

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 (infokomm)

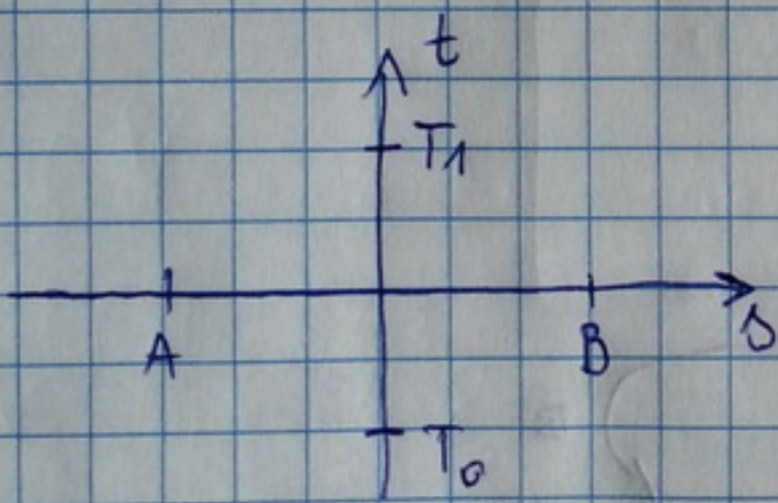
tétel kifejtés

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 / tömítés [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

$\# \bar{\xi} = D^n [D \cdot D \cdot D \dots D]$

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

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

DEEZ MEG NEM JO:

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]
 fehér

○ : $\log_4 \frac{4}{3} = 0,415$ [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)

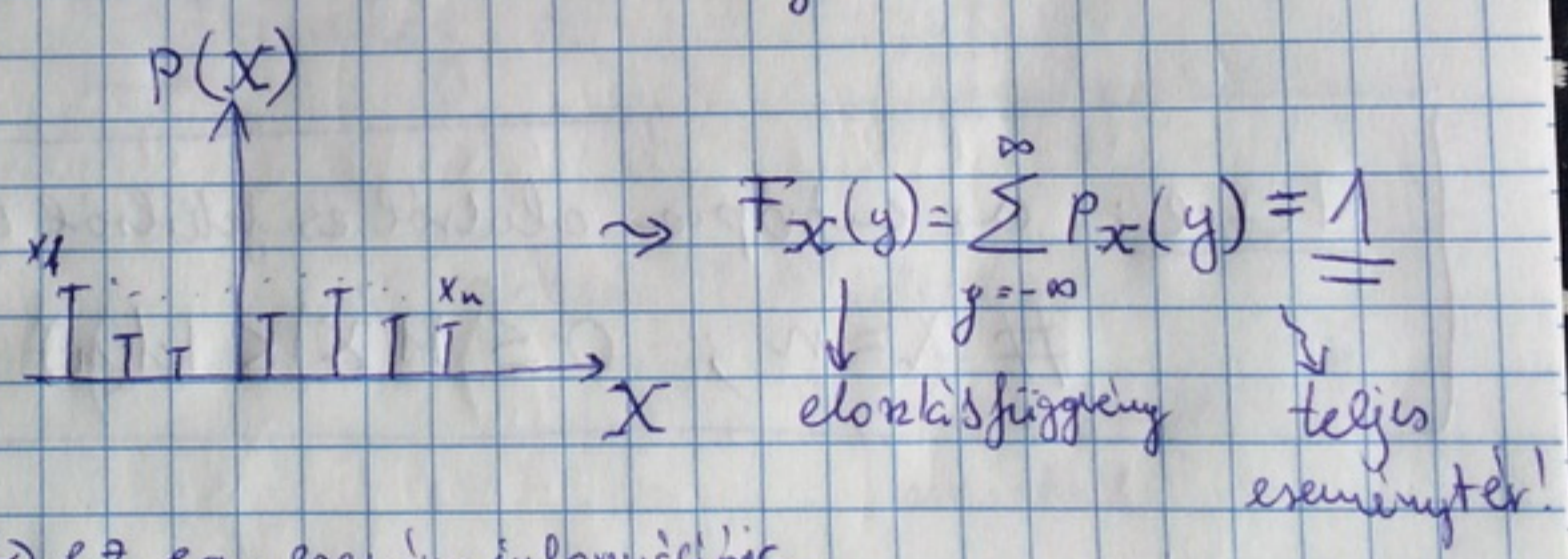
↳ kevesebb info mint egyenletes eloszlásnál

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; $P(X)$ sűrűség f.; $p_i = P(x_i)$ i. dik. esemény)



Def: $I(x_i) = \log \frac{1}{p(x_i)}$ → ez egy esemény információja [bit]

(Labels: \log minél valószínűbb az esemény annál kisebb az info. tartalom; $-\log(p(x_i))$)

(Self Information - az esemény saját információ tartalma)

Def: Entropia, Átlagos információ tartalom (entropy)

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

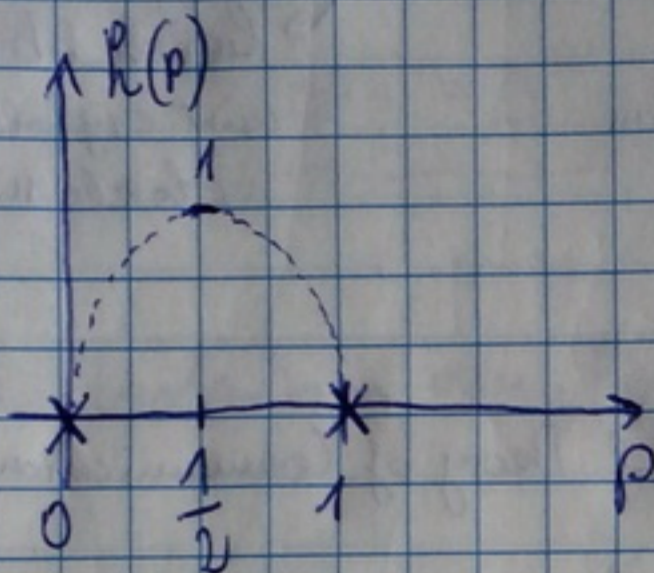
() → utarcsi és a lájkok

- 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 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

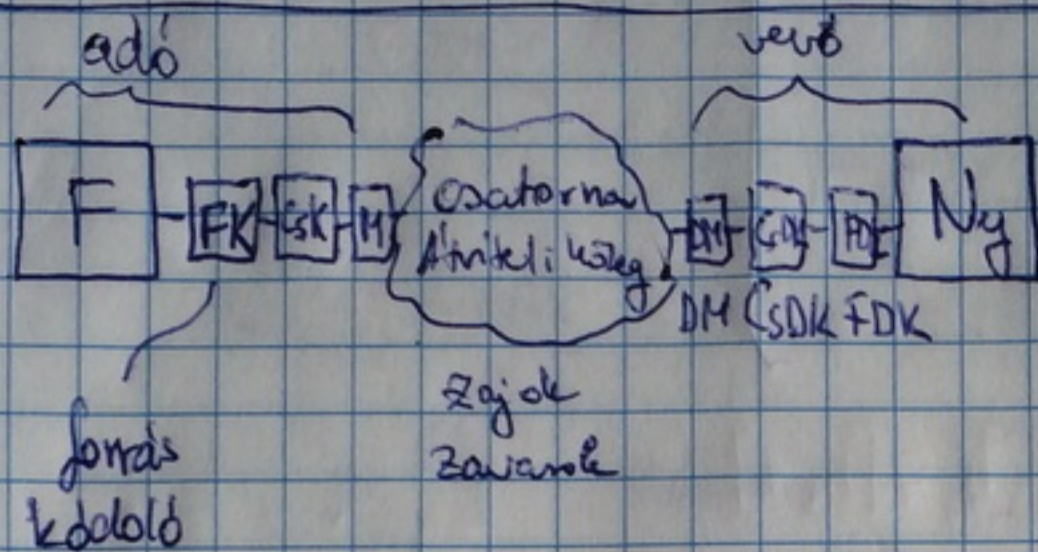
Dallos: Tantárgyi segédlet a hírközlés elmélet tárgyhoz

Prigys I.: Hírközlés rendszerei

Csibi S.: Információ közlése és feldolgozása

}

IRODALOM



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

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

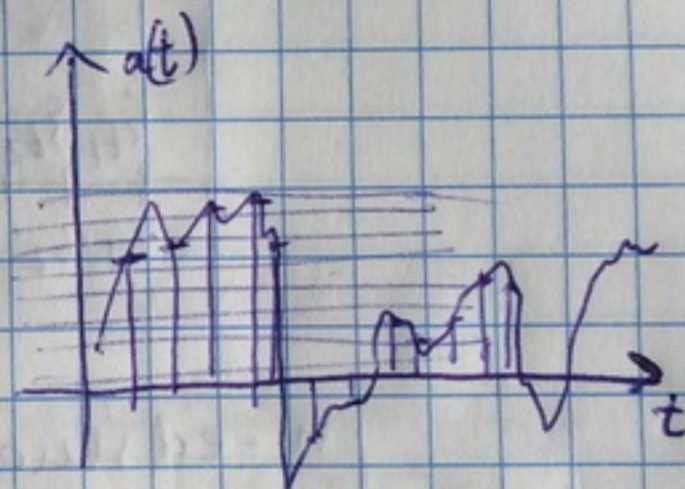
M: modulátor

DM: demodulátor

CsDK: csatorna dekódolás

FDK: ferris dekódolás

F analóg $a(t)$

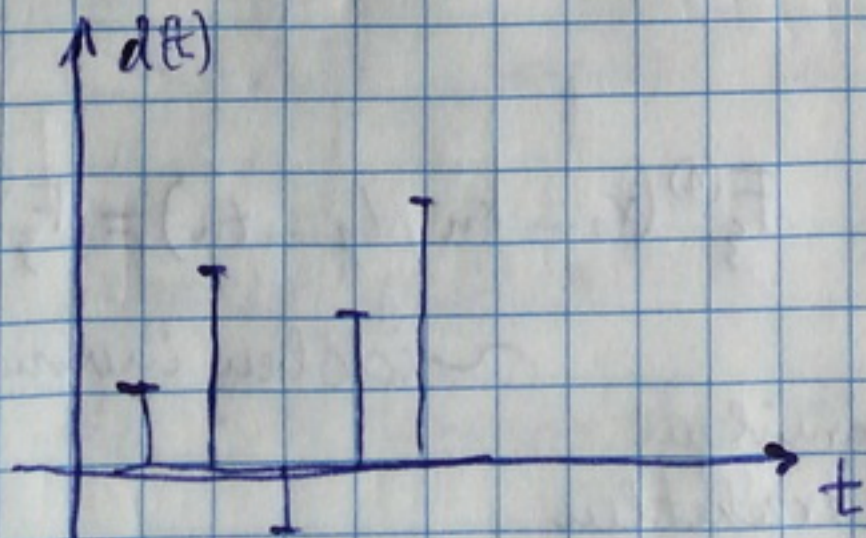


igen Bell idejében ↗

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

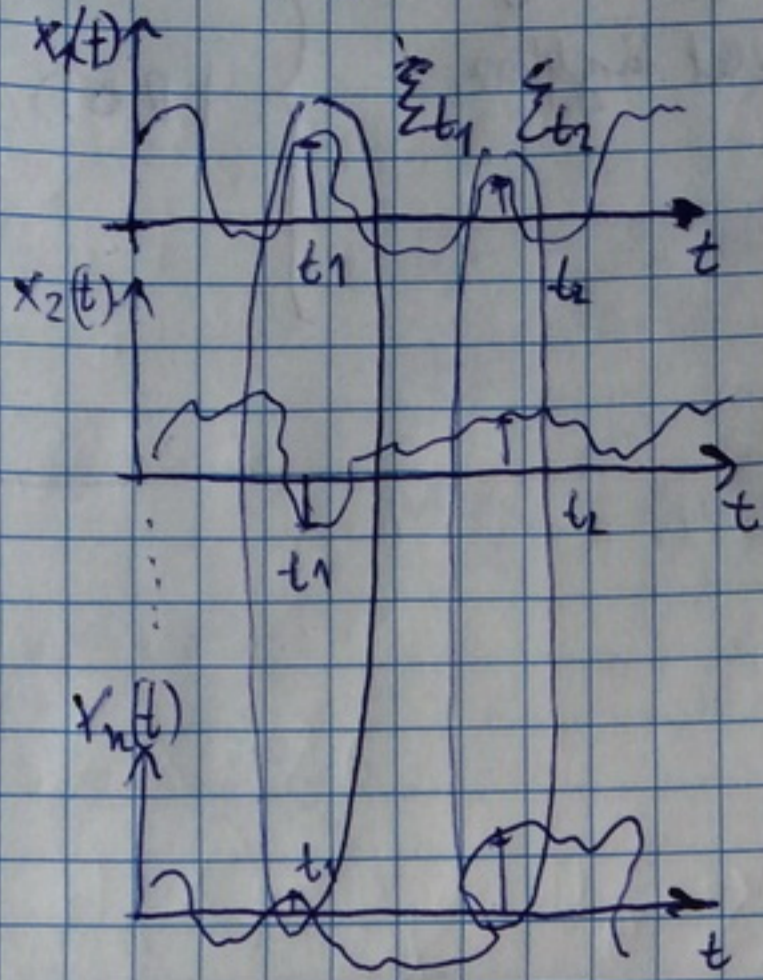
Ma digitális jel:

- időben mintavételezés (T)
- értékben kvantálva



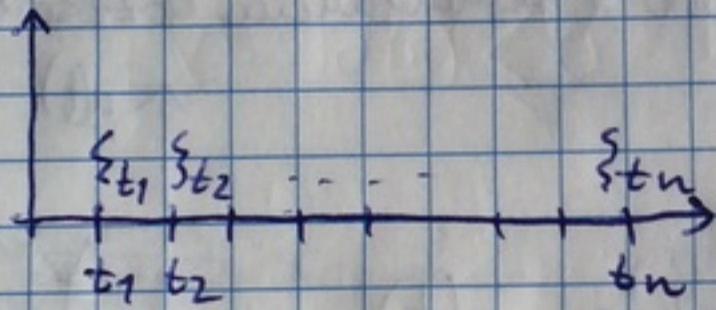
Sztochasztikus folyamatok

① a folyamat realizációjának az együttese



együtt ők a stochasztikus folyamat!

② Valószínűségi változók rendezett (időben) serege



n -ed rendű eloszlás fr. (n dimenziós)

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

eloszlás fr.

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

• 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 invariancia

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

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)

perszemelt: $\forall \Delta T$ 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

folymosított(f)

példa:

$$\#X = 26$$

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

entropia

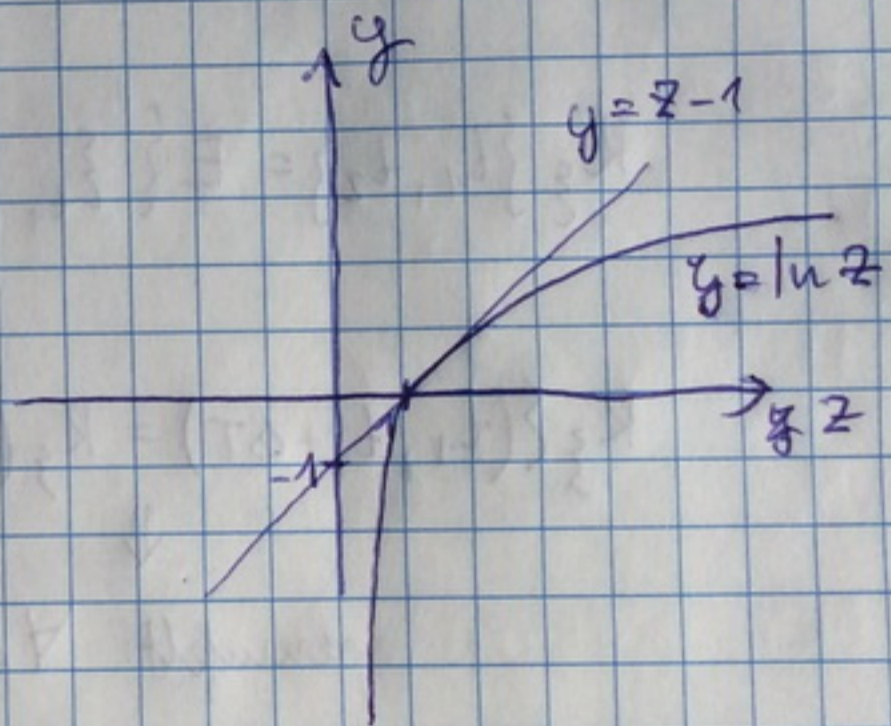
$$\log_a x = \frac{\ln(x)}{\ln(a)}$$

(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

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

potok $H_2(X) = 3 \text{ bit}$

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

0 ✓

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

redundancia

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

3. előadás

~ eddig amiket tanultunk

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

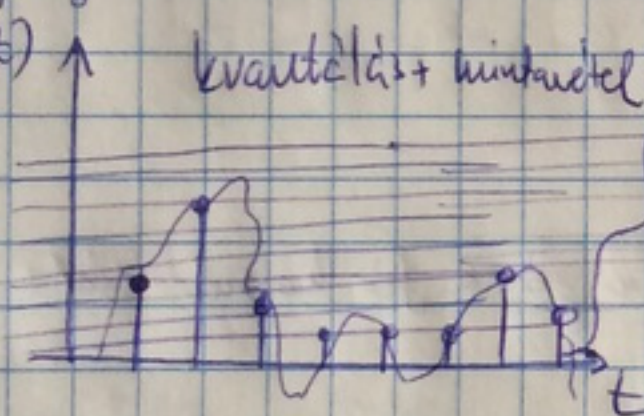
n-ed rend. stacionaris: $F_{\xi}^{(n)}(\bar{x}, t_1 + \Delta T, t_2 + \Delta T, \dots, t_n + \Delta T) = F_{\xi}^{(n)}$

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

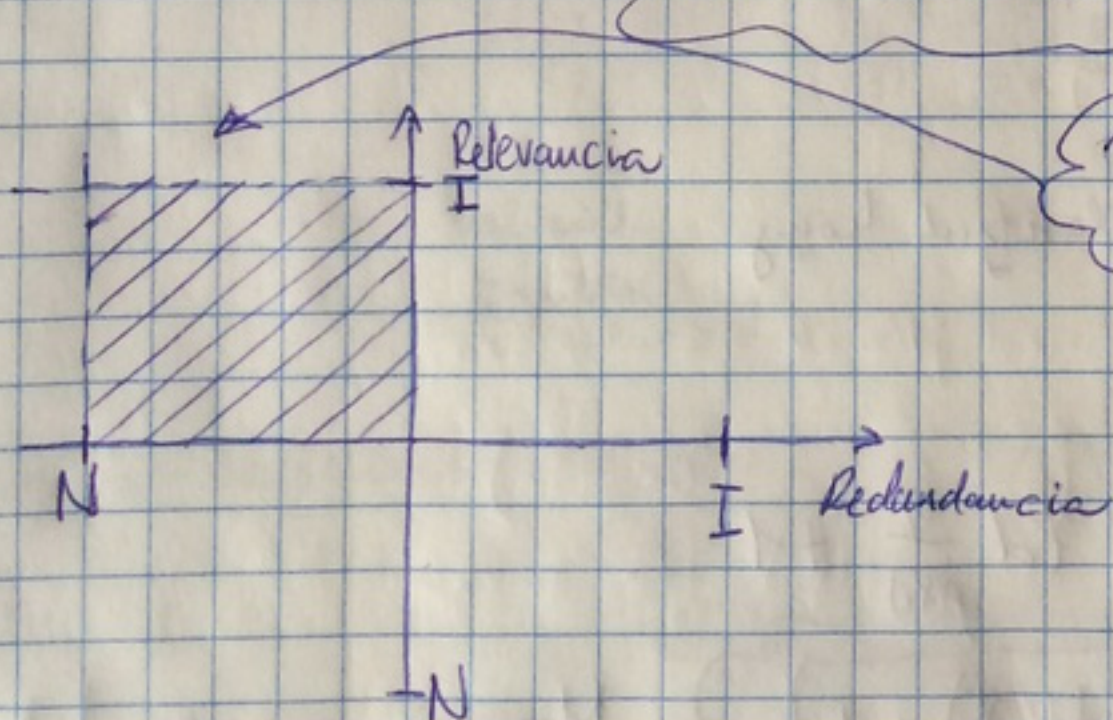
alt) \uparrow kvantálási hirtetés



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

ha változik időben a várható érték \rightarrow
 nem stacionaris

VALÓS VILÁG FOLYAMATAI



relevans információ átírás
 kevés redundanciával

egyenletes
 eloszlás

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

Redundancia

Cél ennek
 a minimalizálása

háromtöveges:

$$\#X = 26$$

$$p(X)$$

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

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

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

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

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

egyszerűsített esetben 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. vlt.
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 entropiaja

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

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] 'olése'

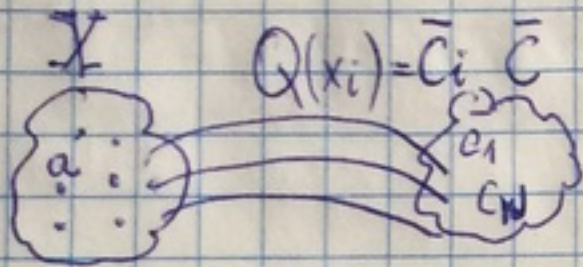
4. előadás

~ 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 elemeit!

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

egy kód
hossza

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

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

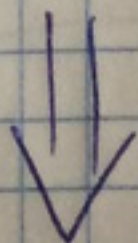
ha $p(x_i) < p(x_j) \Rightarrow l_i > l_j$

entropia kódolás elve ez [Shannon-Fano]

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

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

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

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

kiseb 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

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

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

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

$x_3 \rightarrow 110$

$x_4 \rightarrow 1110$

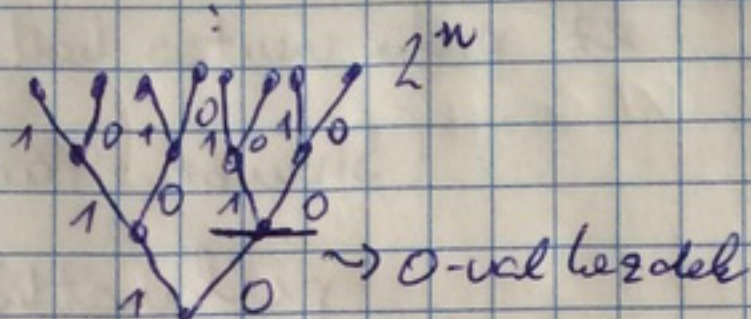
Prefix-kód generálása:

Egy kód prefix \iff ha teljesül a Kraft egyenlőtlenség.

i-edik kód hossza

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

bin. fa:

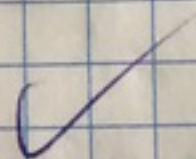


ha elkezdem 0-val \rightarrow lépésenként az ágak



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

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

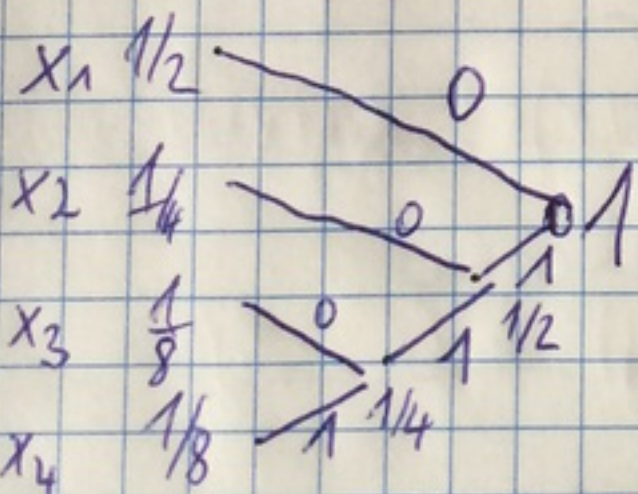


(a teljes fával többet nem vehetők ki)

Kraft.

Huffman:

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

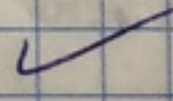


bináris fa

\rightarrow rekurzívum!

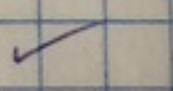
amíg nem csak 1-ből!

$x_1 \rightsquigarrow 0$



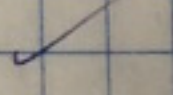
levegőben

$x_2 \rightsquigarrow 10$

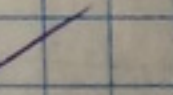


prefix ~~...~~ + Shannon Fano!

$x_3 \rightsquigarrow 110$



$x_4 \rightsquigarrow 111$



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

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

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

HUFFMANN-hoz kell a valószínűség!

nem jó kevés kódnál, és nagy valószínűség differenciál!

kernéljük 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

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

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

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

DHS
 \downarrow
 Stacioneris
 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 eseményleg
 tartozó 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

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

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

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)

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

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

(C)

$H_n(X)$ mon. növekvő

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

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

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

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

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

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

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

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

+ 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

elvé: könyvet át 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'

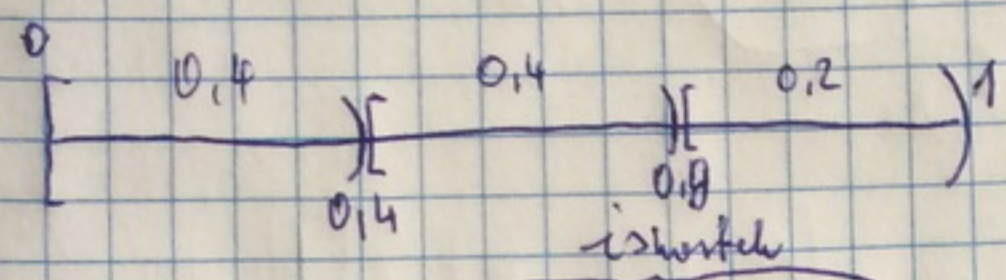
és így tovább

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

→ Nem kell hozzá ismernem a priori az eloszlást.

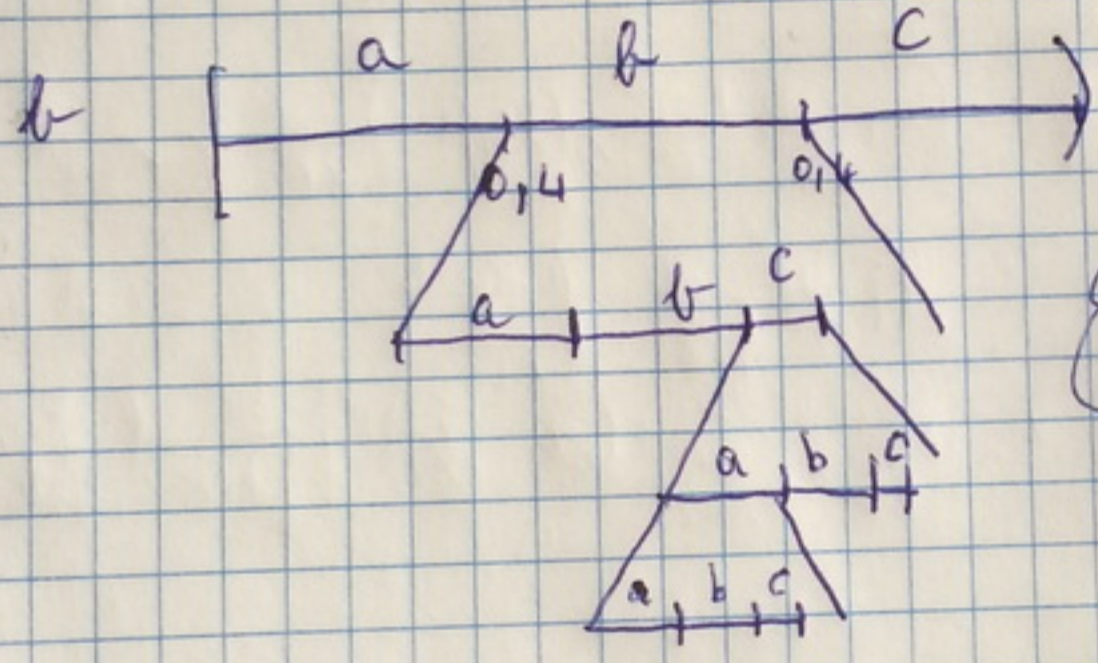
Aritmetikai kódolás:

- 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 jónakitegyezés)

$0.75 = 0.11$
 $2^{-1} 2^{-2}$ 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:

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

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:

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

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

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

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 esetén a maximális érték.

Shannon II. csatorna kapacitás valószínűségi tétel:

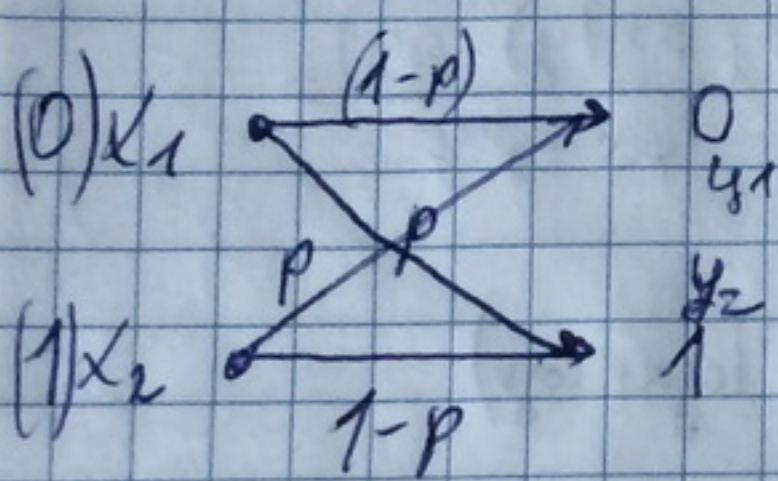
ha: $H(X) < C$ akkor $\exists \Omega(X) = X$
 Perror $\rightarrow \emptyset$ ha $H(X') < C$
 hiba val. s \acute{e} g.

M \acute{e} rs \acute{o} lt 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} rt \acute{o} kb \acute{o} l n n \acute{e} mb \acute{o} l \acute{o}

DMC - discrete memoryless channel

1) BSC

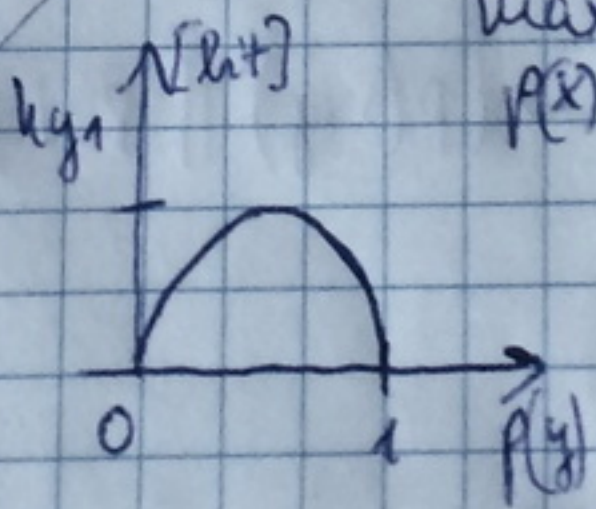


p valószínűséggel hibéz \acute{e} k
 $1-p$ valószínűséggel nem hibéz \acute{e} k

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

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

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

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

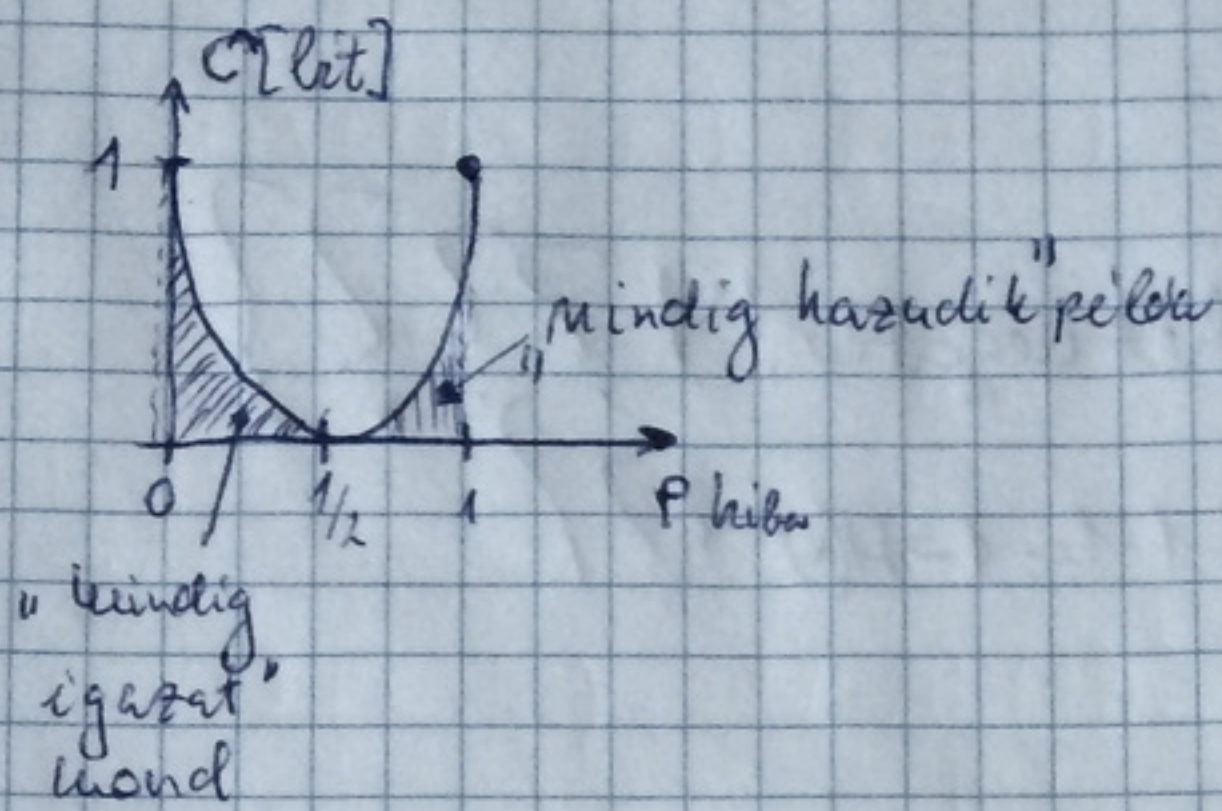
$$\frac{1-p(x)}{x_2} \cdot \left[p \cdot \log_2 \frac{1}{p} + (1-p) \cdot \log_2 \frac{1}{1-p} \right] =$$

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

nem függ a forrás

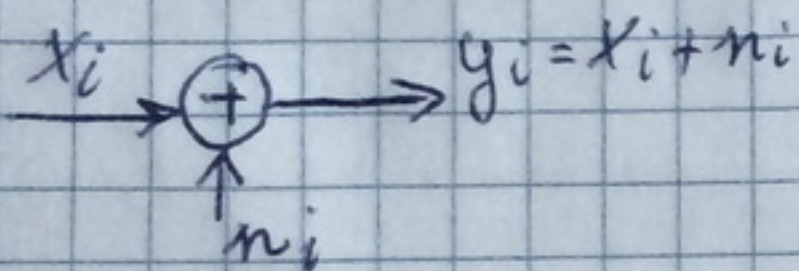
eloszlástól! csak p hibeválts \acute{e} gtől!

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



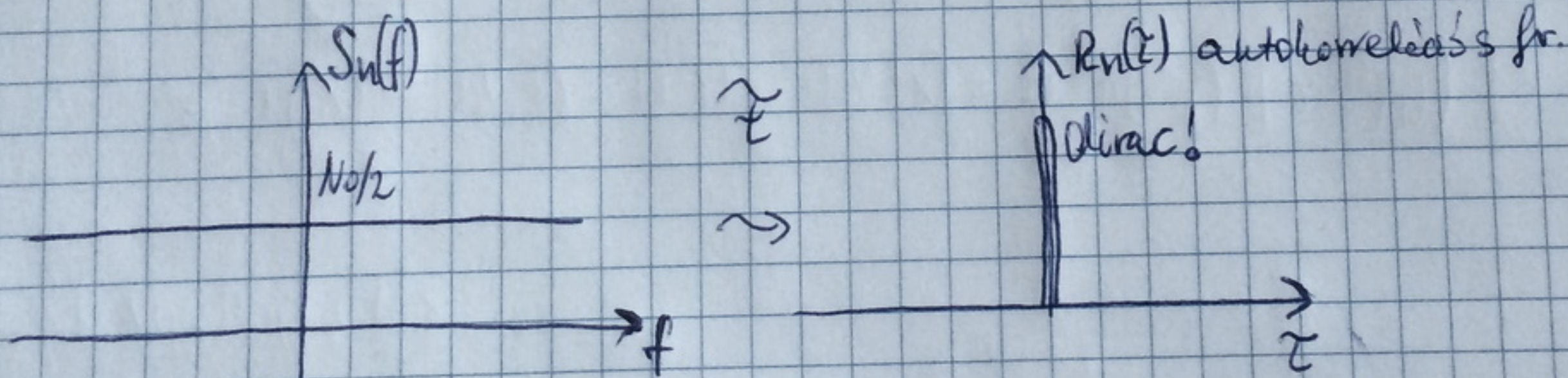
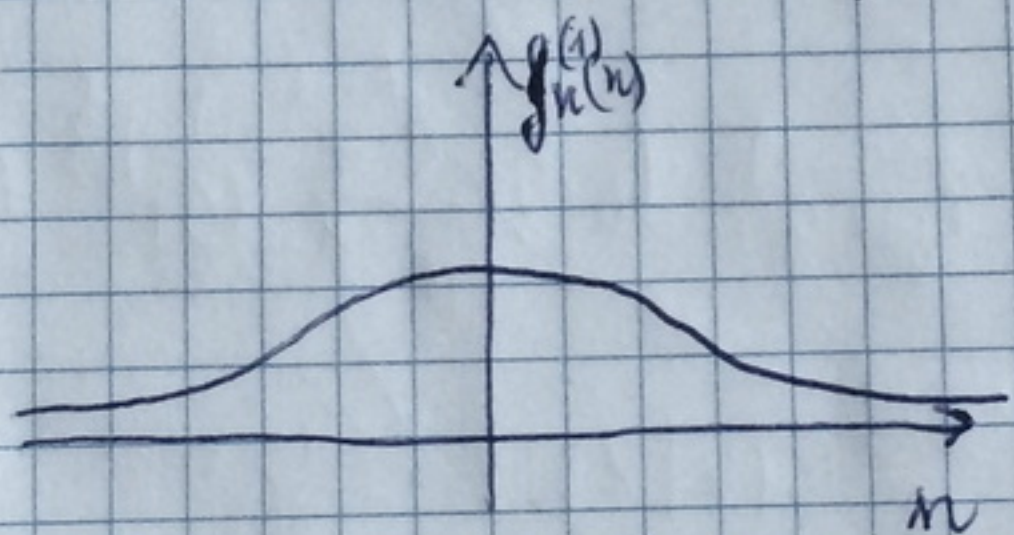
ha $\frac{1}{2}$ akkor foglalom sincs az információról, $C=0$

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



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

előrendű
sűrűségf.



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

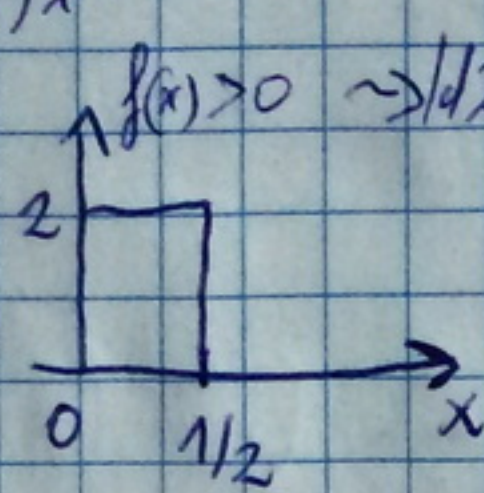
hell az új fogalom!

diszkrét \rightarrow folytonos miatt

differenciális entropia:

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

lehet negatív!!! ???



7. előadás

LOTTO

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

átlékban [bit/s]

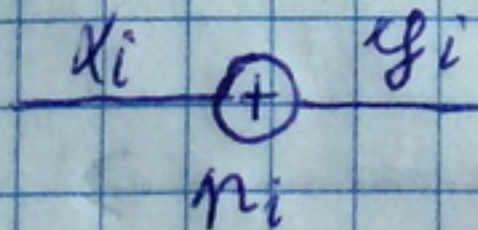
• BSC csatorna:

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

p = hibaválósínűség

DMC - discrete memoryless channel!

D-AGWN:
diszkrétidő
de folyt. értékű

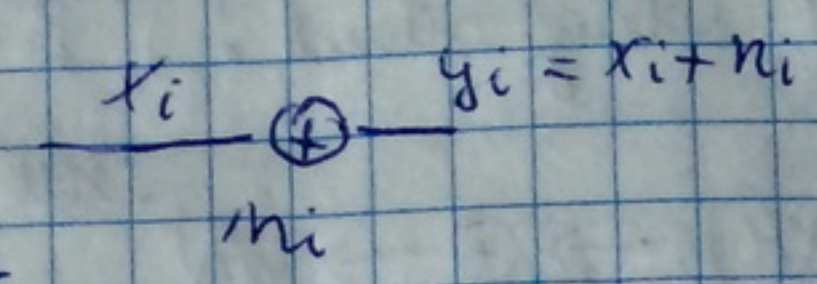


$$H(X(\pm)) = \int_{-\infty}^{\infty} f_X(x) \cdot \text{ld. } \frac{1}{f_X(x)}$$

(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

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

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

D-AGWN esetben! \rightarrow

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

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

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

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

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

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

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

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

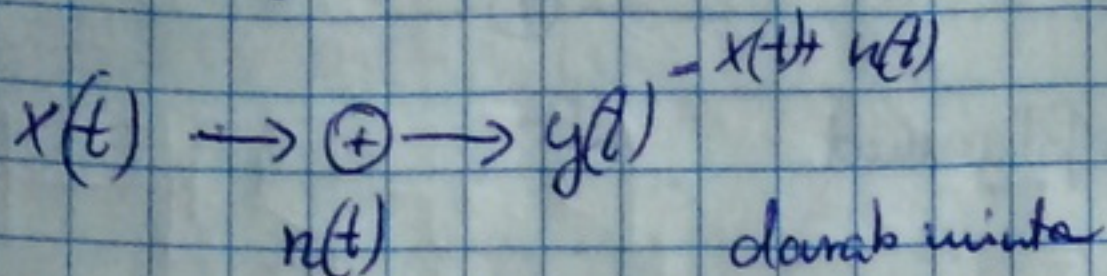
AGWN-nél

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

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

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

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

$= \lim_{T \rightarrow \infty} \frac{1}{T} \max_{P(x)} \underbrace{k}_{\text{ez a D-AGWN csatorma}} I(x, y) = \lim_{T \rightarrow \infty} \frac{1}{T} \cdot \underbrace{k}_{\text{Trinns}} \cdot \underbrace{\text{ld} \left(1 + \frac{\sigma_x^2}{N_0/2} \right)}_{\text{D-AGWN } \sigma_x^2}$

folgt. AGWN

$C = B \cdot \text{ld} \left(1 + \frac{\sigma_x^2}{N_0/2} \right) = B \cdot \text{ld} \left(1 + \frac{\text{PAVG}}{2B \sigma_n^2} \right)$

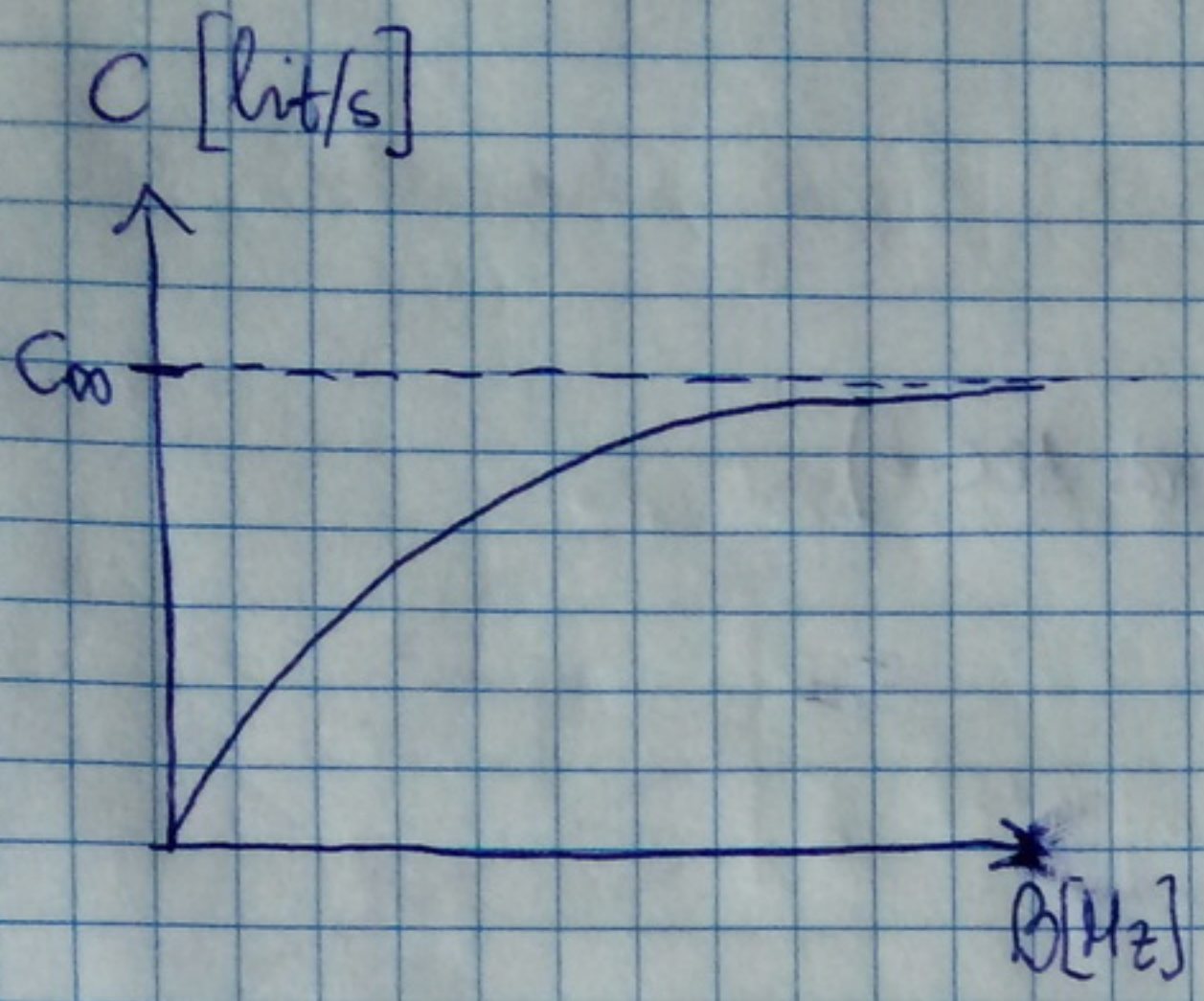
$\sigma_x^2 = \frac{\text{PAVG}}{2B}$

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

$C = B \cdot \text{ld} \left(1 + \frac{\text{PAVG}}{B \cdot N_0} \right) \text{ [bit/s]}$
AGWN
sávkorlátos B
T ideig

$C_{\infty} = \frac{\text{PAVG}}{N_0} \cdot \text{ld} e = \frac{\text{PAVG}}{N_0 \cdot \ln 2}$

ha
lemez
végtelen
felhő



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

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

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

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

8. előadás:

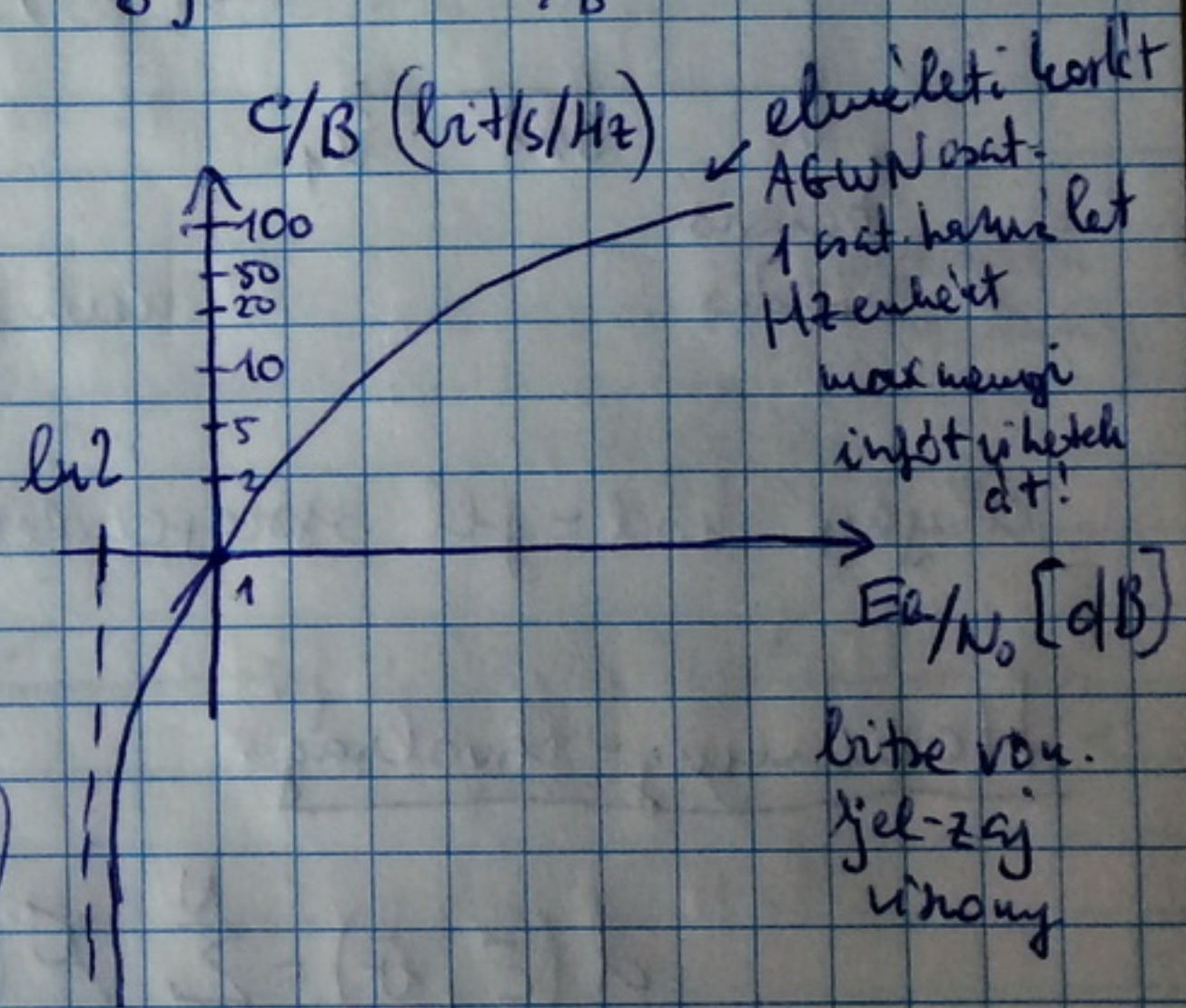
~~$\frac{E_b}{N_0} = \exp \left[\frac{C}{B} \cdot \log_2 \left(1 + \frac{E_b}{N_0} \frac{C}{B} \right) \right]$~~

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

ha $C/B \rightarrow \infty$

ha $C/B \rightarrow 0$

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



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

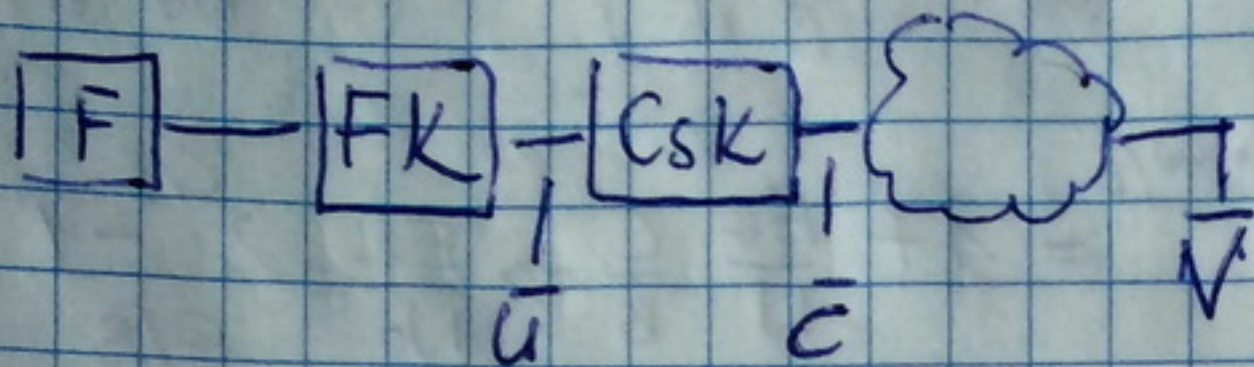
$\lim_{K \rightarrow \infty} \frac{K}{N} < C ; P_e \rightarrow 0$ [1s-re vonatkoztatva van]

$\frac{K}{N} < 1$ erős feltétel !!

Hibajavító kódolás: (N, K, q)

(error correction coding)

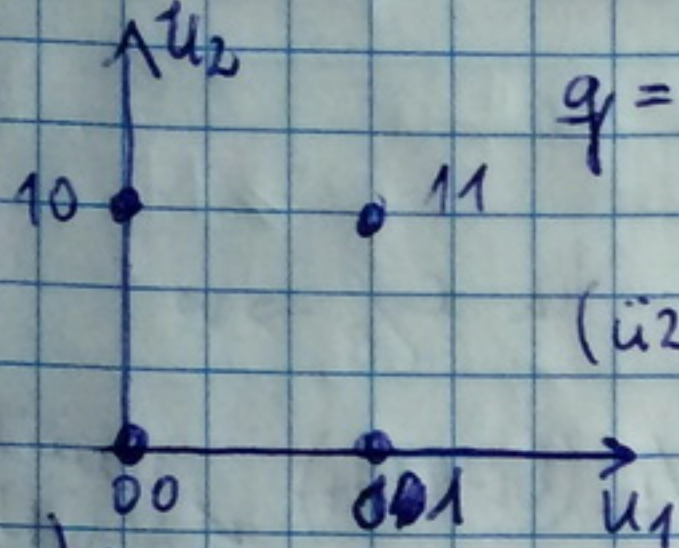
érték halmaz (forrás ABC-e)



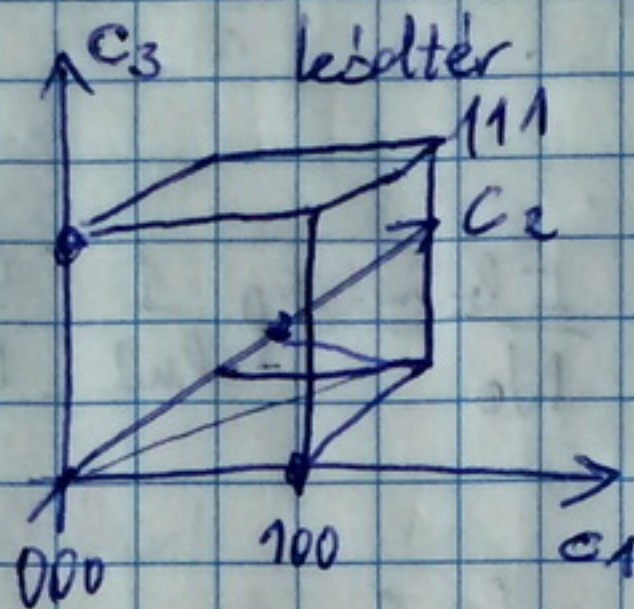
$$\bar{u} = [u_1 \ u_2 \ \dots \ u_k]$$

$(N > K)$

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



(üzenet-tér) \rightarrow



nem értékes olyan összerendelés $\rightarrow 00 \rightarrow 000$
 $01 \rightarrow 001$

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

Hamming-távolság:

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

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

minimális Hamming távolság.

döntő
 vett jel \rightarrow kell amire döntök

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

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

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

+ nem tudok hibát javítani,
 ha $c' \neq c$ de c' érvényes kód!

(másra döntök tökéletesen)

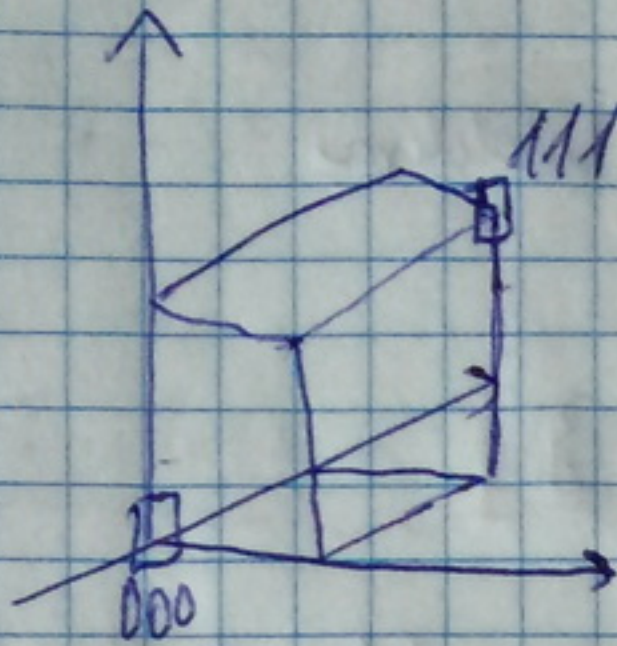
olyan halmazt kapok, ami nem eleme az érték halmaznak!

de tudom detektálni!

ha növekvő $\frac{k}{N}$ -t

00 → 000
11 → 111

ismertleges kódolással



Algebrai konstrukciók: ... következő oldal!

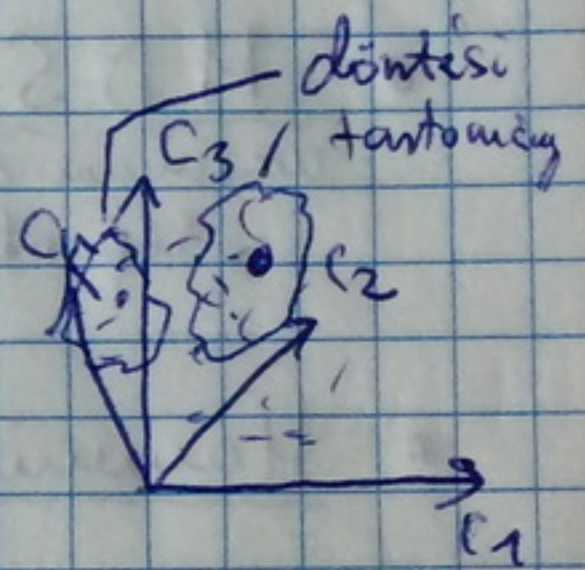
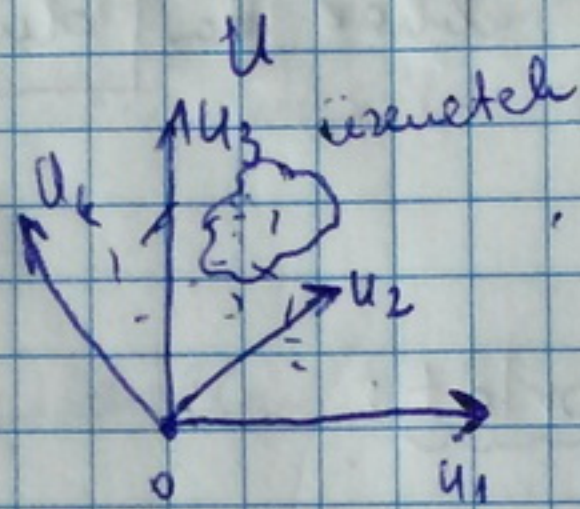
8. előadás

Kezelhető hibák az átvitelben!

üzenetek kódok

$$\bar{u} = [u_1, \dots, u_k] \quad \bar{c} = [c_1, \dots, c_N]$$

q^k q^N

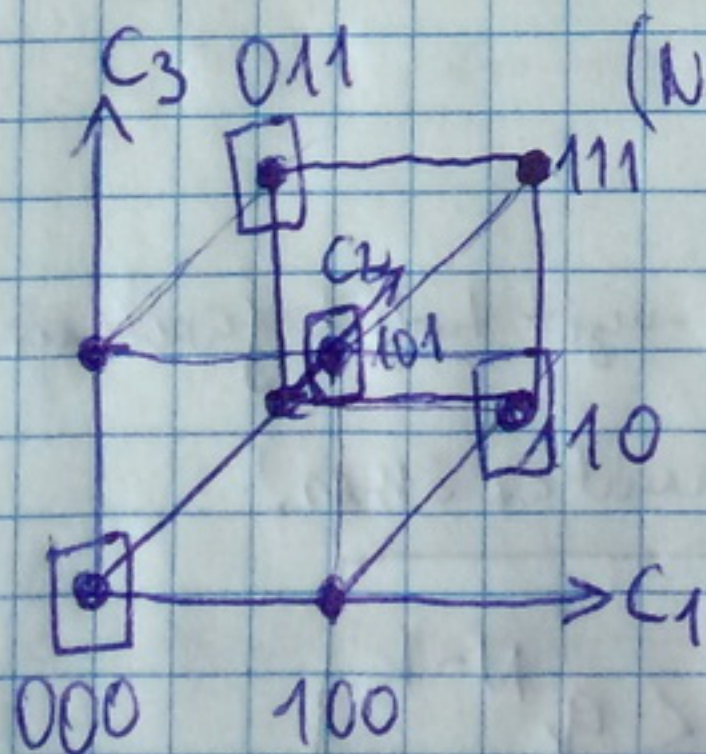


$t_{\text{jelezhető hibák száma}} < d_{\text{min}}$ (diszjunkt halmazok miatt) ; $t_{\text{jelezhető}} = d_{\text{min}} - 1$
[döntési tartományok]

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

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

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



(N=3, k=2, q=2)

1) 000 hozzá közelebb nem vilantom

2) 011, 101, 110, és kész!

ha 110 érkezik ≠ 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?

$M \leq q^k$ ~~$M \leq q^N$~~ $d_{\min} \leq 1 + N - k$ ha = akkor a legjobb!
 (ehelyett van még legtovább)

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

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

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?

$1 + N(q-1)$ [1 ponttól, 1 Hamming távolosítás]

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

t_{jav} esetén $1 + \binom{N}{t_{\text{jav}}}(q-1)^{t_{\text{jav}}}$
1 érvényes kód
 $q-1$ rossz kód

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

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

ezt meg kell, hogy t_{jav} -nyit tudjunk javítani!

üzemeknek néma
~~átvitel~~

- 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:

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

- Perfekt a kód ha:
$$\sum_{i=0}^{t_{\max}} \binom{N}{i} \cdot (q-1)^i = q^{N-k}$$

(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 használható \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!
 $\{C\}$
- generátor

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

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

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

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

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 $\underline{H} = [1 \ 1 \ 1]$

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

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

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

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