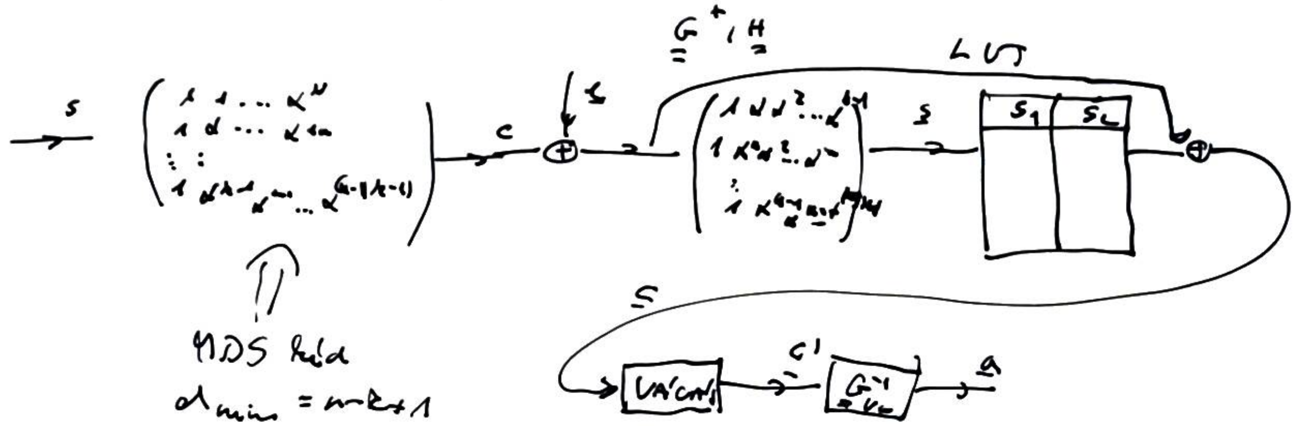
UFO CODE I

Emlékeztető: RS kódok

$$t \to n, k, q \to \alpha \in GF(q)$$



MDS kód

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

vektor r. ⟵ ~~polinom r.~~

$\underline{u} = (u_0, u_1, \ldots, u_{k-1})$ $\qquad u(x) = u_0 + u_1 x + u_2 x^2 + \ldots + u_{k-1} x^{k-1}$

$\underline{c}$

$\underline{e}$

$\underline{v}$

$\underline{s}$

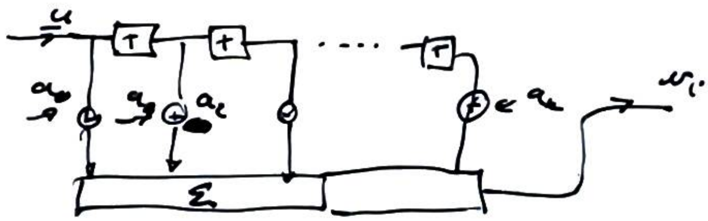
Mire használjuk?

1.) RS MDS kód elegendő volt

2.) implementáció → menet

Shift Regiszteres ~~megvalósítás~~ implementáció

1.) Linear Feedforward Shift Register (LFFSR)



$v_0 = a_0 \cdot u_0$

$v_1 = a_1 u_1 + a_2 u_2$

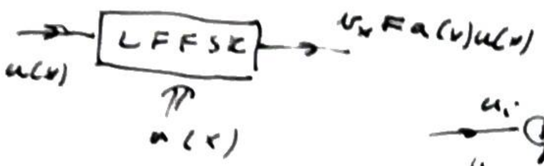
$v_2 = v_1 + a_2 u_2$

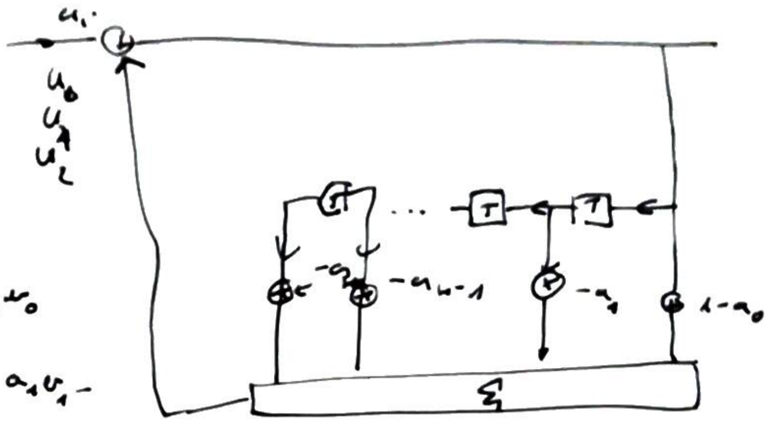
$\vdots$

$\boxed{v(x) = g(x) \cdot u(x)}$ ⟵ $\boxed{v_i = \sum_{j=0} a_j u_i}$

2.) Linear Feedback Shift Register (LFBSR)

i állapot





$v_0 = u_0 + (1-a_0)\, v_0$

$v_1 = u_1 + (1-a_0)\, v_1 - a_1 v_0$

$v_2 = u_2 + (1-a_0)\, v_2 - a_1 v_1 -$

$- a_2 v_0$

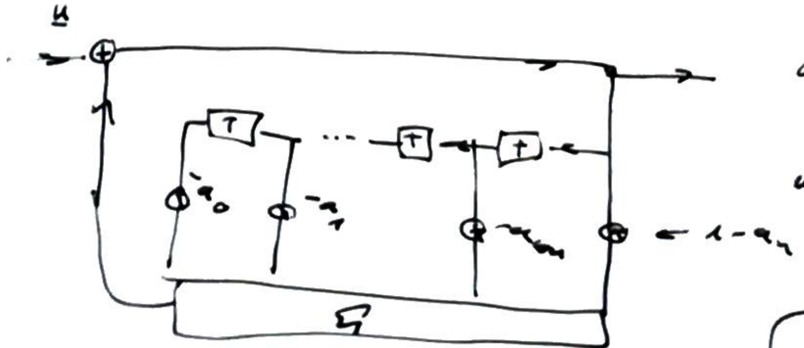
$\vdots$

$v_i = u_i + (1-a_0)\, v_i - a_2 v_{i-2} - \dots a_n v_{i-n}$

$a_0 v_i + a_1 v_{i-1} + \dots + a_n v_{i-n} = u_i$

$$\boxed{\sum_{j=0}^{n} a_j v_{i-j} = u_i}$$

3.) LFBSR with REMINDER (LFBSR w.r.)

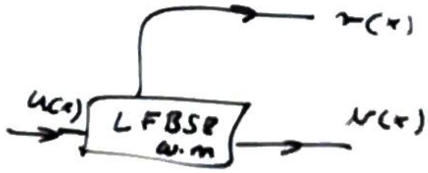


$\deg(u(x)) = n > \deg(a(x)) = m$

$n - m = i$ hányados pol.

$u(x) = v(x) \cdot a(x) + r(x)$ u_0 u_1

maradék pol



$a(x) =$

$= v(x) \deg(a) +$

$+ r(x)$