

Hírközlés elmélet

dr. Bitó János

4 kis ZH van

10 hallgató felett

Szerda 8¹⁵ | EL20

inkrementális ZH rendszer!

össz 15 pont

csütörtök 10¹⁵ E1C

2 legjobb ZH átlaga

4 pont 4,5-7 1

7,5-9 - 2

9,5-11 - 3

11,5-13 - 4

13,5-15 - 5

ZH: 3 rész \rightarrow temat példátétel

10 tentés feleletbeírás (infokommu)

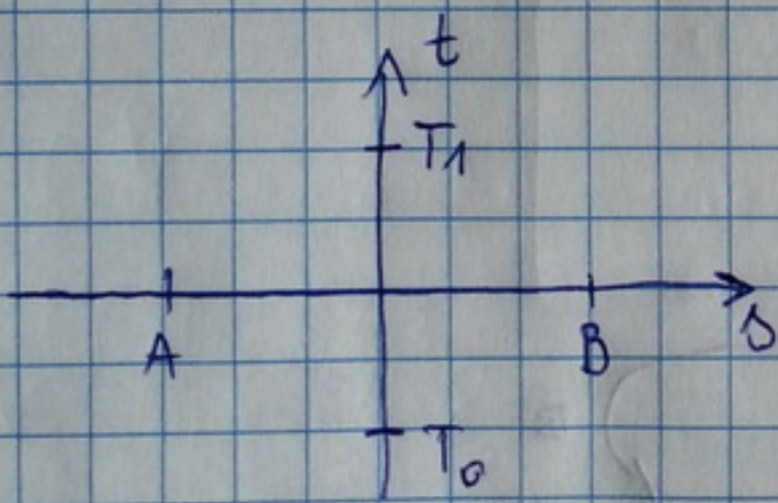
tétel kifejtés

példa nemelés

1. előadás

információ forrásból üzenetként eljuttatás ~ az információ nyelvéhez = HÍRKÖZLÉS

+ zaj, zavar, interferencia (mesterséges vagy természetes)



időben
vagy
térben
elkülönült pontok

forrás kódolás / tömörítés [időben elkülönített kor]

• mi az információ? Jellem-e a nap levegő?

$P(\text{nap}) \rightarrow 0$

Holnap nem kel fel a nap \rightarrow nagy az információ tartalma

• hogyan mérjük az információt?

- kell egy kvantitatív mérték

~ Hartly (1928, Bell System Technical Journal) "Transmission of information" címmel

() az ember alapvető igénye a kommunikáció

ANALÓG! ~ szimulációs jelek reprodukciója volt a feladat (telefon)

↓ elhelyezt!

esemény: $\xi = \{x_1, x_2, x_3, \dots, x_n\}$ infót csak akkor viszünk át, ha az esemény több kimenetelű
 - lényeg a döntés a kimenetek között

$\# \xi = D$ (# ~ ahány esetet felvehet az esemény) $I(\xi)$

$\bar{\xi} = \{\xi_1, \xi_2, \xi_3, \dots, \xi_n\}$ n db val. változó együttese

$\# \bar{\xi} = D^n$ [D · D · D · ... · D]

$I(\bar{\xi}) = n \cdot I(\xi)$

információ tartalom van, ha: több kimenetel van!

$\# \xi = D \quad I(\xi) = \log_a D$
 $\# \bar{\xi} = D^n \quad I(\bar{\xi}) = n \cdot I(\xi)$
 $\log_a D^n = n \cdot \log_a D$

ha $a=2 \rightarrow \log_2$
 ↓
 \log_2 [bit]
 ha $a=10 \rightarrow \log_{10}$
 ↓
 \log [Hartly]

DEEZ MÉG NEM JÓ:

példa:

kealap 4 golyó
 1-et hívunk



$D = 2$

$\log_2 D = 1$ [bit]
bináris digit



() azt várnam hogy fehér lesz ezért jobban meglepődök! több info



● : $\log_4 \frac{4}{1} = 2$ [bit]
 hívok

○ : $\log_4 \frac{4}{3} = 0,415$ [bit]

a baj az, hogy a Hartly értékek nem veszi figyelembe a valószínűségi eloszlást!

[bit] az információ mennyiség értéke

BIT



● = 2
○ = 0,415

$$\frac{1}{4} \cdot 2 + \frac{3}{4} \cdot 0,415 = 0,811 \text{ [bit]}$$

(Labels: $\frac{1}{4}$ - valószínűség, 2 - info. tartalom, $\frac{3}{4}$ - valószínűség, $0,415$ - info. tartalom)

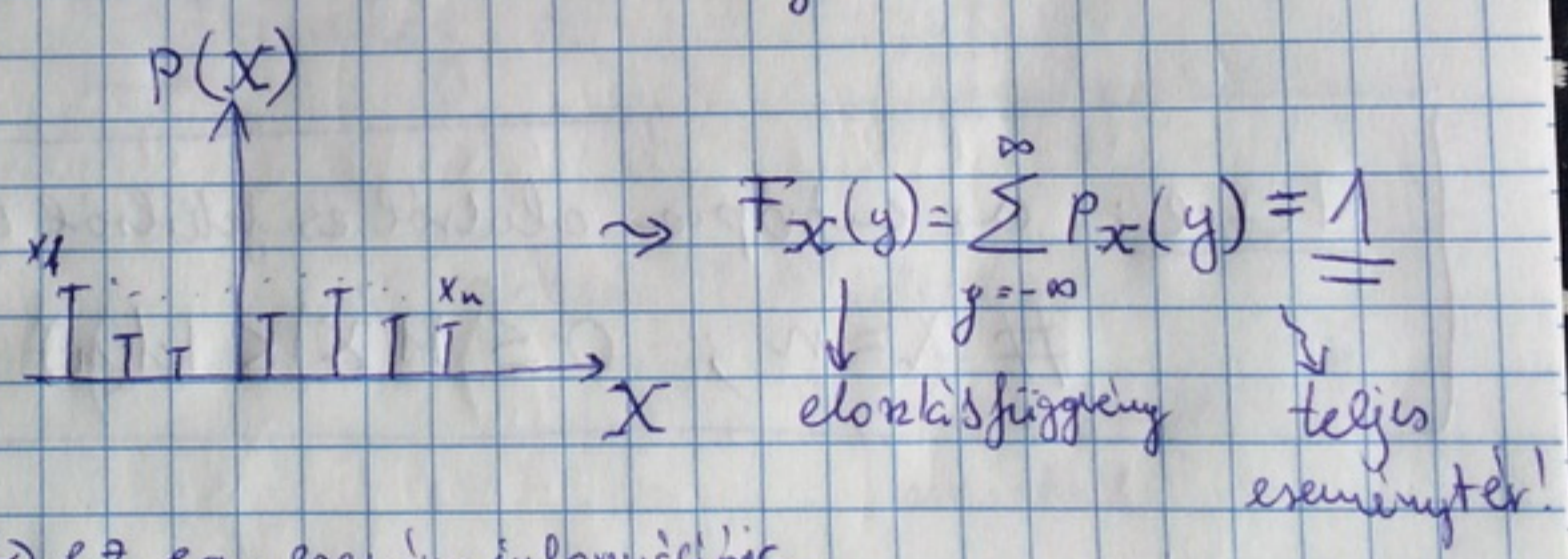
↳ kevesebb info mint egyenletes eloszlásnál

Claude Shannon (1948, BSTS) - "A Mathematical Theory of Communication"

legyen:

$$X = \{x_1, \dots, x_n\}; \quad P(X) = (p_1, \dots, p_n)$$

(Labels: X - diszkrét értékű val. változó; $P(X)$ - valószínűségi f.; $p_i = P(x_i)$ - i. dik. esemény)



Def: $I(x_i) = \log_2 \frac{1}{p(x_i)}$

↳ ez egy esemény információja [bit]
 ↳ $-\log_2(p(x_i))$

(Label: Minél valószínűbb az esemény annál kisebb az info. tartalom)

(Self Information - az esemény saját információ tartalma)

Def: Entropia, Átlagos információ tartalom (entropy)

$$H(X) = E\{I(x_i)\} = \sum_{x_i \in X} p(x_i) \cdot \log_2 \frac{1}{p(x_i)}$$

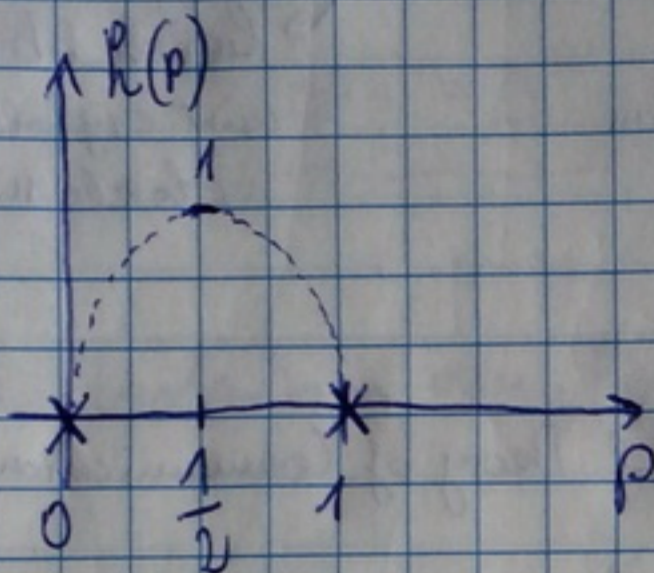
(Label: $I(x_i)$ - \Rightarrow utarcsi és a lájkok)

- legyen $X = \{x_1, x_2\}$, $p(x) = \{p(x_1), p(x_2)\} \Rightarrow \left\{ p(x_1); 1 - p(x_1) \right\}$
 ez az az 1 paraméteres

$$H(X) = \sum_{x_i \in X} p(x_i) \cdot \log_2 \frac{1}{p(x_i)} = p \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p}$$

$h(p) =$ bináris entropia fű

határérték probléma a véletlen!



legyen $x = \frac{1}{p}$

$$p \cdot \log_2 \frac{1}{p} ; \frac{1}{x} \cdot \log_2 x$$

$$\lim_{x \rightarrow \infty} \frac{1}{x} \cdot \log_2 x = \frac{1}{\log_2 2} \cdot \lim_{x \rightarrow \infty} \frac{\log_2(x)}{x} \stackrel{L'H^1}{=} \frac{1}{\log_2 2} \lim_{x \rightarrow \infty} \frac{1}{x}$$

$\Rightarrow 0$

úgy dalom kértél és !!! gölti Bitóval

Tétel: az entropia alulról és felülről is korlátos

$$\# X = n ; 0 \leq H(X) \leq \log_2(n)$$

2. előadás

Proakis, Salehi: Communication Systems Engineering

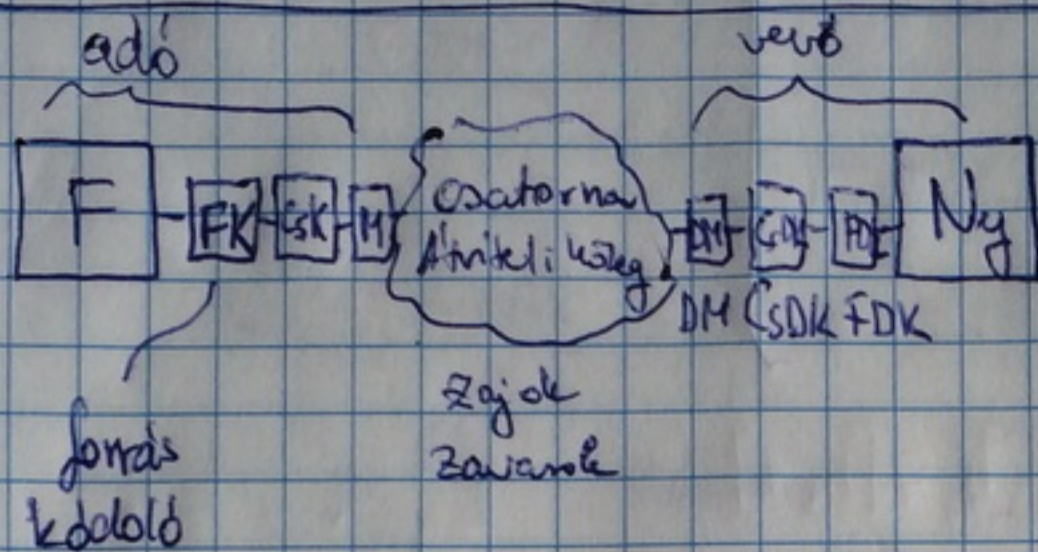
Dallos: Tantárgyi segédlet a hírközlés elmélet tárgyhoz

Prigys I.: Hírközlés rendszerei

Csibi S.: Információ közlése és feldolgozása

}

IRODALOM



FK: ami redundáns, azt töri ki [vesztételes és veszteségmentes]

CsK: a fellepő zavarok nullapítása (hibajavító + redundancia hozzáadás)

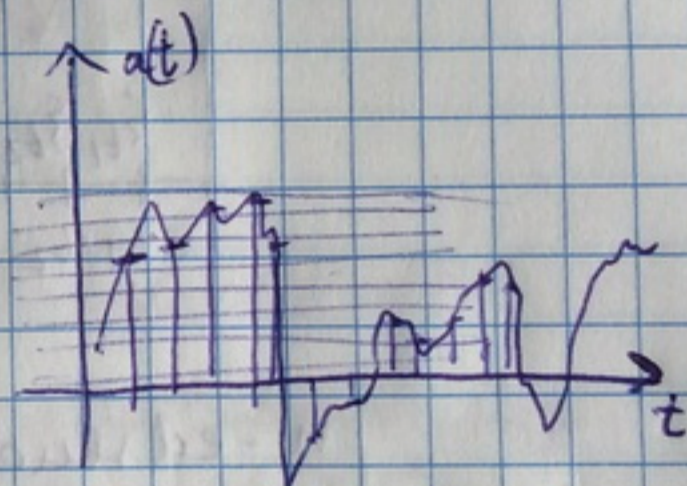
M: modulátor

DM: demodulátor

CsDK: csatorna dekódolás

FDK: ferris dekódolás

F analóg $a(t)$

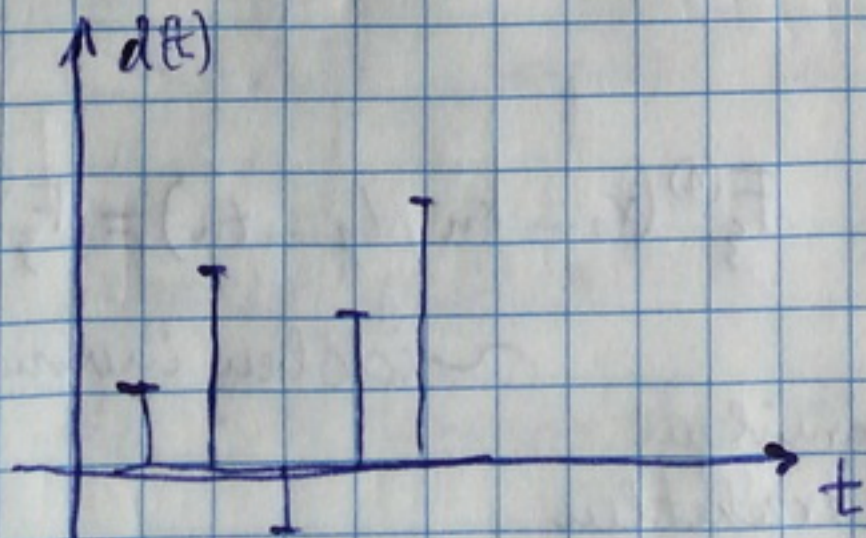


igen Bell idejében ↗

Ba sávkorlátozott $(\frac{1}{2T})$
mv. tétel:

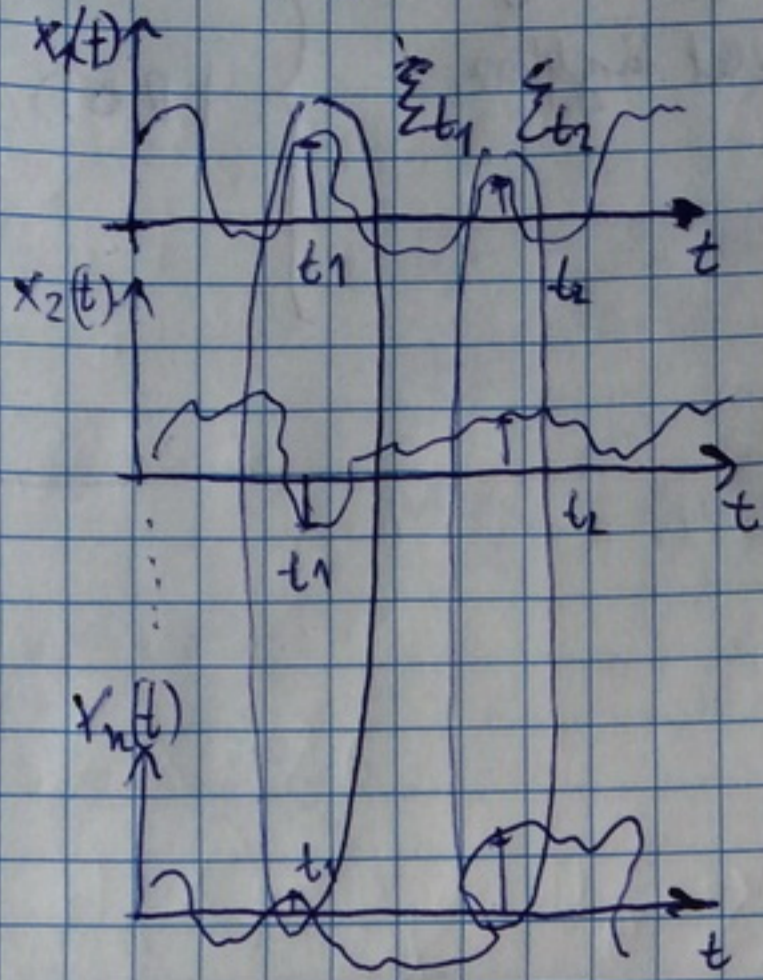
Ma digitális jel:

- időben mintavetelés (T)
- értékben kvantálva



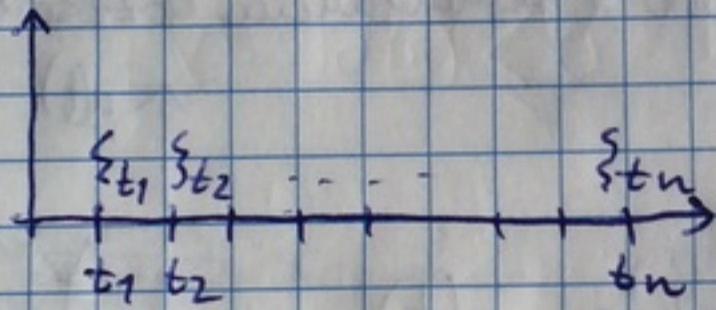
Sztochasztikus folyamatok

① a folyamat realizációjának az együttese



együtt ők a stochasztikus folyamat!

② Valószínűségi változók rendezett (időben) serege



n -ed rendű eloszlás fv. (n dimenziós)

eloszlás fv.

$$F_{\xi}^{(n)}\left(\xi_{t_1}, \xi_{t_2}, \dots, \xi_{t_n}, t_1, t_2, \dots, t_n\right) \triangleq$$

$$F_{\xi}^{(n)}(x_1, \dots, x_n, t_1, t_2, \dots, t_n) \triangleq P\left(\xi_{t_1} < x_1, \xi_{t_2} < x_2, \dots, \xi_{t_n} < x_n, t_1, t_2, \dots, t_n\right)$$

• Erősen stationárius folyamat: $F_{\xi}^{(n)}(x_1, \dots, x_n, t_1, \dots, t_n) = F_{\xi}^{(n)}(x_1, \dots, x_n, t_1 + \tau, \dots, t_n + \tau)$

\sim időben invariáns

$\forall \tau, t_n, \forall \{t\}$

időben bármilyen
eltolásra érzéketlen

Várható érték

$$m_{\xi}(t) \Rightarrow E(\xi_t) = \int_{-\infty}^{\infty} x f_{\xi}(x, t) dx$$

erősen stacion. foly. várható érték
időfügtlen

$$m_{\xi}(t) = m_{\xi} \quad \forall t \text{ esetén}$$

erősen stac. foly. \rightarrow ergodikus foly.
vagy ergodikus foly.
keveréke

- ergodikus folyamat

bármelyik realizációból megvalósítható

$$A(\xi) = \lim_{T \rightarrow \infty} \frac{1}{T} \int_{t_0}^{t_0+T} \xi_t dt = m_{\xi}$$

időátlag

jel energiája

• legyen

$$E_{\xi}(t) = \overbrace{E\{\xi_t^2\}}^{\text{várható érték}} = \int_{-\infty}^{\infty} x^2 \cdot f_{\xi}(x, t) dx$$

energia

• Autokorreláció

$$R_{\xi}\{t_1, t_2\} = E\{\xi_{t_1} \cdot \xi_{t_2}\} = \int_{-\infty}^{\infty} \int_{-\infty}^{\infty} x_1 \cdot x_2 \cdot f_{\xi}(x_1, x_2, t_1, t_2) dx_1 dx_2$$

szimmetrikus.

$$R_{\xi}\{(t_1, t_1 + \Delta T)\} = R_{\xi}\{(t_2, t_2 + \Delta T)\} \rightarrow \text{független az abszolút időtől}$$

csak az időtávolságtól függ (ΔT)

persze felt: $\forall \Delta T$ és $\forall(t_1, t_2)$

• Gyengén stacionárius (Wide-Sense-Stationary)

(másoképpen stacionárius \rightarrow gyengén stacionárius)

$$\textcircled{1} \Rightarrow m_{\xi}(t) = m_{\xi} \quad \forall t \quad \text{időfügtlen}$$

$$\textcircled{2} \Rightarrow R_{\xi}(\Delta T) \quad \text{korreláció csak a különbségtől függ}$$

• ha n rendben stac $\rightarrow n-1$

de n rendben stac $\nrightarrow n+1$

• Memória mentes: λ

- forrás

előző betűtől

$$P(\xi_n = X_n | \xi_1 = X_1, \dots, \xi_{n-1} = X_{n-1}) = P(\xi_n = X_n)$$

diszkrét
sűrűség eloszlás

függvény (f)

példa:

$$\#X = 26$$

$$H_0(X) = \sum_{x_i \in X} p_{x_i} \log_2 \frac{1}{p_{x_i}} = \sum_{x_i \in X} \frac{1}{26} = 4,7 \text{ [bit]}$$

entropia

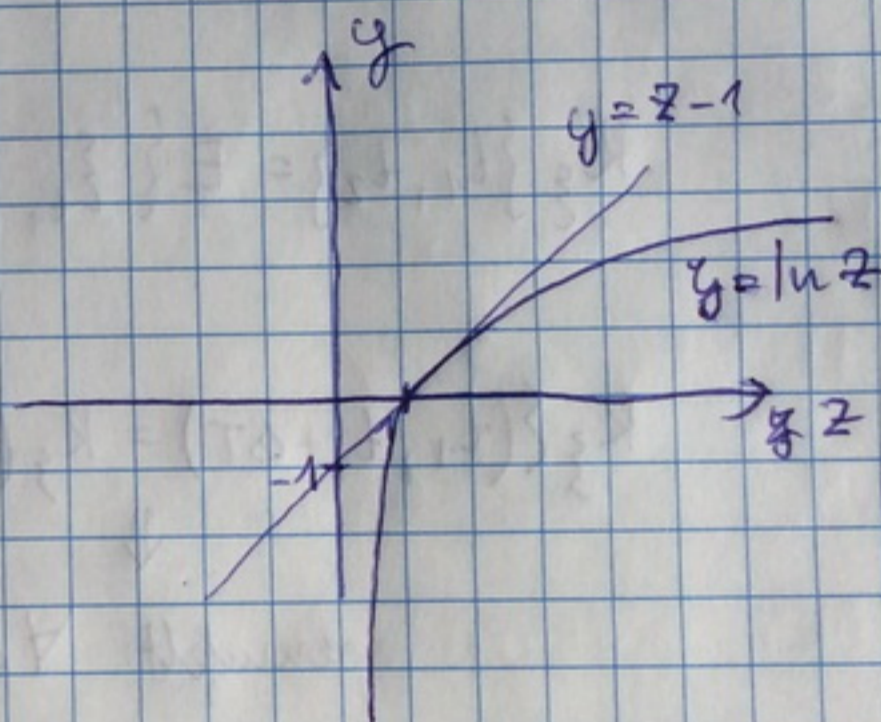
$$\log_a x = \frac{\ln(x)}{\ln(a)}$$

(Tétel: $0 \leq H(X) \leq \log_2(n)$)

$$H(X) - \log_2(n) \leq 0$$

$$\sum_{x_i \in X} p_{x_i} \cdot \log_2 \frac{1}{p_{x_i}} - \sum_{x_i \in X} p_{x_i} \cdot \log_2 n \leq 0$$

mindkét = 1



$$\frac{1}{n \cdot p_{x_i}} = 1$$

$$\Rightarrow p(x_i) = \frac{1}{n}$$

$$\sum p_{x_i} \log_2 \frac{1}{n \cdot p_{x_i}} \leq 0$$

$$\sum p_{x_i} \cdot \ln \left(\frac{1}{n \cdot p_{x_i}} \right) \leq 0$$

$$\frac{1}{\ln 2} \cdot \sum_{x_i \in X} p_{x_i} \cdot \ln \frac{1}{p_{x_i} \cdot n} \leq \frac{1}{\ln(2)} \sum_{x_i \in X} p_{x_i} \left[\frac{1}{n \cdot p_{x_i}} - 1 \right] =$$

$$\frac{1}{\ln(2)} \left[\sum_{x_i \in X} \frac{1}{n} - \sum_{x_i \in X} p_{x_i} \right]$$

német nyelv

$$H(X) = 4,7 \text{ bit}$$

próba $H_2(X) = 3 \text{ bit}$

$$H_0(X) = 1,6 \text{ bit}$$

0 ✓

$$R(X) = H_0(X) - H(X)$$

redundancia

entropia a feltételező kérdéssel a Hagos
 erdelem amire biker hódolai, amelyre
 gyorsan fordul elő.

3. előadás

~ eddig amiket tanultunk

$$F_{\xi}^{(n)}(\xi_1 < x_1, \dots, \xi_n < x_n, t_1, \dots, t_n) = F_{\xi}^{(n)}(\bar{x}, \bar{T}) \quad \forall \Delta T \quad \forall \{T\}$$

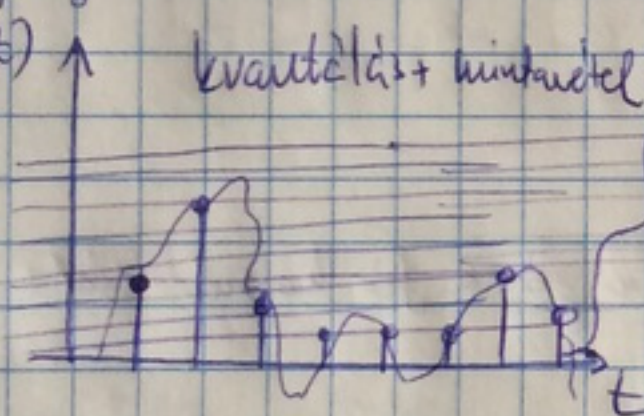
n-ed rend. stationaris: $F_{\xi}^{(n)}(\bar{x}, t_1 + \Delta T, t_2 + \Delta T, \dots, t_n + \Delta T) = F_{\xi}^{(n)}$

WSS $m_{\xi}(t) = m_{\xi} \quad \forall t$ -re, $R_{\xi}(\Delta T)$

erősen stac, ha $\forall n$ -re!

gyengén, ha nem $\forall n$ -re \rightarrow

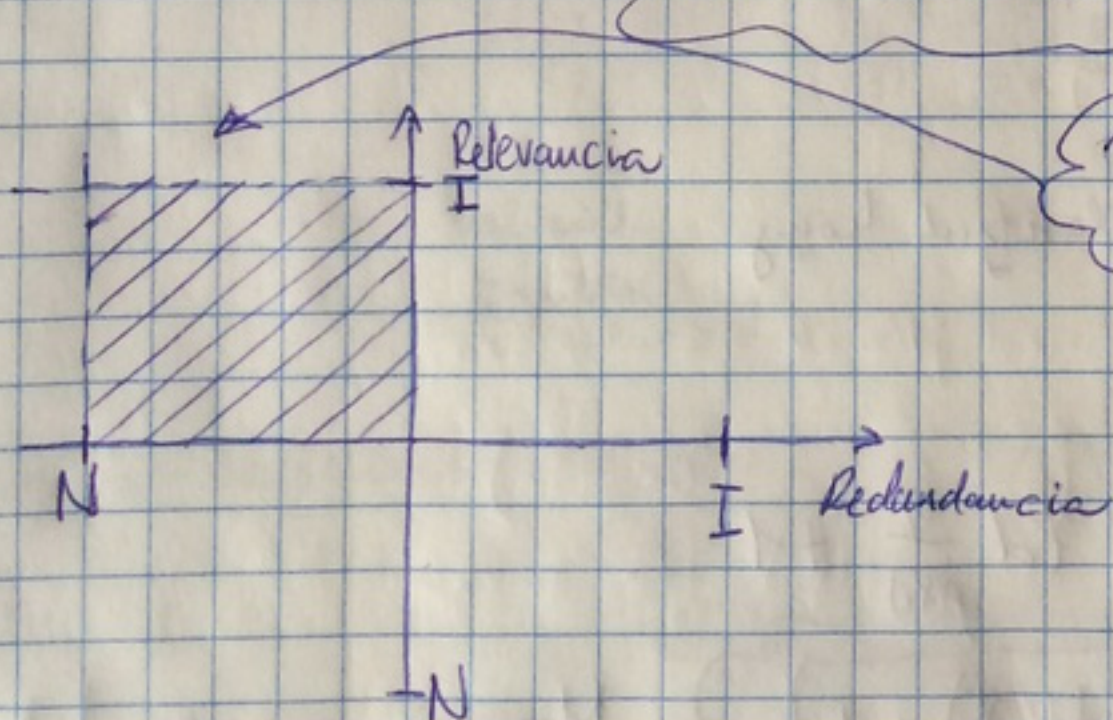
alt) \uparrow kvantálási hirtetés



de! ha elemiszik jel felele' pl. akkor a kvantálási
 telítéskor megy mindig

ha változik időben a várható érték \rightarrow
 nem stationaris

VALÓS VILÁG FOLYAMATAI



relevans információ átírás
 kevés redundanciával

egyenletes
 eloszlás

$$R(X) = H_0(X) - H(X)$$

Redundancia

Cél ennek
 a minimalizálása

háromtöveges:

$$\#X = 26$$

$$p(X)$$

$$H_0(X) = \log 26 = 4,7 \text{ [bit]}$$

$$H_1(X) = 4,1 \text{ [bit]}$$

$$H_{\text{m}}(X) = 1,6 \text{ bit}$$

← csökkent a redundancia

← teljes tövegre (redundancia nélkül)

Ferri's kódolás

- diszkrét, DMS, D+M
discrete memoryless source discrete memory source

- kódolási szabály (Q)

$$Q(x_i) = c_i ; \text{ dehidolhatóság! , fix hosszú kódolás [5 bit]}$$

$$a \rightarrow 00000$$

$$b \rightarrow 00001$$

példa: $X = \{a, b, c, d\}$ $C = \{00, 01, 10, 11\}$

$$p(X) = \left\{ \frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4} \right\}$$

egyszerűes elrendezés esetén jó a fix hosszú kód

- Változó hosszú kódolás:

$$p(X) \quad l_i = l(x_i) \quad L_x = \sum p(x_i) \cdot l(x_i)$$

átlagos
kódhossz

- entropia kódolás \rightarrow $l(x_i)$ -t úgy választjuk hogy

~~$$l(x_i) \leq \log \frac{1}{p(x_i)}$$~~

$$\log \frac{1}{p(x_i)} \leq l(x_i) \leq \log \frac{1}{p(x_i)} + 1$$

$$H(X) \leq L_x < H(X) + 1$$

Shannon I.

Memória-mentes!
forrásra

Shannon-Fano kód \rightarrow a forrás minden szimbóluma (2^{-x})

$$\left(\frac{1}{4}, \frac{1}{8}, \frac{1}{16}, \dots\right)$$

példa: $p(a) = \frac{1}{2}$ $p(b) = \frac{1}{4}$ $p(c) = \frac{1}{8}$ $p(d) = \frac{1}{16}$ $p(e) = \frac{1}{16}$

$2^{(1)}$ $2^{(2)}$ $2^{(3)}$ $2^{(4)}$ $2^{(4)}$

$l_i \Rightarrow$ 1 2 3 4 4

[bit]
hosszi kód
kell

D+M forrás:

\rightarrow A memória:

$$\{X\} \quad p(X_n = x_n | X_1 = x_1, X_2 = x_2, \dots, X_{n-1} = x_{n-1}) = p(x_n | x_1, \dots, x_{n-1})$$

feltételes valószínűség

\rightarrow lehetne feltételes entropia is!

$$H(X_n | X_1, \dots, X_{n-1}) = \sum_{x_1, \dots, x_{n-1} \in X^{n-1}} p(x_1, \dots, x_{n-1}) \cdot \log \frac{1}{p(x_n | x_1, \dots, x_{n-1})}$$

FELTÉTELES ENTROPIA

együttes entropia:

$$H(\bar{X}^n) = H(X_1, \dots, X_n) = \sum_{\bar{X}^n} p(x_1, \dots, x_n) \cdot \log \frac{1}{p(x_1, \dots, x_n)}$$

n darab
val. v. ált.
együttes

együttes valószínűség: $p(x_1, x_2, \dots, x_n) = p(x_1) \cdot p(x_2 | x_1) \cdot p(x_3 | x_2, x_1) \cdot \dots =$

$$\prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1})$$

$$H(\bar{X}^n) = - \sum_{X} \prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1}) \cdot \log \prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1}) =$$

$$\Rightarrow - \sum_{\mathbf{X}} \left(\prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1}) \right) \cdot \underbrace{\log p(x_i)}_{\substack{\text{együtttes val. seg} \\ \text{szükség} \\ x_1, \dots, x_{i-1}}} - \sum p(x_1, \dots, x_n) \cdot \log p(x_2 | x_1) = \dots =$$

$$\sum_{\mathbf{X}} p(x_1, \dots, x_n) \log p(x_n | x_1, \dots, x_{n-1})$$

erős feltételes entropiák

$$H(\bar{X}^n) = H(X_1) + H(X_2 | X_1) + H(X_3 | X_1, X_2) + \dots + H(X_n | X_1, \dots, X_{n-1}) =$$

$$H(\bar{X}^n) = \sum_{i=1}^n H(X_i | X_1, \dots, X_{i-1})$$

1 mintábólunk erős entropia

$$H_n(\bar{X}^n) = \frac{1}{n} H(\bar{X}^n)$$

- Sztochasztikus folyamat entropiája

ha van $\Rightarrow H_{\infty}(X) = \lim_{n \rightarrow \infty} \frac{1}{n} H(\bar{X}^n)$ — együtttes entropia

vagy $\Rightarrow H_{\infty}(X) = \lim_{n \rightarrow \infty} H(X_n | X_1, \dots, X_{n-1})$ ha WSS legalább a folyamat

DMS esetben

$$\hookrightarrow p(x_1, x_2, \dots, x_n) = \prod_{i=1}^n p(x_i)$$

ftlen események

$$H(\bar{X}^n) = \sum_{i=1}^n H(X_i) \rightarrow \text{mert ftlenek az entropiák is?}$$

ha WSS a forrás (időftlen \rightarrow index ftlen)

$$\Downarrow$$

$$H(X_i) = H(X_{i+1}) = \dots = H(X_{i-1})$$

$$H(\bar{X}^n) = n \cdot H(X)$$

Ferrás-kódolás:

atl. kódosm

Shannon I. $H(X) \leq L_x \leq H(X) + 1$

Shannon Fano $P(x_i) = 2^{-k} \quad k \in \mathbb{N}^+$

$$L_x = \frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{8} \cdot 3 + \frac{1}{8} \cdot 4$$

[abcd példára]

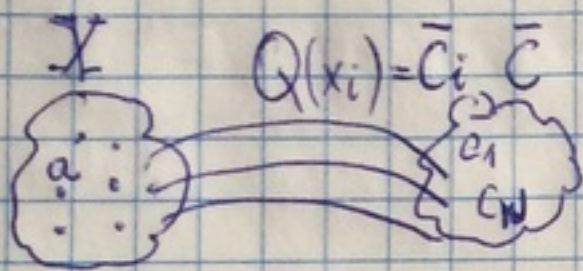
4. előadás

~ leddem ZH

EIB 18¹⁵

tenzt, példa, tétel

Ferrás kódolás



DMS + memória

ferrás ABC
diszkrét

kód ABC
diszkrét

hőkönyv
egyetlen
kapcsolat

pillanat kódoknál kell lenni \rightarrow azonnal
el kell tudjam
dönteni a
ferrás ABC elemét!

$l_i: \bar{C}_i = (c_{i1}, \dots, c_{in})$ legyen $L_x = \sum_{x_i \in X} p(x_i) \cdot l_i$

egy kód
hossza

kódszimbólumok
ahát $[0, 1]$ de lehet
más is!

[Shannon I] $H(X) \leq L_x < H(X) + 1$

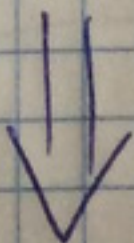
ha $p(x_i) < p(x_j) \Rightarrow l_i > l_j$

entropia kódolás elve ez [Shannon-Fano]

ha $p(x_i) \in 2^{-k_i}$

$\Rightarrow l_i = k_i = \lceil \log_2 \frac{1}{p(x_i)} \rceil$

ez teljesíti-e a Shannon I-et?



$H(X) = \sum_{x_i} p(x_i) \cdot \log_2 \frac{1}{p(x_i)} \rightarrow$ egyenlőség van "alulról"
 ez alá nem tudok menni

$L_x = \sum p(x_i) l_i$
 $l_i = \log_2 \frac{1}{p(x_i)}$

$h_0 = \frac{H(X)}{L_x} \rightarrow$ mindig kisebb, mint 1

hatékonyabb a fenns kódnak

Shannon-Fano \rightarrow minimális ^{átlagos} kód hossz

Példa:

X	p(x _i)	fix hossz
x ₁	1/2	00
x ₂	1/4	01
x ₃	1/8	10
x ₄	1/8	11

$H(X) = \frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{4} \cdot 3 \Rightarrow 1,75$ [bit]

ez pillanat kód!!!

Ⓐ $L(X) = 2$ fix hosszú kód miatt!

eset $h_0 = \frac{1,75}{2} = 0,875$ miért nem 100% \rightarrow nem használhat az a priori ismeretet (a valószínűségeket)

\rightarrow fix hosszú kódot mindig lehet dekodolni!

01|00|11|01|10|00|1

legyen
 x₁ \rightarrow 0
 x₂ \rightarrow 1
 x₃ \rightarrow 00
 x₄ \rightarrow 11

$L_{x_0} = 1 \cdot \frac{3}{4} + 2 \cdot \frac{1}{4} \Rightarrow 1,25$

kisebbség az entropiánál ????



nem dekodolható!

Ⓑ eset

C prefix kód $x_1 \rightarrow 0$ $x_3 \rightarrow 110$
 eset (változóhosszú kód) $x_2 \rightarrow 10$ $x_4 \rightarrow 111$

$\bar{C}_i = (c_{i1} \dots c_{i\ell_i})$ akkor ~~X~~ olyan \bar{C}_j ^{ahol} $\forall \ell_j > \ell_i$, $C_j = (c_{j1} \dots c_{j\ell_j})$

az eleje
 olyan mint
 a másik kód

$$L_x = \frac{1}{2} + \frac{1}{4} \cdot 2 + \frac{1}{4} \cdot 3 = \underline{\underline{1,75}}$$

$$h_{qc} = \frac{1,75}{1,75} = 100\%$$

ez prefix mentes kód \rightarrow dekodálható
 (Shannon-Fano kód)

pillanat kód

D szeparátor be: pl egy vessző!

[comma-code]

$x_1 \rightarrow 0$ elválasztó
 $x_2 \rightarrow 01$
 $x_3 \rightarrow 011$
 $x_4 \rightarrow 0111$

$$L_x = \frac{1}{2} + \frac{1}{4} \cdot 2 + \frac{3}{8} + \frac{1}{2} \Rightarrow 1,875$$

$$h_{qc} = \frac{1,75}{1,875} \rightarrow$$

E {prefix és comma-code}

$x_1 \rightarrow 0$

$$L_x = 1,875$$

$x_2 \rightarrow 10^{\wedge}$ szeparátor

$x_3 \rightarrow 110$

$x_4 \rightarrow 1110$

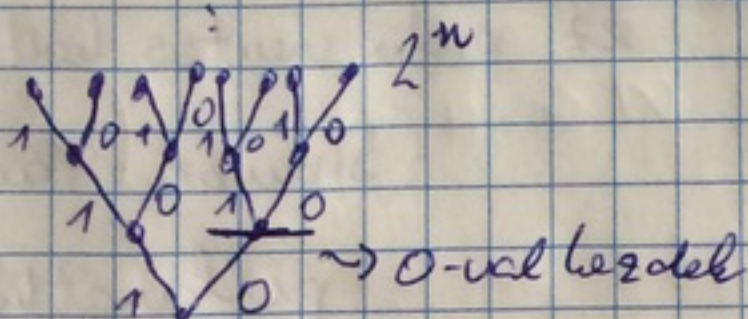
Prefix-kód generálása:

Egy kód prefix \iff ha teljesül a Kraft egyenlőtlenség.

Kraft egyenlőtlenség: $\sum_{i=1}^N 2^{-l_i} \leq 1$ [bináris kódokra igaz]

i -edik kód hossza

bin. fa:

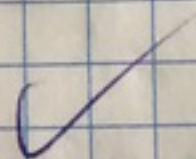


ha elkezdem 0-val \rightarrow lépésenként az ágak



$N - l_i$ szintű részfa hat végük ki egy l_i -hosszú kód szerkesztéséhez

$$\sum_{i=1}^N 2^{N-l_i} \leq 2^N \quad \text{teljes fa!} \quad \rightsquigarrow \quad \boxed{\sum_{i=1}^N 2^{-l_i} \leq 1}$$

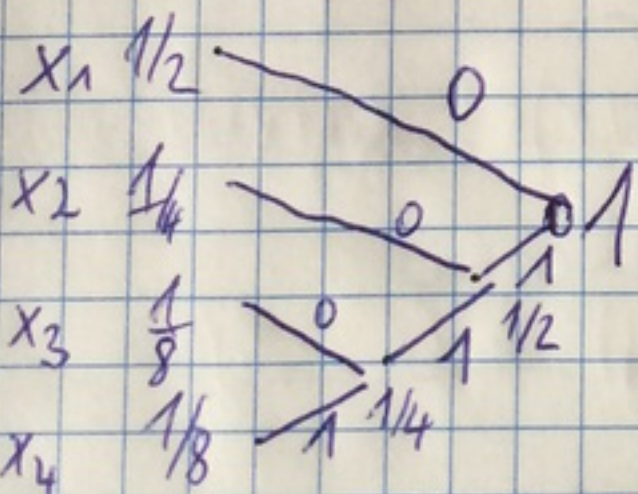


(a teljes fával többet nem vághatok ki)

Kraft.

Huffman:

- ① \rightarrow előfordulási valószínűség szerint sorba rendezés!
- ② \rightarrow bináris fa, 2 legkisebb valószínűségű eseményt kötök össze!

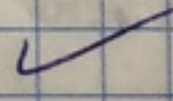


bináris fa

\rightarrow rekurzívum!

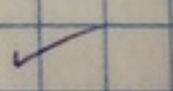
amíg nem csak 1-ből!

$x_1 \rightsquigarrow 0$



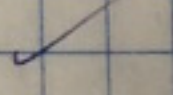
levélgyűjtemény

$x_2 \rightsquigarrow 10$

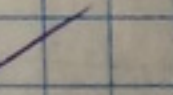


prefix ~~...~~ + Shannon Fano!

$x_3 \rightsquigarrow 110$



$x_4 \rightsquigarrow 111$



DE!!! \rightarrow akkor is működik ha a val. ségek nem 2^{-k_i} szerint oszlanak el!

pl:

x_1	0,4		$x_2 \rightarrow 1$
x_2	0,25		$x_2 \rightarrow 0,0$
x_3	0,2		$x_3 \rightarrow 0,11$
x_4	0,15		$x_4 \rightarrow 0,10$

HUFFMANN

0,5 0,6 0,45

$$L_x = 0,4 + \frac{1}{4} \cdot 2 + \frac{1}{5} \cdot 3 + 0,15 \cdot 3 = 1,95$$

$$H(x) = 0,4 \cdot \log_2 \frac{1}{0,4} + 0,25 \cdot \log_2 \frac{1}{0,25} + 0,2 \cdot \log_2 \frac{1}{0,2} + 0,15 \cdot \log_2 \frac{1}{0,15} =$$

HUFFMANN-hoz kell a valószínűség!

nem jó kevés kódnál, és nagy valószínűség differenciál!

kannáljuk a forráskiterjesztés módszerét!

$x_1 x_1$

$x_1 x_2$

$x_1 x_3$

$x_1 x_4$

$x_2 x_1$

kell ismernünk az eseménypárok val. ségét

2
4 extra van!

ha DHS \rightarrow akkor $p(x_1, x_2) = p(x_1) \cdot p(x_2)$
 nem független
 nem független

$$p(x_1, \dots, x_n) = \prod_{i=1}^n p(x_i)$$

$$H(\bar{X}^n) = H(x_1, \dots, x_n) \stackrel{\text{DHS}}{=} n \cdot H(x)$$

kiterjesztett forrás hoz
 megegyezik $n \cdot H(x)$

stacionárius
 időlen(n)
 nem változik
 $H(x) = H(x_i) \forall i \in n$

$$n \cdot H(x) = H(x_1, \dots, x_n) \leq L_{x_1, \dots, x_n} < H(\bar{X}^n) + 1 \quad | \quad n \text{ darabra}$$

n -darab val. változó
 által generált események
 tartozói kód

$$H(x) \leq L_x \leq H(x) \cdot \frac{1}{n} \rightarrow \text{ha a kiterjesztést növelem}$$

akkor 100% felé tartok!
 ez jó DHS esetben!

MS esetén

$$p(x_1, \dots, x_n) = p(x_1) \cdot p(x_2 | x_1) \cdot p(x_3 | x_2, x_1) \cdot \dots \cdot p(x_n | x_1, \dots, x_{n-1})$$

$$= \prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1})$$

$$H(x_1, \dots, x_n) = -\sum_{i=1}^n \prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1}) \cdot \log \left(\prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1}) \right) =$$

n val. vält.
egysített entropiaja

$$= \sum_{i=1}^n H(x_i | x_1, \dots, x_{i-1})$$

$$H(X)_n = \frac{1}{n} \cdot H(x_1, \dots, x_n)$$

1 szimbólumra
eső entropia

ha $n \rightarrow \infty$

$$H_\infty(X) = \lim_{n \rightarrow \infty} \frac{1}{n} H(x_1, \dots, x_n)$$

↓
stochasztikus
folyamat

végelen sokszert
val. vält. sorozat!

? ha létezik

MS esetén

$$p(x_1, \dots, x_n) = p(x_1) \cdot p(x_2 | x_1) \cdot p(x_3 | x_2, x_1) \cdot \dots \cdot p(x_n | x_1, \dots, x_{n-1})$$

$$= \prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1})$$

log/szorzat = összeg (log)

$$H(x_1, \dots, x_n) = -\sum_{i=1}^n \prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1}) \cdot \log \prod_{i=1}^n p(x_i | x_1, \dots, x_{i-1}) =$$

n val vált.

együttes entropia

$$= \sum_{i=1}^n H(x_i | x_1, \dots, x_{i-1})$$

$$H(X)_n = \frac{1}{n} \cdot H(x_1, \dots, x_n)$$

ha $n \rightarrow \infty$

1 változó ér? ha letezik

$$H_\infty(X) = \lim_{n \rightarrow \infty} \frac{1}{n} H(x_1, \dots, x_n)$$

↓
stochasztikus
folyamat

végelen rendezett
vél. vált. sorozat!

1 szimbólum
erő entropia

~~$H(X)_n$~~ ~~$H(X)_n$~~

$$H_\infty(X) = \lim_{n \rightarrow \infty} H(x_n | x_1, \dots, x_{n-1})$$

1 szimbólum
erő entropia
egy stochasztikus
folyamatnál!

Ⓐ Gallager bizonyítás:

• $H(x_n | x_1, \dots, x_{n-1})$ monoton csökkenő!

$$H(x_n | x_1, \dots, x_{n-1}) \leq H(x_n | x_2, \dots, x_{n-1}) = H(x_{n-1} | x_1, \dots, x_{n-2})$$

kevesebb előismeret
nagyobb bizonytalanság!
nagyobb entropia

ha a folyamat
legalább n-ed rendben
stacionárius legyen
(eltolásra érhető)

(B)

$$H_n(X) \geq H(X_n | X_1 \dots X_{n-1})$$

$$H_n(X) = \frac{1}{n} \cdot \left[\overset{\text{def!}}{H(X_1 \dots X_n)} \right] = \frac{1}{n} \cdot \sum_{i=1}^n H(X_i | X_1 \dots X_{i-1}) \geq \frac{1}{n} \cdot \overset{\text{velem. n-rek.}}{\downarrow} H(X_n | X_1 \dots X_{n-1}) \quad \text{(A) miatt}$$

(C)

$H_n(X)$ mon. csökkenő

$$H_n(X) = \frac{1}{n} \left[\underbrace{H(X_1 \dots X_{n-1})}_{n-1 \text{ var változó}} + \overset{\text{következő}}{H(X_n | X_1 \dots X_{n-1})} \right] = \frac{1}{n} \left[(n-1) \cdot H_{n-1}(X) + \dots \right]$$

$$H(X_n | X_1 \dots X_{n-1}) \leq \frac{n-1}{n} \cdot H_{n-1}(X) + \frac{1}{n} \cdot H_n(X) \Rightarrow$$

$$\frac{1}{n} \cdot \sum_{i=1}^n H(X_i | X_1 \dots X_{i-1}) = H_n(X)$$

$$\Rightarrow \frac{n-1}{n} \cdot H_n(X) \leq \frac{n-1}{n} \cdot H_{n-1}(X) \quad \text{mon. csökkenő} \checkmark$$

$$1 \rightarrow (n-1) \quad n \rightarrow (n+j)$$

$$H_{n+j}(X) = \frac{1}{n+j} \left[H(X_1 \dots X_{n-1}) + \sum_{i=n}^{n+j} H(X_i | X_1 \dots X_{i-1}) \right] \leq \frac{1}{n-j} \cdot H(X_1 \dots X_{n-1}) + \frac{j+1}{n+j} H(X_n | X_1 \dots X_{n-1})$$

$$\lim_{j \rightarrow \infty} H_{n+j}(X) \leq H(X_n | X_1 \dots X_{n-1})$$

$$\lim_{\substack{n \rightarrow \infty \\ j \rightarrow \infty}} H_{n+j}(X) \leq \lim_{n \rightarrow \infty} H(X_n | X_1 \dots X_{n-1})$$

+ stochasztikus folyamat!

erős egyenlőség csak akkor igazolható ha egyenlőség

$$\lim_{n \rightarrow \infty} H_n(X) \geq \lim_{n \rightarrow \infty} H(X_n | X_1 \dots X_{n-1})$$

ez akkor van ha erősen stoc. a folyamat

ha van forrás kiképzés:

$$H(X_1, \dots, X_n) \leq L_{X_1, \dots, X_n} \leq H(X_1, \dots, X_n) + 1$$

$$H_n(X) \leq L^*x \leq H_n(X) + \frac{1}{n}$$

ha $n \rightarrow \infty \rightarrow L^*x = H_n x$ (ha teljesen ismerem a folyamatot?)

azatl. ködhossz elvehet az entropiáig.

$$L_x = H_{\infty}(X)$$

optimum

apriori ismerem kell

a forrást!

L-Z kódolás (deupel-Ziv)

- apriori ismeretek nélkül is működik és közelíti az optimumot
- UNIX-ban ez működik

elve: könyvtárát akarok vinni, ehhez felelt egy könyvtárat is csak a cívet kell megadnom.

a könyvtár:	tár hely	tartalom	kód	tartalom	$L_x = 5$ fix hosszú kódok
1	0001	0	00000	0	
2	0010	1	00001	1	
3	0011	11	00101	1	
4	0100	00	00010	0	
	0101	10	00100	0	
	0110	100	01010	0	

itt van az '1'

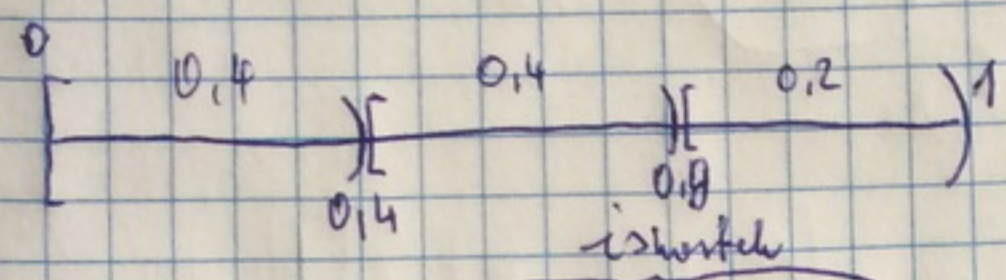
és így tovább

0,1,11,00,10
 ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓
 [01110010100111001] bitorozat

→ Nem kell hozzá ismernem a priori az eloszlást.

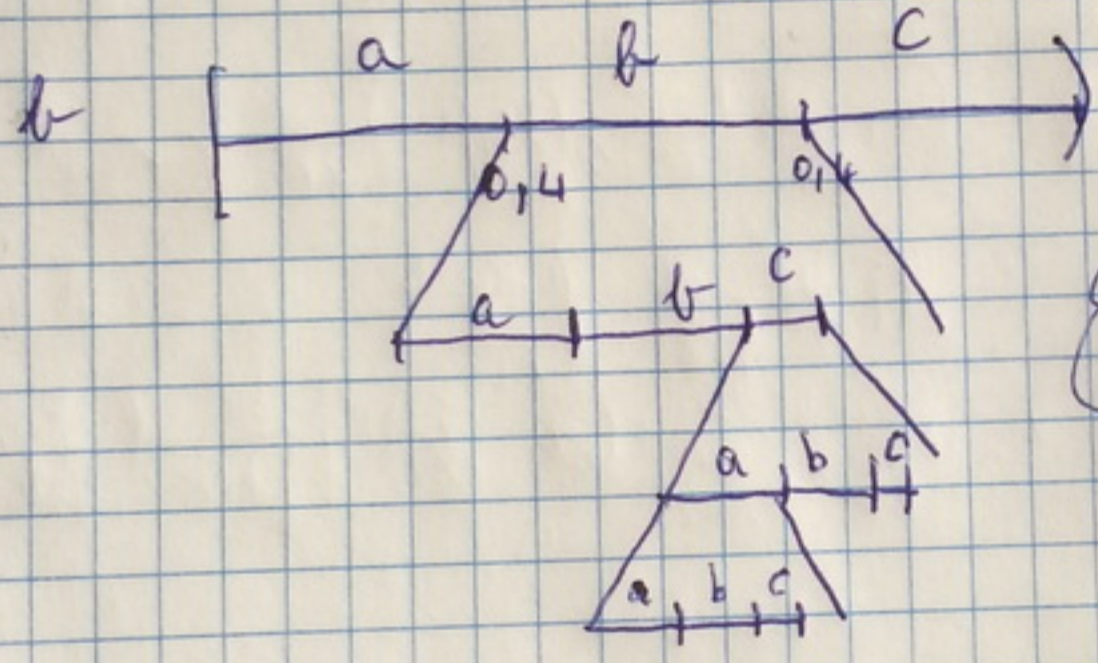
Aritmetikai kódolás:

- o kell a $P(x)$
- o tart az optimális Huffman kódhoz
- o ritka sorozat → rövid kód, gyakori sorozat → rövid kód



$$X = \{ a, b, c, p(a) = 0.4, p(b) = 0.4, p(c) = 0.2 \}$$

[b, c, a] árendő sorozat



elég 1. rendben ismerni az eloszlást!
(még nem feltétlen kell jónak kiterjesztés)

$0.75 = 0.11$ (with $2^{-1} 2^{-2}$ above it) bca

ezt különbözít mert ez egyértelműen meghatároz egy rémintervallumot.

de változó hosszú a kód
kell mindenhepp egy stop szimbólum p!

~~nem prefix nem tart~~

1. ZH eddig

6. előadás

$P(x)$ a forrás eloszlása (nem ismerjük, de becslés tudjuk)

$Q(x)$ -zel becsljük a $P(x)$ eloszlást

relatív entropia:
(Kullback-deibler távolság) $\sum p(x_i) \cdot \log \frac{p(x_i)}{q(x_i)}$

Def: A relatív entropia:

$$D(P(x) \parallel Q(x)) = \sum_{x \in X} p(x_i) \log \frac{p(x_i)}{q(x_i)}$$

távolság

2 eloszlás mennyire hasonlít egymásra! ha $p(x_i) = q(x_i) \rightarrow$ távolság = 0

$$H(x) + D(p \parallel q) \leq L_x < H(x) + D(p \parallel q) + 1$$

Shannon I.

ahol $D(p \parallel q)$

p és q eloszlás
Kullback-deibler
távolság

... forráskódolás sége ...

a-posteriori entropia:

$$H(X|Y) = H(X) - \underbrace{I(X;Y)}_{\text{val. vált.}}$$

átlagos kölcsönös információ (x,y-branch megrán)

$$\text{és } H(X|Y) \leq H(X)$$

def: kölcsönös információ:

$$I(x_i, y_i) = \log \frac{p(x_i|y_i)}{p(x_i)}$$

megfigyelve y_i -t

minis kölcsönös információ

ha $p(x_i)$ független $p(y_i)$ -től

akkor $p(x_i|y_i) = p(x_i)$

$$\log 1 \Rightarrow I(x_i, y_i) = 0$$

Bayes x_i, y_i egymással valószínűség / $p(x_i, y_i)$

$$\downarrow \Rightarrow \log \frac{p(x_i, y_i)}{p(x_i) \cdot p(y_i)}$$

Átlagos kölcsönös információ:

$$I(X, Y) = \sum_x \sum_y p(x, y) \cdot \log \frac{p(x, y)}{p(x) \cdot p(y)} = \sum_x \sum_y p(x, y) \log \frac{p(x|y) \cdot p(y)}{p(x) \cdot p(y)} =$$

$$\underbrace{\sum_x \sum_y p(x, y) \log \frac{1}{p(x)}}_{H(X)} - \underbrace{\sum_x \sum_y p(x, y) \log \frac{1}{p(x|y)}}_{H(X|Y)} \quad (\log(ab) = \log a + \log b)$$

$$= H(X) - H(X, Y) = H(Y) - H(Y|X) = D(p(x, y) \parallel p(x) \cdot p(y)) \quad [\text{bit}]$$

Csatorna kapacitás:

$$C = \max_{p(x)} I(X, Y) \quad \begin{matrix} \text{bit/} \\ \text{csatorna} \\ \text{kanál} \end{matrix} \rightarrow \begin{matrix} \text{bit/s} \\ \text{Bitrate} \end{matrix}$$

Összes lehetséges beosztás
előrelételetti max.

Ha több
Ha kevesebb

Shannon II. csatornakiapacitás valószínűségi tétel:

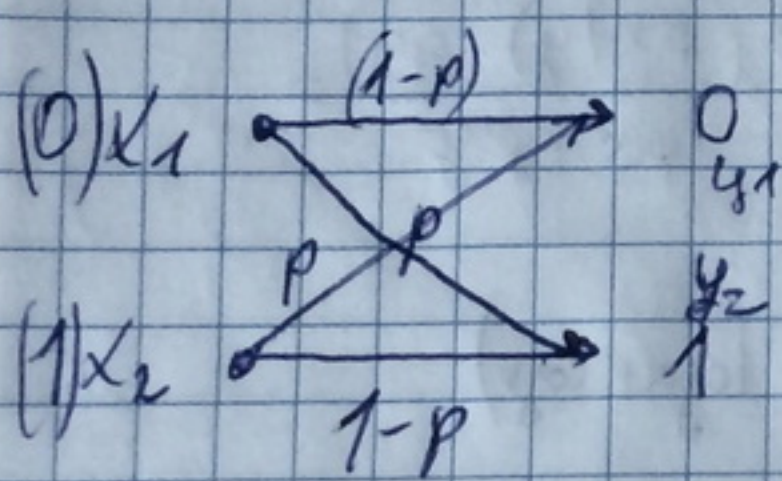
ha: $H(X) < C$ akkor $\exists \Omega(X) = X$
 Perror $\rightarrow \emptyset$ ha $H(X') < C$
 hiba val. s \acute{e} g.

M \acute{e} rv \acute{e} si Shannon II.:

k -s blokk $X \rightarrow N \cdot X'$; $\lim_{k \rightarrow \infty} \frac{k}{N} < C$ Perror $\rightarrow \emptyset$
 k b \acute{e} tr \acute{e} s l \acute{e} tsz \acute{e} l n n \acute{e} rv \acute{e} l \acute{e} s

DMC - discrete memoryless channel

1) BSC

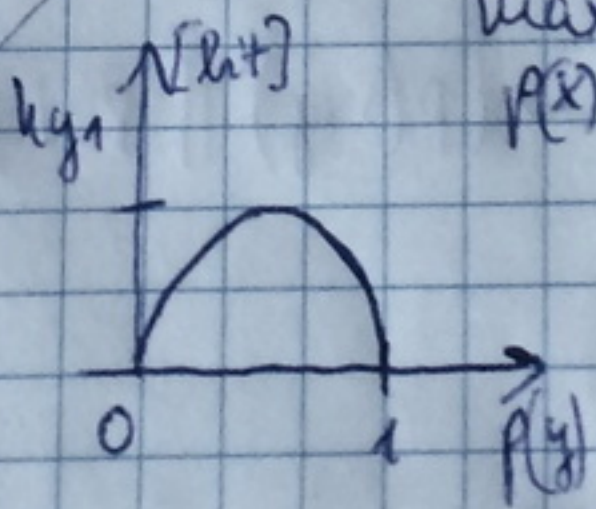


p valószínűséggel hibézik
 $1-p$ valószínűséggel nem hibézik

$p(x) \rightarrow x_1$ $p(y) \rightarrow y_1$
 $1-p(x) \rightarrow x_2$ $1-p(y) \rightarrow y_2$

$$C_{BSC} = \max_{p(x)} [H(Y) - H(Y|X)]$$

H_Y
 lin. entropia
 f \acute{u} .



$\max_{p(x)} H(Y) = 1$ [bit], ha $p(x) = 1/2 \Rightarrow p(y) = 1/2$
 egyenletes eloszlás

$$H(Y|X) = \sum_x \sum_y p(x,y) \cdot \log_2 \frac{1}{p(y|x)} = p(x) \cdot \left[(1-p) \cdot \log_2 \frac{1}{1-p} + p \cdot \log_2 \frac{1}{p} \right] +$$

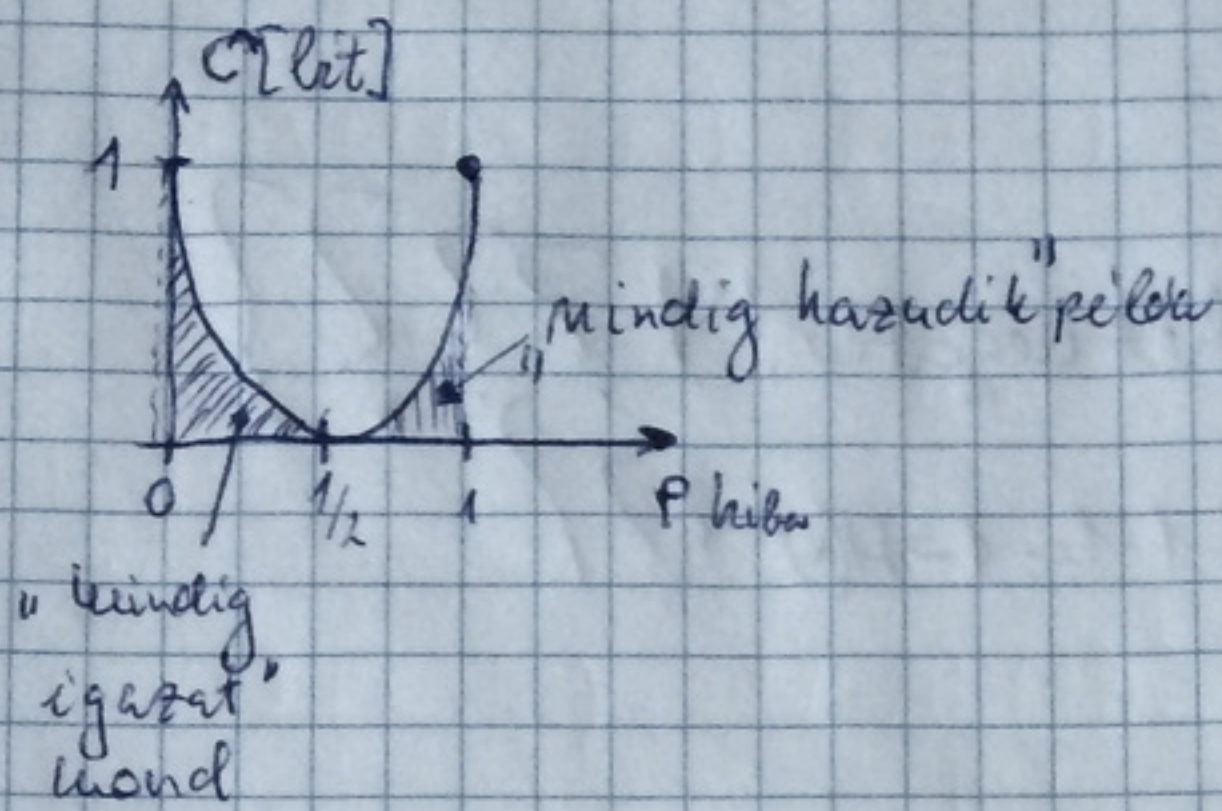
$$\frac{1-p(x)}{x_2} \cdot \left[p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p} \right] =$$

$$= p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p}$$

nem függ a forrás

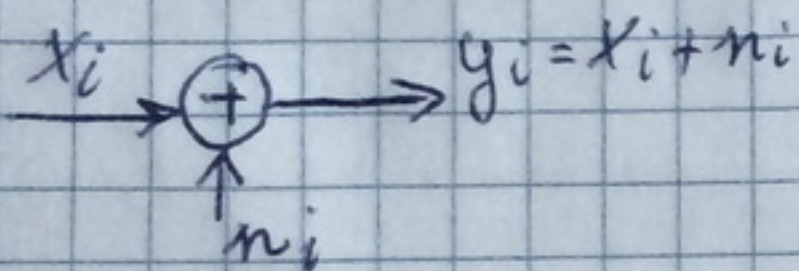
eloszlástól! csak p hibeválts \acute{e} g \acute{e} lt!

$$C_{BSC} = \max [H(Y) - H(Y|X)] = 1 - h_p$$



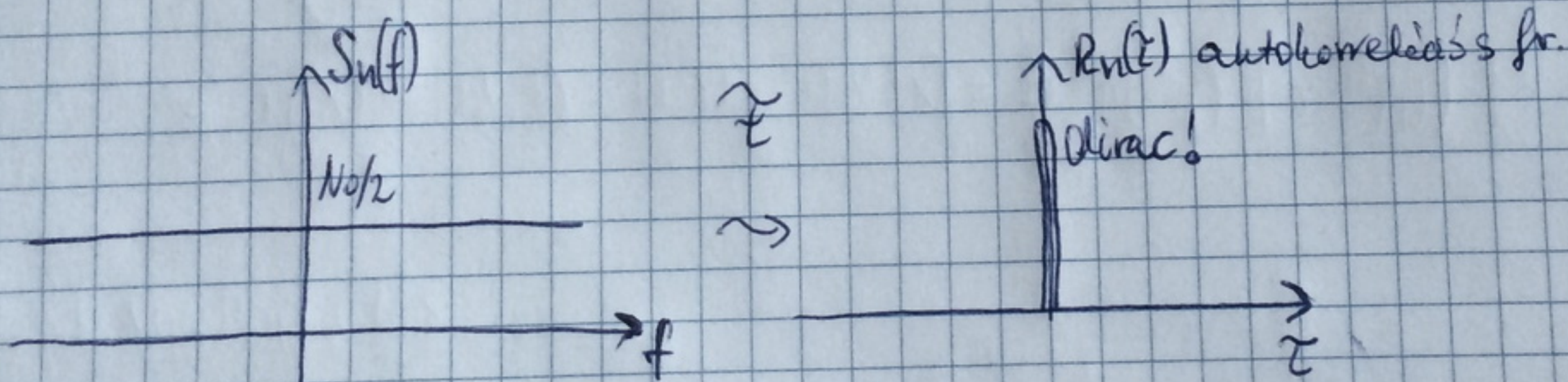
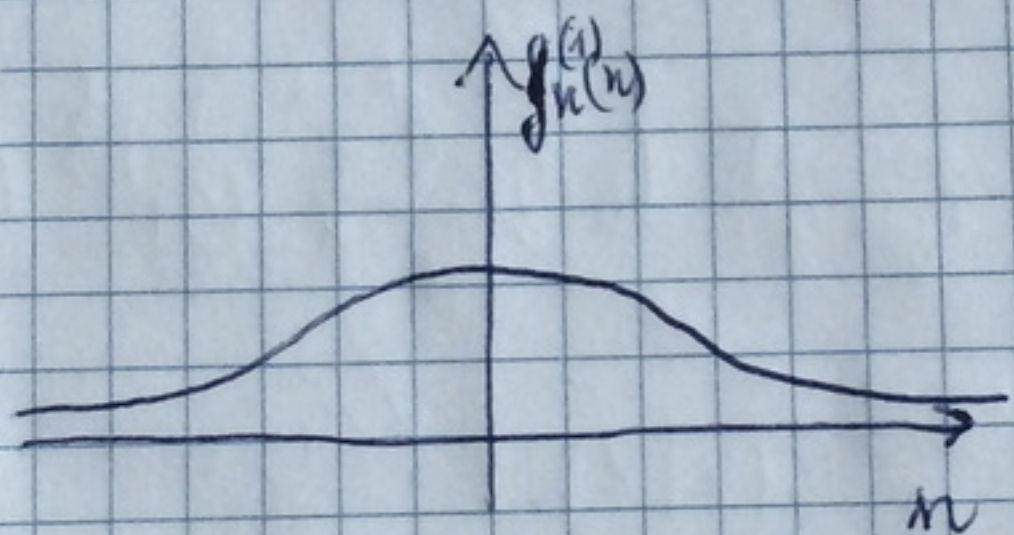
ha $\frac{1}{2}$ akkor foglalom sincs az információról, $C=0$

• DMC eset, D-AGWN additív white Gaussian Noise.



~~$f_n^{(1)}$~~ $f_n^{(1)} = G(\mu_n = 0; \sigma^2 = N_0/2; \varphi = 0) = \frac{1}{\sqrt{2\pi} \cdot \sigma_n} \cdot \exp\left[-\frac{n^2}{2\sigma_n^2}\right]$

előrendű sűrűségf.



$$N_0 = \frac{h \cdot f}{e^{hf/kT_0} - 1}$$

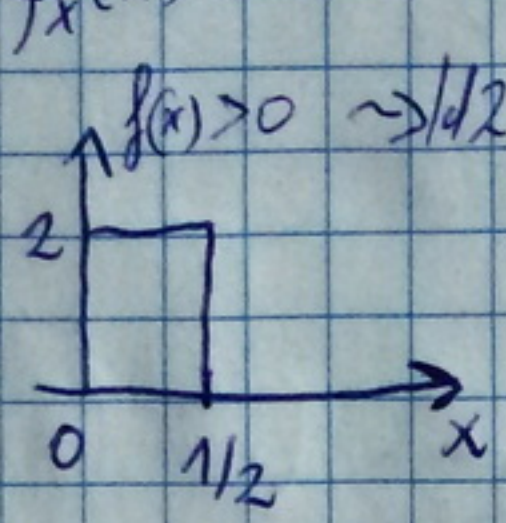
Kell az új fogalom!

diszkrét \rightarrow folytonos miatt

differenciális entropia:

$$H(X) = \int_{-\infty}^{\infty} f_X(x) \text{ld. } \frac{1}{f_X(x)} dx$$

lehet negatív!!! ???



$f(x) > 0 \rightarrow 1/2^{-1} = -1 \cdot 1 = -1 = H(X) ???$

7. előadás

LOTTO

$$C \triangleq \max_{p(x)} I(X, Y) \quad \begin{matrix} \text{[bit/sad. n. annálet]} \\ \text{átlalában [bit/s]} \end{matrix}$$

közös információ

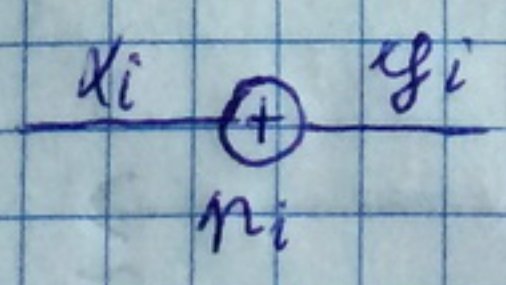
• BSC csatorna:

$$C = 1 - h(p)$$

$p =$ hibaváltsátság

DMC - discrete memoryless channel!

D-AGWN:
diszkrét idő
de folyt. értékű

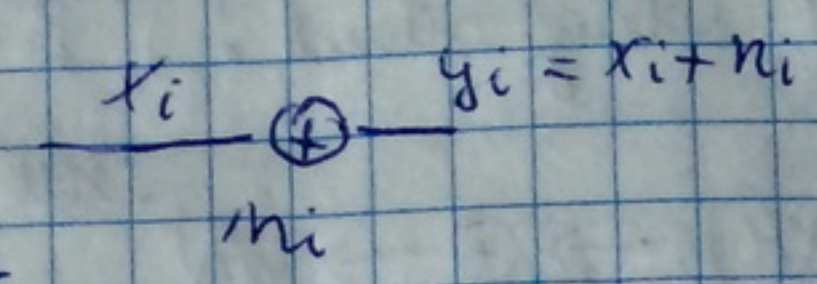


$$H(X(\pm)) = \int_{-\infty}^{\infty} f_X(x) \cdot \text{ld. } \frac{1}{f_X(x)}$$

(folytonos val. változóra az entropia)

$$C \triangleq \max_{p(x)} D(p(x,y) \parallel p(x)p(y)) = \max_{p(x)} [H(X) - H(X|Y)] = \max [H(Y) - H(Y|X)]$$

apostériori entropia (Gauss lesz!)



n_i tennitűs zajra
 $G_n(\mu_n=0, \sigma_n, \rho=0)$ Gauss folyamat
 $\tau=0 \rightarrow$ dirac

emnek az entropiája:

$$H(n) = - \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_n} \cdot \exp\left[-\frac{n^2}{2\sigma_n^2}\right] \cdot \ln \frac{1}{\sqrt{2\pi}\sigma_n} \exp\left[-\frac{n^2}{2\sigma_n^2}\right] dn$$

teljes valóság
 $dn=1$

ld helyett ln legyen

$$= \frac{1}{\ln 2} \int_{-\infty}^{\infty} \frac{1}{\sqrt{2\pi}\sigma_n} \exp\left[-\frac{n^2}{2\sigma_n^2}\right] \left[\ln \frac{1}{\sqrt{2\pi}\sigma_n} - \frac{n^2}{2\sigma_n^2} \right] dn$$

$$= \frac{1}{2} \ln(2\pi e \cdot \sigma_n^2)$$

D-AGWN esetben! \rightarrow

X, folyt. ért. val. változó, Gauss eloszlással!

$$C \triangleq \max (H(Y) - H(Y|X)) =$$

$$f_x(x) = G(\mu=0, \sigma_x, \rho)$$

$$= \max_{p(x)} (H(X+N) - H(N)) \quad (\text{mert } y_i = x_i + n_i) \quad \text{max akkor ha } x_i \text{ is Gauss eloszlás}$$

$$P_{avg} = \left[\lim_{K \rightarrow \infty} \frac{\sum_{k=1}^K x_k^2}{K} \right] \cdot \frac{1}{K} = \sigma_x^2$$

$$\rightarrow = \frac{1}{2} \ln(2\pi e (\underbrace{\sigma_x^2}_{P_{avg}} + \sigma_n^2)) - \frac{1}{2} \ln(2\pi e \cdot \sigma_n^2) =$$

$$= \frac{1}{2} \ln \left(\frac{2\pi e (\sigma_x^2 + \sigma_n^2)}{2\pi e \cdot \sigma_n^2} \right) = \frac{1}{2} \ln \left(\frac{\sigma_x^2 + \sigma_n^2}{\sigma_n^2} \right) =$$

$$\frac{1}{2} \ln \left(1 + \frac{\underbrace{\sigma_x^2}_{P_{avg}}}{\underbrace{\sigma_n^2}_{N_0/2}} \right) = \frac{1}{2} \ln \left(1 + \frac{P_{avg}}{N_0/2} \right)$$

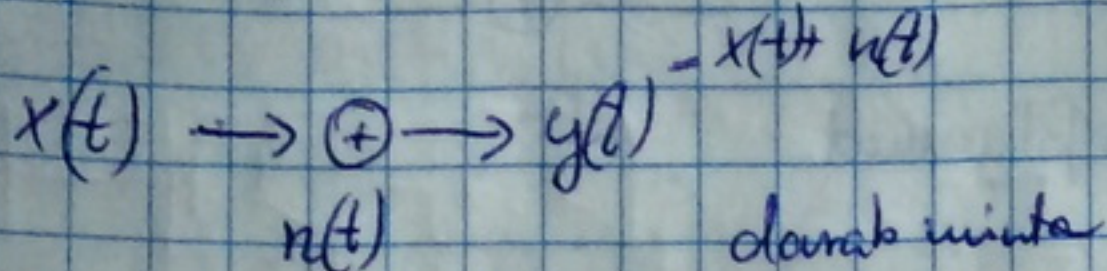
AGWN-nél

$$C = \frac{1}{2} \ln \left(1 + \frac{P_{avg}}{N_0/2} \right) \quad [\text{bit/s}]$$

AGWN

→ folytonos időben, AGWN esetében!
ma's

T ideig adunk! , B sávkorláti jelet, PAVG
korlátos átlag telj.



$T_{\text{mintaveteli idd}} \leq 1/(2B) \rightarrow \frac{T}{T_m} = k \rightarrow T_m = \frac{T}{k} = \frac{1}{2B} \rightarrow \boxed{k = 2B \cdot T}$
darab minták

$C \triangleq \lim_{T \rightarrow \infty} \frac{1}{T} \max_{P(x)} I(x(t), y(t)) = \lim_{T \rightarrow \infty} \frac{1}{T} \max_{P(x)} \sum_{i=1}^k I(x_i, y_i) \stackrel{?}{=} \uparrow$

$x(t) = [x_1 \dots x_k]$

legjobb WSS
és korreláltak!

WSS miatt

$y(t) = [y_1 \dots y_k]$

$n(t) = [n_1 \dots n_k]$

$= \lim_{T \rightarrow \infty} \frac{1}{T} \max_{P(x)} \underbrace{k}_{\text{és a D-AGWN csatormáé}} I(x, y) = \lim_{T \rightarrow \infty} \frac{1}{T} \cdot \underbrace{k}_{\text{Trinns}} \cdot \underbrace{\text{ld} \left(1 + \frac{\text{PAVG}}{No/2} \right)}_{\text{D-AGWN } \sigma_x^2}$

folgt. AGWN

$C = B \cdot \text{ld} \left(1 + \frac{\text{PAVG}}{2B \sigma_n^2} \right) = B \cdot \text{ld} \left(1 + \frac{\text{PAVG}}{2B \sigma_n^2} \right)$

2-dimenzionos!

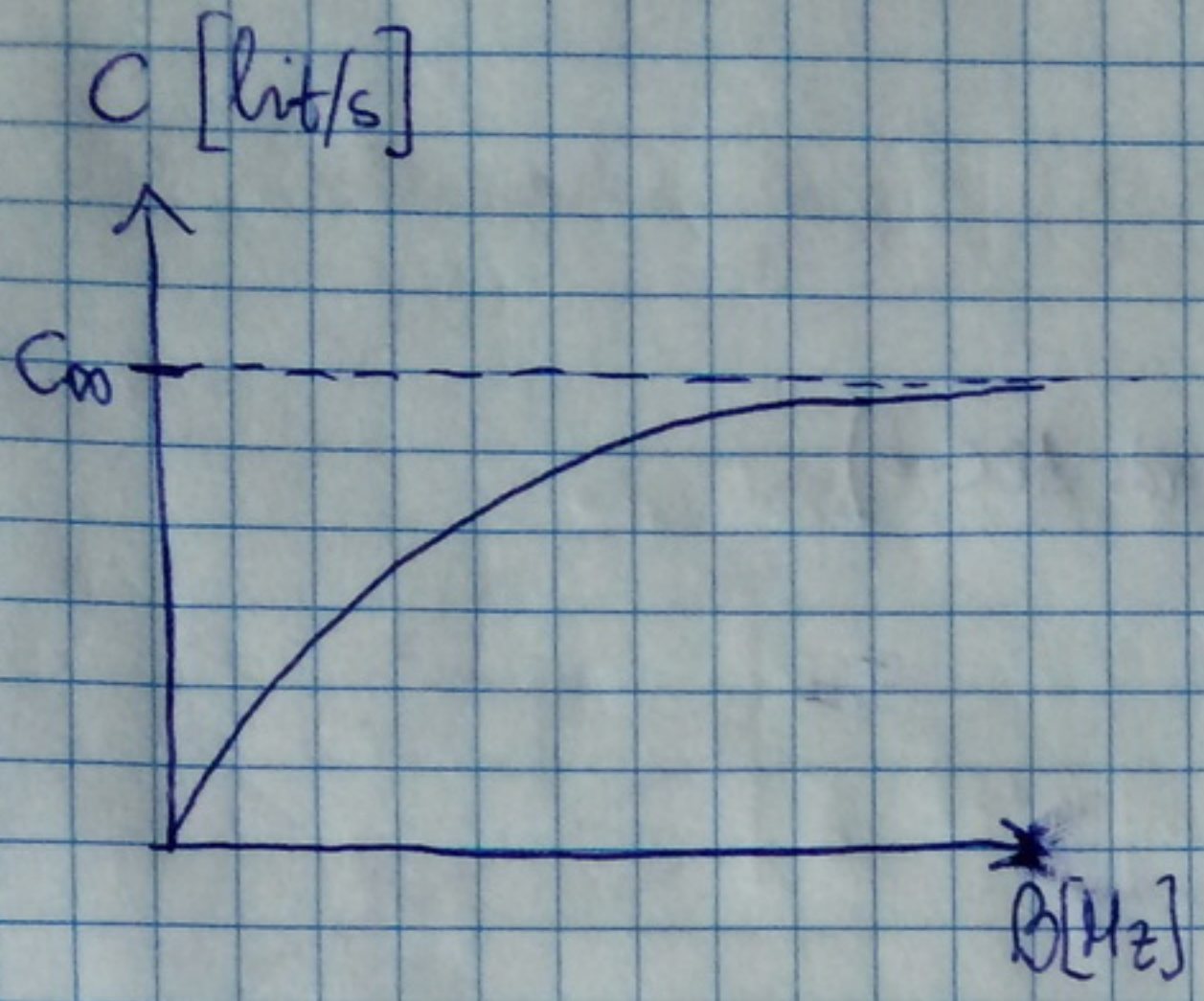
$\text{PAVG} = \lim_{T \rightarrow \infty} \frac{1}{T} \int_0^T E\{x(t)^2\} dt = \lim_{T \rightarrow \infty} \frac{1}{T} \sum_{k=1}^k E\{x_k^2\} \stackrel{\text{WSS}}{=} \lim_{T \rightarrow \infty} \frac{1}{T} k \cdot E\{x^2\} = 2B \cdot \sigma_x^2$
(sávkorlátozva)

$\sigma_x^2 = \frac{\text{PAVG}}{2B}$

$C = B \cdot \text{ld} \left(1 + \frac{\text{PAVG}}{B \cdot No} \right) \text{ [bit/s]}$

AGWN
sávkorlátoz B
T ideig

$C_{\infty} = \frac{\text{PAVG}}{No} \cdot \text{ld} e = \frac{\text{PAVG}}{No \cdot \ln 2}$
ha lenne végtelen felhő



normalizált C : $[\text{bit/s}/\text{Hz}] = C/B$

$P_{\text{avg}} = E_b \cdot C$
 átlagenergia

$\frac{C_{\text{AGWN}}}{B} = \log_2 \left(1 + \frac{E_b \cdot C}{B \cdot N_0} \right) = \log_2 \left(1 + \frac{E_b}{N_0} \frac{C}{B} \right)$

$2^{C_{\text{AGWN}}/B} = 1 + \frac{E_b}{N_0} \frac{C}{B} \Rightarrow \frac{E_b}{N_0} = 2^{C/B} - 1$

8. előadás:

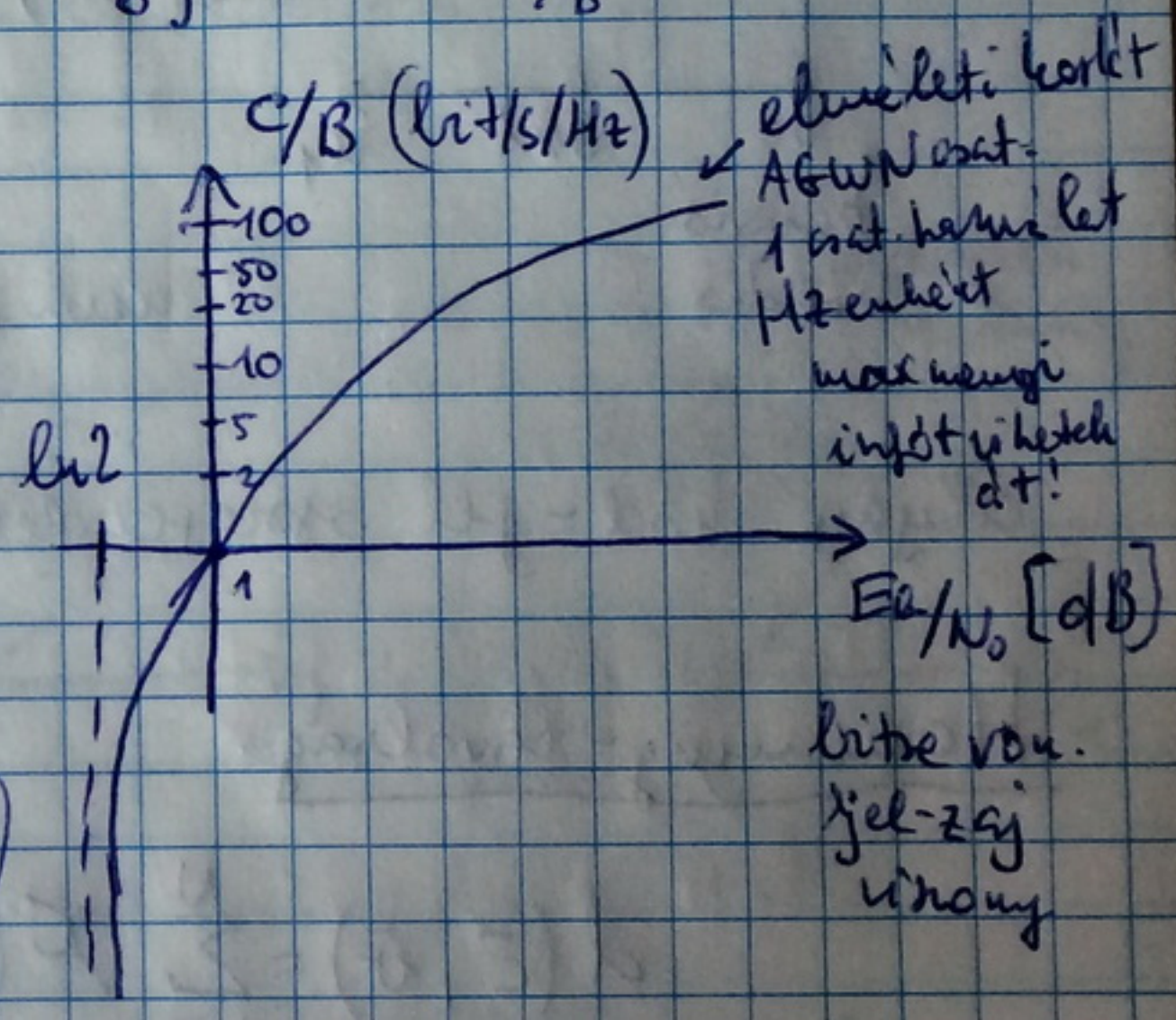
~~$\frac{E_b}{N_0} = \exp \left[\frac{C}{B} \cdot \log_2 \left(1 + \frac{E_b}{N_0} \frac{C}{B} \right) \right]$~~

$\frac{E_b}{N_0} \approx \exp \frac{1}{\ln 2} \left[\frac{C}{B} \cdot \log_2 \left(1 + \frac{E_b}{N_0} \frac{C}{B} \right) \right]$

ha $C/B \rightarrow \infty$

ha $C/B \rightarrow 0$

$\frac{E_b}{N_0} \Rightarrow \ln 2$
 (-1.6 dB)



Shannon II tetele:

amíg $R < C \rightarrow \exists$ olyan Ω , hogy $P_e \rightarrow 0$
 bitáram sebessége kapacitás
 operátor
 Forrás közt Forrás közt

ha $K \xrightarrow{\Omega} N > K$
 szimbólum ↓
 inkább N-et

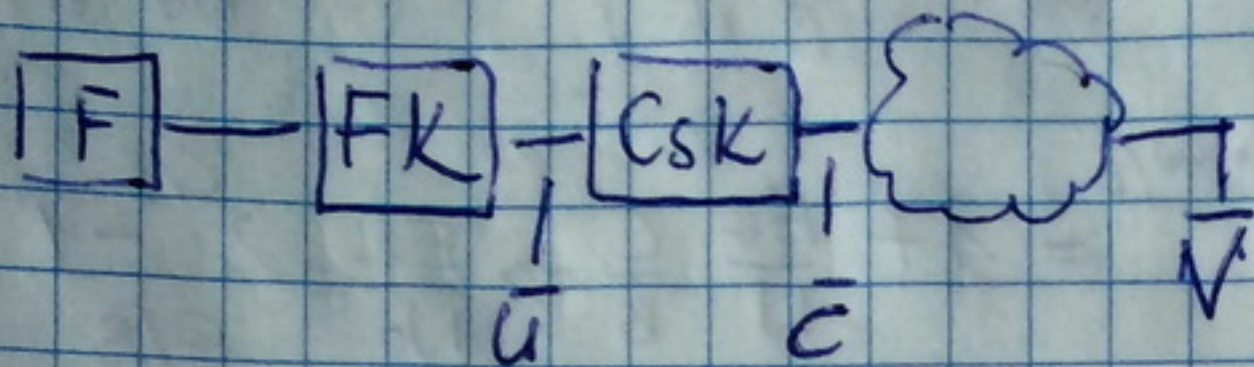
$\lim_{K \rightarrow \infty} \frac{K}{N} < C ; P_e \rightarrow 0$ [1s-re vonatkoztatva van]

$\frac{K}{N} < 1$ erős feltétel !!

Hibajavító kódolás: (N, K, q)

(error correction coding)

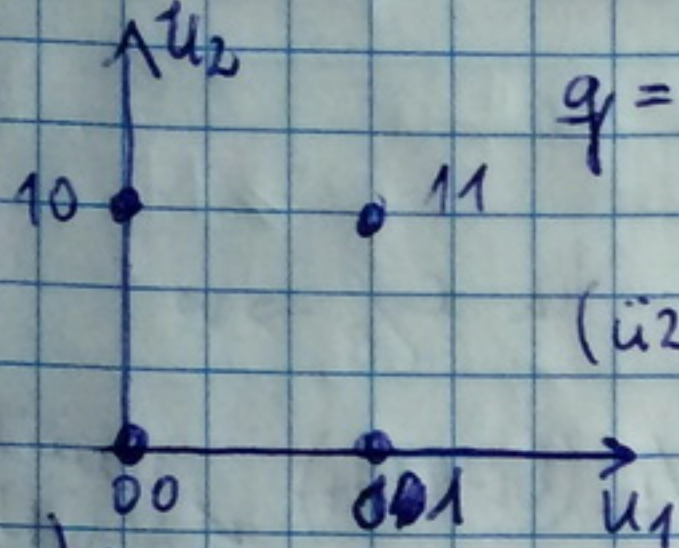
érték halmaz (forrás ABC-e)



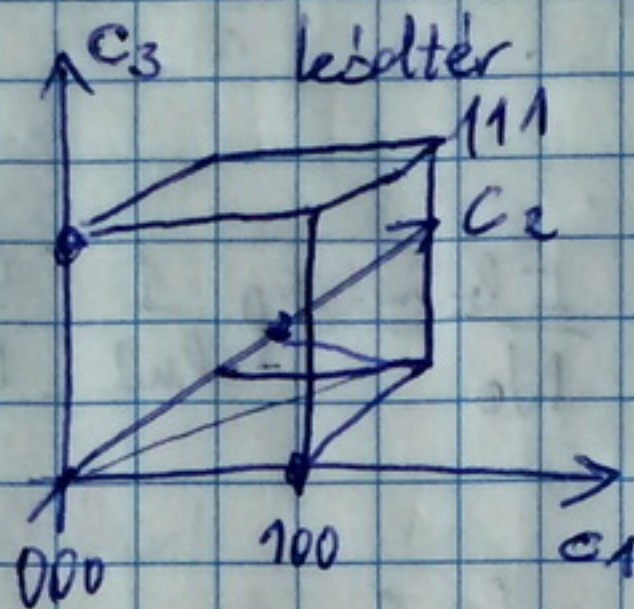
$$\bar{u} = [u_1 \ u_2 \ \dots \ u_k]$$

$(N > K)$

$$q = 2, K = 2, N = 3$$



(üzenet-tér) →



nem értékes olyan összerendelés → 00 → 000
01 → 001

olyan kód-jel összerendelés kell, amely térben távol van egymástól!

Hamming-távolság:

$$d(\bar{c}, \bar{v}) = \sum_{i=1}^N \chi(c_i \neq v_i) \rightarrow 2 \text{ vektor } d(\bar{c}, \bar{v}) = \sum c \text{ hol különböznek!}$$

$$d_{\min} = \min_{\substack{i=j \\ i \neq j}} d(c_i, c_j) \rightarrow \text{érveles kódzavarok közt}$$

minimális Hamming távolság.

döntő
vett jel
→ kell amire döntök

$$D(\bar{v}) = \bar{c}' \quad P_e = \emptyset, \text{ ha } \bar{u}' = \bar{u} : \bar{c}' = \bar{c}$$

$$\Omega^{-1}(\bar{c}') = \bar{u}' \quad \text{ha } \bar{v} = \bar{c}_i \text{ tehát a dekodolás bemenetén érveles kódok van, akkor ez triviális}$$

nem tudok hibát javítani ha $\bar{v} = \bar{c}_j \neq \bar{c}$

+ nem tudok hibát javítani,

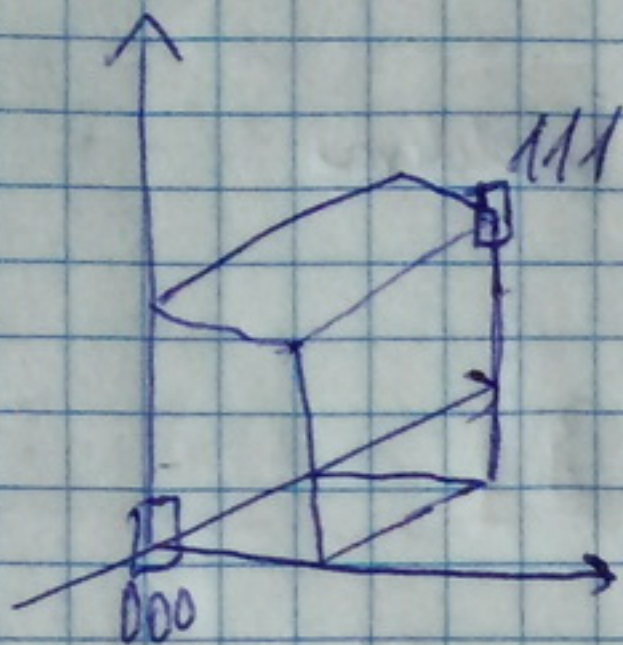
ha $c' \neq c$ de c' érveles kód!

(másra döntök tökéletesen)

olyan halmazt kapok, ami nem eleme az érték halmaznak!

de tudom detektálni!

ha növekvő $\frac{k}{N}$ -t $00 \rightarrow 000$ ismétléses kódolással
 $11 \rightarrow 111$

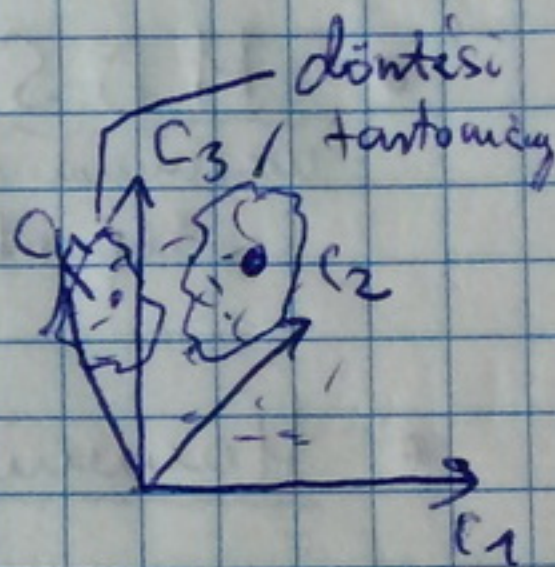
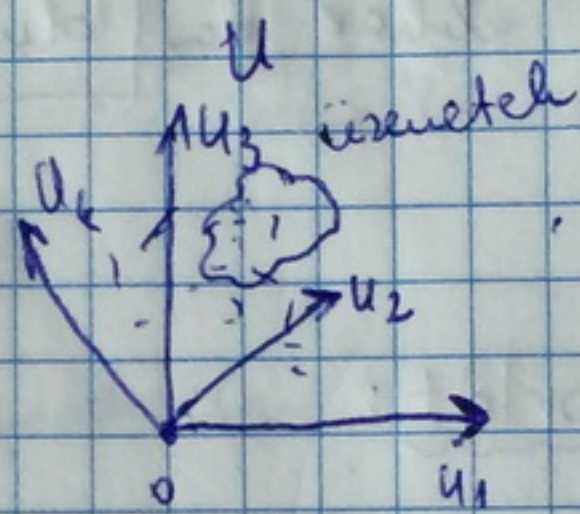


Algebrai konstrukciók: ... következő oldal!

8. előadás

Kezelhető hibák az átvitelben!

üzenetek $\vec{u} = [u_1, \dots, u_k]$ q^k
 kódok $\vec{c} = [c_1, \dots, c_N]$ q^N

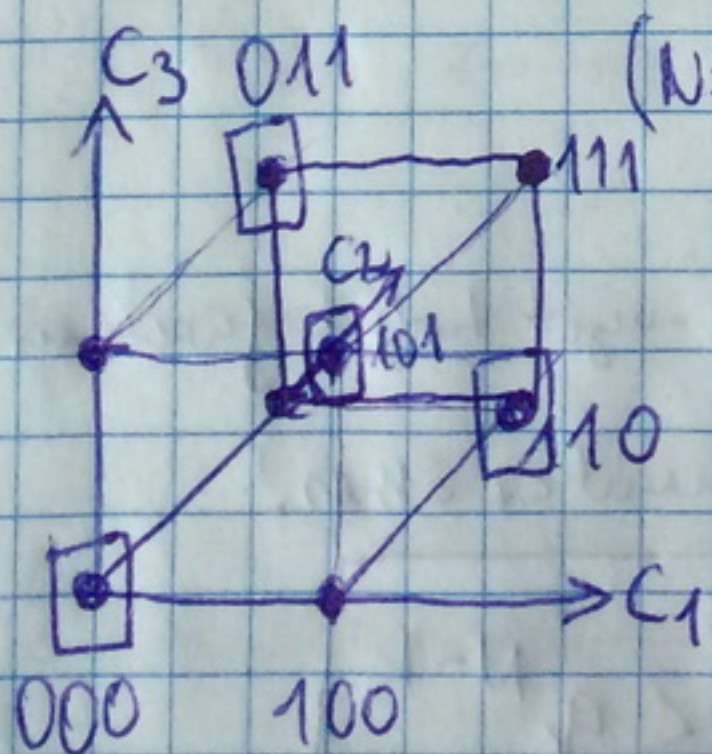


$t_{\text{jelezhető hibák száma}} < d_{\text{min}}$ (diszjunkt halmazok miatt) ; $t_{\text{jelezhető}} = d_{\text{min}} - 1$
 [döntési tartományok]

$t_{\text{javítható hibák száma}} = \lfloor \frac{d_{\text{min}} - 1}{2} \rfloor$

$t_{\text{törölhető}} = d_{\text{min}} - 1$

demodulátor
 nem akar dönteni mert nem biztos benne inkább újra kér majd mert tudom, hogy hol volt a hiba!



1) 000 hozzá közelebbet nem vilantom

2) 011, 101, 110, és kész!

ha 110 érkezik $\neq 10$ (törölhető hiba)

de tudom h. csak 110 lehet

[$d_{\text{min}} - 1$ távolságra levőt tudok javítani]
 $t_{\text{törölhető}}$

Kódkonstrukciós törvények:

- Singleton korlát (N, k, q) paraméterű kódokra
üzemeltet
kódtör állapot
 adott d_{\min}

és $N, k, q : M = ?$ hány üzenetem lehet?

$$M \leq q^k \quad \cancel{M \leq q^k} \quad d_{\min} \leq 1 + N - k \quad \text{ha} = \text{ahhoz a legjobb!}$$

(ehhez vanunk legtávolabbi)

$$M \leq q^{N-d_{\min}+1}$$

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

hány érvényes kódvektor lehet?

- MDS maximum distance separation akkor ha $d_{\min} = 1 + N - k$

- Hamming korlát:

adott t_{jav} mellett mi a kapacitás (N, k, q) között?

$$1 + N(q-1) \quad [1 \text{ ponttól, } 1 \text{ Hamming távolosságra}]$$

$$1 + N(q-1) + \binom{N}{2}(q-1)^2 \quad [1 \text{ ponttól } 2 \text{ Hamming táv}]$$

$$t_{\text{jav}} \text{ esetén } 1 + \binom{N}{t_{\text{jav}}}(q-1)^{t_{\text{jav}}} \Rightarrow t_{\text{jav}} : \sum_{i=0}^{t_{\text{jav}}} \binom{N}{i}(q-1)^i$$

1 érvényes kód
 $q-1$ rossz kód

$$q^k \cdot \sum_{i=0}^{t_{\text{jav}}} \binom{N}{i} (q-1)^i$$

üzemeknek néma
diszkrét

szükség van, hogy t_{jav} -nyit tudjunk javítani!
 - és ez biztos kisebb mint az összes!

$$q^k \cdot \sum_{i=0}^{t_{\text{jav}}} \binom{N}{i} (q-1)^i < q^N \cdot \sum_{i=0}^{t_{\text{jav}}} \binom{N}{i} (q-1)^i < q^{N-k}$$

$q=2$ esetén:

$$\sum_{i=0}^{t_{jav}} \binom{N}{i} \ll 2^{N-k}$$

- Perfekt a kód ha: $\sum_{i=0}^{t_{jav}} \binom{N}{i} \cdot (q-1)^i = q^{N-k}$
(a tér minden pontját felhasználjuk!)

pl: $(N=3, k=1, q=2)$

000 és 111 \rightarrow 1 hibét tudok javítani!

Hanning 1 döntési távolságra \rightarrow minden kódok használata \Rightarrow PERFEKT és MDS

Ez jó, de hogyan lehetne algoritmizálni?

Algebrai kódkonstrukció:

- lineáris tér: műveletelvezett
- kódok altér alkotók (lineáris altér)
- lin. független
- bázis: úszervektorokkal súlyozott összege a bázisokból \rightarrow előáll. az összes kód!
 $\{ \underline{c} \}$
- generátor

$$\begin{matrix} [00] \\ \underline{u} \end{matrix} \begin{matrix} \left[\begin{array}{cc} 0 & 1 & 1 \\ 1 & 0 & 1 \end{array} \right] \updownarrow k \\ \leftarrow \underline{N} \rightarrow \\ G \end{matrix} \quad \boxed{\underline{u} \cdot G = \underline{c}}$$

generátor mátrix: keress bázisvektorokat, amelyek lin. kombinációjával minden kódot előállíthatok!

ha a generátormátrix valahol tartalmazza az egység mátrixot $\frac{k}{k}$, akkor

$$G_{szintematikus} = \left[\begin{array}{c|c} \underline{I} & \underline{P} \end{array} \right] \updownarrow k \\ \leftarrow \underline{N} \rightarrow$$

szintematikus a kód!

$$\underline{G} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \text{sorrend!} \quad \underline{I} \quad \underline{P} \\ \underline{G}_{\text{minstekem}} = \begin{bmatrix} \underline{1} & \underline{0} \\ \underline{0} & \underline{1} \end{bmatrix}$$

H paritás ellenőrző matrix

legyen H olyan, hogy ~~$\underline{G} \cdot \underline{H}^T = \underline{0}$~~ $\underline{H} = [-\underline{P}^T \quad \underline{I}]$

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

példá $\underline{H} = [1 \ 1 \ 1]$

$$\underline{u} \cdot \underline{G} \underline{H}^T = \underline{u} \cdot \underline{0} = \underline{0}$$

$$\underline{c} \quad \underline{c} \underline{H}^T = \underline{0} = \underline{H} \cdot \underline{c}^T \quad \text{ha nem } \underline{0} \Rightarrow \text{szindróma}$$

$$\underline{x} = \underline{c} + \underline{e}$$

$$\underline{H} \underline{x}^T = \underline{H} (\underline{c} + \underline{e})^T = \underline{H} \underline{c}^T + \underline{H} \underline{e}^T = \underline{s}^T$$

10. előadás

$\underline{c} = \underline{u} \cdot \underline{G}$

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

szisztematikus kód esetén: $\underline{G} = \begin{bmatrix} \underline{I} & \underline{P} \end{bmatrix} \begin{matrix} k \\ N \end{matrix}$

$\underline{v} = \underline{c} + \underline{e}$
 |
 vett kód hibák
 vektor

\underline{v} erősség $\cdot e^T$ igen $\rightarrow \hat{e}$

$\underline{H} = \begin{bmatrix} -\underline{P}^T & \underline{I} \end{bmatrix} \begin{matrix} N-k \\ N \end{matrix} \rightarrow \underline{H}^T = \begin{bmatrix} -\underline{P}^T \\ \underline{I} \end{bmatrix} \begin{matrix} N \\ N-k \end{matrix}$ $\underline{G} \underline{H}^T = \begin{bmatrix} \underline{I} & \underline{P} \end{bmatrix} \begin{bmatrix} -\underline{P}^T \\ \underline{I} \end{bmatrix} = \underline{0}$

$\underline{H} \cdot \underline{v}^T = \underline{H} \cdot \underline{c}^T + \underline{H} \cdot \underline{e}^T = \underline{s}^T \rightarrow \underline{s}^T = \underline{H} \cdot \underline{e}^T$ szindróma

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

$\underline{e} = [000 \dots 100]$ 1 hiba van!
 N \rightarrow ezt szorzom \underline{H} -vel

(több hiba is lehet, ekkor az egyes oszlopok lin. kombinációja)
 amikor ez kiválaszt egy oszlopot \underline{H} -ban!

$t_{j\text{ar}} = 1 ; q = 2$

$1 + N \leq 2^{N-k}$ (Hamming-korlátból)

$N = 2^m - 1 ; k = 2^m - 1 - m$

$m = 2$ ✓

$m = 3$

R_c	N	K	m
1/3	3	1	$m = 2$
4/7	7	4	$m = 3$
11/15	15	11	$m = 4$

jóbb választás a cél (kisebbségi redundancia)

Kód arány

$R_c = \frac{K}{N}$ minél jobb minél nagyobb

$w = \sum_{i=1}^N X(c_i \neq 0)$
 ahol $c_i = 0$

lin. esetben: a kódban mindig (1) van.

$N-k$ páros ahol $t_{j\text{ar}} = 1$

ezek **PERFECTEK!** k lehetne kisebb is de akkor nem perfect!

lineáris kódokra

$d_{\text{min}} = \min w(c_i)$
 $\forall i$
 hibák
 $\underline{c} = \underline{0}$

$t_{jar} = 2, q = 2$

$1 + N + \frac{N(N-1)}{2} \leq 2^{N-k}$

N	k	Rc	m
5	1	1/5	
90	78	78/90	

→ kijön, de ilyen nincs!

↑
ide kell helyettesíteni és kijön N és k

Binary Hamming kód:

példa (7, 4, 2) → $t_{jar} = 2$, es perfekt a Hamming kódot

ne legyen H-bean két soros onlop!

~~$H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$~~

$H = \begin{bmatrix} 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \end{bmatrix}$

$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$ ↑ 2^1
 $N-k$ 2^2
 2^3

↑
ide azokat rakom amik meg nem voltak I-bean unolegy unilyen sorrendben.

$G = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 \end{bmatrix}$
 $k \times N$

$u = [1101] \rightarrow c = [1101100]$
 ↑
 lista

$u = c + e \rightarrow s^T = [101] \rightarrow H$ -nek 4. onlopa → 4. bit van ott el! c-be!

ha nem binaris a kod. $q = 3$

$1 + N(q-1) = q^{N-k}$
 ↑
 perfekt eset $(t_{jar} = 1)$
 de $n \geq 3$ miatt

$t_{jar} = 1$

N	k	Rc
4	2	1/2
6	4	66%

q=3
q=5

$GF(q = p^n)$
 Galois-test
 prim rendű

ha $N = k + 2$
 MDS is!

$$t_{\text{jar}} = 1 \quad 1 + N(q-1) = q^{N-k}$$

$$q=3 \rightsquigarrow \begin{matrix} N & k \\ 13 & 10 \end{matrix} \rightsquigarrow \text{nem MDS, mert } 13-10 \neq 2$$

$$q=5 \rightsquigarrow \begin{matrix} N & k \\ 31 & 28 \end{matrix} \rightsquigarrow \text{nem MDS!}$$

Neuberrinis Hamming kódok (MDS és perfekt) $t_{\text{jar}} = 1$

$$\underline{H} = \begin{bmatrix} 1 & 1 & 1 & 0 \\ \alpha^1 & \alpha^2 & 0 & 1 \end{bmatrix}$$

$$\underline{e} = [00 \dots e 00]$$

nem lineáris!
 szubsorom e -vel
 a hibéértéket

$(4, 2, 3)$ kód
 N, k, q

$$\begin{matrix} 2 & 1 \\ (4 \bmod 3 = 1) \end{matrix}$$

$$GF(q=3) = \{0, 1, 2\}$$

$\alpha^0 \alpha^1 \alpha^2$

$$\alpha^2 = 2 \quad \alpha^{q-1} = 1$$

primitív elem

11. előadás

Hamming kód: $t_{\text{jar}} = 1$ perfekt és MDS

mindket felkarralok $d_{\text{min}} = \text{maximalis}$

$$N-k=2 \Rightarrow d_{\text{min}}=3 \quad \text{és } t_{\text{jar}} = \left\lfloor \frac{d_{\text{min}}-1}{2} \right\rfloor = 1$$

$$GF(q=p^m) = \{0, 1, \dots, q-1\}$$

prim

és $x \neq 0$

$$a \in GF(q) \quad \deg(a) = x \rightsquigarrow a^x = 1 \quad (\text{primitív elem})$$

legkisebbs

$$\deg(\alpha) = q-1 \rightsquigarrow \boxed{\alpha^{q-1} = 1}$$

α primitív elem

α hatványozásával vizsgálható a teszt!

a test felett értelmezett a szorzás és összeadás

$a, b, c \in GF(q)$ asszociatív, kommutatív, disztributív

példa: $GF(7) = \{0, 1, 2, 3, 4, 5, 6\}$

primitív elem = ?

$\alpha=2$ $2^1=2$ $2^2=4$ $2^3=1 \pmod{7}$ \downarrow

MOD 7

$\alpha=3$ $3^1=3$ $3^2=2$ $3^3=6$ $3^4=4$ $3^5=5$ $3^6=1$

$\alpha=5$ is igaz!

több α is lehet!

nem bináris Hamming kód:

$k_i \rightarrow$ hibakéty, $e_i =$ hiba érték
 $e_i = q-1$ fele = **4**

MDS legyen $\rightarrow N-k=2$

$N=6$ $k=4$ $q=5$ $GF(5)$ **$\alpha=2$** érveljes

$H = \left[\begin{array}{cccc|cc} 1 & 1 & 1 & 1 & 1 & 0 \\ \alpha^1 & \alpha^2 & \alpha^3 & \alpha^4 & 0 & 1 \end{array} \right]$ $\downarrow N-k$
 $\leftarrow N-k$

$\left[\begin{array}{c} s^T \\ e_i^T \end{array} \right] = k_i^T$ egyik oszlop
 normálisan

minden oszlop vesérelése 1 kell legyen

hogy buljunk az értéket

$H = \left[\begin{array}{cccc|cc} 1 & 1 & 1 & 1 & 1 & 0 \\ 2 & 4 & 3 & 1 & 0 & 1 \end{array} \right]$

$G = \left[\begin{array}{cccc|cc} 1 & 0 & 0 & 0 & 4 & 3 \\ 0 & 1 & 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 0 & 4 & 2 \\ 0 & 0 & 0 & 1 & 4 & 4 \end{array} \right]$
 Ksor
 Vektor

$C = [3 \ 0 \ 2 \ 4 \ 1 \ 4]$

$u = [3 \ 0 \ 2 \ 4]$

$v = [3 \ 0 \ 2 \ 4 \ 4 \ 4]$

$e = [0 \ 0 \ 0 \ 0 \ 3 \ 0]$

$S = ?$ $v^T = \begin{bmatrix} 3 \\ 0 \\ 2 \\ 4 \\ 4 \\ 4 \end{bmatrix}$

$\cdot H = s^T = \begin{bmatrix} 3 \\ 0 \end{bmatrix} \rightarrow$ normáljuk $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightarrow$ H-ban az 5. oszlop értéke

3024 **14**
3

R-S hódoló: Reed-Solomon hódoló

többszörös hibét is tud javítani

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

$$\deg(u(x)) = k-1$$

$$k = K \quad n = N$$

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

⊕ polinomiális GF(q) felett

$$a(x) + b(x) = c(x) \quad c_i = a_i + b_i \pmod q$$

$$\deg(c(x)) = \max(\deg(a), \deg(b)) \quad \text{polinom fele}$$

* korzais GF(q) felett

$$c(x) = a(x) \cdot b(x)$$

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

$$\deg(c(x)) = \deg(a(x)) + \deg(b(x))$$

⊕ osztás GF(q) felett

$$a(x) \text{ és } b(x) \neq 0 \rightarrow q'(x), r(x) \quad \begin{matrix} \text{kvociens} \\ \text{residuum} \end{matrix}$$

$$a(x) = q(x) \cdot b(x) + r(x)$$

⊖ $c \in GF(q)$; $a(x)$ gyöke c
 $a(c) = 0$

R-S leírása:

$$C_0 = u(d^0)$$

$$\textcircled{1} C_1 = u(d^1)$$

$$\textcircled{2} C = U \cdot G$$

összeadom

$$G = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & d & d^2 & \dots & d^{u-1} \\ 1 & d^2 & d^4 & \dots & d^{2(u-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & d^{k-1} & d^{2(k-1)} & \dots & d^{(k-1)(u-1)} \end{bmatrix}$$

$$C_{N-1} = u(d^{N-1})$$

$$\Rightarrow N-1 \leq q-2 \quad \left(\text{mert } q-1 \text{ mert } \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \text{ 2 sorok van} \right) \text{ mert } d^{q-1} = 1$$

$$(3) \quad C = \{C^k, c(\alpha^i) = \emptyset, i=1, \dots, n-k\}$$

$$C_0 = \{c, H \in T = \emptyset\}$$

$$H = \begin{bmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{N-1} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \alpha^{N-k} & \dots & \dots & \alpha^{(N-k)(N-1)} \end{bmatrix} \begin{matrix} \uparrow \\ N-k \\ \downarrow \end{matrix}$$

← N →

$$\text{MDS} : w(\underline{c}) = d_{\min}$$

↑
BIZ

MDS elvadás a kód!

$$w(\underline{c}) = N - \#C(\text{mellekmei}) \geq N - u(x) \text{ gyök} \geq N - (k-1)$$

+ Singletonos $d_{\min} \geq N - k + 1$

amiatt! \Rightarrow $d_{\min} = w(\underline{c})$

12. előadás

primitív elem

Reed-Solomon kódok: $RS(N, k, q)$, $GF(q)$, α

$$G = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \dots & \alpha^{(k-1)(N-1)} \end{bmatrix} \begin{matrix} \uparrow \\ N-k \\ \downarrow \end{matrix}$$

← N →

eset MDS kódok $\rightarrow d_{\min} = N - k + 1$

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

$$2t_{jav} = N - k$$

paritás szimbólumok száma

$$H = \begin{bmatrix} 1 & \alpha^1 & \alpha^2 & \dots & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(N-1)} \\ \vdots & \vdots & \vdots & \dots & \vdots \\ 1 & \alpha^{N-k} & \alpha^{2(N-k)} & \dots & \alpha^{(N-k)(N-1)} \end{bmatrix} \begin{matrix} \uparrow \\ N-k \\ \downarrow \end{matrix}$$

← N →

$$N-1 \stackrel{(k)}{=} q-2$$

$$\alpha^{q-1} = \text{egység elem}$$

$$RS(N=q-1, k=N-2t_{jav}, q)$$

legjobb esetben

Peterson-Gorenstein-Zierler algoritmus:

$$t_{\text{jav}} = 2 \text{ és } q = 7 \leadsto N = 6, k = 2$$

hiba pozíció: i, j

hiba érték: e_i és e_j

hiba lokátorok: $h_i \dots h_j$ a pontos ell. mátrix i, j oslopánál első elemei.

$$\bar{e} = [0 \dots \overset{i}{e_i} \dots \overset{j}{e_j} \dots 0] \quad h_i = \alpha^{ki} \quad h_j = \alpha^{kj} \quad \leadsto \text{lokalizálják a hibát.}$$

\leftarrow hiba vektor

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

$$\bar{s}^T = \underline{H} \cdot \underline{e}^T \Rightarrow \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \begin{bmatrix} \vdots \\ \vdots \\ \vdots \\ \vdots \end{bmatrix} \rightarrow \boxed{\bar{s}^T = e_i \cdot \bar{h}_i^T + e_j \cdot \bar{h}_j^T} \rightarrow \begin{cases} s_1 = h_i \cdot e_i + h_j \cdot e_j \\ s_2 = h_i^2 \cdot e_i + h_j^2 \cdot e_j \\ s_3 = h_i^3 \cdot e_i + h_j^3 \cdot e_j \\ s_4 = h_i^4 \cdot e_i + h_j^4 \cdot e_j \end{cases}$$

nem lin. egyenlet rvsz.

lokátorpolinom: gyöke h_i és h_j

$$L(x) = (x - h_i)(x - h_j) = x^2 - (h_i + h_j) \cdot x + h_i \cdot h_j$$

$$L_1 = -(h_i + h_j)$$

$$L_0 = h_i \cdot h_j$$

$$\Rightarrow \cancel{x^2 + L_1 x + L_0} \rightarrow \boxed{x^2 + L_1 x + L_0}$$

$$h_i \cdot e_i \cdot L(h_i) = e_i \cdot h_i^3 + L_1 \cdot h_i^2 \cdot e_i + L_0 \cdot h_i \cdot e_i = \emptyset$$

0 len
mert gyök
van.

$$h_j \cdot e_j \cdot L(h_j) = e_j \cdot h_j^3 + L_1 \cdot h_j^2 \cdot e_j + L_0 \cdot h_j \cdot e_j = \emptyset$$

$$h_i^2 \cdot e_i \cdot L(h_i) = e_i \cdot h_i^4 + e_i h_i^3 \cdot L_1 + e_i h_i^2 \cdot L_0 = \emptyset$$

$$h_j^2 \cdot e_j \cdot L(h_j) = e_j \cdot h_j^4 + L_1 \cdot h_j^3 \cdot e_j + L_0 \cdot h_j^2 \cdot e_j = \emptyset$$

(+)

$$e_i h_i^3 + e_j h_j^3 + L_1 (h_i^2 \cdot e_i + h_j^2 \cdot e_j) + L_0 (h_i \cdot e_i + h_j \cdot e_j) = 0$$

$$e_i h_i^4 + e_j h_j^4 + L_1 (e_i h_i^3 + h_j^3 e_j) + L_0 (h_i^2 e_i + h_j^2 e_j) = 0$$

$$\Delta_3 + L_1 \cdot \Delta_2 + L_0 \cdot \Delta_1 = 0$$

$$\Delta_4 + L_1 \cdot \Delta_3 + L_0 \cdot \Delta_2 = 0$$

uwar linearis
eigenwertrechner!

RS(6, 2, 7)

$$G = \begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{bmatrix} \quad [1 \alpha^1 \alpha^2 \alpha^3 \alpha^4 \alpha^5] \text{ mod } 7.$$

~~$$H = \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$~~

$$H = \begin{bmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{bmatrix}$$

$$u = [3 \ 5]$$

$$\bar{c} = [1 \ 4 \ 6 \ 5 \ 2 \ 0]$$

$$\bar{e} = [0 \ 2 \ 0 \ 0 \ 3 \ 0]$$

$$N = [1 \ 6 \ 6 \ 5 \ 5 \ 0]$$

$$S^T = \underline{H}^T \cdot \underline{v} \Rightarrow$$

$$H^T \begin{matrix} & \begin{matrix} e_i \\ 2 \end{matrix} & & & \begin{matrix} e_j \\ 3 \end{matrix} & \\ \begin{matrix} h_i \\ 1 \end{matrix} & \boxed{3} & 2 & 6 & \boxed{4} & 5 \\ \begin{matrix} h_j \\ 1 \end{matrix} & 2 & 4 & 1 & 2 & 4 \\ \begin{matrix} h_k \\ 1 \end{matrix} & 6 & 1 & 6 & 1 & 6 \\ \begin{matrix} h_l \\ 1 \end{matrix} & 4 & 2 & 1 & 4 & 2 \end{matrix} \begin{bmatrix} 1 \\ 6 \\ 6 \\ 5 \\ 5 \\ 0 \end{bmatrix} = \begin{bmatrix} 4 \\ 3 \\ 1 \\ 6 \end{bmatrix}$$

$$1 + L_1 \cdot 3 + 4L_0 = 0$$

$$6 + L_1 \cdot 1 + 3 \cdot L_0 = 0$$

$$\rightarrow \cancel{4} + 2L_0 = 0$$

$$\cancel{L_0} = 3/2$$

$$\boxed{L_0 = 5}$$

$$2L_0 = 3 \text{ mod } 7 \\ L_0 = 10 \rightarrow \checkmark$$

$$6 + L_1 + 15L_0 = 0 \rightarrow \boxed{L_1 = 5}$$

$$L_1 = -(h_i + h_j)$$

$$L_0 = h_j \cdot h_i$$

$$\boxed{h_i = 3}$$

$$\boxed{h_j = 4}$$

másodfokú egyenlethöz

$$\begin{aligned} \phi &= -(h_i + h_j) \\ 5 &= h_i \cdot h_j \end{aligned}$$

$$4 = 6 + 4e_j \rightarrow \boxed{e_j = 3}$$

$$\left. \begin{aligned} 4 &= 3e_i + 4e_j \\ 3 &= 2e_i + 2e_j \end{aligned} \right\} \rightarrow 5 = 6e_i \rightarrow \boxed{e_i = 2}$$

végül \underline{H} -ban megkeresem $\rightarrow \underline{v} = [166550]$

$$e = [020030]$$

$$\hat{c} = [146520]$$

javítottam 2 hibát!

2015.04

Hibbelm.

15-EA.

$GF(p^m) = \{0, 1, 2, \dots, p^m - 1\}$, $p = GF(p)$ primitív elem β^i

$GF(2^2) = \{0, 1, 2, 3\} = \{0, 1, x, x+1\}$

$\{[0], [1], [x], [x+1]\}$ x^2+x_0
 $[\beta^i \ \beta^j \ \dots \ \beta^x]$ $\begin{matrix} 0 & 0 \\ 0 & 1 \\ 1 & 0 \\ 1 & 1 \end{matrix}$
 m db

$p(x) \in GF(p) \{0, 1, x, x+1, x^2, x^2+1\}$

$p(x)$ max. $m-1$ -edik fokú lehet

$\{x^0, x^1, x^2, \dots, x^{m-2}\}$

⊕ Példa:

$0 + 1 = 1$

→ konstans-hinté mod p aritmetikával összegezzük

⊕	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

* Szorzás

$a(x) \cdot b(x) \pmod{p(x)}$ felbonthatatlan

$p(x)$, m -ed fokú irreducibilis polinom

$\nexists c_1(x) \text{ és } c_2(x) \quad p(x) \neq c_1(x) \cdot c_2(x)$

$0 < \deg(c_1(x)) < \deg(p(x))$

$0 < \deg(c_2(x)) < \deg(p(x))$

1. Példa

Példa:

1. fokú: $x, x+1$

2. fokú: x^2, x^2+1, x^2+x+1

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

$1 \cdot x = x$

$x \pmod{p(x)} = x$

$$(N, K, q) = (5, 3, 14)$$

$$t_{\text{jav}} = 1$$

$$1 + N(q-1) = q^{N-K}$$

$$\bar{H} = \begin{bmatrix} 1 & 1 & 1 & 1 & 0 \\ 1 & 2 & 3 & 0 & 1 \end{bmatrix}$$

$\begin{matrix} \nearrow \\ \searrow \end{matrix}$ $\begin{matrix} 1 \\ 2 \\ 3 \end{matrix}$ $\begin{matrix} \nearrow \\ \searrow \end{matrix}$ $\begin{matrix} 1 \\ 2 \\ 3 \end{matrix}$ $\begin{matrix} \nearrow \\ \searrow \end{matrix}$ $\begin{matrix} 1 \\ 2 \\ 3 \end{matrix}$

$$\bar{G} = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 2 \\ 0 & 0 & 1 & 1 & 3 \end{bmatrix}$$

$$\bar{u} = [2 \ 3 \ 2]$$

$$\bar{c} = [2 \ 3 \ 2 \ 3 \ 2]$$

$$\bar{e} = [0 \ 0 \ 1 \ 0 \ 0]$$

$$\bar{v} = [2 \ 3 \ 3 \ 3 \ 2]$$

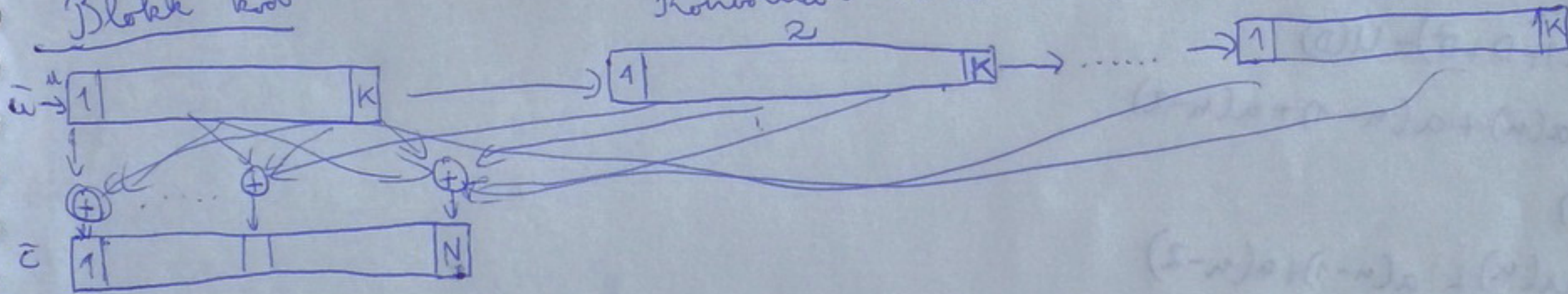
$$\bar{s}^T = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$$

$$\bar{s}^F = \begin{bmatrix} 1 \\ 3 \end{bmatrix}$$

$$e = 1$$

csiba értéke: s^T első nem 0 eleme

Blokk kód

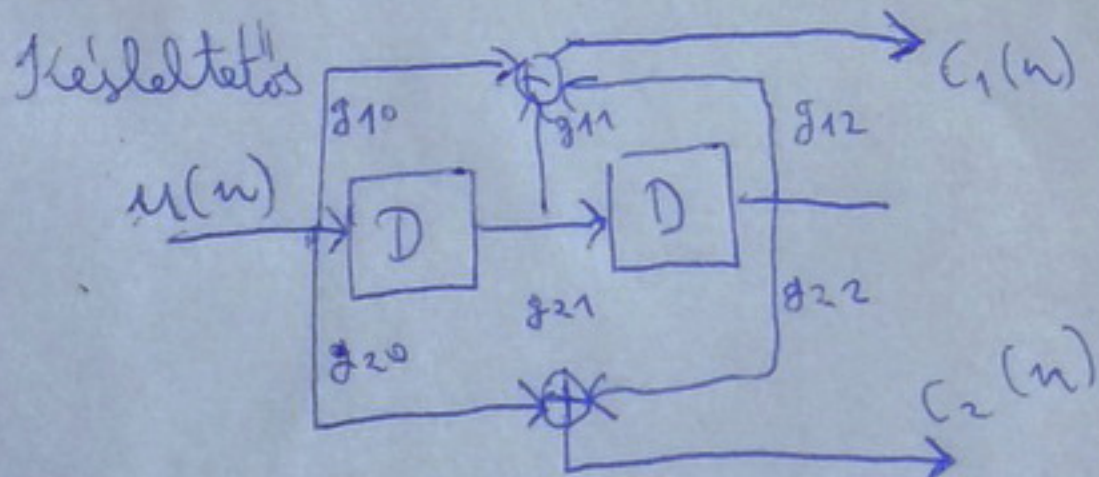
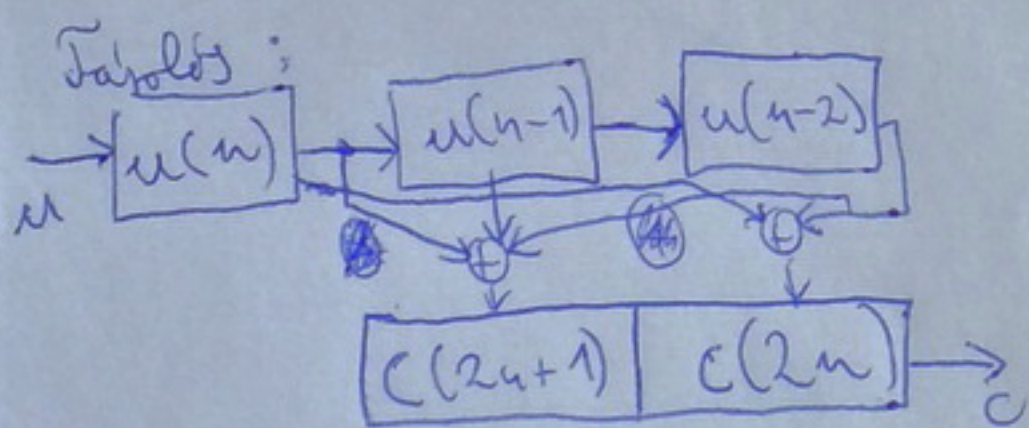


Konvolúciós kód, Trellis kód

az aktuális kód az L-k-val azelőtti szimbólumoktól is függ

$$(N, k, L, q)$$

$$(2, 1, 3, 2)$$



$$\bar{c}_1 = \bar{u} * \bar{g}_1$$

$$\bar{c}_2 = \bar{u} * \bar{g}_2$$

$$\bar{c}_i = \sum_{j=0}^{L-1} u(n-j) g_{ij}$$

$$\bar{g}_1 = [1 \ 1 \ 1] = 7_{10}$$

$$\bar{g}_2 = [1 \ 0 \ 1] = 5_{10}$$

$$\bar{g}_i = [g_{i0} \ g_{i1} \ \dots \ g_{iL-1}]$$

$$Z(X) = \sum_{i=0}^{\infty} x_i Z^{-i}$$

$$D = Z^{-1}$$

$$U(D) = \sum_{i=0}^{\infty} u_i \cdot D^i$$

$$G_1(D) = 1 + D + D^2$$

$$G_2(D) = 1 + D^2$$

$$C_i(D) = U(D) \cdot G_i(D)$$

$$\vec{C}(D) = [C_1(D) \dots C_N(D)]$$

$$C(D) = U(D) \cdot \vec{G}(D) \\ = U(D) [G_1(D) \dots G_N(D)]$$

Szisztematikus - nem sziszet.

Rekurzív nem rek.
 NSC, RSC
 non recursive non systematic convolutional
 rekurzív, szisztematikus

$$G_1(D) \rightarrow G_1'(D) = 1$$

$$G_2(D) \rightarrow G_2'(D) = \frac{G_2(D)}{G_1'(D)}$$

$$C_1'(D) = U(D) \cdot G_1'(D)$$

$$C_2'(D) = U(D) \cdot G_2'(D) = U(D) \cdot \frac{G_2(D)}{G_1(D)} = \underbrace{\frac{U(D)}{G_1(D)}}_{A(D)} \cdot G_2(D) = A(D) \cdot G_2(D)$$

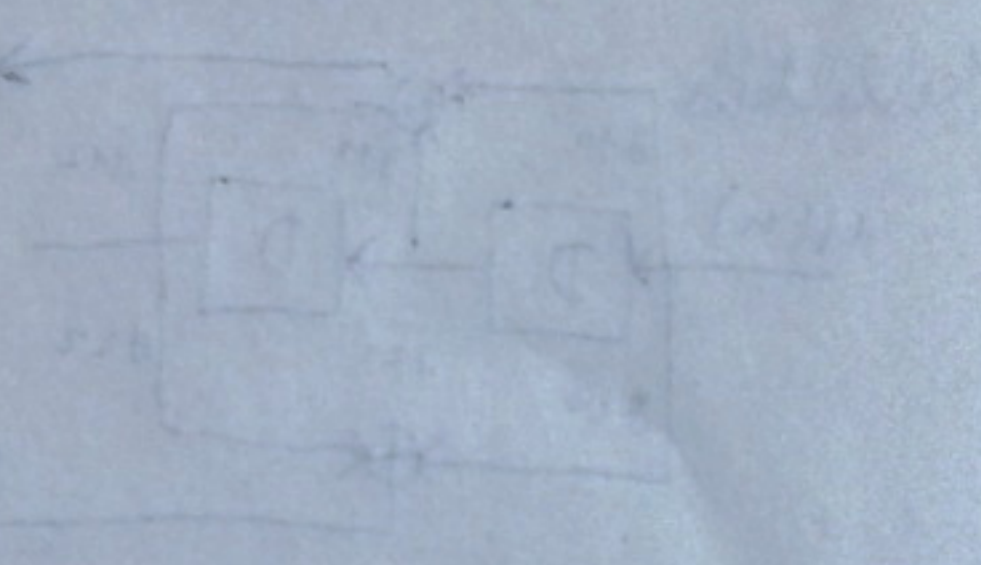
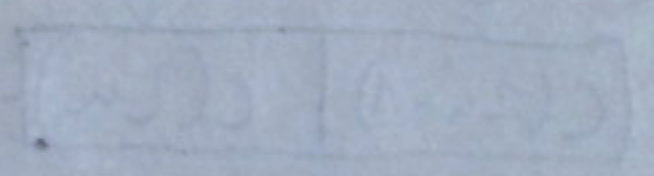
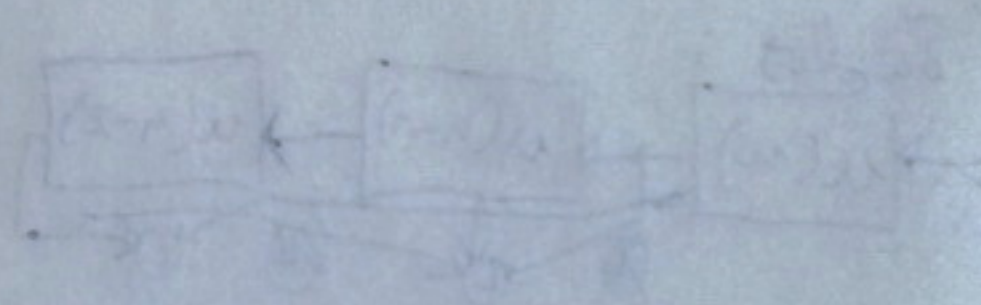
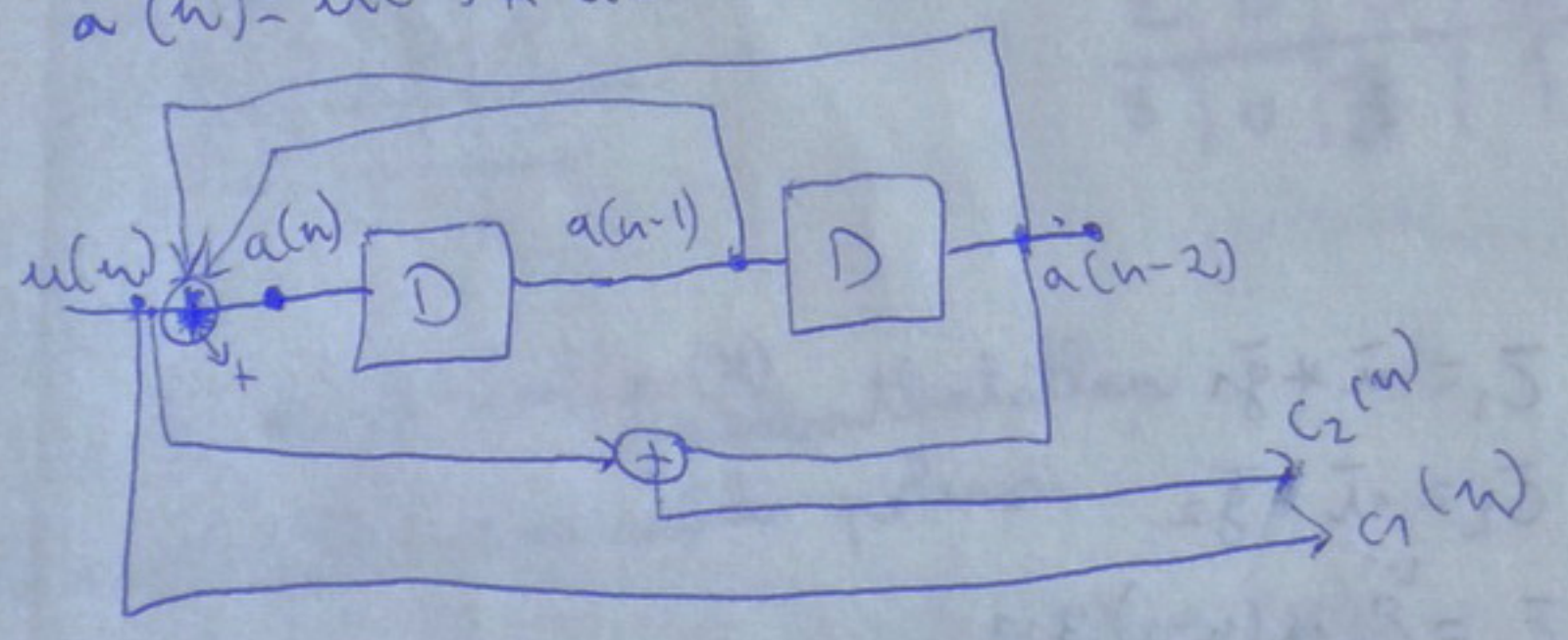
$$A(D) = \frac{U(D)}{G_1(D)} = \frac{U(D)}{1+D+D^2}$$

$$\Rightarrow A(D)(1+D+D^2) = U(D)$$

$$u(n) = a(n) + a(n-1) + a(n-2)$$

GF(2)

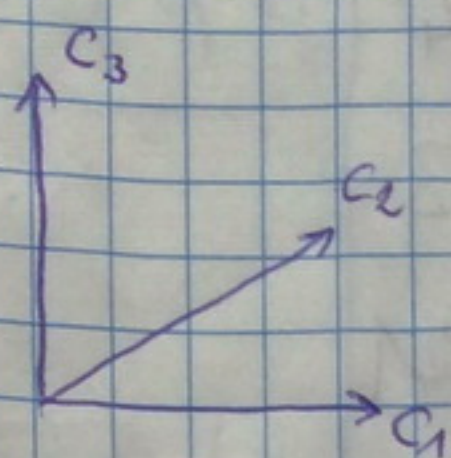
$$a(n) = u(n) + a(n-1) + a(n-2)$$



13. előadás

Block kódolás: ciklikus kód

pl: CRC
"cyclic redundancy check"



(3,2,2)

Ciklikus kódok: (N, k, q)

érvényes kódok legyenek: $[C_0, C_1, \dots, C_{N-1}]$

ahol érvényes kódok lennek ez is: $[C_{N-1}, C_0, C_1, C_2, \dots, C_{N-2}]$

[ciklikus eltolja egy kódunk szintén kód]

$$C(x) = C_0 + C_1 x + C_2 x^2 + \dots + C_{N-1} x^{N-1}$$

$$x \cdot C(x) = C_{N-1} + C_0 x + C_1 x^2 + C_2 x^3 + \dots + C_{N-1} x^N \quad | + C_{N-1} - C_{N-1}$$

$$= C_{N-1} + C_0 x + \underbrace{C_{N-2} x^{N-1} + C_{N-1} x^N}_{C_1(x)} = C_1(x)$$

hogyan áll elő: $C_1(x) \rightarrow x \cdot C(x) \pmod{x^N - 1}$

ez éppen a maradék

$$C_i(x) = x^i \cdot C(x) \pmod{x^N - 1}$$

1 kódból az összes előállítható

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

$$u(x) = u_0 + u_1 x + \dots + u_{k-1} x^{k-1}$$

$$(x^N - 1) = g(x) \cdot h(x)$$

üzenet

(k-1) fok

$$c(x) = u(x) g(x) \pmod{h(x)} \rightarrow c(x) \cdot h(x) = u(x) g(x) \cdot h(x) = u(x) \cdot (x^N - 1)$$

fokok: $(N-1)$ $(k-1)$ $N-k$

$$\underbrace{u(x) g(x)}_{c(x)} \cdot h(x) \pmod{x^N - 1} = \emptyset \leftarrow \text{szüntető len}$$

$$\boxed{u(x) \cdot h(x) \pmod{x^N - 1} = \emptyset} \quad \text{ehhez jó}$$

hitt
jel

ha $v(x) = c_i(x)$ lett értéke egyszerű az eredetivel

Tétel: $g(x)$ generátor, ha $(x^N - 1)$ osztható $g(x)$ -nel és $\deg(g(x)) = N - k$.

Biz: $c(x) = \underbrace{x^{k-1}}_{\text{üzenet}} \cdot g(x)$ ahelyettesítés megvan. • Minden köd szó osztható $g(x)$ generátor polinommal.

$$c(x) = \underbrace{x^k \cdot g(x)}_{\text{maradék}} - \underbrace{(x^N - 1)c_{N-1}}_{\text{definíció}}$$

$x^k \cdot g(x)$ osztható $g(x)$ -el és $(x^N - 1)$ osztható $g(x)$ -el $\rightarrow c_i(x)$ osztható $g(x)$ -el

Q.E.D.

$[N=7; k=4; q=2]$ $GF(2)$ feletti felbontások

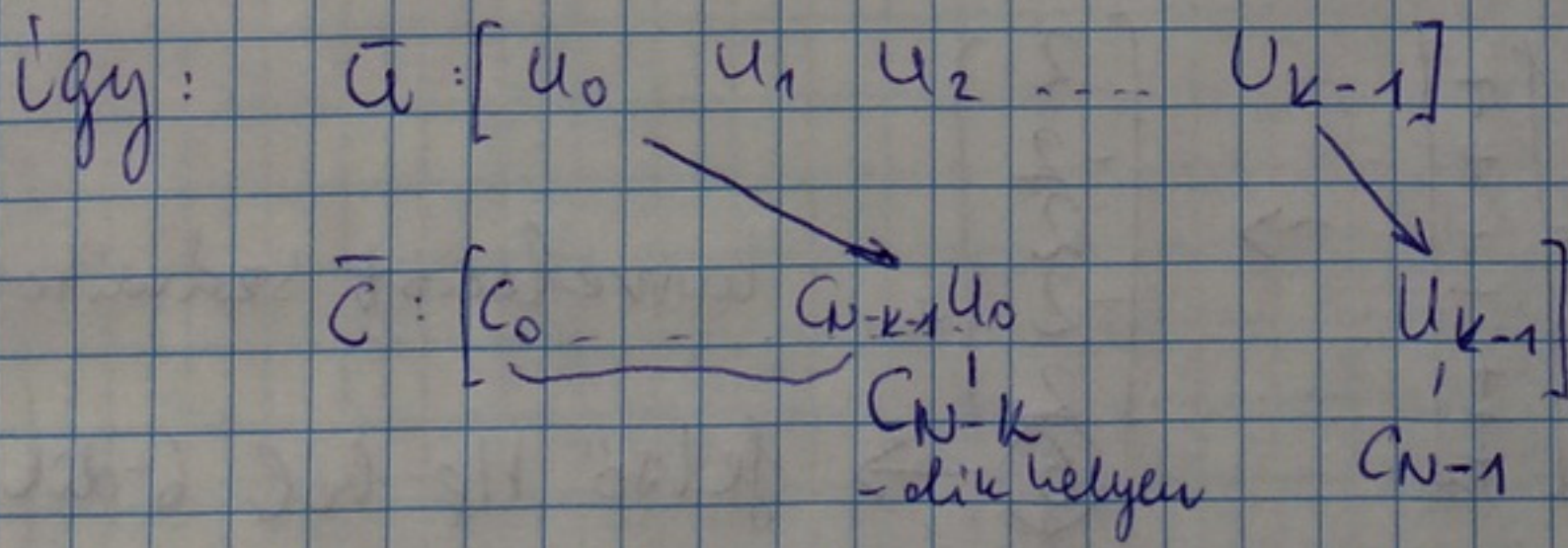
$$(x^7 - 1) = \underbrace{(x+1)}_{h(x)} \underbrace{(x^3 + x + 1)}_{g(x)} \underbrace{(x^3 + x^2 + 1)}_{g(x)} = (x^4 + x^3 + x^2 + x + 1)(x^3 + x^2 + 1) =$$

$$x^7 + x^6 + x^5 + x^4 + x^3 + x^6 + x^5 + x^4 + x^3 + x^2 + x^4 + x^3 + x^2 + x + 1 = x^7 + \cancel{x^6} + \cancel{x^5} + \cancel{x^4} + \cancel{x^3} + \cancel{x^2} + \cancel{x} + 1 = x^7 + 1 = x^7 - 1 \text{ (GF(2) miatt)}$$

$g(x)$ és $h(x)$ megvan

CRC: szisztematikus, ciklikus

$$c(x) = u(x) \cdot x^{N-k} - \underbrace{\left[u(x) \cdot x^{N-k} \text{ mod } g(x) \right]}_{\substack{\text{maradék } r(x) \\ \text{osztható } g(x)\text{-el}}} \rightarrow \deg(r(x)) = N - k - 1$$



üzenetet felshifteltem
üzenet van a kód szővében.

ez ciklikus és szisztematikus is!

$$t_{j\omega} = \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

$$N = 4m \rightsquigarrow t_{j\omega} = \left\lfloor \frac{2m - 1}{2} \right\rfloor = m - 1$$