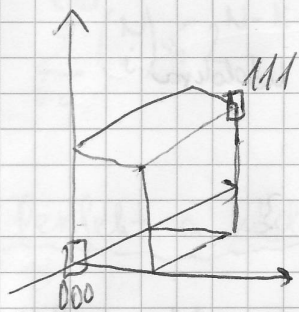


ha növeltem $\frac{k}{N} \rightarrow$ $00 \rightarrow 000$ ismétléses kódolással
 $11 \rightarrow 111$



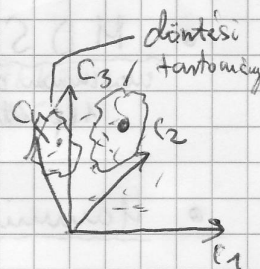
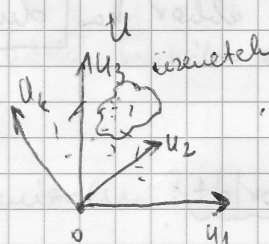
Algebrai konstrukciók: ... következő oldal!

98. előadás

Kezelhető hibák az átvitelben!

$$\bar{u} = \begin{bmatrix} u_1 & \dots & u_k \end{bmatrix} \quad \bar{c} = \begin{bmatrix} c_1 & \dots & c_n \end{bmatrix}$$

q^k q^N



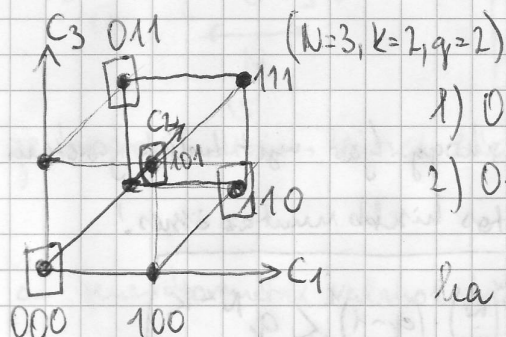
$t_{\text{jelezhető}} < d_{\min}$ (diszkrét helyezés miatt); $t_{\text{jelezhető}} = d_{\min} - 1$
 [döntési tartományok]

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

hibák száma

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

↓
 demodulátor
 nem akar dönteni inkább újra bizi majd
 mert nem biztos benne mert tudom, hogy hal volt
 a hiba!



- 1) 000 hozzá közelítet nem várakozom
- 2) 011, 101, 110, és kész!

ha 110 elrontott #10 (törölhető hiba)

de tudom h. csak 110 lehet

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

Kódkonstrukciós törvények:

- Singleton korlát (N, K, q) paraméterű kódokra
adott $d_{\min}$ esetén

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

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

(vagyis $d_{\min} \leq 1 + N - K$ mindig teljesíthető)

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

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

Hány érvényes kódvektor lehet?

- MDS
maximum distance
separation

ahor ha $d_{\min} = 1 + N - K$

- Hamming korlát:

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

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

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

$$t_{\text{jav}} \text{ esetén } 1 + \binom{N}{1}(q-1) + \binom{N}{2}(q-1)^2 + \dots + \binom{N}{t_{\text{jav}}}(q-1)^{t_{\text{jav}}}$$

1 érvényes kód
 $q-1$ rossz kód

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

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

üzenetek száma

ezt kell, hogy t_{jav} -nyit tudjak javítani!
- és ez biztos kisebb mint az összes!

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

$q=2$ esetén:

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

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

(a tér minden pontját felkaphatjuk!)

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

000 és 111 $\rightarrow$ 1 hibét tudunk javítani!

Hamming 1 döntési távolságra $\rightarrow$ minden kódhoz használható $\Rightarrow$ PERFEKT és MDS

ez jó, de hogyan lehetne algoritmizálni?

Algebrai kódkonstrukció:

- lineáris tér: műveletelvező
- kódok altérként alkotnak (lineáris altér)
- lin. független
- bázis: üzenetvektorokból súlyozott összege a bázisvektorok $\rightarrow$ előáll. ez összes kód!
 $\{\bar{c}\}$
- generátor
$$\begin{bmatrix} 0 & 0 & 0 \end{bmatrix} \xrightarrow{u} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \xrightarrow{N} \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \xrightarrow{G}$$

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

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

ha a generátormátrix valahol tartalmazza az egység mátrixot $\frac{1}{2}$, akkor

$$\underline{G}_{\text{szisztematikus}} = \begin{bmatrix} \underline{I} & \underline{P} \end{bmatrix} \xrightarrow{N}$$

szisztematikus a kód!

sorcsere!

$$\underline{G} = \begin{bmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \end{bmatrix} \quad \underline{G}_{\text{minstern}} = \begin{bmatrix} \bar{1} & 0 & \bar{1} \\ 0 & 1 & 1 \end{bmatrix}$$

H paritás ellenőrző matrix

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

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

példá H = [1 1 1]

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

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

$$x = c + e$$

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

2. ZH
anyagára
eddig

10. előadás

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

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

Szisztematikus kód esetén: $\underline{G} = \begin{bmatrix} \underline{I} & \underline{P} \end{bmatrix} \begin{matrix} K \\ N-K \end{matrix}$

$$\underline{V} = \underline{C} + \underline{e}$$

vekt. hiba

$\underline{V}$ értékes-e? igen $\rightarrow \hat{\underline{e}}$

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

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

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

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

$$\underline{e} = [000 \dots 100] \begin{matrix} N \end{matrix}$$

1 hiba van!
ezt szorozom $\underline{H}$ -vel

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

ahol ez kiválaszt egy oszlopot $\underline{H}$ -ban!

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

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

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

$$m = 2 \checkmark$$

$$m = 3$$

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

jóbb kódolás a cél (kisebbségi redundancia)

Kódavány

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

minél nagyobb

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

hányszor van 1

lin. esetben: a hibák hány(1) van.

$N-K$ párok ahol $t_{j\text{ar}} = 1$

eset PERFEKTEK! K lehetne kisebb is de akkor nem perfekt!

lineáris kódok

$$d_{\min} = \min W(c_i)$$

$\forall i$
hibák
 $\underline{C} = \underline{0}$

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

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

↑
ide hell
heljettenitgetin
es lijon N es K

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

→ lijon, de iljon
mines!

bindis Hamming lind:

pelda $(7, 4, 2) \leadsto t_{\text{jar}} = 2$, es perfekt a Hamming kodet
mines!

me leggen H-ben let osowos onlop!

$$\underline{H} = \begin{bmatrix} \text{---} \\ \text{---} \\ \text{---} \\ \text{---} \end{bmatrix}$$

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

ide
osoket
raham anlik megneen voetik I-ben
minology minen somendben.

$$\begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix} \begin{matrix} \uparrow 2^1 \\ \uparrow N-K \\ \uparrow 2^2 \\ \uparrow 2^3 \end{matrix}$$

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

$k \times N$

$$\underline{u} = [1101] \leadsto \underline{c} = [1101100]$$

↑
liha

$$\underline{u} = \underline{c} + \underline{e} \leadsto \underline{s}^T = [101] \leadsto \underline{H}\text{-nak 4. onlop} \leadsto 4. \text{ bit}$$

vanlitt el!
c-ben!

ha uen bindis a kod. $q=3$

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

↑
perfekt
eret
duin ≥ 3 erintt

$$GF(q=p^n)$$

Galois-test
prim rendis

ha $N = k+2$
MDS is!

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

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

$q=3$
 $q=5$

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

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

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

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

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

$$(4, 2, 3) \text{ kód} \quad (4 \bmod 3 = 1)$$

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

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

primitív elem

$$e = [00 \dots e00]$$

nem lineáris!

Súlyozom e -vel a kódértéket

11. előadás

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

minimális felharmadok

$d_{\text{min}} = \text{maximális}$

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

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

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

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

α primitív elem

α hatványozással vizsgálható a testben!

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 = ?

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

MOD 7

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

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

több α is lehet!

nem bináris Hamming kód:

$h_i \rightarrow$ hibakód, $e_i =$ hiba értéke
 $e_i = q-1$ jele = **4**

MDS legyen $\rightarrow N-K=2$

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

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

$$\left[\frac{s^T}{e_i^T} = h_i^T \right] \text{ egyik oszlop}$$

minden oszlop vesztelése $\frac{1}{1}$ kell legyen

hogy bajtunk az értéket

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

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

Kör
Nem kör

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

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

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

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

$\underline{s} = ?$

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

$$\underline{H} = \underline{s}^T = \begin{bmatrix} 3 \\ 0 \end{bmatrix}$$

$\rightarrow$

normáljuk

$$\begin{bmatrix} 1 \\ 0 \end{bmatrix}$$

$\rightarrow$ H-ban

az

5. oszlop értéke

$$3024 \begin{pmatrix} 1 \\ 4 \end{pmatrix} \begin{pmatrix} 3 \\ 0 \end{pmatrix}$$

R-S kódolás: Reed-Solomon kódolás

több hibét is tud javítani

$$U(x) = U_0 + U_1 \cdot x + U_2 \cdot x^2 + \dots + U_{k-1} \cdot x^{k-1}$$

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

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

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

⊕ polinomiális $GF(q)$ felett

$$a(x) + b(x) = c(x) \quad C_i = a_i + b_i \pmod{q}$$

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

⊗ morza's $GF(q)$ felett

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

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

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

÷ osztás $GF(q)$ felett

$$a(x) \text{ és } b(x) \neq 0 \rightarrow q(x), r(x)$$

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

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

R-S leírása:

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

$$① \quad C_1 = u(d^1)$$

$$② \quad C = U \cdot G$$

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

összesen

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

$$\Rightarrow \boxed{N-1 \leq q-2} \quad (\text{mert } q-1 \text{ mert } \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} \text{ 2 sorok megegyeznek})$$

mert $d^{q-1} = 1$

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

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

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

$\xleftarrow{\quad N \quad}$

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

$\uparrow$
B12

MDS elhár a kód!

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

+ Singleton $\text{dimin} \leq N - k + 1$

erősebb! $\Downarrow$
 $\boxed{\text{dimin} = w(\underline{c})}$

12. előadás

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

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

$\xleftarrow{\quad N \quad}$

eset MDS kódok $\rightarrow \text{dimin} = N - k + 1$

$t_{\text{jav}} = \left\lfloor \frac{\text{dimin} - 1}{2} \right\rfloor$

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

paritás szimbólumok száma

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

$\xleftarrow{\quad N \quad}$

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

$\alpha^{q-1} = \text{egység elem}$

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

Peterson - Gorenstein - Zierler algoritmus:

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

hiba pozíció: i, j

hiba értéke: e_i és e_j

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

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

$\leftarrow$ hiba vektor

~~5/12~~

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

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

nem lin. egyenletrendszer.

lokátorpolinom: gyöke h_i és h_j

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

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

$$L_0 = h_i \cdot h_j$$

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

$$h_i \cdot e_i \cdot \underbrace{L(h_i)}_{\substack{\text{0 len} \\ \text{mert gyök} \\ \text{van.}}} = e_i \cdot h_i^3 + L_1 \cdot h_i^2 \cdot e_i + L_0 \cdot h_i \cdot e_i = 0$$

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

$$h_i^2 \cdot e_i \cdot L(h_i) = e_i \cdot h_i^4 + e_i \cdot h_i^3 \cdot L_1 + e_i \cdot h_i^2 \cdot L_0 = 0$$

$$h_j^2 \cdot e_j \cdot L(h_j) = e_j \cdot h_j^4 + L_1 \cdot h_j^3 \cdot e_j + L_0 \cdot h_j^2 \cdot e_j = 0$$

(+)

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

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

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

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

war leeres
Eigenwertrechner!

$$RS(6, 2, 7)$$

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

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

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

$$u = [3 \ 5]$$

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

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

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

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

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

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

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

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

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

$$\boxed{L_0 = 5}$$

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

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

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

$$L_0 = h_j \cdot h_i$$

$$\boxed{h_i = 3}$$

$$\boxed{h_j = 4}$$

másodfokú egyenlethöz

$$\emptyset = -(h_i + h_j) \\ 5 = h_i \cdot h_j$$

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

$$4 = 3e_i + 4e_j$$

$$3 = 2e_i + 2e_j$$

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

$$\text{végén } \underline{H} \text{-ban megmértem} \rightarrow \underline{v} = [166550]$$

$$e = [020030]$$

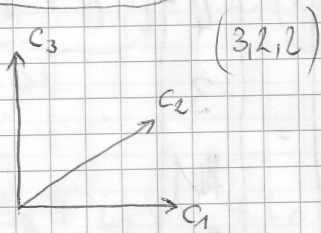
$$\hat{c} = [146520]$$

javítottunk 2 hibát!

13. előadás

Block kódok: ciklikus kód

pl: CRC
"cyclic redundancy check"



Ciklikus kódok: (N, k, q)

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

ahogy érvényes kódok lennének: $[C_{N-1}, C_0, C_1, C_2, \dots, C_{N-2}]$

[Ciklikus eltolja egy kódok szintén kód]

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

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

hogy áll elő: $\underbrace{C_1(x)}_{\substack{\text{ez éppen} \\ \text{a maradék}}} \rightarrow x \cdot C(x) \bmod (x^N - 1)$

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

1 kódból az összes előlelithető

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

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

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

üzenet

$(k-1)$ fokú

$$c(x) = u(x) \cdot g(x) \quad | \cdot h(x) \rightarrow c(x) \cdot h(x) = u(x) \cdot g(x) \cdot h(x) = \underbrace{u(x)}_{\substack{\text{entireben} \\ \text{entireben}}}} \cdot (x^N - 1)$$

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

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

hét
jól

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

ha $v(x) = c_i(x)$ vett érték egyezik az eredménnyel

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

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

$$c(x) = x^k \cdot g(x) - (x^N - 1) C_{N-1}$$

maradék

definiált

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

✓ C.E.D.

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

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

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

$g(x)$ és $h(x)$ osztható

CRC: szisztematikus, ciklikus

$$c(x) = u(x) \cdot x^{N-k} - [u(x) \cdot x^{N-k} \bmod g(x)]$$

maradék $r(x)$ $\rightarrow \deg(r(x)) = N - k - 1$
osztható $g(x)$ -el

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

$\bar{c} = [c_0 \ \dots \ c_{N-k-1} \ c_{N-k} u_0 \ \dots \ c_{N-1} u_{k-1}]$
-dik helyen c_{N-k}

üzenetet felshifteltetve
üzenet van a kódolásban

ez ciklikus és szisztematikus is!

1893

(inverzibilis blokk kód)

Hadamard kód, matrix:

$N \times N$ négyzetes matrixok, $N = 8 \cdot m$, $m \in \mathbb{Z}$, $\epsilon = \pm 1$

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

Kronecker
szorzat

$$H_1 = [1]$$

$$H_2 = \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$$

$$H_3 = \begin{bmatrix} 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 \\ 1 & 1 & -1 & -1 \\ 1 & -1 & -1 & 1 \end{bmatrix}$$

$$H_8 = \begin{bmatrix} \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus \\ \oplus & \ominus & \oplus & \ominus & \oplus & \ominus & \oplus & \ominus \\ \oplus & \oplus & \ominus & \ominus & \oplus & \oplus & \ominus & \ominus \\ \oplus & \ominus & \ominus & \oplus & \oplus & \ominus & \ominus & \oplus \\ \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus \\ \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus \\ \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus \\ \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus & \oplus \end{bmatrix} \begin{matrix} 0000 \\ 0001 \\ 0010 \\ 0011 \\ 0100 \\ 0101 \\ 0110 \\ 0111 \end{matrix}$$

(bármiely 2 sorok)
minden sorai ortogonálisak
 $\bar{z}_i \cdot \bar{z}_j = 0$

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

$$(N, \text{rd}(2N), 2)$$

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

érvegyesek!

$$H_N \cdot H_N^T = N \cdot I$$

hibe detektálás
és javítás

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

ha $v = c_i$

példét: 0101

$$\underline{v} = \begin{bmatrix} + \\ + \\ + \\ - \\ + \\ + \\ + \\ + \end{bmatrix}$$

 $\rightarrow$

$$\begin{bmatrix} 2 \\ -2 \\ 2 \\ -2 \\ 2 \\ 2 \\ 2 \\ -2 \end{bmatrix}$$

konverziót számítottam

felso' H₈-ból 6-dik $\rightarrow 0101$

hiba javítás

$$d_{\min} = \frac{N}{2} = \frac{\text{súly}}{\text{min}} w(c)$$

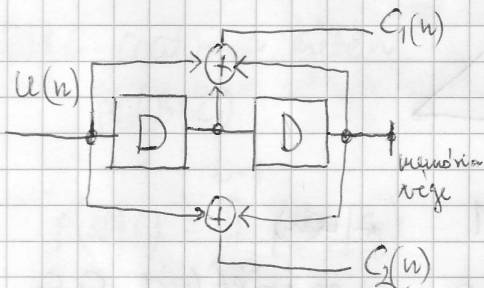
$$t_{j\text{ar}} = \left\lfloor \frac{d_{\text{min}} - 1}{2} \right\rfloor$$

$$N = 4m \rightarrow t_{j\text{ar}} = \left\lfloor \frac{2m-1}{2} \right\rfloor = m-1$$

(V)
15. előadás

Konvolúciós kódoló: memóriával rendelkezik

(n, k, L, q) L : tárolószelvény $\rightarrow$ mennyi ideig tart a kóddolási ablak?
 $q=2$ eset $(2, 1, 3, 2)$ $R_c = 1/2$

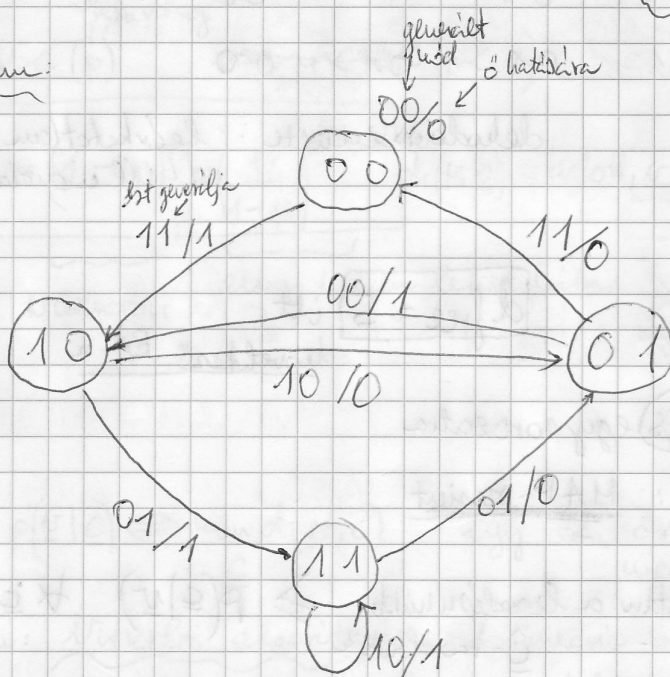


$\rightarrow$ ábrázolhatjuk állapotdiagram-on

$L=3 \rightarrow 3$ tároló van van hirtelen ez elbizonyos?

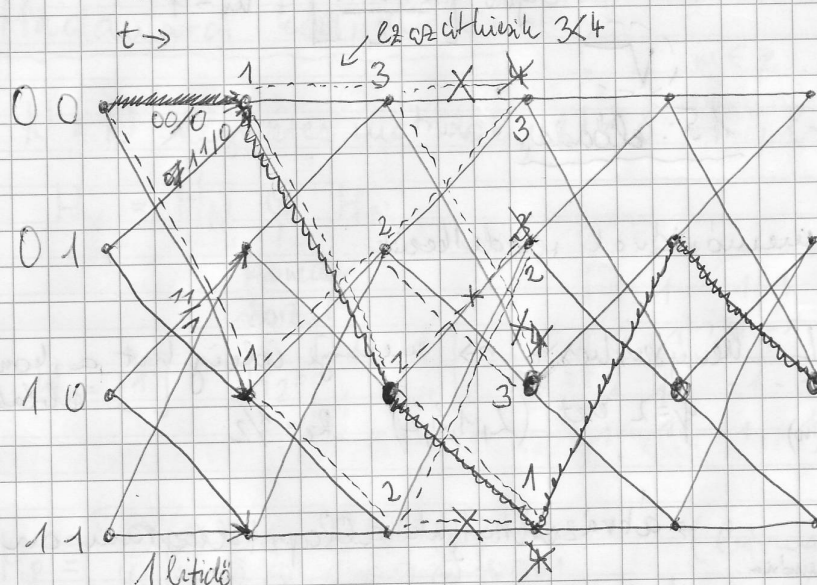
$C_1(n)/C_2(n)$ alátka

Állapot diagram:



Trellis kód diagram

ez nem blokk kód



u	0	1	1	0	1	$\leftarrow u(n)$
C	00	11	01	01	00	$\leftarrow$ generált kód C_1, C_2
$\hat{u}$ hibés	01	11	01	01	00	

hibás
szavak

dekódolás menete: ledékhatalan!
el kell mondani!

MAP döntést hoz
max a posteriori probability

$d_{free} = 5$ itt
következő bit-n

Dekódolás, döntés egy sorozatra

Optimális döntés: MAP-prinzip

$$P(\hat{c} | \underline{v}) \underset{\hat{c} \text{-ra döntés}}{\text{után a legvalószínűbb}} \geq P(c | \underline{v}) \quad \forall c \text{ esetére}$$

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

$$P(\hat{c} | \underline{v}) P(\underline{v}) \geq P(c | \underline{v}) P(\underline{v})$$

$$P(\hat{c} | \underline{v}) \geq P(c | \underline{v})$$

$$P(\underline{v} | \hat{c}) \cdot P(\hat{c}) \geq P(\underline{v} | c) \cdot P(c)$$

$$\hat{c} = \arg \max_c (P(\underline{v} | \hat{c}) \cdot P(\hat{c}))$$

$p(c)$ a priori kód eloszlás! ezt ha nem tudjuk $\rightarrow$ nem lesz optimális

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

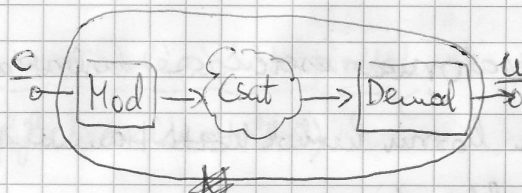
$ML = MAP \Leftrightarrow p(c)$ egyenletes eloszlás (max entropiájú)

$$\hat{c} = \arg \max_c (p(\bar{u} | \bar{c}))$$

DMC csatorma esetén

pl (BSC)

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



N üzenetbit (N hosszú üzenet!)

Spec. eset: BSC (p) ^{hibaválasz} ~~paraméter~~ ($0 < p < 1/2$)

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

N üzenetbit

ennyi helyen lehet hiba

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

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

ML: $\max_c p(\underline{u} | \underline{c}) \Leftrightarrow \min_{\underline{c}} d(\underline{u}, \underline{c})$ egy 2^N összehasonlítás + kéne megtenni

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

2 bit a Trellisen nem tud a hirtérhosszal rövidebb hirtér a/korai.

MLSE döntés

estimation!
sequence

16. előadás

Viterbi dekodó algoritmus: suboptimális döntés
Maximum likelihood döntés
(a-posteriori ismeretek után döntünk)
sorozat kóddal lineárisan
nő

BSC (p) esetén a hibaváltságszám

d_{free} : min. hosszú kódközi Hamming távolságok minimuma
Trellis diagramon
(minél messzebbek az utak)

pl: 000000
 111100
 110 $P_{hibe} \rightarrow P_5 = \binom{5}{3} p^3 (1-p)^2$ 3 hiba van
 $d_{free}=5$

$$P_d = \begin{cases} \text{páratlan} & \sum_{i=0}^d \binom{d}{i} p^i (1-p)^{d-i} \\ \text{páros} & \sum_{i=0}^{d/2} \frac{1}{2} \binom{d}{i} p^{d/2} (1-p)^{d/2} + \sum_{i=d/2+1}^d \binom{d}{i} p^i (1-p)^{d-i} \end{cases}$$

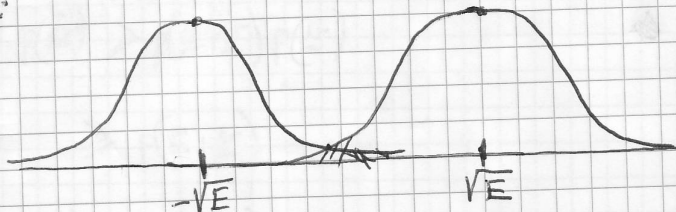
BSC

$$P_e \leq \sum_{d=d_{free}}^{\infty} a_d P_d \quad \left. \begin{array}{l} \downarrow \\ \text{előző} \end{array} \right\} \text{ez javult!}$$

~~kódközi~~ hurok száma
attól Hamming távolsága d

AGWN esetben:

Energia



$$P_e = \frac{1}{2} \text{erfc} \left[\sqrt{\frac{E_b}{N_0}} \right]$$

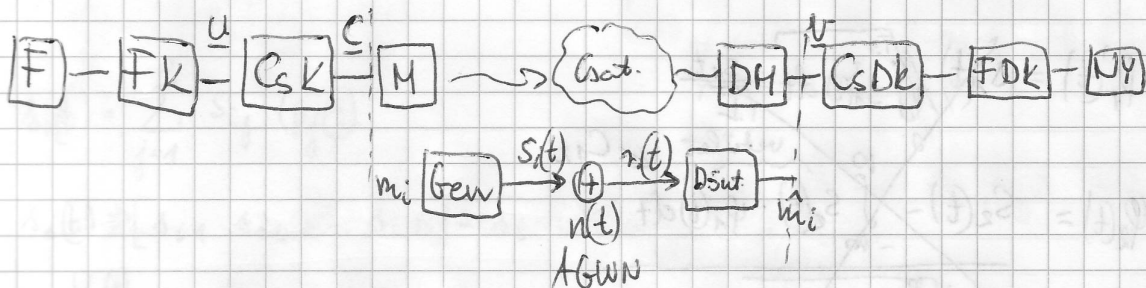
$$P_{\text{ERROR}} = \frac{1}{2} \text{erfc} \left[\sqrt{\frac{E_b}{N_0}} \right]$$

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

R_c - kódolás
 d - futó párhuzos
 E_b - bítenergia
 N_0 - spektr. teljesítmény sűrűség

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

Digitális modulációs eljárások (vízfekvénység átvitel)



$$\begin{aligned}
 &M \{m_i\}^M \\
 &\updownarrow \\
 &S \{s(t)\}^M
 \end{aligned}$$

M véges kell legyen!

véges számú üzenet lehet véges való $\rightarrow$ más hálónak nem tudok dönteni.

véges típusú jelek, véges tartójú jelek, véges energiájú, véges elemű.

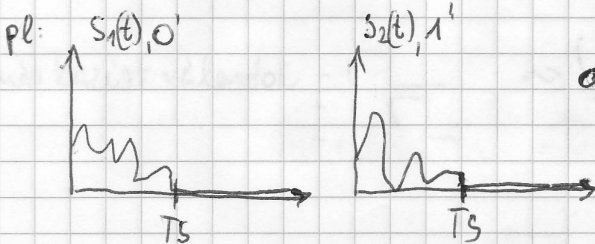
$\forall s_i(t) = 0, \forall [t < 0 \quad t > T_s]$

 véges tartó T_s ideig

$\forall s_i(t)$ más jelalakú

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

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



a döntés a vett jel alapján

optimális ha

$$\text{MAP } p(\hat{s}_i(t) | r(t))$$

max

Feltétel: (Gram-Schmidt ortogonalizációs eljárás)

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

$$\underbrace{\int_{-\infty}^{\infty} \phi_i^2(t) dt = 1}_{\text{alkotunk egy tétel}} \leadsto \int_{-\infty}^{\infty} \phi_i(t) \phi_j(t) dt = \begin{cases} 1 & i=j \\ 0 & i \neq j \end{cases}$$

véges tartományak! ortogonális
rendszerek

neem jelölésben könnyebb, hanem vektorok!

G-S:

$$\begin{aligned} \phi_1'(t) &= s_1(t) / \sqrt{\int_{-\infty}^{\infty} s_1^2(t) dt} = \frac{s_1(t)}{\sqrt{E_1}} \\ \phi_2(t) &= s_2(t) - \underbrace{\int_{-\infty}^{\infty} s_2(t) \cdot \phi_1(t) dt}_{\text{vetület}} \leftarrow C_{12} \\ &\quad \underbrace{\sqrt{\int_{-\infty}^{\infty} s_2^2(t) - C_{12}^2 dt}} \end{aligned}$$

$$\psi_1(t) = s_1(t) / \sqrt{\int_{-\infty}^{\infty} s_1^2(t) dt} = \frac{s_1(t)}{\sqrt{E_1}}$$

$$C_{12} = \int_{-\infty}^{\infty} s_2(t) \cdot \psi_1(t) dt$$

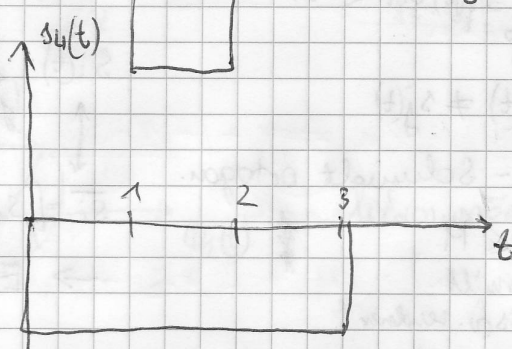
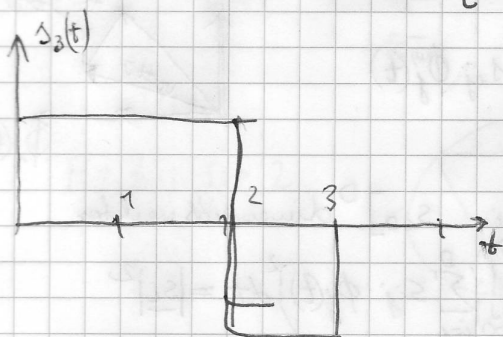
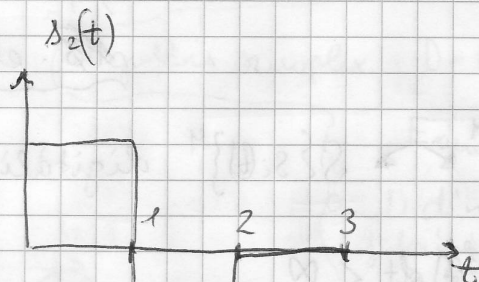
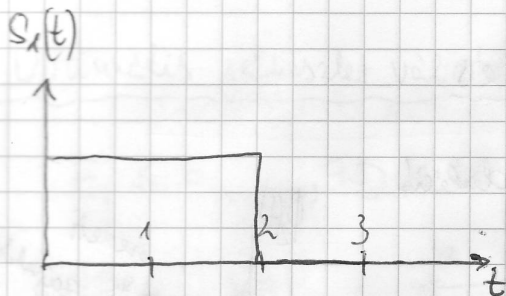
$$\psi_2(t) = \frac{\phi_2'(t)}{\sqrt{\int_{-\infty}^{\infty} \phi_2'^2(t) dt}}$$

$$s_2(t) - C_{12} \cdot \psi_1(t) = \psi_2'(t)$$

$$C_{ij} = \int_{-\infty}^{\infty} s_j(t) \cdot \psi_i(t) dt$$

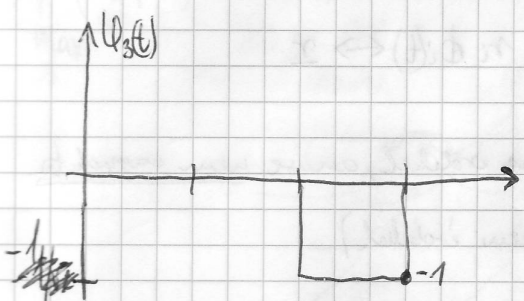
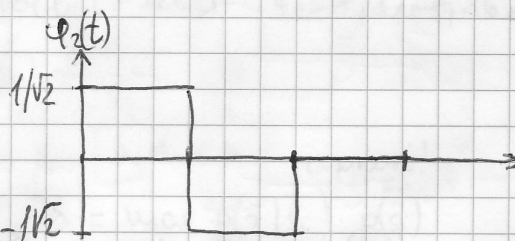
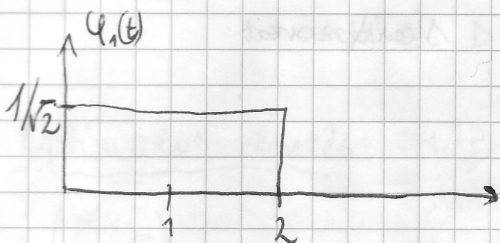
$$\psi_j'(t) = s_j(t) - \sum_{k=1}^{j-1} C_{kj} \cdot \psi_k(t)$$

$$\Rightarrow \psi_j(t) = \frac{\psi_j'(t)}{\sqrt{\int_{-\infty}^{\infty} \psi_j'^2(t) dt}}$$



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

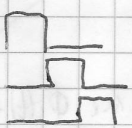
$$s_i(t) \Rightarrow [s_{i1} \ s_{i2} \ \dots \ s_{iD}] = \bar{s}_i$$



3 dimenziós tér

$$\varphi_4(t) = \emptyset \text{ nem fellel}$$

előbb más bázist választok -



$\leadsto$ 3 vektorokkal számolhatok

17
18. előadás

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

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

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

Gram-Schmidt ortogon.

$D \leq M$
ortonormált
bázisf. vektor!

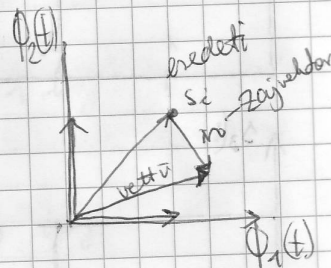
$\{\phi_i(t)\}^D \rightarrow D$ dimenziós vektor!

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

$$\underline{s}_i = [s_{i1} \ s_{i2} \ \dots \ s_{iD}]^D \text{ dimenziós vektor.}$$

$$\rightarrow E_i = \int_{-\infty}^{\infty} \left(\sum_{j=1}^D s_{ij} \phi_j(t) \right)^2 dt = |\underline{s}_i|^2$$

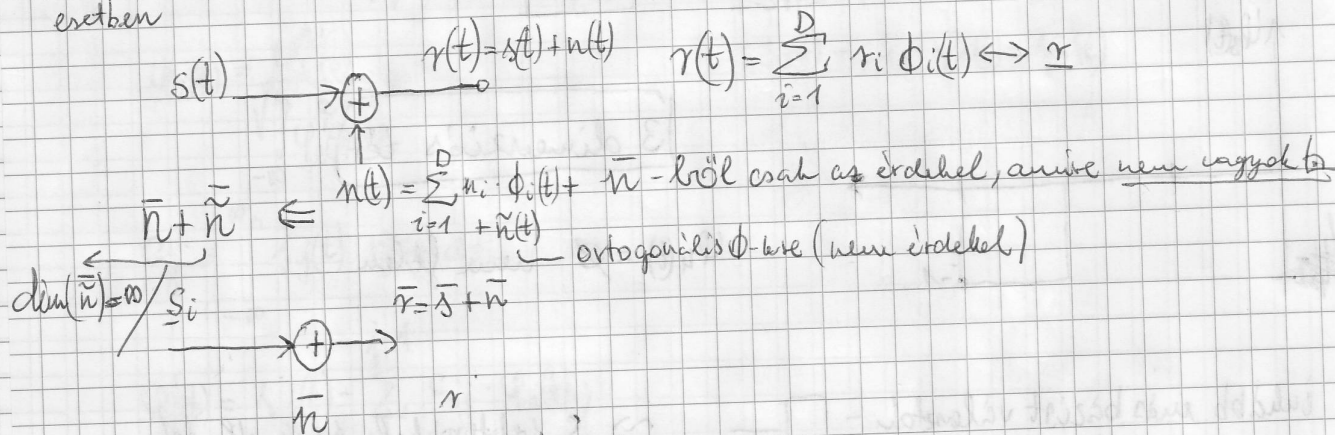
(Pitágorasz)



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

skalárszorzat

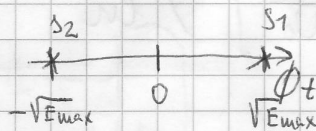
AGWN:
erősen



Optimális jelészlet választás : reguláris simplex $D = M - 1$

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

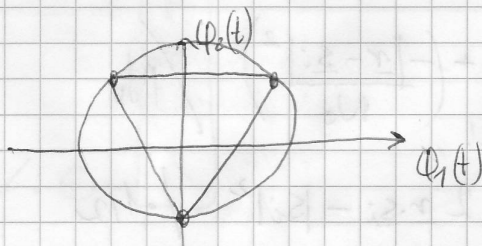
$$M=2 \quad D=1$$



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

a D dim. gömb felsínei vannak!
 $\bar{s}_i \cdot \bar{s}_j = -\frac{E_{\max}}{D}$

$$M=3; D=2$$



háromszög

$$M=4; D=3$$

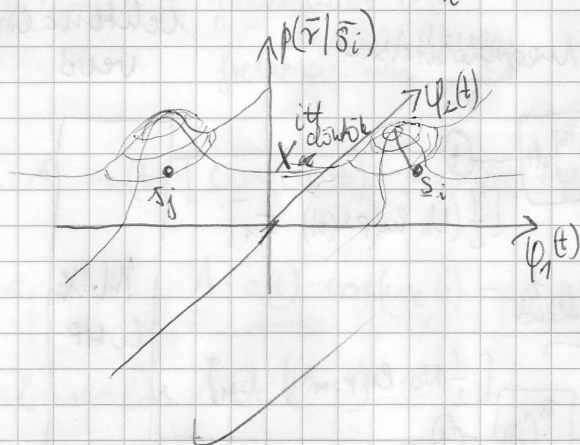
tetraéder

Növeljük a dimenziószámot $\rightarrow$ nagyobb szórókéesség.
 inkább suboptimális megoldás

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

Optimális döntés: MAP

$$\max_i p(\bar{s}_i | \bar{r}) \quad \text{max a posteriori valószínűség} \rightarrow = \max_i p(\bar{r} | \bar{s}_i) \cdot p(\bar{s}_i) \quad \text{a priori!}$$



AGWN esetben

D -dim Gauss-eloszlást követ

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

$\sigma_n^2 = N_0/2 \quad \text{nem } \sqrt{(2N_0)^{D/2}}$

döntési térben kell egy D dim. tartomány minden vektorhoz!

(így jobb len!)

hiba valószínűség:

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

$$P_{\text{correct}_i} = \int_{U_i^D} p(\bar{s}_i | \bar{r}) d\bar{r} = \int_{U_i^D} p(\bar{s}_i) \cdot p(\bar{r} | \bar{s}_i) d\bar{r}$$

U_i^D
 D -dim. integrál

nem kell szimmetikus legyen feltekintve a 2 felület

ha nincs ISI, A GWN akkor az optimális döntőképző:

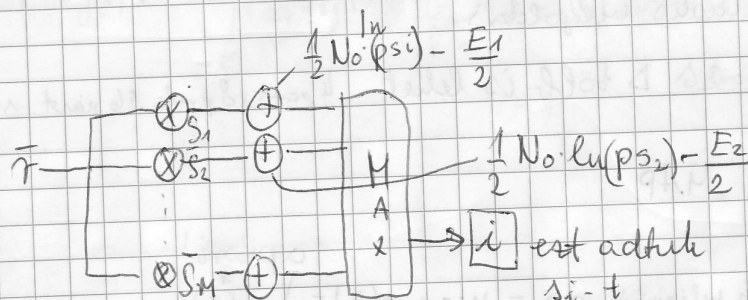
$$\max_{\substack{\text{apriori} \\ s_i}} p(s_i) \cdot \frac{1}{\sqrt{\pi} \cdot N_0} \cdot \exp \left[-\frac{\overset{(r-s_i)}{\downarrow} |r-s_i|^2}{N_0} \right] \quad \text{MAP} \quad \text{---} / \ln$$

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

$$N_0 \cdot \ln p(s_i) - \underbrace{|r|^2}_{\text{fktlen i-től}} + 2 r \cdot s_i - |s_i|^2 \quad \text{---} / \cdot 1/2$$

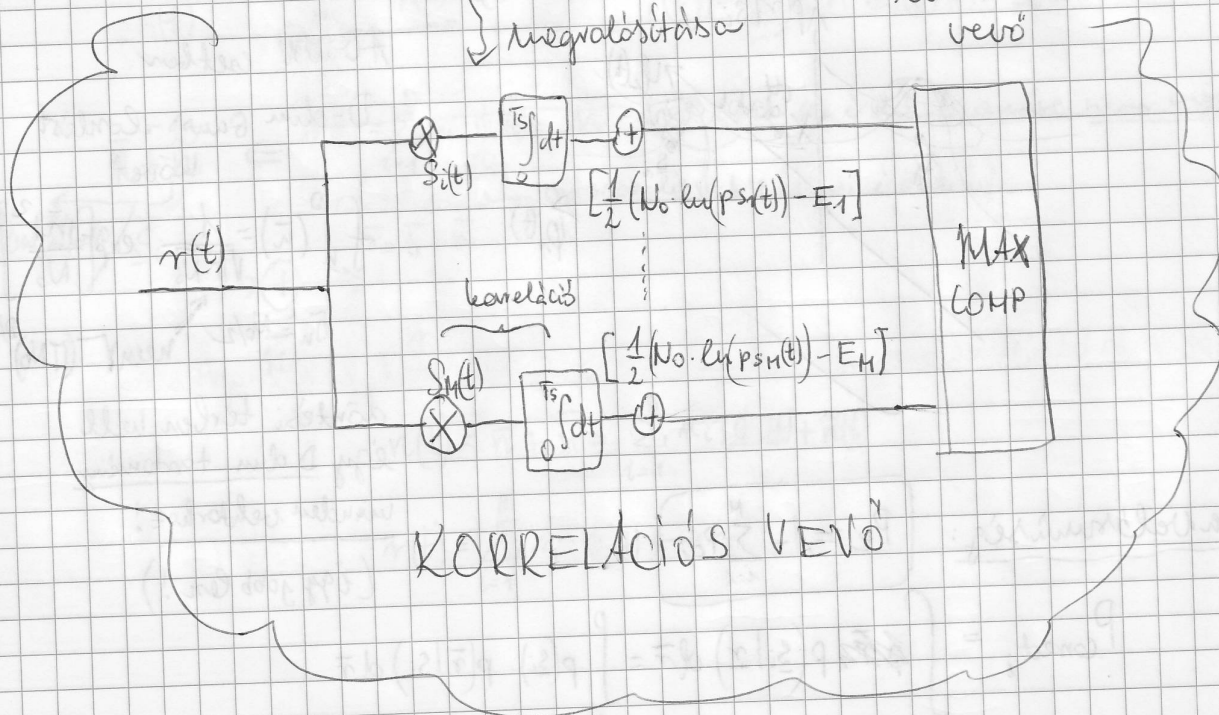
$$\frac{1}{2} \cdot N_0 \cdot \ln p(s_i) + \underbrace{r s_i - \frac{|s_i|^2}{2}}_{\text{korreláció}} \quad \text{energia}$$

így:

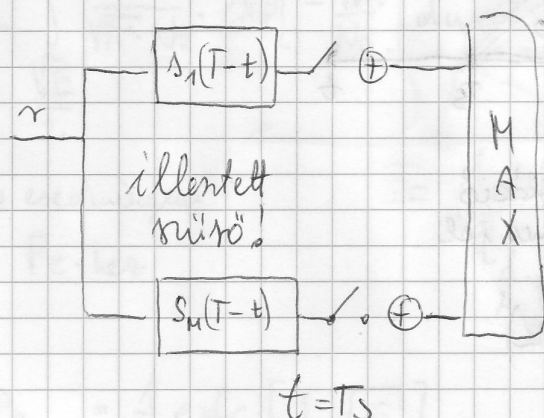


Integrálás

opt. relatióvalis vevő



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



18. előadás

Vivőfrekvenciás átvitel

$$r(t) = \sqrt{2} \cdot A \cdot \cos(\omega_c t + \phi)$$

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

amplitúdó moduláció $m(t)$

mög mod. $\vartheta(t) \rightarrow$ fázis mod $\vartheta(t)$

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

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

kvadratura alah: $A \cdot a(t) \cdot \cos(\omega_c t) - A \cdot q(t) \cdot \sin(\omega_c t)$

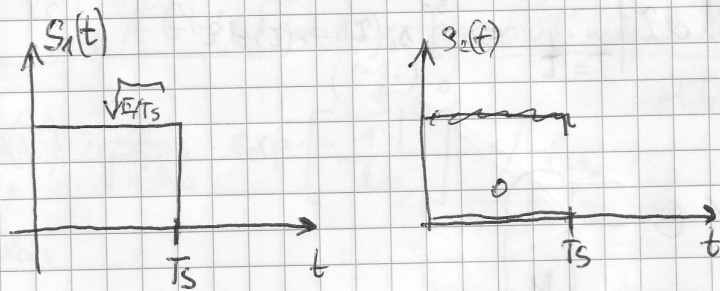
komplex burkolás leírás

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

komplex
burkolás

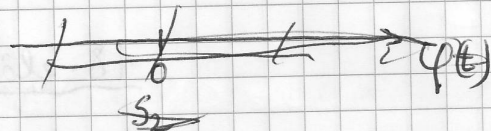
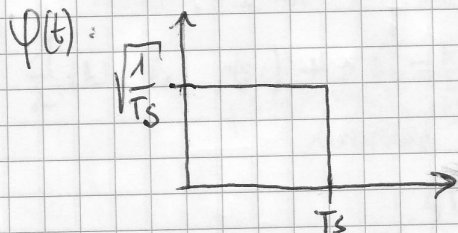
$$M, D = M - 1$$

$$M = 2$$

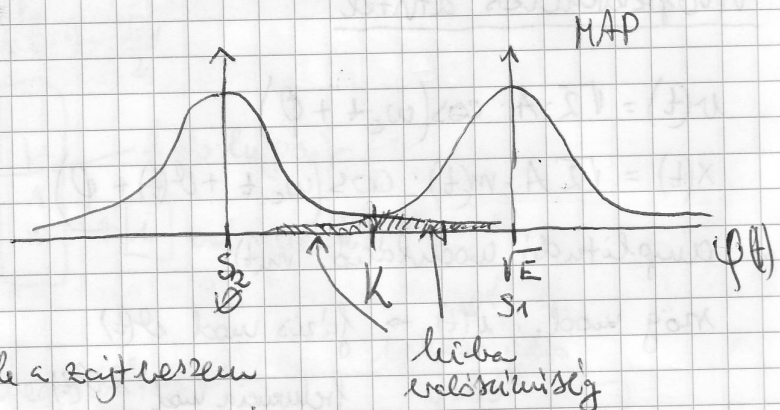


OOK moduláció
vagy jel / nincs jel
vagy
(2-ASK)

Gram-Schmidt ortogonalizáció:



AGWN csatorna
korrelációs bevé



s_2 -t adom $\Rightarrow 0 \rightarrow$ csak a zaj bevé

s_1 -t adom $\Rightarrow$ kiderül a várható érték

ahol $p(s_1) = p(s_2) \rightarrow K$ küszöbérték

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

$$p(s_1) = p(s_2)$$

feltessük
a max entropiát

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

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

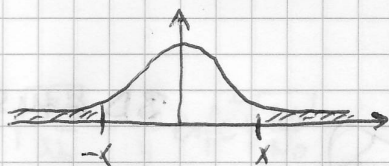
$$2Ks_1 = s_1^2$$

$$K = \frac{s_1}{2}$$

$$\rightarrow \frac{\sqrt{E}}{2}$$

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

$$\operatorname{erfc}(x) =$$



$$= \frac{2}{\sqrt{\pi}} \int_x^{\infty} \exp[-u^2] du$$

$\frac{1}{2} \cdot \frac{2}{\sqrt{\pi}} \int_{\frac{\sqrt{E}}{2}}^{\infty} \frac{1}{\sqrt{\pi} \cdot N_0} \cdot \exp\left[-\frac{u^2}{N_0}\right] du$

az eredményem
 Pe-hez

$$u = \frac{n}{\sqrt{N_0}}$$

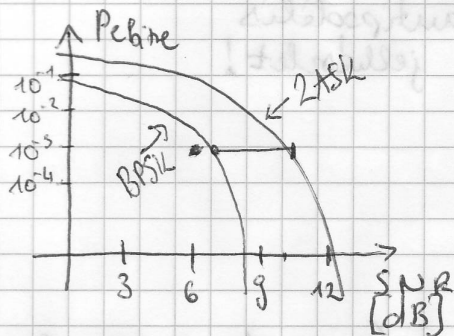
helyettesítéses integrál

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

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

OKK
 2-ASK
 erfc
 miatti
 leontais

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



$$M=2 \quad s_1(t) = \sqrt{\frac{2E}{T}} \cdot \cos(\omega_c t + \phi_1)$$

2-PSK moduláció

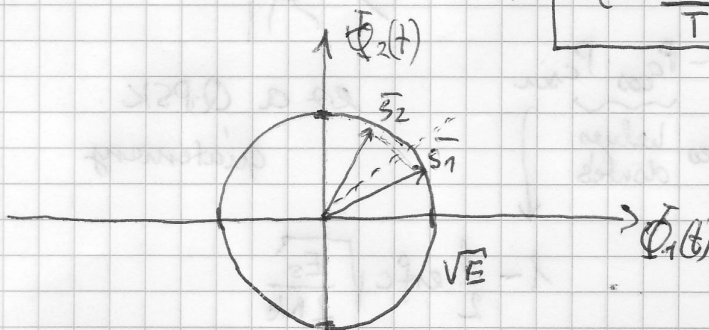
$$s_2(t) = \sqrt{\frac{2E}{T}} \cdot \cos(\omega_c t + \phi_2)$$

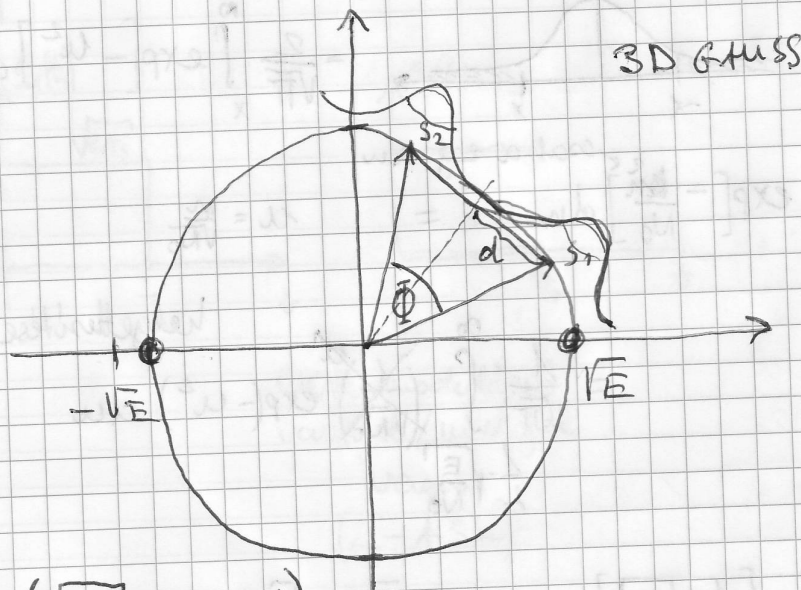
$$\Phi_1(t) = \sqrt{\frac{2}{T}} \cos(\omega_c t)$$

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

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

$$\Leftrightarrow \omega_c = \frac{2k\pi}{T}$$





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

PSK

max $\Phi = 180^\circ \rightarrow$ BPSK $\rightarrow$ 1Dimesziós lett
elfajul 1D-sse!

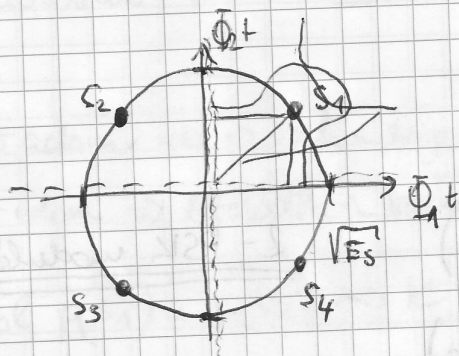
$$P = \frac{1}{2} \text{erfc} \left[\sqrt{\frac{E_b}{N_0}} \right]$$

BPSK

$\Downarrow$
antipodális
jelhalmaz!

$M=4$ MPSK (4PSK)

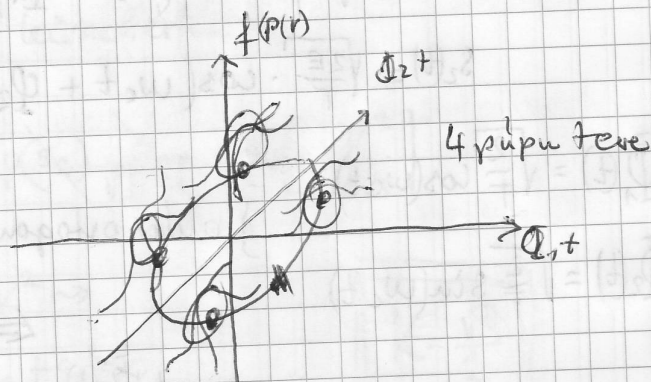
$D=2$



valós / képzetes rész

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

2 Gauss eloszlású lesz
terben



ez a Q-PSK
quaternary

$$P_e = 1 - (1 - P_c)^2 = 1 - P_{c \cos} \cdot P_{c \sin}$$

QPSK

$\downarrow$
valós / képzetes
részekben
helyesen
döntök

$\downarrow$
helyes
döntés

$$1 - \frac{1}{2} \text{erfc} \left[\sqrt{\frac{E_s}{2N_0}} \right]$$

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

QPSK

+ Gray kod überlappung → Fehler