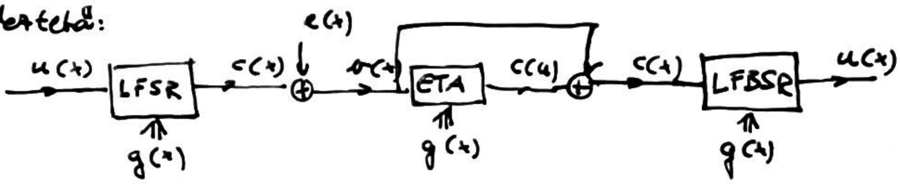
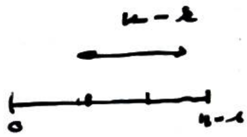
Infocode előadás

10.19.

Emlékeztető:



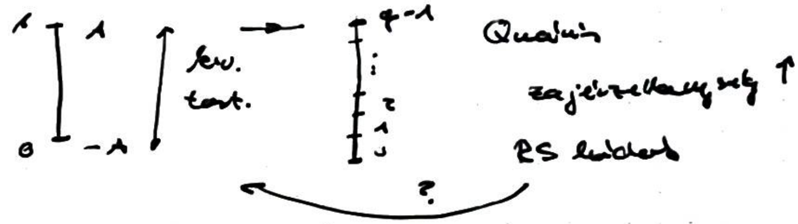


$$g(x)=\prod_{i=1}^{n-k}(x-\alpha^i) \quad \alpha\in GF(q)$$

RS ciklikus kód = MDS + SR impl.

(optimális) (valósíthatóság m.)

↳ <u>DE</u> Bináris kódolatoknál



$\alpha\in GF(2^m)$

$\alpha \to (\underbrace{0\;1\;1\;1\;0\;\dots\;0}_{m})$!

<u>példa</u>: $GF(8)$ $\quad 4\cdot 2 \bmod 8 = 0$ ↯ nem alkalmas

<u>Algebra $GF(p^m)$ felett</u>

irreducibilis polinom $p(y) \neq p_1(y)p_2(y)$ $\quad \deg(p_i(y)) < \deg(p(y)) = m$

$i=1,2$

	szimbólumtér elemei	vektor reprezentáció	polinom reprezentáció
	0	$000\dots0$	$0y^{m-1}+0y^{m-2}+\dots+0y^0=0$
	1	$000\dots1$	$0y^{m-1}+0y^{m-2}+\dots+1y^0=1$
	$\vdots$		
	$\to \alpha$	$\vec{a}_{m-1}\vec{a}_{m-2}\dots\vec{a}_0$	$a_{m-1}y^{m-1}+a_{m-2}y^{m-2}\dots+a_0y^0=a(y)$
	$\to \beta$	$\vec{b}_{m-1}\vec{b}_{m-2}\dots\vec{b}_0$	$b_{m-1}y^{m-1}+b_{m-2}y^{m-2}+\dots+b_0y^0=b(y)$
$\alpha\cdot\beta=\gamma$	$\leftarrow \gamma$	$\vec{c}_{m-1}\vec{c}_{m-2}\dots\vec{c}_0$	$c_{m-1}y^{m-1}+c_{m-2}y^{m-2}\dots+c_0y^0=c(y)$
	$\vdots$		
	p^m-1	$p-1\;p-1\dots p-1$	$\dots$

$a(y)\,b(y) \bmod p(y)$

$a(y)b(y)=q(y)p(y)+c(y)$

$\deg(c(y)) < \deg(p(y)) = m$

$a(y) + b(y) = q'(y)\,p(y) + c'(y)$

példa: $p(y) = y^2 + y + 1 \qquad m = 2$

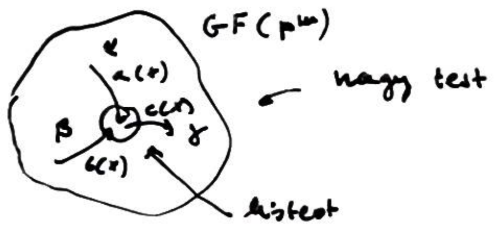
$y^3 + y + 1$

$y^4 + y + 1$

$y^5 + y^2 + 1 \qquad m = 5$

$\vdots$

Megjegyzés:



példa: $GF(4) = GF(2^2)$

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

ELEMEK	VEKTOROS R.	POLINOM R.
0	00	$0\cdot y^1 + 0y^0 = 0$
1	01	$0\cdot y^1 + 1y^0 = 1$
2	10	$1\cdot y^1 + 0\cdot y^0 = y$
3	11	$1\cdot y^1 + 1y^0 = y+1$

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

$1 + 1 \neq 2$

$0\cdot y^1 + 1y^0 + 0y^1 + 1y^0 = 1+1$

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

$1+2 = 1+y \Rightarrow 3$

$1+3 = 1+y+1 \Rightarrow 2$ $\alpha+\beta=\gamma$

$2+3 \Rightarrow y+y+1 = (1+1)y + 1\cdot y^0 = 1$

×	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

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

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

példa: GF(8) feletti algebra $[GF(2^3)]$ $p(y) = y^3 + y + 1$

ELEMEK	VEKTOROS R.	POLINOM R.
0	000	0
1	001	1
2	010	$0y^2 + 1y^1 + 0y^0 = y$
3	011	... $y+1$
4	100	... y^2
5	101	... y^2+1
6	110	..... y^2+y
7	111	$1y^2 + 1y + 1y^0 = y^2+y+1$

GF(8) hatványtábla

Megj: $GF(p^m)$ p primitív elem → $GF(2^3)$ 2 a prim elem.

2^0	y^0	1	1
2^1	y^1	y	2
2^2	y^2	y^2	4
2^3	y^3	$y+1$	3
2^4	y^4	y^2+y	6
2^5	y^5	y^2+y+1	7
2^6	y^6	y^2+1	5
2^7	y^7	1	1
2^8	y^8	y	2
⋮	⋮		

↓ ismétlődik ciklikusan

$$y^3 = (y^3+y+1) + y+1$$
$$y^4 = y(y^3+y+1) + y^2+y$$
$$y^5 = (y^2+1)(y^3+y+1) + y^2+y+1$$

Műveletvégzés: (szorzás)

GF(8) $\quad 2\cdot 4 \Rightarrow y\cdot y^2 = y^3 \Rightarrow \underline{\underline{3}}$

$\quad 3\cdot 6 \Rightarrow y^3\cdot y^4 = y^7 \Rightarrow \underline{\underline{1}}$

másképp $\quad 3\cdot 6 \Rightarrow (y+1)(y^2+y) = y^3+y^2+y^2+y =$

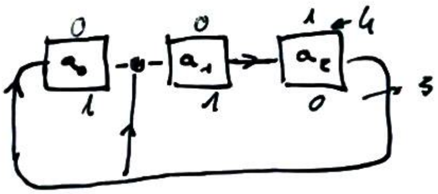
$\quad = y^3+y = (y^3+y+1)+1 = 1 \Rightarrow \underline{\underline{1}}$

GF(2^m) szorzás impl. SR-en

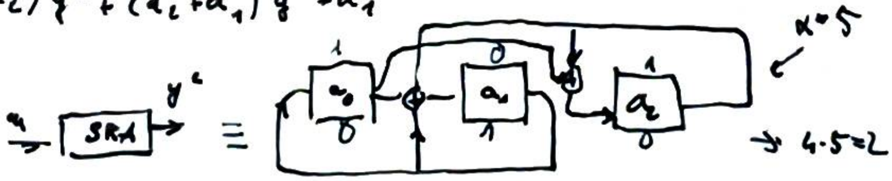
példa: $GF(2^3)$

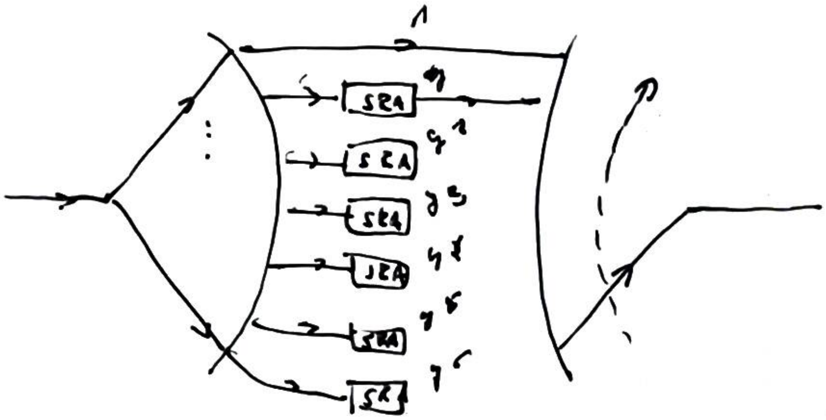
$\alpha \in GF(2^3)$

$$2\cdot\alpha = y(a_2y^2+a_1y+a_0) = a_2y^3+a_1y^2+a_0y = a_2(y+1)+a_1y^2+a_0y = a_2y+a_2+a_1y^2+a_0y = a_1y^2+(a_2+a_0)y+a_2$$



$$4\cdot\alpha \Rightarrow y^2(a_2y^2+a_1y+a_0) = a_2(y^2+y)+a_1(y+1)+a_0y^2 = a_2y^2+a_2y+a_1y+a_1+a_0y^2 = (a_0+a_2)y^2+(a_2+a_1)y^1+a_1$$




SRA
SRA
SRA
SRA
SRA
SRA