

levendor @ hit.bme.hu

fogadóra : csüt 16⁰⁰-

12k + pz
↳ dec 4. csüt 8⁰⁰-10⁰⁰

Györfi, Györi, Vajda: Információ- és Kódelmélet
elegendő az e.a. anyag.

- spektrális hatékonyság: bit/sec/Hz

gyár: 0,48

elm: 5,2

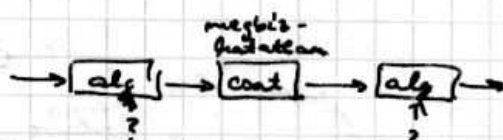
● Hibajavító kódolás: hogyan lehet egy megbízhatatlan csatornában megbízhatóan kommunikálni?

csatorna:

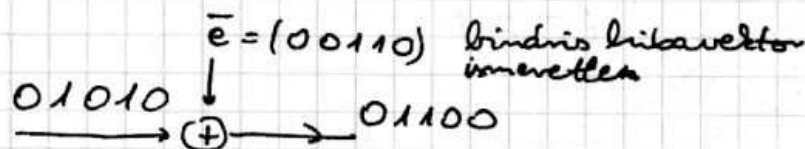
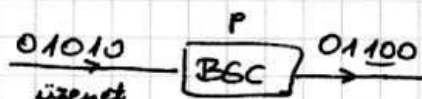
BSC
(binary
symmetric
channel) a 2 puggara:

$\begin{cases} 0 \xrightarrow{p} 1 \\ 1 \xrightarrow{p} 0 \end{cases}$

$p = 0,3$: 1000 db 0-ből 300 db 1-es



$0 \leq p \leq 0,5$ különben invertálenduk értelmes néző



$$p(\bar{e}) = 0,3^2 \cdot 0,7^3$$

$$p = 0,3$$

$$1-p = 0,7$$

súly: egyesek száma az adott vektorban, w

$$w(\bar{e}) = 2$$

$$p(\bar{e}) = p^{w(\bar{e})} \cdot (1-p)^{n-w(\bar{e})}$$

$$p(\bar{e}) = \left(\frac{p}{1-p}\right)^{w(\bar{e})} \cdot (1-p)^n$$

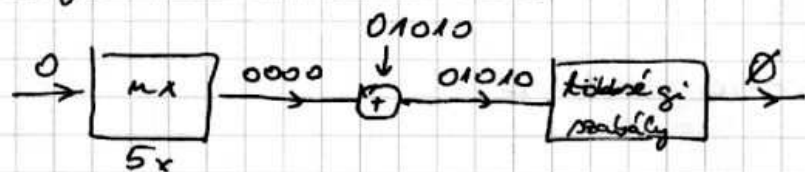
$$\frac{p}{1-p} < 1$$

Mivel kisebb a súly egy hibavektorban $w(\bar{e})$, annál valószínűbb

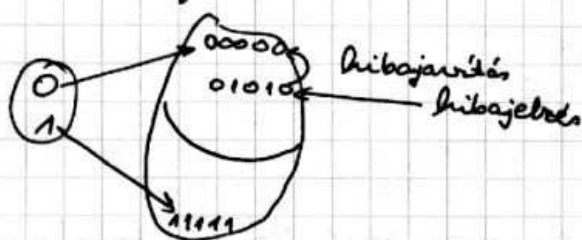
$$P_{\text{correct}} = (1-p)^n \xrightarrow{\text{most}} 0, \neq 5 \text{ nagyon kicsi}$$

megbízható kommunikáció: helyes ábrítel valószínűsége

Hibajavító kódolás ismertetése



Geometria: integráció



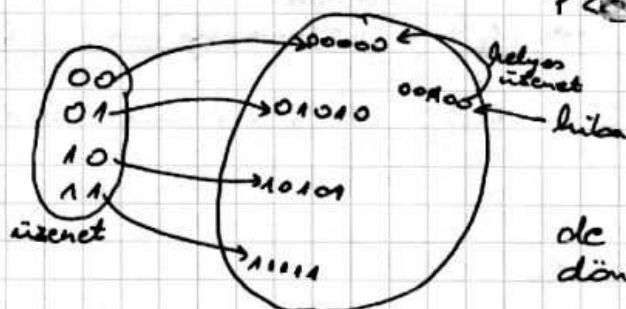
$$P_{\text{hiba}} = \sum_{i=1}^n \binom{n}{i} p^i (1-p)^{n-i}$$

adatátviteli seb. növelés

$$\text{ha } n \rightarrow \infty \Rightarrow P \rightarrow 0$$

$$P < 10^{-3} \text{ - hoz is van } n$$

Általánosítás

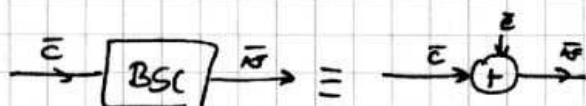


de lehet, hogy nem tudunk dönteni.

Kód teljesíthetősége

Hibajelzés: $d_{\min} - 1$

$$d_{\min} : \min_{\substack{\bar{c}, \bar{c}' \in C \\ \bar{c} \neq \bar{c}'}} d(\bar{c}, \bar{c}')$$



$$d(\bar{r}, \bar{c}) < d(\bar{r}, \bar{c}')$$

$$d(\bar{c}, \bar{c}') \leq d(\bar{r}, \bar{c}') + d(\bar{r}, \bar{c})$$

$$d(\bar{r}, \bar{c}') \geq d(\bar{c}, \bar{c}') - d(\bar{r}, \bar{c})$$

$$d(\bar{r}, \bar{c}) \leq d(\bar{c}, \bar{c}') - d(\bar{r}, \bar{c})$$

$$2 d(\bar{r}, \bar{c}) \leq d_{\min}$$

Opt. kód $\rightarrow \max d_{\min}$

$$\text{Hibajavítás: } \left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor$$

jelölések és definíciók

- $\bar{a} = (a_1, \dots, a_n) \leftarrow$ sorvektor
 $\bar{a}^T = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \leftarrow$ oszlopvektor

üzenet: $\bar{u} = (u_1, \dots, u_k) \in \{0, \dots, q\}^k \rightarrow$ redundanciája 2^k

$$\dim(\bar{u}) = k$$

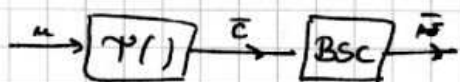
Kódstruktúra: $C = \{\bar{c}^{(1)}, \bar{c}^{(2)}, \dots, \bar{c}^{(n)}\}, M = 2^k$

$$\dim(\bar{c}^{(n)}) = n > k$$

- $C(n, k)$

redundancia: $n - k, \frac{k}{n}$

Kódolás: $\gamma: \{0, 1\}^k \rightarrow C; \gamma(\bar{u}) = \bar{c}$ egyértelmű és megfordítható f.



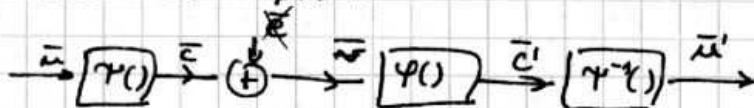
Nett vektor, $\bar{r} \in \{0, 1\}^n$

$$C \subset \{0, 1\}^n$$

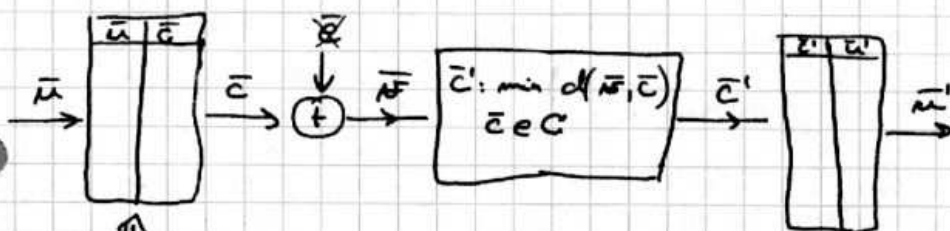
- Dekódálás: $\varphi: \{0, 1\}^n \rightarrow C, \varphi(\bar{r}) = \bar{c}$

Dekódolás: $\gamma^{-1}: C \rightarrow \{0, 1\}^k, \gamma^{-1}(\bar{c}) = \bar{u}$

Kommunikációs alapséma:



Implementáció



$\times d_{\min}$
hibajelzés
hibajavítás OK

$$n - k < \alpha$$

$C(5,2) : \mathcal{O}\left(\binom{2^5}{2^2} \binom{2^2}{2}\right)$ lami nismatensis : off-line

$$\mathcal{O} = \binom{2^m}{2^k} \binom{2^k}{2}$$

On-line karmatensis : $3 \cdot \mathcal{O}(2^k)$

Probléma:

Off-line probléma: $\frac{2^m!}{(2^m-2^k)! \cdot 2^k!} \cdot \frac{2^k}{(2^k-2)! \cdot 2!}$ táblázatban kereséssel kell az idő

On-line probléma: $3 \cdot 2^k$ lassú az adatátvitel is.

Nem REAL-TIME!!!

Optimális kód $\rightarrow$ Szisztematikus kód: $\bar{C} = (\underbrace{u_1, \dots, u_k}_{\text{üzenetösszeg}}, \underbrace{p_1, \dots, p_{n-k}}_{\text{paritásjegyek}})$
ahol $d_{\min} \leq m - k + 1$

ahol $d_{\min} = m - k + 1$

MDS-kód (Maximum Distance Separable)

CÉL: Real-time MDS kódok fejlesztése!!!

↓
algoritmus
komplexitás

↓
teljesítő
képeség

Lineáris, bináris kódok

$$G = \{\bar{g}^{(1)}, \bar{g}^{(2)}, \dots, \bar{g}^{(k)}\}$$

$$\dim(\bar{g}^{(i)}) = m \quad \forall i = 1, \dots, k$$

$$C = \mathcal{L}_C\{G\} \rightarrow \bar{C} = \sum_{i=1}^k u_i \cdot \bar{g}^{(i)} \Rightarrow \bar{C}, \bar{C}' \in C \Rightarrow \bar{C} + \bar{C}' \in C, \bar{0} \in C$$

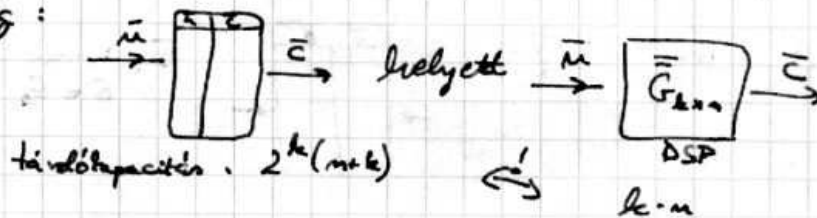
Generátormátrix:

$$\bar{G}_{k \times m} = \left(\begin{array}{c} \bar{g}^{(1)} \\ \bar{g}^{(2)} \\ \vdots \\ \bar{g}^{(k)} \end{array} \right) \quad \left. \vphantom{\begin{array}{c} \bar{g}^{(1)} \\ \bar{g}^{(2)} \\ \vdots \\ \bar{g}^{(k)} \end{array}} \right\} k$$

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

$$\underbrace{(\dots \bar{C} \dots)}_m = (\dots \bar{u} \dots) \left(\begin{array}{c} \bar{g}^{(1)} \\ \vdots \\ \bar{g}^{(k)} \end{array} \right)$$

Technológiai jelentőség:



(B2)

szisztematikus

 $C(5,2)$

$$\overline{G} = \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$(0 \ 0) \cdot \begin{pmatrix} 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 \end{pmatrix}$$

$$(0 \ 1)$$

$$\overline{c}^{(1)} = (00000)$$

$$\overline{c}^{(2)} = (01101)$$

$$\overline{c}^{(3)} = (10010)$$

$$\overline{c}^{(4)} = (11011)$$

Szisztematikus kódolás:

$$\overline{G}_{k \times n} = \left(\overline{I}_{k \times k} \quad \overline{B}_{k \times (n-k)} \right)$$

Paritásellenőrző mtr:

$$\overline{H}_{(n-k) \times n}: \overline{H} \cdot \overline{c}^T = \overline{0}^T \rightarrow \overline{H} (\overline{u} \cdot \overline{G})^T = \overline{0}^T \quad \forall \overline{u}$$

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

Szisztematikus kódok:

$$\overline{H}_{(n-k) \times n} = \left(\overline{A}_{(n-k) \times k}, \overline{I}_{(n-k) \times (n-k)} \right)$$

$$\left(\overline{A}_{(n-k) \times k}, \overline{I}_{(n-k) \times (n-k)} \right) \cdot \begin{pmatrix} \overline{I}_{k \times k} \\ \overline{B}_{(n-k) \times k}^T \end{pmatrix} = \overline{0} \Rightarrow \overline{A}_{(n-k) \times k} + \overline{B}_{(n-k) \times k}^T = \overline{0}$$

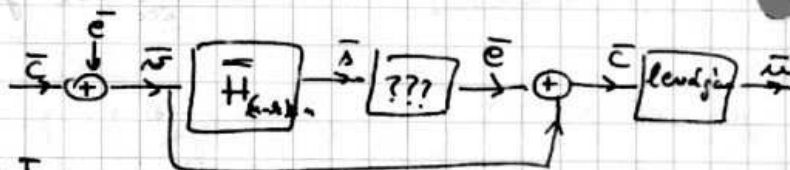
$$\boxed{\overline{A} = -\overline{B}^T}$$

↑
a 0 nem is kell a mod 2 műve

$$\overline{H}_{3 \times 5} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \end{pmatrix}$$

$\overline{A}_{3 \times 2} \quad \overline{I}_{3 \times 3}$

A paritásellenőrző mtr jelentősége:

Szindrómavektor: $\overline{H} \cdot \overline{u}^T = \overline{\delta}^T$

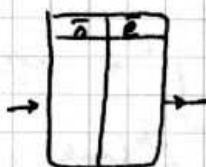
$$\overline{u} = \overline{c} + \overline{e} \rightarrow \overline{H} \cdot \overline{u}^T = \overline{H} \cdot (\overline{c} + \overline{e})^T = \overline{H} \cdot \overline{c}^T + \overline{H} \cdot \overline{e}^T = \overline{H} \cdot \overline{e}^T = \overline{\delta}^T$$

hiszen művelet

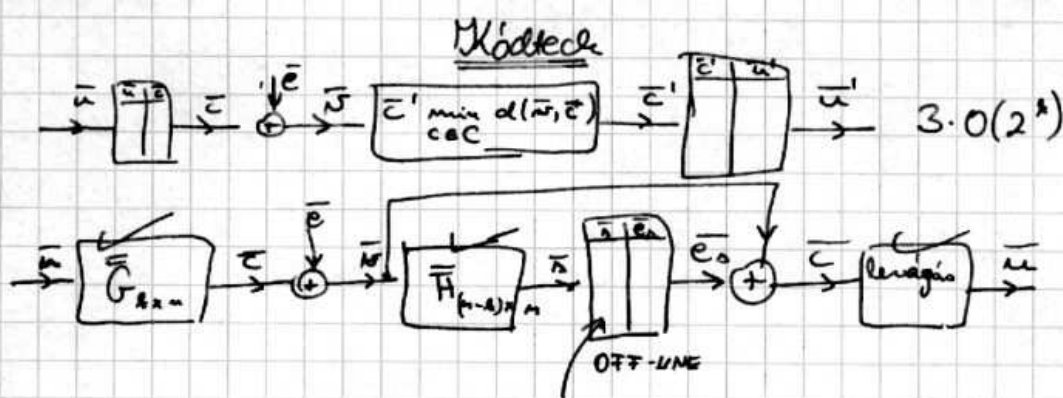
$$\text{is az} \rightarrow \boxed{\overline{H} \cdot \overline{e}^T = \overline{\delta}^T}$$

hiszen művelet

$$E_n = \{ \overline{e} : \overline{H} \overline{e}^T = \overline{n}^T \}$$



$\overline{e}_n : \min_{\overline{e} \in E_n} w(\overline{e})$, a legvalószínűbb hibát kevesen meg, azaz minimális



"utdne permonáln
diszkréion
folytatódjút".

$$O(2^{n-2}) \ll 3 \cdot O(2^k)$$

mindenféle elhárítási táblázat

P2

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

$C(5,3)$, rendszeres

$$E_s = \{ \bar{e} : \bar{H} \cdot \bar{e}^T = \bar{\Delta}^T \}$$

$$\dim(\bar{\Delta}) = 2$$

$$\bar{\Delta} = (1, 1)$$

$$\bar{H}_{2 \times 5} = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

$$\bar{e}, \bar{e}' : \begin{aligned} \bar{H} \cdot \bar{e}^T &= \bar{\Delta}^T \\ \bar{H} \cdot \bar{e}'^T &= \bar{\Delta}^T \end{aligned}$$

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

$$\bar{H} \cdot \bar{e}'^T = \bar{H} \cdot \bar{e}^T + \bar{H} \cdot c^T = \bar{H} \cdot \bar{e}^T = \bar{\Delta}^T$$

$$E_s = \{ (00100); (00011); \dots \}$$

ezt fogjuk a táblázatba beírni

$$\bar{c}^{(1)} = (00000)$$

$$\bar{c}^{(5)} = (10001)$$

$$\bar{c}^{(2)} = (00111)$$

$$\bar{c}^{(6)} = (10110)$$

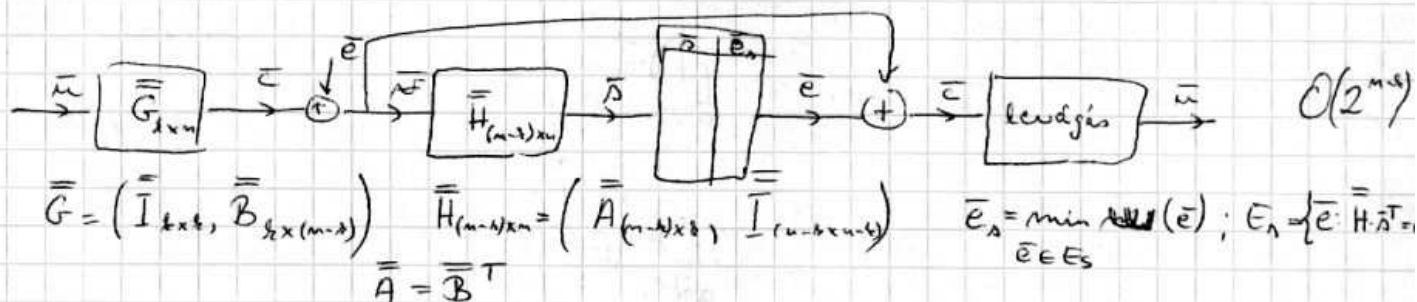
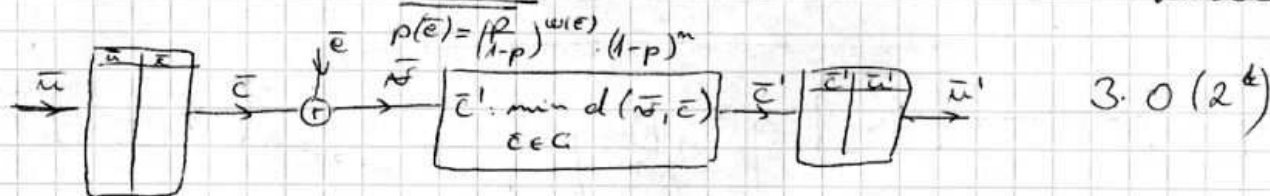
$$\bar{c}^{(3)} = (01010)$$

$$\bar{c}^{(7)} = (11011)$$

$$\bar{c}^{(4)} = (01101)$$

$$\bar{c}^{(8)} = (11100)$$

Kódok



Bináris lineáris kód $d_{\min}$ -je?

$$d(\bar{a}; \bar{b}) = w(\bar{a} + \bar{b})$$

$$\begin{array}{r} 010010 \\ 001011 \\ \hline 011001 \end{array}$$

$$d_{\min} = \min_{\substack{\bar{c}, \bar{c}' \in C \\ \bar{c} \neq \bar{c}'}} d(\bar{c}, \bar{c}') = \min_{\substack{\bar{c}, \bar{c}' \in C \\ \bar{c} \neq \bar{c}'}} w(\bar{c} + \bar{c}') = \min_{\substack{\bar{c}'' \in C \\ \bar{c}'' \neq \bar{0}}} w(\bar{c}'') \rightarrow O(2^k)$$

$$\binom{2^k}{2} \rightarrow \sim 2^{2k}$$

$\forall$ 1 hibát javító (Hamming) kódok

$$\bar{c} + \bar{e}^{(i)} = \bar{r}$$

$$\bar{e}^{(i)} = (000 \dots 010 \dots 0)$$

$$\bar{H}_{(n-k) \times n} = \begin{pmatrix} \bar{a}^{(1)T} & \bar{a}^{(2)T} & \dots & \bar{a}^{(n)T} \end{pmatrix}$$

$$\dim(\bar{a}^{(i)}) = n-k, \quad \forall i = 1, \dots, n$$

$$\bar{H} \cdot \bar{r}^T = \bar{A}^T \rightarrow \bar{H}(\bar{c} + \bar{e}^{(i)})^T = \bar{H} \bar{c}^T + \bar{H} \bar{e}^{(i)T} = \bar{A}^T \rightarrow \bar{H} \bar{e}^{(i)T} = \bar{A}^T = \bar{a}^{(i)T}$$

$$\begin{pmatrix} \bar{a}^{(1)T} & \bar{a}^{(2)T} & \dots & \bar{a}^{(n)T} \end{pmatrix} \cdot \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix} = \bar{a}^{(i)T}$$

• $\forall \bar{a}^{(i)}$ különböz

• egyik $\bar{a}^{(i)}$ sem lehet $\bar{0}$

Hamming-kódok:

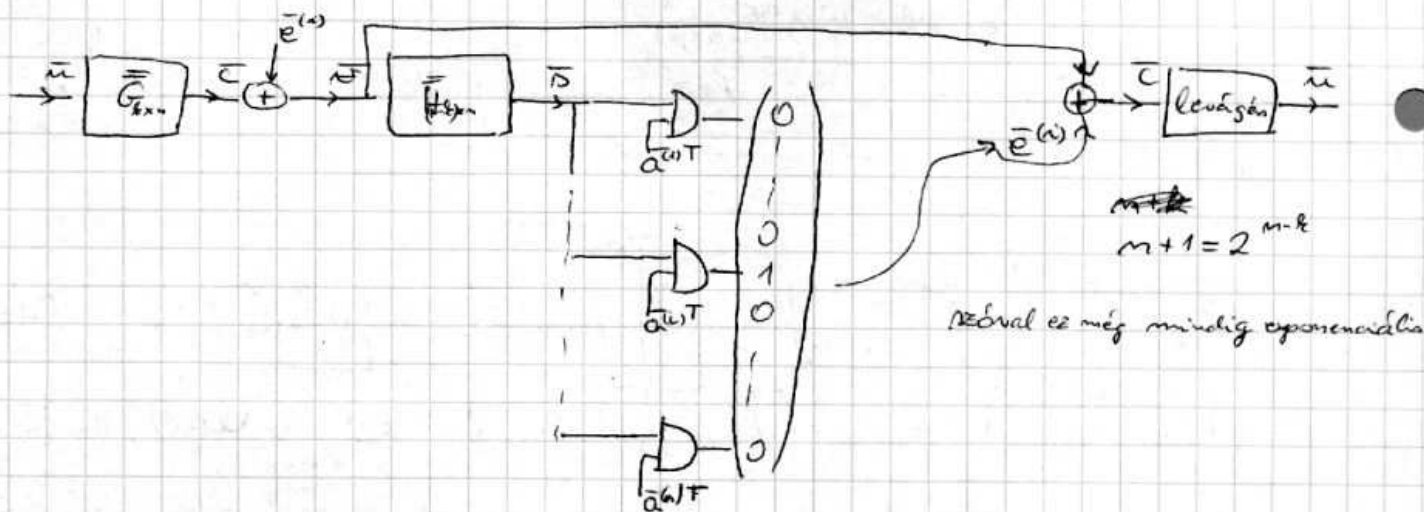
k	n
1	3
4	7
11	15
...	...

$$2^{n-k} - 1 = n$$

$\uparrow$ összes kód szó $\uparrow$ egyenlőtlenek száma

$$n+1 = 2^{n-k}$$

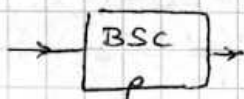
Kódtervezés: $(n, 2) \rightarrow n+1 = 2^{47} \rightarrow H \rightarrow G$



Költségek kommunikációs technikáival

$$P_b < 10^{-3} = 10^{-8}$$

γ QOS



$$P_{\text{adott}} = 1 - m \cdot p$$

(7) $C(7, 4)$

$$H_{3 \times 7} = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix} \rightarrow G_{5 \times 7}$$

35647 decimālis atvārtam mēvelod sērend.

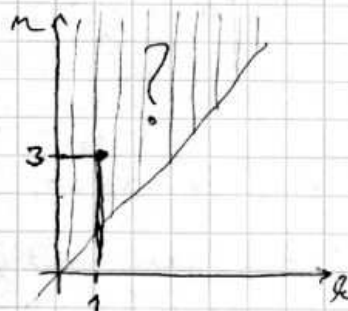
$$\bar{G}_{4 \times 7} = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{pmatrix}$$

$\bar{a}$	$\bar{c}$
001	0000001
010	0000010
100	0000100
111	0001000
110	0010000
101	0100000
011	1000000

 $C(1,3)$

$$3 \leq d_{\min} \leq m - k + 1 = 3$$

$$d_{min} = m - k + 1 = 3 \quad \text{DMS good}$$



Hogyan lehet több hibát javítani?

Pl: $\forall$ 2 hiba javítása: $\bar{e}^{(ij)} = (0 \dots 0 \overset{i}{1} 0 \dots 0 \overset{j}{1} 0 \dots 0)$

$$\bar{H} \bar{A}^T = \bar{A}^T \rightarrow \bar{H} (\bar{C} + \bar{e}^{(ij)})^T = \bar{H} \bar{C}^T + \bar{H} \bar{e}^{(ij)T} = \bar{A}^T \rightarrow \bar{H} \bar{e}^{(ij)T} = \bar{A}^T$$

$$\left(\begin{array}{c} \bar{a}^{(1)T} \\ \bar{a}^{(2)T} \\ \bar{a}^{(3)T} \\ \bar{a}^{(4)T} \end{array} \right) \cdot \begin{pmatrix} 0 \\ \vdots \\ 1 \leftarrow i \\ \vdots \\ 1 \leftarrow j \\ \vdots \\ 0 \end{pmatrix} = \bar{a}^{(i)T} + \bar{a}^{(j)T} = \bar{A}^T$$

↑
additív

↑
?

↑
konmutatív

• $\forall \bar{a}^{(i)T} + \bar{a}^{(j)T}$ különböző

• $\forall \bar{a}^{(i)T}$ különböző

• $\bar{a}^{(i)T} \neq \bar{0}; \bar{a}^{(i)T} + \bar{a}^{(j)T} \neq \bar{0}$

← ez túl szigorú feltétel bűnrészre

Lemma: $d_{\min} = n_{\min} \rightarrow \bar{H}$ mátrix lin. fgt. oszlopvektorainak száma $n_{\min} - 1$

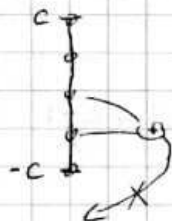
$$\bar{H} \bar{C}^T = \bar{0}^T \quad \sum_{j=1}^{w(C)} \bar{a}^{(i_j)T} = \bar{0}$$

$$\begin{pmatrix} 0 \\ \vdots \\ 1 \leftarrow i_1 \\ \vdots \\ 1 \leftarrow i_2 \\ \vdots \\ 0 \end{pmatrix}$$

Ábrák

Többállapú (q-ális) kódok

Megfontolás:



Véges test

$$GF(q)$$



-0,15

• megjavítja a hibajavító képességet.

• elvonja a vétel esélyét (pontosabban vért)

Négyes testek $GF(q) = \{\alpha_0, \alpha_1, \dots, \alpha_{q-1}\} = \{0, 1, \dots, q-1\}$

" + "

" * "

$$\forall \alpha, \beta \in GF(q) \rightarrow \alpha + \beta \in GF(q)$$

$$\forall \alpha, \beta \in GF(q) \rightarrow \alpha \cdot \beta \in GF(q) \setminus \{0\}$$

$$\alpha + \beta = \beta + \alpha$$

$$\alpha \cdot \beta = \beta \cdot \alpha$$

$$\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$$

$$\alpha \cdot (\beta \cdot \gamma) = (\alpha \cdot \beta) \cdot \gamma$$

$$\alpha \in GF(q) \exists \beta : \alpha + \beta = 0 ; \beta = \alpha^{-1}$$

$$\exists \alpha \in GF(q) \setminus \{0\} : \exists \beta : \alpha \cdot \beta = 1, \beta = \alpha^{-1}$$

$$\alpha(\beta + \gamma) = \alpha \cdot \beta + \alpha \cdot \gamma$$

q prim

mod q

$$\alpha + \beta = \gamma \rightarrow \alpha + \beta = \alpha \cdot q + \gamma$$

$$\alpha \cdot \beta = \kappa \rightarrow \alpha \cdot \beta = m \cdot q + \kappa$$

$GF(7)$ felelti hatványozás

elem	1	2	3	4	5	6	rend
1	1						1
2	2	4	1				3
3	3	2	6	4	5	1	6
4	4	2	1				3
5	5	4	6	2	3	1	6
6	6	1					2

primitív elem

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

$$3^3 = 2^6 \text{ mod } 7 = 6 \text{ helyett}$$

$$3^3 = 3^1 \cdot 3^2$$

$\forall$ Galois testben $\exists$ legalább 1 primitív elem
(mely az elemrend generálja)

Polynomok a $GF(q)$ felett

$$a(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n \quad x, a \in GF(q)$$

$$\deg(a(x)) = n$$

$$a(x) \cdot b(x) \rightarrow c_i = \sum_{j=0}^{m+n-i} b_{i-j} \cdot a_j$$

$GF(q)$ felelti hatványozás

Adott $a(x)$, $d(x)$
↑ osztando ↑ osztó

$$\deg(a(x)) = m > \deg(d(x)) = n$$

$$\begin{array}{ccc} a(x) & \xrightarrow{\quad} & q(x) \\ d(x) & \xrightarrow{\quad} & r(x) \end{array} \Rightarrow a(x) = q(x) d(x) + r(x)$$

$$\deg(r(x)) < \deg(d(x))$$

1.)

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix}$$

a) $A = (01)$ $e_n = ?$

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

$$\bar{A}^T = H \cdot \bar{e}^T = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$$G_{k \times n} = [I_{k \times k}, B_{k \times (n-k)}]$$

$$H_{(n-k) \times n} = [A_{(n-k) \times k}, I_{(n-k) \times (n-k)}]$$

$$C = M \cdot G = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 0 \end{pmatrix}$$

$\Rightarrow$ Csoporthatás: 0000 nagy 1000.

$$e_1 = 00000$$

$$e_2 = 00001$$

$$00010$$

$\vdots$

$$10000$$

$$\lambda_1 = 00$$

$$\lambda_2 = 01$$

$$\bar{A}^T = H \cdot \bar{e}$$

csoporthatás + $\{e\}$ = hibajelző-csoport

c) $p = 0,1$

$$p \cdot (1-p)^4 = 0,1^1 \cdot 0,9^4 = 0,06561$$

2.)

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 & 1 \end{pmatrix} \rightarrow H = \begin{pmatrix} 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 \end{pmatrix} \rightarrow \bar{A}^T = \bar{H} \cdot \bar{e}_1^T = \bar{H} \cdot \bar{e}_2^T = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$$

$e_1 = (10000)$ és $e_2 = (00001)$ nem megkül.

b) $p = 0,2 \Rightarrow p(\text{hiba}) = p \cdot (1-p)^4 = \dots$

3.)

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 & 1 & 1 & 1 \end{pmatrix} \xrightarrow{B=A^T} A = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}$$

$C(7,3)$ -as kód.

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

$\bar{C} = \bar{H} \cdot \bar{G} \rightarrow$ Kés az összes $\bar{u}$ -t megismerve $\bar{G}$ -vel megkapjuk az összes $\bar{x}$ -et

hibajelző képesség: $d_{\min} - 1 = 2$

hibajavító képesség: $\left\lfloor \frac{d_{\min} - 1}{2} \right\rfloor = 1$

$d_{\min} = \min_{\bar{u} \neq \bar{v}} w(\bar{u} - \bar{v}) = 3$

BSC $p=0,1$

$$\bar{x} = (1101001)$$

$$p(\bar{x}) = ?$$

$$\bar{s} = \bar{x} \cdot \bar{H}^T = \bar{H} \cdot \bar{e}^T$$

$$s = \bar{x} \cdot \bar{H}^T = (1101001)$$

$$\begin{pmatrix} 0110 \\ 1001 \\ 1111 \\ 1000 \\ 0100 \\ 0010 \\ 0001 \end{pmatrix} = (0110)$$

Syndromdekodiert:

$$\begin{array}{c|c} \bar{e} & \bar{s} \\ \hline \vdots & \vdots \end{array}$$

$$\Rightarrow \bar{e} = 1000000 \quad \bar{s} = 0110$$

Bin. $\downarrow$

$$w(\bar{e}) = 1$$

$$P(\bar{x}) = p \cdot (1-p)^6 = 0,1 \cdot 0,9^6 = 0,0531$$

$$\bar{G}_{k \times n} = \begin{pmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-1} & \alpha^{2(n-1)} & \dots & \alpha^{(n-1)(n-1)} \end{pmatrix} \rightarrow \bar{H}_{(n-k) \times n} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \dots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \dots & \alpha^{2(n-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & \alpha^{n-k} & \alpha^{2(n-k)} & \dots & \alpha^{(n-k)(n-1)} \end{pmatrix}$$

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

$$C(x) \Big|_{x=\alpha^i} = 0 \quad i=1, \dots, n-k$$

$$C_0 + C_1 \alpha + C_2 \alpha^2 + \dots + C_{n-1} \alpha^{n-1} = 0$$

$$C_0 + C_1 \alpha^2 + C_2 \alpha^4 + \dots + C_{n-1} \alpha^{2(n-1)} = 0$$

Matrix

$$C_0 + C_1 \alpha^{n-k} + C_2 \alpha^{2(n-k)} + \dots + C_{n-1} \alpha^{(n-k)(n-1)} = 0$$

$$(\bar{H} \cdot \bar{C}^T) \mathbf{0} = 0$$

$$\sum_{i=0}^{n-1} \alpha^{ki} \cdot C_i = \sum_{i=0}^{n-1} \alpha^{ki} \cdot \sum_{j=0}^{k-1} \alpha^{ij} \cdot u_j = \sum_{j=0}^{k-1} u_j \left(\sum_{i=0}^{n-1} \alpha^{(k+j)i} \right) = \sum_{j=0}^{k-1} u_j \frac{(\alpha^{k+j})^n - 1}{\alpha^{k+j} - 1} = 0$$

$$n = q-1 \Rightarrow \alpha^n = 1$$

12) V 2 kiba javításra alk. Reed-Solomon kód.

$$m, k : t=2 = \left\lfloor \frac{n-k}{2} \right\rfloor, \text{ kötés: } n = \text{prím}-1, \text{ min } 2 \text{ prím}$$

$$C(6,2) \quad 2 = \left\lfloor \frac{6-2}{2} \right\rfloor$$

$$\bar{G}_{2 \times 6} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix} \rightarrow \bar{H}_{4 \times 6} = \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 6 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{pmatrix}$$

- nem szimmetrikus $\Rightarrow$ dekodáláshoz nem használhatjuk a levégást.

$$\bar{u} \cdot \bar{G} = \bar{c} \leftarrow \text{kihatalmazott egyenletrendszer: } k \text{ db ismeretlen.}$$

? adott ismert

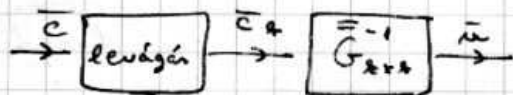
levegés

n db egyenlet, $n > k$

$$\bar{u} \cdot \bar{G}_{k \times k} = \bar{c}_k \rightarrow k \text{ db egyenlet.}$$

$$\bar{G}_{k \times k}^{-1} \cdot \bar{c}_k = \bar{u} \rightarrow \text{gond nélkül megoldható}$$

mindig egyértelműen dekodálható, mert $|\bar{G}_{k \times k}| \neq 0$



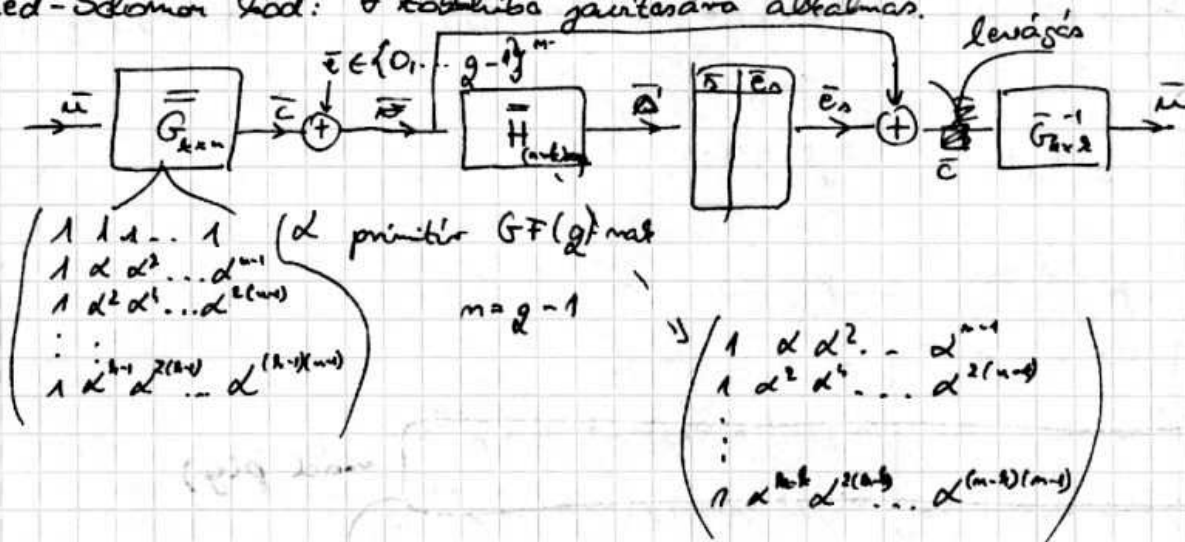
Nyitott kérdések:

- Hogyan lehet real-time detekció? (szindróma-detektálási táblázat kiszámítás)
- Hogyan tudunk visszatérni hibaüzenet elvitelére?

$5 \rightarrow 101$, de parancsok, mert csak 7 szimbólum van.

$$2^m = 2^m \text{ jelek.}$$

Reed-Solomon kód: t hibátörés javítására alkalmas.



MDS $d_{min} = n - k + 1$

Input: t db hibajav.

$$n, k: \left\lfloor \frac{n-k}{2} \right\rfloor = t, \quad n = q-1, \quad \min 2$$

$$C(n, k), q, \alpha \Rightarrow \bar{G}, \bar{H}$$

Optimális kódal ábrákhoz hibajavítás, nemcsak récsi, ami real-time.

!!! Probléma:

1.) q -ális $\rightarrow$ bináris

2.) teljesen real-time: táblázat kiíratása ($O(q^m)$) $\rightarrow$ polinomialis komplexitás?

1.) Véges test bináris átvitel:

$GF(5)$

$$\vec{c}(1, 3, 4, 2) \rightarrow (001, 011, 100, 010)$$

lefordított
binárisra.

szöveg kódolása

pozitív: 101, 110, 111 - nek nincs szerepe.

$$\text{ld } 2 \leq \lceil \text{ld } 2 \rceil$$

$$q = 2^m \xrightarrow{\text{megoldás}} \frac{1}{T_s} \cdot \frac{\text{ld } q}{\lceil \text{ld } q \rceil} \text{ nagy vereség}$$

DE mod 2^m aritmetika nem lineáris

pl: $GF(4)$ $2 \cdot 2 = 4 \cdot \text{mod } 4 = 0$ jó

Antiretika a $GF(p^m)$ -ben, $p = \text{prím}$

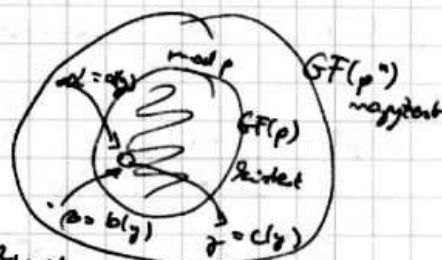
Irreducibilis polinom: $p(y) \neq a_1(y) + a_2(y)$

$d_y(a_1(y); a_2(y)) \nmid d_y(p(y))$

pl: $y^2 + y + 1$ $y^4 + y + 1$
 $y^3 + y + 1$ $y^5 + y^2 + 1$

$GF(p^m)$	p-írás szám	polinom
0	0 0 ... 0	0
1	0 0 ... 1	1
$\vdots$	$\vdots$	$\vdots$
$\rightarrow \alpha \rightarrow$	$a_{n-1} a_{n-2} \dots a_0$	$a(y) = a_0 + a_1 y + \dots + a_{n-1} y^{n-1}$
$\rightarrow \beta \rightarrow$	$b_{n-1} b_{n-2} \dots b_0$	$b(y) = b_0 + b_1 y + \dots + b_{n-1} y^{n-1}$
$\rightarrow \gamma \rightarrow$	$c_{n-1} c_{n-2} \dots c_0$	$c(y) = c_0 + c_1 y + \dots + c_{n-1} y^{n-1}$
$p^m - 1$	$p-1 \ p-1 \dots p-1$	

mod $p(y)$



Antiretika a $GF(4)$ -ben

elem	bináris	polinom
0	0 0	0
1	0 1	1
2	1 0	y
3	1 1	y + 1

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

+	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

·	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

$1 + 2 = 1 + y$

$1 + y + 1 = (1 + 1) y^0 + 1 = y^0 = 1$

$y + y = (1 + 1) y = 0$

$y + y + 1 = 1 + (1 + 1) y = 1$

$3 + 3 = y^1 + 1 + y + 1 = (1 + 1) y^1 + (1 + 1) y^0 = 0$

$2 \cdot 2 = y \cdot y = y^2 = 1(y^2 + y + 1) + y + 1$

$2 \cdot 3 = y \cdot (y + 1) = y^2 + y = 1(y^2 + y + 1) + 1 = 1$

$3 \cdot 3 = (y + 1)(y + 1) = y^2 + 2y + 1 = 1(y^2 + y + 1) + (y + 1) + y + 1 = 2$

Határozható a $GF(8)$ felé

$GF(8) = GF(2^3) \rightarrow p(y) = y^3 + y + 1$

elem	bináris	polinom
0	0 0 0	0
1	0 0 1	1
2	0 1 0	y
3	0 1 1	y + 1
4	1 0 0	y^2
5	1 0 1	y^2 + 1
6	1 1 0	y^2 + y
7	1 1 1	y^2 + y + 1

$[y]$ primitív elem

y^0	1	1
y^1	y	2
y^2	y^2	4
y^3	y + 1	5
y^4	y^2 + y	6
y^5	y^2 + y + 1	7
y^6	y^2 + 1	5
y^7	1	3

$y^3 = 1 \cdot (y^3 + y + 1) + y + 1$

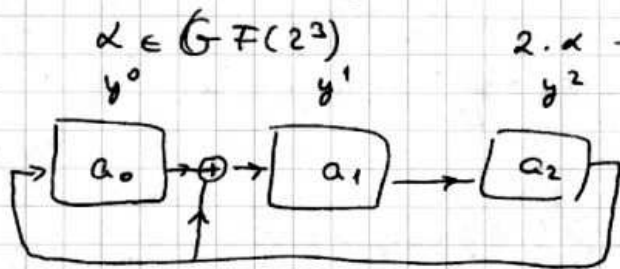
$y^4 = y(y^3 + y + 1) = y^4 + y^2 + y + 1 = y^2 + y + 1$

$y^5 = (y^2 + 1)(y^3 + y + 1) + y^2 + y + 1$

$y^6 = (y^2 + y + 1)(y^3 + y + 1) + y^2 + 1$

Következő

Aritmetika SHR-ekkel



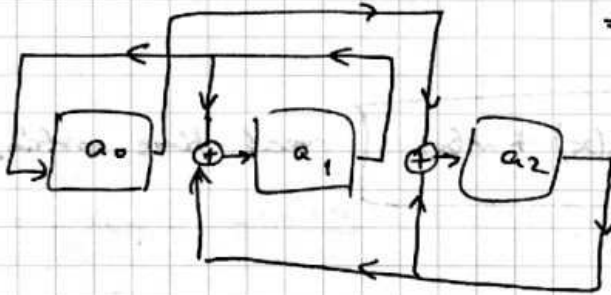
$$2 \cdot x \rightarrow y(a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 =$$

$$= a_0 y + a_1 y^2 + a_2 (y + 1) =$$

$$= 2_2 + (a_0 + a_2) y + a_1 y^2$$

$$4 \cdot x \rightarrow y^2(a_0 + a_1 y + a_2 y^2) = a_0 y^2 + a_1 y^3 + a_2 y^4 = a_0 y^2 + a_1 (1 + y) + a_2 (y + y^2)$$

$$= a_1 + (a_1 + a_2) y + (a_0 + a_2) y^2$$



Polinomiál GF(p^n) felelt

$$\alpha(x) = \alpha_0 + \alpha_1 x + \alpha_2 x^2 + \dots + \alpha_n x^n$$

$\alpha_1, \alpha_2, \dots, \alpha_n \in GF(p^n)$

$$\alpha_0 = 3 \rightarrow \alpha_0(y) = y + 1$$

$$\alpha(x) = \alpha_0(y) + \alpha_1(y)x + \alpha_2(y)x^2 + \dots + \alpha_n(y)x^n$$

Standard leírás:

$$\alpha(x) = y^{i_0} + y^{i_1} x + y^{i_2} x^2 + \dots + y^{i_n} x^n$$

$$GF(8) \quad \alpha(x) = 5 + 3x^2 + 4x^3 + 6x^4 =$$

$$= y^5 + y^3 x^2 + y^2 x^3 + y^4 x^4$$

101 011 100 110

$$101 \rightarrow y^2 + 1 \rightarrow y^5$$

$$011 \rightarrow y + 1 \rightarrow y^3$$

$$100 \rightarrow y^2$$

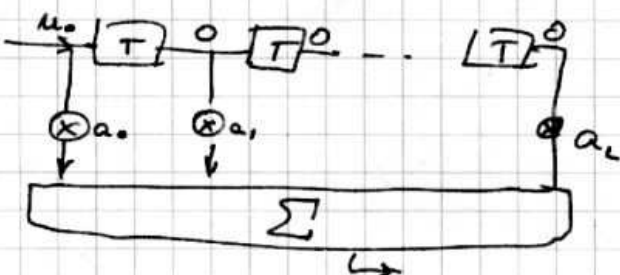
$$110 \rightarrow y^2 + y \rightarrow y^4$$

$$\alpha(x) = 6 + 2x + 7x^2 + 5x^3 + 4x^4$$

$$\alpha() = 11001011101100$$

SHR - szintézis (műveleti polinomiál közt SHR-nd)

LFSR - Linear Feed Forward Shift Register.



$$u_0 = a_0 u_0$$

$$u_1 = a_0 u_1 + a_1 u_0$$

$$u_2 = a_0 u_2 + a_1 u_1 + a_2 u_0$$

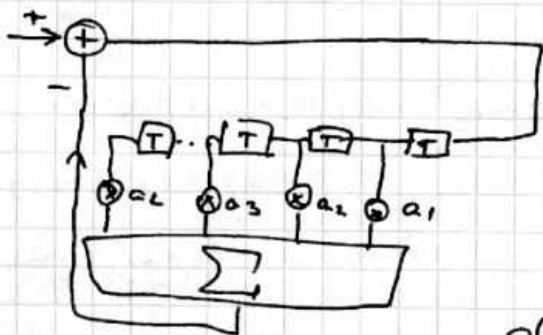
$$u_i = \sum_{j=0}^L a_j \cdot u_{i-j}$$

$u(x) = a(x) \cdot u(x)$

$u(x) \xrightarrow{\text{LFSR}} u(x) = a(x) \cdot u(x)$

Ábrák

Linear Feedback Shift Register (LFBSR)



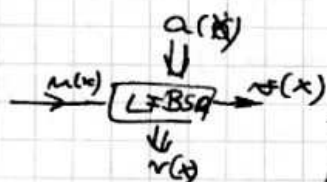
$$y_i = u_i - \sum_{j=1}^L a_j \cdot y_{i-j}$$

$$a_0 y_i + \sum_{j=1}^L a_j y_{i-j} = u_i$$

$$\sum_{j=0}^L a_j y_{i-j} = u_i$$

$$a(x) y(x) = u(x)$$

$$y(x) = \frac{u(x)}{a(x)} \quad \text{octave}$$

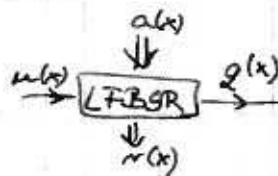
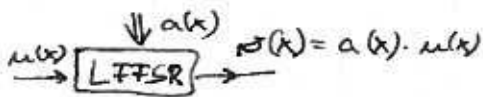


$$u(x) = y(x) \cdot a(x) + v(x) \quad \text{real-time octave, Eulerian algorithm}$$

octave, octave, bit, time, time

Shift register

<http://neural.hut.bme.hu>



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

legolapább, leggyorsabb ilyen elemek → real-time algoritmusok

Létezik-e olyan kódok, amelyek SZR-en implementálhatók? ← technológia

Létezik-e olyan kódok, amelyek polinom műveletek alapján működnek? ← algoritmus

Válasz: lineáris ciklikus kódok

$$\bar{c} = (c_0 \ c_1 \ \dots \ c_{n-2} \ c_{n-1}) \rightarrow \bar{c}' = S \bar{c} = (c_{n-1} \ c_0 \ c_1 \ \dots \ c_{n-2})$$

$$\text{ciklikus: } \bar{c} \in G \Rightarrow S^k \bar{c} \in G$$

$$\text{lineáris: } \bar{c}, \bar{c}' \in G = \alpha \bar{c} + \beta \bar{c}' \in G$$

$$\bar{c} \rightarrow c(x) = c_0 + c_1 x + \dots + c_{n-2} x^{n-2} + c_{n-1} x^{n-1}$$

$$\bar{c}' \rightarrow c'(x) = c_{n-1} + c_0 x + \dots + c_{n-3} x^{n-2} + c_{n-2} x^{n-1}$$

$$\} \Rightarrow c'(x) = x \cdot c(x) \bmod (x^n - 1)$$

$$\textcircled{2} \quad x \cdot c(x) = x c_0 + c_1 x^2 + c_2 x^3 + \dots + c_{n-2} x^{n-1} + c_{n-1} x^n$$

$$\downarrow$$

$$x \cdot c(x) = c_{n-1} \cdot (x^n - 1) + c'(x)$$

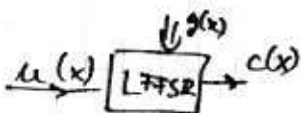
$\forall C(m, k)$ lin. cikl. kód esetén $\exists g(x)$ generátorpolinom:

$$\bullet \deg(g(x)) = n - k$$

$$\bullet g_{n-k} = 1$$

$$\bullet g(x) \mid x^n - 1$$

$$\bullet c(x) = g(x) \cdot u(x) \quad \forall c(x) \in G \rightarrow \text{technológiai implikáció}$$



!!! gyors

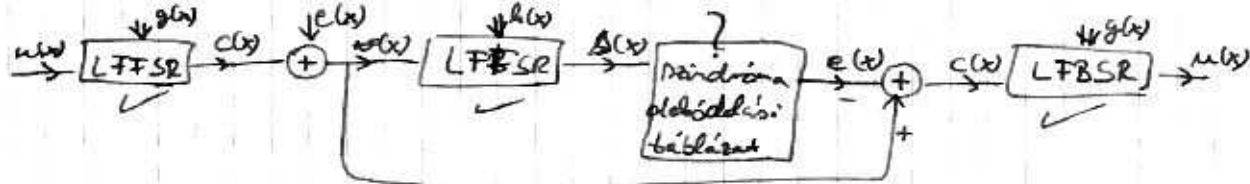
Paritás ellenőrző polinom

$$h(x) : h(x) \cdot c(x) = 0 \bmod (x^n - 1) \quad \forall c(x) \in G$$

$$h(x) \cdot g(x) \cdot u(x) = 0 \bmod (x^n - 1) \quad \forall u(x)$$

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

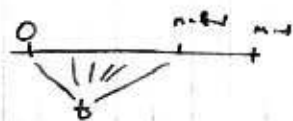
$$h(x) = \frac{x^n - 1}{g(x)}$$



$$r(x) = c(x) + e(x) = g(x) \cdot u(x) + e(x)$$

$$r(x) = a(x) \cdot g(x) + r(x) \Leftarrow \text{LFBSR}$$

$$r(x) = c(x); \quad a(x) = u(x)$$



Csak akkor jó, ha $\deg(c(x)) \leq m-k-1$ + nagyon könnyű osztani maradék

A hibáról feltételezni kell, mert

? kideríthető: $\xrightarrow{\Delta(x)} \text{LFBSR} \rightarrow e(x)$

Létezik-e MDS kód?

Optimális ciklikus kód? (MDS kód teljesítménye)

A Reed-Solomon kódok ciklikusak is. $\Rightarrow$ MDS (opt)
 $\downarrow$
real-time

Biz: $c(x) \mid \phi$

$y^i, i=1, \dots, m-k$ ← ez a definíció

$c(x) = g(x) \cdot u(x)$ ← ciklikus kód

$$g(x) = \prod_{i=1}^{m-k} (x - y^i)$$

$$h(x) = \frac{x^m - 1}{g(x)} = \frac{\prod_{i=1}^m (x - y^i)}{\prod_{i=1}^{m-k} (x - y^i)} = \prod_{i=n-k+1}^m (x - y^i)$$

$$x^m - 1 \mid 0 \quad (y^i)^m = (y^m)^i = (y^{2^m})^i = 1^i = 1$$

(Pc) 4 2 hiba javítására alkalmas RS kód konstruálása a $\text{GF}(8)$ felett.

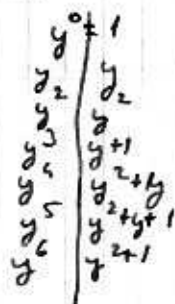
$g(x) = ?$, $h(x) = ?$

$C(7,3)$

$$t=2 = \left\lfloor \frac{m-k}{2} \right\rfloor \Rightarrow k=3$$

$$g(x) = \prod_{i=1}^4 (x - y^i) = (x+y)(x+y^2)(x+y^3)(x+y^4) =$$

$$= (x^2 + (y+y^2)x + y^3)(x^2 + (y^3+y^4)x + 1) = (x^2 + y^4x + y^3)(x^2 + y^6x + 1) = x^4 + y^4x^3 + x^2 + y^6x^3 + y^3x^2 + y^3x + y^3 =$$



$$z = \boxed{x^4 + y^3 x^3 + x^2 + yx + y^3 = g(x)} = (011 \ 010 \ 001 \ 011 \ 001 \ 000 \ 000 \ 000)$$

Ciklikus kódok szisztematikus generálása

$$c(x) \rightarrow \bar{c} = (u_0 \dots u_{k-1} \dots)$$

$$x^{m-k} \cdot u(x) = a(x) \cdot g(x) + r(x)$$

$$0 \leq \deg(r(x)) \leq m-k+1$$

$$c(x) = u(x) - x^k \cdot r(x)$$

$$\Downarrow$$

$$k \leq \deg(x^k \cdot r(x)) \leq m-1$$

$$\textcircled{11}$$

$$\bar{c} = (\underbrace{u_0 u_1 \dots u_{k-1}}_{\text{rendszerezett}} \dots u_{k-1} \dots \underbrace{r_0 r_1 \dots r_{m-k+1}}_{\text{üres}})$$

rendszerezett ~~üres~~ üres

$$\textcircled{B} \ g(x) \mid c(x) \rightarrow x^k \cdot x^{m-k} \cdot u(x) = x^k \cdot a(x) \cdot g(x) + x^k \cdot r(x) \bmod (x^m - 1)$$

$$\deg(a(x)) \leq m-1$$

$$x^m a(x) \bmod (x^m - 1) = a(x)$$

$$x^m a(x) = (x^m - 1) a(x) + \boxed{a(x)}$$

$$x^k u(x) = x^k a(x) g(x) + x^k r(x)$$

$$c(x) = u(x) - x^k g(x) = x^k a(x) \cdot g(x)$$

A Reed-Solomon kódok

ciklikusság!

<http://www.mti.hu/~kvt/kvt/kvt.html>

MDS $\Rightarrow$ optimális

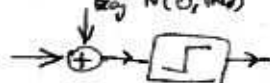
Shift Registers implementáció

$$t = \left\lfloor \frac{n-k}{2} \right\rfloor$$

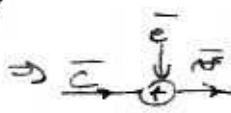
REAL-TIME

Csatorna

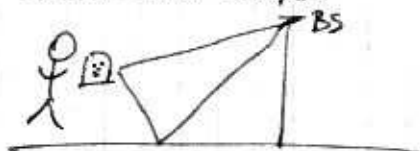
véletlen csatornamodell



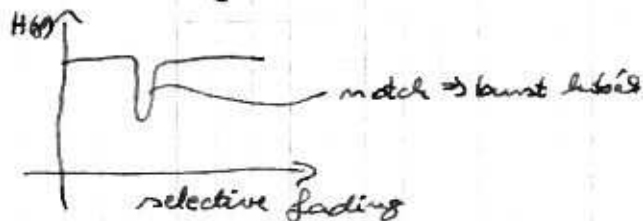
$$P = \Phi(-\sqrt{\text{SNR}}) = \Phi\left(-\sqrt{\frac{1}{N_0}}\right)$$



burst hiba állapot



$$H(f) = 1 + \rho \cdot e^{-2j\pi f \lambda T}$$



Hogyan tudunk olyan kódot csinálni, ami a burst hibákat is javítja.

$C(n, k) \rightarrow$ bursthibajavítóképeség?

$$bl(\bar{a}) = l; \quad \underbrace{1 \ 0 \ 1 \ \dots \ \bar{a} \ \dots \ 1 \ 0}_{l}$$

Standard array

$\bar{e} = 0$	$\bar{c}^{(1)}, \bar{c}^{(2)}, \dots, \bar{c}^{(n)}$
$\bar{e}^{(1)}$	$\bar{e}^{(1)} + \bar{c}^{(1)}, \bar{e}^{(1)} + \bar{c}^{(2)}, \dots, \bar{e}^{(1)} + \bar{c}^{(n)}$
$\bar{e}^{(2)}$	$\bar{e}^{(2)} + \bar{c}^{(1)}, \bar{e}^{(2)} + \bar{c}^{(2)}, \dots, \bar{e}^{(2)} + \bar{c}^{(n)}$
$\vdots$	
$\bar{e}^{(l)}$	$\bar{e}^{(l)} + \bar{c}^{(1)}, \bar{e}^{(l)} + \bar{c}^{(2)}, \dots, \bar{e}^{(l)} + \bar{c}^{(n)}$

$$2^{n-k} \cdot 2^k = 2^n$$

$\bar{e}', \bar{e}''$ 2^k megkülönböztethető, ha $\bar{e}' + \bar{e}'' \neq \bar{c}$

Ha $bl(\bar{e}) \leq l \rightarrow bl(\bar{c}) > 2l$

$$\bar{e} + \bar{e}' \neq \bar{c}$$

Ha $bl(\bar{c}) > 2l \rightarrow 2l \leq n-k$

Reiger...

burst hiba javar $l \leq \left\lfloor \frac{n-k}{2} \right\rfloor$

random hiba javar $t \leq \left\lfloor \frac{n-k}{2} \right\rfloor$

$\rightarrow$ Nagy kódok
 $n-k$ nagy

$$-bl(\bar{a}) \leq 2l \quad \underbrace{\quad\quad\quad}_{2l} \quad 2^{2l} < 2^{n_{\text{tot}}}$$

~~de~~ Nagy kódot kell előállítani! ← lehet-e más kódokból nagy kódot generálni?

Bináris kód: $C(n, k); GF(2^m), t$. (kódkombinációk)

$$C_{\text{bin}}(nm; m, k) \quad \underbrace{\quad\quad\quad}_m \underbrace{\quad\quad\quad}_m \underbrace{\quad\quad\quad}_m \dots \underbrace{\quad\quad\quad}_m$$

(1) (2) (3) (n)

$$l_{\text{bin}} = m \cdot t$$

$$t \leq t_{\text{bin}} \leq m \cdot t$$

λ -interleaving

$$\lambda \left\{ \begin{array}{c} C(n, k) \\ \underbrace{\quad\quad\quad}_{\lambda \cdot k} \\ \underbrace{\quad\quad\quad}_{\lambda \cdot m} \end{array} \right.$$

$l = \lambda \cdot t$ db bintűsítés javításán
alkalmas, a véletlen csúszáshoz
kell átírni, de kódolás pedig
soroként kell.

- Készenléti nagy, mert az utolsó csúszást is
meg kell várni $\Rightarrow$ nem Real-time

Szorzatkód: $C_1(n_1, k_1), t_1; C_2(n_2, k_2), t_2$

$$\begin{array}{c} C_1(n_1, k_1) \\ k_1 \\ n_1 \\ C_2(n_2, k_2) \\ k_2 \end{array} \left(\begin{array}{cc} \overline{p_{11}} & \overline{p_1} \\ \overline{p_2} & \overline{p_{12}} \end{array} \right)$$

$$k = k_1 \cdot k_2$$

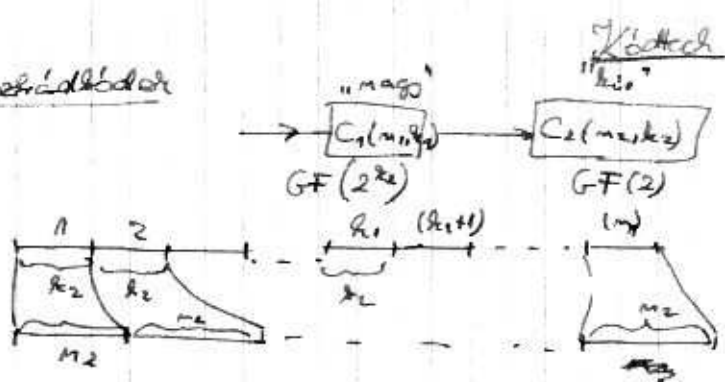
$$w_{\text{min}} \geq w_{\text{min}}^{(1)} \cdot w_{\text{min}}^{(2)} \xrightarrow{\text{lineáris}} d_{\text{min}} = d_{\text{min}}^{(1)} \cdot d_{\text{min}}^{(2)}$$

vagy így, hogy csúszást a 2. csúszás } mindig, ugyanez lesz
vagy soroként kódolás az 1. csúsz.

csúszást. átírás $\Rightarrow$ vélemintesen t_1 hibát javít $\Rightarrow \boxed{t_1 \cdot n_2 + t_2}$ max bintűsítés
javítás.

$$\text{csúszást. átírás} \Rightarrow \boxed{m_1 \cdot t_2 + t_1}$$

$$l = \max \{ m_1 \cdot t_2 + t_1; m_2 \cdot t_1 + t_2 \}$$



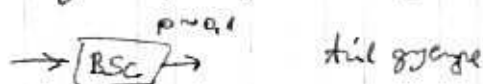
$$k = k_1 \cdot k_2$$

$$m = m_1 \cdot k_2$$

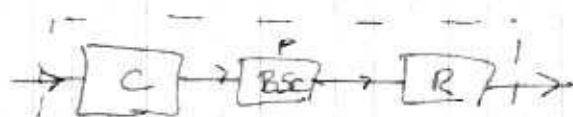
$$n_{min} = n_{min}^{(1)} \cdot n_{min}^{(2)}$$

$$d_{min} = d_{min}^{(1)} \cdot d_{min}^{(2)}$$

Kódok teljesítménye a dekódálási minőségnek tekintve:



→ kódolás $C(m, k, t, GF(2^k))$



$p' = \Phi(p)$

$$P_{nyit} = \sum_{j=1}^m \binom{m}{j} p^j \cdot (1-p)^{m-j}$$

$$P_{block-er} = \sum_{i=tn}^m \binom{m}{i} \cdot P_{nyit} \cdot (1 - P_{nyit})^{m-i}$$

$$P_{block-correct} = 1 - P_{block-er}$$

$$P_{block-correct} = (1 - p^i)^{m \cdot m}$$

$p \sim 10^{-1} \rightarrow C(7, 3), GF(8), t=2 \rightarrow p' \approx 0.0031 \leftarrow 2$ nagyságrendet lehet javítani.

ADATBIZTONSÁG

- értékes adatok védelme
- kriptográfia $\rightarrow$ algoritmusként tervezése, implementáció
- fizikai védelem
- rendszerszabály jellegű védelem
- kriptológia (tudomány)
 - kriptográfia, titkosítás
 - kriptanalízis: illetéktelenül megfejtünk kódot.

Rejtjelzés: küldő $\rightarrow$ vevő

M - plaintext: az, amit át akarunk küldeni

C - ciphertext: a kódolt üzenet

$$E(M) = C$$

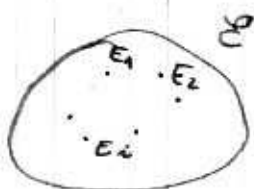
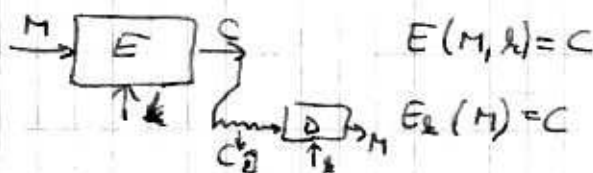
D - decryption: fejtés

$$D(C) = M$$

E - kódoló transzformáció / encryption

$$D(E(M)) = M$$

k - key; kulcs



A kulccsal kiválasztunk 1 transzformációt a pol között.
↑
titkos $|K| \sim 2^{100}$

A transzformációt választja a támadó is ismeri, csak azt nem tudja, hogy melyikkel dolgozik

Szimmetrikus kulcsos rejtjelzés: régi

ugyanaz az adata és a rejtő

Aszimmetrikus k.r.: modern, népszerű eljárás $\rightarrow$ nyilvános kulcsos rejtjelzés.

A támadó mindent tud, kivéve a rejtjelző kulcsát.

ugyanaz az eszköz, szoftver.

algoritmusként

- block: egyenként jönnek és mennek a 100 bites blokkok, a kulcs fix
- stream rejtjelző: üzenetfolyam és kulcsfolyam, mind 2 irányba történik.

Publikus / nyíltan kulcsú rij-t

- a 70-es évek közepétől
- k_1 kódoló és k_2 dekódoló kulcs
↑ ↑
nyíltan titkos
kulcs kulcs
RSA
- támadás
- támadó
- kompromittálás: úgy szerezni meg a kulcsot, hogy elvesziük.

Támadás: • csak a C ~~titkos~~ van birtokunkban: $P_1, P_2, \dots, P_i$ -hez tartozó $E(P_1), E(P_2), \dots, E(P_i)$
rejtett üzenet alapú támadás (pl. rádiósatlama kihalás)

- ismert ^{nyílt} üzenetű támadás: ismert $P_1, P_2, \dots, P_i, E(P_1), E(P_2), \dots, E(P_i)$
- választott nyílt üzenetű támadás: feltehető, de juttatható vala
- adaptív választott $\dots$: az eredményismeretében kihasználva az új ~~rejtett~~ P_i -t
- választott üzenetű támadás: P_i -hez megkapom $E(P_i)$ -t, $E(P_i)$ -hez P_i -t
↓
legrosszabb támadás, ez ellen is kell néznie a kód.

Biztonság

- költség: nem éri meg, ha meghaladja a nyitási költségét.
- komplexitás: • adat: mennyi adat kell a támadás végrehajtásához.
 - feltételei $\&$: mennyi idő kell a megfigyelésre (elérési idő)
 - támadási erő
- ↓
értelmezhetővé válik a támadás erőfeszítésével kapcsolatban.
- feltétel nélküli birt: az algoritmus biztonságos a támadás erőfeszítésétől függetlenül.
- feltétel nélküli birt: akkor jó, ha a támadás költsége / erőfeszítése korlát alatt marad.
- Steganográfia: az üzenet elrejtése a hálón

One-Time Pad

egyszer használatos (kulcsáramú rejtjelzésnél)

kulcsbitfolyam: valódi random sorozat (például)

kódolás: mod 2 összeadás az üzenettel.

dekódolás: mely egyszer hozzáadom a kulcsot.

- akkor jó, ha nem akkor generálok a kódot, amikor a kulcsot

- a 26 betűs angol ábécével is lehet használni mod 26.

Shannon

tökéletes rejtjelzés!

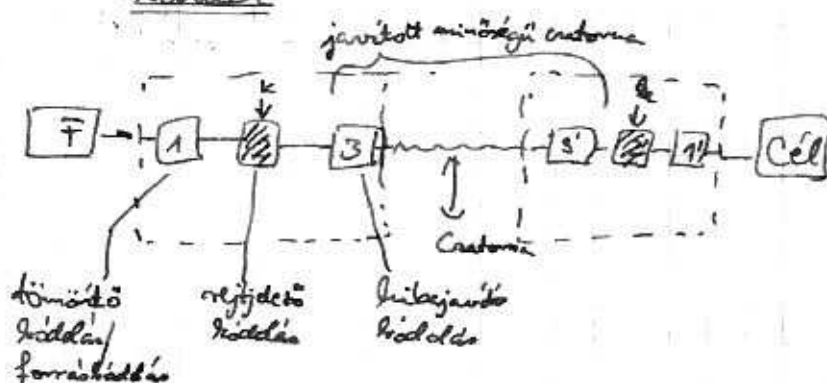
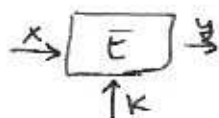
a kódolás után a kimenet a kimenet egymástól függt.

① a OTP tökéletes rejtjelző

$$Y = X + K$$

$$P(Y=y | X=x) = P(X+K=y | X=x) = P(K=y-x | X=x) = P(K=y-x) = 2^{-N} \quad \left. \vphantom{P(Y=y | X=x)} \right\} \Rightarrow \text{füg. v.}$$

$$P(Y=y) = \sum_x P(X+K=y | X=x) \cdot P(X=x) = 2^{-N} = P(Y=y | X=x)$$



mael 20 ggr¹⁰

$$D = C = K = \mathbb{Z}_{26}$$

$$E_k(x) = x + 2 \pmod{26}$$

Egy betűt eldobunk néhánymal

$$D_2(y) \equiv y - 2 \pmod{26}$$

Cézár - rejtelmes, kimerítő ~~hatalmas~~ ^{kezes} ~~publikációs~~ ^{szöveges} fejtető, visszafelé szifeltetés

Rot 13 : nem kell visszafele' forgatni

Lineáris nyitjelcső

$$y = Ax + b$$

$x: N$ hominid network

$A: N \times N$ -es invertálható lin. mátrix

b: N Aardvark *Did. aztecus*

← nagyon parányi, $N \cdot (N+1)$ véletlen
bit eloszlással

támadás, ismét nyílt támadás

cdl: A lab negh.

normal: $y = Ax_0 + b$

$$y_1 - y_0 \leq A(x_1 - x_0)$$

$$y_1 = Ax_1 + b$$

$$\rightarrow y_2 - y_0 = A(x_2 - x_0)$$

$$y_N = Ax_N + b$$

$$y_N - y_0 = A(x_N - x_0)$$

még jobb: $x_1 - x_0 = \underline{e} \Rightarrow$ atomal megfogás

A 27 October

Ha én választom meg a bemenetet,
még hatékonyabb vagyok.

$$X = (x_1 - x_0, x_2 - x_0, \dots, x_N - x_0)$$

$$y = (y_1 - y_0, y_2 - y_1, \dots, y_N - y_1)$$

$$Y = AX$$

$$A = Y \cdot X^{-1}, \text{ da } \exists X^{-1}$$

est feldt/dorhegüt, met ang:
x-c-t mileradent, hays bogen
göthel N lin fgt a mtr-ban

Hill ngjelero

$$E_f(x) = x \cdot k \pmod{26}$$

$$D_1(y) = y \cdot k^{-1} \bmod 26$$

$x = \frac{\text{Friday}}{\text{PQ CP KU}}$

$$m=2 \quad y = PQC \neq KV$$

$$E_2(5, 17) = (15, 16)$$

$$E_A(8,3) = (2,5)$$

$$E_R(0, 24) = (10, 20)$$

$$\begin{pmatrix} 15 & 16 \\ 2 & 5 \end{pmatrix} = \begin{pmatrix} 5 & 17 \\ 2 & 3 \end{pmatrix} \begin{pmatrix} g_{11} & g_{12} \\ g_{21} & g_{22} \end{pmatrix}$$

$$\begin{pmatrix} 5 & 17 \\ 8 & 3 \end{pmatrix}^{-1} = \begin{pmatrix} 9 & 1 \\ 2 & 15 \end{pmatrix} \rightarrow K = \begin{pmatrix} 51 & 156 \\ 24 & 25 \end{pmatrix} \begin{pmatrix} 156 & 25 \\ 83 & 3 \end{pmatrix}$$

Algoritma neįveikė

$$K_2(a,b) \in \mathbb{Z}_{26} \times \mathbb{Z}_{26} : \gcd(a, 26) = 1$$

$$P = C = \mathbb{Z}_{26}$$

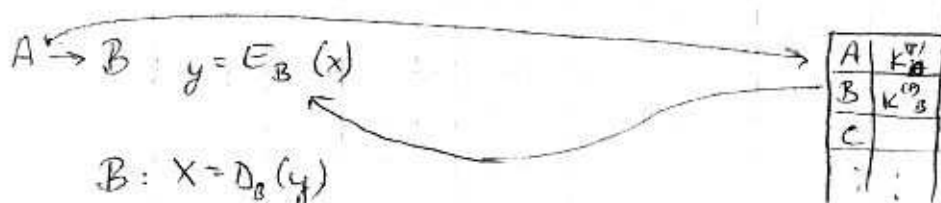
$$E_2(x) = ax + b \pmod{26}$$

$$D_2(y) = a^{-1}(y - b) \pmod{26}$$

a 2-metis o 13-metis mutais inversai

$$a \text{ žinodami } 12 \cdot 26 = 312 \text{ mod } 26$$

$$\uparrow \\ \varphi(26) = 12 \cdot 1 = 12$$



$$B: x = D_B(y)$$

$$B: (K_B^{(P)}, K_B^{(S)})$$

Diffie-Hellman: kettősoldós titkosítás ötlete (1975)

RSA:

1) p_1, p_2 nagy prímszámok

2) $m = p_1 \cdot p_2$

$$\phi(m) = (p_1 - 1)(p_2 - 1)$$

$$e: 1 \leq e < \phi(m), \quad (\phi(m), e) = 1$$

3) $d = e^{-1} \pmod{\phi(m)}$

4) $E^e = (m, e)$ nyilvánvaló

$$E^d = (d, p_1, p_2) \text{ titkos}$$

$$\text{Kódolás: } y = x^e \pmod{m} \quad 1 \leq x < m$$

$$\text{Dekódolás: } x = y^d \pmod{m} \quad 1 \leq y < m$$

$$1 = (e, \phi(m)) = s \cdot e + \phi(m) \cdot t$$

$$e^{-1} = ? \pmod{\phi(m)}$$

$$e^* \cdot e^{-1} = 1 \pmod{\phi(m)}$$

$$e^* \cdot e = \cancel{1} \pmod{\phi(m)} + 1$$

$$e^* \cdot e - q \cdot \phi(m) = 1 \Rightarrow e^* = e^{-1}$$

Chinese remainder theorem

$m_1, m_2, \dots, m_r > 0$ párhuzamos rel. pr.

$$a_1, a_2, \dots, a_r \in \mathbb{Z}$$

$$x = a_i \pmod{m_i} \quad i = 1, 2, \dots, r \text{ - nek van közös megoldása, pontosan 1 db mod } m_1 \cdot m_2 \cdot \dots \cdot m_r$$

(7e) $p_1 = 5, p_2 = 11$

Legendre's symbol, quadratic residues?

$d = 28$

$$40 = 13 \cdot 3 + 1$$

$$1 \cdot 40 + (-13) \cdot 3 = 1$$

$\uparrow$ or as inverse

$$-13 = 27 \pmod{40}$$

$$m = 55 = p_1 \cdot p_2$$

$$\varphi(m) = 40 = (p_1 - 1)(p_2 - 1)$$

$e = 3$ $(e, \varphi(m)) = 1$

Kódteche

1) Adva van egy $C(6,3)$ RS kód.

a) generátormatrix?

b) Paritásellenőrző mtr?

c) Jelezés, javítás?

$$G_{n \times m} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{pmatrix}$$

$$c) m = q - 1 \Rightarrow GF(7)$$

elem	hatvány	rend
1	1	1
2	2 4 1	3
3	3 2 6 4 5 1	6
4	4 2 1	3
5	5 4 6 2 3 1	6
6	6 1	2

$$b) H_{(n-k) \times m} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} \end{pmatrix} = \begin{pmatrix} 1 & 5 & 4 & 6 & 2 & 3 \\ 1 & 4 & 2 & 1 & 4 & 2 \\ 1 & 6 & 6 & 1 & 6 & 1 \end{pmatrix}$$

$$c) d_{\min} = n - k + 1 = 4$$

$$\text{hibajelezés: } d_{\min} - 1 = 3$$

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

2) $\forall 2$ hibát javítani képes RS kód $GF(7)$ feletti

a) kód paraméterei?

b) generátormatrix, ^{paritásellenőrző} ~~paritásellenőrző~~ mtr.

$$a) n = q - 1 = 6$$

$$d_{\min} = n - k + 1$$

$$\frac{d_{\min} - 1}{2} \geq 2 \Rightarrow d_{\min} \geq 5 \Rightarrow k = 2$$

$C(6,2)$ kód

$$b) \bar{G} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 3 & 2 & 6 & 4 & 5 \end{pmatrix}$$

$$\bar{H} = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \alpha^4 & \alpha^5 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 & \alpha^8 & \alpha^{10} \\ 1 & \alpha^3 & \alpha^6 & \alpha^9 & \alpha^{12} & \alpha^{15} \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} & \alpha^{16} & \alpha^{20} \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 & 6 & 4 & 5 \\ 1 & 2 & 4 & 1 & 2 & 4 \\ 1 & 6 & 1 & 6 & 1 & 1 \\ 1 & 4 & 2 & 1 & 4 & 2 \end{pmatrix}$$

3) Adja meg egy $GF(7)$ feletti RS kód $g(x)$ -t és $h(x)$ -t, a leghatékosabb primitív elemet használva.

$$\alpha = 3 \quad g(x) = \prod_{i=1}^{n-k} (x - \alpha^i)$$

$$t=1 \quad d_{\min}=3 \quad n=6 \quad k=4$$

$$g(x) = (x - \alpha)(x - \alpha^2) = (x - 3)(x - 2)$$

$$h(x) = \prod_{i=n-k+1}^n (x - \alpha^i)$$

$$h(x) = (x - \alpha^3)(x - \alpha^4)(x - \alpha^5)(x - \alpha^6)$$

4) GF(11) RS kód

a) $n, k = ?$

b) $\bar{H} = ?$ a kód a lehető ^{legnagyobb üzemeltetési} ~~legnagyobb~~ hibák javítására mellett $t=3$ hibát javítson.

$$a) t=3 = \left\lfloor \frac{d_{\min}-1}{2} \right\rfloor \Rightarrow d_{\min} = 7$$

$$n = 10 \quad k = 4$$

$$\bar{H}_{(n-t) \times n} = \bar{H}_{6 \times 10} = \dots$$

5) Mennyi 7×6 a GF(8)-ban. Irred: $g(y) = y^3 + y + 1$

Törtek	Polinom
0	0
1	1
2	x
3	$x+1$
4	x^2
5	x^2+1
6	x^2+x
7	x^2+x+1

$$\begin{aligned} 7 \cdot 6 &= (x^2+x+1)(x^2+x) = x^4 + x^3 + x^2 + x^3 + x^2 + x = \\ &= x^4 + x = x(x^3+x+1) + x^2 = x^2 \neq 1 \end{aligned}$$