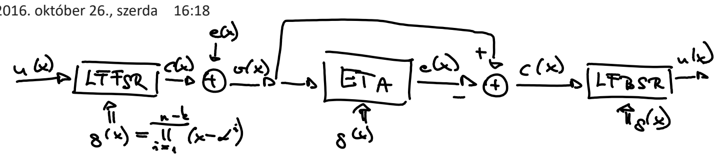

given "t" → q, n, k, α

RS codes → optimal (MDS) + Shift Register implementation: realtime

Problem: if q is large, then the difference is small, so small noise can corrupt it.

→ WE use binary codes because binary code needs large noise to be corrupted

→ We get the binary code of the Galois Field number

→ Problem q must be prime, but binary codes cover the range $[0, 2^m)$

→ Let's define an algebra over $GF(2^m)$ that is good for coding (2^m is not prime)

Algebra over $GF(2^m)$:

'p' is prime → p = 2

$p(y)$, $deg(p(y)) = m$

$p(y) \neq p_1(y) \cdot p_2(y)$ → $p(y)$ is not reducable →
- $p(y) = y^2 + y + 1$
- $p(y) = y^3 + y + 1$
- $p(y) = y^4 + y + 1$
- $p(y) = y^5 + y^2 + 1$

$deg(p_i(y)) < deg(p(y))$ · i = 1, 2

'Op' domain

symbolic	elements	p-ary representation	polinomial representation
	0	0 0 ... 0	$0 \cdot y^{m-1} + 0 \cdot y^{m-2} + \dots + 0 \cdot y^0 = 0$
	1	0 0 ... 1	$0 \cdot y^{m-1} + 0 \cdot y^{m-2} + \dots + 1 \cdot y^0 = 1$
	⋮	⋮	⋮
	α	$a_{m-1} a_{m-2} \dots a_0$	$a_{m-1} y^{m-1} + a_{m-2} y^{m-2} + \dots + a_0 y^0 = a(y)$
	⋮	⋮	
	β	$b_{m-1} b_{m-2} \dots b_0$	$b_{m-1} y^{m-1} + b_{m-2} y^{m-2} + \dots b_0 y^0 = b(y)$
	⋮		⋮
	γ	$c_{m-1} c_{m-2} \dots c_0$	$c_{m-1} y^{m-1} + c_{m-2} y^{m-2} + \dots c_0 y^0 = c(y)$
	⋮		
	$p^{m-1} - 1$	p-1 p-1 ... p-1	$(p-1) y^{m-1} + (p-1) y^{m-2} + \dots (p-1)$

$\alpha + \beta$ → $a(y) + b(y) = q(y) p(y) + c(y)$ → γ

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

$\alpha \cdot \beta$ → $a(y) b(y) = q'(y) p(y) + c'(y)$ → $a(y) b(y) \bmod p(y) = c'(y)$ → γ

Example:

Algebra over $GF(2^2)$, $p(y) = y^2 + y + 1$

elements	binary rep.	polinomial rep.
0	0 0	$0 y^1 + 0 \cdot y^0 = 0$
1	0 1	$0 \cdot y^1 + 1 \cdot y^0 = 1$
2	1 0	$1 \cdot y^1 + 0 \cdot y^0 = y$
3	1 1	$1 \cdot y^1 + 1 \cdot y^0 = y + 1$

⇒

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

*	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	3	1
3	0	3	1	2

primitive element

Power table over GF(8)

elements	binary rep	polinomial rep
0	000	0
1	001	1
2	010	y
3	011	$y+1$
4	100	y^2
5	101	y^2+1
6	110	y^2+y
7	111	y^2+y+1

$p(y) = y^3 + y + 1 \quad 2 \to y^{2^{-1}} = y^{7} = 1$

y^0	1	
y^1	y	
y^2	y^2	
y^3	$y+1$	$y^3 = 1\,(y^2+y+1) + y+1$
y^4	y^2+y	$y^4 = y(y^3+y+1) + y^2+y$
y^5	y^2+y+1	$y^5 = (y^2+1)(y^3+y+1) + y^2+y+1$
y^6	y^2+1	$y^6 = (y^3+y+1)(y^3+y+1) + y^2+1$
y^7	1	
y^8	y	
y^9	y^2	
y^{10}	$y+1$	

...

$6 \cdot 3 = y^4 \cdot y^3 = y^7 = 1$

$6 + 3 = y^2 + y + y + 1 = y^2 + 1 = 5$

$2\alpha = y \cdot (a_0 + a_1 y + a_2 y^2) = a_0 y + a_1 y^2 + a_2 y^3 = a_0 y + a_2 y^2 + a_2 (y+1) = \boxed{a_2 + (a_0 + a_2) y + a_1 y^2}$

Implementation on shift registers: