~~Mobil és vezeték nélküli hálózatok~~

Hírközlés elmélet

dr. Bitó János

Szerda 8^{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 rész ⇒ teszt példa tétel

10 tesztes feleletkifejtős (infokomm)

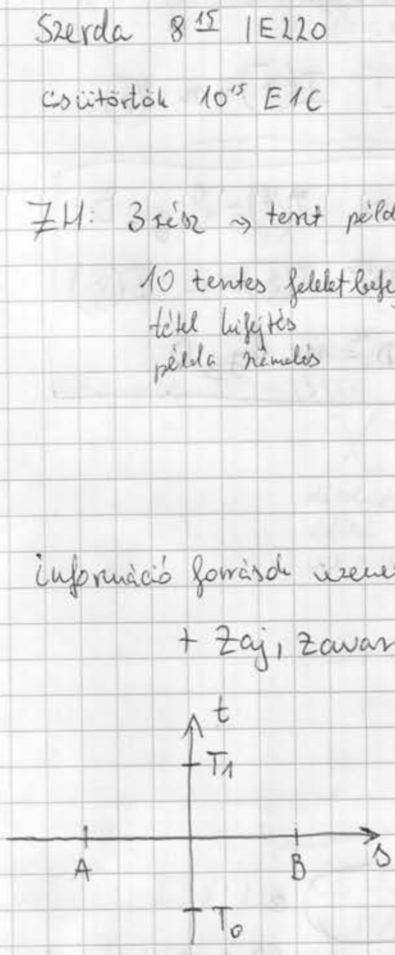
tétel kifejtés

példa számolás

1. előadás

információ forrásoknak üzeneteinek eljuttatása az információ nyelőjéhez = HÍRKÖZLÉS

+ zaj, zavar, interferencia (mesterséges vagy természetes)



időben vagy térben elkülönült pontok

forrás kódolás / tömörítés [időben elkülönültkor]

• mi az információ? felkel-e a nap holnap?

P(nap) → 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

eddig ↓

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

~~nem~~ ↓ elhelyett!

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!

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

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

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

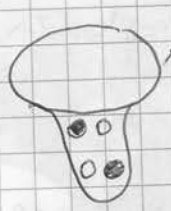
ha $a = 2 \rightsquigarrow \log_2$ ⇓ ld [bit]

ha $a = 10 \rightsquigarrow \log_{10}$ ⇓ lg [Hartly]

DE2 MÉG NEM JÓ:

példa:

lealap
4 gdyó
1-et húznunk



$D = 2$

ld $D = 1$ [bit]

binary digit

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

B

fehér: ld $\frac{4}{1} = 2$ [bit]

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

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

[bit] az információmennyiség mértéke

BIT

B

● = 2
O = 0,415

$$\underbrace{\frac{1}{4}}_{\text{valség}} \cdot \underbrace{2}_{\text{info tartalom}} + \underbrace{\frac{3}{4}}_{\text{valség}} \cdot \underbrace{0{,}415}_{\text{info tartalom}} = \underline{0{,}811\,[bit]}$$

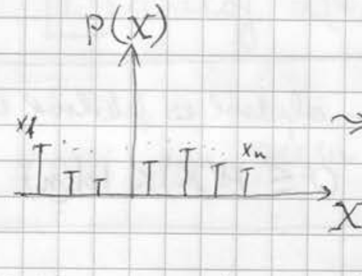
↳ kevesebb infó mint egyenletes eloszlásnál

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

legyen:

$$\underbrace{X}_{\text{diszkrét értékű val. változó}} = \{x_1 \ldots x_n\}; \quad \underbrace{p(X)}_{\text{sűrűség fv.}} = (p_1 \ldots p_n)$$

$p_i = p(x_i)$ i-dik esemény



$$\rightsquigarrow F_X(y) = \sum_{y=-\infty}^{\infty} p_X(y) = \underline{1}$$

↓ eloszlásfüggvény; ↳ teljes eseménytér!

<u>Def</u>: $I(x_i) = ld\,\frac{1}{p(x_i)}$ ⇝ ez egy esemény információja

minél valószínűbb az esemény annál kisebb az info. tartalom

$\to -ld\,(p(x_i))$ [bit]

(Self Information – az esemény saját információ tartalma)

<u>Def</u>: Entrópia, Átlagos információtartalom (entropy)

$$H(X) = E\{I(x_i)\} = \sum_{x_i \in X} p(x_i) \cdot \overbrace{ld\,\frac{1}{p(x_i)}}^{I(x_i)}$$

( ) ⇒ Marci és a lájkok

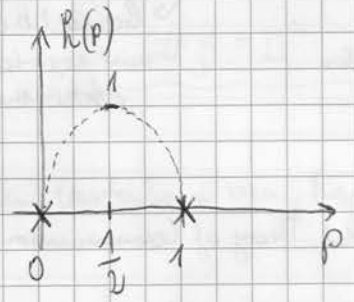
- legyen $X = \{x_1, x_2\}$, $p(X) = \{p(x_1), p(x_2)\} \Rightarrow \{\overset{p}{p(x_1)}; \overset{1-p}{1-p(x_1)}\}$

ezért ez 1 paraméteres

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

$h(p)$ = bináris entrópia fv

határérték probléma a széleken!



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

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

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

$\Rightarrow 0$

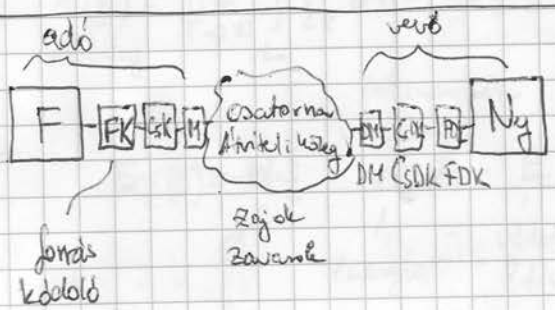
irodalom keresés!!! szóló Bitóiak

<u>Tétel:</u> az entrópia alulról és felülről is korlátos

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

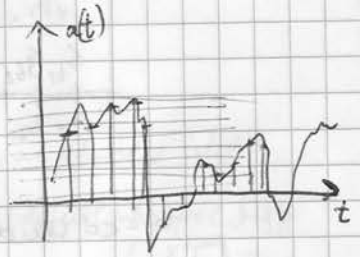
2. előadás

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 törli [veszteséges és veszteségmentes]
CsK: a fellépő zavarok csillapítása (hibajavító + redundancia hozzáadó)
M: modulátor
DM: demodulátor
CsDK: csatorna dekóder
FDK: forrás dekódoló

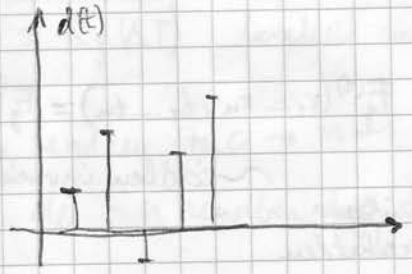
F analóg a(t)



zéger Bell idejében

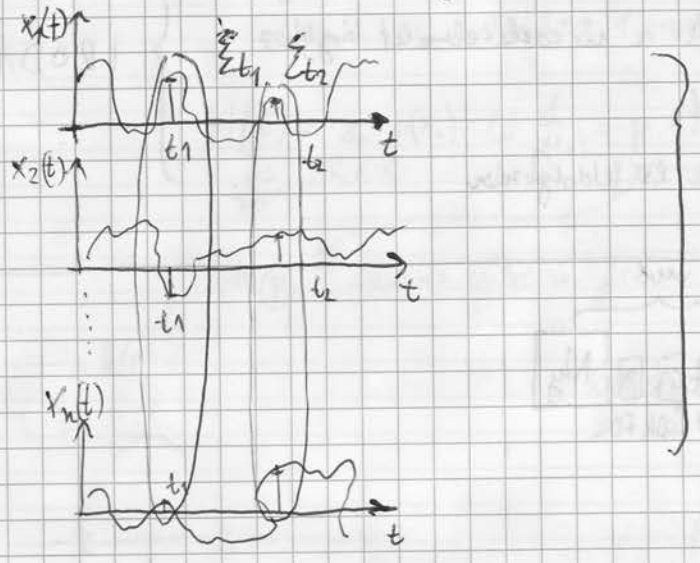
Ha sávkorlátozott ($\frac{1}{2T}$) mv.-tétel!

Ua digitális jel:
- időben mintavételezem (T)
- értékben kvantálom



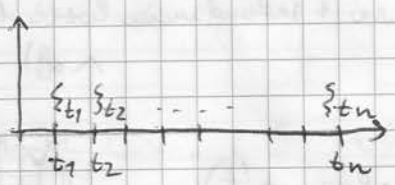
Sztochasztikus folyamatok

① a folyamat realizációjának az együttese



együtt ők a sztochasztikus folyamat!

② Valószínűségi változók rendezett (időben) serege



n-ed rendű eloszlás fv (n dimenziós)

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

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. folyam. várható értéke időfüggetlen

erősen stac. folyam → ergodikus folyam vagy ergodikus folyam keveréke

- ergodikus folyamat

bármelyik realizációból meghatározható

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

- legyen

$$\cancel{E_\xi(t) = m_\xi} \qquad \overbrace{e_\xi(t)}^{\text{jel energiája}} = \underset{\text{várható érték}}{E}\{\xi_t^2\} = \int_{-\infty}^{\infty} x^2 \cdot f_\xi(x,t)\, dx$$

(cancelled: $E_\xi(t) = m_\xi$ — átlag; $e_\xi(t)$ — energia)

- Autokorreláció

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

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

⇓ csak az időkülönbségtől függ (ΔT)

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

- Gyengén stacionárius (Wide-Sense-Stationary)

(másodrendben stacionárius → gyengén stacionárius)

① $\Rightarrow m_\xi(t) = m_\xi$ $\forall t$ idő feltől

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

- ha n rendben stac → $n-1$

de - n rendben stac $\not\Rightarrow n+1$

- Memória nélküli: X

- forrás

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

diszkrét
stacionárius eloszlás

folytonos is(f)

példa:

$$\#X = 26$$

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

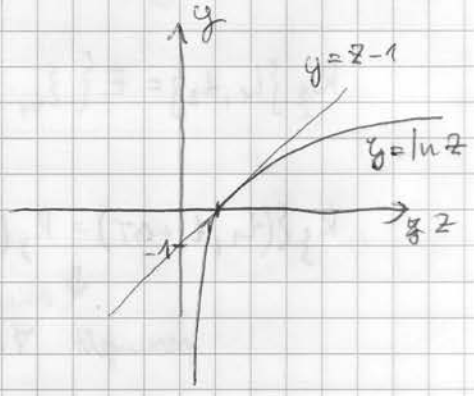
entrópia

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

(Tétel: $0 \le H(X) \le \operatorname{ld}(n)$

$$H(X) - \operatorname{ld}(n) \le 0$$

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



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

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

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

$$\sum p_{x_i} \cdot \operatorname{ld} \underbrace{\left(\frac{1}{n p_{x_i}}\right)}_{z} \le 0$$

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

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

$$1 - 1 = 0$$

Német ugrive

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

párok $H_2(X) = 3\ bit$

$$H_{10}(X) = 1{,}6\ bit$$

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

redundancia

entrópia a feltehető kérdések átlagos száma

értelmes annyi biten kódolni, amelyikre gyakran fordul elő.

3. előadás

- eddig amiket tanultunk

röviden

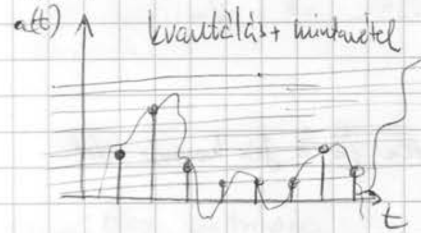
$$F_\xi^{(n)}(\xi_{t_1} < x_1 \dots \xi_{t_n} < x_n, t_1 \dots t_n) = F_\xi^{(n)}(\bar{x}, \bar{T}) \quad \forall \Delta T \; \forall \{\bar{T}\}$$

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

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

erősen stac, ha $\forall$ n-re !

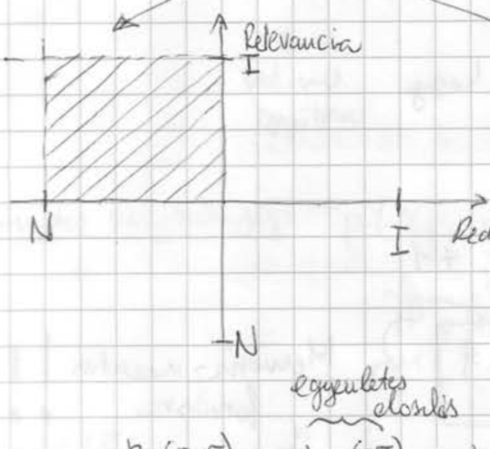
gyengén, ha nem $\forall$ n-re ~



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

ha változik időben a várható érték → nem stacionárius

VALÓS VILÁG FOLYAMATAI



releváns információ átvitel kevés redundanciával

egyenletes eloszlás

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

redundancia

cél ennek a minimalizálása

Német szöveg:

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

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

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

Forrás kódolás

- diszkret, 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: $X = \{a, b, c, d\}$ $\quad C = \{\underset{a}{00}, \underset{b}{01}, \underset{c}{10}, \underset{d}{11}\}$

$p(X) = \{\frac{1}{4}; \frac{1}{4}; \frac{1}{4}; \frac{1}{4}\}$ 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

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

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

$$\boxed{H(X) \leqslant L_X < H(X) + 1}$$

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 $[l_i+]$

kószavai kód hossz

D+M forrás:

⇝ A memória:

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

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:

$$H(\bar{X}_1^n) = H(X_1 \dots X_n) = \sum_{\bar{X}^n} p(x_1, \dots x_n) \cdot ld \frac{1}{p(x_1 \dots x_n)}$$

n darab val. vált. együttese

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

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

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

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

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

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

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

1 szimbólumra eső entrópia

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

- Sztochastikus folyamat entrópiája

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

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 eseményel

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

ha WSS a forrás (időftlen ⇒ indexftlen)

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

$\Downarrow$

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

Forrás-kódolás:

átl. kódhossz

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

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

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

„élése"

[abcd példára]

~ kedden ZH

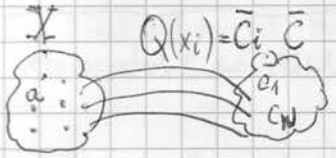
E1B 18 15

terjt, példa, tétel

---

4. előadás

Forrás kódolás



forrás ABC diszkrét ↑ kód ABC diszkrét

kölcsönösen egyértelmű kapcsolat

DMS + memória nás

pillanat kódolónak kell lenni ⇝ azonnal el kell tudjam dönteni a forrás ABC elemeit!

$l_i : \bar{C}_i = (c_{i1}, \dots, c_{il_i})$

l_i: egy kód hossza

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

legyen $L_x = \sum_{x_i \in X} p(x_i)\cdot l_i$

[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 ?

$\Downarrow$

$H(X) = \sum_{x_i} p(x_i) \cdot ld \frac{1}{p(x_i)}$ → 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 kódhosszú

Példa:

		fix hosszú
X	p(x_i)	(A)
x_1	1/2	0 0
x_2	1/4	0 1
x_3	1/8	1 0
x_4	1/8	1 1

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

ez pillanatkód!!!

(A) eset $L(X) = 2$ fix hosszú kód miatt!

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

→ fix hosszú kódot mindig lehet dekódolni!

0 1 | 0 0 | 1 1 | 0 1 | 1 0 | 0 0 | 1

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

(B) eset

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

kisebb az en bópicuk ????

nem dekódolható!

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

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

$\bar{c}_i = (c_{i1} \dots c_{il_i})$ akkor ~~$\forall$~~ olyan $\bar{c}_j$: $\overset{akkor}{\forall}$ $l_j > l_i$, $c_j = (c_{i1} \dots c_{il_i}, c_{i+1} \dots c_{ej})$

azaz eleje olyan mint a másik kód

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

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

ez prefix mentes kód ⇝ dekódolható

(Shannon - Fano kód)

pillanatkód

(D) szeparátort kezdtünk be: pl egy vesszőt!

[comma - code]

$x_1 \rightsquigarrow 0$ elválasztó

$x_2 \rightsquigarrow 01$

$x_3 \rightsquigarrow 011$

$x_4 \rightsquigarrow 0111$

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

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

(E) {prefix és comma-code}

$x_1 \rightsquigarrow 0$

$x_2 \rightsquigarrow 10$ ↖ separator

$x_3 \rightsquigarrow 110$ /

$x_3 \rightsquigarrow 1110$

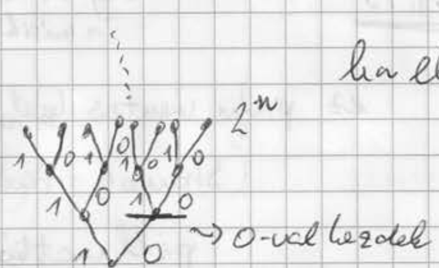
$L_x = 1{,}875$

Prefix-kód generálása:

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

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

bin. fa:



ha elkezdem 0-val → fel lefűrészelem az ágat

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

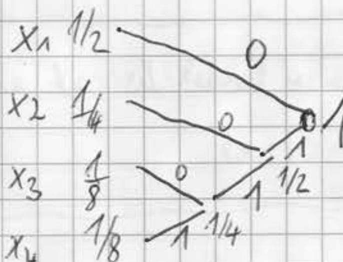
$$\sum_{i=1}^{N} 2^{N-l_i} \leq 2^N \rightsquigarrow \boxed{\sum_{i=1}^{N} 2^{-l_i} \leq 1} \checkmark$$

teljes fa! Kraft.

(a teljes fánál többet nem vághatok ki)

Huffmann:

① ⇝ előfordulási valség szerint sorba rendezd!
② ⇝ bináris fa, 2 legkisebb valségű eseményt kódd össze!
→ rekurzívan!
amíg nem érek 1-hez!



bináris fa

$X_1 \rightsquigarrow 0$ ✓ levágom

$X_2 \rightsquigarrow 10$ ✓ prefix + Shannon Fano!

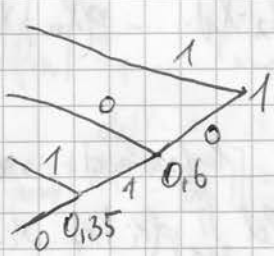
$X_3 \rightsquigarrow 110$ ✓

$X_4 \rightsquigarrow 111$ ✓

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

Pl:

	$p(x_i)$	$\bar{C}$
x_1	0,4	$x_1 \rightsquigarrow 1$
x_2	0,25	$x_2 \rightsquigarrow 00$
x_3	0,2	$x_3 \rightsquigarrow 011$
x_4	0,15	$x_4 \rightsquigarrow 010$



HUFFMANN

0,5 0,6 0,45

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

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

HUFFMANN-hoz kell a valószínűség!

nem jó kevés kóddnál, és nagy valószínűség differenciánál!

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

X_1X_1
X_1X_2
X_1X_3
X_1X_4
X_2X_1
⋮

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

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

memóriamentes

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

DMS ↓

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

↑ n-ed rendben stacionárius időben (n) nem változik $H(X) = H(x_i)\ \forall i$-re

Kiterjesztett forrás hossz rendelt $n \cdot H(X)$

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

n-darab val.változó által generált eseményhez tartozó kód

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

MS extra

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

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

log(szorzat) = összeg (log)

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

n val vált. együttes entrópiája

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

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

1 szimbólumra eső entrópia

1 változóra eső? ha létezik

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

↓

sztochasztikus folyamat végtelen sorozott 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 folyamatnak!

(A) Gallager bizonyítás:

- $H(X_n | X_1 \dots X_{n-1})$ monoton csökkenő!

$$H(X_n | X_1 \dots X_{n-1}) \leq H(X_n | X_2 \dots X_{n-1}) = H(X_{n-1} | X_1 \dots X_{n-2})$$

Hosszabb előzmény nagyobb bizonytalanság! nagyobb entrópia

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

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

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

(C) $H_n(X)$ mon. csökkenő

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

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

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

$H_n(X) \leq \frac{n-1}{n} \cdot H_{n-1}(X) + \frac{1}{n} \cdot H_n(X)$

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

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

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

$n \to \infty \Rightarrow 0 \qquad n \to \infty \Rightarrow 1$

felül becslés

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

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

+ stochastikus folyamat!

ezek egyszerre csak akkor igazak ha egyenlők

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

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

azáltl. kódhossz elvehet az entrópiáig.

L-Z kódolás (dempel-Ziv)

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

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

$L_x = 5$ fix hosszú kóddal

a könyvtár:	tárhely	tartalom	kód	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

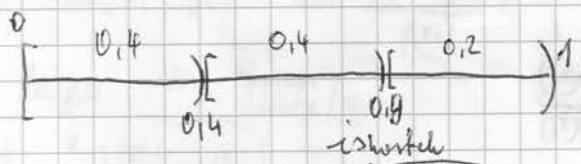
[0111001010011111001] kódsorozat

→ Nem kell hozzá ismernem apriori az eloszlásokat.

Aritmetikai kódolás:

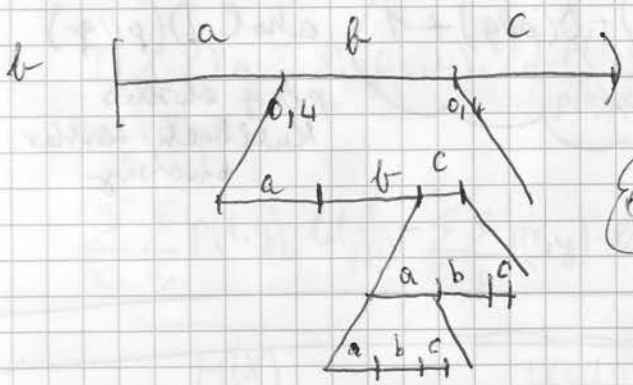
- kell a $P(x)$ •
- tart az optimális kódhossz
- ritka sorozat → ~~hosszú~~ rövid kód, gyakori sorozat → rövid kód

(H)



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

[b, c, a] átírandó sorozat



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

$0,75 = 0.11$ ($2^{-1} 2^{-2}$) bca

ezt kódolom át
mert ez egyértelműen meghatároz egy részintervallumot!

de változó hosszú a kód
kell minden egy stop szimbólum p(!)

~~nem prefix nem tart~~

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

(Kullbach - 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 $p(x_i) = q(x_i) \rightsquigarrow$ távolság $= 0$

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

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

... forráskódolás vége ...

a-posteriori entrópia:

$$H(X|Y) = H(X) - I(X;Y) \qquad \text{és} \quad H(X|Y) \leq H(X)$$

(val.vált.)

$I(X;Y)$: átlagos kölcsönös információ (x_i, y_i-ben is megvan)

def: kölcsönös információ:

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

(← megfigyelve y_i-t)

ha $p(x_i)$ független $p(y_i)$-től akkor $p(x_i|y_i) = p(x_i)$, $\text{ld}\,1 \Rightarrow I(x_i;y_i) = 0$

(nincs kölcsönös információ)

Bayes ↓

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

(x_i-ből együttes valószínűség / $p(y_i)$)

Átlagos kölcsönös információ:

Bayes tétel ↓

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

(X, Y: val.változók)

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

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

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

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

Csatorna kapacitás:

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

(Bitrate)

összes lehetséges bemeneti eloszlás feletti max.

Shannon II. csatornakapacitás kódolás tétele:

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

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

hiba val.ség.

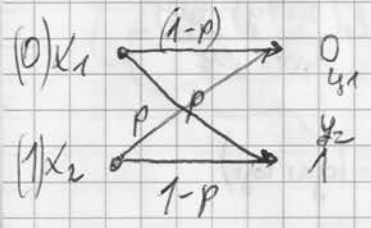
mérnöki Shannon II.:

$$K\text{-s blokk } X \longrightarrow \underbrace{N}_{\text{n nicetőlem}} \cdot X' \;;\; \lim_{K\to\infty} \frac{K}{N} \Rightarrow < C \quad P_{error} \to \emptyset$$

Kódbinfó bitből

DMC - discrete memoryless channel

(1) BSC



p valséggel hibázik

1-p valséggel nem hibázik

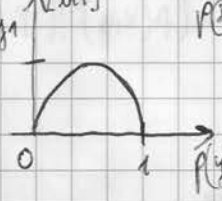
$p(x) \to x_1$ $\quad p(y) \to y_1$

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

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

hy

bin. entrópia fv.



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

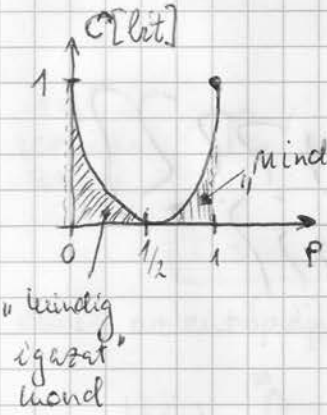
egyenletes eloszlás

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

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

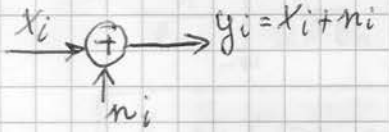
$= p \cdot ld \frac{1}{p} + (1-p) \cdot ld \frac{1}{1-p}$ nem függ a forrás eloszlástól! csak p hibavalószínűségtől

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



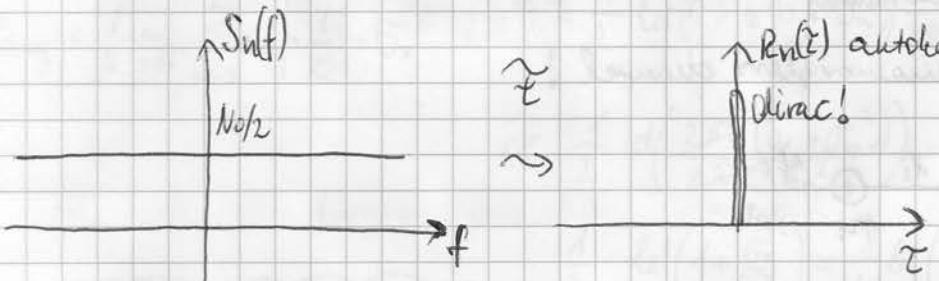
ha 1/2 akkor fogalmam sincs az információról, $C=0$

- 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



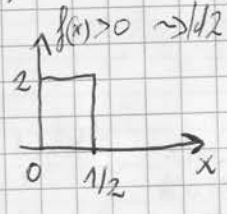
$$N_0 = \frac{h \cdot f}{e^{hf/kT_0} - 1}$$
~~~~

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!!! ??? ...



7. előadás

LOTTÓ

$$C \triangleq \max_{p(x)} I(X,Y)$$

[bit/ksad. mennyiség] — kölcsönös információ — általában [bit/s]

- BSC csatorna:

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

p = hibavalószínűség

DMC ~ discrete memoryless channel!

D-AGWN: $x_i \oplus n_i = y_i$

diszkrét idő, 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)

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

$H(X|Y)$: aposteriori entrópia

Gauss eset!

$x_i \rightarrow (+) \rightarrow y_i = x_i + n_i$, n_i

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

$\xi = 0 \rightarrow$ dirac

ennek az entrópiája:

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

ld helyett ln legyen

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

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

D-AGWN esetben!

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

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

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

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

max akkor ha x_i is Gauss eloszlású

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

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

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

AGWN-nél

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

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

→ folytonos időben, AGWN esetben! más

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

$x(t) \rightarrow \oplus \rightarrow y(t)$ $= x(t) + n(t)$

$n(t)$

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

darab minta

darab minta

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

$x(t)$ legáldább WSS és korrelálatlan!

WSS miatt

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

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

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

$$= \lim_{T\to\infty} \frac{1}{T} K \underbrace{I(X,Y)}_{\text{ez a D-AGWN csatornáé}} \quad \max_{p(x)}$$

$$= \lim_{T\to\infty} \frac{2BT}{T} \cdot \left(\frac{1}{2} \cdot ld\left(1 + \frac{P_{AVG}}{N_0/2}\right)\right) \quad \text{D-AGWN } \sigma_x^2$$

$T_{mintás}$

folyt. AGWN

σ_x^2 -dinamikára!

$$C = B \cdot ld\left(1 + \frac{P_{AVG}}{\sigma_n^2}\right) \quad \sigma_n^2 = N_0/2$$

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

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

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

$K = 2BT$

$$= 2B \cdot \sigma_x^2$$

(sávkorlátozva)

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

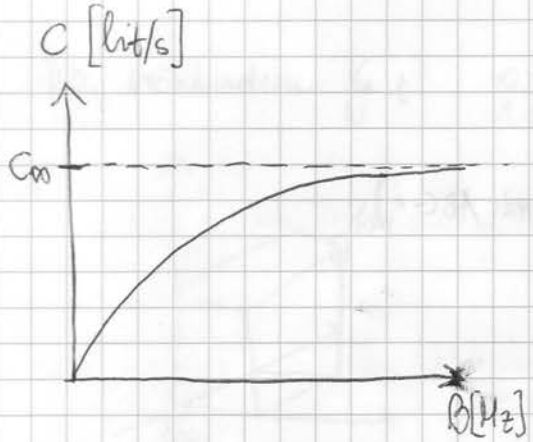
$$C = B \cdot ld\left(1 + \frac{P_{AVG}}{B \cdot N_0}\right) \left[\text{bit/s}\right]$$

AGWN sávkorlátos B Tideig

zaj

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

ha lenne végtelen sávi



normalizált C: $[bit/s]/[Hz] = C/B$

$P_{ave} = E_b \cdot C$ (átlagos teljesítmény)

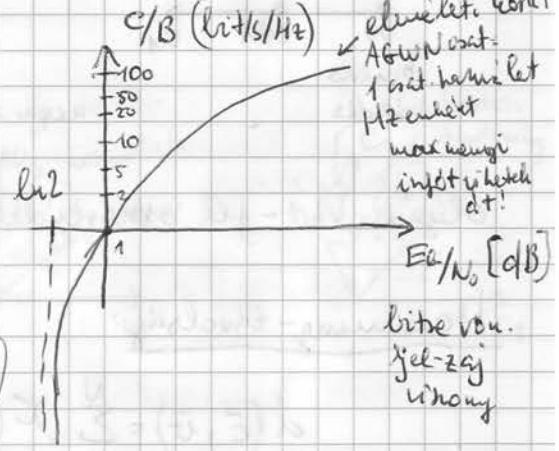
$$\frac{C_{AGWN}}{B} = ld\left(1 + \frac{E_b \cdot C}{B \cdot N_0}\right) = ld\left(1 + \frac{E_b}{N_0} \cdot \frac{C}{B}\right) =$$

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

8. előadás:

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

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



Shannon II tétele:

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

(Ω: Forrás kódoló, Forrás dekódoló lépést)

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

K: információ, N: ennél nagyobb

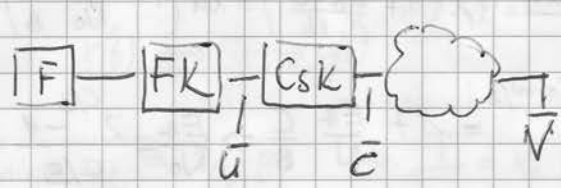
$\lim_{K \to \infty} \frac{K}{N} < C$; $P_e \to 0$ [1 s-re vonatkoztatva van]

$\frac{K}{N} < 1$ erős feltétel !!

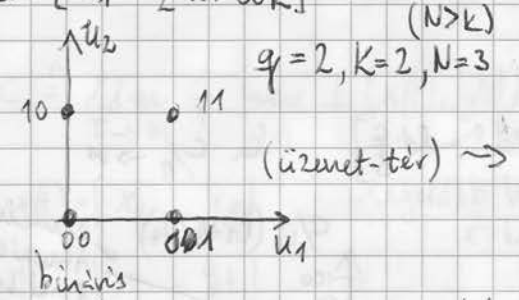
Hibajavító kódolás: (N, K, q)

(error correction coding)

q: értékkészlet (forrás ABC-e)

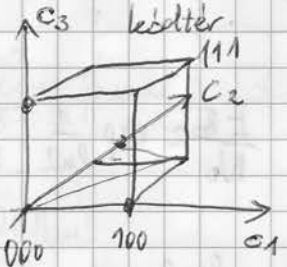


$\bar{u} = [u_1\ u_2 \dots u_K]$



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

(üzenet-tér) →



nem értelmes olyan összerendelés → 00 → 000
01 → 001

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

Hamming-távolság:

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

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

döntő / vett jel → kód szerinti döntés

$D(\bar{v}) = \bar{c}'$ $\quad P_e = \emptyset$, 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 $\bar{v} = \bar{c}_j \neq \bar{c}$

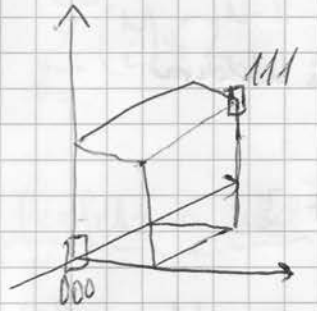
olyan kódot kapok, ami nem eleme az értékkészletnek!

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

de tudom detektálni!

(másra döntök tökéletesen)

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



Algebrai konstrukciók: ... következő oldal!

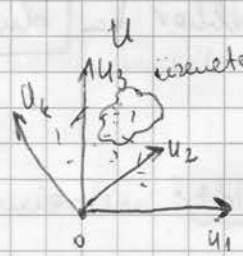
9. előadás

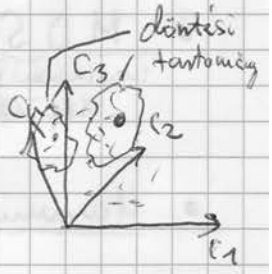
Kezelhető hibák az átvitelben!

üzenetek kódok

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

q^k q^N





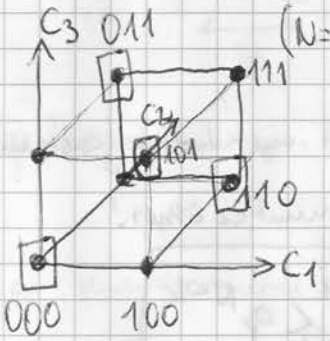
$t_{\text{jelezhető hibák száma}} < d_{min}$ (diszjunkt halmazok miatt) [döntési tartományok] ; $t_{jelezhető} = d_{min} - 1$

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

↓

demodulátor nem akar dönteni mert nem biztos benne

inkább újra kér 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]

$t_{\text{törléses}}$!

Kódkonstrukciós törvények:

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

  adott d_{min}

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

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

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

  hány érvényes kódvektor lehet ?

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

- **Hamming korlát:**

  adott t_{jav} mellett mi a lehetőség (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 tév]

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

  $q^k \cdot \sum_{i=0}^{t_{jav}} \binom{N}{i} \cdot (q-1)^i$ annyi kell, hogy t_{jav} -nyit tudjak javítani !

  üzenetek száma ~~távolsági~~ - és ez biztos kisebb mint az 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 hozzánk $\Rightarrow$ 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 kódot! $\{\underline{c}\}$
- generátor

$$[00] \begin{bmatrix} 011 \\ 101 \end{bmatrix} \updownarrow k \qquad \boxed{\underline{u} \cdot \underline{G} = \underline{c}}$$

$\underline{u}$ $\quad \leftrightarrow N$ $\quad G$

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

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

$$G_{\text{szisztematikus}} = [\underbrace{\underline{I}}_{\leftrightarrow N} \mid \underline{P}] \updownarrow k$$

$\underline{\underline{G}} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix}$ sorcsere! $G_{\text{rendszer}} = \left[\begin{array}{c|c} \underline{\underline{I}} & \underline{\underline{P}} \\ \hline \underline{\underline{0}} & 1 \\ 1 & 1 \end{array}\right]$

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

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

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

példa $\underline{\underline{H}} = [1\,1 \mid 1]$

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

$\bar{c}$

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

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

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

2. ZH anyaga eddig

10. előadás

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

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

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

$\underline{v} = \underline{c} + \underline{e}$ — $\underline{v}$ vett vektor, $\underline{c}$ kód, $\underline{e}$ hiba

$\underline{v}$ érvényes-e? igen $\rightarrow \hat{\underline{c}}$

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

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

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

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

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

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

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

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

$1 + N \leq 2^{N-K}$ (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 kódarány 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!

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

kódsúlya — ahol nem 0

lin. esetben: a kódban hány (1) van.

lineáris kódokra

$d_{min} = \min_{\forall i} w(c_i)$ kivéve $\underline{c} = \underline{\emptyset}$

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

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

↑ ide kell helyettesítgetni és kijön N és K

N	K	R_c	m
5	1	1/5	
90	78	78/90	

→ kijön, de ilyen nincs!

binaris Hamming kód:

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

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

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

N−K; 2^1, 2^2, 2^3

ide azokat rakom amik még nem voltak $\underline{I}$-ben mindegy milyen sorrendben.

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

$k \times N$

$\underline{u} = [1101]$ ⇝ $\underline{c} = [1101100]$ ↑ hiba

$\underline{v} = \underline{c} + \underline{e}$ ⇝ $\underline{s}^T = [101]$ ⇝ $\underline{H}$-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

$d_{min} \geq 3$ 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 prímszendű

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 $13-10 \neq 2$

$\qquad\quad 13 \quad 10$

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

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

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

2" 1' $(4 \bmod 3 = 1)$

$(4,2,3)$ kód
$N\ K\ q$

$\underline{e}=[0\,0\,\ldots\,\underbrace{e}_{\text{nem bináris!}}\,0\,0]$

súlyozom e-vel a hibaértékkel

$GF(q=3)=\{0;1;2\}$ $\quad \alpha^{-\infty}\ \alpha^0\ \alpha^1$ $\qquad \alpha^b=2$ primitív elem $\qquad \alpha^{q-1}=1$

11. előadás

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

perfekt: minden hibamintát felismer; MDS: d_{min} = maximális

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

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

p prím

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

$deg(\alpha)=q-1 \rightsquigarrow \boxed{\alpha^{q-1}=1}$ 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: $h_i \rightarrow$ hibahely, e_i = hiba értéke

$e_i = q - 1$ féle = $\boxed{4}$

MDS legyen $\rightarrow N - K = 2$

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

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

$\leftrightarrow N-K$

$\boxed{\frac{S^T}{e_i} = h_i^T}$ egyik oszlopa

normálva

minden oszlop vezéreleme $\underline{\underline{1}}$ lesz legyen

hogy kiolvasni az értéket

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

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

Ksor Nsklop

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

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

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

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

$\underline{S} = ?$ $\quad \underline{V}^T = \begin{bmatrix} 3 \\ 0 \\ 2 \\ 4 \\ 4 \\ 4 \end{bmatrix} \cdot \underline{\underline{H}} = \underline{S}^T = \begin{bmatrix} 3 \\ 0 \end{bmatrix} \rightsquigarrow$ normáljuk $\begin{bmatrix} 1 \\ 0 \end{bmatrix} \rightsquigarrow$ $\underline{\underline{H}}$-ban az 5. oszlop értéke

3 0 2 4 (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

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

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

⊛ szorzás (GF(q)) felett

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

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

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

⊘ osztás GF(q) felett

hányados, maradék

$a(x)$ 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:

$$C_0 = u(\alpha^0)$$

① $C_1 = u(\alpha^1)$ ② $\underline{c} = \underline{u} \cdot \underline{G}$ $G = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & & \alpha^{N-1} \\ 1 & \alpha^2 & \alpha^4 & & \\ 1 & \vdots & & & \\ 1 & \alpha^{k-1} & \alpha^{2(k-1)} & \dots & \alpha^{(k-1)(N-1)} \end{bmatrix}$ (oszlopdom)

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

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

(3) $\mathcal{C} = \{ C_k,\ c(d^i) = \emptyset,\ i = 1, \dots q^k - 1 \}$

$\mathcal{C}_0 = \{ \underline{c},\ H\underline{c}^T = \emptyset \}$

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

$\longleftrightarrow N$

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

$\Updownarrow$

BIZ

MDS akkor a kód!

$w(\underline{c}) = N - \#C(\text{nullhelyei}) \geq N - \text{U(x) gyök} \geq N-(K-1)$

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

$\Downarrow$

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

12. előadás

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

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

$\longleftrightarrow N$

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

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

$2t_{jave} = \underbrace{N-K}_{\text{paritás szimbólumok száma}}$

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

$\longleftrightarrow N$

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

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

Peterson - Gorenstein - 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 <u>első elemei</u>.

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

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

$$\bar{S}^T = \underline{\underline{H}} \cdot \bar{e}^T \Rightarrow \begin{bmatrix} S_1 \\ S_2 \\ S_3 \\ S_4 \end{bmatrix} = \left[\rightsquigarrow \boxed{\bar{S}^T = e_i \bar{h}_i^T + e_j \bar{h}_j^T} \right] \rightsquigarrow$$

$$S_1 = h_i \cdot e_i + h_j \cdot e_j$$
$$S_2 = h_i^2 \cdot e_i + h_j^2 \cdot e_j$$
$$S_3 = h_i^3 \cdot e_i + h_j^3 \cdot e_j$$
$$S_4 = h_i^4 \cdot e_i + h_j^4 \cdot e_j$$

nem lin. egyenletrsz.

lokátorpolinom: gyöke h_i és h_j

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

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

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

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

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

(+)

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

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

$$\underbrace{e_i h_i^3 + e_j h_j^3}_{S_3} + L_1\left(\underbrace{h_i^2 e_i + h_j^2 e_j}_{S_2}\right) + L_0\left(\underbrace{h_i e_i + h_j e_j}_{S_1}\right) = 0$$

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

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

$$\underbrace{S_4 + L_1 \cdot S_3 + L_0 \cdot S_2 = 0}_{\text{vår lineære egenskap!}}$$

⊛ $RS(6, 2, 7)$

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

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

$u = [3\ \ 5]$

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

$\bar{v} = [1\ \ 6\ \ 6\ \ 5\ 5\ 0]$

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

e_i (2) $\quad$ e_j (3)

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

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

$6 + L_1 \cdot 1 + 3 \cdot L_0 = 0$ $\rightsquigarrow$ $4 + 2L_0 = 0$

$L_0 = 3/2$

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

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

$L_1 = -(h_i + h_j)$

$L_0 = h_j \cdot h_i$

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

$\emptyset = -(h_i + h_j)$

$5 = h_i \cdot h_j$

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

$4 = 3e_i + 4e_j$

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

végén $\underline{\underline{H}}$-val megszorzom $\rightarrow \underline{v} = [1\,6\,6\,5\,5\,0]$

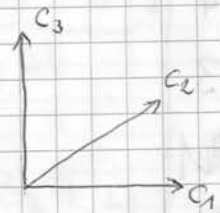
$e = [0\,2\,0\,0\,3\,0]$

$\hat{C} = [1\,4\,6\,5\,2\,0]$

javítottunk 2 hibát!

13. előadás

Blokk kódolás: ciklikus kód pl: CRC „cyclic redundancy check"



$(3,2,2)$

ciklikus kódok: (N,k,q)

érvényes kódszó legyen: $[c_0, c_1 \dots c_{N-1}]$

akkor érvényes kódszó lesz ez is: $[c_{N-1}\ c_0\ c_1\ c_2 \dots c_{N-2}]$

[ciklikus eltoltja egy kódnak szintén kód]

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

$$x \cdot C(x) = c_{N-1} + c_0 x + c_1 x^2 + c_2 x^3 \dots c_{N-1} \cdot x^N \quad | + c_{N-1} - c_{N-1}$$

$$= \underbrace{c_{N-1} + c_0 x + \dots c_{N-2} \cdot x^{N-1}}_{C_1(x)} + c_{N-1}(x^N - 1)$$

hogy áll elő: $C_1(x) \rightsquigarrow x \cdot C(x) \bmod (x^N - 1)$

↓ ez éppen a maradék

$$C_i(x) = x^i \cdot C(x) \bmod (x^N - 1)$$

1 kódból az összes előállítható

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

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

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

$C(x) = u(x) \cdot g(x) \quad | \cdot h(x) \Rightarrow C(x) \cdot h(x) = u(x) \cdot g(x) \cdot h(x) = \underbrace{u(x) \cdot (x^N - 1)}_{\text{osztható lesz}}$ ($(k-1)$-fok)

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

$$\underbrace{u(x) g(x)}_{c_x} \cdot h(x) \bmod (x^N - 1) = \underline{\underline{\emptyset}}$$

$$\boxed{c(x) \cdot h(x) \bmod (x^N - 1) = \emptyset}$$ ekkor jó

vett jel

ha $v(x) = c_i(x)$ hett értéku egyezik az eredetivel

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

Biz: $c(x) = \underbrace{x^{k-1}}_{\text{üzenet}} \cdot g(x)$

$c_1(x) = \underbrace{x^k \cdot g(x)}_{\text{maradék}} - \overbrace{(x^N - 1)}^{\text{átlépnek vagyon.}} c_{N-1}$

- Minden lódzó osztható $g(x)$ generátor polinommal.

$\underbrace{x^k \cdot g(x)}_{\text{definíció}}$ osztható $g(x)$-el és (x^N-1) osztható $g(x)$-el $\rightsquigarrow c_i(x)$ osztható $g(x)$-el

✓ Q.E.D.

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

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

$$x^7+x^6+x^5+x^4+x^3+x^6+x^5+x^4+x^3+x^2+x^4+x^3+x^2+x+1 = x^7 + \cancel{2x^6} + \cancel{2x^5} + \cancel{2x^4} + \cancel{2x^3} + \cancel{2x^2} + x + 1$$

$g(x)$ és $h(x)$ magyar

$= x^7 + 1 = x^7 - 1$ GF(2) miatt ✓

CRC: szisztematikus, ciklikus

$$c(x) = u(x) \cdot x^{N-k} - \underbrace{\left[u(x) \cdot x^{N-k} \bmod g(x)\right]}_{\text{maradék } (r(x)) \rightsquigarrow \deg(r(x)) = N-k-1}$$

osztható $g(x)$-el

Így: $\bar{u} = [u_0\ u_1\ u_2\ \dots\ u_{k-1}]$

$\bar{c} = [c_0\ \dots\ \underbrace{c_{N-k-1}}_{c_{N-k}\text{-dik helyen}}\ u_0\ \dots\ u_{k-1}]$ (u_{k-1}: c_{N-1})

üzenetet felshiftelteem üzenetnő van a lódszóban.

ez ciklikus és szisztematikus is!

1893 (lineáris, bináris blokk kód)

Hadamard kód, mátrix:

$N \times N$ négyzetes mátrixok, $N = 8 \cdot m$, $m \in \mathbb{Z}$, bináris ± 1

$$H_{2N} = H_N \otimes H_N$$

Kronecker szorzat

$$H_1 = [1] \qquad H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \qquad H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

H_8 = (bármely 2 sora)

0000
0001
0010 ennek sorai ortogonálisak
0011
0100 $\overline{z_i} \cdot \overline{z_j} = \emptyset$
0101 ←

$$\begin{bmatrix} H_8 \\ -H_8 \end{bmatrix} / \begin{bmatrix} H_N \\ -H_N \end{bmatrix}$$

$(N, \mathrm{ld}(2N), 2)$

$$H_{2N} = \begin{bmatrix} H_N & H_N \\ H_N & -H_N \end{bmatrix}$$

$$H_N \cdot H_N^T = N \cdot \underline{\underline{I}}$$

} érvényesek!

hibadetektálás és javítás

$$\underline{S}^T = \underline{\underline{H}}\, \underline{v}^T = \pm N \cdot \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \text{-} i\text{-sor}$$

ha $v = c_i$

üzenet: 0101

$$v = \begin{bmatrix} + \\ + \\ + \\ - \\ + \\ - \\ + \\ - \end{bmatrix} \rightsquigarrow \begin{bmatrix} 2 \\ -2 \\ 2 \\ -2 \\ 2 \\ (6) \\ 2 \\ -2 \end{bmatrix} = \text{korrelációt számítottam}$$

→ felső H_8-ból 6-dik

→ 0101

hiba javítva

súly

$$d_{min} = \frac{N}{2} = \underset{min}{w(\underline{c})}$$

$t_{jav} = \left\lfloor \frac{d_{min} - 1}{2} \right\rfloor$ $\quad N = 4m \rightsquigarrow t_{jav} = \left\lfloor \frac{2m-1}{2} \right\rfloor = m - 1$

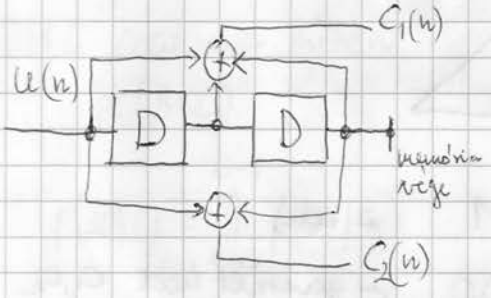
V

15. előadás

Konvolúciós kódoló: memóriával rendelkezik

(n, k, L, q) $\quad L$ - kényszerhossz $\rightsquigarrow$ mennyi ideig hat a kom ablak?

$q = 2$ eset $(2, 1, 3, 2)$ $\quad R_c = 1/2$

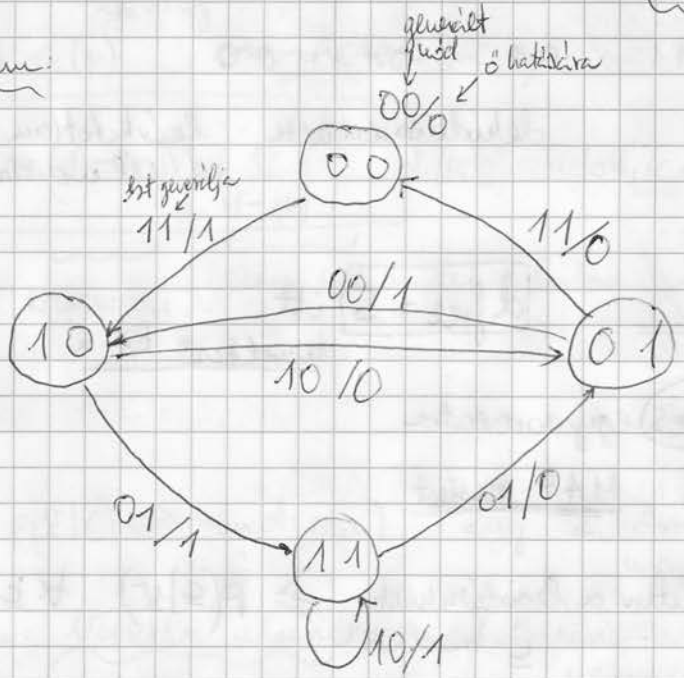


→ ábrázolhatjuk állapotdiagram-on

$L = 3 \rightsquigarrow$ 3 kódnó ra van hatása az előzőek!

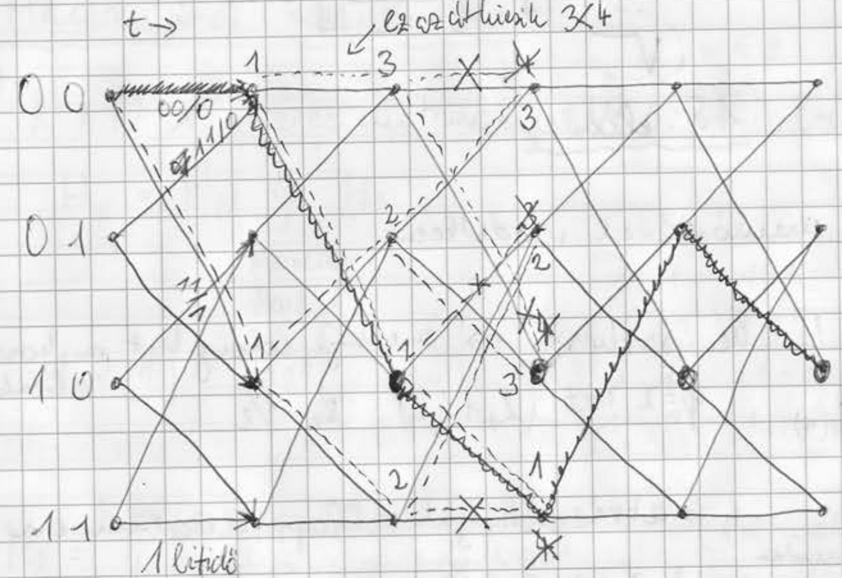
{$c_1, c_2 / q(n)$ alakban}

Állapot diagram:



Trellis kód, diagram

ez nem blokk kód



u	0	1	1	0	1	← u(n)
c	00	11	01	01	00	← generált kód c_1, c_2.
$\hat{v}$ hibás	01	11	01	01	00	

hibázik a csatorna

dekódolás menete: lerajzolhatatlan! el kell mondani!

MAP döntést hoz (max aposteriori probability)

$d_{free} = 5$ itt következő EA-n

Dekódolás, döntés egy sorozatra

Optimális döntés: MAP-szerint

$P(\hat{\underline{c}} \mid \underline{v})$ $\underline{v}$ után a legvalószínűbb $\hat{\underline{c}}$-ra döntök $\geq P(\underline{c} \mid \underline{v})$ $\forall \underline{c}$ esetére

Bayes döntések: statisztikus döntés, ahol a MAP az optimális!

$$p(\hat{\underline{c}} \mid \underline{v})\, p(\underline{v}) \geq p(\underline{c} \mid \underline{v})\, p(\underline{v})$$

$$p(\hat{\underline{c}}, \underline{v}) \geq p(\underline{c}, \underline{v})$$

$$p(\underline{v} \mid \hat{\underline{c}}) \cdot p(\hat{\underline{c}}) \geq p(\underline{v} \mid \underline{c})\, p(\underline{c})$$

$$\hat{\underline{c}} = \arg\max_{\underline{c}} \left(p(\bar{v} \mid \bar{c}) \cdot p(\bar{c}) \right)$$

$P(\underline{c})$ apriori kód eloszlás ! ezt ha nem tudjuk → nem lesz optimális

ehelyett: ML (maximum likelihood) [szub-optimális döntés]

$ML = MAP \iff P(\underline{c})$ egyenletes eloszlású (max entrópiájú)

$$\hat{\underline{c}} = \arg\max_{\underline{c}} \left(p(\underline{v} | \underline{c}) \right)$$

DMC csatorna esetén

pl (BSC)

$$p(\underline{v} | \underline{c}) = \prod_{i=0}^{N-1} p(v_i | c_i)$$

Spec. eset: BSC (p) (hibavalószínűség) ~~p<1/2~~ $(0 < p < 1/2)$

$$p(\underline{v} | \underline{c}) = (1-p)^N \cdot \left(\frac{p}{1-p} \right)^{d(\underline{v},\underline{c})}$$

$d(\underline{v},\underline{c})$ adott, $\underline{v}$ és $\underline{c}$ mellett a Hamming-távolság

N üzenetbit — ennyi helyen lehet hiba

$$0 < \frac{p}{1-p} < 1$$

ML: $\max_{\underline{c}} p(\underline{v} | \underline{c}) \Leftrightarrow \min_{\underline{c}} d(\underline{v},\underline{c})$ így 2^N összehasonlítást kéne végezni

ehelyett legyen: Viterbi algoritmusa (lineáris a üzenethosszal! nem exponenciális)

L

2 út a Trellisen nem tud a hosszánál rövidebb hurkot alkotni.

MLSE döntés ⇔

"sequence" || "estimation!"

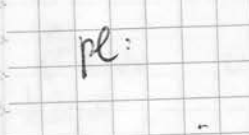
16. előadás

Viterbi dekódoló algoritmus: szuboptimális döntés
Maximum Likelyhood döntés
(a-posteriori ismeretek után döntünk)
sorozat hosszával lineárisan nő

BSC (p) csatorna esetén a hibavalószínűség

d_{free}: min hosszú hurkok közti Hamming távolságoknak minimuma
Trellis diagramon
(minél kisebbnek az utak)

pl:



$P_{hiba} \rightarrow P_5 = \binom{5}{3} p^3 (1-p)^2$ 3 hiba van
$d_{free}=5$

$$P_d = \begin{cases} \text{ptlan} & \sum_{i=\frac{d+1}{2}}^{d} \binom{d}{i} p^i (1-p)^{d-i} \\ \text{páros} & \frac{1}{2}\binom{d}{d/2} p^{d/2}(1-p)^{d/2} + \sum_{i=d/2+1}^{d} \binom{d}{i} p^i (1-p)^{d-i} \end{cases}$$

BSC

$$P_e \leq \sum_{d=d_{free}}^{\infty} a_d P_d$$

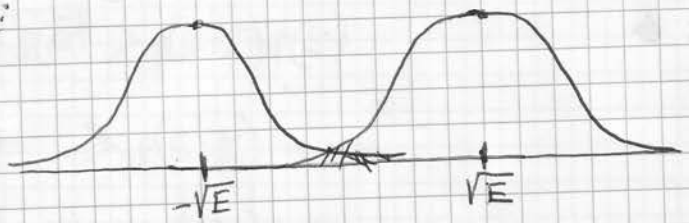
↓ ↘ előző

} ez javít!

a_d: hurkok száma amik Hamming távolsága d

A GWN esetben:

Energia



$P_e \leq P_{EB} \leq \frac{1}{2}\,erfc$

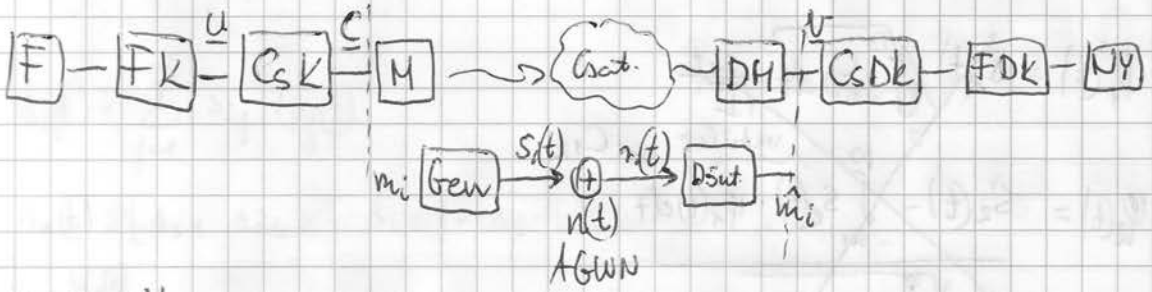
$P_{ERROR} = \frac{1}{2}\, a_d \cdot erfc\left[\sqrt{\frac{E_b}{N_0}}\right]$

$$P_{ERROR} \leq \frac{1}{2} \cdot \sum_{d=d_{free}}^{\infty} a_d \cdot \operatorname{erfc}\left[\sqrt{\frac{E_b}{N_0} \cdot R_c \cdot d}\right]$$

R_c - kódarány
d - futó fábbos
E_b - bitenergia
N_0 - spektr. teljesítmény sűrűség

a_d miatt a hiba lin. nőne, de az $R_c \cdot d$ nagyon nagy és így erfc exponenciálisan csökken.

Digitális modulációs eljárások
(vivőfrekvenciás átvitel)



$M\{m_i\}^M$ M véges kell legyen!
véges számú üzenet lehet véges sok → más különben nem tudok dönteni.

$\Updownarrow$

$S\{s_i(t)\}^M$ véges típusú jelek, véges tartójú jelek, véges energiájú, véges elemszámú

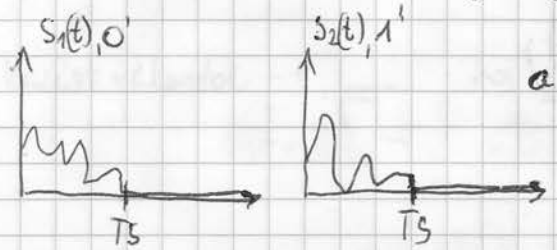
$\forall s_i(t) = 0, \forall [t<0 \quad t>T_s]$  véges tartó T_s ideig

$\forall s_i(t)$ más jelalakú

$$E_i = \int_0^{T_s} s_i^2(t)dt < \infty$$

$$s_i(t) \neq s_j(t) \quad i \neq j \quad \forall i,j \in (1 \dots m)$$

pl:



a döntés a vett jel alapján optimális ha

MAP $\max p\left(\hat{s}_i(t) \mid r(t)\right)$

Feltér: (Gram-Schmidt ortogonalizációs eljárás)

$S\{s_i(t)\}^m$ $\quad D \leq M \quad D = M \Leftrightarrow$ ha D is b

D: alkotunk egy teret

$\Phi\{\phi_i(t)\}^D$ $\int_{-\infty}^{\infty} \phi_i^2(t)\,dt = 1$ $\Rightarrow$ $\int_{-\infty}^{\infty} \phi_i(t)\,\phi_j(t)\,dt = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$

végestartójúak! ortonormált rendszer

nem jelalakok lesznek, hanem vektorok!

G-S:

$\varphi_1'(t) = s_1(t) \Big/ \sqrt{\int_0^{T_s} s_1^2(t)\,dt} = \frac{s_1 t}{\sqrt{E}}$

$\varphi_2(t) = \dfrac{s_2(t) - \int_{-\infty}^{\infty} s_2(t)\cdot\varphi_1(t)\,dt}{\sqrt{\int_{-\infty}^{\infty} s_2(t) - c_{12}\,dt}}$ $\quad$ vetület $\leftarrow c_{12}$

$\varphi_1(t) = s_1(t) \Big/ \sqrt{\int_0^{T_s} s_1^2(t)\,dt} = \frac{s_1(t)}{\sqrt{E_1}}$ $\qquad c_{12} = \int_{-\infty}^{\infty} s_2(t)\cdot\varphi_1(t)\,dt$

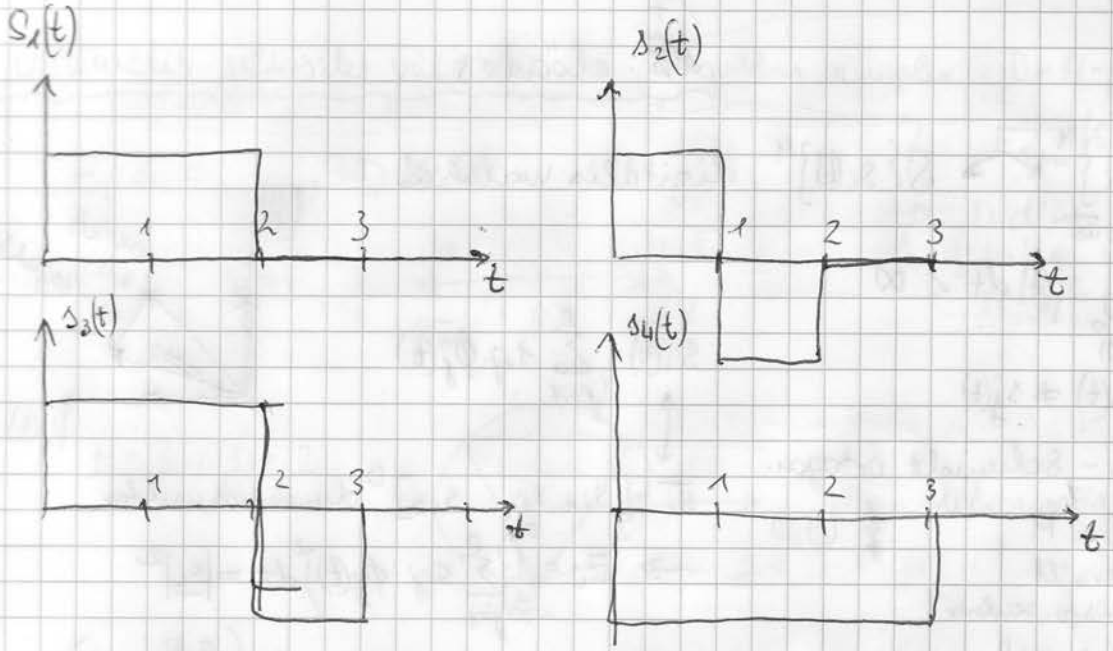
$s_2(t) - c_{12}\cdot\varphi_1(t) = \varphi_2'(t)$

$\varphi_2(t) = \dfrac{\varphi_2'(t)}{\sqrt{\int_{-\infty}^{\infty} \varphi_2'^2(t)\,dt}}$

$c_{ij} = \int_{-\infty}^{\infty} s_j(t)\cdot\varphi_i(t)\,dt$

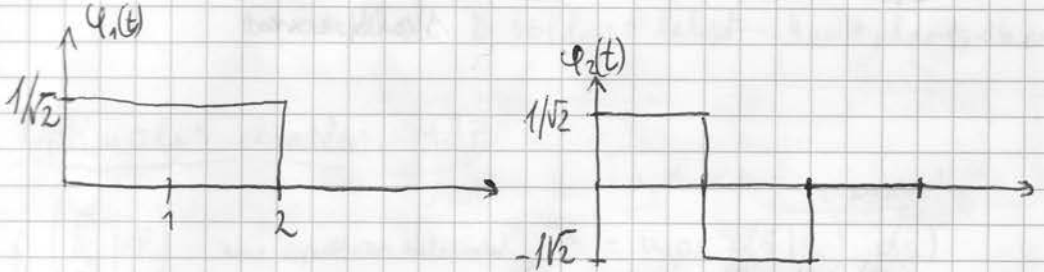
$\varphi_j'(t) = s_j(t) - \sum_{k=1}^{j-1} c_{ij}\cdot\varphi_i(t)_j$

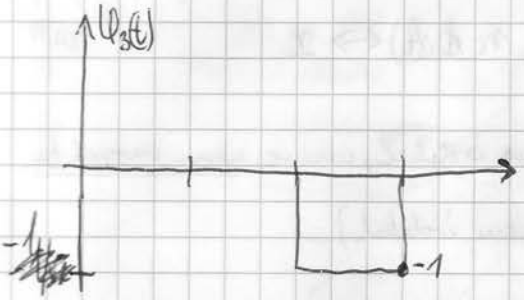
$\Rightarrow \varphi_j t = \dfrac{\varphi_j'(t)}{\sqrt{\int_{-\infty}^{\infty} \varphi_j'^2(t)\,dt}}$



$$s_i(t) = \sum_{j=1}^{D} s_{ij} \cdot \varphi_j(t)$$

$$s_i(t) \Rightarrow [s_{i1}\ s_{i2} \dots s_{iD}] = \bar{s}_i$$





3 dimenziós tér

$\varphi_4(t) = \emptyset$ nem ftlen

ilyenkor más bázist választok -  $\rightsquigarrow$ 5 vektorokkal számolhatok

17. előadás

$\mathcal{M}\{m_i\}_1^M \leftrightarrow \mathcal{S}\{s_i(t)\}_1^M$ digitális modulációk

$E_i = \int_{-\infty}^{\infty} s_i^2(t)\,dt < \infty$ (Ts)

$T_S,\ s_i(t) \neq s_j(t)$

Gram-Schmidt ortogonalizáció

$D \leq M$

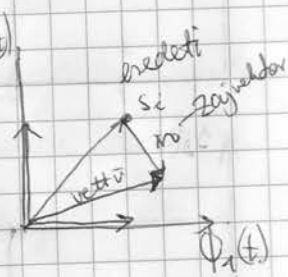
ortonormált bázisfv. rendszer!

$\{\phi_i(t)\}_1^D \rightarrow$ D dimenziós jelter!

$s_i(t) = \sum_{j=1}^{D} s_{ij}\,\phi_j(t)$

$\underline{s_i} = [s_{i1}\ s_{i2} \dots s_{iD}]$ D dimenziós vektor.

$\rightarrow E_i = \int_{-\infty}^{\infty} \left[\sum_{j=1}^{D} s_{ij}\cdot\phi_j(t)\right]^2 dt = |\underline{s_i}|^2$ (Pithagorasz)



$\int_{-\infty}^{\infty} s_i(t)\cdot s_j(t)\,dt = \int_{-\infty}^{\infty} \left(\sum_{i=1}^{D} s_{ij}\phi_j(t)\right)\left(\sum_{k=1}^{D} s_{jk}\phi_k(t)\right) dt = \underline{s_i}\cdot\underline{s_j}$

skalárszorzat

AGWN esetben

$r(t) = \sum_{i=1}^{D} r_i\,\phi_i(t) \leftrightarrow \underline{r}$

$n(t) = \sum_{i=1}^{D} n_i\cdot\phi_i(t) + \tilde{n}(t)$ — $\bar{n}$-ből csak az érdekel, amire nem vagyok ü.

$\bar{n} + \tilde{\bar{n}} \Leftarrow$ ortogonális ϕ-kre (nem érdekel)

$\dim(\bar{\bar{n}}) = \infty$ / $\underline{s_i}$

$n(t) = \bar{n} + \bar{\bar{n}} = \sum_{i=1}^{D} n_i\cdot\phi_i(t) + \tilde{n}(t)$

$r(t) = \sum_{i=1}^{D} r_i\cdot\phi_i(t) \leftrightarrow \underline{r}$

Optimális jelkészlet választás : (reguláris simplex $D = M-1$)

$E_{max} = |\bar{s}_i|^2$

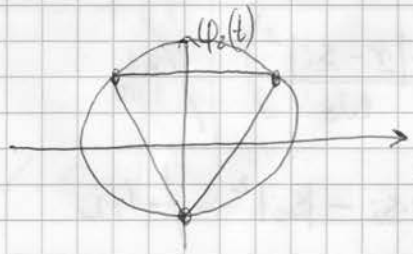
a D dim. gömb felszínén vannak!

$\bar{s}_i \cdot \bar{s}_j = -\frac{E_{max}}{D}$

$E_i \leq E_{max}$, $D \leq M$

$M=2$ $D=1$

$M=3$; $D=2$



kiválasztás

$M=4$; $D=3$ tetraéder

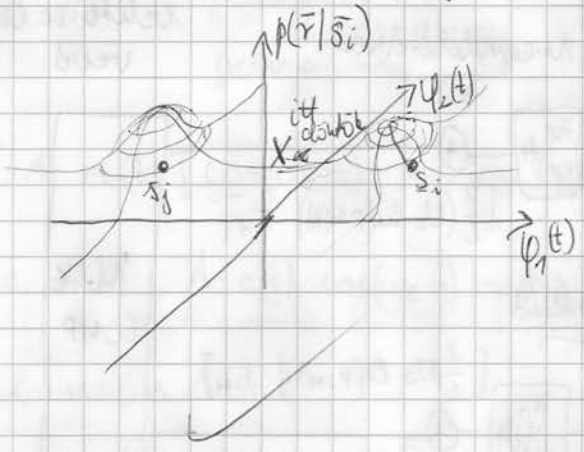
Növeljük a dimenziószámot → nagyobb távolság.

Inkább szuboptimális megoldás

$M=2$ D több is lehet 4 pont, 8 pont, 16 pont stb.

Optimális döntés: MAP

$\underset{i}{\max}\, p(\bar{s}_i|\bar{r})$ max aposteriori valószínűség $\rightsquigarrow = \underset{i}{\max}\, p(\bar{r}|\bar{s}_i) \cdot p(\bar{s}_i)$ (apriori!)



AGWN esetben

D-dim Gauss-eloszlást követ

$$f_{\underline{n}}^{D}(\bar{n}) = \frac{1}{\sqrt{\pi \cdot N_0}} \cdot \exp\left[\frac{|\bar{n}|^2}{N_0}\right]$$

$\sigma_n^2 = N_0/2$ ← nem $\sqrt{(\pi N_0)^{D/2}}$

döntési térben kell egy D dim. tartomány minden vektorhoz!

(így jobb lesz!)

Hibavalószínűség: $P_e = 1 - \sum_{i=1}^{M} P_{ci}$

$$P_{correct_i} = \int_{v_i^D} p(\underline{s}_i|\underline{r})\, d\bar{r} = \int_{v_i^D} p(\underline{s}_i) \cdot p(\bar{r}|s_i)\, d\bar{r}$$

D-dim. integrál

nem kell szimetrikus legyen felületenként a 2 felület

ha nincs ISI, AGWN akkor az optimális döntőkörülék:

MAP

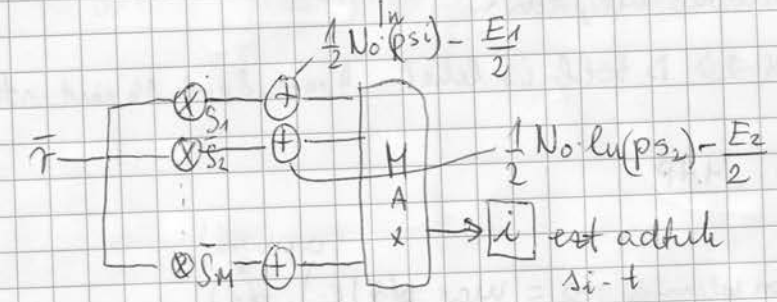
$$\max \underbrace{p(\underline{s}_i)}_{\text{apriori}} \cdot \frac{1}{\sqrt{\pi \cdot N_0}} \cdot \exp\left[-\frac{|\underline{r}-\underline{s}_i|^2}{N_0}\right] \quad / \ln$$

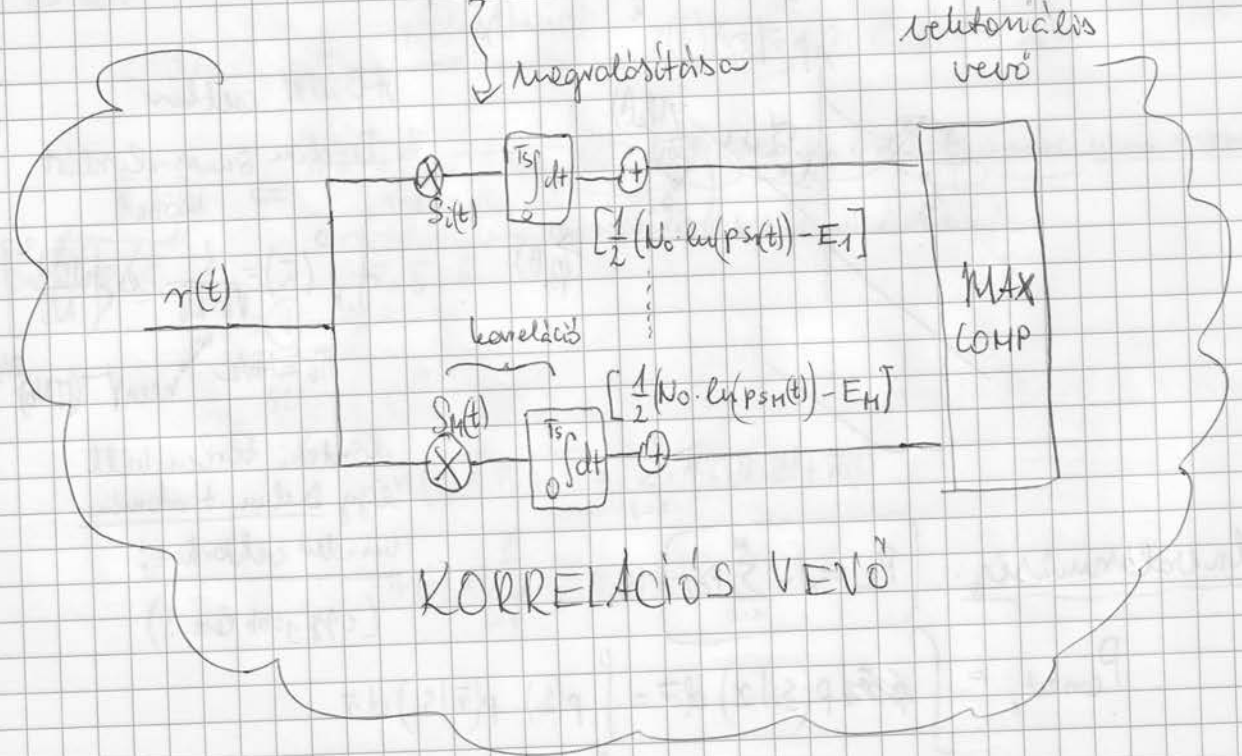
$$\ln p(\underline{s}_i) + \underbrace{\ln \frac{1}{\sqrt{\pi N_0}}}_{\text{ffen i-től}} + \left(-\frac{|\underline{r}-\underline{s}_i|^2}{N_0}\right) \quad / N_0$$

$$N_0 \cdot \ln p(\underline{s}_i) - \underbrace{|\underline{r}|^2}_{\text{ffen i-től}} + 2\,\underline{r}\cdot\underline{s}_i - |\underline{s}_i|^2 \quad / \cdot 1/2$$

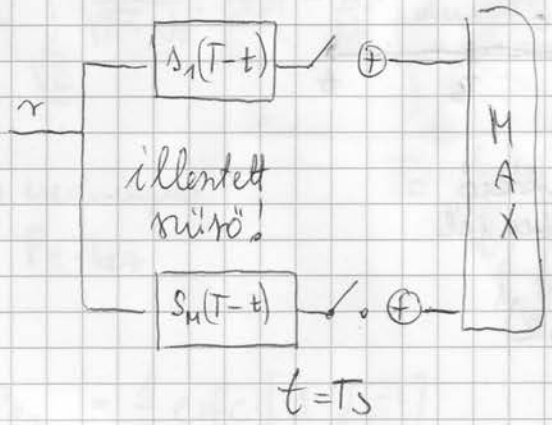
$$\frac{1}{2} \cdot N_0 \cdot \ln p(s_i) + \underbrace{\underline{r}\,\underline{s}_i}_{\text{korreláció}} - \frac{|\underline{s}_i|^2}{2} \Big\} \text{energia}$$

így:





$$\int_0^{T_s} s_i(T-t+\tau)\, r(\tau)\, d\tau \Big|_{T=t} \Rightarrow \int_0^{T_s} s_i(\tau)\cdot r(\tau)\, d\tau$$



18. előadás

Vivőfrekvenciás átvitel

$$u(t) = \sqrt{2}\cdot A\cdot \cos(\omega_c t + \varphi)$$

$$x(t) = \sqrt{2}\, A\cdot m(t)\cdot \cos(\omega_c t + \vartheta(t) + \varphi)$$

amplitudó modulációs $m(t)$

szög mod. $\vartheta(t) \Rightarrow$ fázis mod $\vartheta(t)$

frekvencia mod $\frac{\partial \vartheta(t)}{\partial t}$

$$x(t) = \sqrt{2}\cdot A\cdot m(t)\cdot\left[\cos(\omega_c t)\cdot\cos(\vartheta(t)+\varphi) - \sin(\omega_c t)\cdot\sin(\vartheta t+\varphi)\right]$$

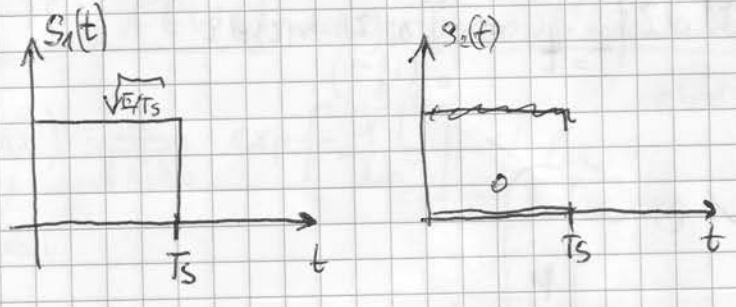
kvadratúra alak: $A\cdot a(t)\cdot\cos(\omega_c t) - A\, q(t)\cdot\sin(\omega_c t)$

komplex burkolós leírás

$$x(t) = A\Rightarrow Re\left[\left[\underbrace{\left(a(t)+j\cdot q(t)\right)}_{\text{komplex burkoló}}\right]\cdot e^{j\omega_c t}\right]$$

M, D = M-1

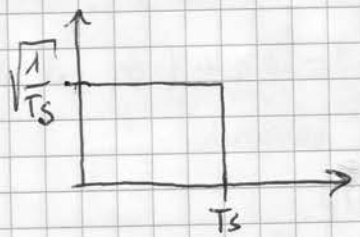
M = 2



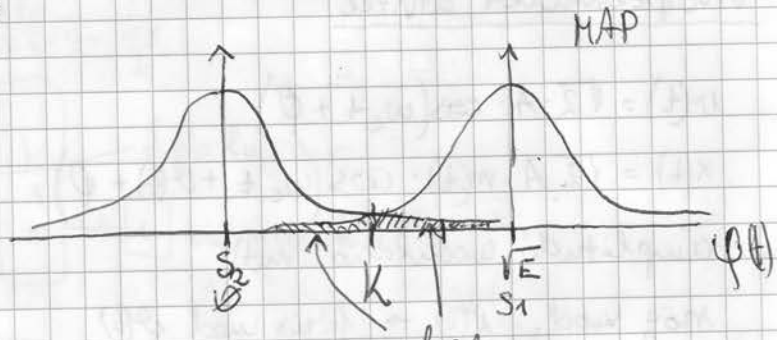
OOK moduláció
van jel / nincs jel
vagy
(2-ASK)

Gram-Schmidt ortogonalizáció:

$\varphi(t)$:



AGWN csatorna
korrelációs vevő



s_2-t adom = 0 → csak a zajt veszem

s_1-t adom ⇒ eltolódik a várható érték

ahol $p(s_1) = p(s_2)$ ⇝ K küszöbérték

$$p(s_1) \cdot \frac{1}{\sqrt{\pi N_0}} \cdot \exp\left[-\frac{|K-s_1|^2}{N_0}\right] = p(s_2) \frac{1}{\sqrt{\pi N_0}} \cdot \exp\left[-\frac{K^2}{N_0}\right]$$

$\boxed{p(s_1) = p(s_2)}$

feltesszük
a max európiát

$$(K-s_1)^2 = K^2 \rightsquigarrow$$

$$-2Ks_1 + s_1^2 = 0$$

$$2Ks_1 = s_1^2$$

$$\boxed{K = \frac{s_1}{2}} \rightsquigarrow \boxed{\frac{\sqrt{E}}{2}}$$

$$\boxed{K = \frac{\sqrt{E}}{2}}$$

$$\operatorname{erfc}(x) = \text{[Gaussian curve, shaded tail from } x \text{ to } \infty\text{]} = \frac{2}{\sqrt{\pi}} \int_x^{\infty} \exp[-u^2]\,du$$

$$\frac{1}{2} \cdot 2 \int_{\frac{\sqrt{E}}{2}}^{\infty} \frac{1}{\sqrt{\pi \cdot N_0}} \cdot \exp\left[-\frac{\left(u\sqrt{N_0}\right)^2}{N_0}\right] du \quad \text{(csak a zajnak)} \qquad u = \frac{n}{\sqrt{N_0}}$$

$\frac{1}{2}$ mert valószínűség

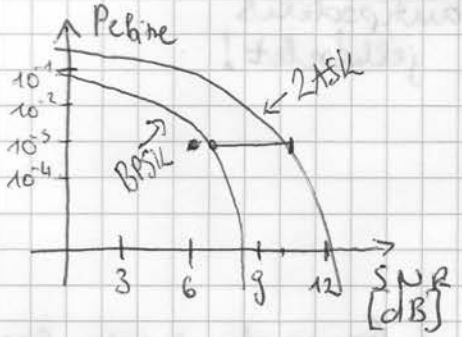
fordított helyettesítéses integrál

$$= \frac{1}{\sqrt{\pi}} \int_{\frac{1}{2}\sqrt{\frac{E}{N_0}}}^{\infty} \left(\sqrt{N_0}\right) \exp(-u^2)\,du$$

az eredményem Pe-hez

$$P_{eb} = \frac{1}{2}\operatorname{erfc}\left[\frac{1}{2}\sqrt{\frac{E}{N_0}}\right] \qquad \bar{E} = \frac{E}{2} \Rightarrow \frac{1}{2}\cdot\operatorname{erfc}\left[\frac{1}{2}\sqrt{\frac{\bar{E}}{N_0}}\right]$$

OOK 2-ASK $\frac{1}{2}$ erfc miatti leosztás



$M = 2$ $\quad s_1(t) = \sqrt{\frac{2E}{T}} \cdot \cos(\omega_c t + \varphi_1)$ $\quad$ 2-PSK moduláció

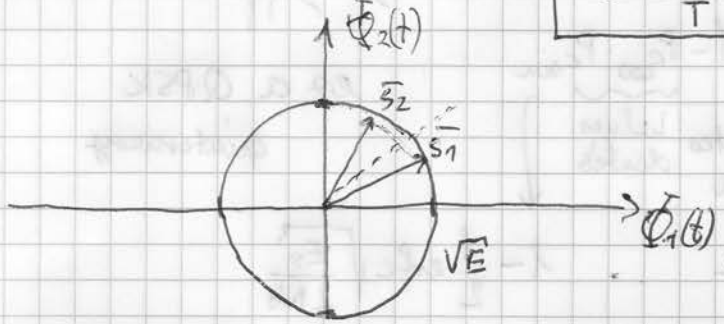
$$s_2(t) = \sqrt{\frac{2E}{T}} \cdot \cos(\omega_c t + \varphi_2)$$

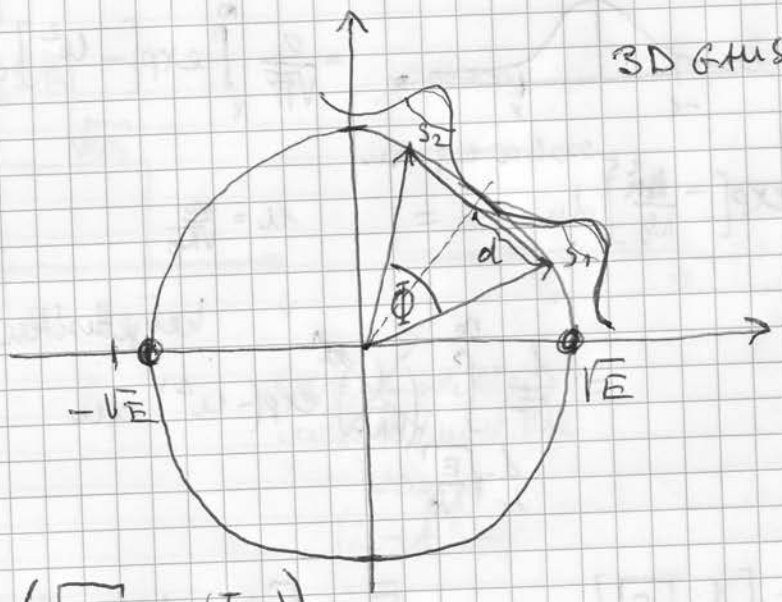
$$\Phi_1(t) = \sqrt{\frac{2}{T}}\cos(\omega_c t)$$

$$\Phi_2(t) = \sqrt{\frac{2}{T}}\sin(\omega_c t)$$

} akkor ortogonálisak, ha $\int_{-\infty}^{\infty} \Phi_1(t)\,\Phi_2(t)\,dt = 0$

$$\Longleftrightarrow \boxed{\omega_c = \frac{2k\pi}{T}}$$





$$P_{PSK} = \frac{1}{2} \cdot \operatorname{erfc}\left(\sqrt{\frac{E}{N_0}} \cdot \sin(\Phi/2)\right)$$

max ↗ $\Phi = 180°$ → BPSK → 1 Dimenziós lett elfajul 1D-ssé

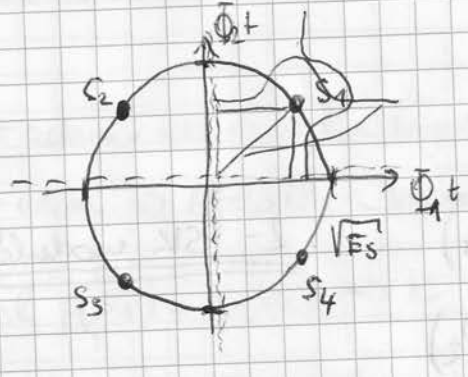
⇓

antipodális jellemzők!

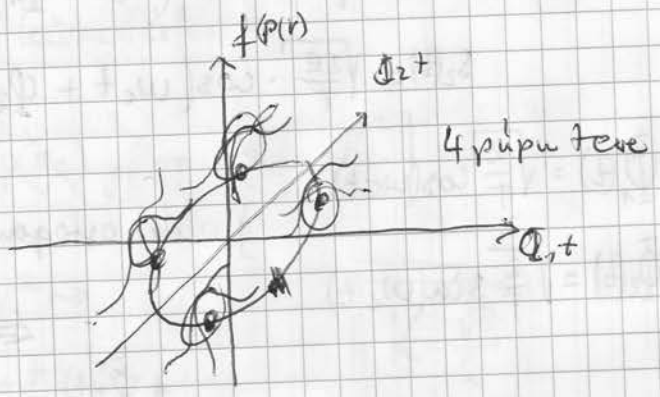
$$P_{BPSK} = \frac{1}{2} \operatorname{erfc}\left[\sqrt{\frac{E_b}{N_0}}\right]$$

$M = 4$ MPSK (4PSK)

$D = 2$



2 Gauss dombocska egy térben



valós / képzetes rész

$\sqrt{E}/\sqrt{2}$

$$P_{e_{QPSK}} = \cancel{1 - (1 - P_c)^2} = 1 - P_{c_{cos}} \cdot P_{c_{sin}}$$

↓ valós/képzetes részekben helyesen döntök; $P_{c_{cos}}$ helyes döntés

$$1 - \frac{1}{2} \operatorname{erfc} \sqrt{\frac{E_s}{2N_0}}$$

ez a QPSK quaternary

$$P_{err,QPSK} = \operatorname{erfc}\sqrt{\frac{E_b}{N_0}} - \frac{1}{4}\operatorname{erfc}^2\sqrt{\frac{E_b}{N_0}}$$

+ Gray kód $\Rightarrow$ szomszédok $\rightarrow$ jelhiba