Hírközlés elmélet

dr. Bitó János

Szerda $8^{\underline{15}}$ IE220

Csütörtök 10^{15} E1C

4 kis ZH van

inkrementális ZH rendszer!

2 legjobb ZH átlaga

10 hallgató felett

össz 15 pont

4 pont 4,5-7 1

7,5, 9 - 2

9,5 - 11 - 3

11,5 - 13 - 4

13,5 - 15 - 5

ZH: 3 részr ⇒ tesz példa tétel

10 tentes feleletbefejezés (infokommunikáció)

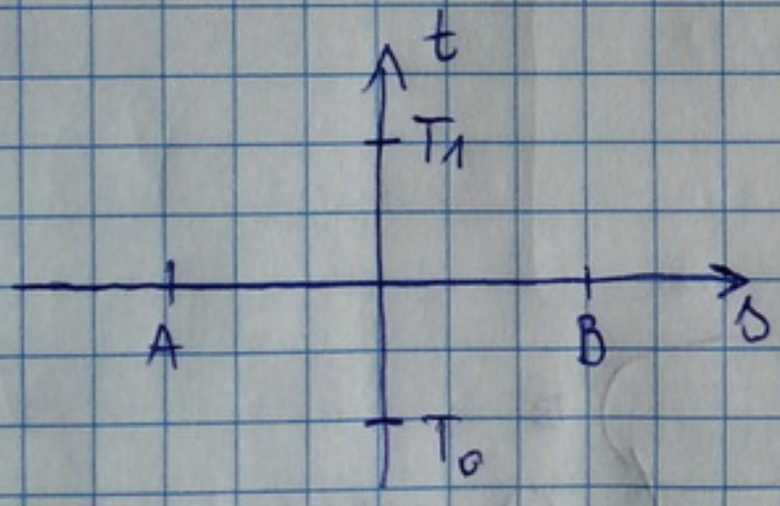
tétel kifejtés

példa számolás

1. előadás

információ források üzeneteinek eljuttatása az információ vevőjéhez = HÍRKÖZLÉS

+ Zaj, zavar, interferencia (mesterséges vagy természetes)



időben vagy térben elkülönült pontok

forrás kódolás / tömörítés [időben elkülönültkor]

- mi az információ? Fellel-e a nap holnap?

$P(\text{nap}) \rightsquigarrow 0$ Holnap nem kel fel a nap ⇒ nagy az információ tartalma

- hogyan mérem az információt?

  - kell egy kvantitatív mérték

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

    () az ember alapvető igénye a kommunikáció

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

... ↓ elhelyezés!

(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 kimenetelek közt

$\#\xi = D$ (# ~ 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!

$\#\xi = D$ $I(\xi) = \log_a D$

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

$\log_a D^n = n \cdot \log_a D$

ha $a = 2 \rightsquigarrow \log_2$
⇓
ld [bit]
ha $a = 10 \rightsquigarrow \log_{10}$
⇓
lg [Hartley]

DE2 MÉG NEM JÓ:

példa:

kalap
4 gdyś
1-et húzunk

$D = 2$

$\text{ld } D = 1$ [bit]
bináris digit

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

$\int$

a baj az, hogy a Hartley értéket nem veszi figyelembe a valószínűségi eloszlást!

fehér: $\text{ld } \frac{4}{1} = 2$ [bit]

0 $\text{ld } \frac{4}{3} = 0{,}415$ [bit]

[bit] az információmennyiség mértéke

BIT

B

● = 2

○ = 0,415

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

valószínűség — info tartalom; valószínűség — info tartalom

⇝ kevesebb infó mint egyenletes eloszlásnál

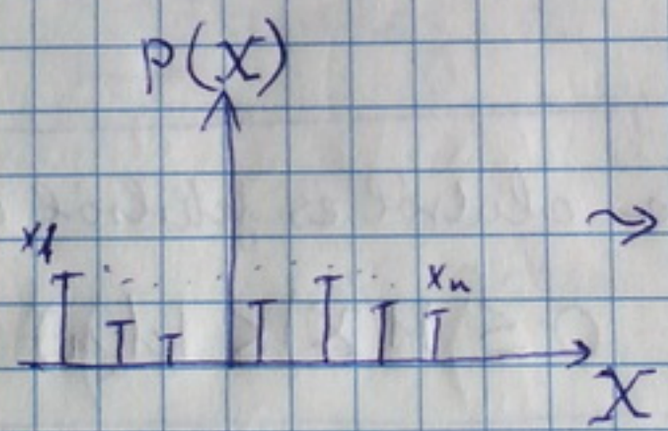
Claude Shannon (1948, BSTJ) – "A Mathematical Theory of Communication"

legyen:

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

X: diszkrét értékű val. változó; $P(X)$: sűrűségfv.

$p_i = p(x_i)$ i-dik esemény



$\Rightarrow F_X(y) = \sum_{y=-\infty}^{\infty} P_X(y) = 1$

$F_X(y)$: eloszlásfüggvény; $= 1$: teljes eseménytér!

Def: $I(x_i) = ld \frac{1}{P(x_i)}$ ⇝ ez egy esemény információja

Minél valószínűbb az esemény annál kisebb az info. tartalom

$\rightarrow -ld(P(x_i))$ [bit]

(Self Information – az esemény saját információ tartalma)

Def: Entrópia, Átlagos információtartalom (entropy)

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

() ⇒ Ugyanis a fájlok

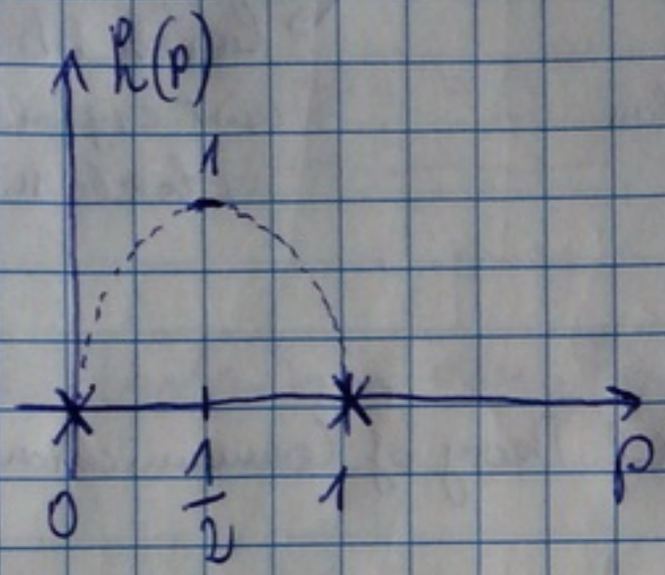
- legyen $X = \{x_1, x_2\}$, $p(X) = \{p(x_1), p(x_2)\} \Rightarrow \{\overset{p}{p(x_1)}; \overset{1-p}{1-p(x_1)}\}$

ezért ez 1 paraméteres

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

$h(p)$ = bináris entrópia fv

határérték probléma a réálon!



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

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

$$\lim_{x \to \infty} \frac{1}{x} \cdot ld x = \frac{1}{\ln(2)} \cdot \lim_{x \to \infty} \frac{\ln(x)}{x} \overset{L'H'}{=} \frac{1}{\ln(2)} \lim_{x \to \infty} \frac{1}{x}$$

$\Rightarrow 0$

irodalom keresés !!! gróki Bitónak

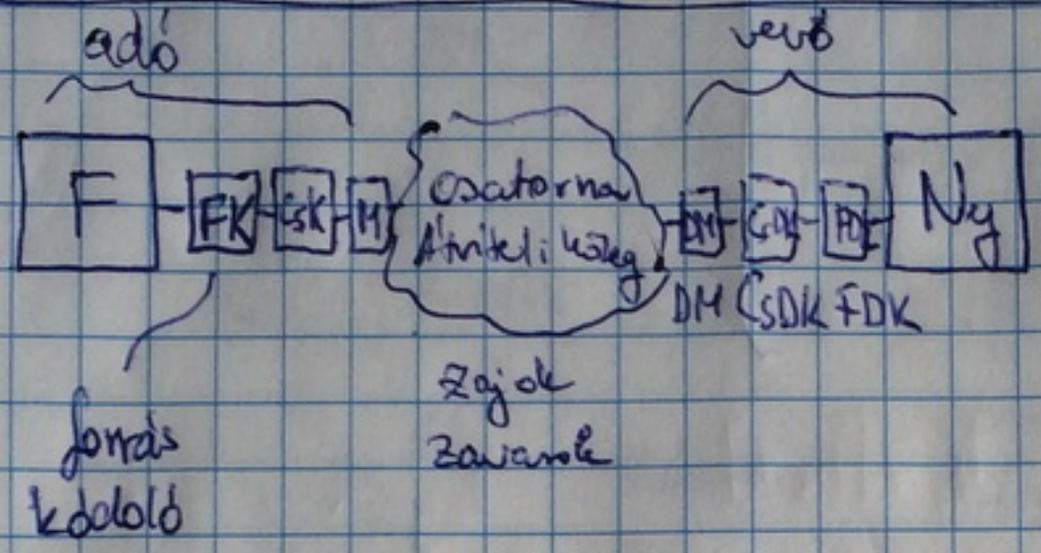
Tétel: az entrópia alulról és felülről is korlátos

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

2. előadás

Proakis, Salehi: Communication Systems Engineering
Dallos: Tantárgyi segédlet a hírközlés elmélet tárgyhoz
Prigyl I.: Hírközlő rendszerek
Csibi S.: Információ közlése és feldolgozása

} IRODALOM



FK: amit redundáns, azt tömöríti [veszteséges és veszteségmentes]

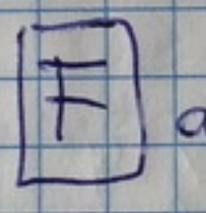
CsK: a fellépő zavarok csillapítása (hibajavító + redundancia hozzáadó)

M: modulátor

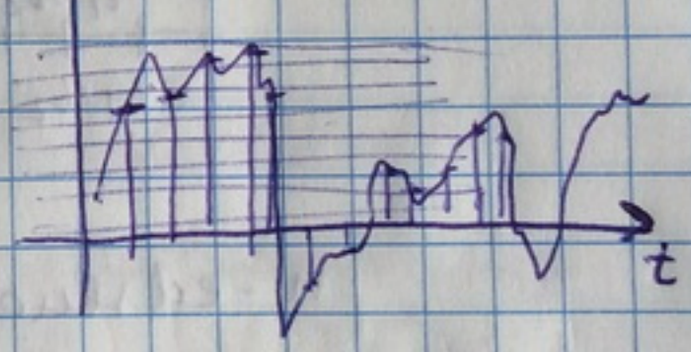
DM: demodulátor

CsDK: csatorna dekóder

FDK: forrás dekódoló



analóg a(t)

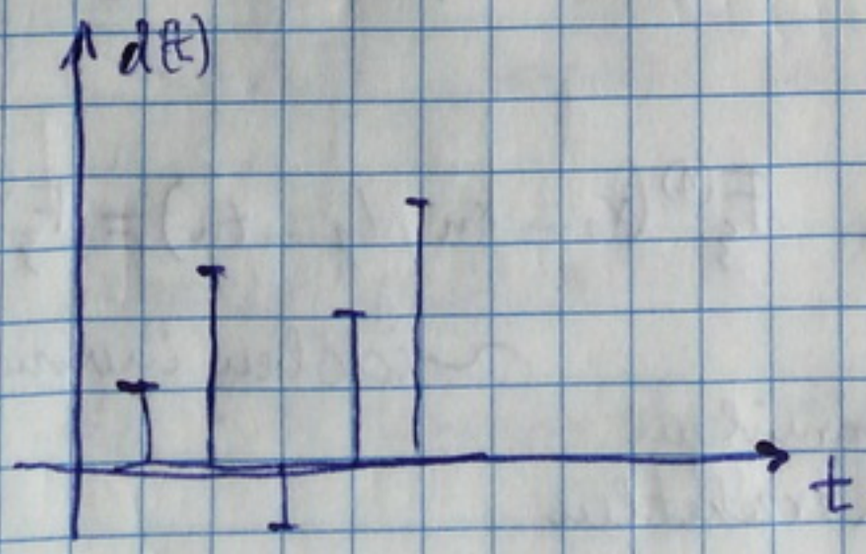


végen Bell idejében

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

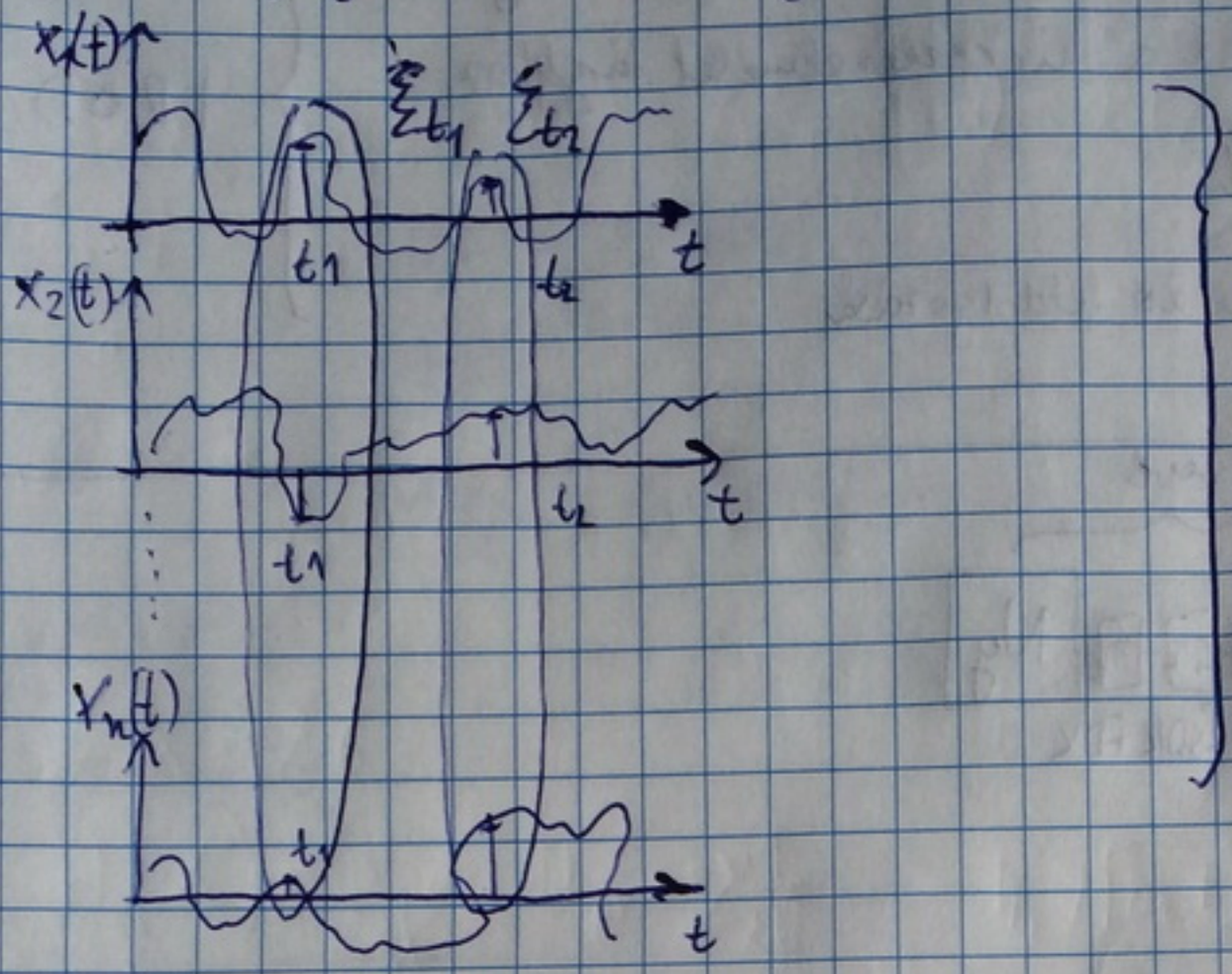
ua digitális jel:

- időben mintavételezett (T)
- értékben kvantált



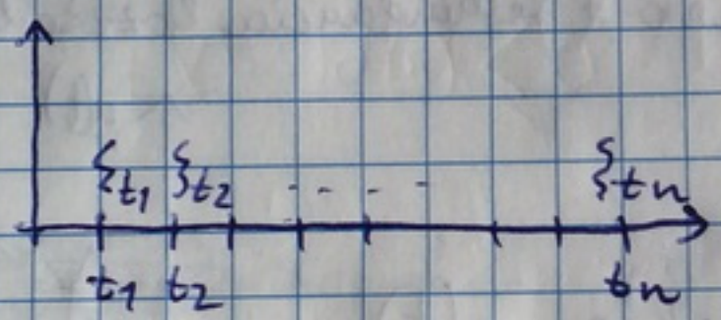
Sztochasztikus folyamatok

① a folyamat realizációjának az együttese



együtt ők a sztochasztikus folyamat!

② Valószínűségi változók rendezett (időben) sereg



n-ed rendű eloszlás fv. (n dimenziós)

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

ξ t_1 t_2 t_n

eloszlás fv.

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

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

  ~ időben invariáns

  $\forall\ \tau, \forall_n, \forall\{t\}$ időben bármilyen eltolásra érzéketlen

Várható értéke

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

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

erősen stacion. folyt. várható értéke időfüggetlen

erősen stac. folyt → ergodikus folyt vagy ergodikus folyt. keveréke

- ergodikus folyamat

bármelyik realizációból meghatározható

$$A(\xi) = \lim_{T\to\infty} \int_{t_0}^{t_0+T} \xi_t\, dt = m_\xi$$

időátlag

- legyen

$$\overbrace{e_\xi(t)}^{\text{jel energiája}} = E\{\xi_t^2\} = \int_{-\infty}^{\infty} x^2 \cdot f_\xi(x,t)\, dx$$

energia, várható érték

- Autokorreláció

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

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

⇓ csak az időkülönbségtől függ (ΔT)

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

- Gyengén staciondrius (Wide-Sense-Stationary)

(másodrendben stacionárius → gyengén stacionárius)

① ⇒ $m_{\xi(t)} = m_\xi$ $\forall t$ időfüggetlen

② ⇒ $R_\xi(\Delta T)$ korreláció csak a különbségtől függ

- ha n rendben stac → $n-1$

de n rendben stac ↛ $n+1$

- Memória mentes: χ

  - forrás

$$P(\xi_n = x_n \mid \underbrace{\xi = x_1, \dots, \xi_{n-1} = x_{n-1}}_{\text{előző betűvetterett}}) = P(\xi_n = x_n)$$

diszkrét
sztochasztikus eloszlás
folytonos(f)

példa:

$$\#X = 26$$

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

entrópia

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

(Tétel: $0 \leq H(X) \leq ld(n)$

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

$$\sum_{x_i \in X} p_{x_i} \cdot ld \frac{1}{p_{x_i}} - \underbrace{\sum_{x_i \in X} p_{x_i} \cdot ld\, n}_{\text{nivel}=1} \leq 0$$

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

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

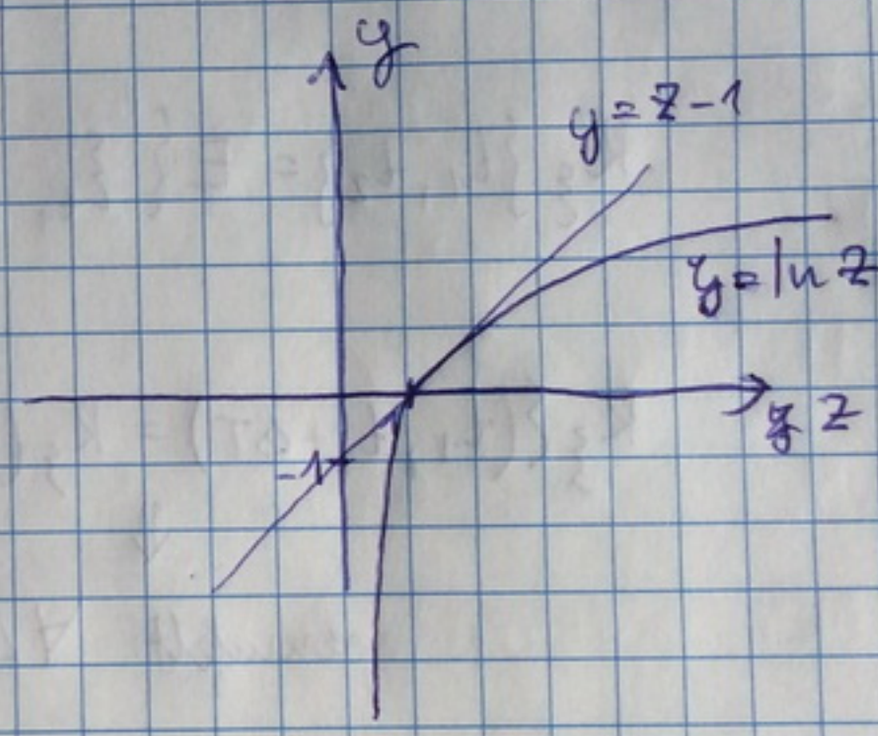
$$\sum p_{x_i} \cdot ld \frac{1}{n \cdot p_{x_i}} \leq 0$$

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

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

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

$$1 - 1 = 0$$



Tömör kódolás

$$H(X) = 4,1 \text{ bit}$$

példa $H_2(X) = 3 \text{ bit}$

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

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

redundancia

entrópia a feltehető kérdések átlagos száma

érdemes annyi biten kódolni, amennyire gyakran fordul elő.

3. előadás

~ eddig amiket tanultunk

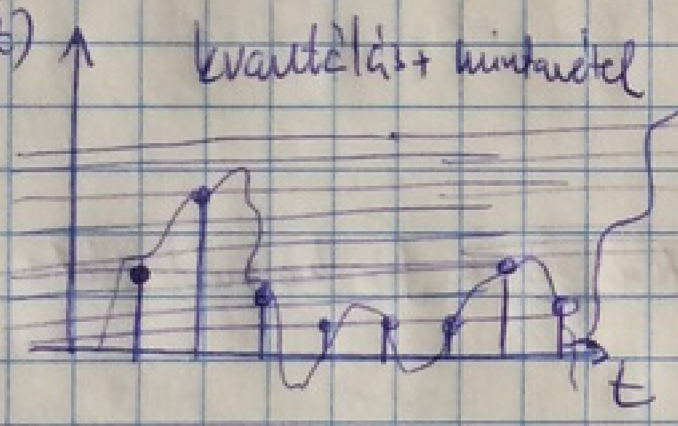
$$F_\xi^{(n)}(\xi_{t_1} < x_1 \ldots \xi_{t_n} < x_n, t_1 \ldots t_n) \overset{\text{röviden}}{=} F_\xi^{(n)}(\overline{x}, \overline{T}) \quad \forall \Delta T \quad \forall \{\overline{T}\}$$

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

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

erősen stac, ha $\forall n$-re !

gyengén, ha nem $\forall n$-re ~

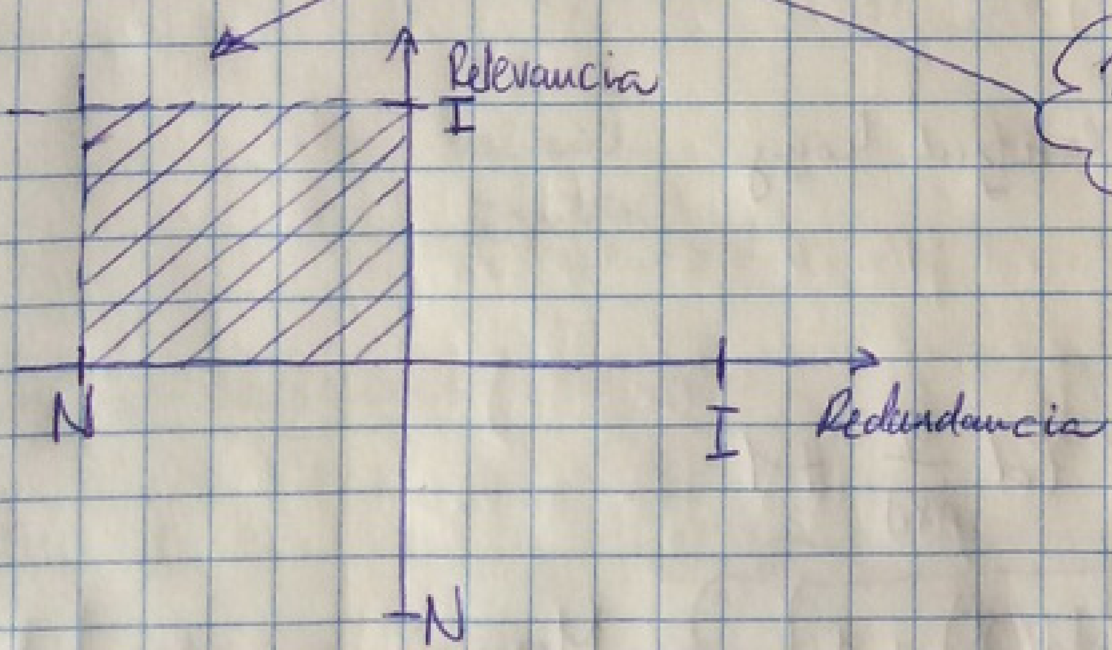


de! ha elcsúszik jel felfelé pl. akkor a kvantáló telítődbe megy mindig

ha változik időben a várható érték ~ nem stacionárius

VALÓS VILÁG FOLYAMATAI

relaváns információ átvitel kevés redundanciával



$$R(X) = \underbrace{\overset{\text{egyenletes eloszlás}}{H_0(X)} - H(X)}_{\text{cél ennek a minimalizálása}}$$

redundancia

Német szöveg:

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

$p(X)$ $\quad H_1(X) = 4,1 \text{ [bit]}$ ← tudjuk a redundanciát

$H_\infty(X) = 1,6$ bit ← teljes szövegre (redundánsabb)

Forrás kódolás

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

- kódolási szabály (Q)

$Q(x_i) = c_i$; dekódolhatóság!, fix hosszú kódolás [5 bit]

a → 00000
b → 00001

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

$p(X) = \{\frac{1}{4}, \frac{1}{4}, \frac{1}{4}, \frac{1}{4}\}$ egyenletes eloszlás esetén jó a fix hosszú kód

- <u>változó hosszú kódolás</u>:

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

átlagos kódhossz

- entrópia kódolás ⇝ $l(x_i)$-t úgy választjuk hogy

~~$l(x_i) \geq \text{ld } \frac{1}{p(x_i)}$~~

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

$$\boxed{H(X) \leq L_x < H(X) + 1}$$

Shannon I.

Memória-mentes!!
forrásra

Shannon-Fano kód ⇝ 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 $[l_i +]$

kompakt kód kell

D+M forrás:

⇝ A memória:

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

feltételes valószínűség

⇝ lehetne feltételes entrópia is!

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

FELTÉTELES ENTRÓPIA

együttes entrópia:

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

n darab val. vált. együttese

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

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

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

$$\Rightarrow -\sum_X \underbrace{\left(\prod_{i=1}^{n} p(x_i \mid x_1 \dots x_{i-1})\right)}_{\text{együttes val.sz}} \underbrace{ld\, p(x_1)}_{\text{sülyozva } x_1\text{-gyel}} - \sum p(x_1 \dots x_n) \cdot ld\, p(x_2 \mid x_1) - \dots -$$

$$\underbrace{\sum_X p(x_1 \dots x_n)\, ld\, p(x_n \mid x_1 \dots x_{n-1})}_{\text{ezek feltételes entrópiák}}$$

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

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

1 szimbólumra eső entrópia

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

- Sztochastikus folyamat entrópiája

ha van $\Rightarrow$ $\boxed{H_\infty(X) = \lim_{n\to\infty} \frac{1}{n} \cdot H(\bar{X}^n)}$ — együttes entrópia

vagy $\Rightarrow$ $H_\infty(X) \overset{(\exists)}{=} \lim_{n\to\infty} H(X_n \mid X_1 \dots X_{n-1})$ ha WSS legalább a folyamat

DMS esetben

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

ftlen események

$H(\bar{X}^n) = \sum_{i=1}^{n} H(X_i)$ → mert ftlenek az entrópiái!

ha WSS a forrás (:időftlen → index ftlen)

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

$\Downarrow$

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

Forrás-kódolás:

dtt. kódhossz

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

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

$L_X = \frac{1}{2}\cdot 1 + \frac{1}{4}\cdot 2 + \frac{1}{8}\cdot 3 + \underbrace{\frac{1}{8}\cdot 4}_{\text{„élése"}}$

[abcd példára]

~ kedden ZH

E1B 18$^{\underline{15}}$)

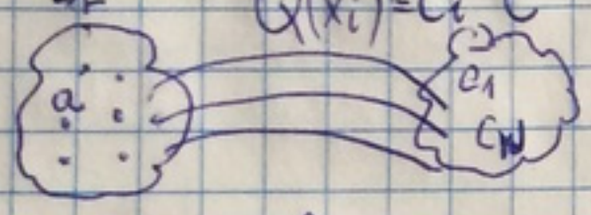
---

4. előadás

tanár: példa, tétel

Forráskódolás

X $\quad Q(x_i) = \bar{C}_i$ $\bar{C}$



forrás ABC diszkrét $\quad\uparrow\quad$ kód ABC diszkrét

kódszavakon egyértelmű kapcsolat

DMS + memória

pillanatnyi kódolónak kell lenni ⇝ azonnal el kell tudjam dönteni a forrás ABC elemet!

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

↓ egy kód hossza

kódszimbólumok ahány [0,1] de lehet más is!

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

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

entrópia kódolás elve ez [Shannon-Fano]

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

$\Downarrow$

$l_i = k_i = ld\ \frac{1}{p(x_i)}$

ez teljesíthető-e a Shannon I-et ?

$\Downarrow\Downarrow$

$$H(X) = \sum_{x_i} p(x_i) \cdot ld \frac{1}{p(x_i)}$$ → egyenlőség van "alulról"

ez alá nem tudok menni

$L_x = \sum p(x_i) l_i$

$l_i = ld \frac{1}{p(x_i)}$

$$h_Q = \frac{H(X)}{L_X}$$ → mindig kisebb, mint (1)

hatékonysága a forráskódnak

Shannon-Fano → minimális átlagos kódhossz

Példa:

X	p(x_i)	fixhossz Ⓐ
x_1	1/2	00
x_2	1/4	01
x_3	1/8	10
x_4	1/8	11

$$HX = \frac{1}{2} \cdot 1 + \frac{1}{4} \cdot 2 + \frac{1}{4} \cdot 3 \Rightarrow 1{,}75 \text{ [bit]}$$

ez pillanatkód!!!

Ⓐ $L(X) = 2$ fix hosszú kód miatt!

eset $h_{Q_Ⓐ} = \frac{1{,}75}{2} = 0{,}875$ miért nem 100% → nem használtuk az apriori ismeretet (a valószínűségeket)

→ fix hosszú kódot mindig lehet dekódolni!

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

legyen $x_1 \rightarrow 0$, $x_2 \rightarrow 1$, $x_3 \rightarrow 00$, $x_4 \rightarrow 11$

Ⓑ eset

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

lehetséges dekódolások ????

nem dekódolható!

Ⓒ prefix kód $x_1 \rightsquigarrow 0$ $x_3 \rightsquigarrow 110$

eset (változóhosszú kód) $x_2 \rightsquigarrow 10$ $x_4 \rightsquigarrow 111$

↓

$\bar{c}_i = (c_{i1} \dots c_{ik_i})$ akkor ~~X~~ olyan $\bar{c}_j$ ~~$\exists$~~ $\forall$ ahol $l_j > l_i$, $c_j = (\underbrace{c_{i1} \dots c_{ik_i}}_{\text{azelje olyan mint a másik kód}}, c_{j(k_i+1)} \dots c_{ej})$

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

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

ez prefix mentes kód ⇝ dekódolható

(Shannon - Fano kód)

pillanatkód

Ⓓ szeparátort kezetünk be: pl egy vesszőt! [comma - code]

$x_1 \rightsquigarrow 0$ elválasztó

$x_2 \rightsquigarrow 01$

$x_3 \rightsquigarrow 011$

$x_4 \rightsquigarrow 0111$

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

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

Ⓔ {prefix és comma-code}

$x_1 \rightsquigarrow 0$

$x_2 \rightsquigarrow 10$ ← separator

$x_3 \rightsquigarrow 110$

$x_3 \rightsquigarrow 1110$

$L_x = 1{,}875$

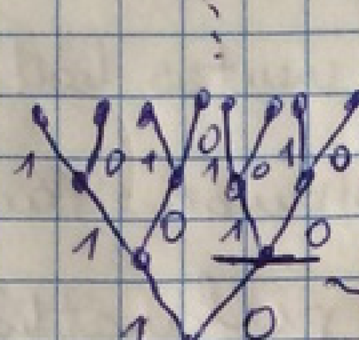
Prefix-kód generálása:

egy kód prefix $\Longleftrightarrow$ ha teljesül a Kraft egyenlőtlenség.

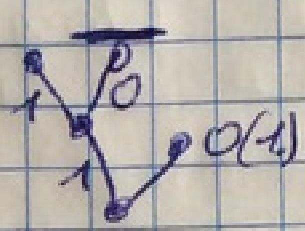
(i-edik kód hossza)

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

bin. fa:



ha elkezdem 0-val → lefűrészelem az ágat



$N - l_i$ szintű részfákat vágok ki egy l_i-hosszú kód szerkesztésekor

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

teljes fa! Kraft. ✓

(a teljes fánál többet nem vághatok ki)

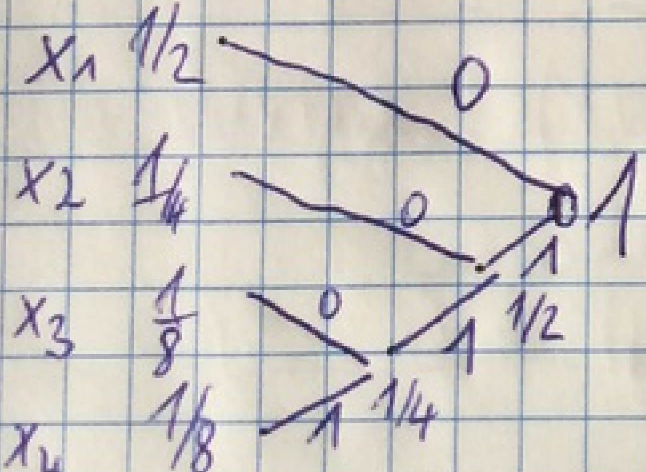
Huffmann:

① ~> előfordulási valség szerint sorba rendezed!

② ~> bináris fa, 2 legkisebb valségű eseményt rakd össze!

→ rekurzívan!

amíg nem érek 1-hez!



bináris fa

$x_1 \rightsquigarrow 0$ ✓ levágom

$x_2 \rightsquigarrow 10$ ✓

$x_3 \rightsquigarrow 110$ ✓

$x_4 \rightsquigarrow 111$ ✓

prefix + Shannon Fano!

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

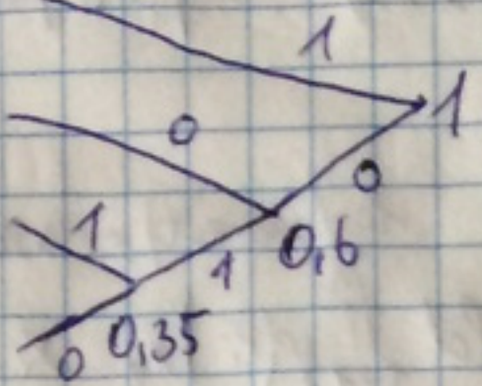
$p(x_i)$ $\quad$ c

Rl: x_1 $0,4$ $\quad x_1 \to 1$

x_2 $0,25$ $\quad x_2 \to 00$

x_3 $0,2$ $\quad x_3 \to 011$

x_4 $0,15$ $\quad x_4 \to 010$



HUFFMANN

$0,5 \quad 0,6 \quad 0,45$

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

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

HUFFMANN-hoz kell a valószínűség!

nem jó kevés hibával, és nagy valószínűség különbségnél!

használjuk a <u>forráskiterjesztés módszerét</u>!

$x_1 x_1$

$x_1 x_2$

$x_1 x_3$

$x_1 x_4$

$x_2 x_1$

$\vdots$

4^2 esetünk van! ↗ kell ismernünk az eseménypárok val.ségét

↘ ha DMS → akkor $p(x_1, x_2) = p(x_1) \cdot p(x_2)$

mindig igaz

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

$H(\bar{X}^n) = H(x_1 \dots x_n) = n \cdot H(X)$ ← DMS → stacionárius időben (n) nem változik $H(X) = H(X_i) \; \forall i$-re

kiterjesztett forrás hoz tartozó

↑ tetszőleges $\quad \underbrace{n \cdot H(X)} \quad \underbrace{H(\bar{X})} + 1$

$n \cdot H(X) = H(X_1 \dots X_n) \leq L_{x_1 \dots x_n} < H(\bar{X}) + 1 \quad \Big| : n$ darabra

n-darab val.változó által generált eseményhez tartozó hdd

$H(X) \leq L_X < H(X) \cdot \frac{1}{n}$ ⇝ ha a kiterjesztést növelem akkor 100%-hoz tartok!

ez jó DMS esetben!

MS esetén

$$p(X_1 \dots X_n) = p(X_1) \cdot p(X_2 \mid X_1)\, p(X_3 \mid X_2 X_1) \cdot \dots \cdot p(X_n \mid X_1 \dots X_{n-1})$$

$$= \prod_{i=1}^{n} p(X_i \mid X_1 \dots X_{i-1})$$

log(szorzat) = összeg (log)

$$H(X_1 \dots X_n) = -\sum \prod_{i=1}^{n} p(x_i \mid x_1 \dots x_{i-1}) \cdot \log \prod_{i=1}^{n} p(x_i \mid x_1 \dots x_{i-1}) =$$

n val vált.
együttes entrópiája

$$= \sum_{i=1}^{n} H(X_i \mid X_1 \dots X_{i-1})$$

? ha létezik

$$\frac{1}{n} H(X)_n = \frac{1}{n} \cdot H(X_1 \dots X_n) \qquad \text{ha } n \to \infty \quad H_\infty(X) = \lim_{n \to \infty} \frac{1}{n} H(X_1 \dots X_n)$$

1 szimbólumra
eső entrópia

↓
sztochasztikus
folyamat
végtelen sokszor
val. vált. szerg!

MS esetén

$$p(X_1 \dots X_n) = p(X_1) \cdot p(X_2 | X_1)\, p(X_3 | X_2 X_1) \cdot \dots \cdot p(X_n | X_1 \dots X_{n-1})$$

$$= \prod_{i=1}^{n} p(X_i | X_1 \dots X_{i-1})$$

log(szorzat) = összeg (log)

$$H(X_1 \dots X_n) = -\sum \prod_{i=1}^{n} p(X_i | X_1 \dots X_{i-1}) \cdot ld \prod_{i=1}^{n} p(X_i | X_1 \dots X_{i-1}) =$$

n val vált.
együttes entrópiája

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

$$H_n(X) = \frac{1}{n} \cdot H(X_1 \dots X_n)$$

ha $n \to \infty$ $H_\infty(X) = \lim_{n \to \infty} \frac{1}{n} H(X_1 \dots X_n)$

1 változón erő! ? ha létezik

1 szimbólumra eső entrópia

sztochasztikus folyamot végtelen sendtett val. vált. sereg!

~~$H_\infty(X)$~~ ~~X_n~~

$$H_\infty(X) = \lim_{n \to \infty} H(X_n | X_1 \dots X_{n-1})$$

1 szimbólumra eső entrópia egy sztochasztikus folyamnak!

(A) 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 entrópia

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

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

$$H_n(X) = \frac{1}{n} \cdot [H_{(\text{szabály})}(X_1 \dots X_n)] \overset{\text{def!}}{=} \frac{1}{n} \cdot \sum_{i=1}^{n} H(X_i | X_1 \dots X_{i-1}) \geq \frac{1}{n} \cdot n \, H(X_n | X_1 \dots X_{n-1})$$

n-szer lesem. ↓ (A) miatt

(C) $H_n(X)$ mon. csökkenő

$$H_n(X) = \frac{1}{n}\left[H(\underbrace{X_1 \dots X_{n-1}}_{n-1 \text{ val változó}}) + H(\overbrace{X_n | X_1 \dots X_{n-1}}^{\text{követező}}) \right] = \frac{1}{n}\left[(n-1) \cdot H_{(n-1)}(X) + \right.$$

$$\left. H(X_n | X_1 \dots X_{n-1}) \right] \leq \frac{n-1}{n} \cdot H_{n-1}(X) + \frac{1}{n} \cdot H_n(X) \rightsquigarrow$$

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

$\rightsquigarrow \frac{n-1}{n} \cdot H_n(X) \leq \frac{n-1}{n} H_{n-1}(X)$ mon. csökkenő ✓

$1 \to (n-1)$ $n \to (n+j)$ $n \to \infty \Rightarrow 1$ $n \to \infty \Rightarrow \infty$

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

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

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

+ sztochasztikus folyamat!

ezek egyszerre csak akkor igazak ha egyenlők

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

ez akkor van ha erősen stac. a folyamat

ha van forrás kiterjesztés:

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

$$H_n(X) \leq L'x < H_n(X) + \frac{1}{n}$$

ha $n \to \infty \to L'x = H_n x$ (ha teljesen ismerem a folyamatot!)

azáltal kódhossz elvehet az entrópiáig.

$L_x = H_\infty(X)$
optimum
apriori ismernem kell
a forrást!

L-Z kódolás (Lempel-Ziv)
- apriori ismeretek nélkül is működik és közelíti az optimumot
- UNIX-ban ez működik

elve: könyvet átalakok vinni, ehhez felépít egy könyvtárat
és csak a címet kell megadnom.

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

← itt van az „1"

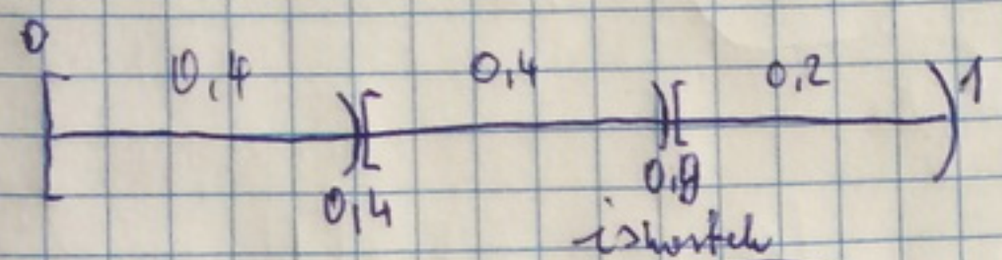
és így tovább

0,1,11,00,10
[011100101001111001] bitsorozat

→ nem kell hozzá ismernem apriori az eloszlásokat.

Aritmetikai kódolás:

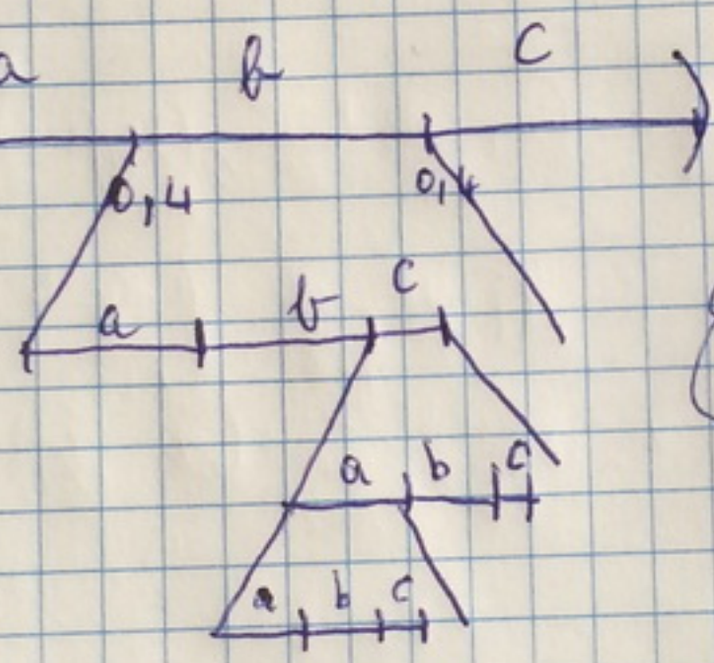
- kell a P(x)
- tart az optimális hosszú kódhoz
- hitka sorozat → rövid kód, gyakori sorozat → rövid kód



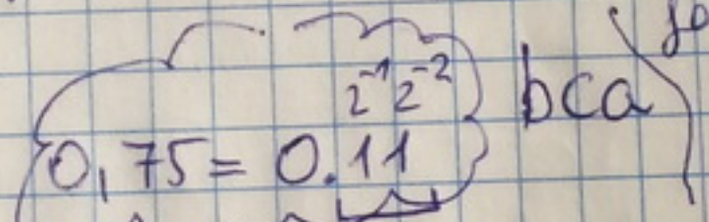
ismertek

$X = \{ a, b, c,\ p(a) = 0,4,\ p(b) = 0,4,\ p(c) = 0,2 \}$

[b, c, a] átvendő sorozat



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



ezt küldöm át
mert ez egyértelműen meghatároz
egy résintervallumot!

de változó hosszú a kód

kell mindenképp egy
stop szimbólum p(!)

~~nincs prefix mentes~~

1. ZH eddig

6. előadás

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

$q(x)$ - szel becsüljük a $P(x)$ eloszlást

relatív entrópia: $\sum p(x_i) \cdot ld \frac{P(x_i)}{q(x_i)}$

(Kullback - Leibler távolság)

Def: A relatív entrópia:

$$D(P(x) \| q(x)) = \sum_{x \in X} p(x_i) ld \frac{p(x_i)}{q(x_i)}$$

távolság

2 eloszlás mennyire hasonlít egymásra! ha $p(x_i) = q(x_i) \rightsquigarrow$ <u>távolság = 0</u>

$$H(X) + D(p\|q) \leq L_x < H(X) + D(p\|q) + 1$$

Shannon I.

ahol $D(p\|q)$ p és q eloszlás Kullbach - Leibler távolság

... forráskódolás végé ...

a-posteriori entrópia:

$$H(X|Y) = H(X) - I(X;Y)$$

(val. vált.)

$H(X|Y)$: átlagos kölcsönös információ (X,Y-ban mennyi megvan)

és $H(X|Y) \leq H(X)$

def: kölcsönös információ:

$$I(x_i, y_i) = ld \frac{p(x_i|y_i)}{p(x_i)} = \text{Bayes} = ld \frac{p(x_i, y_i)}{p(x_i)\cdot p(y_i)}$$

($x_i y_i$ együttes valósége / $p(y_i)$)

$p(x_i|y_i)$: megfigyelve y_i-t

ha $p(x_i)$ független $p(y_i)$-től

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

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

nincs kölcsönös információ

Átlagos kölcsönös információ:

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

(val. változók; Bayes tétel)

$$= \sum_x \sum_y p(x,y) \cdot ld \frac{1}{p(x)} - \sum_x \sum_y p(x,y) \cdot ld \frac{1}{p(x|y)} \quad [\log(ab) = \log a + \log b]$$

$\underbrace{\quad}_{H(X)}$ $\underbrace{\quad}_{H(X|Y)}$

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

Csatorna kapacitás:

ha sec (időben)

$$C = \max_{p(x)} I(X,Y) \quad bit/\text{csatorna használat} \Rightarrow bit/s$$

BitRate

össz lehetséges bemeneti eloszlás feletti max.

Shannon II. csatornakapacitás kódolás tétele:

ha: $H(X) < C$ akkor $\exists\ \Omega(X) = X'$

$P_{error} \to \emptyset$ ha $H(X') < C$

hibavalószínűség.

Mérnöki Shannon II.:

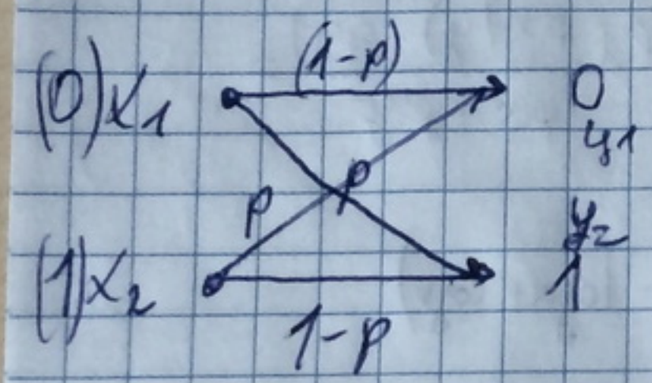
k-s bitből $X \longrightarrow \underset{n}{N} \cdot X'$; $\lim_{k\to\infty} \frac{k}{N} < C$ $P_{error} \to \emptyset$

kódbinfó bitből

n számból

DMC - discrete memoryless channel

(1) BSC



p valséggel hibázik

1-p valséggel nem hibázik

$p(x) \to x_1$ $p(y) \to y_1$

$1-p(x) \to x_2$ $1-p(y) \to y_2$

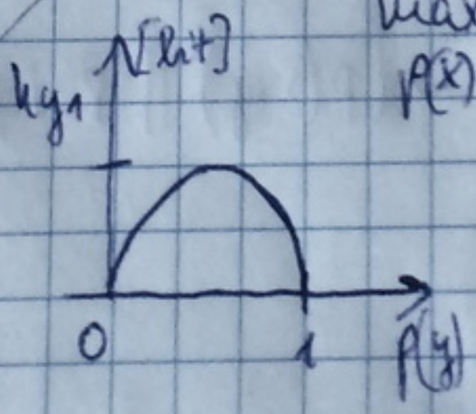
$$C_{BSC} = \max_{p(x)} \left[H(Y) - H(Y|X) \right]$$

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

egyenletes eloszlás

H_y

bin. entrópia fv.

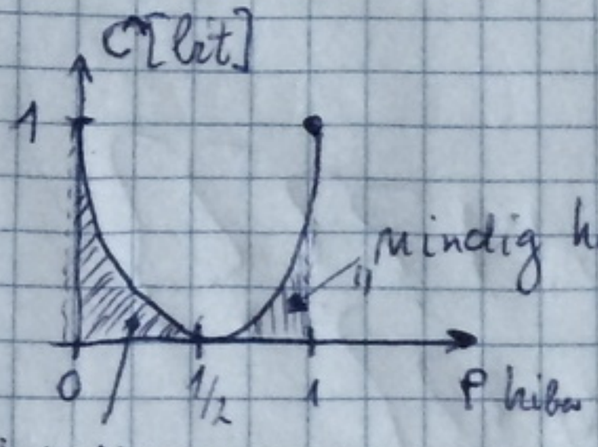


$$H(Y|X) = \sum_x \sum_y p(x,y) \cdot ld \frac{1}{p(y|x)} = \underset{x_1}{p(x)} \cdot \Big[\underbrace{(1-p)}_{y_1} \cdot ld \frac{1}{1-p} + \underbrace{p}_{y_2} ld \frac{1}{p} \Big] +$$

$$\underbrace{1-p(x)}_{x_2} \cdot \Big[\underbrace{p \cdot ld \frac{1}{p}}_{y_1} + \underbrace{(1-p) ld \frac{1}{(1-p)}}_{y_2} \Big] =$$

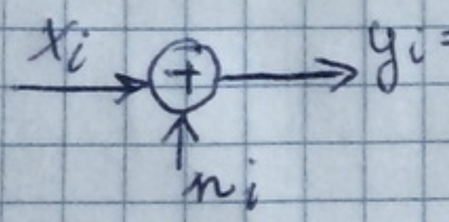
$= p \cdot ld \frac{1}{p} + (1-p) ld \frac{1}{(1-p)}$ nem függ a forrás eloszlástól! csak p hibavalószínűségtől!

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



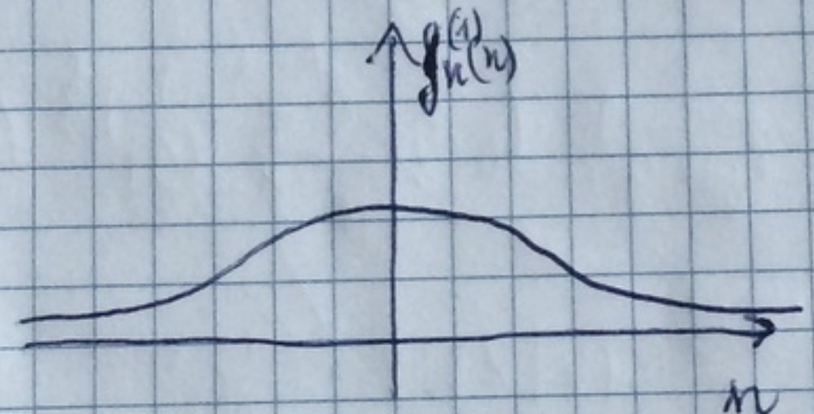
ha 1/2 akkor fogalmam sincs az információról, $C=0$

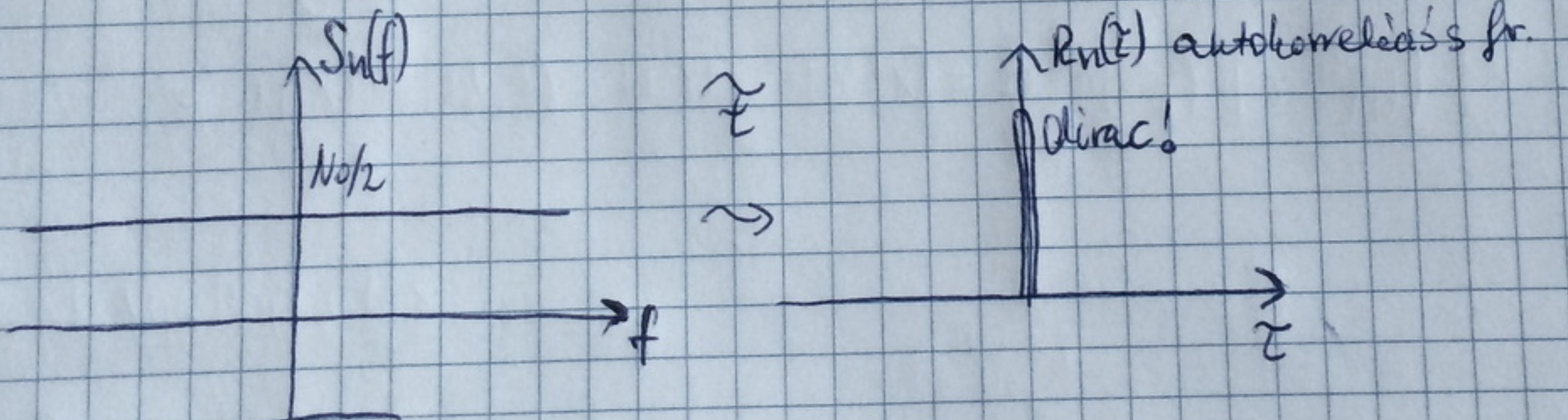
- DMC eset, D-AGWN additiv white Gaussian Noise.



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

elsőrendű sűrűségfv





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

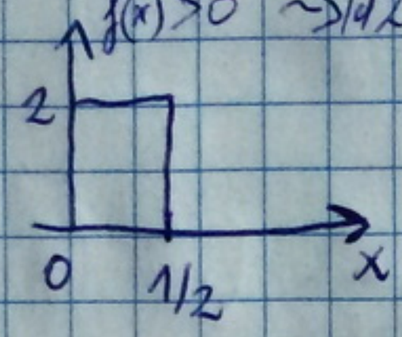
kell az új fogalom!

diszkrét -> folytonos miatt

differenciális entrópia:

$$H(X) = \int_{-\infty}^{\infty} f_x(x) \operatorname{ld} \frac{1}{f_x(x)} dx$$

lehet negatív!!!???!?



$\Rightarrow ld 2 = -1 \cdot 1 = -1 = H(X)$???

7. előadás

LOTTÓ

$$C \triangleq \max_{p(x)} I(X,Y) \quad \text{kölcsönös információ}$$

[bit/ksad. hannálat]

általában [bit/s]

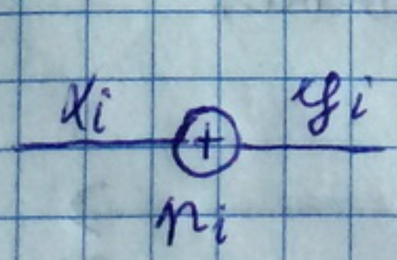
- BSC csatorna:

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

p = hibavalószínűség

DMC - discrete memoryless channel!

D-AGWN: diszkrétidő de folyt. értékű



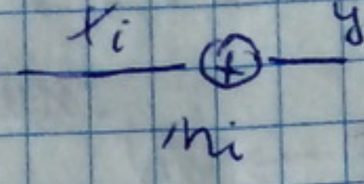
$$H(X(t)) = \int_{-\infty}^{\infty} f_x(x) \cdot \operatorname{ld} \frac{1}{f_x(x)}$$

(folytonos val. változóra az entrópia)

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

apostériori entrópia

(Gauss eset!



n_i tenikus zaj-ra : $G_n(\mu_n = 0, \sigma_n, \varrho = 0)$ Gauss folyamat

$\tau = 0 \rightarrow$ dirac

ennek az entrópiája:

teljes valószínűség $\cdot dw = 1$

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

ld helyett ln legyen

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

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

D-AGWN esetben!

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

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

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

$$= \max_{p(x)} (H(X+N) - H(N)) \quad (\text{mert} \quad y_i = x_i + n_i)$$

max akkor ha x_i is Gauss eloszlású

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

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

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

$$\frac{1}{2} \cdot \ld \left(1 + \frac{\overbrace{\sigma_x^2}^{P_{AVG}}}{\underbrace{\sigma_n^2}_{N_0/2}}\right) = \underline{\frac{1}{2} \ld \left(1 + \frac{P_{AVG}}{N_0/2}\right)}$$

AGWN-nél

$$C_{AGWN} = \frac{1}{2} \ld \left(1 + \frac{P_{avg}}{N_0/2}\right) \quad [bit/s]$$

→ folytonos időben, AGWN esetben!
más

T ideig adunk, B sávkorlátú jelet, P_{AVG} korlátos átlag telj.

$x(t) \longrightarrow \oplus \longrightarrow y(t)$ $\quad y(t) = x(t) + n(t)$

$n(t)$

$T_{mintavételi\ idő} \leq 1/(2B) \rightsquigarrow \frac{T}{T_m} = K \rightsquigarrow T_m = \frac{T}{K} = \frac{1}{2B} \rightsquigarrow \boxed{K = 2B \cdot T}$

darab minta

darab minta

$$C \triangleq \lim_{T\to\infty} \frac{1}{T} \max_{p(x)} I(x(t), y(t)) = \lim_{T\to\infty} \frac{1}{T} \max_{p(x)} \sum_{i=1}^{k} I(x_i, y_i) =$$

legalább WSS és korrelálatlan!

WSS miatt

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

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

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

$$= \lim_{T\to\infty} \frac{1}{T} K \underbrace{I(X,Y)}_{\text{ez a D-AGWN csatorna}} = \lim_{T\to\infty} \frac{KBT}{T} \cdot \left(\frac{1}{2} \cdot ld\left(1 + \frac{\sigma_x^2}{N_0/2}\right)\right)$$

$\max_{p(x)}$

T nincs

D-AGWN

σ_x^2 - diszkrét!

folyt. AGWN

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

$\sigma_n^2 = N_0/2$

$$= B \cdot ld\left(1 + \frac{P_{AV}}{2B\sigma_n^2}\right)$$

$$\sigma_x^2 = \frac{P_{AVG}}{2B}$$

$$P_{AVG} = \lim_{T\to\infty} \frac{1}{T} \int_0^T E\{x(t)^2\}\, dt =$$

$$= \lim_{T\to\infty} \frac{1}{T} \sum_{k=1}^{k} E\{x_k^2\} \underset{\text{WSS}}{=} \lim_{T\to\infty} \frac{1}{T} k \cdot E\{x^2\} =$$

$k \to 2BT$

$$= \underline{\underline{2B \cdot \sigma_x^2}}$$

(sávkorlátozva)

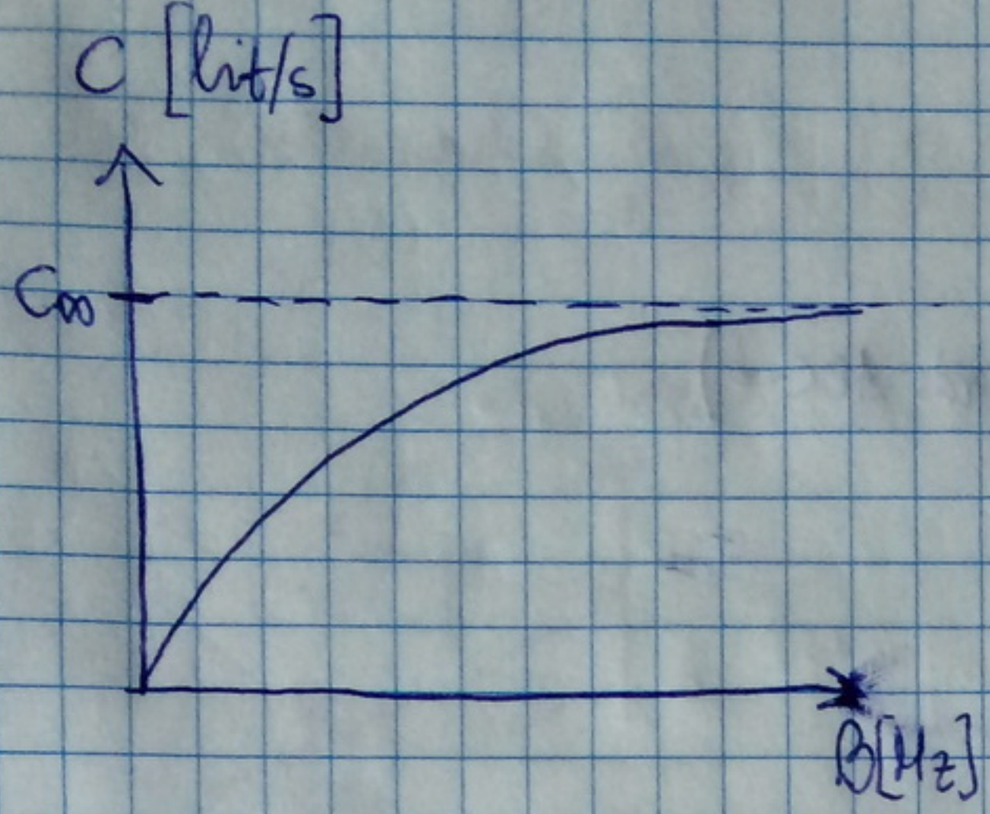
$$C = B \cdot ld\left(1 + \frac{P_{AVG}}{B \cdot N_0}\right) \left[bit/s\right]$$

$B \cdot N_0$ – zaj

AGWN
sávkorlátos B
Tideig

$$C_\infty = \frac{P_{AVG}}{N_0} \cdot ld\, e = \frac{P_{AVG}}{N_0 \cdot \ln 2}$$

ha $B \to \infty$ végtelen felé



normalizált C: $[bit/s]/[Hz] = C/B$

$P_{ava} = E_b \cdot C$ (bitenergia)

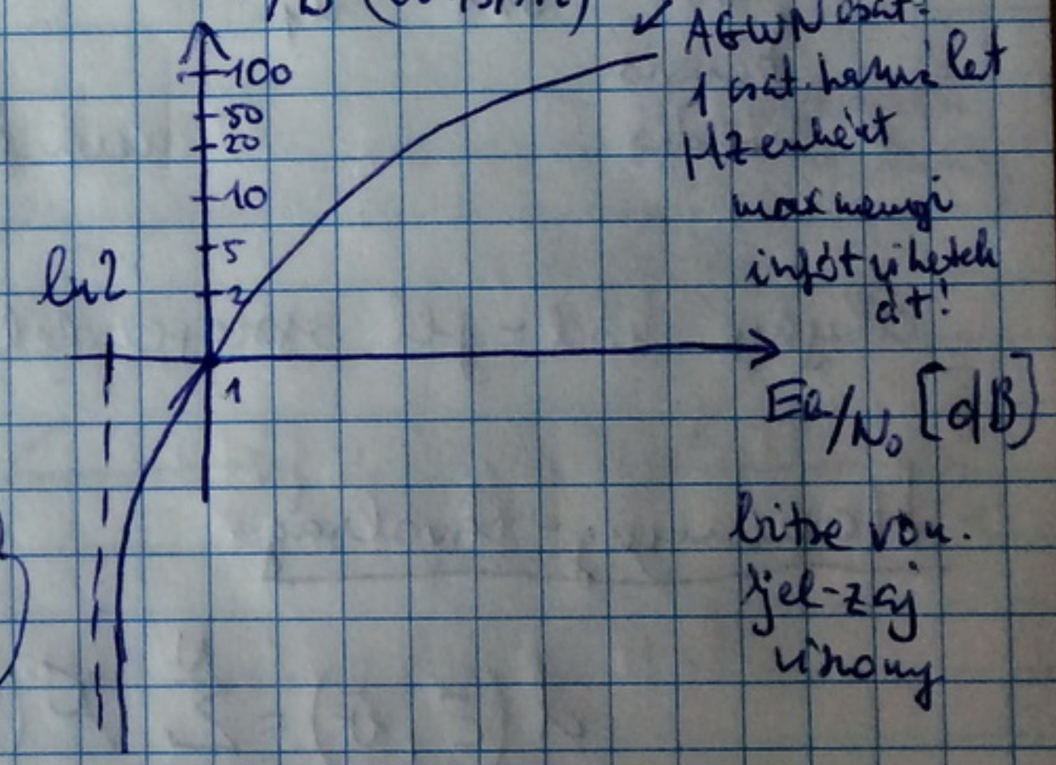
$$\frac{C_{AGWN}}{B} = ld\left(1 + \frac{E_b \cdot C}{B \cdot N_0}\right) = ld\left(1 + \frac{E_b}{N_0}\cdot\frac{C}{B}\right) =$$

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

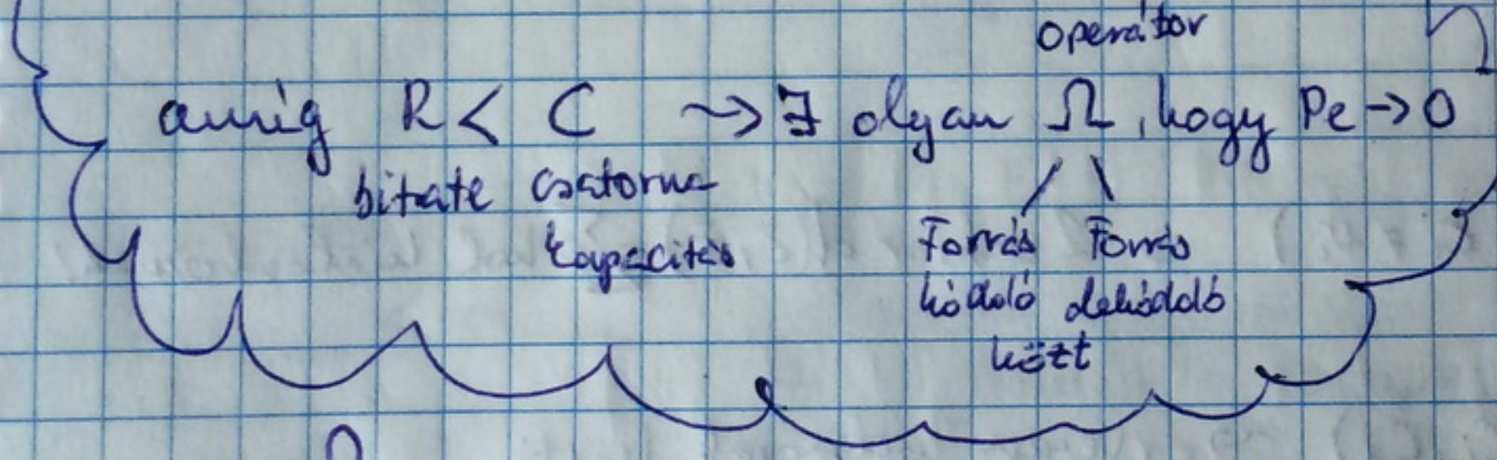
8. előadás:

$\frac{E_b}{N_0} \approx \exp$ $\qquad \frac{E_b}{N_0} \approx \exp \frac{1}{\ln 2}\left[\frac{C}{B}\cdot ld 2 - ld\frac{C}{B}\right]$ $\qquad$ ha $C/B \to \infty$

ha $C/B \to 0$ $\qquad \frac{E_b}{N_0} \Rightarrow \ln 2$ (-1,6dB)



Shannon II tétele:



amíg $R < C$ (bitate csatorna kapacitás) $\rightarrow \exists$ olyan Ω operátor, hogy $P_e \to 0$

(Forrás kódoló / Forrás dekódoló között)

ha $K \xrightarrow{\Omega} N > K$

szimbólum → újabb N-et

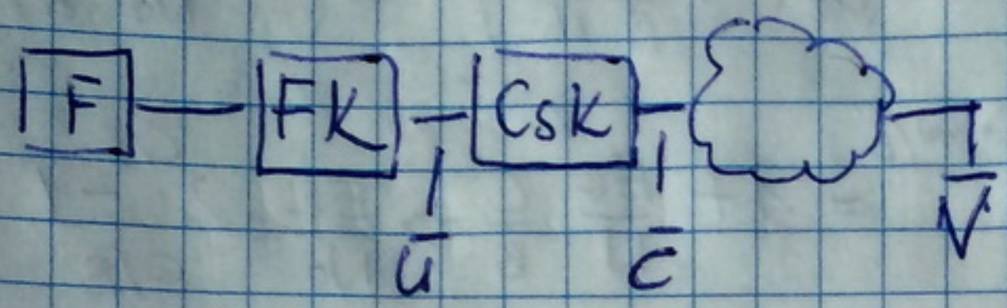
$\lim_{K\to\infty} \frac{K}{N} < C$; $P_e \to 0$ [1 s-re vonatkoztatva van]

$\frac{K}{N} < 1$ erős feltétel !!

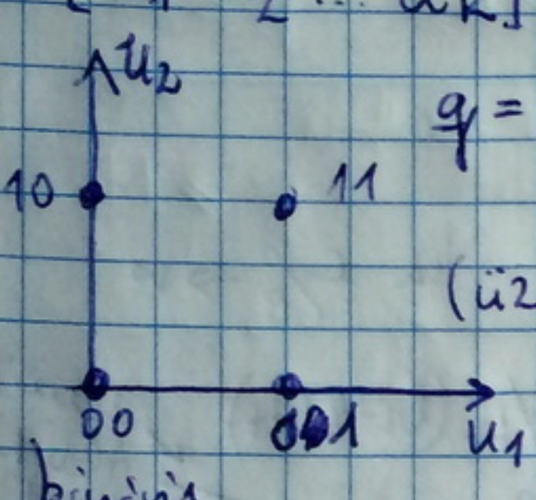
Hibajavító kódolás: (N, K, q)

(Error correction coding)

q: elték lehetséges (forrás ABC-e)

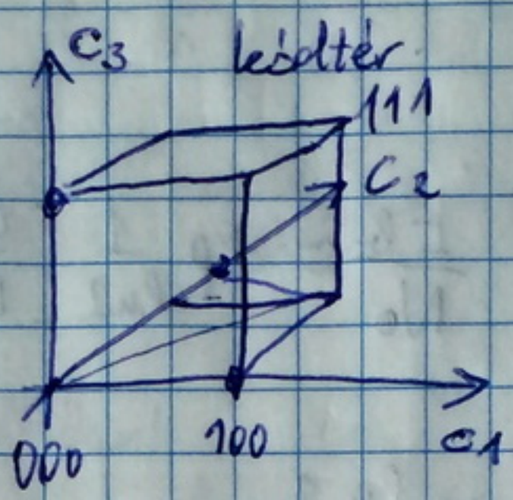


$\bar{u} = [u_1\ u_2 \dots u_K]$



$q = 2, K = 2, N = 3$ $(N > K)$

(üzenet-tér) →



nem értelmes olyan összerendelés → 00 → 000
01 → 001

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

Hamming-távolság:

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

$$d_{min} = \min_{\substack{i=j \\ i,j}} d(c_i, c_j) \rightarrow \text{érvényes kódszavak közti minimális Hamming távolság.}$$

döntő / vett jel → kód szerinti döntés

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

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

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

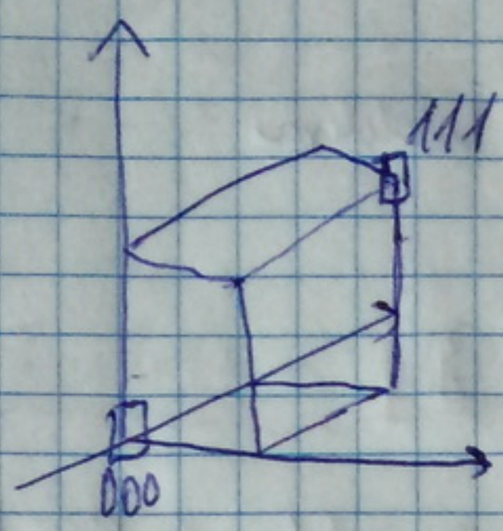
olyan kódot kapok, ami nem eleme az értékkészletnek!

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

de tudom detektálni!

(másra döntök tökéletesen)

ha növelem $\frac{K}{N}$-t 00 → 000 ismétléses kódolással
                          11 → 111



Algebrai konstrukciók: ... következő oldal!

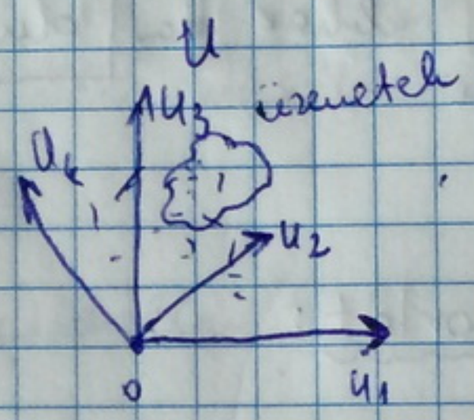
8. előadás

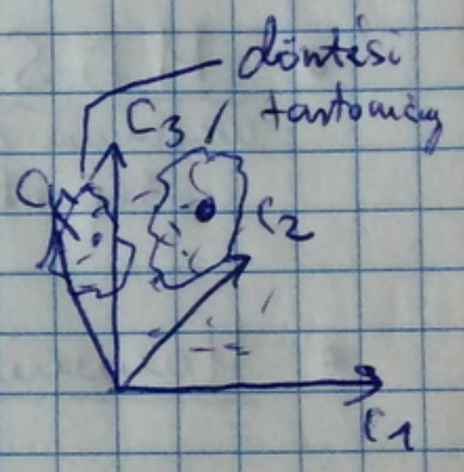
Kezelhető hibák az átvitelben!

üzenetek kódok

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

q^k q^N





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

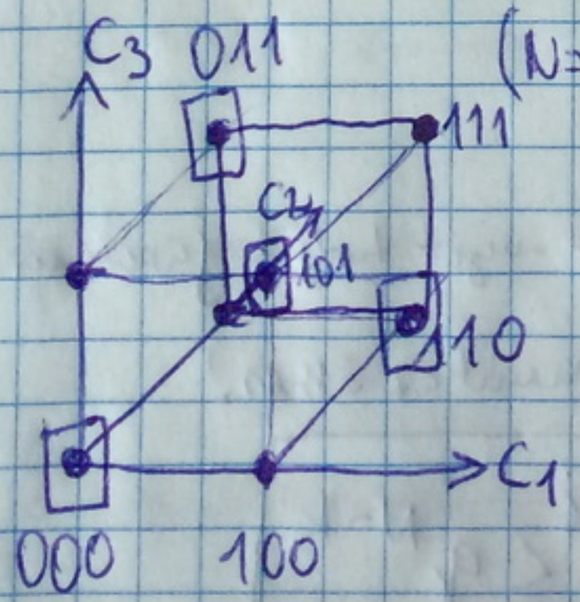
$t_{\text{javítható hibák száma}} = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$

$t_{törléses} = d_{min} - 1$

↓

demodulátor nem akar dönteni mert nem biztos benne

inkább újra hiszi majd mert tudom, hogy hol volt a hiba!



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

1) 000 hozzá közelebbet nem választom

2) 011, 101, 110, és kész!

ha 110 elromlik *10 (törléses hiba)

de tudom h. csak 110 lehet

[$d_{min} - 1$ távolságra levőt tudok javítani]

$t_{törléses}$!

Kódkonstrukciós törvények:

- **Singleton korlát** (N, K, q) paraméterű kódokra
  (üzenetek, kódtér, állapot)

  adott d_{min}

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

  $M \leq q^K$ ~~$M \leq q^K$~~ $d_{min} \leq 1 + N - K$ ha = akkor a legjobb!
  (ekkor vannak legtávolabb)

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

  hány érvényes kódvektor lehet ?

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

- **Hamming korlát:**

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

  $1 + N(q-1)$ [1 pontból, 1 Hamming távolságra]

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

  t_{jav} ezekben $+ \ldots - + \binom{N}{t_{jav}} \cdot \underbrace{(q-1)^{t_{jav}}}_{\substack{1 \text{ érvényes kód} \\ q-1 \text{ rossz kód}}}$ $\Longrightarrow$ $t_{jav} : \sum_{i=0}^{t_{jav}} \binom{N}{i}(q-i)^i$

  $q^k \cdot \sum_{i=0}^{t_{jav}} \binom{N}{i} \cdot (q-1)^i$ annyi kell, hogy t_{jav}-ujat tudjak javítani!
  - és ez biztos kisebb mint az összes!
  üzenetek száma összes

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

$q=2$ esetén:

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

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

(a tér minden pontját felhasználjuk!)

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

000 és 111 $\rightsquigarrow$ 1 hibát tudok javítani!

1 döntési távolságra $\rightarrow$ minden kódok használok $\Rightarrow$ PERFEKT és MDS

(Hamming)

ez jó, de hogyan lehetne algoritmizálni?

Algebrai kódkonstrukció:

- lineáris tér: műveletekre zárt
- kódok altért alkotnak (lineáris altért)
- lin. független
- bázis: üzenetvektorokkal súlyozott összege a bázisoknak $\rightarrow$ előáll. az összes kódból! $\{\underline{c}\}$
- generátor

$$[\underline{u}] \begin{bmatrix} 0\,1\,1 \\ 1\,0\,1 \end{bmatrix} \updownarrow K \quad \longleftrightarrow N \quad = G$$

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

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

ha a generátormátrix valahol tartalmazza az egységmátrixot $\underline{\underline{I}}$, akkor szisztematikus a kód!

$$G_{\text{szisztematikus}} = \left[\underline{\underline{I}} \mid \underline{\underline{P}}\right] \updownarrow K \quad \longleftrightarrow N$$

sorcsere! $\underline{\underline{I}}\ \underline{\underline{P}}$

$\underline{\underline{G}} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ $G_{rendszer} = \left[\begin{array}{cc|c} 1 & 0 & 1 \\ 0 & 1 & 1 \end{array}\right]$

$\underline{\underline{H}}$ paritás ellenőrző mátrix

legyen $\underline{\underline{H}}$ olyan, hogy $\bar{H} = [-\underline{\underline{P}}^T\ \underline{\underline{I}}]$

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

példa $\underline{\underline{H}} = [11|1]$

$$\underbrace{\bar{u} \cdot \underline{\underline{G}}}_{\bar{c}}\ \underline{\underline{H}}^T = \bar{u} \cdot \underline{\underline{\emptyset}} = \underline{\underline{\emptyset}}$$

$\underline{c}\ \underline{\underline{H}}^T = \emptyset = \underline{\underline{H}} \cdot \underline{c}^T$ ha nem $\emptyset \Rightarrow$ szindróma

$v = c + e$

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

10. előadás

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

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

szisztematikus kód esetén: $\underline{\underline{G}} = \left[\underbrace{\underline{\underline{I}}}_{K \times K} \mid \underline{\underline{P}} \right] \updownarrow K$ ($\leftrightarrow N$)

$\bar{V} = \bar{C} + \bar{e}$ (vett vektor, kód, hiba)

$\bar{V}$ érvényes-e? igen $\rightarrow \hat{\bar{C}}$

$\underline{\underline{H}} = \left[-\underline{\underline{P}}^T \; \underline{\underline{I}} \right] \updownarrow N-K$ ($\leftrightarrow N$) $\rightarrow \underline{\underline{H}}^T = \left[\begin{matrix} -\underline{\underline{P}}^T \\ \underline{\underline{I}} \end{matrix} \right] \updownarrow N$ ($\leftrightarrow N-K$)

$\underline{\underline{G}}\,\underline{\underline{H}}^T = \left[\underline{\underline{I}} \; \underline{\underline{P}} \right] \left[\begin{matrix} -\underline{\underline{P}}^T \\ \underline{\underline{I}} \end{matrix} \right] = \emptyset$

$\underline{\underline{H}} \cdot \underline{V}^T = \underline{\underline{H}} \cdot \underline{C}^T + \underline{\underline{H}}\,\underline{e}^T = \underline{S}^T$ $\rightsquigarrow \underline{S}^T = \underline{\underline{H}}\,\underline{e}^T$ szindróma

$\underline{\underline{H}} \cdot \underline{C}^T = \emptyset$ ($\underline{C}\,\underline{\underline{H}}^T = \emptyset$)

$\underline{e} = [000\ldots100]$ (1 hiba van!) ($\leftrightarrow N$)

↘ ezt szorzom $\underline{\underline{H}}$-val

(több hiba is lehet, akkor az egyes oszlopok lin. kombinációja)

$t_{jav} = 1$; $q = 2$

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

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

$m = 2$ ✓

$m = 3$

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

jobb kódolásnál a cél (kevesebb redundancia)

$N-K$ párok ahol $t_{jav}=1$

ezek PERFEKTEK! k lehetne kisebb is de akkor nem perfekt!

kódarány

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

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

kódszóban ahol nem 0

lin. esetben: a kódban súly(1) van.

lineáris kódokra

$d_{min} = \min_{\forall i} w(c_i)$

kódban $\underline{c} = \underline{\emptyset}$

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

$$1 + N + \frac{N(N-1)}{2} \le 2^{N-K}$$

↑ ide kell helyettesíteni és kijön N és K

N	K	R_c	
5	1	1/5	
90	78	78/90	→ kijön, de ilyen nincs!

<u>bináris Hamming kód:</u>

példa (7, 4, 2) ~> $t_{jav} = 2$, és perfekt a Hamming korlát miatt.

ne legyen $\underline{H}$-ban két azonos oszlop!

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

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

(the right-hand I block: $N-K$ × $N-K$; rows 2^1, 2^2, 2^3)

ide azokat rakom amik még nem voltak I-ben mindegy milyen sorrendben.

$$\underline{\underline{G}} = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{bmatrix}$$

$K \times N$

$\underline{u} = [1\,1\,0\,1] \rightarrow \underline{c} = [1\,1\,0\,1\,1\,0\,0]$ (↑ hiba)

$\underline{v} = \underline{c} + \underline{e} \rightarrow \underline{s}^T = [1\,0\,1]$ ~> $\underline{\underline{H}}$-nak 4. oszlopa → 4. bit romlott el! c-ben!

ha nem bináris a kód. $q = 3$

$$1 + N(q-1) = q^{N-K} \quad (t_{jav} = 1)$$

↑ perfekt eset

$d_{min} \ge 3$ miatt

$t_{jav} = 1$

N	K	R_c	
4	2	1/2	$q=3$
6	4	66%	$q=5$

$GF(q = p^n)$

Galois-test prímrendű

ha $N = K + 2$ MDS is!

$t_{jav}=1 \qquad 1+N(q-1)=q^{N-k}$

$q=3 \rightsquigarrow \quad N \quad K$ $\rightsquigarrow$ nem MDS, mert $13-10 \neq 2$

$13 \quad 10$

$q=5 \rightsquigarrow \quad 31 \quad 28 \rightsquigarrow$ nem MDS!

Nemlineáris Hamming kódok (MDS és perfekt) $t_{jav}=1$

$$\underline{\underline{H}}=\left[\begin{array}{cc|cc} 1 & 1 & 1 & 0 \\ \alpha^1 & \alpha^2 & 0 & 1 \end{array}\right]$$

2 db $\quad$ 1 db $\quad (4 \bmod 3 = 1)$

$(4,2,3)$ kód

$N \; K \; q$

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

$-\infty \quad 0 \quad 1$

$\alpha \quad \alpha^0 \quad \alpha^1$

$\alpha^b=2$ primitív elem $\qquad \alpha^{q-1}=1$

$\underline{e}=[0\,0\,\ldots\,\underset{\text{hiba}}{e}\,0\,0]$

hiba lokátor!

súlyozom e-vel a hibaértékkel

11. előadás

Hamming kód: $t_{jav}=1$ perfekt és MDS

minden hibamintához $\quad d_{min}=$ maximális

$N-K=2 \Rightarrow d_{min}=3$ és $t_{jav}=\left\lfloor \frac{d_{min}-1}{2} \right\rfloor = 1$

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

prím

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

legkisebb

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

α primitív elem

α hatványozásával végigmehetünk a testen!

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 = ?

$\alpha = 2 \quad 2^1 = 2 \quad 2^2 = 4 \quad 2^3 = 1 \bmod 7$ ↯ MOD 7

$\boxed{\alpha = 3} \quad 3^1 = \underline{3} \quad 3^2 = \underline{2} \quad 3^3 = \underline{6} \quad 3^4 = \underline{4} \quad 3^5 = 5 \quad 3^6 = 1$

$\boxed{\alpha = 5}$ is igaz!

több α is lehet!

nem bináris Hamming kód:

MDS legyen $\rightarrow N - K = 2$

$N = 6 \quad K = 4 \quad q = 5 \quad GF(5) \quad \boxed{\alpha = 2}$ érvényes

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

$\leftrightarrow N-K$

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

$h_i \rightarrow$ hibahely, $e_i =$ hiba érték
$e_i = q - 1$ féle $= \boxed{4}$

$\left[\begin{array}{c} \underline{s}^T \\ e_i \end{array}\right] = h_i^T$ egyik oszlopa

normálom

minden oszlop vesszőreluva $\underline{\underline{1}}$ kell legyen

hogy biztosan az értéket

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

Ksor Noszlop

$\underline{u} = [3\ 0\ 2\ 4]$

$\underline{c} = [3\ 0\ 2\ 4\ 1\ 4]$

$\underline{v} = [3\ 0\ 2\ 4\ 4\ 4]$

$\underline{e} = [0\ 0\ 0\ 0\ 3\ 0]$

$\underline{s} = ?$

$$\underline{v}^T = \begin{bmatrix} 3 \\ 0 \\ 2 \\ 4 \\ 4 \\ 4 \end{bmatrix} \cdot \underline{\underline{H}} = \underline{s}^T = \begin{bmatrix} 3 \\ 0 \end{bmatrix} \rightsquigarrow \text{normáljuk} \begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightsquigarrow \underline{\underline{H}}\text{-ban az 5 dik oszlop értéke}$$

30241(1)4

(3)

R-S kódoló: Reed-Solomon kódoló

több hibát is tud javítani

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

$$\deg(u(x)) = k-1 \qquad k = K \quad n = N$$

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

⊕ polinomiális GF(q) felett

$$a(x) + b(x) = c(x) \qquad c_i = a_i \cdot b_i \mod q$$

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

⊛ szorzás GF(q) felett

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

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

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

⊘ osztás GF(q) felett — kvóciens, reziduum

$a(x)$ és $b(x) \neq \emptyset \rightsquigarrow q(x), r(x)$

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

√ $c \in GF(q)$; $a(x)$ gyöke c

$$a(c) = 0$$

R-S leírása:

① $c_0 = u(\alpha^0)$

$c_1 = u(\alpha^1)$

$c_{N-1} = u(\alpha^{N-1})$

② $\underline{c} = \underline{u} \cdot \underline{G}$ — szabadon

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

$\Rightarrow \boxed{N-1 \leq q-2}$ (mert $q-1$ mert $\begin{bmatrix} 1 \\ 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix}$ 2 sorban mert $\alpha^{q-1} = 1$)

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

$C_0 = \{\bar{c},\ H\underline{c}^T = \emptyset\}$

$$H = \begin{bmatrix} 1 & \alpha & \cdots & \alpha^{(N-1)} \\ 1 & \alpha^2 & & \\ \vdots & & & \\ 1 & \alpha^{N-K} & \cdots & \alpha^{(N-K)(N-1)} \end{bmatrix} \quad \updownarrow N-K \qquad \leftrightarrow N$$

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

$\uparrow$

BCH

MDS akkor a köd!

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

+ Singleton $d_{min} \leq N-K+1$

$\Downarrow$

emiatt! $\boxed{d_{min} = w(\underline{c})}$

12. előadás

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

$$\underline{\underline{G}} = \begin{bmatrix} 1 & 1 & 1 & & 1 \\ 1 & \alpha & \alpha^2 & & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & & \\ \vdots & & & & \\ 1 & \alpha^{k-1} & \alpha^{2k-2} & & \alpha^{(k-1)(N-1)} \end{bmatrix} \quad \updownarrow k \qquad \leftrightarrow N$$

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

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

$2t_{jav} = \underbrace{N-K}_{\text{paritás szimbolumok száma}}$

$$\underline{\underline{H}} = \begin{bmatrix} 1 & \alpha^1 & & & \alpha^{N-1} \\ 1 & & & & \\ \vdots & & & & \\ 1 & \alpha^{N-K} & & & \alpha^{(N-1)(N-K)} \end{bmatrix} \quad \updownarrow N-K \qquad \leftrightarrow N$$

$N-1 \overset{(k)}{=} q-2 \qquad \alpha^{q-1} = \text{egységelem}$

$RS(\underbrace{N=q-1}_{\text{legjobb esetben}},\ K=N-2t_{jav},\ q)$

Peterson - Goresstein - Zierler algoritmus:

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

hiba pozíció: i, j

hiba érték: e_i és e_j

hiba lokátorok: $h_i \dots h_j$ a paritás ell. mátrix i, j oszlopának első eleme.

$\bar{e} = [0 \dots \overset{i}{e_i} \dots \overset{j}{e_j} \dots 0]$ ← hibavektor $\quad h_i = \alpha^i \quad h_j = \alpha^j$ $\rightsquigarrow$ lokalizálják a hibát.

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

$\bar{S}^T = \underline{\underline{H}} \cdot \bar{e}^T \Rightarrow \begin{bmatrix} s_1 \\ s_2 \\ s_3 \\ s_4 \end{bmatrix} = \dots \rightsquigarrow \boxed{\bar{S}^T = e_i \bar{h}_i^T + e_j \cdot \bar{h}_j^T} \rightsquigarrow$

$s_1 = h_i \cdot e_i + h_j \cdot e_j$
$s_2 = h_i^2 \cdot e_i + h_j^2 \cdot e_j$
$s_3 = h_i^3 \cdot e_i + h_j^3 \cdot e_j$
$s_4 = h_i^4 \cdot e_i + h_j^4 \cdot e_j$

nem lin. egyenletrsz.

lokátorpolinom: gyöke h_i és h_j

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

$L_1 = -(h_i + h_j)$
$L_0 = h_i \cdot h_j$

$\Rightarrow \cancel{x^2 + L_1(x) + L_0}$ $\boxed{x^2 + L_1 \cdot x + L_0}$

$h_i \cdot e_i \cdot \underbrace{L(h_i)}_{\text{ø lesz mert gyök van.}} = e_i \cdot h_i^3 + L_1 \cdot h_i^2 \cdot e_i + L_0 \cdot h_i \cdot e_i = \emptyset$

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

$\Big] \oplus$

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

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

$$\underbrace{\quad\quad}_{S_3} \qquad \overset{S_2}{\Downarrow} \qquad \overset{S_1}{\Downarrow}$$

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

$$\underbrace{e_i h_i^4 + e_j h_j^4}_{S_4} + L_1\underbrace{(e_i h_i^3 + h_j^3 e_j)}_{S_3} + L_0\underbrace{(h_i^2 e_i + h_j^2 e_j)}_{S_2} = 0$$

$$S_3 + L_1 \cdot S_2 + L_0 \cdot S_1 = 0$$

$$S_4 + L_1 \cdot S_3 + L_0 \cdot S_2 = 0$$

Här löses denna ekvationssystem!

RS(6, 2, 7)

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

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

$$u = [3 \quad 5]$$

$$\bar{c} = [1 \quad 4 \quad 6 \quad 5 \quad 2 \quad 0] \qquad \bar{e} = [0 \; 2 \; 0 \; 0 \; 3 \; 0]$$

$$v = [1 \quad 6 \quad 6 \quad 5 \quad 5 \quad 0]$$

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

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

e_i e_j

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

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

$\rightsquigarrow 4 + 2 L_0 = 0$

$L_0 = 3/2$

$\boxed{L_0 = 5}$ $\quad 2 L_0 = 3 \mod 7$, $L_0 = 10 \rightsquigarrow$ ✓

$6 + L_1 + 15 L_0 = 0 \rightsquigarrow \boxed{L_1 = \emptyset}$

$L_1 = -(h_i + h_j)$

$L_0 = h_j \cdot h_i$

$\boxed{h_i = 3}$ $\boxed{h_j = 4}$ másodfokú egyenletből

$\emptyset = -(h_i + h_j)$

$5 = h_i \cdot h_j$

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

$4 = 3 e_i + 4 e_j$

$3 = 2 e_i + 2 e_j$ $\Big] \rightarrow 5 = 6 e_i \Rightarrow \boxed{e_i = 2}$

Végül $\underline{\underline{H}}$-ban megnézem $\rightarrow \underline{v} = [166550]$

$e = [020030]$

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

Javítottunk 2 hibát!