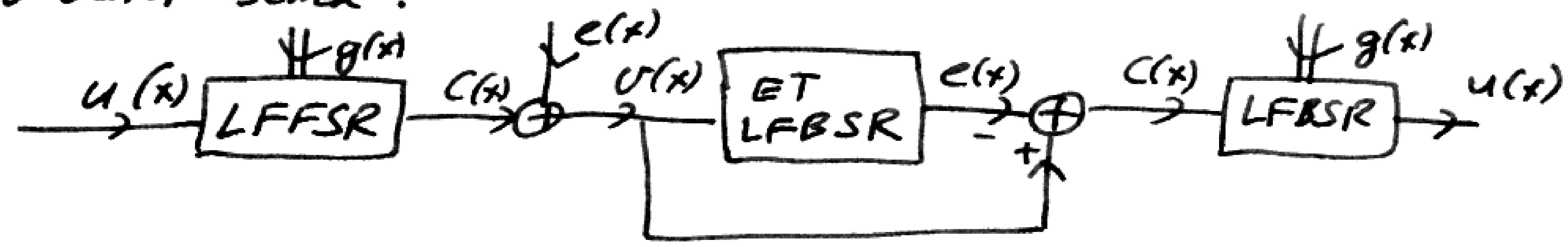
$g_{n-k} = 1$ (főegyütthatós)

$\forall c(x).\ c(x) = u(x) g(x) \Rightarrow$



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

Kódolási séma:



jó, mert
- REAL TIME
- SHR-en implementálható

Kérdés: Milyen a kód teljesítő-képessége, hány hiba javítható? $t = ?$

adott "t" $\xrightarrow[?]{}$ $g(x)$

Állítás: Az RS kódok ciklikusak. = minden, mit írtunk.

⇓ → minden SHR-en implementálható

MDS (optimális)

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

Bizonyítás:

$c(x)\Big|_{x=y^i} = 0,\ \forall i = 1, \dots, n-k;\ \deg(c(x)) = n-k$

gyöktényezős alak:

$$c(x) = \left(\prod_{i=1}^{n-k} (x - y^i)\right) u(x)\ ;\ g(x) = \prod_{i=1}^{n-k} (x - y^i)$$

$$x^n-1\Big|_{x=y^i}=\varnothing \quad i=1,\dots,n \Rightarrow (y^i)^n-1=(y^n)^i-1=1^i-1=1-1=\varnothing .$$

$$x^n-1=\prod_{i=1}^{n}(x-y^i)=\underbrace{\prod_{i=1}^{n-k}(x-y^i)}_{\text{generátor polinom } g(x)}\cdot\underbrace{\prod_{i=n-k+1}^{n}(x-y^i)}_{\text{paritás ellenőrző polinom}}$$

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

Kódtervezés:

adott: t

1, a kód paramétereinek megkeresése:

$$t=\left\lfloor\frac{n-k}{2}\right\rfloor, \quad n=2^m-1 \Rightarrow n,k,m$$

2, $GF(2^m) \rightarrow$ y primitív elem $\rightarrow g(x)=\prod_{i=1}^{n-k}(x-y^i)$

3, implementációs séma

Példa: Tervezzünk egy $t=2$ hiba javítására alkalmas ciklikus RS kódot.

$t=2$

1)
$$2=\left\lfloor\frac{n-k}{2}\right\rfloor \Rightarrow n-k\geq 4 \quad \text{(lehető legkisebb } n,k)$$

$$n=2^m-1$$

iteráció: $m=1$ —

$m=2 \quad n=3$ —

$\boxed{m=3 \quad n=7 \quad k=3}$

2) $C(7,3)$, $GF(2^3)$

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	y^1
y^8	y
y^9	y^2 (ismétlődik)

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

$$=(x^2+y^4x+y^3)(x^2+y^6x+1)=\underline{x^4}+\underline{y^6x^3}+\underline{x^2}+\underline{y^4x^3}+$$

$$+\underline{y^3x^2}+\underline{y^4x}+\underline{y^3x^2}+\underline{y^2x}+\underline{y^3}=y^4\underline{x^4}+\underline{y^3x^3}+\underline{x^2}+\underline{yx}+\underline{y^3}$$

$$h(x)=\prod_{i=5}^{7}(x-y^i)=\dots$$ (hibacsapda-alg.-kal nem kell)

3) el implementálandó sémán

10-10-12 Kodtech

A Kommunikációs mérnökség és a hibajavító kódolás kapcsolata

$$SNR = \frac{\text{jel adó teljesítmény}}{\text{zajenergia}} = \frac{A^2}{N_0} \rightarrow \frac{\text{technológia}}{\text{természet}}$$

(jel-zaj viszony paraméter)

(kimérhető)

$QoS = P_b$ = bithiba - valószínűség

(a szolgáltatás minősége)

$P_b \stackrel{?}{=} \psi(SNR, d_{min})$ → ezt kutatjuk

célállat: $y \in \{0,1\}$ → BSC → $\hat{y} = \{0,1\}$

valóság: $y \in \{-1, A\}$

zaj: $\gamma \sim N(0, \sqrt{N_0})$ normális eloszlású

$x = y + \gamma$ → Σ → $\hat{y} = \text{sgn}(x)$

döntő

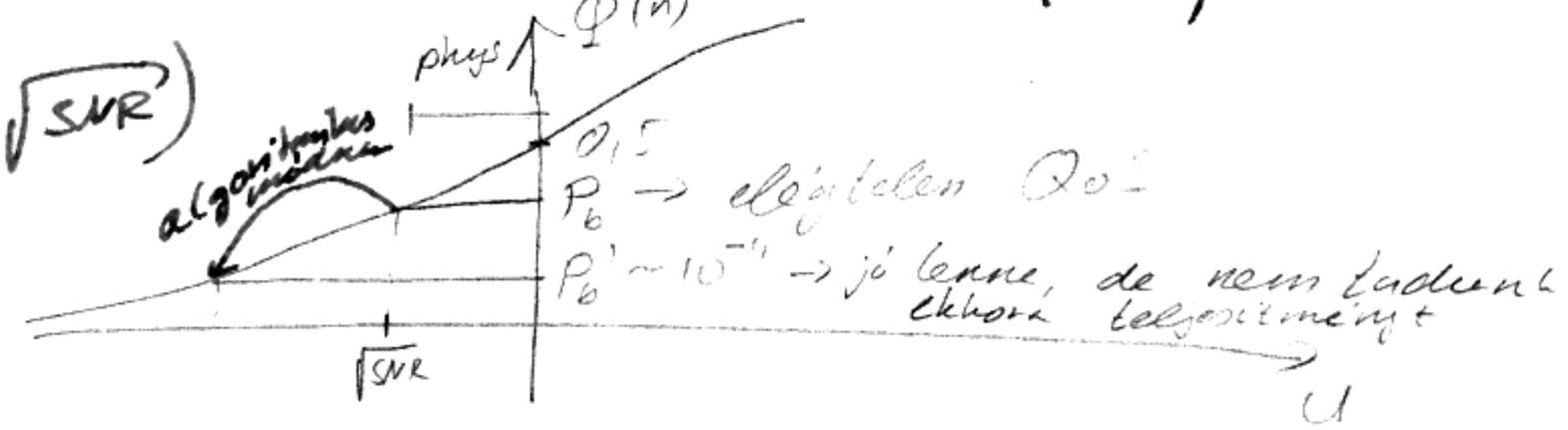
$$P_b = P(\hat{y} \neq y) = \frac{1}{2} P(\hat{y} = 1 | y = -A) + \frac{1}{2} P(\hat{y} = -1 | y = A) =$$

$$= \frac{1}{2} \{ P[\text{sign}(-A+\gamma) = 1] + P(\text{sign}(A+\gamma) = -1) \} =$$

$$= \frac{1}{2} \{ P(-A+\gamma > 0) + P(A+\gamma < 0) \} =$$

$$= \frac{1}{2} \{ P(\gamma > A) + P(\gamma < -A) \} = \Phi\left(-\frac{A}{N_0}\right) = \phi\left(-\sqrt{\frac{A^2}{N_0}}\right) =$$

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



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

$SNR = \frac{A^2}{N_0}$

$P_b' \approx \phi(\sqrt{d_{min} \cdot SNR})$ → algoritmikus kódolás → algoritmikus módszerrel helyettesítjük a nagyobb adóteljesítményt

— MOZI —

A digitális adatátvitel javítása ....

10-10-14 Kodtech

BCH kódok

Reed-Solomon kódok ciklikusan implementálhatók

↓

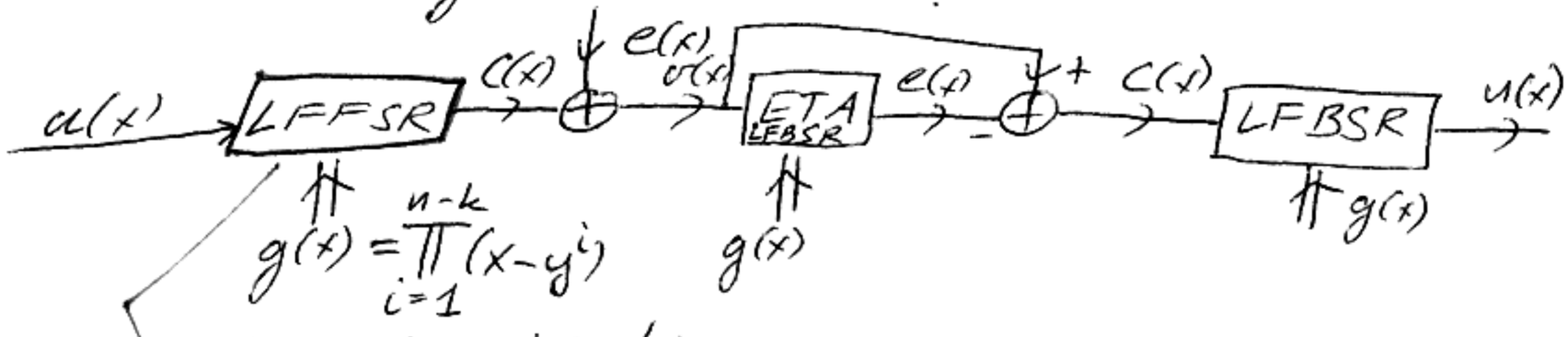
optimális kód

↓

első SHR-en

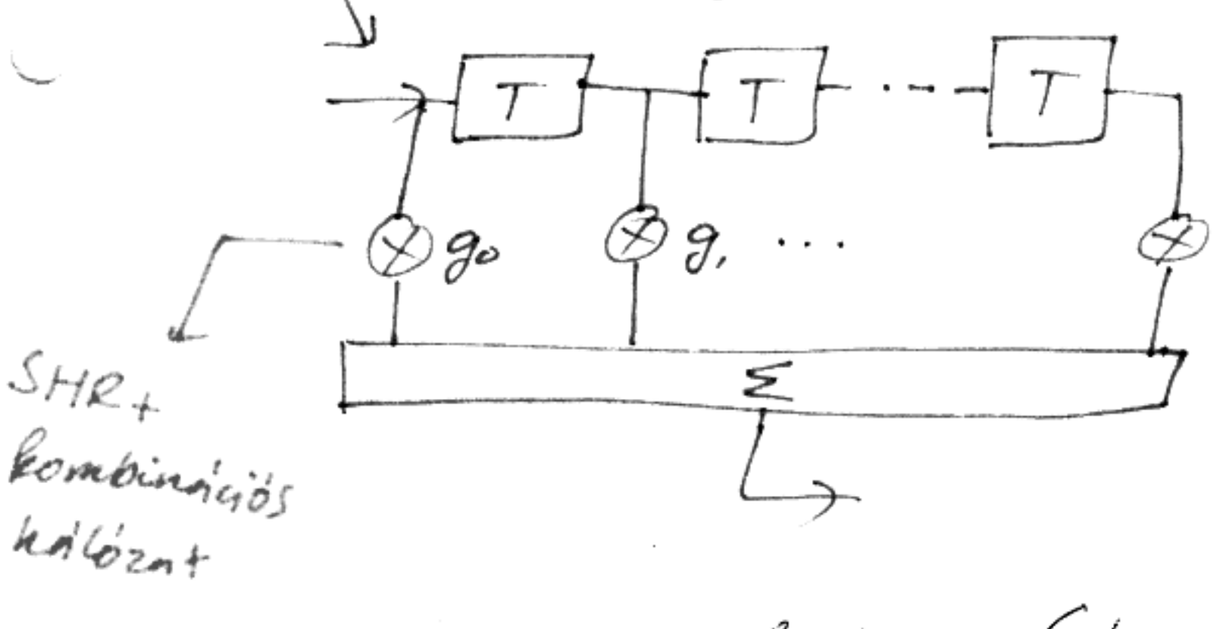
⇓

jobb a spektrális kihasználtság



Tervezés: $t \rightarrow \left\lfloor \frac{n-k}{2} \right\rfloor = t$, $n = 2^m - 1$ → $n, k, m \rightarrow GF(2^m)$

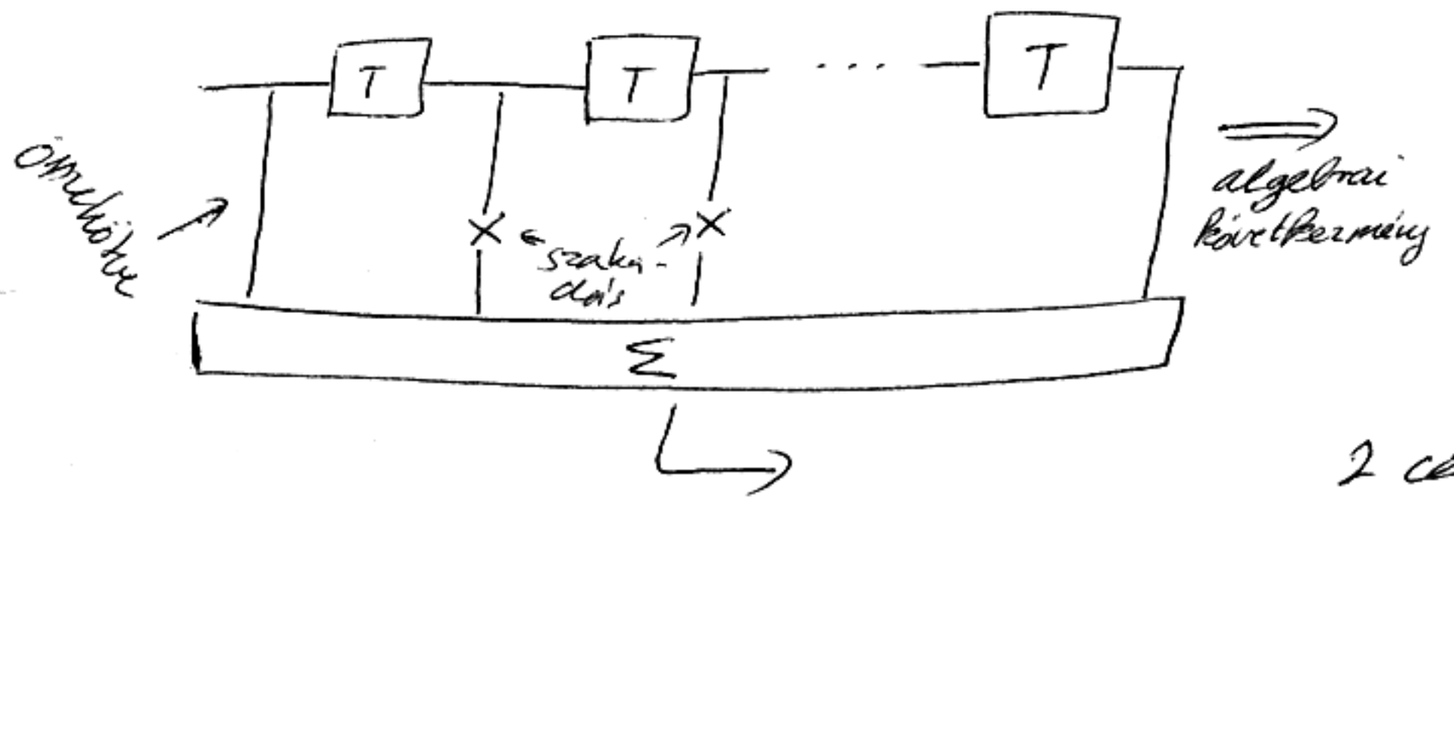
$g(x) \rightarrow P_b \rightarrow SE$



→ Túl nagy, bonyolult

→ VLSI-n nem integrálható

Kívánt architektúra (cél: kevesebb összekötetési legyen):



$g(x) = g_0 + g_1 x + \ldots + g_{n-k} x^{n-k}$

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

↓

$GF(2)$ feletti polinom

2 cél: szegénnyes együtthatók

gazdag gyökök

↓

Ezt hívják BCA kódnak.

A $GF(2)$ feletti polinomok tulajdonságai:

$f(x) = f_0 + f_1 x + f_2 x^2 + \ldots + f_n x^n, \quad f_i \in \{0, 1\} \; \forall i = 0, \ldots, n$

Állítás:

$$f(x^{2^l}) = [f(x)]^{2^l}$$

Részbizonyítás:

$f(x^2) = [f(x)]^2 : f^2(x) = f_0^2 + f_0(f_1 x + f_2 x^2 + \ldots + f_n x^n) + f_0(f_1 x + f_2 x^2 + \ldots + f_n x^n) +$

$+ (f_1 x + f_2 x^2 + \ldots + f_n x^n)^2 = f_0^2 + f_1^2 x^2 + f_1(\ldots) + f_1(\ldots) + (f_2 x^2 + f_3 x^3 + \ldots + f_n x^n) =$

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

Következmény: $f(\beta) = \emptyset \Rightarrow f(\beta^{2^i}) = \emptyset$

Biz: $f(\beta) = \emptyset \to f^2(\beta) = f(\beta^2) = \emptyset$

$\beta, \beta^2, \beta^4, \dots, \beta^{2^i} \to$ konjugált gyökök

Minimálpolinomok GF(2) felett: $\phi(x)$, $\phi(\beta) = \emptyset \Rightarrow \phi(\beta^{2^i}) = \emptyset$;

$deg(\phi(x)) < deg(f(x))$, $f(\beta) = \emptyset$

1, $\phi(x)$ irreducibilis: $\emptyset = \phi(x)\big|_{x=\beta} \neq p_1(x)\big|_{x=\beta} p_2(x)\big|_{x=\beta}$

2, $\phi(x) \mid f(x)$; $f(x)\big|_{x=\beta} = q(x)\phi(x)\big|_{x=\beta} + r(x)\big|_{x=\beta} = \emptyset \Rightarrow r(x) = \emptyset$

Példa: $\phi(x)$ konstrukciója GF(8)-ban.

konjugált gyökcsaládok $(y, y^2, y^4) \to \phi_1(x)$

$(y^3, y^6, y^5) \to (y^3, y^5, y^6) \to \phi_3(x)$ ($y^5 = y^{12}$)

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
⋮	⋮

$\phi_1(x) = (x-y)(x-y^2)(x-y^4) = (x^2+y^4x+y^3)(x+y^4) =$

$= x^3 + y^4x^2 + y^3x + x^2y^4 + y^8x + y^7 = x^3 + (y+1)x + yx + 1 = x^3 + x + 1$

($y^8 = y$, $y^7 = 1$, $(y+1)x + yx = x$)

Ez jó, mert 0 v 1 együttható

$\phi_3(x) = (x+y^3)(x+y^5)(x+y^6) = (x^2 + y^3x + y^5x + y^8)(x+y^6) = x^3 + y^2x^2 + yx + y^6x^2 +$

$+ y^8x + y^7 = x^3 + x^2 + 1$

($y^3x + y^5x = y^2x$, $y^8 = y$, $y^8x = yx$, $y^7 = 1$)

Ez is jó, mert minden együttható 0 v. 1

Bose - Chaudhuri - Hocquenheim (BCH) kód

"t" hiba javítása

$g(x)$ GF(2) feletti

$g(x) = \phi_1(x)\phi_2(x)\phi_3(x)\phi_4(x)\dots\phi_{2t-1}(x)$

⇕

$g(x)\big|_{x=y^i} = \emptyset$, $i = 1, \dots, 2t$

$c(x)\big|_{x=y^i} = u(x)g(x) = \emptyset$ $i = 1, \dots, 2t$

$$\left.\begin{matrix} c_0 + c_1y + c_2y^2 + \dots + c_{n-1}y^{n-1} = \emptyset \\ c_0 + c_1y^2 + c_2y^4 + \dots + c_{n-1}y^{2(n-1)} = \emptyset \\ \vdots \\ c_0 + c_1y^{2t} + c_2y^{4t} + \dots + c_{n-1}y^{t(n-1)} = \emptyset \end{matrix}\right\} \begin{pmatrix} 1 & y & y^2 & \dots & y^{n-1} \\ 1 & y^2 & y^4 & \dots & y^{2(n-1)} \\ \vdots \\ 1 & y^{2t} & y^{4t} & \dots & y^{t(n-1)} \end{pmatrix}$$

$\Rightarrow$ 2t db oszlopvektor kiválasztása $\Rightarrow$ van der Monde $\Rightarrow$ 2t db lineárisan független oszlopvektor

⇓

$d_{min} = 2t + 1 \Rightarrow t$ hiba jav.

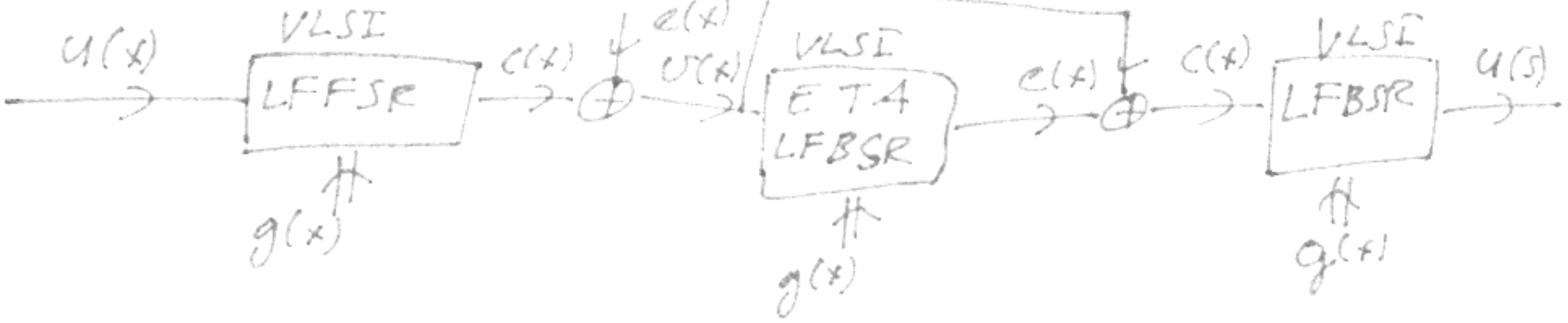
10-10-14 Kodtech

Példa (általános)

adott: "t" hiba javítandó

$\phi_1(x), \phi_3(x), \dots, \phi_{2t-1}(x)$

$$g(x) = \phi_1(x)\,\phi_3(x) \cdot \dots \cdot \phi_{2t-1}(x)$$

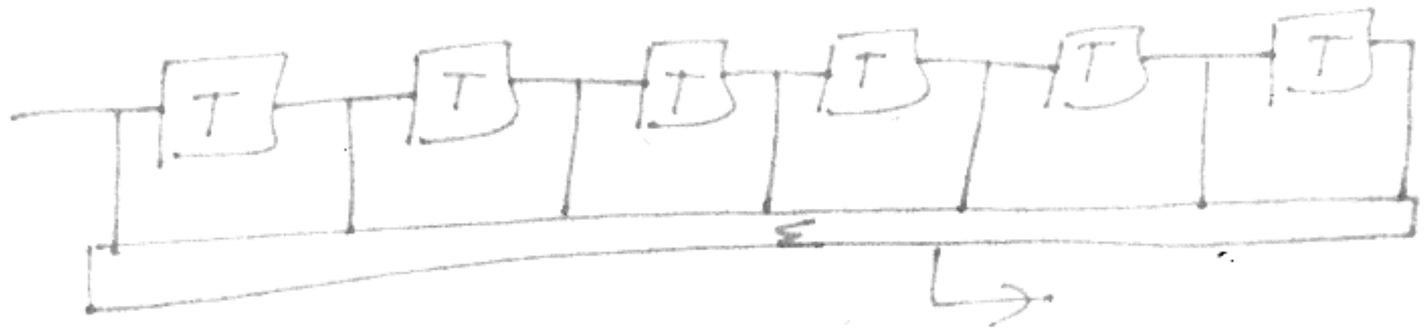


Példa (konkrét):

t=2 hiba javítása BCH kóddal a GF(8) felett

$t=2 \rightarrow 2t-1=3$

$g(x) = \phi_1(x)\,\phi_3(x) = (x^3+x+1)(x^3+x^2+1) = x^6 + x^5 + x^3 + x^2 + x^5 + x^4 + x^3 + x + 1 = x^6 + x^4 + x^2 + x + 1$



Ténteség: $\deg(g(x)) = 6 = n-k$

$n = 8-1$

$C^{BCH}(7,1)$

$C^{RS}(7,3)$ → Ez nem RS kód, nagyobb a redundancia.

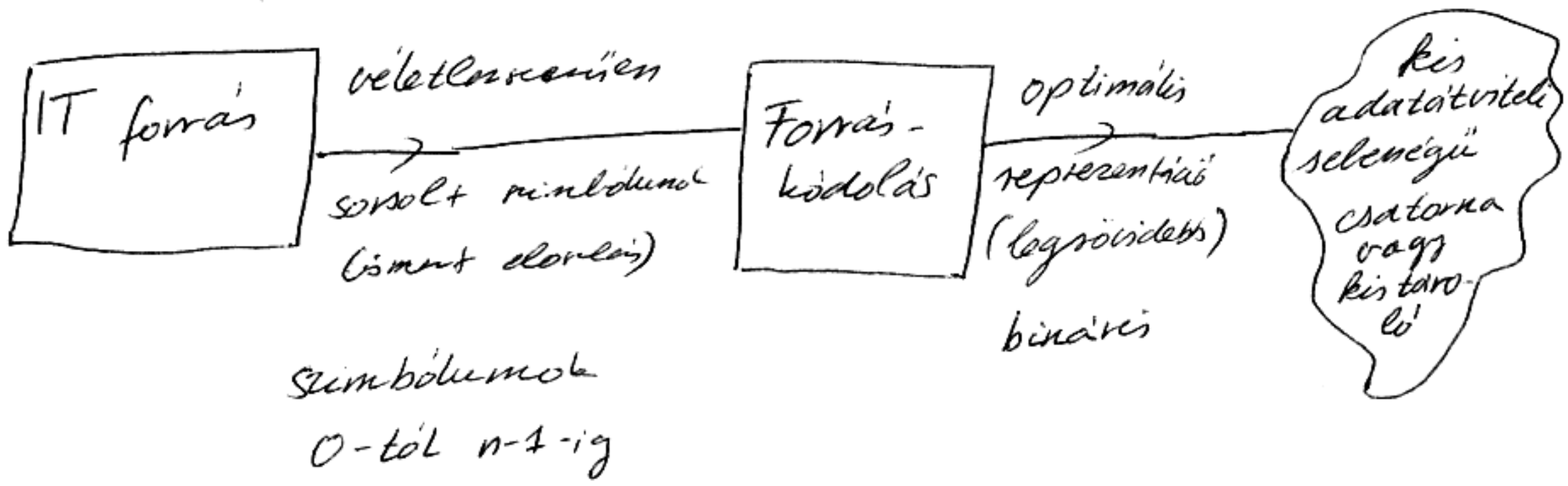
Példa szabványok:

CCITT 16-bit $g(x) = x^{16} + x^{12} + x^5 + 1$

Ethernet $g(x) = x^{32} + x^{26} + x^{23} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

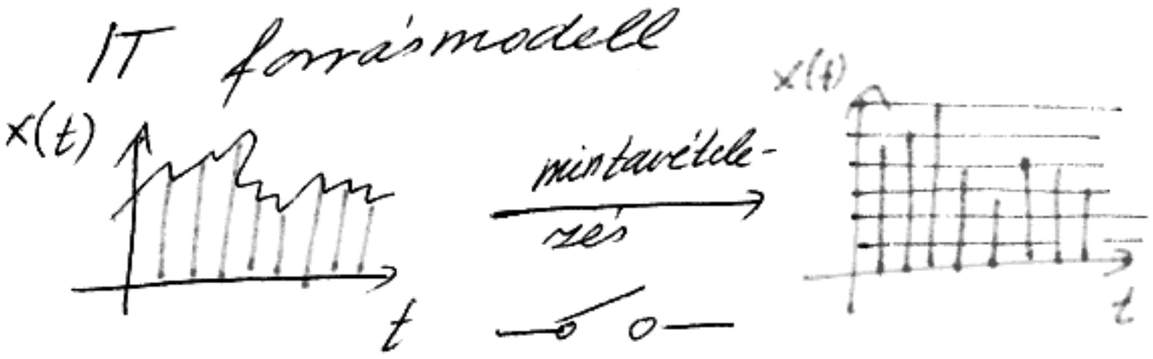
10-10-14 Kodtech

Forráskódolás
Adattömörítés



szimbólumok
0-tól n-1-ig

IT forrásmodell



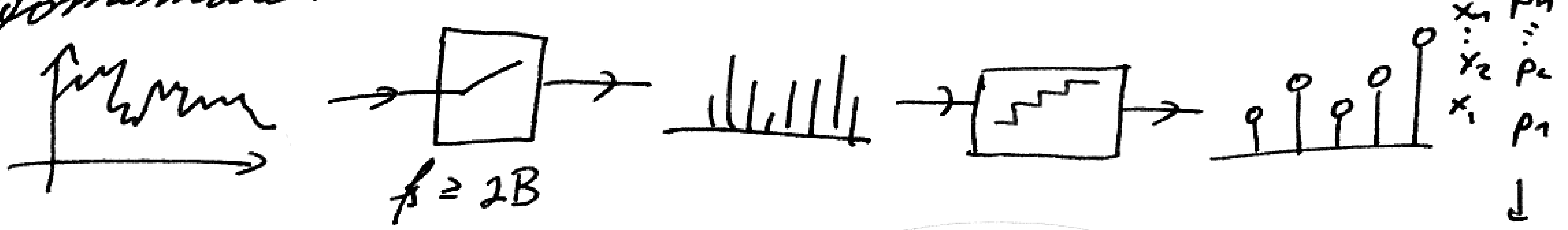
R adatátviteli sebesség
fs · n → csökkenthető"

↓ ↓
8 kHz n = 8
64 kbps vezetékes telefon

↓
a mobiltelefon keskeny sávval, jobban tömörít

10-10-19 Kódtech

Forrásmodell



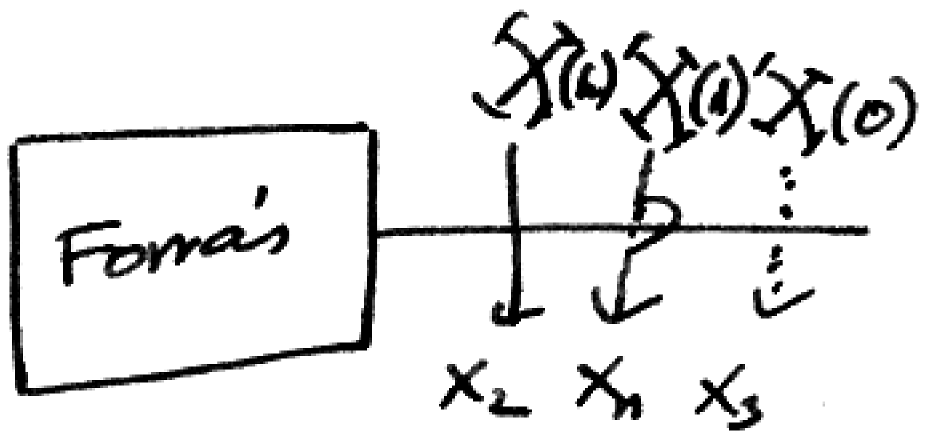
↓

diszkrét valószínűségi eloszlás

↓

X valószínűségi változó.

Ez mind a forrás



Ergodikus, stacionér emlékezetmentes forrás

$$P(X(k)=x_2 \mid X(k-1)=x_i \dots X(1)=x_n, X(0)=x_3) = P(X(k)=x_2)$$

az eloszlás időtől (k) nem függ

ergodicitás: az időbeli sokasági átlagai megegyeznek (mindegy, hogy egy marék érmét egyszerre v. egymás után dobunk le)

$$\boxed{IT} \rightarrow X \in \begin{matrix} p_1 & p_2 & \dots & p_n & \leftarrow p(x) \\ \{x_1, & x_2 & \dots & x_n\} & \leftarrow X \\ \bar{c}_1 & \bar{c}_2 & \dots & \bar{c}_N & \leftarrow \bar{c}(x) \\ \downarrow & \downarrow & & \downarrow & \\ l_1 & l_2 & & l_n & \leftarrow l(x) \end{matrix}$$

x	$\bar{c}$
x_1	0110
x_2	11
⋮	
x_n	110

⇑

G_{opt}

cél: $\min_G L$

$$L := E_x(l(x)) = \sum_x p(x) L(x)$$

$$R' = f_s \cdot L$$

intuitív ötlet: — p_i nagy → x_i gyakori → $\bar{c}_i$ → l_i kicsi
— p_i kicsi → x_i ritka → $\bar{c}_i$ → l_i nagy is lehet

problémák:

- hogyan lehet nem egyenletes hosszúságú kódot egyértelműen dekódolni?
- $l(x) \stackrel{?}{=} \Psi(p(x))$

1) Egyértelmű dekódolás

pl. Egybögrefkarejjóketmár

Σ-ott vágjunk, akkor értelmes szót találtunk

nem lenne jó:

$\bar{c}_i \prec \bar{c}_j$

(01) (01|110)

$\rightarrow$ ezt $\bar{c}_i$-nek dekódolnánk

prefixmentes kód kell

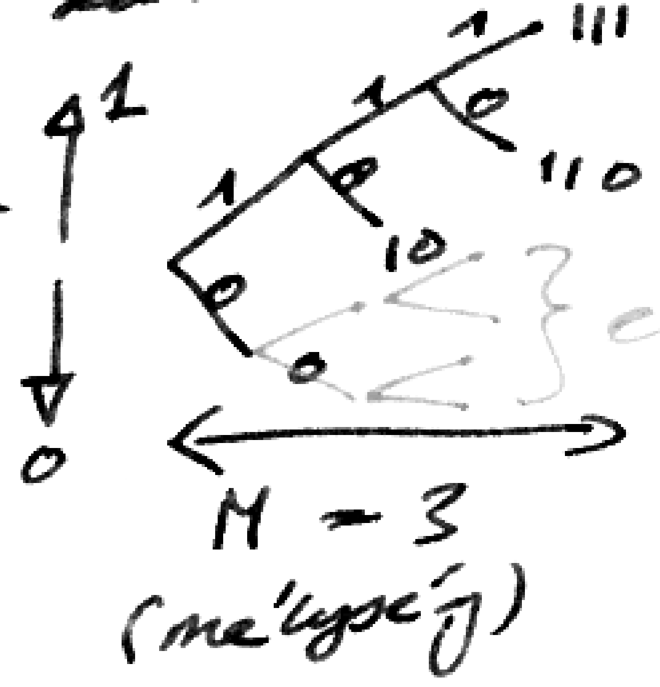
$\bar{c}_i \not\prec \bar{c}_j \quad \forall i,j = 1, \ldots, N \quad i \neq j$ $\Rightarrow$ prefix-free

Határány:

prefixmentes kódok homuisága – Kraft egyenlőtlenség

$\Updownarrow$

bináris fa



elhagyott végpontok száma

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

$$2^{M-l(x)} = 2^{3-1} = 4$$

$\Downarrow$

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

Kraft-egyenlőtlenség

$\Downarrow$

kellenek kisebb kódszavak is

Információ: $I(x) = \operatorname{ld} \frac{1}{p(x)}$ ld: 2-es alapú logaritmus

Entrópia: a forrás átlagos információtartalma

$$H(X) = E_x\, I(x) = \sum_x p(x) \operatorname{ld} \frac{1}{p(x)}$$

I-divergencia

$p(x)$, $q(x)$ eloszlások

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

Biz: lemma: $\operatorname{ld}(u) \leq u - 1$

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

$$-D(p\|q) \leq 0 \Rightarrow D(p\|q) \geq 0 \quad \square$$

10-10-19 Kodtech

$$\emptyset \leq H(X) \leq \mathrm{ld}\, N$$

↑ minden tag pozitív az összegben

↖

$$\emptyset \leq D(p(x)\|q(x)) = \sum_x p(x) \mathrm{ld} \frac{p(x)}{\frac{1}{N}} = \sum_x p(x) \mathrm{ld}(N \cdot p(x)) =$$

$q(x) = \frac{1}{N}$

$$= \sum_x p(x)\{\mathrm{ld}N + \mathrm{ld}\,p(x)\} = \mathrm{ld}N + \sum_x p(x)\,\mathrm{ld}\,p(x) \geq 0$$

$$\mathrm{ld}N \geq \sum_x p(x) \mathrm{ld}\frac{1}{p(x)}$$

az információelmélet első alaptétele – forráskódolási tétel

$L \geq H(x)$ A forrás nem tömöríthető jobban, mint ahogy azt az entrópia megengedi (ha nincs információ-vesztés)

$\sum_x p(x) L(x)$

↑

L_{opt}

Adott: $p(x)$

virtuális eloszlás $q(x) := \frac{2^{-L(x)}}{\sum_y 2^{-L(y)}}$; $\emptyset \leq q(x) \leq 1$;

$\sum q(x) = 1$

$$\emptyset \leq D(p(x)\|q(x)) = \sum_x p(x) \mathrm{ld}\left(\frac{p(x)}{q(x)}\right) = \sum_x p(x) \mathrm{ld}\, \frac{p(x)}{\frac{2^{-L(x)}}{\sum 2^{-L(y)}}} =$$

$\sum 2^{-L(y)} \leq 1$ (Kraft)

$$= \sum_x p(x) \mathrm{ld}\left(\frac{p(x)\sum_y 2^{-L(y)}}{2^{-L(x)}}\right) \leq \sum_x p(x) \mathrm{ld}\left(\frac{p(x)}{2^{-L(x)}}\right) =$$

$$= \sum p(x) \mathrm{ld}\left(2^{L(x)} p(x)\right) = \sum_x p(x)\{\underbrace{\mathrm{ld}\,2^{L(x)}}_{L(x)} + \mathrm{ld}\,p(x)\} =$$

$$= \sum_x p(x) L(x) + \sum_x p(x) \underbrace{\mathrm{ld}\,p(x)}_{= -\mathrm{ld}\frac{1}{p(x)}} \geq \emptyset$$

$$\leq p(x)L(x) \geq \sum_x p(x) \mathrm{ld}\frac{1}{p(x)}$$

$$\boxed{L \geq H(x)}$$

Shannon – Fano kódolás

Algoritmus: Adott $p(x) \to l(x) = \lceil ld \frac{1}{p(x)} \rceil \to$ bináris fán növeltjük a kódot $\bar{c}(x)$

lemma: $a \leq \lceil a \rceil \leq a+1$

pl. $2{,}31 \leq \lceil 2{,}31 \rceil = 3 \leq 3{,}31$

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

x	$\bar{c}(x)$
x_1	$\bar{c}_1$
$\vdots$	$\vdots$
x_n	$\bar{c}_n$

1, $$\sum_x 2^{-l(x)} = \sum_x 2^{-\lceil ld \frac{1}{p(x)} \rceil} \leq \sum_x 2^{-ld \frac{1}{p(x)}} = \sum_x 2^{ld\, p(x)} = \sum_x p(x) = 1$$

2, Teljesítőképesség: $H(X) \leq L \leq H(x) + 1$

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

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

Példa:

x_1 $p_1 = 0{,}49$

x_2 $p_2 = 0{,}14$

x_3 $p_3 = 0{,}14$

x_4 $p_4 = 0{,}07$

x_5 $p_5 = 0{,}07$

x_6 $p_6 = 0{,}04$

x_7 $p_7 = 0{,}02$

x_8 $p_8 = 0{,}02$

x_9 $p_9 = 0{,}01$

1. lépés: kódszóhosszak

$l_1 = \lceil ld \frac{1}{p_1} \rceil = \lceil 1{,}029 \rceil = 2$

$\vdots$

$l_2 = 3$

$l_3 = 3$

$l_4 = 4$

$l_5 = 4$

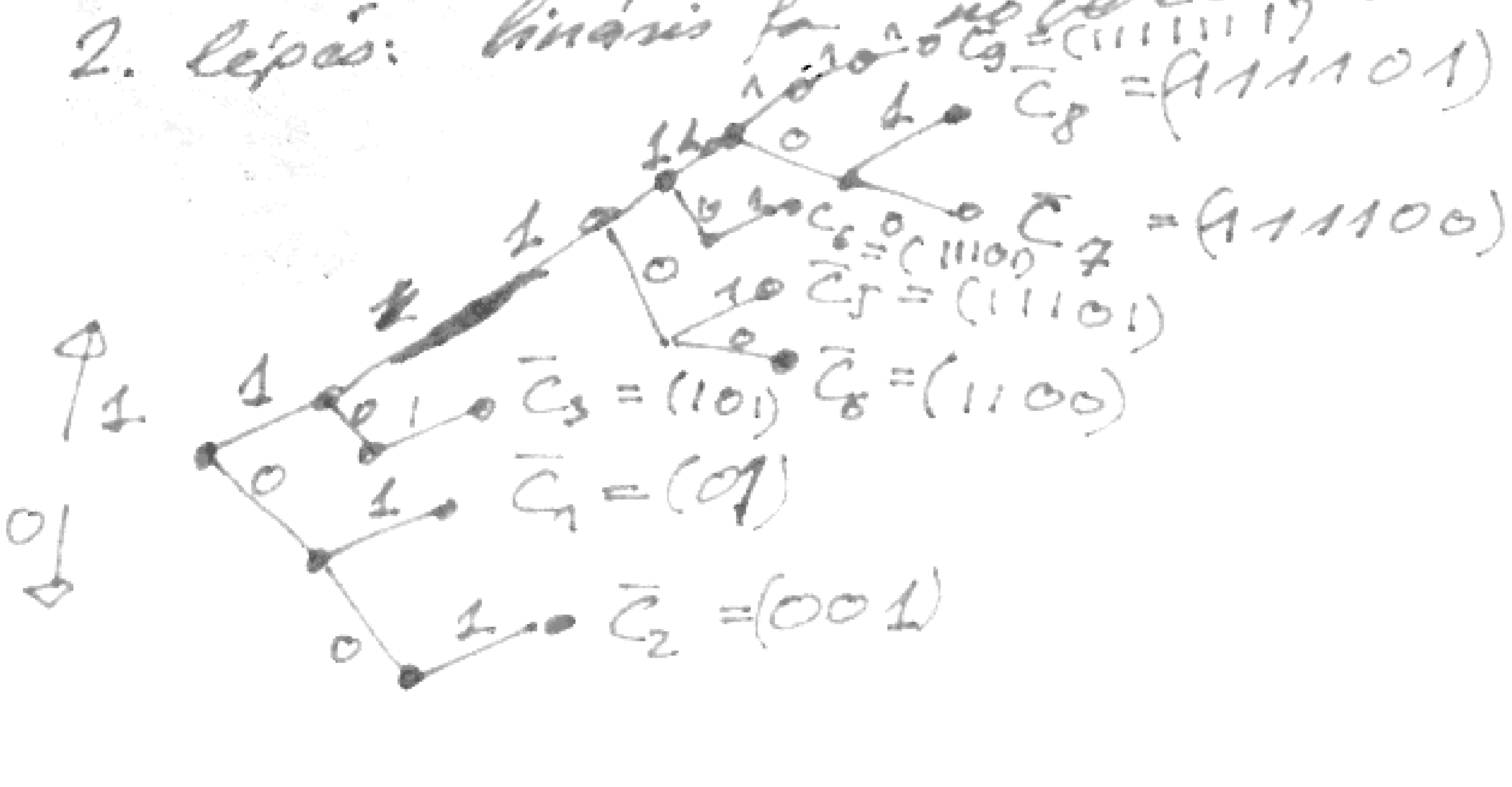
$l_6 = 5$

$l_7 = 6$

$l_8 = 6$

$l_9 = 7$

2. lépés: bináris fa növekedése:

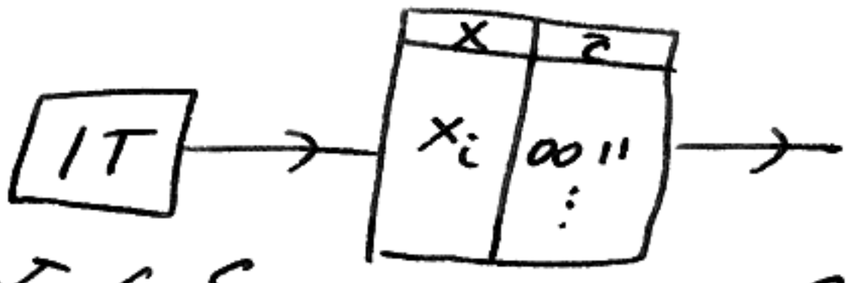


problémák:

nem egyértelmű

nem optimálisan rövid

10-10-21 Kodtech



$X \in \{x_1, x_2 \dots x_N\} \rightarrow \{p_1, p_2 \dots p_N\}$

$\bar{c}_1 \; \bar{c}_2 \dots \bar{c}_N$

$l_1 \; l_2 \dots l_n$

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

↑ a forrás entrópiája

Shannon-Fano kód

$l(x) = \lceil \operatorname{ld} \frac{1}{p(x)} \rceil \rightarrow$ bináris fa $\rightarrow$ "levelei" ledolgozása nem optimális (ez a példán is látszott):

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

Kérdés: mi lesz az optimális kód? L_{min}

Optimális forráskódolás

A Huffman-kód

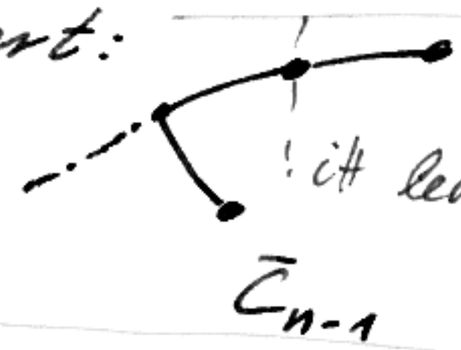
Optimális tulajdonságok:

- $p_1 > p_2 > \dots > p_{N-1} > p_N$

$\downarrow \quad \downarrow$

$l_{N-1} = l_N$

mert:



! itt levágható, úgy még jó, de rövidebb

- Ha $p_i > p_j \rightarrow l_i < l_j$

bizonyítás (indirekt):

~~$l_i > l_j$~~ $l_i > l_j$

$$L = \sum_{m \neq i,j} p_m l_m + p_i l_i + p_j l_j \geq \sum_{m \neq i,j} p_m l_m + p_i l_j + p_j l_i = L'$$

$$p_i (l_i - l_j) > p_j (l_i - l_j)$$

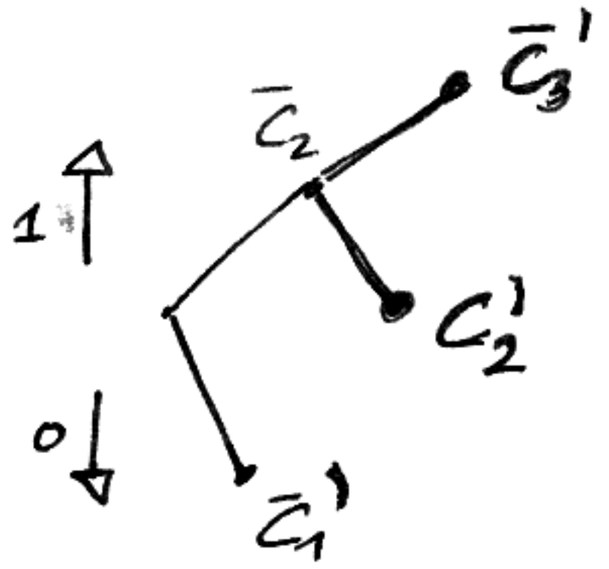
Implementáció:

$X \in \{x_1, x_2\}$

$p_1 > p_2$

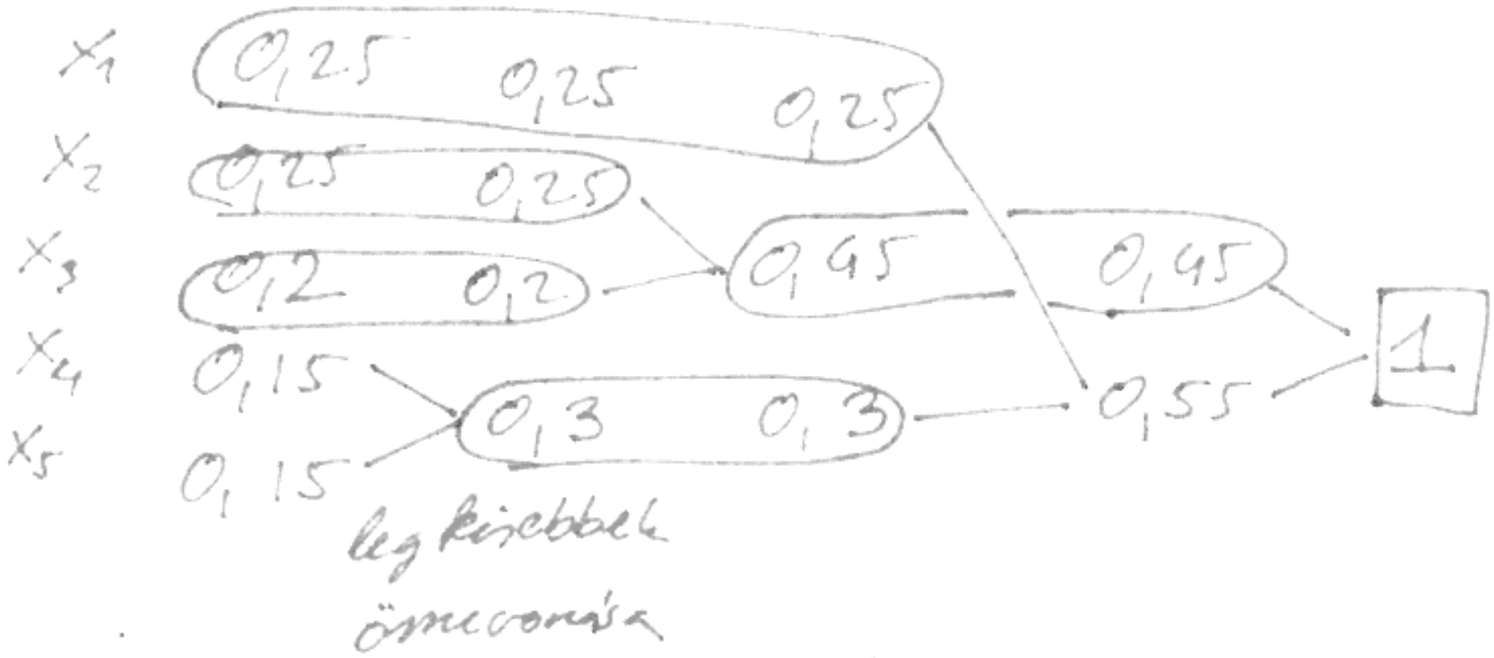
$X' \in \{x_1', x_2', x_3'\}$ $\quad p_1' = p_1$

$p_1' > p_2' > p_3'$ $\quad p_2' + p_3' = p_2$



rekurzív eljárás visszafelé is megy

Példa:



Jobbról balra kiolvasva:

X	$\bar{C}$
X_1	(11)
X_2	(01)
X_3	(11)
X_4	(101)
X_5	(100)

→ Lopt de túl komplex az algoritmus, nem real-time ~

Shannon-Fano-Elias (SFE) kód

Lemma: $0 < a \leq L \rightarrow$ bináris konverziója $\bar{a}$

$$\bar{a} = \sum_{i=1}^{\infty} a_i \cdot 2^{-i}$$

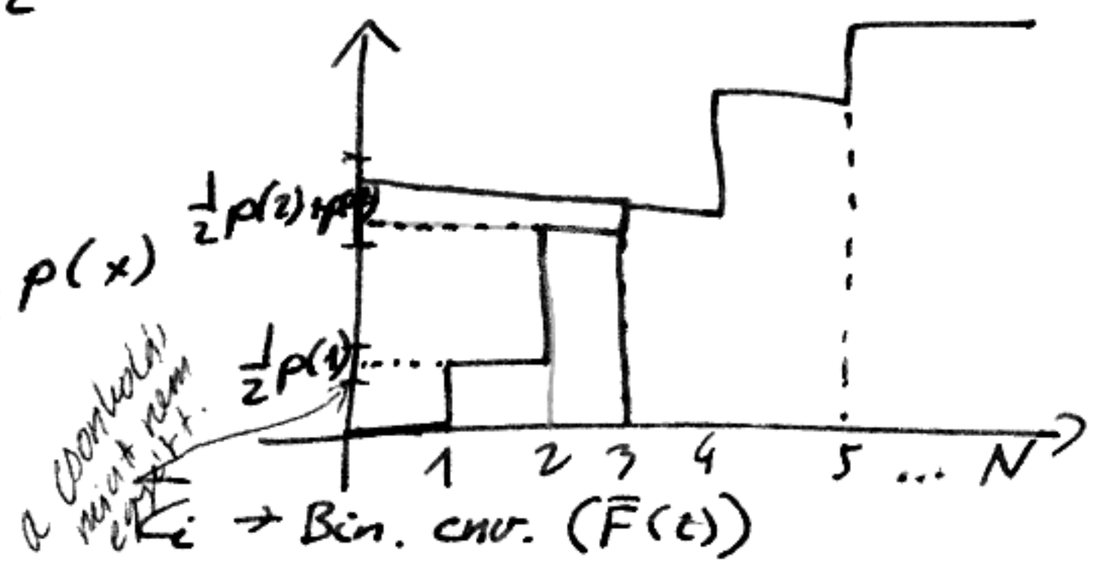
$$a' = \lfloor a \rfloor_\ell = \sum_{i=1}^{\ell} a_i \cdot 2^{-i}$$

$$a - a' = a - \lfloor a \rfloor_\ell \leq 2^{-\ell}$$

$x \rightarrow \{1, 2 \dots N\}$

$$F(x) = \sum_{a:\, a<x} p(a)$$

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



10-10-21 Kodtech

$\bar{c}_i \to \text{Bin cmp}\left(\bar{F}(i)\right) \to \left\lfloor \bar{F}(x) \right\rfloor_{l(x)}$;

$$l(x) = \left\lceil ld \frac{1}{p(x)} \right\rceil + 1 \to 2^{-l(x)} \leq \frac{p(x)}{2}$$

$$\bar{F}(x) - \left\lfloor \bar{F}(x) \right\rfloor_{l(x)} \leq 2^{-l(x)} < \frac{p(x)}{2}$$

Algoritmus: Adott $\{p_1 \dots p_N\} \to \bar{F}(x) \to \left\lfloor \bar{F}(x) \right\rfloor_{l(x)} \to$

$\to \{\bar{c}_1, \bar{c}_2 \dots \bar{c}_N\}$

Példa:

	SFE – felső	$F(x)$	$\bar{F}_{bin}(x)$
1	0,25	$0,125 = p_1/2$	0,001
2	0,25	$0,375 = p_1 + p_2/2$	0,011
3	0,2	$0,6 = p_1 + p_2 + p_3/6$	$0,1\overline{0011}$
4	0,15	0,475 :	$0,11\overline{00011}$
5	0,15	0,925	0,1110110

végtelen törtek, a felülvonás sor ismétlődik

	$l(x) = \left\lceil ld \frac{1}{p(x)} \right\rceil + 1$	$\bar{c}$
1	3	001
2	3	011
3	4	1001
4	4	1100
5	4	1110

x	$\bar{c}$
x_1	001
x_2	011
x_3	1001
x_4	1100
x_5	1110

$L^{SFE} = L^{Huffman} + 1,2$ → olcsóbb leggyártani, de gyengébb

Általában ennyivel gyengébb:

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

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

$$+ \sum_x p(x) + 1 = H(x) + 2$$

$$\boxed{H(x) \leq L^{SFE} \leq H(x) + 2}$$

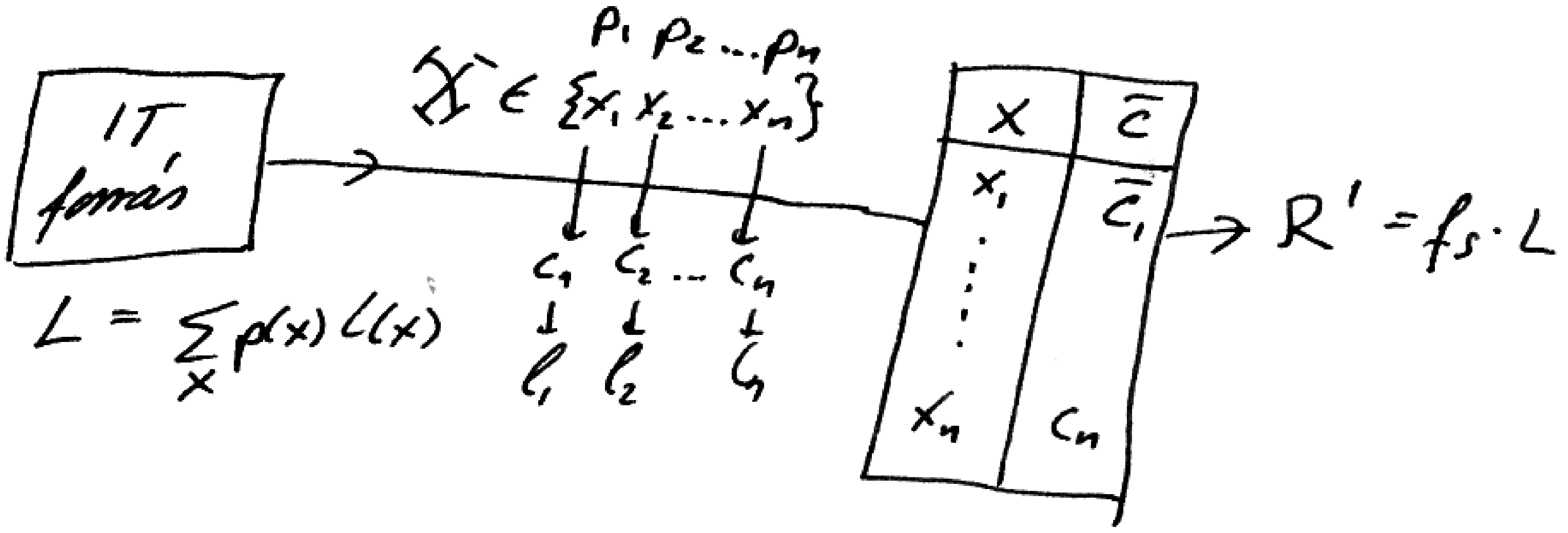
Entrópia alapú adattömörítés

név	teljesítőképesség	algoritmus komplexitása
SFE	$L \le H(x) + 2$	Bináris kereső + számolás
SF	$L \le H(x) + 1$	Bináris fa
Huff	L_{opt}	rekurzív két legkisebb p_i keresése + bináris fa

↑ algoritmikus könnyebbség

↓ jobb teljesítőképesség

10-10-26 Kódtech



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

Probléma:

- $H(X) \le L \le H(X) + \varepsilon$
  kis algoritmikus komplexitással
- $p(x)$ ismeretlen
  eloszlásfüggetlen kódolás

— MOZI —

Cél: az első alsó határhoz ε közelségbe kerülni

Az entrópia tulajdonságai

$$H(X) = \sum_x p(x)\, ld(p(x)) \to H(X,Y) = \sum_x \sum_y p(x,y)\, ld \frac{1}{p(x,y)}$$

$$H(X|Y) = E_x H(Y|X=x) = \sum_x p(x) \sum_y p(y|x)\, ld \frac{1}{p(y|x)} =$$

$$= \sum_x \sum_y p(x,y)\, ld \frac{1}{p(x,y)}$$

biz:

$$H(X,Y) = H(Y|X) + H(X) = \sum_x \sum_y p(x,y)\, ld \frac{1}{p(x,y)} =$$

$$= \sum_x \sum_y p(x,y)\, ld \frac{1}{p(y|x)p(x)} = \sum_x \sum_y p(x,y) \left\{ ld \frac{1}{p(y|x)} + ld \frac{1}{p(x)} \right\} =$$

$$= \sum_x \sum_y p(x,y)\, ld \frac{1}{p(y|x)} + \sum_x \underbrace{\sum_y p(x,y)}_{p(x)}\, ld \frac{1}{p(x)} = H(Y|X) + H(X)$$

független

$$H(X,Y) = \sum_x \sum_y p(x)p(y)\, ld \frac{1}{p(x)p(y)} = \sum_x \sum_y p(x)p(y) \left\{ ld \frac{1}{p(x)} + ld \frac{1}{p(y)} \right\} =$$

$$= \underbrace{\left(\sum_y p(y)\right)}_{1} \underbrace{\sum_x p(x)\, ld \frac{1}{p(x)}}_{H(X)} + \underbrace{\left(\sum_x p(x)\right)}_{1} \underbrace{\sum_y p(y)\, ld \frac{1}{p(y)}}_{H(Y)} = H(X) + H(Y)$$

$X_1, X_2 \dots X_N \rightarrow H(X_1, X_2 \dots X_N) = \sum_{i=1}^{N} H(x_i) = N \cdot H(X)$

függetlenek

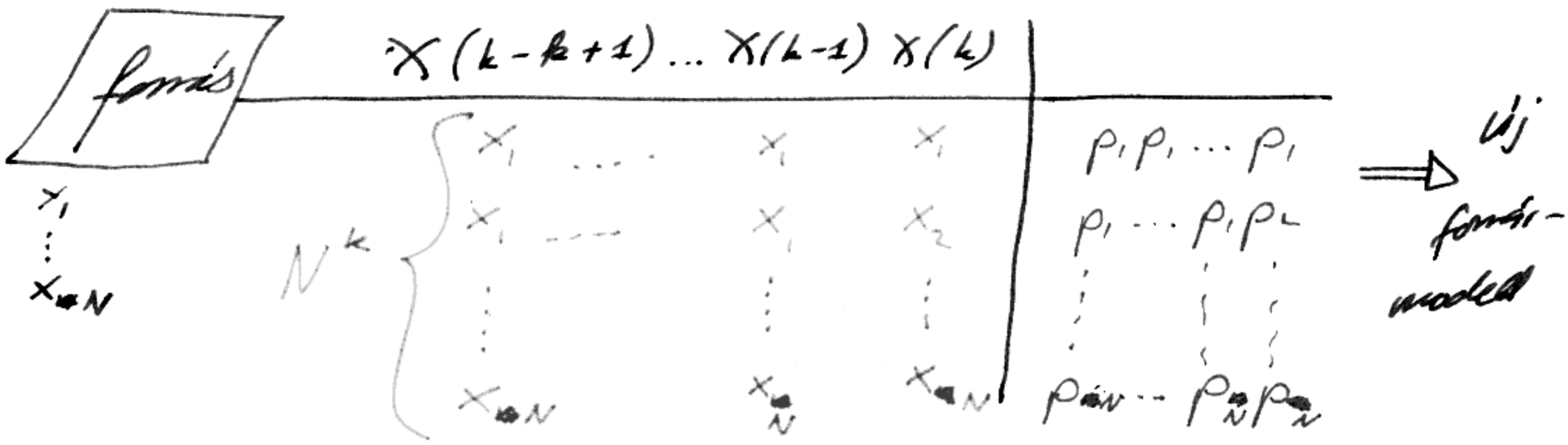
Kölcsönös információ : $I(X, Y) = D(p(x,y) \| p(x)p(y)) =$

$$= \sum_x \sum_y p(x,y) \operatorname{ld} \frac{p(x,y)}{p(x)p(y)} = \sum_x \sum_y p(x,y) \operatorname{ld} \frac{p(y|x)p(x)}{p(y)p(x)} =$$

$$= \sum_x \underbrace{\sum_y p(x,y)}_{p(y)} \left\{ \operatorname{ld} \frac{1}{p(y)} - \operatorname{ld} \frac{1}{p(y|x)} \right\} = H(Y) - H(Y|X)$$

Hogyan lehet az entrópiával tetszőlegesen közel kerülni?

→ Blokk-kódolás



$$\Rightarrow \begin{array}{c|c} Y & p' \\ \hline y_1 & p_1' \\ y_2 & p_2' \\ \vdots & \vdots \\ y_{N^k} & p_{N^k}' \end{array} \quad \text{SFE} \Rightarrow \quad H(Y) \le L^{(k)} \le H(Y)+2$$

$$H(Y) = H(X(k-k+1) \dots X(k-1)\ X(k)) =$$

$$= H(Y) = k \cdot H(X)$$

$$\lambda^{(k)} = \frac{L^{(k)}}{k}$$

egy szimbólumra jutó kódhossz

$$H(X) \le \lambda^k \le H(X) + \frac{2}{k} \rightarrow$$ az elvi alsó határ tetszőlegesen megközelíthető blokk-kódolással

10-10-26 Kodtech

Trade-off:

Adattárolás ⟺ (??) ⟺ Komplexitás

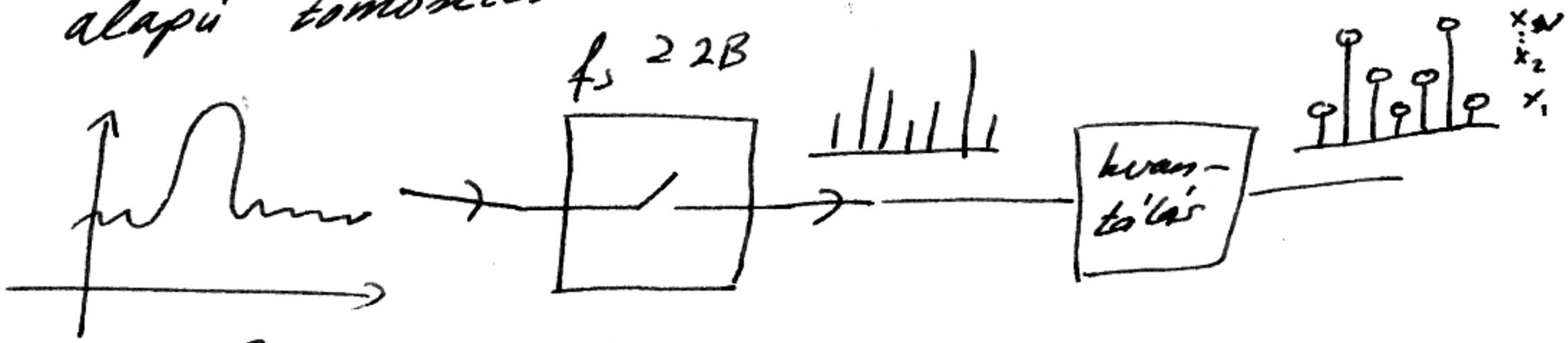
$O(\frac{1}{K})$ ⟺ $O(N^k)$

↓

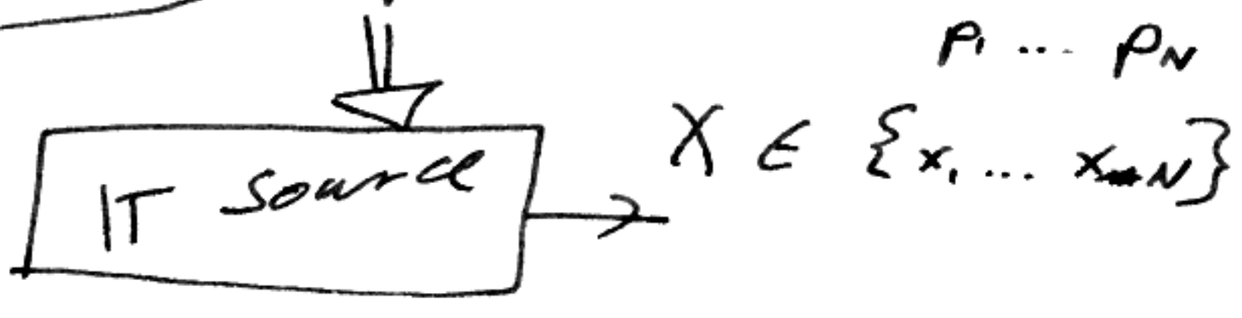
ma ez a
fontosabb,
mert erősek
a gépek és
keskenyek a
csatornák

10-10-28 Kodtech

Beszédtömörítő algoritmusok – kvantálás és korrelációra alapú tömörítés

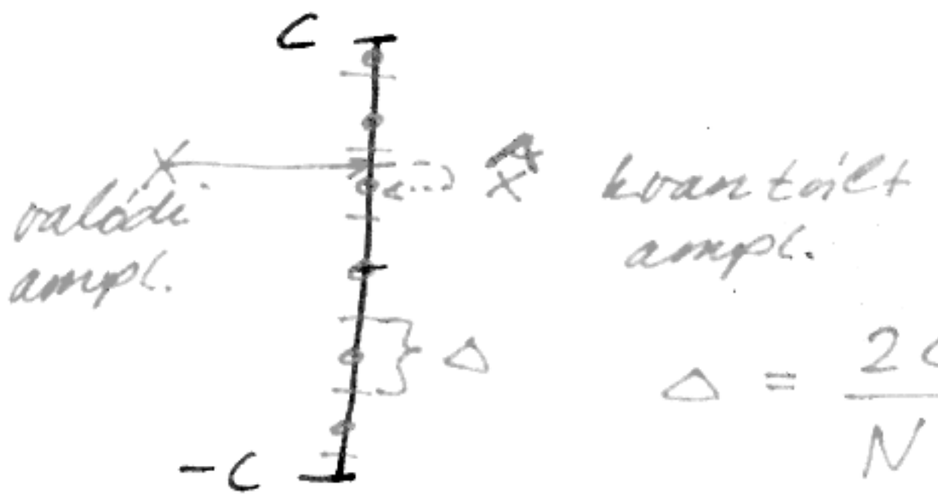


$$x(t) = \int_{-B}^{B} x(f)\, e^{+j\pi f t}\, df$$



Cél: optimális kvantálás

Egyenletes kvantálás



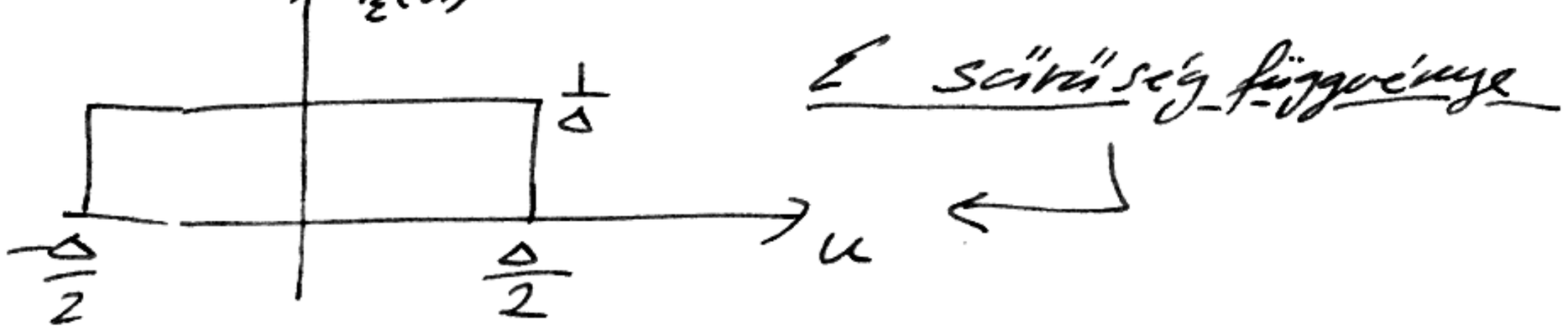
$$\Delta = \frac{2C}{N}; \quad N = 2^n; \quad \text{leggyakrabban: } N = 2^8$$

Kvantálási hiba:

$$\varepsilon := x - \hat{x} \in \left[-\frac{\Delta}{2}; \frac{\Delta}{2}\right]$$

↓

valószínűségi változó



ε sűrűségfüggvénye

QoS.: $SNR = \frac{\text{jelenergia}}{\text{zajenergia}} = \frac{C^2/2}{\Delta^2/12} = 6\frac{C^2}{\Delta^2} = \frac{6}{9}\cdot\frac{4C^2}{\Delta^2} = \frac{2}{3}N^2 = \frac{2}{3}2^{2n}$

Signal-to-Noise-Ratio

a minőség exponenciálisan függ a bitek számától

jelenergia:

$X \rightarrow$ szinusos jelből vett minta

$C^2/2$

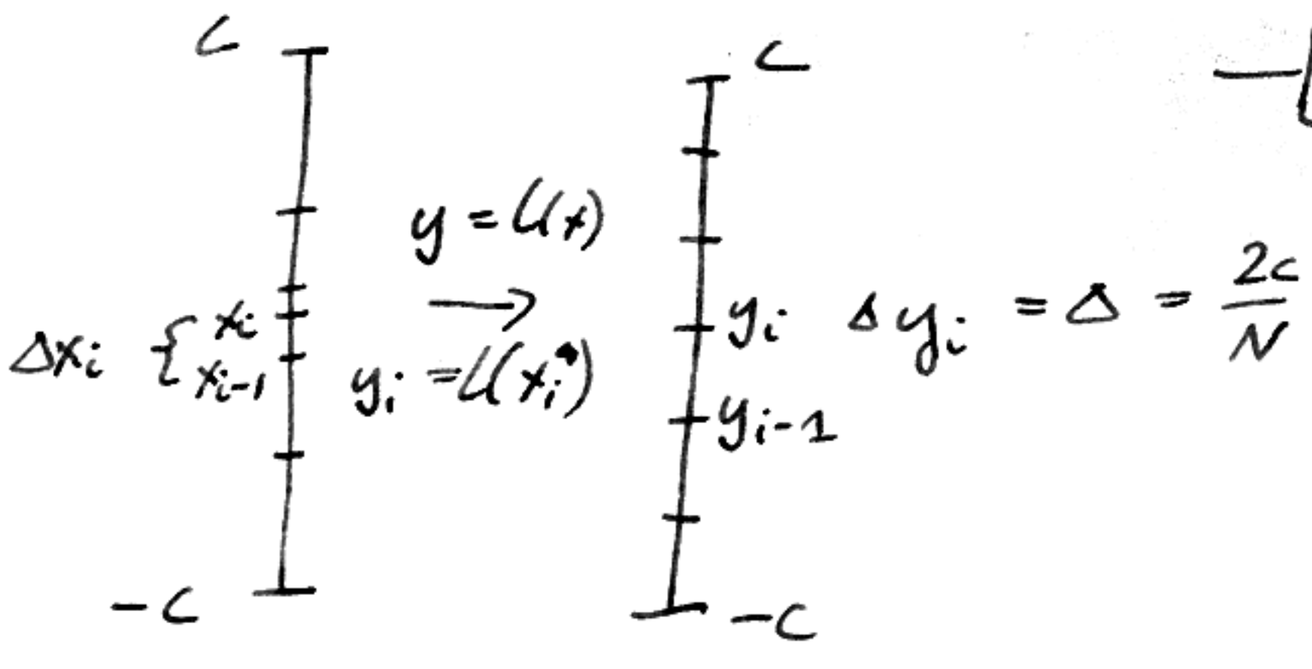
zajenergia: $\mathbb{E}(\varepsilon^2) = \int_{-\Delta/2}^{\Delta/2} u^2 p(u)\,du = \int_{-\Delta/2}^{\Delta/2} u^2 \frac{1}{\Delta}\,du = \frac{\Delta^2}{12}$

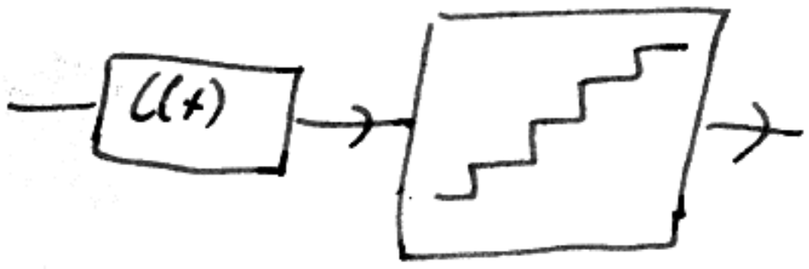
várható érték

Miért nem jó az egyenletes kvantálás?

$C' = C/2 \rightarrow SNR' = \frac{3}{2}\frac{4C'^2}{\Delta^2} = \frac{3}{2}\cdot\frac{4\cdot\frac{1}{4}C^2}{\Delta} = \frac{SNR}{2}$

egyenletes kvantálás





$\Delta x_i \sim \frac{\Delta}{L'(x_i)}$ $\Leftarrow$ $\frac{\Delta}{\Delta x_i} = \frac{\Delta y_i}{\Delta x_i} \approx L'(x_i)$

$SNR = \frac{\text{jelenergia}}{\text{zajenergia}} = \frac{\int_{-C}^{C} x^2 p(x)\,dx}{\frac{\Delta^2}{12}\int_{-C}^{C}\frac{1}{L'^2(x)}\cdot p(x)\,dx}$; $L_{opt}(x) = \max_{L(x)} \frac{\int_{-C}^{C} x^2 p(x)\,dx}{\int_{-C}^{C}\frac{1}{L'^2(x)}p(x)\,dx}$

ezt nem tudjuk kiszámolni, túl bonyolult, bár van rá iterációs algoritmus, de túl lassú

Jelenergia $= \mathbb{E}(X^2) = \int_{-C}^{C} x^2 p(x)\,dx$;

Zajenergia $= \sum_i \mathbb{E}(\varepsilon^2 / x \in \Delta x_i)\,P(x \in \Delta x_i) = \sum_i \frac{\Delta x_i^2}{12}\cdot p(x_i)\Delta x_i =$

$= \sum_i \frac{\Delta^2}{12}\cdot\frac{1}{L'^2(x_i)}\,p(x_i)\Delta x_i = \frac{\Delta^2}{12}\int_{-C}^{C}\frac{1}{L'^2(x)}\,p(x)\,dx$

10-10-28 Kodtech

Cél:

$$\frac{\int_{-c}^{c} x^2 p(x)\,dx}{\int_{-c}^{c} \frac{1}{l'^2(x)} p(x)\,dx} = const \Rightarrow \frac{1}{l'^2(x)} \sim x \rightarrow l'(x) \sim \frac{1}{x}$$

↑ l' vessző négyzet, nem l^{12}

$l(x) \sim \log(x)$

- "A" law — európa
- μ "Law" — USA, távolkelet

Korreláció alapú adattömörítés

Azon alapul, hogy a forrás nem memóriamentes

$$P(X(k)=x_i \mid x(k-1)=x_j \;\dots\; X(k0)=x_m) \neq P(X(k)=x_i)$$

a múlt számít → statisztikai értelemben meghatározza a jelent.

Pl.:

Kérek egy üveg sö –
- → rt ← nagy valószínűség
- → tét gépolajat ← kis valószínűség

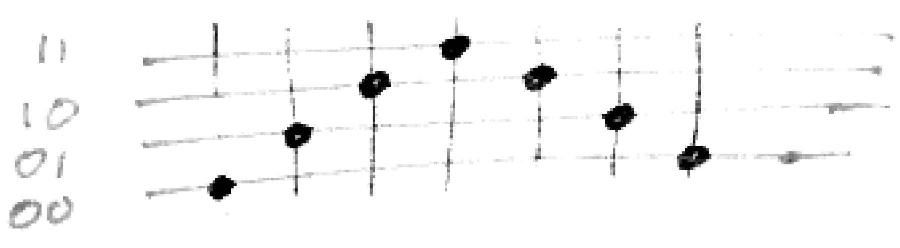
⇓

a hiba eloszlása távol van az egyenletestől

$$H(x) \gg H(\varepsilon)$$

↑ jel entrópiája, ↑ hiba entrópiája → erre jobb a kódot csinálni, elég a gyenge de gyors algoritmus is

Delta-modulátor



⇒ 00 01 10 11 10 01 00 → 14 bit

helyett: 1 – növekedés
0 – csökkenés

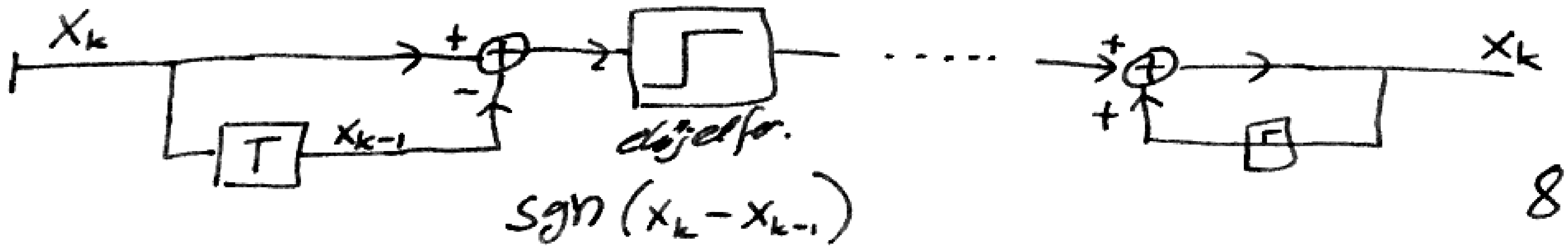
$R = n \cdot fs$

⇓

00 1 1 1 0 0 0 → 8 bit

első jel

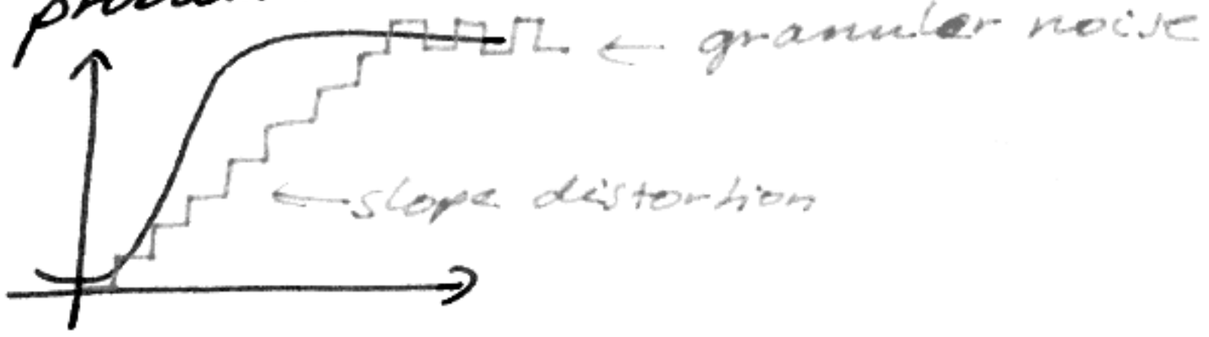
$R' = 1 \cdot fs$



$sgn(x_k - x_{k-1})$

8kbps < 64kbps

problémák:



megoldás:

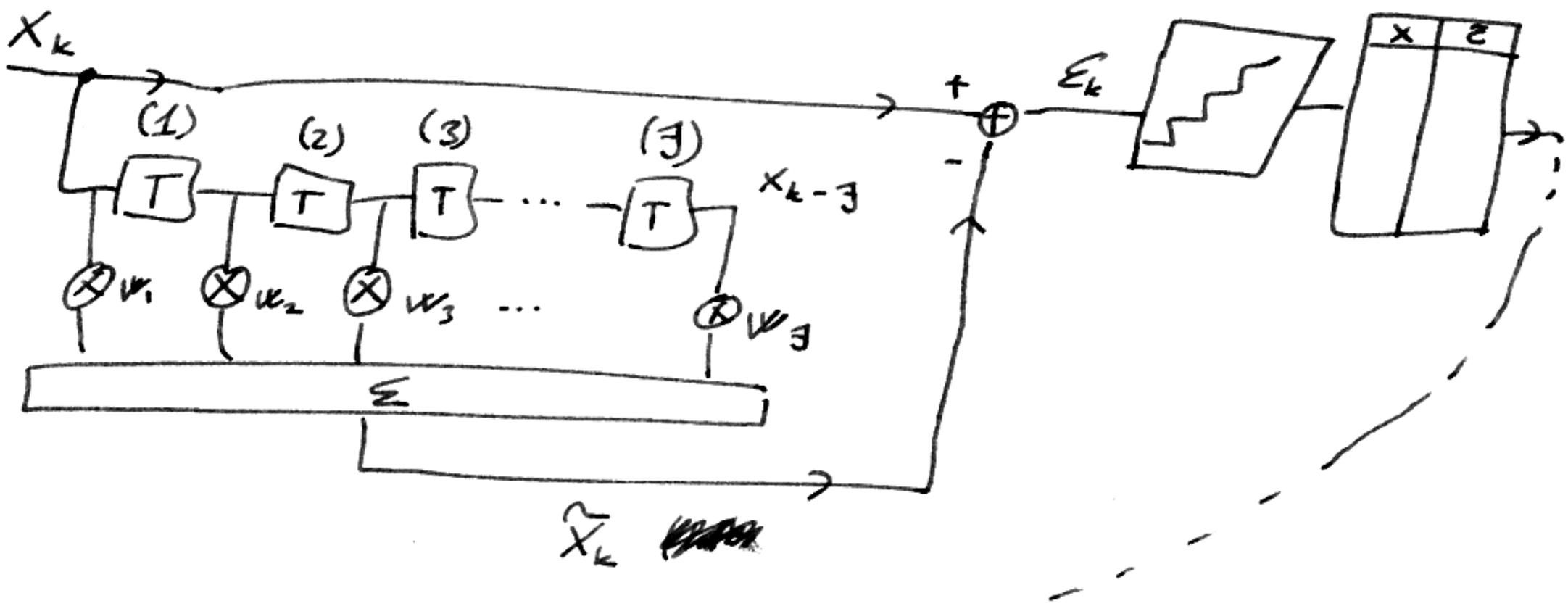
nagyobb mintavételi frekvencia (f_s')

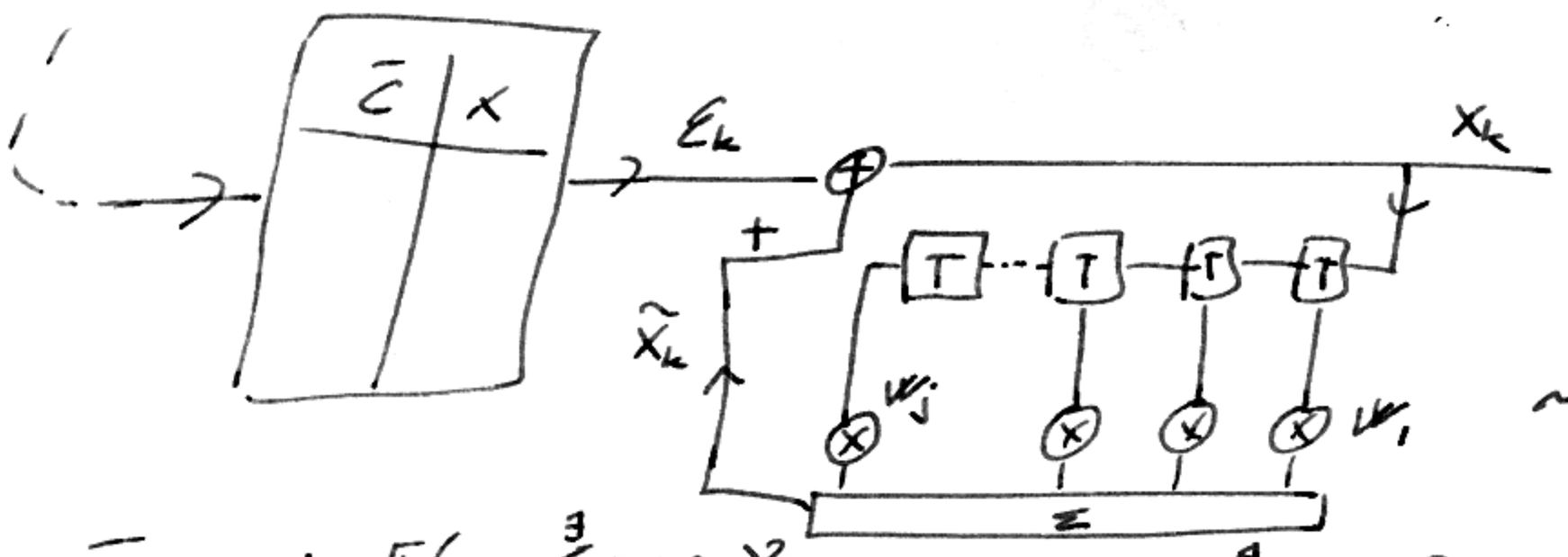
kérdés: $f_s' \overset{?}{<} f_s \cdot n$

$x_k \rightarrow$ keresd idősora ; $R(l) := \mathbb{E}(x_k \cdot x_{k-l})$;

$$\hat{x}_k = \sum_{j=1}^{N} w_j x_{k-j} \quad ; \quad \text{becslési hiba} \quad \varepsilon_k := x_k - \hat{x}_k$$

$$x_k = \varepsilon_k + \hat{x}_k$$





$$\bar{w}_{opt} : \min_{\bar{w}} \mathbb{E}(\varepsilon_k^2) \sim$$

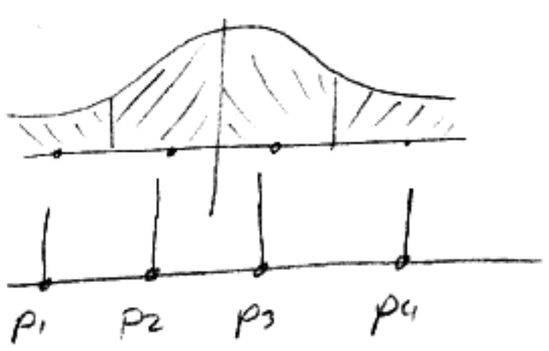
$$\sim \min_{\bar{w}} \mathbb{E}\left(x_k - \sum_{j=1}^{J} w_j x_{k-j}\right)^2$$

$$\bar{w}_{opt} : \min_{\bar{w}} \mathbb{E}\left(x_k - \sum_{j=1}^{J} w_j x_{k-j}\right)^2 ; \quad J(\bar{w}) := \mathbb{E}\left(x_k - \sum_{j=1}^{J} w_j x_{k-j}\right)^2 = \mathbb{E}(x_k^2) - 2\sum_{j=1}^{J} w_j \mathbb{E}(x_k x_{k-j}) +$$

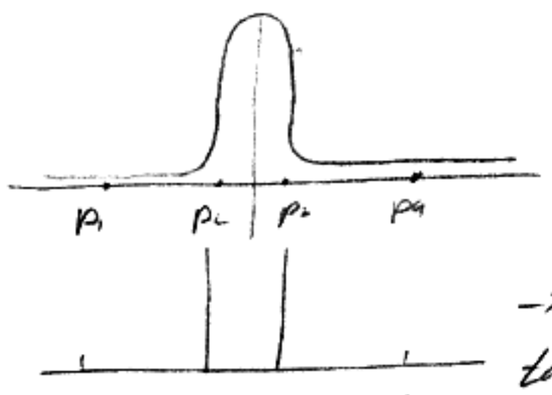
$$+ \sum_{i=1}^{J}\sum_{j=1}^{J} w_i w_j \mathbb{E}(x_{k-i} x_{k-j}) = \sum_{i=1}^{N}\sum_{j=1}^{N} w_i w_j R_{ij} - 2\sum_{j=1}^{N} w_j r_k + \mathbb{E}(x_k^2) = \bar{w}^T \bar{\bar{R}} \bar{w} - 2\bar{r}^T \bar{w} + \mathbb{E}(x_k^2)$$

$$J(\bar{w}_{opt}) = \mathbb{E}(x_k^2) - \bar{w}_{opt}^T \bar{\bar{R}} \bar{w}_{opt} \ll \mathbb{E}(x_k^2) \Rightarrow \mathbb{E}(\varepsilon_k^2) \ll \mathbb{E}(x_k^2)$$

$$\bar{w}_{opt} : \bar{\bar{R}} \bar{w} = \bar{r}$$



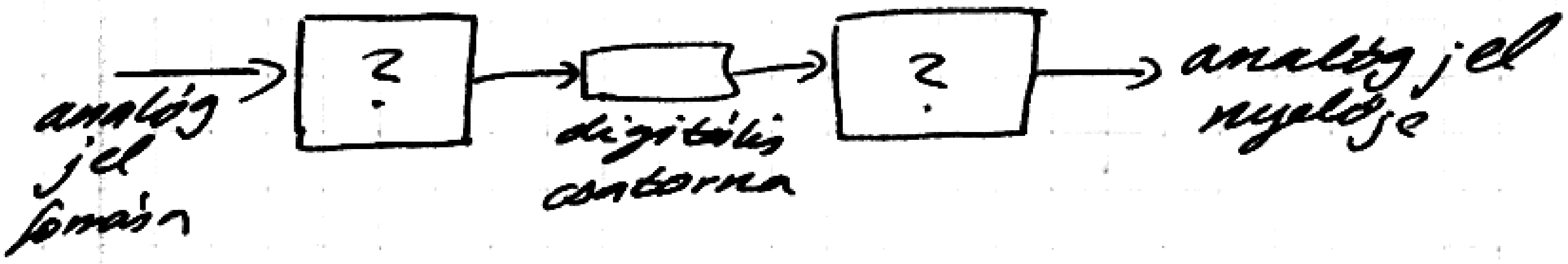
Eredeti minta



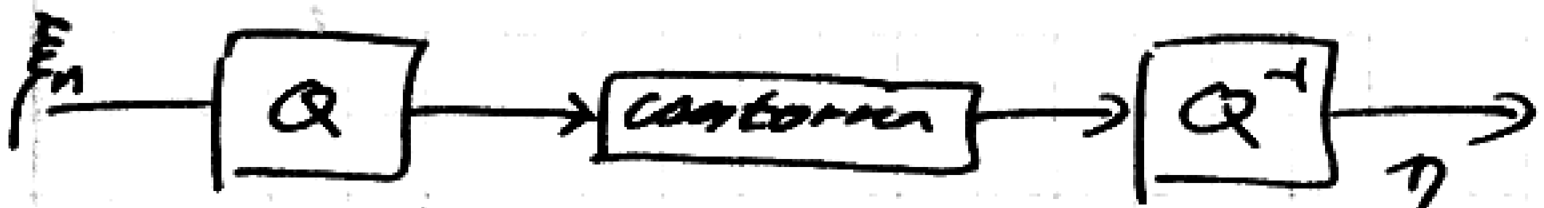
Predikciós minta → ez van távolabb az egyenletes eloszlástól

$$\Rightarrow H(x_k) \gg H(\varepsilon_k)$$

10-11-02 Kodtech



$F = \frac{1}{T}$



kvantáló:
mintavételezés
amplitúdó kv.
kódolás

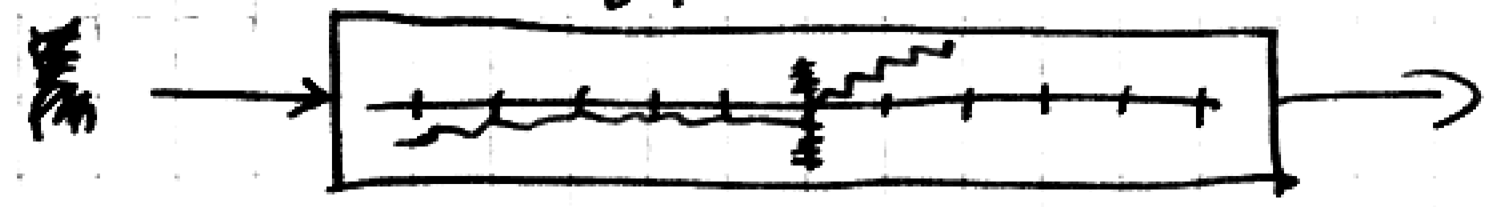
inverz kvantáló

$\eta_n = \xi_n + \varepsilon_n$

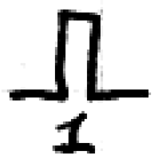
↑

kvantálási hiba; $\varepsilon_n = \eta_n - \xi_n$

forrás: kvantáló:



– egyenletes kvantáló q



Most legyen az egyszerűség érdekében:

$E\{\xi_n) = 0$

$P_\xi = E(\xi_n^2)$

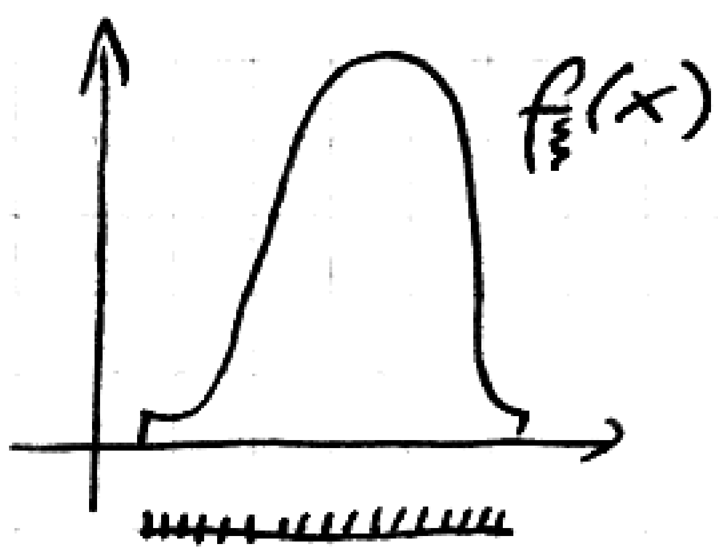
$P_\varepsilon = E(\varepsilon_n^2)$

$$SNR = \frac{P_\xi}{P_\varepsilon}$$

R bites kvantáló = R bites kódol

$I = F \cdot R$ bit/sec $(F = \frac{1}{T})$

$L = 2^R$

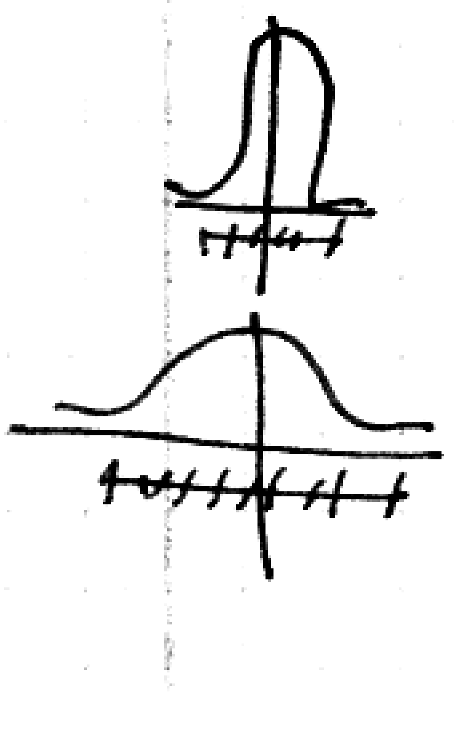


q

illesztett kvantáló

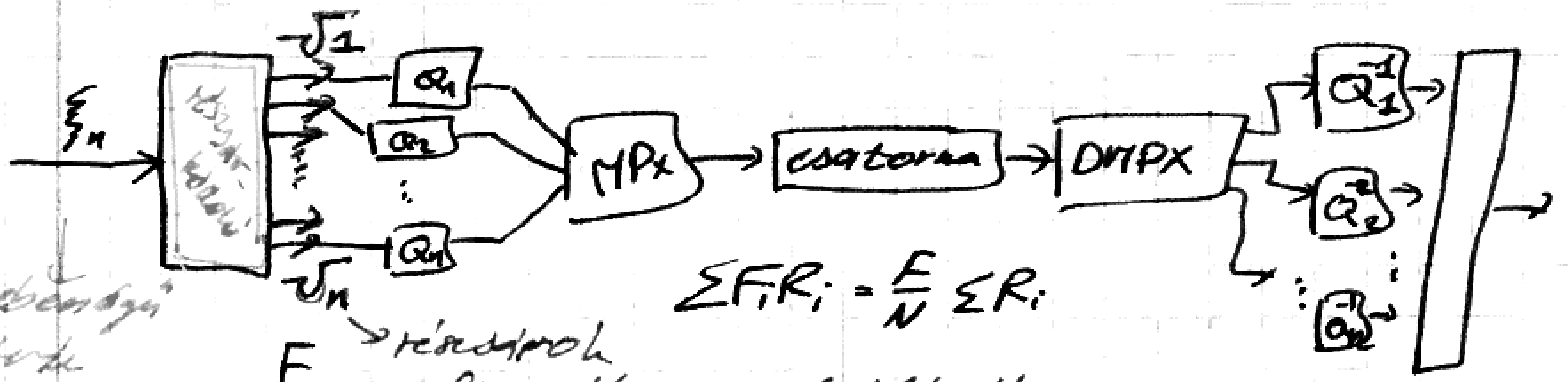
P_ξ

$$P_\varepsilon = c_n \cdot 2^{-2R} \cdot P_\xi$$



$SNR = c_2 \cdot 2^{2R}$ → 6 dB/bit

Részsávú kódoló:



$\sum F_i R_i = \frac{F}{N} \sum R_i$

nagysebességű aluláteresztő bemenet

v_n → részsávok független valószínűségi változók

$\frac{F}{n}$

↓

kisebb sebességű keskenysávú kimenet

szintézis szűrőbank | sávszűrő-szintézis

↓

újra kódolja amit a részsávkódoló munkáját

$P_\xi = \sum P_i$

$P_{\varepsilon_i} = c \cdot P_i \cdot 2^{-2R_i}$

$SNR_{SC} = \frac{P_\xi}{\sum_i P_{\varepsilon_i}}$

$FR = \frac{1}{N} F \sum R_i$

$NR = \sum R_i$

Kérdés:

adott N, R

keressük $R_1, R_2 \dots R_N$; max SNR_{SC}, $NR = \sum R_i$

⇕

$\min \sum_i P_{\varepsilon_i} = \min \sum c P_i 2^{-2R_i}$

$NR - \sum R_i = 0$

megoldás: $\frac{\partial}{\partial R_i} \left\{ \sum_i P_i 2^{-2R_i} + \lambda \cdot (NR - \sum R_i) \right\} = 0$

$i = 1 \dots N$

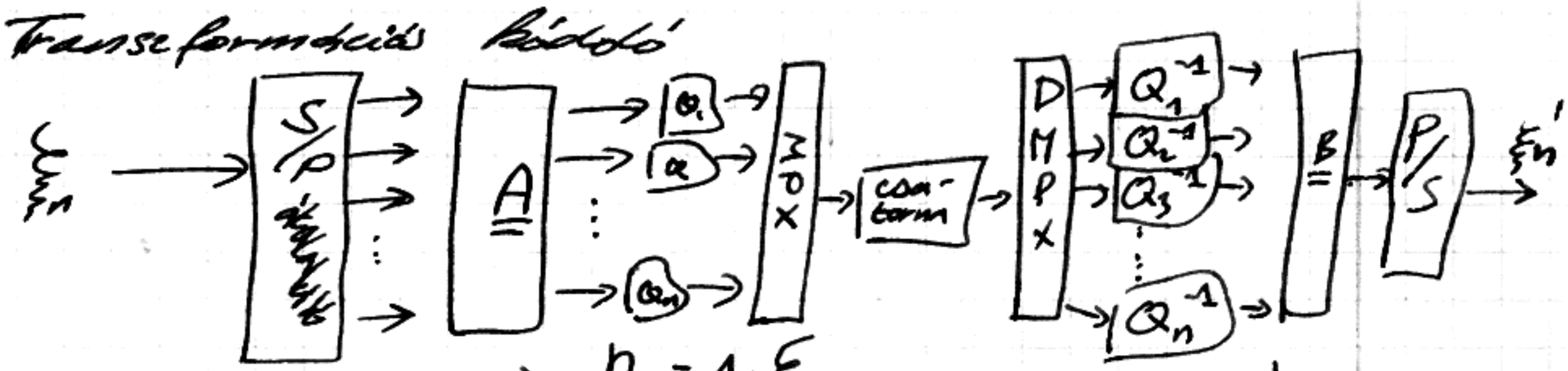
$R_i = R + \frac{1}{2} \mathrm{ld} \frac{P_i}{\sqrt[N]{\prod R_i}} \quad i = 1 \dots N$

$SNR_{SC} = \Big|_{R_i = R_{iopt} \text{ } i\text{-dik } N} = G_{SB} \cdot SNR_Q = \frac{\frac{1}{N} \sum R_i}{\sqrt[N]{\prod_i P_i}} \cdot c \cdot 2^{2R}$

$\frac{\text{számtani közép}}{\text{mértani közép}}$

10-11-02 Kortech

Transzformációs kódoló



$$\underline{\xi} = \begin{pmatrix} \xi_n \\ \xi_{n-1} \\ \vdots \\ \xi_1 \end{pmatrix} \qquad \underline{\eta} = \underline{\underline{A}} \cdot \underline{\xi}$$

$$\underline{\eta}' = \underline{\eta} + \underline{\xi}$$

$$\underline{\xi}' = \underline{\eta}' \underline{\underline{B}}$$

Aszimptotikusan, nagyon finom kvantálás:

$$\underline{\varepsilon} = \underline{0}$$

$$\underline{\eta}' = \underline{\eta}$$

$$\underline{\underline{B}} = \underline{\underline{A}}^{-1}$$

$$\underline{\xi}' = \underline{\eta}' \underline{\underline{B}}$$

$$\begin{matrix} \xi_1 \\ \xi_2 \\ \vdots \\ \xi_n \end{matrix} = \left| \begin{matrix} b_1 & b_2 & \dots & b_N \\ | & | & & | \\ | & | & & | \\ | & | & & | \end{matrix} \right| \begin{matrix} \eta_1 \\ \eta_2 \\ \vdots \\ \eta_N \end{matrix}$$

$$\underline{\xi} = \sum_{i=1}^{N} \eta_i b_i$$

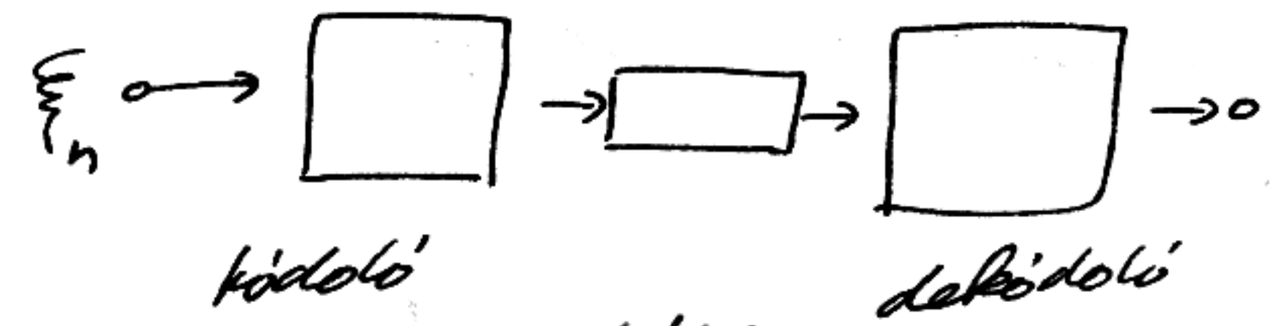
$$\underline{b}_i^T \cdot \underline{b}_\sigma = \delta_{i\sigma} = \begin{cases} 1 & \text{ha } i = j \\ 0 & \text{egyébként} \end{cases}$$

$$\underline{\underline{A}} = \underline{\underline{B}}^{-1}$$

$\underline{\underline{B}} \cdot \underline{\underline{B}}^T =$ egységmátrix

- 10-11-04 Kodtech

Veszteséges kódolás / digitális csatorna analóg forrás



F

<u>Sima kvantálás:</u>

$\varepsilon_n = \eta_n - \xi_n$

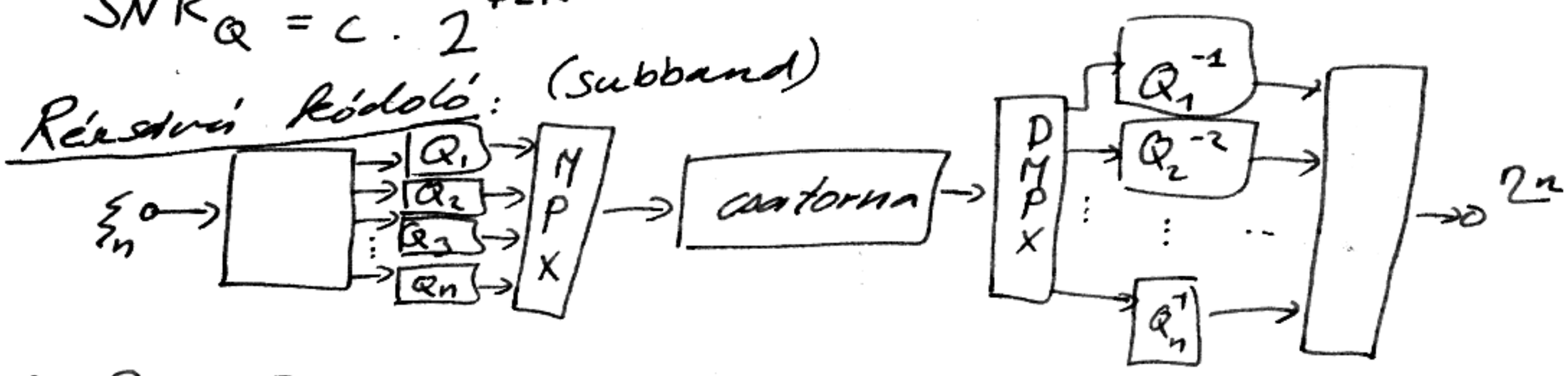
$P_\varepsilon = \mathbb{E}\{\varepsilon_n^2\} = c \cdot P_\xi \cdot 2^{-2R}$

$P_\xi = \mathbb{E}(\xi_n^2)$

$$SNR = \frac{P_\xi}{P_\varepsilon}$$

$SNR_Q = c \cdot 2^{+2R}$

<u>Résztvevő kódoló:</u> (subband)



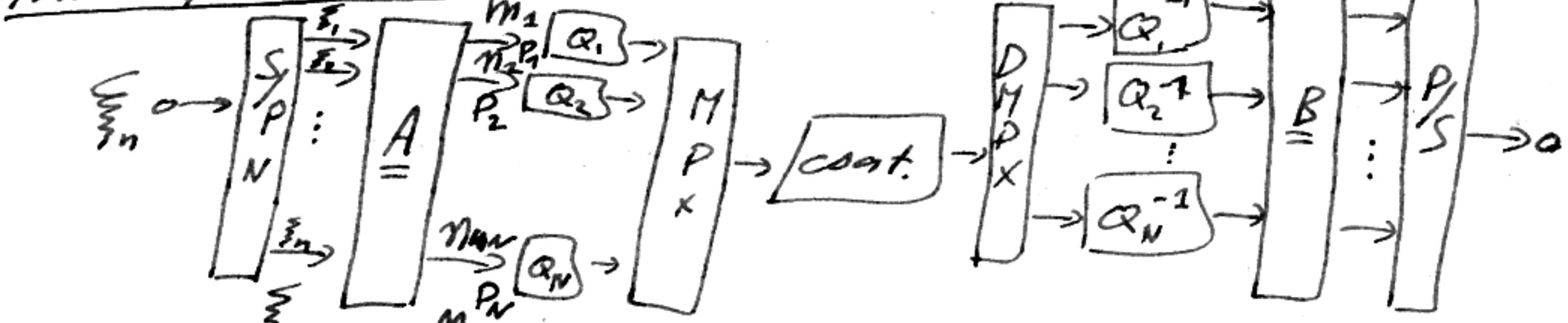
$SNR_{sc} = G_{SB} \cdot SNR_Q$

$$G_{SB} = \frac{\frac{1}{N}\sum P_i}{\sqrt[N]{\prod P_i}} \geq 1$$

(szimtani - mértani közép közti egyenlőtlenség miatt)

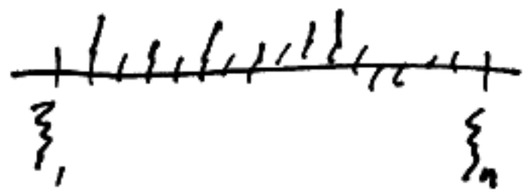
$$R_i = R + \frac{1}{2} ld \frac{\lambda_i}{\sqrt[N]{\prod P_i}}$$

<u>Transzformációs kódolás:</u>



$\underline{\eta} = \underline{\underline{A}} \cdot \underline{\xi}$; $\underline{\underline{B}} = \underline{\underline{A}}^{-1}$; $\underline{\underline{B}} = [\underline{b}_1 \underline{b}_2 \cdots \underline{b}_N]$ $\underline{\xi}' = \sum_i \eta_i' \underline{b}_i$

$\underline{\underline{B}}^{-1} = \underline{\underline{B}}^T = \underline{\underline{A}}$



Optimális transzformációs kódoló $\quad \underline{\eta} = \underline{\underline{A}} \cdot \underline{\xi}$

- az ortogonális transzformáció jó megtartja
- normatartó

$$\sum \underline{\xi} = \sum \underline{\eta}$$

$$MAX : SNR_{TC} \iff \min : \prod P_i$$

$$P_i = \mathbb{E}(\eta_i^2)$$

$$\underline{\underline{R}}_{\eta} = \mathbb{E}(\underline{\eta} \cdot \underline{\eta}^T) = \left[\tau(i-j) \right]$$

$$\begin{pmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \vdots \\ \eta_N \end{pmatrix} (\eta_1\ \eta_2 \dots \eta_N) = \begin{pmatrix} \eta_1\eta_1 & \eta_1\eta_2 & \eta_1\eta_3 & \dots & \eta_1\eta_N \\ \eta_2\eta_1 & \ddots & & & \vdots \\ \eta_3\eta_1 & & \ddots & & \vdots \\ \vdots & & & \ddots & \vdots \\ \eta_N\eta_1 & \dots & \dots & \dots & \end{pmatrix}$$

valószínűségi változók mátrixa

a várható értékük ugyanilyen

def $\quad E(\eta_i \cdot \eta_{i+n}) = \tau_{\eta}(n)$

$$E(\eta_i \cdot \eta_i) = \tau_{\eta}(0) = P_i$$

$$\underline{\underline{R}}_{\eta} = \mathbb{E}(\underline{\underline{A}}\,\underline{\xi} \cdot \underline{\xi}^T \cdot \underline{\underline{A}}^T) = \underline{\underline{A}} \cdot \mathbb{E}(\underline{\xi} \cdot \underline{\xi}^T) \cdot \underline{\underline{A}}^T$$

$$\underline{\underline{R}}_{\eta} = \underline{\underline{A}} \cdot \underline{\underline{R}}_{\xi} \cdot \underline{\underline{A}}^T$$

$$\det(\underline{\underline{R}}_{\eta}) = \det(\underline{\underline{R}}_{\xi})$$

$$\prod_i P_i = \prod_i \underline{\underline{R}}_{\xi}^{r}(i,i) \geq \det(\underline{\underline{R}}_{\eta})$$

$$\underline{\underline{C}} \cdot \underline{l}_i = \lambda_i \cdot \underline{l}_i \qquad i = 1, 2 \dots N$$

$$\underline{\underline{C}}\,[\underline{l}_1\ \underline{l}_2 \dots \underline{l}_N] = [\underline{l}_1\ \underline{l}_2 \dots \underline{l}_N] \begin{bmatrix} \lambda_1 & & \emptyset \\ & \lambda_2 & \\ \emptyset & & \ddots \\ & & & \lambda_N \end{bmatrix}$$

$$\underline{\underline{C}}\,\underline{\underline{L}} = \underline{\underline{L}} \cdot \underline{\underline{D}}$$

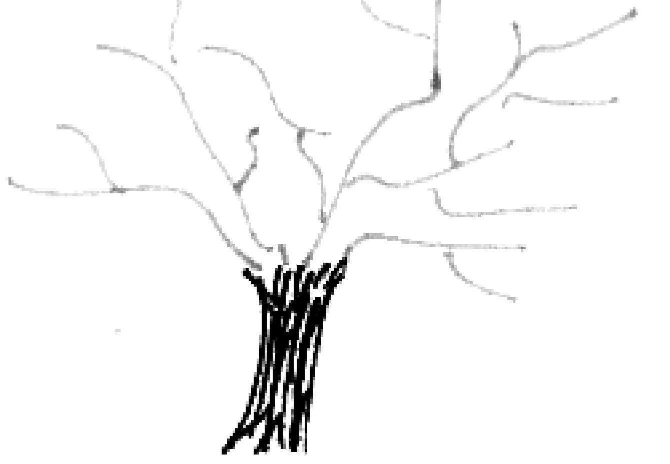
$$\underline{\underline{C}} = \underline{\underline{L}}\,\underline{\underline{D}}\,\underline{\underline{L}}^{-1} \rightarrow \text{diagonizálható} : \quad \underline{\underline{D}} = \underline{\underline{L}}^{-1}\,\underline{\underline{C}}\,\underline{\underline{L}}$$

10-11-09 Kodtech

ha $\underline{\underline{R}}_\eta = \underline{\underline{A}}\,\underline{\underline{R}}_\xi\,\underline{\underline{A}}^t$

$$\underline{\underline{R}}_\eta = \underline{\underline{B}}^T \cdot \underline{\underline{R}}_\xi \cdot \underline{\underline{B}}$$

ha $\underline{\underline{B}} = |\underline{L}_1 \underline{L}_2 \dots \underline{L}_N|$ $\underline{L}_i$ az $\underline{\underline{R}}_\xi$ i-edik sora



KLT (Karhunen-Loeve transzformáció)

→ elvi határ, legjobb

Szuboptimális kódolók

FFT

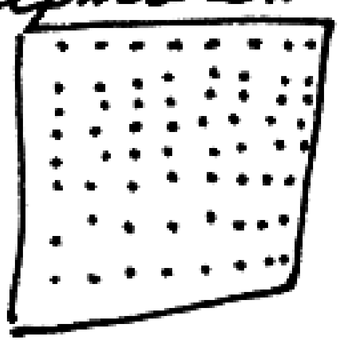
DCT (diszkrét cosinus transzformáció)

WHT

$$\frac{1}{9}\begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

Többdimenziós forrás

képmodell:



raszterezve már, nem folytonos egyszínű

8×8 $\xi(i,j)$

$\underline{\underline{\eta}} = \underline{\underline{A}}_V \cdot \underline{\underline{\xi}} \cdot \underline{\underline{A}}_H$ $\eta(k,l) = \sum_i \sum_j a(i,k,j,l)\,\xi(i,j)$

négydimenziósan indexelt együttható

dupla Σ (i és j szerint)

$\underline{\underline{\eta}} = \underline{\underline{A}} \cdot \underline{\underline{\xi}} \cdot \underline{\underline{A}}^T$

$$a(i,k,j,l) = a_v(i,k) \cdot a_h(j,l)$$

→ ha ez így felírható, akkor a kétdimenziós leképezés két egydimenziós egymásutánja

$$\underline{\underline{\xi}}' = \underline{\underline{A}}^t \cdot \underline{\underline{\eta}}' \cdot \underline{\underline{A}} = \sum_i \sum_j \eta'_{i,j} \cdot \underline{\underline{B}}_{ij}$$

$$\underline{\underline{B}}_{i,j} = \underline{b}_i \cdot \underline{b}_j^t$$

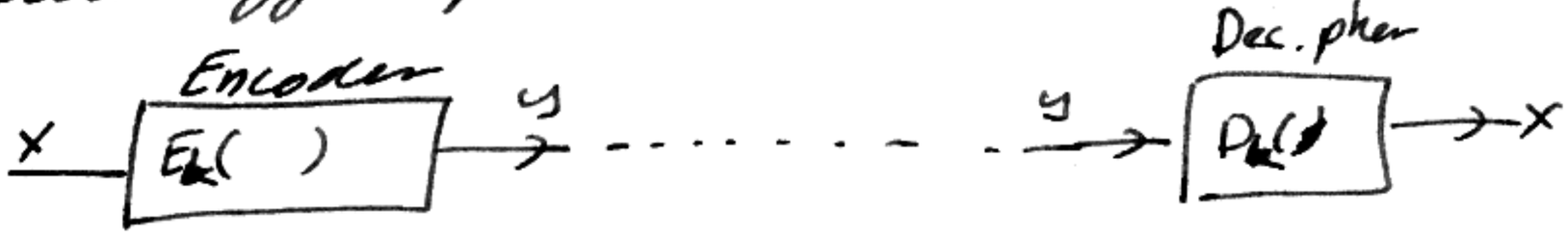
JPEG

8×8-as blokkok → [DCT] → [kvantálás] → [cikk-cakk letapogatás futamhossz-kód] → [Huffman] →

10-11-09 Kodtech

Titkosítás
Kriptográfia

Cél: nem nyilvános (privát) információk átvitele előírt biztonsággal publikus csatornán



$y = E_k(x)$

$x = D_k(y)$

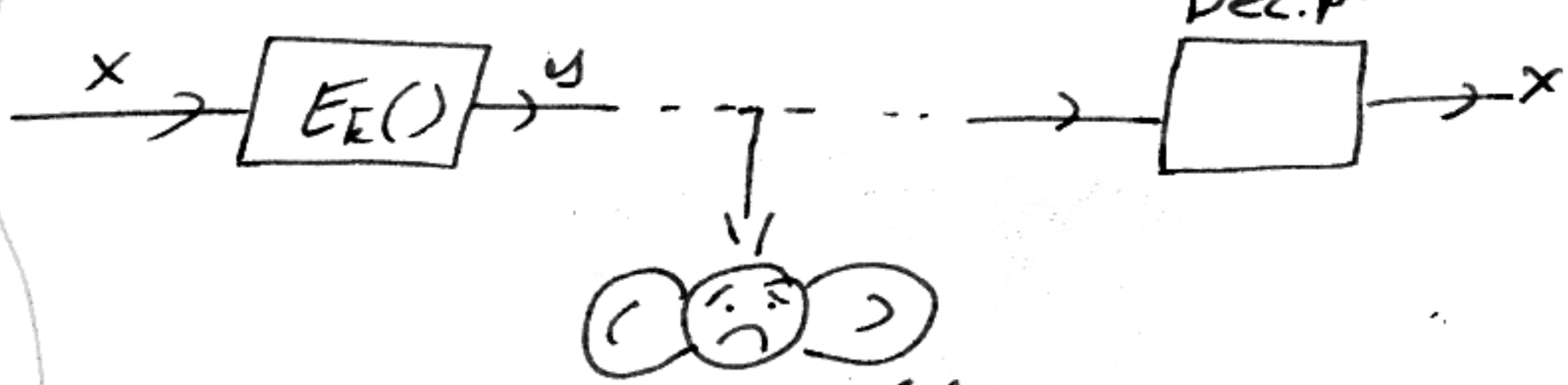
Alapfilozófia:

$E(\ )$; $D(\ )$ ismert

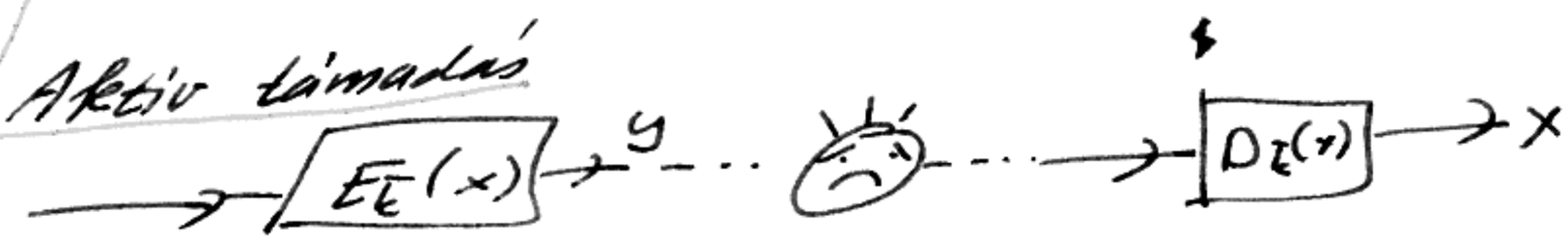
$\bar{k}$ nem ismert

$y = E_{\bar{k}}(x) \longrightarrow \bar{k}$ birányában nehezen megfordítható

Passzív támadás



Aktív támadás



Fajtái:
- Zárt szövegű (csak y-t látja)
- nyílt szövegű (x-ek-y párokat lát)
- választott nyílt-zárt szövegű (ő generál x-t is)

Tradicionális módszerek:

$\equiv y_i \oplus k_i = y_i$

$\equiv$ permutációs módszer: $x_1 x_2 \dots x_L \mapsto x_{i_1} x_{i_2} \dots x_{i_L}$

$x_{L+1} x_{L+2} \dots x_{2L} \mapsto x_{i_{L+1}} x_{i_{L+2}} \dots x_{i_{2L}}$

permutációs tábla

1	2	…	L
i_1	i_2	….	i_L

→ probléma: a kulcsnak mindkét oldalon ott kell lennie, azt is sit kell cserélni

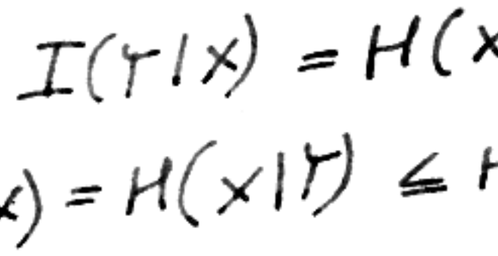
$\equiv$ OTP (One Time Pad)

$\bar{k} = (k_1, \dots k_N)$ N db üzenethossz

random sorsolva, Bernoulli eloszlás

$y_i = x_i \oplus k_i, \quad i = 1 \dots N$

$Y = X + K, \quad I(X,Y) = \emptyset$ → olyan, mint egy $\emptyset$ kapacitású csatorna



Biz:

$P(Y|X) = P(K = Y - X) = \frac{1}{2^N}$

$P(Y) = \sum_x P(Y|x) P(x)$

$\sum_x \frac{1}{2^N} P(X) = \frac{1}{2^N} \sum_x P(x) = \frac{1}{2^N}$

$P(Y) = P(Y|x)$ → x, Y függetlenek

$H(X) \overset{?}{\leq} H(K)$ Biz:

$\emptyset = I(Y|X) = H(x) - H(X|Y) \rightarrow H(X) = H(X|Y)$

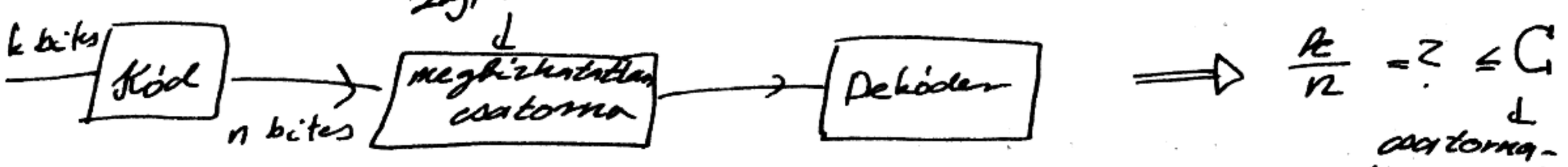
$H(x) = H(x|Y) \leq H(x, K|Y) = H(X|K,Y) + H(K,Y) \leq H(K)$

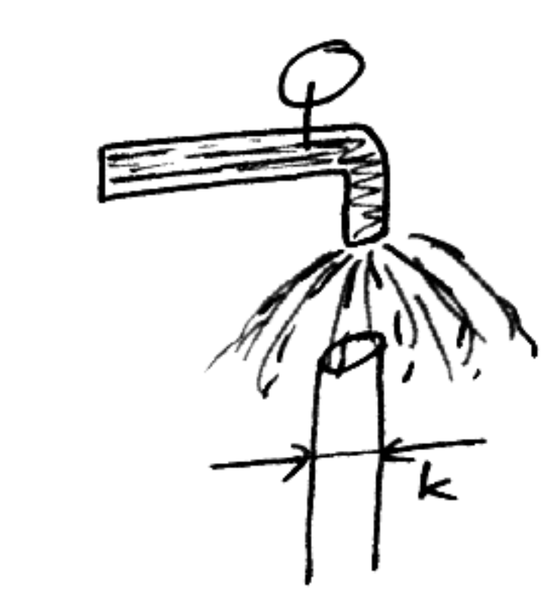
$H(X) \leq H(K)$

10-11-09 Kodtech

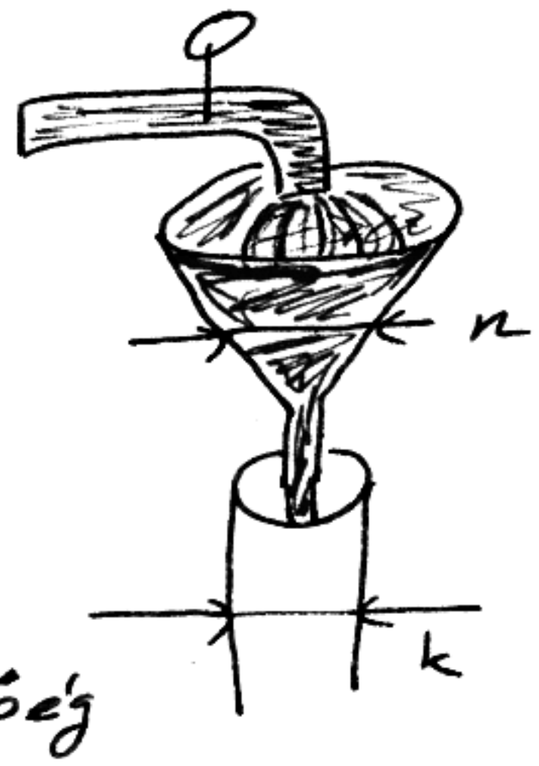
Adattömörítés: információ hatékony tárolása és továbbítása

Hatékony kommunikáció: hogyan lehet megbízhatatlan csatornán is megbízhatóan kommunikálni?





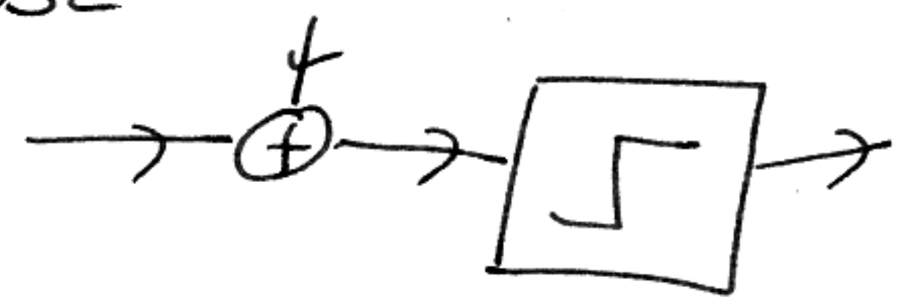
vízcsap
sok vízveszteség



$\frac{k}{n}$

→ tölcsér → vízveszteség nincs, helyette időveszteség

BSC - bináris szimmetrikus csatorna

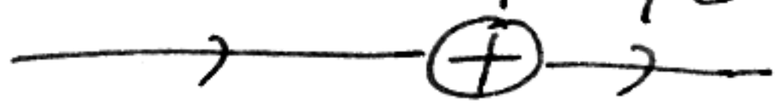


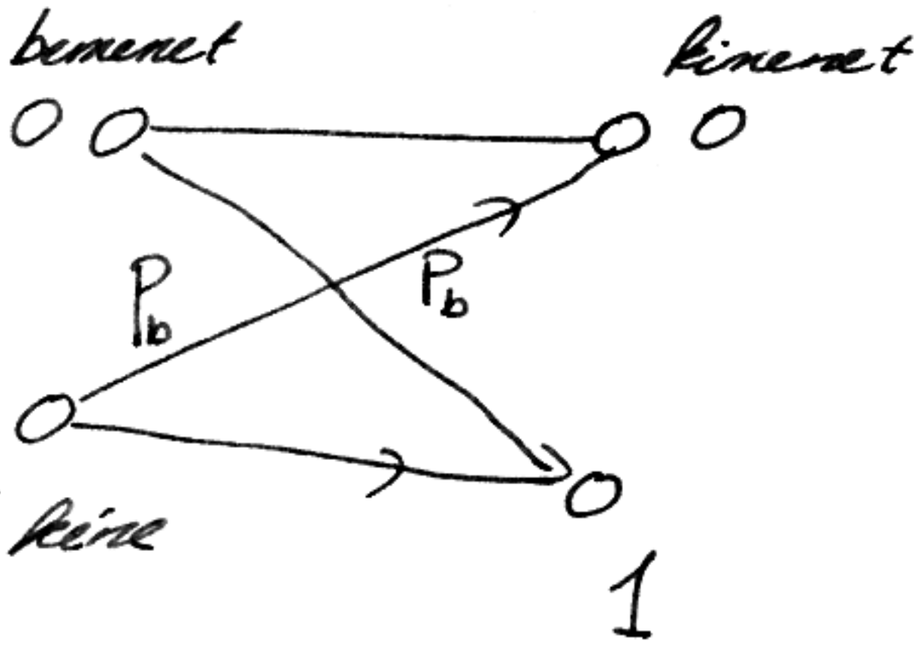
$P_b = \Phi\left(-\sqrt{SNR}\right)$

$SNR = \frac{1}{N_0}$

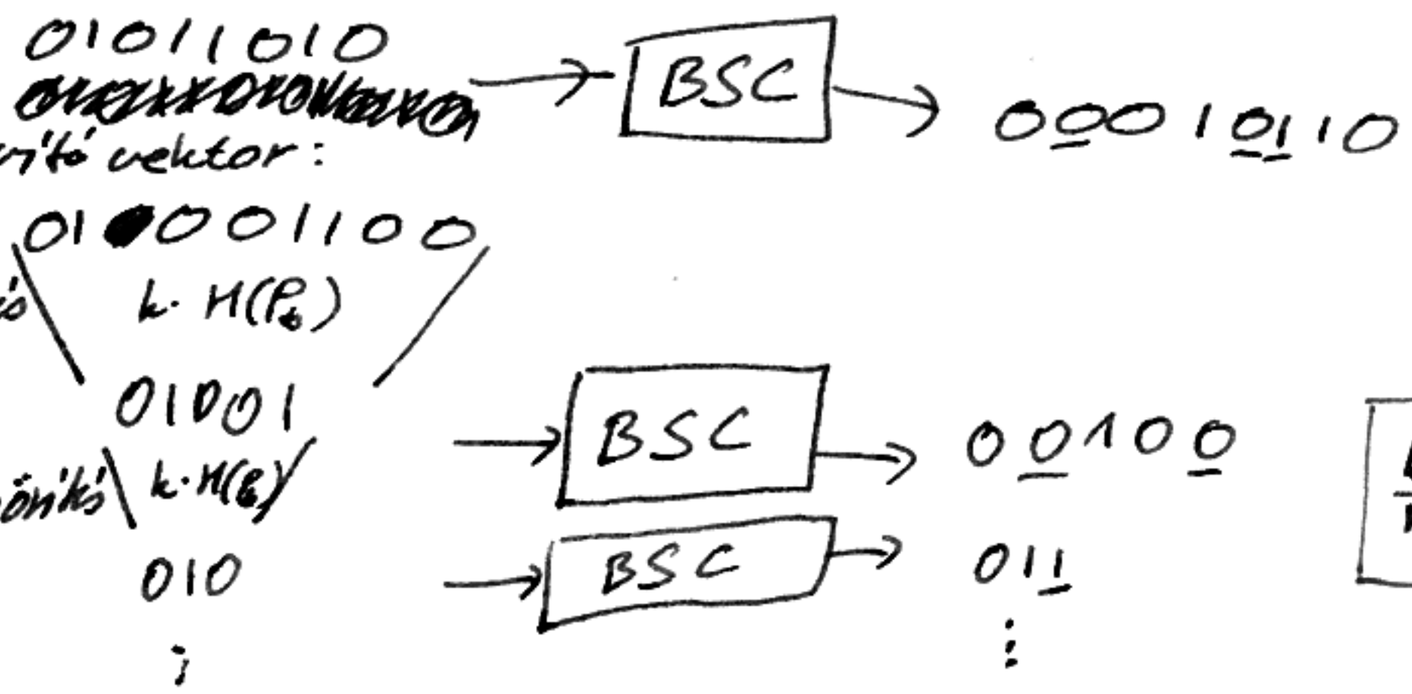
bithiba-valószínűség

$X \in \{0,1\}$ $+^k$ $Y \in \{0,1\}$





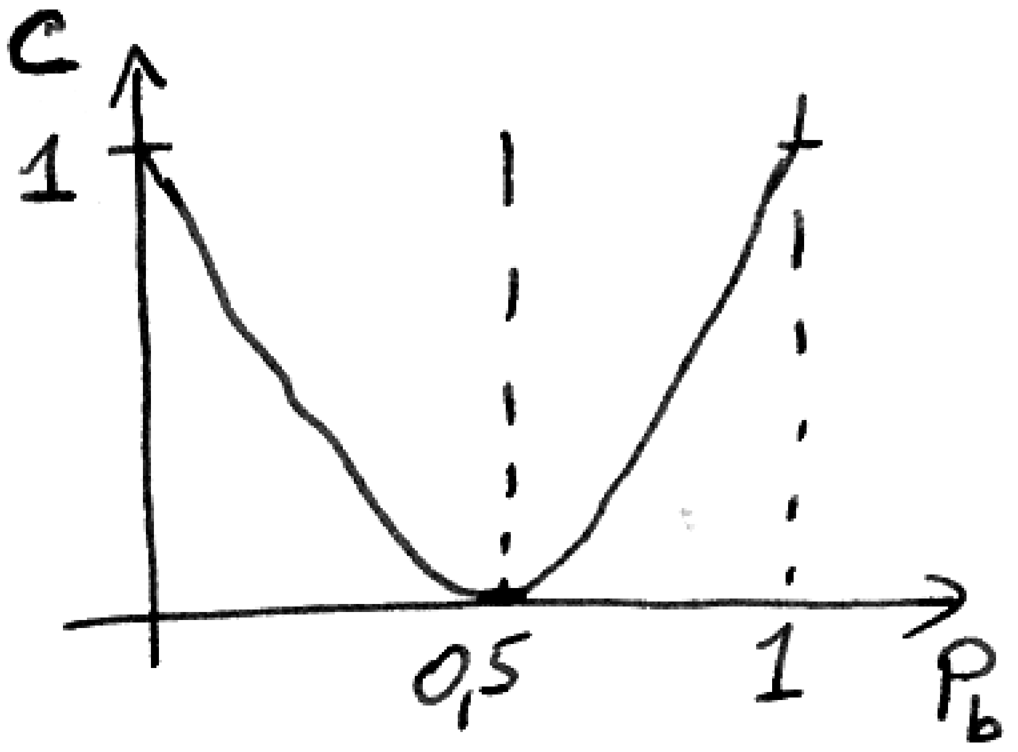
⇒ hibamentes átvitel lehet



$n = k + kH(P_b) + kH^2(P_b) + \ldots$

$n = k \sum_{i=0}^{\infty} H^i(P_b) = k \frac{1}{1 - H(P_b)}$

$\boxed{\frac{k}{n} = C = 1 - H(P_b)}$



$$G = \max_{p(x)} I(x,y) = \max_{p(x)} H(Y) - H(Y|X) = \max_{p(x)} H(X) - H(X|Y)$$

együttes eloszlás

$$I(x,y) = D\left(p(x,y) \| p(x)p(y)\right) = \sum_x \sum_y p(x,y) \, ld \frac{p(x,y)}{p(x)p(y)}$$

$$H(Y) = \sum_y p(y) \, ld \frac{1}{p(y)}$$

$$H(Y|X) = \sum_x p(x) \sum_y p(y|x) \, ld \frac{1}{p(y|x)}$$

Kihatás a spektrális kihasználtságra

A kommunikációs mérnökség alapjai

mi a kapcsolat?

Be: erőforrások
- adóteljesítmény ($\Leftrightarrow$ jel-zaj viszony) SNR
  korlátozott
- sávszélesség (megvásárolt rádióspektrum) B
  drága

Ki: célok – QoS:
- bithiba-valószínűség (P_b)
- R (sávszélesség)

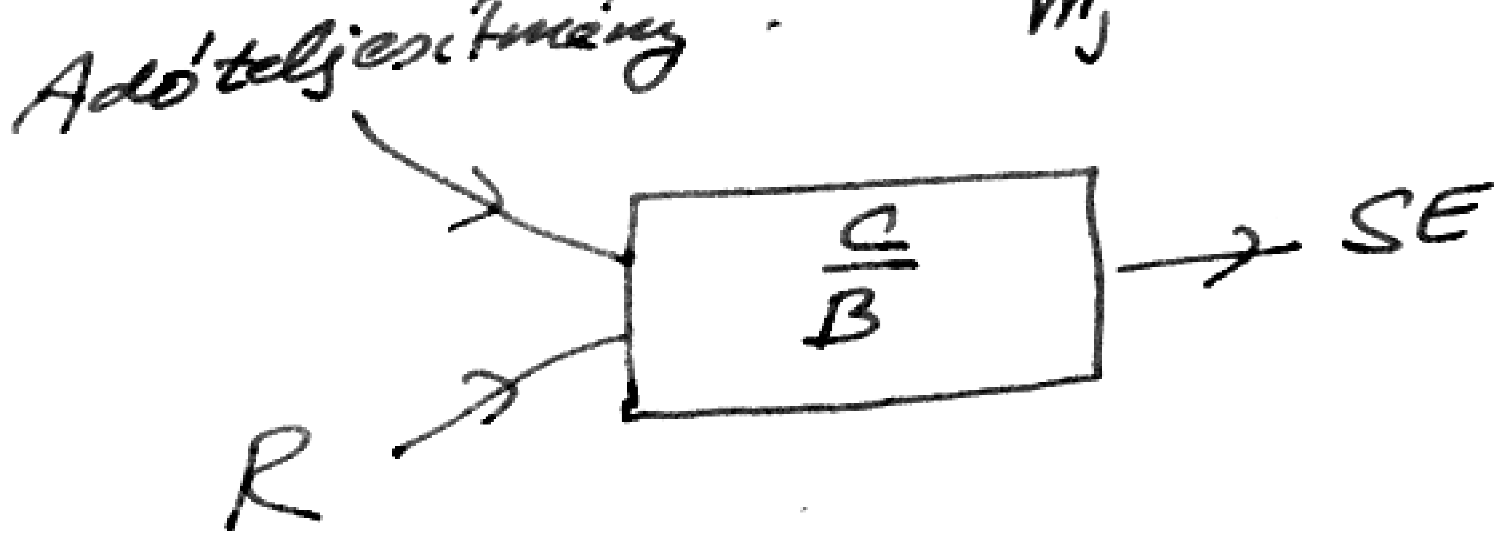
} SE
Spectral Efficiency
[bit/sec/Hz] $\approx \frac{C}{B}$

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

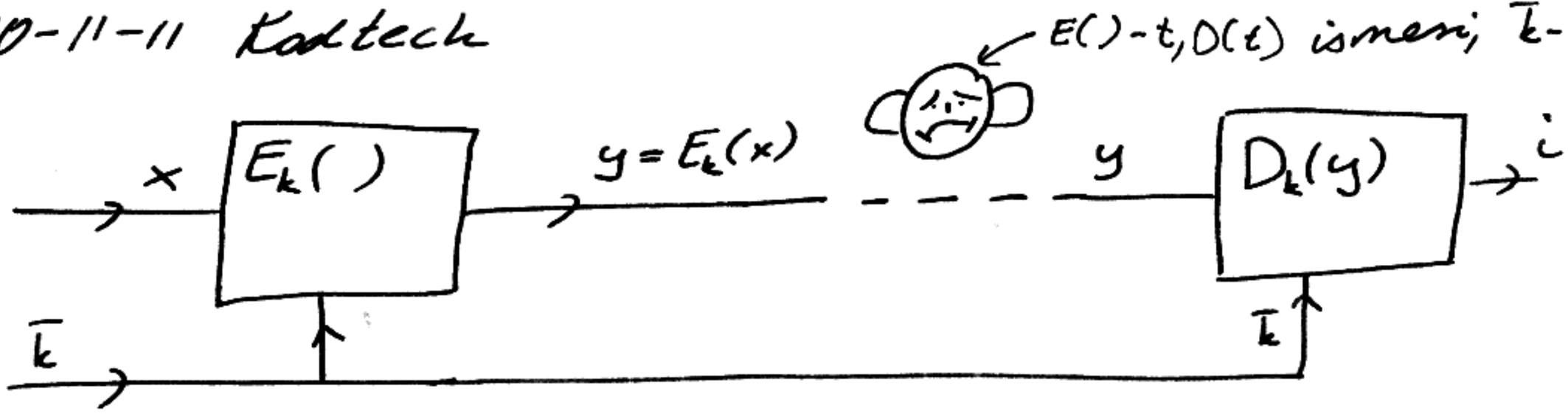
$$R \sim B \cdot m_j$$

↓ rádióspektrum

$$SE = \frac{1 - \Phi(-\sqrt{SNR}) \, ld \frac{1}{\Phi(-\sqrt{SNR})} - \left(1 - \Phi(-\sqrt{SNR})\right) ld \frac{1}{1-\Phi(-\sqrt{SNR})}}{\frac{1}{m_j} R}$$



- 10-11-11 Kalltech



- $y_i = x_i \oplus k_i \mod(25), \quad i = 1 \dots N$

  25^N

  $x_i = y_i \ominus k_i \mod 25$

- 1 2 3 9
  3 2 9 1

  $L!$

x_1	x_2	...	x_L
1	2	...	L
i_1	i_2	...	i_L
x_{i_1}	x_{i_2}	x_{i_3}	x_{i_L}

permutációs tábla

- OTP

  $x_i \in \{0,1\} \qquad k_i \in \{0,1\}$

  $y_i \in = x_i \oplus k_i \qquad x_i = y_i \oplus k_i$

  $I(x, Y) = \emptyset$

Probléma: az adó és a vevő is ugyanazt a kulcsot használja

Kommutatív kulcsú titkosítás:
3x átvitel, de nincs kicserélés

$A \longrightarrow B$

$x \longrightarrow y_A = E_{k_A}(x) \overset{csat.}{\Longrightarrow} y_A \to y_{AB} = E_{k_B}(y_A) \overset{csat}{\Longrightarrow} y_{AB} \to y_B = D_{k_A}(y_{AB}) \Longrightarrow$

$E_{k_B}(E_{k_A}(x)) \qquad D_{k_A}\left(E_{k_B}\left(E_{k_A}(x)\right)\right) = E_{k_B}(x)$

kommutatívitás kell, hogy ezek felcserélhetők legyenek

$\overset{csat}{\Longrightarrow} y_B \to D_{k_B}(y_B) = D_{k_B}\left(E_{k_B}(x)\right) = x$

kommutatív kódolási módnerek:

I. Pk. $\bar{y}_A = \bar{x} \oplus \bar{k}_A$
$\bar{y}_{BA} = \bar{x} \oplus \bar{k}_A \oplus \bar{k}_B$
$\bar{y}_B = \bar{x} \oplus \bar{k}_B$
} megjelennek a contextusban

probléma: $\underbrace{\bar{y}_A \oplus \bar{y}_B \oplus \bar{y}_{BA}}_{\text{megfigyelheti a támadó}} = \bar{x}$

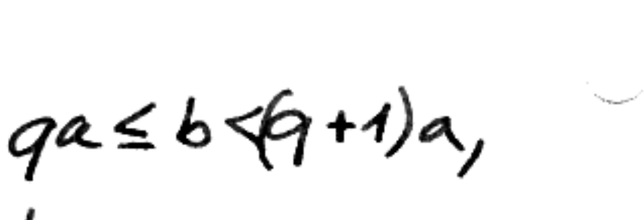
II. $(x^{k_A})^{k_B} = (x^{k_B})^{k_A}$ ez jobb

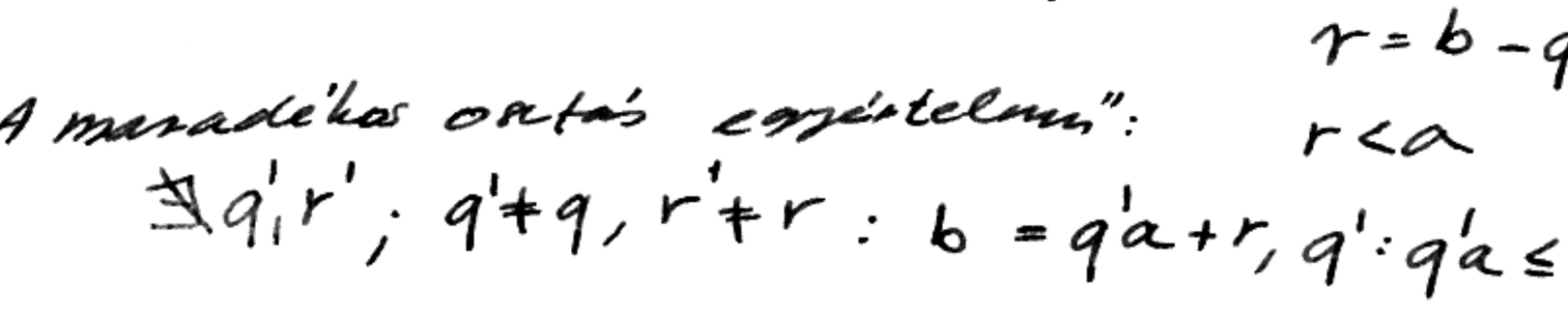
Nyilvános kulcsú titkosítás

A felkanmáló: $k_p^{(A)}$, $k_s^{(A)}$

k_p ↓ nyilvános kulcs
k_s ↓ titkos kulcs

Nyilvános kulcsok: $k_{p1}^{(A)}, k_p^{(B)}, \ldots, k_p^{(Z)}$





$D_{k_p^{(A)}}(y)$ nagyon nehéz függvény, gyakorlatilag lehetetlen megtalálni

Számelméleti összefoglalás:

Maradékos osztás:

$k > a > 0 \rightarrow \exists q, r : b = qa + r$, $q: qa \le b < (q+1)a$,
$r = b - qa$
$r < a$

A maradékos osztás egyértelmű":

$\exists q', r'$; $q' \neq q, r' \neq r : b = q'a + r$, $q': q'a \le b < (q'+1)a$,
$r' = b - q'a$
$r' < a$

Közös osztó:

$x | a \Leftrightarrow a = q\,x$

osztó $x|a$, $x|b$ közös osztó

$\nexists x' > x \quad x'|a \wedge x'|b \Rightarrow x = (a,b)$
ha nincs nagyobb közös osztó akkor ő a legnagyobb
LCD = LNKO

- Euklideni algoritmus – legnagyobb közös osztó meghatározására
- $b > c > 0$; $(b,c) = x$;

Áll: $x = sb + tc$ (a legnagyobb közös osztó felírható a számok lineáris kombinációjaként)

10-11-11 Kodteck

- $\exists m : m \mid b-a \iff b = a \pmod m$

$$\left.\begin{aligned} b &= q_1 m + r \\ b &= q_2 m + r \end{aligned}\right\} (b-b) = (q_1 - q_2)m$$

- $(a,m) = 1$

$\exists b : b = a^{-1} \pmod m$ $\quad ba = qm + 1$, $ba - qm = 1$

Fermat-tétel:

p prím, $p \nmid c \rightarrow c^{p-1} = 1 \mod p$

Biz: $c, 2c, \dots, (p-1)c$ Különbözőek

$i, j < p \quad i \cdot c \neq j \cdot c \rightarrow (i-j)c = \not{0} \mod p \rightarrow \cancel{(i-j)c = qp}$

$c \cdot 2c \cdot 3c \cdot \dots \cdot (p-1)c = 1 \cdot 2 \cdot \dots \cdot \xi \cdot (p-1) \rightarrow c^{p-1} = 1$

$c^{p-1} \cdot \cancel{1 \cdot 2 \cdot \dots (p-1)} = \cancel{1 \cdot 2 \dots (p-1)}$

$c^{p-1} = 1$

Általánosítás:

$p_1 \nmid c$; $p_2 \nmid c \rightarrow (p_1, p_2, c) = 1$

$c^{(A-1)(p_2-1)} = 1 \pmod{p_1 p_2} \Rightarrow \left(c^{p_1-1}\right)^{p_2-1} - 1 \mod p_1$

Euler-Fermat tétel:

$\left(c^{p_2-1}\right)^{p_1-1} = 1 \mod p_2$

$p_1, p_2 \dots p_n$

$m = p_1 p_2 \cdots p_n$

$\phi(m) = (p_1 - 1)(p_2 - 1) \cdots (p_n - 1) \rightarrow c^{\phi(m)} = 1 \mod m$

RSA algoritmus:

kulcsvilanta: p_1, p_2 prímek $\rightarrow m = p_1 p_2$, $\phi(m) = (p_1-1)(p_2-1)$

$d = e^{-1} \mod \phi(m) \rightarrow de = q\phi(m) + 1$

elkész met prím-tényezőkre kell bontani → nagy számoknál leb. lehetetlen

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

$k_p = (e, m)$

$k_s = (p_1, p_2, d)$

$x \rightarrow [x^e \mod m] \xrightarrow{y = x^e \pmod m} [y^d \mod m] \rightarrow x = y^d \mod m$

$k_p = (e, m)$ $\qquad k_s = (p_1, p_2, d)$

$(x^e)^d \overset{?}{=} x$; $x^{ed} \overset{?}{=} x$, $x^{q\phi(m)+1} = x$

1, $(x,m) = 1$

2, $(x,m) > 1$:

$p_1 \mid x \to x = wp_1$

$(w,m) = 1$

$x^{q\phi(m)} \cdot x \overset{\xi}{=} x^{q(p_1-1)(p_2-1)} x =$

$= \left(\underbrace{x^{(p_1-1)(p_2-1)}}_{1}\right)^q x = x$

$x^{q\phi(m)+1} = (wp_1)^{q\phi(m)+1} = \underbrace{w}^{q\phi(m)+1} \cdot \underbrace{p_1}^{q\phi(m)+1} = w \cdot p_1 = x$

w p_1

$w^{q\phi(m)+1} = w^{q\phi(m)} \cdot w = \left(\underbrace{w^{(p_1-1)(p_2-1)}}_{1}\right)^q = w$

$p^{q\phi(m)+1} = \left(\left(p^{(p_2-1)}\right)^{(p_2-1)}\right)^q p_1 = p_1 \mod p_2$

$p_1^{q\phi(m)+1} = p_1 \mod m$

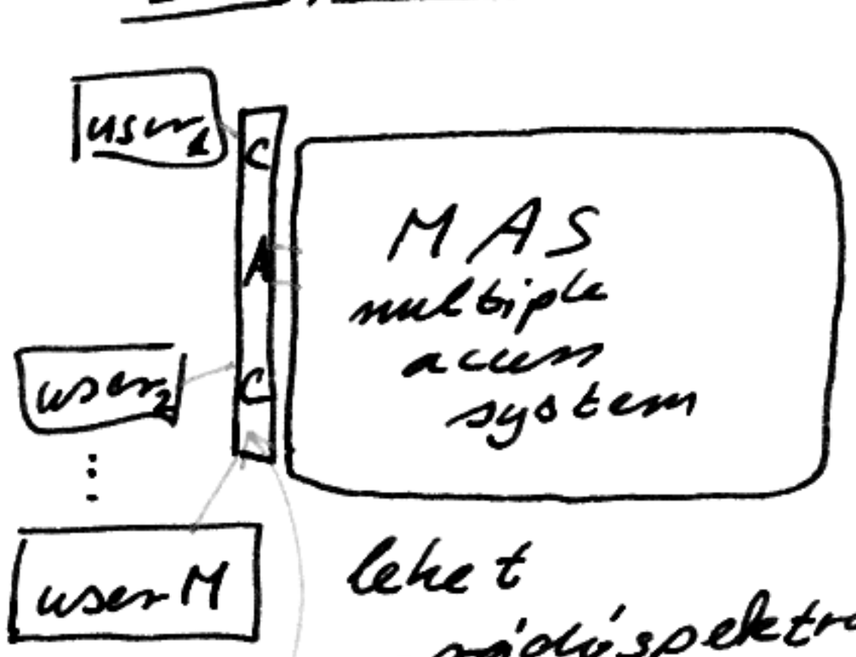
$p\ q\phi(m)+1$

10-11-23 Kodtech

ZH: dec. 3. Péntek 16-18 60-70 perc hossz

ZH előtti előadáson konzultáció

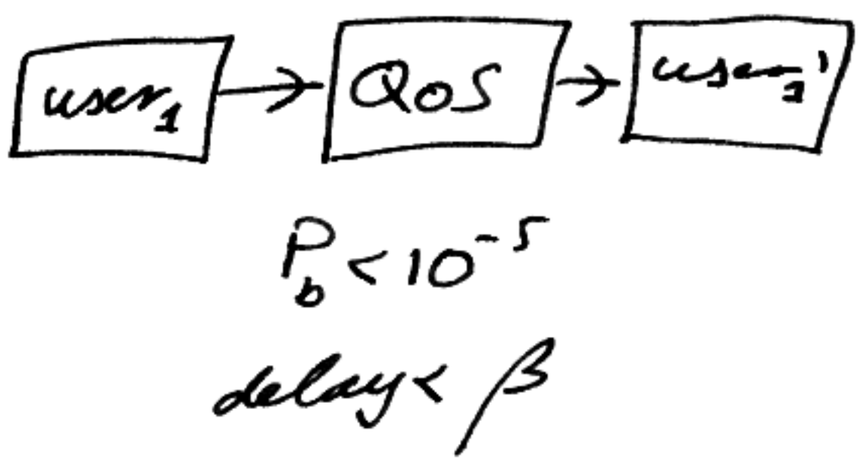
Sokfelhasználós rendszerek, kódolási algoritmusok



lehet
- rádióspektrum
- kábel
⋮

lényeg: közös médium

amit ebből a user kát

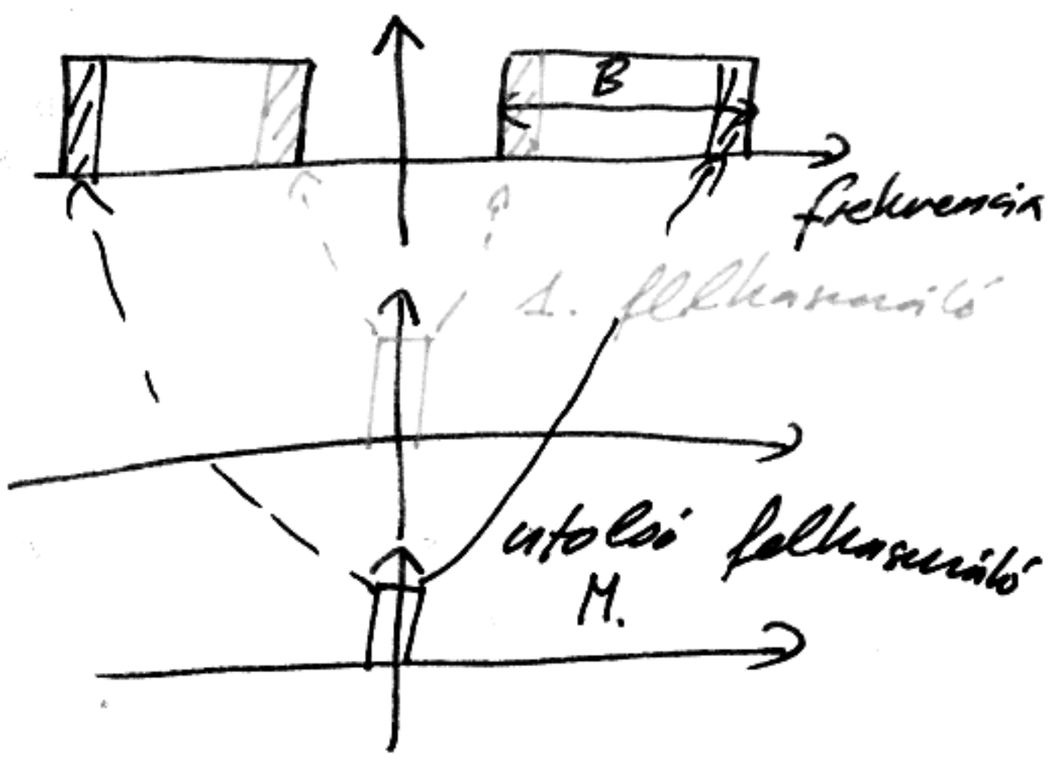


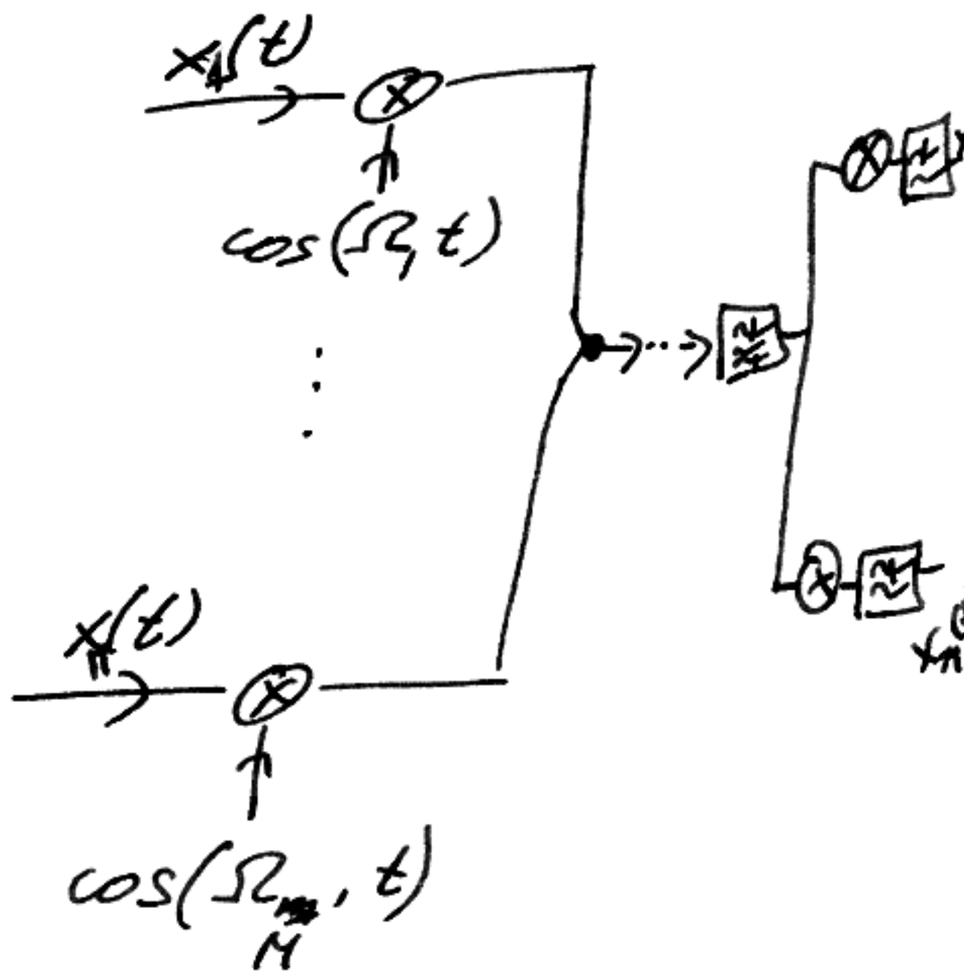
A service provider célja:
mat M (M a felhasználók száma)
kényszer:

$$MUI \leq \omega$$

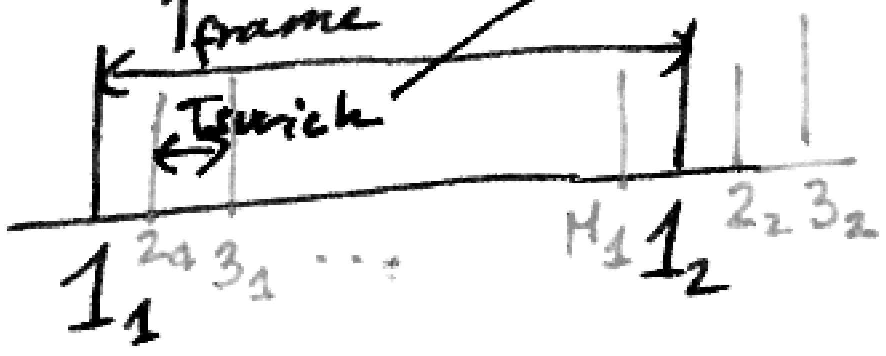
Történet

- FDMA – Frequency Division Multiple Access (1G mobil)
USA, '60 - '70 körül

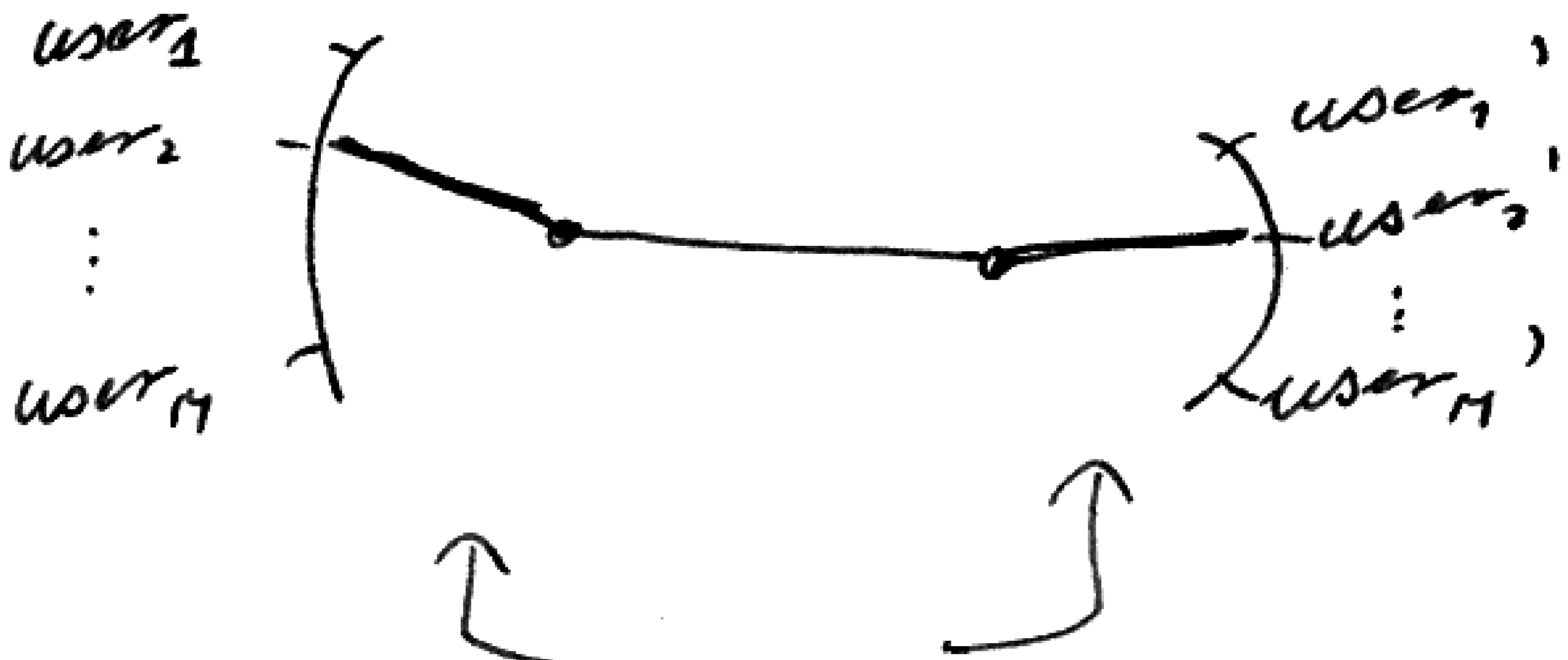




- TDMA (Time Division Multiple Access) – 2G mobil
  pl. GSM



$T_{frame} = \frac{1}{f_s} = 125\ ms$ beszédnél



$M = \frac{T_{frame}}{T_{switch}} = \frac{f_{sw}}{f_{fram}} \Rightarrow \frac{\text{technológia}}{\text{szolgáltatás}}$

↓

sajnos ezek túl közel vannak, keveset nyerünk

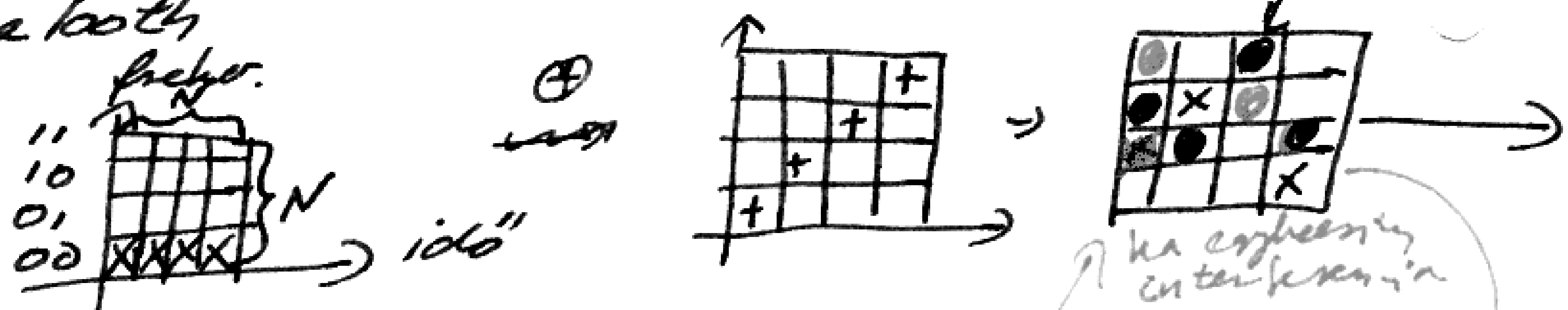
- beszédfelhasználó T_{frame}
- adatfelhasználó $T_{frame}' < T_{frame}$
  őt sűrűbben kellett mintavételezni.

ISDN

- CDMA (Code Division Multiple Access)

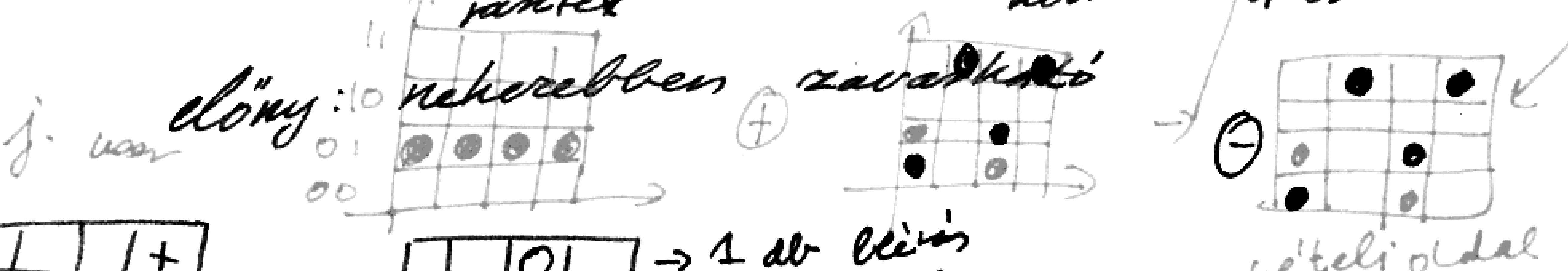
~~FH~~

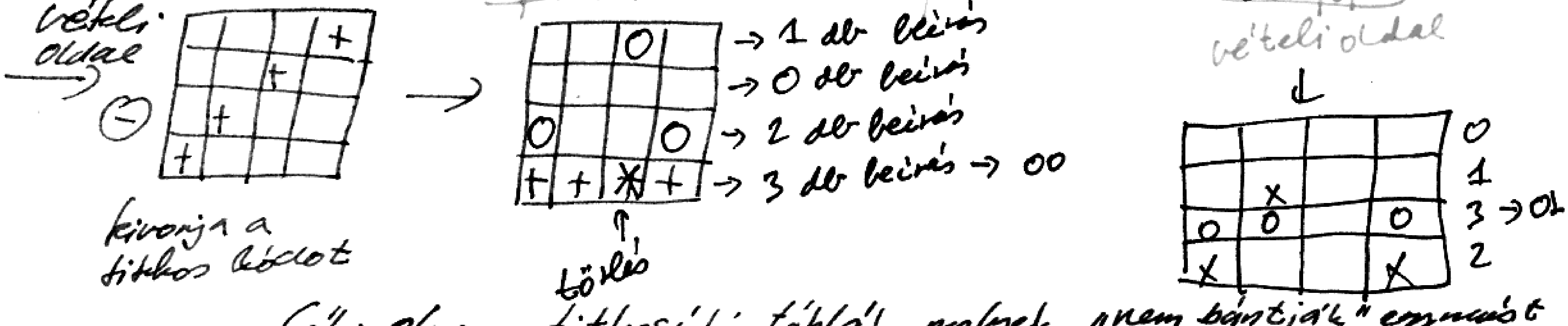
FH (Frequency Hopping)
pl. BlueTooth



idő-frekvencia panel   titkos kód   ez megy a csatornán

előny: nehezebben zavarható





kivonja a titkos kódot

Cél: olyan titkosító táblák, melyek „nem bántják" egymást

10-11-23 Kodtech

Einarsson → $O(N^2)$

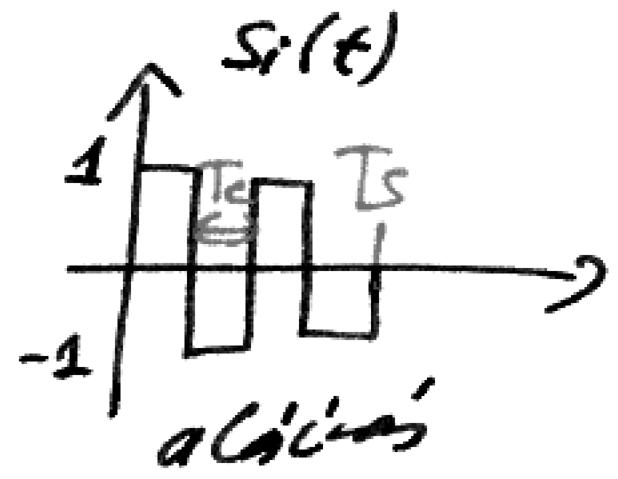
N: frekvenciasávok száma (= idősávok száma)

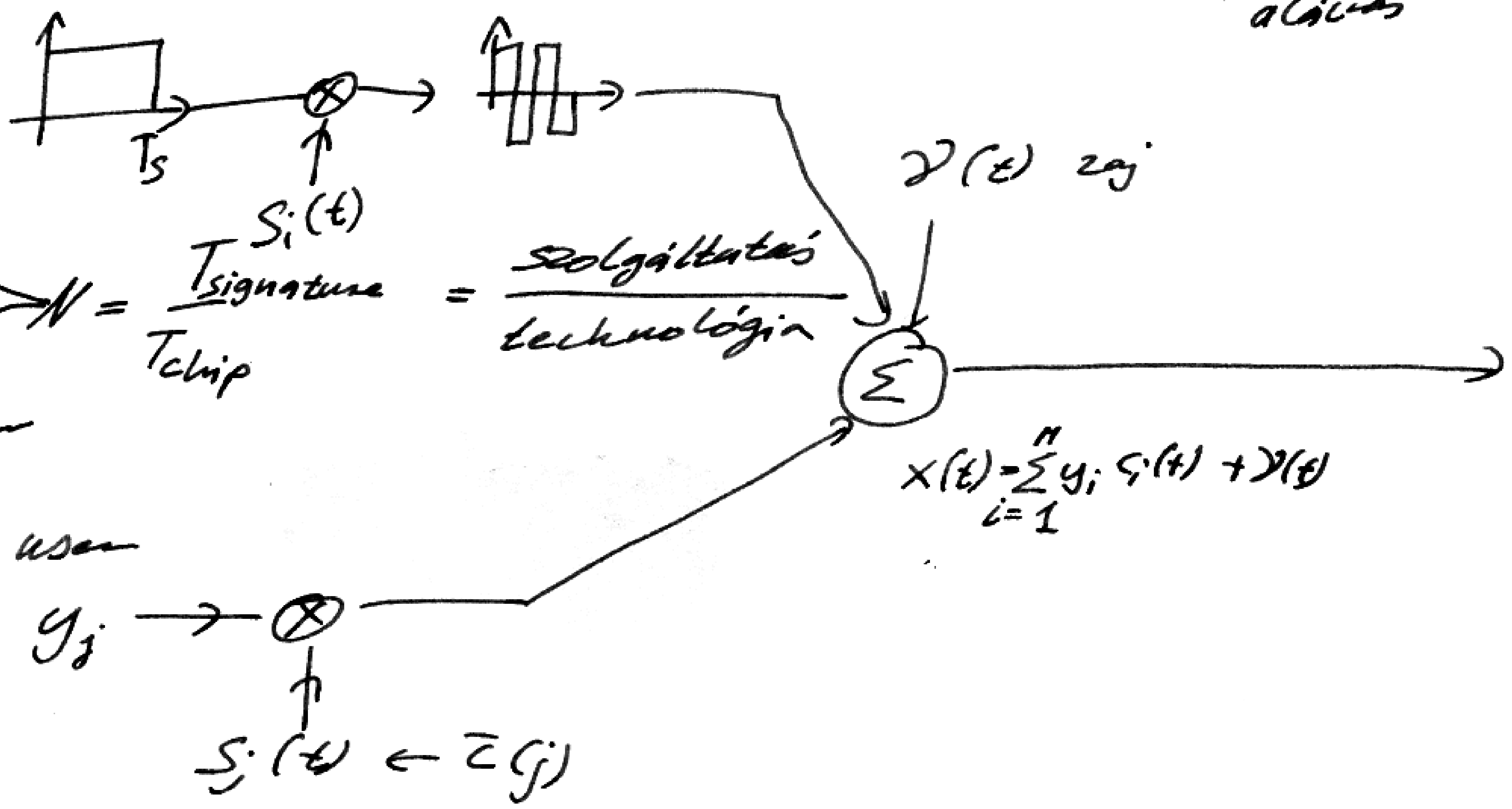
Beltéren azért jó, mert ott egy keskeny sávú zavarást okoz a visszaverődés (→ többutas terjedés), ez a módszer erre védett.

- CDMA / DS (Direct Sequence)

i. user $y_i \in \{-1, 1\}$

$\underline{z}^{(i)} = (1\ -1\ 1\ -1) \in \{-1, 1\}^N$ →





$x(t) = \sum_{i=1}^{M} y_i s_i(t) + \nu(t)$

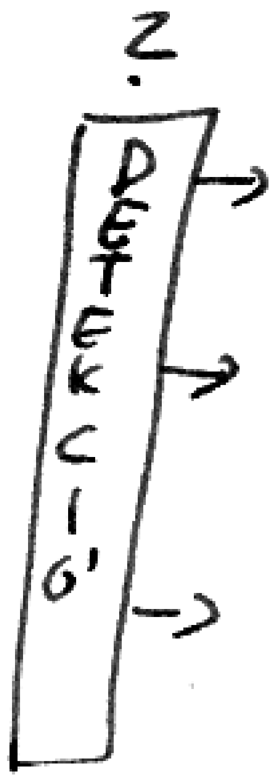
$N = \frac{T_{signature}}{T_{chip}} = \frac{\text{szolgáltatás}}{\text{technológia}}$

ma: 100–1000 nagy van

5–6 adatuser

$$\frac{1}{T_s}\int_0^{T_s} s_i(t)x(t)\,dt \to x_i$$

$$\frac{1}{T_s}\int_0^{T_s} s_j(t)x(t)\,dt \to x_j$$



Igazi modell:

$$x(t) = \sum_{i=1}^{M} \alpha_i y_i s_i(t - T_i) + \nu(t)$$

α_i: különböző csillapítás; T_i: különböző késleltetés

Még igazibb modell:

$$x(t) = \sum_{i=1}^{M} y_i s_i(t) * k_i(t) + \nu(t)$$

Mi van az egyenes modellel országgyűlés.

"ℓ" $x_\ell = \frac{1}{T_s}\int_0^{T_s} x(t) y_\ell(t)\,dt = \frac{1}{T_s}\int_0^{T_s}\left(\sum_{i=1}^{M} y_i s_i(t) + \nu(t)\right) s_\ell(t)\,dt =$

$$\sum_{i=1}^{M}\frac{1}{T_s}\int_0^{T_s} s_\ell(t)\, s_i(t)\,dt\, y_i + \frac{1}{T_s}\int_0^{T_s}\nu(t)\, s_\ell(t)\,dt$$

$$\overline{\overline{R}}: R_{\ell i} = \frac{1}{T_s}\int_0^{T_s} s_\ell(t)\, s_i(t)\,dt = \frac{1}{N}\sum_{m=1}^{N} c_m^{(\ell)} c_m^{(i)} = \frac{1}{N}\bar{c}^{(\ell)} T \bar{c}^{(i)}$$

$$x_L = \sum_{i=1}^{M} R_{\ell i} y_i + \nu_\ell = R_{\ell i} y_\ell + \underbrace{\sum_{\substack{i=1 \\ i\neq\ell}}^{M} R_{\ell i} y_i}_{M \cup I = \emptyset} + \nu_\ell$$

$M \leq N$, hogy a c-k ortogonálisak legyenek

10-11-16 Kodtech

Bátfai Norbert
MIT

http://www.inf.unideb.hu/~batfai/

/courses/BSc_Coding-Tech/index.html

— 14021 —

hMAC - kétszer hasonlítja a kulcsot, az elején és a végén is
hatékony
gyors
biztonságos

CBC : cycle block chain

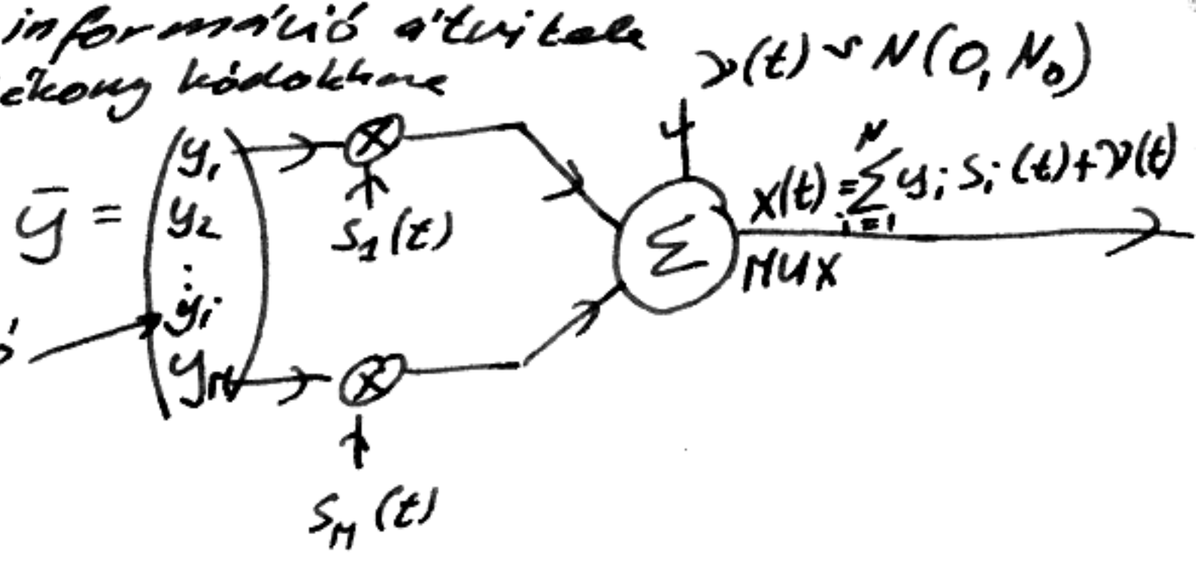
CDMA / MS → multiuser információ átvitele kaotikus kódokkal

10-11-25 Kodtech

$\bar{y} \in \{-1, 1\}^M$

felhasználók: $i = 1 \dots M$

"i"-ik felhasználó

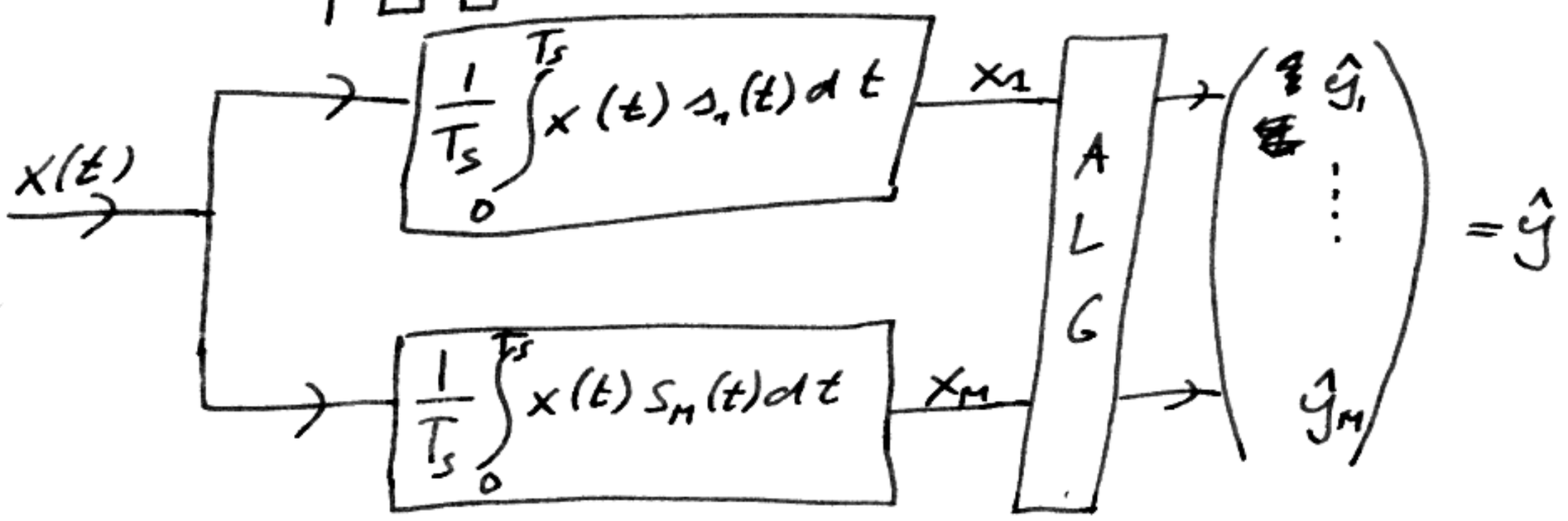


$\bar{c}^{(i)} \in \{-1, 1\}^N$

$\downarrow$

$S_i(t)$

$\Rightarrow N = \frac{T_s}{T_c} \sim \frac{\text{kapcsolási frekv.}}{\text{adatátviteli sebesség}}$



$P(y_i \neq \hat{y}_i) < 10^{-\gamma} \Longrightarrow C = \{\bar{c}^{(i)},\ i = 1, \dots, M\}$?

Mak M ?

ALG = ?

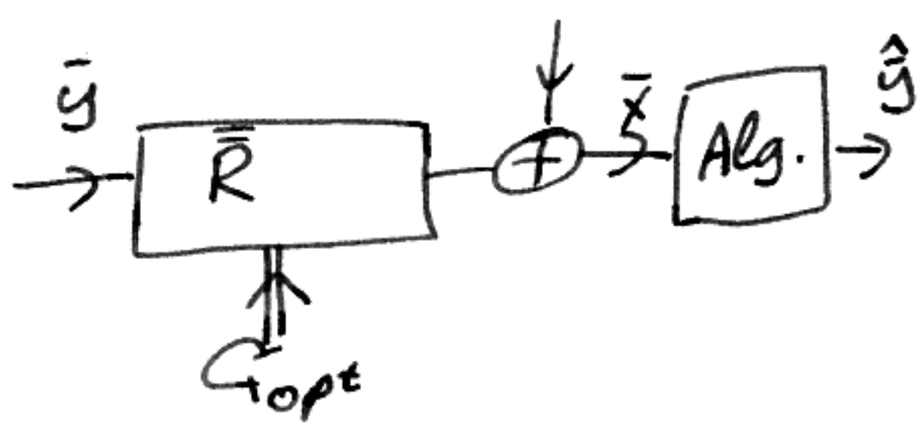
$$x_l = \frac{1}{T_s}\int_0^{T_s} x(t)\, s_l(t)\, dt = \frac{1}{T_s}\int_0^{T_s} \left(\sum_{i=1}^{M} y_i\, s_i(t) + \gamma(t)\right) s_l(t)\, dt =$$

$$= \sum_{i=1}^{M} \frac{1}{T_s}\int_0^{T_s} s_l(t)\, s_i(t)\, dt\, y_i + \frac{1}{T_s}\int_0^{T_s} \gamma(t)\, s_l(t)\, dt$$

$\bar{\bar{R}}$ $R_{ij} = \frac{1}{T_s}\int_0^{T_s} s_l(t)\, s_j(t)\, dt = \frac{1}{N}\sum_{n=1}^{N} c_m^{(l)} c_m^{(j)} = \frac{1}{N}\bar{c}^{(i)T} c^{(j)}$

$$R_{lj} = \frac{1}{N}\sum_{m=1}^{N} c_m^{(l)\,2} = 1$$

$$x_l = \sum_{i=1}^{M} R_{lj}\, y_i + \gamma_l \rightarrow \bar{x} = \bar{\bar{R}}\,\bar{y} + \bar{\nu}$$



$$x_l = y_l + \sum_{\substack{i=1 \\ i \neq l}}^{M} R_{li}\, y_i + \gamma_l$$

$$R_{li} = \emptyset \quad \forall i,l = 1,\dots,M \quad l \neq i$$

$C \Rightarrow$ ortogonális vektorok

$M \leq N$

Kérdés: hogyan lehet $M > N$?

Ortogonális kódválasztás → Walsh - Hadamard kódok

$$\bar{\bar{C}}_{2\times2} = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \Rightarrow \bar{\bar{C}}_{4\times4} = \begin{pmatrix} \bar{\bar{C}}_{2\times2} & \bar{\bar{C}}_{2\times2} \\ \bar{\bar{C}}_{2\times2} & -\bar{\bar{C}}_{2\times2} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{pmatrix}$$

$$\bar{\bar{C}}_{2^{n+1}\times 2^{n+1}} = \begin{pmatrix} \bar{\bar{C}}_{2^n\times 2^n} & \bar{\bar{C}}_{2^n\times 2^n} \\ \bar{\bar{C}}_{2^n\times 2^n} & -\bar{\bar{C}}_{2^n\times 2^n} \end{pmatrix}$$

Nem ortogonális kódok esete: $M > N$

$$\bar{x} = \bar{\bar{R}}\bar{y} + \bar{\nu} \rightarrow \bar{\nu} \sim N(\bar{0}, \bar{\bar{R}})$$

↑ nem ortogonális $\bar{\bar{R}}$?

$N < M$

$$K_{i,j} = \mathbb{E}(\nu_i, \nu_j) - \mathbb{E}\left(\frac{1}{T_s}\int_0^{T_s} \nu(t) s_i(t)\,dt \cdot \frac{1}{T_s}\int_0^{T_s} \nu(\tau) s_j(\tau)\,d\tau\right) =$$

$$= \mathbb{E}\left(\frac{1}{T_s^2}\int_0^{T_s}\int_0^{T_s} \nu(t)\nu(\tau) s_i(t) s_j(\tau)\,dt\,d\tau\right) =$$

$$= \frac{1}{T_s^2}\int_0^{T}\int_0^{T} s_i(t) s_j(\tau) \underbrace{\mathbb{E}\left(\nu(t)\nu(\tau)\right)}_{N_0 \delta(t-\tau)} dt\,d\tau =$$

$$= \frac{1}{T_s^2}\int_0^{T_s}\int_0^{T_s} s_i(t) s_j(t) N_0 \delta(t-\tau)\,dt\,d\tau =$$

$$= \frac{N_0}{T_s^2}\int_0^{T_s} s_i(t) s_j(t)\,dt = N_0' \cdot \frac{1}{T_s}\int_0^{T_s} s_i(t) s_j(t)\,dt =$$

$$= N_0' R_{ij}.$$

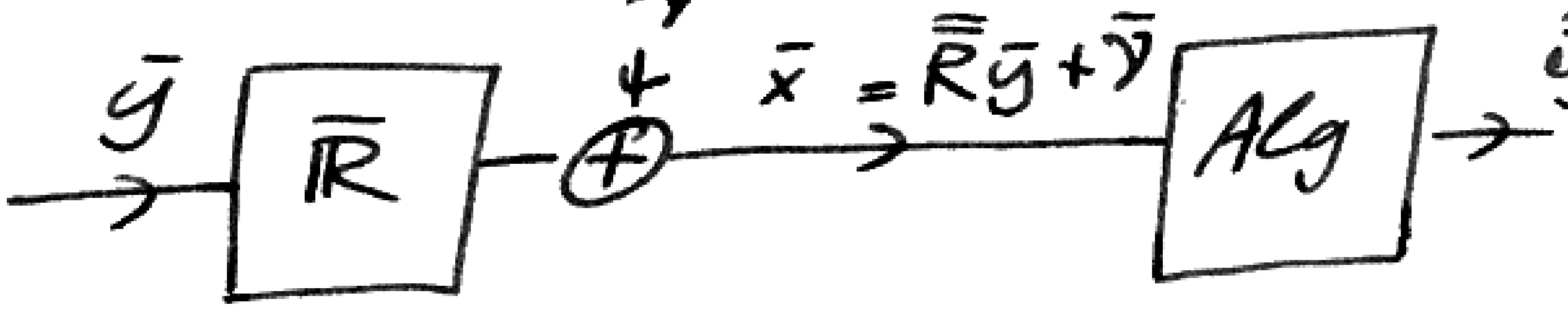
$$\bar{\nu} \sim N(\bar{0}, N_0' \bar{\bar{R}}) \Rightarrow$$

$$\Rightarrow \frac{1}{\sqrt{(2\pi)^M \det(N_0' \bar{\bar{R}})}} \cdot e^{-\frac{1}{2}\bar{u}^T \frac{\bar{\bar{R}}^{-1}}{N_0} \cdot \bar{u}}$$

E2 KELL

Levezetés, nem kell tudni

10-11-25 Kodtech



$\hat{y}$ $\max P(\bar{y} | \bar{x})$
$\bar{y} \in \{-1, 1\}^M$

$M > N$

$\bar{y} \in \{-1, 1\}^M$

$$\frac{P(\bar{x}|\bar{y})P(\bar{y})}{P(\bar{x})}$$

konstansok, maximalizálás alkalmazásakor elhagyhatók

$\bar{\nu} \sim N(0, N_0\bar{\bar{R}})$

$$\sim \max_{\bar{y} \in \{-1,1\}^M} \frac{1}{(2\pi)^M \det(N_0\bar{\bar{R}})} \cdot e^{-\frac{1}{2}(\bar{x}-\bar{\bar{R}}\bar{y})^T \frac{\bar{\bar{R}}^{-1}}{N_0} (\bar{x}-\bar{\bar{R}}\bar{y})} \sim$$

konstans — monoton fv.

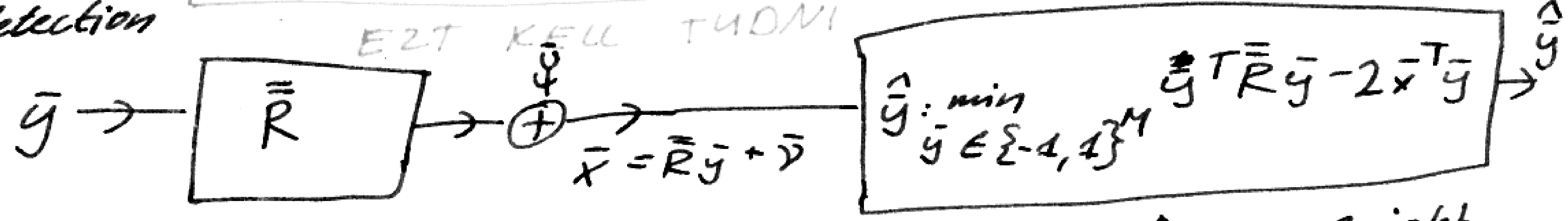
$$\sim \max_{\bar{y} \in \{-1,1\}^M} -\frac{1}{2}(\bar{x}-\bar{\bar{R}}\bar{y})^T \frac{\bar{\bar{R}}^{-1}}{N_0}(\bar{x}-\bar{\bar{R}}\bar{y}) \sim \min_{\bar{y} \in \{-1,1\}} (\bar{x}-\bar{\bar{R}}\bar{y})^T \bar{\bar{R}}^{-1} (\bar{x}-\bar{\bar{R}}\bar{y})$$

konstans — konstans

MUD
multi
user
detection

$$\hat{y} : \min_{\bar{y} \in \{-1,1\}^M} \bar{y}^T \bar{\bar{R}} \bar{y} - 2\bar{x}^T\bar{y}$$

EZT KELL TUDNI



a legjobb QoS

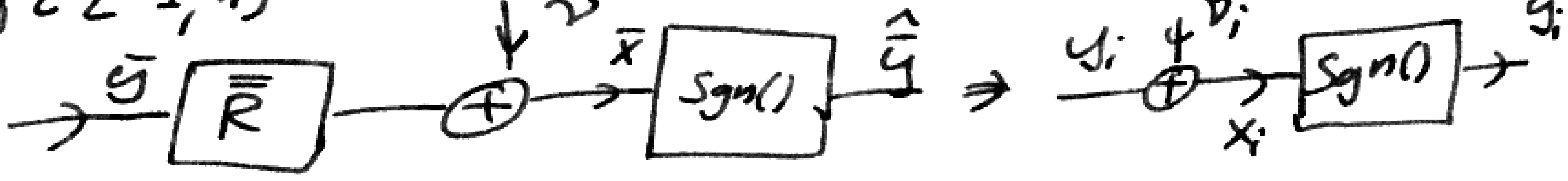
baj: $O(2^M)$ komplexitású

nem real-time

Vissza az ortogonális kódokhoz

Ha G ortogonális, akkor $\bar{\bar{R}}$ diagonális $\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ 0 & \dots & \dots & 1 \end{pmatrix}$

$$\hat{y} \min_{\bar{y} \in \{-1,1\}^M} \bar{y}^T(\bar{y} - 2\bar{x}) \Rightarrow \hat{y} = sgn(\bar{x}) \rightarrow y_i = sgn(x_i)$$



$$\bar{y}(k+1) = -sgn\{\bar{\bar{R}}'\bar{y}(k) - \bar{x}\} \rightarrow O(M^2)$$

$$\hat{y} \min_{\bar{y} \in \{-1,1\}^M} \bar{y}^T \bar{\bar{R}} \bar{y} - 2\bar{x}^T\bar{y}$$

$$y_l(k+1) = sgn\{\sum_{j=1}^{M} R'_{lj} y_j(k) - x_l\} \Rightarrow DSP$$

10 - 11 - 30 Kodtech

ZH: dec. 3. péntek 16 h (1 óra)

Teremberosztás:

IB026	Andrásnyi	Bujdák
IB027	Bús	Trigó
IB028	Gál	Kovács
QI	Körmöczy	Soós
QII	Sövös	Zsigmond

Aki nem megfelelő teremben próbálkozik, eleve érvénytelen a dolgozata.

Kell:
- 4 lap
- számológép
- toll
- diák/személyi

A forma le van írva a lap tetején, azt le kell tartani, különben jó.

---

http://www.hit.bme.hu/oktatas/tantargyaink

kódolástechnika

adatlap → eredmények, megtekintés ideje is itt

Ciklikus Reed-Solomon kód a GF(8) felett

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

$$n = q - 1 \Rightarrow n = 7$$

$$n-k = 2 \Rightarrow C(7,5)$$

Paritásellenőrző polinom:

$$\deg(h(x)) = k$$

$$h(x) = (x+y^3)(x+y^4)(x+y^5)(x+y^6)(x+y^7)$$

↑ + = −

$$\begin{cases} h(x)\,g(x) = x^n - 1 \\ g(x) = \prod_{i=1}^{n-k} (x - y^i);\quad h(x) = \prod_{i=n-k+1}^{n} (x - y^i) \end{cases}$$

Javítható hibák száma:

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

↑ mivel Reed-Solomon kód

Jelezhető hibák száma: 2

$$h(x) = (x^2 + y^6 x + 1)(x^2 + yx + y^2)(x+1) =$$

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

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

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

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

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

- Kérdések:

Két azonos szindrómavektorhoz tartozó hibavektorokból a kisebb súlyút kell dekódolási → IGAZ

Egy C(n, G) paraméterű kódkészlet Hamming-kód. → IGAZ

A szisztematikus kódok paritásellenőrző mátrixának az utolsó k×k-s négyzetre egységmátrix → HAMIS

Forráskódolás

Adott egy emlékezet nélküli forrás, 3 szimbólumot bocsát ki: $p_1 = 0,7$

$p_2 = 0,2$

$p_3 = 0,1$

Adja meg a tömöríthetőség alsó határát!

- az alsó korlát az entrópia: $H(x) \leq L$

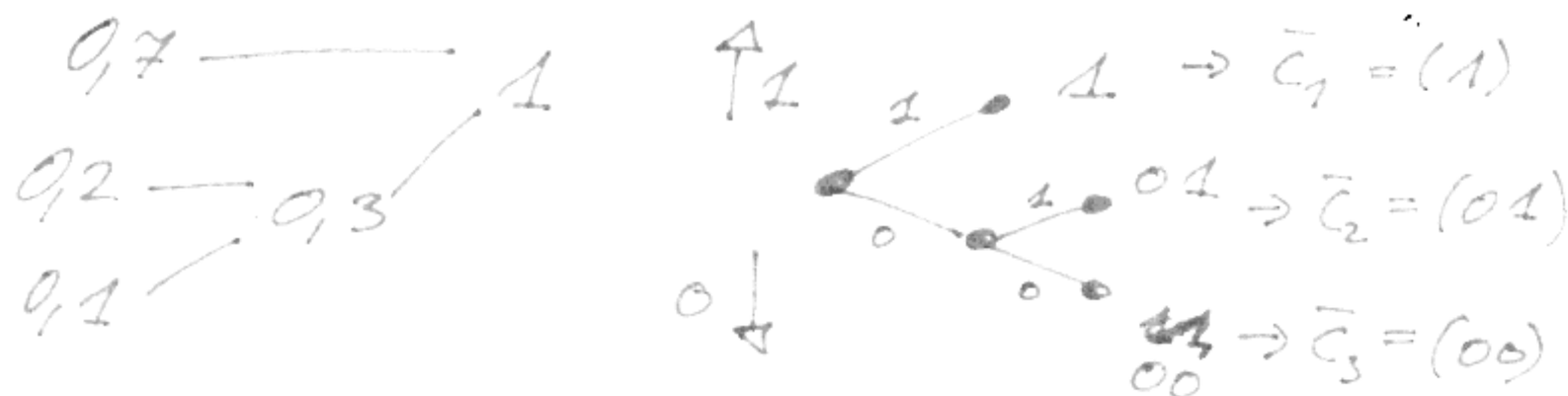
$$L = \sum_{i=1}^{n} p_i l_i$$

$$H(x) = \sum_{i=1}^{n} p_i \cdot ld \frac{1}{p_i} = 0,7 \cdot ld \frac{1}{0,7} + 0,2 \cdot ld \frac{1}{0,2} + 0,1 \cdot ld \frac{1}{0,1} =$$

$$= 1,1559$$

$$\left(L = \sum_{i=1}^{3} p_i l_i \right)$$

Konstruáljon Huffman-kódot!



X	C
x_1	1
x_2	01
x_3	00

$1 \rightarrow \bar{C}_1 = (1)$

$01 \rightarrow \bar{C}_2 = (01)$

$00 \rightarrow \bar{C}_3 = (00)$

$(L = 1 \cdot 0,7 + 2 \cdot 0,2 + 2 \cdot 0,1 = 1,3 \rightarrow$ kicsit több, mint az elvi korlát)

Milyen minimum és maximumértékek közé esik egy 4 szimbólumos forrás entrópiája? 0 és 2 közé

Egy 8 szimbólumot tartalmazó egyenletes eloszlású forrásnál hány bitesek lennek a kódszavak? 3

Egy 5 szimbólumot kódnál a következő kódkészletek adottak:

$l_1 = 2 \quad l_2 = 2 \quad l_3 = 2 \quad l_4 = 3 \quad l_5 = ?$

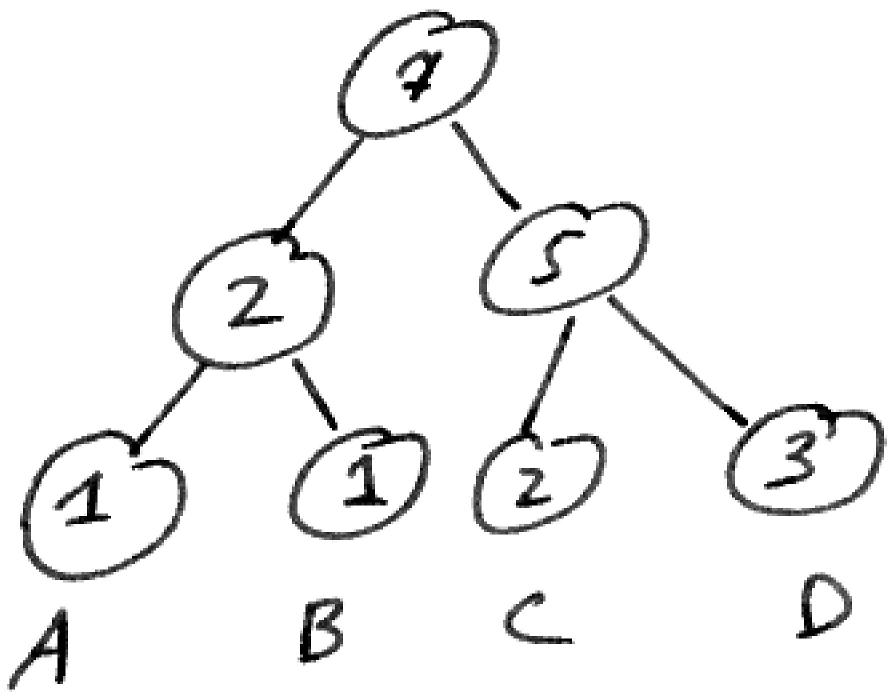
$$\sum_{i=5}^{n} 2^{-l_i} \leq 1 \rightarrow$$

$$2^{-2} + 2^{-2} + 2^{-2} + 2^{-3} + 2^{-?} \leq 1$$

$\rightarrow ? = 5$

10-11-30 Kódtech

Lehet-e ez egy adaptív Huffman-kódoló állapotgráfja?



– szükséges tulok:

- a gyerek-node-ok összege a szülő (ez OK)
- balról jobbra és felfelé olvasva növekvő sor kell

1 1 2 3 2 5 7
↓
itt rossz!

OTP kódolás

$Y_i = X_i \oplus K_i$

$P(K_i = 1) = 0{,}6$ $P(K_i = 0) = 0{,}4$

Milyennek kell lennie a szövegnek, hogy ez jó kódolás legyen?

$I(X,Y) = \emptyset \Rightarrow H(X) \le H(K) = 0{,}9709$

⇓

az üzenet entrópiája a kulcsénál kisebb legyen

Adott egy lineáris bináris hibajavító kód.

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

Adja meg a kód típusát!

$C(5,3)$

Lehet-e bináris Hamming-kód?

$2^{n-k} \neq n+1$

Mennyi a kódtávolság?

Legeneráljuk a kódszavakat és a legkisebb súlyát vesszük (de nem a csupanullát).

$\bar{u} = (000) \rightarrow \bar{c} = (00000)$

$\bar{u} = (001) \rightarrow \bar{c} = (00111)$

$\bar{u} = (011) \rightarrow \bar{c} = (01101)$ $W_{min} = d_{min} = 2$

$\bar{u} = (010) \rightarrow \bar{c} = (01010)$

$\bar{u} = (100) \rightarrow \bar{c} = (11100)$

$\bar{u} = (101) \rightarrow \bar{c} = (10110)$

$\bar{u} = (110) \rightarrow \bar{c} = (11011)$

$\bar{u} = (111) \rightarrow \bar{c} = (11100)$

Standard array-t megvizsgálni

$\log_2(a)$

$$F_s = \left\{ \bar{e} : \bar{\bar{H}} \bar{e}^T = \bar{s}^T \atop \bar{c}' = \bar{e} + \bar{c} \right\} \to |E_s| = 8$$

$3 \to \dim(3) = 2 \qquad \bar{s} = (1\,1)$

$E_s = \{ \bar{e} : \bar{\bar{H}} \bar{e}^T = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$\bar{\bar{H}}_{2\times5} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \qquad \bar{\bar{H}}_{2\times5} \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

$E_s = \{(00100), (00011), (01001), \dots\}$

Tömörítés LZ-75-tel

0|1|00|0 1|010|0101|000

0, 1, 00, 01, 010, 0101, 000

"1" "2" "3" "4" "5" "6" "7"

001 010 011 100 101 110 111

(000, 0)(000, 1)(001, 0)(001, 1)(100, 0)(101, 1)(011, 0)