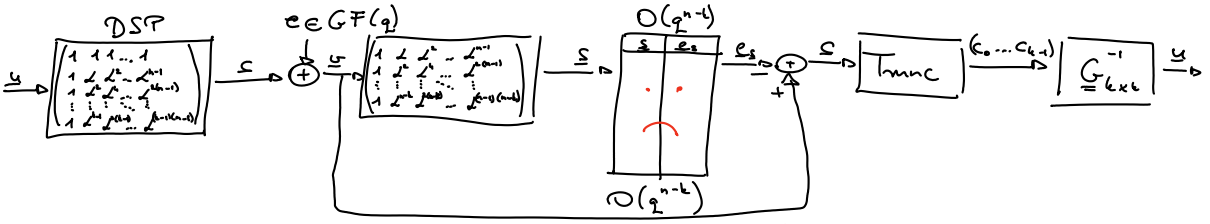
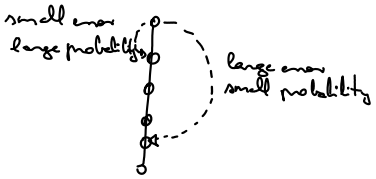
RS code

2016. október 12., szerda 16:22



$E_s = \{e : H e^T = s^T\}$; $e_s = \max_{e \in E_s} p(e)$



$e = (0,0,5,0,5,0)$

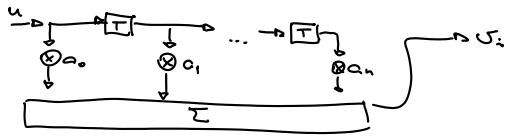
$e' = (0,1,1,1,0,0)$

Design: given "t" errors

$n = q-1$; $n-k = 2t$; "q" prime

$\rightarrow \mathcal{L} \in GF(q)$

Linear FeedForward Shift Register

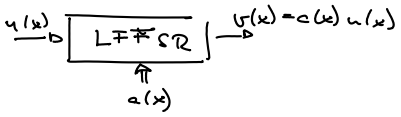


$i = 0 \quad v_0 = a_0 u_0$

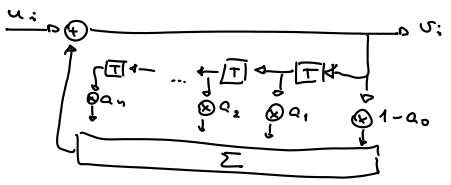
$i = 1 \quad v_1 = a_0 u_0 + a_1 u_1$

$i = 2 \quad v_2 =$

$i \quad v_i = \sum_{j=1}^{i} a_j u_{i-j} \xrightarrow{\Sigma} v(x) = a(x)\, u(x)$



Linear FeedBack Shift Register (LFBSR)



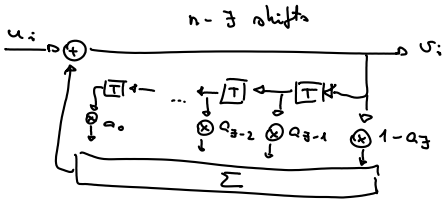
$v_i = (1-a_0)v_i - a_1 v_{i-1} - a_2 v_{i-2} - \dots - a_j v_{i-j} + u_i$

$v_i - (1-a_0)v_i + a_1 v_{i-1} + a_2 v_{i-2} + \dots + a_j v_{i-j} = u_i$

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

$a(x)\, v(x) = u(x) \rightarrow v(x) = \frac{u(x)}{a(x)}$

Linear FeedBack Shift Register with remainder (LFBSR with r.)



$u(x) = v(x)\, a(x) + r(x)$

$\deg u(x) = u >$

Example: in GF(5)

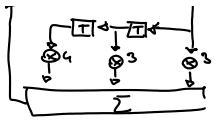
$(x^3 + 4x + 4) : (x^2 + 2x + 3) = x + 3$

$a(x)$

$a_0 \rightarrow 1 - a_0 = 1 - 3 = -2 = 3$

$i = 0 \rightarrow v_0 = 3 v_0 + 4$

$-2 v_0 = 4$



$3\sigma_0 = 4$

$\sigma_0 = (3^{-1}) \cdot 4 = 2 \cdot 4 = 3$

$i=1 \rightarrow \sigma_1 = 3\sigma_1 + 4 + 4 \Rightarrow \sigma_1 = 1$

$i=2 \rightarrow \sigma_2 = 3\sigma_2 + 3 + 2$

$\sigma_2 = 3\sigma_2 + 0 \rightarrow \sigma_2 = 0$

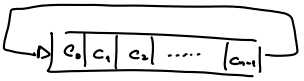
$i=3 \rightarrow \sigma_3 = 3\sigma_3 + 4 + 1$

$\sigma_3 = 3\sigma_3 + 0 \rightarrow \sigma_3 = 0$

0 0 1 3 ⇒ yes it is truly the solution

Cyclic Shift Operator

$\underline{c} = (c_0, c_1, c_2, \dots c_{n-1}) \rightarrow \underline{c}' = S^1\underline{c} = (c_{n-1}, c_0, c_1, \dots c_{n-2})$



$c(x) = c_0 + c_1 x + c_2 x^2 + c_3 x^3 + \dots c_n x^n$

$c^1(x) = x \cdot c(x) \mod (x^n - 1)$

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

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

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

Linear cyclic code:

$\underline{c} \rightarrow c(x)$

If $\underline{c} \in C \rightarrow \underline{c}' = S\underline{c} \in C$ (if $c(x) \in C$ then $x \cdot c(x) \mod (x^n - 1) \in C$)

$\underline{c}, \underline{c}' \in C \rightarrow (\alpha c(x) + \beta c'(x)) \in C$

$C(n, k) \rightarrow \exists g(x)$

- $\deg(g(x)) = n - k$
- $g_{n-k} = 1$
- $\forall c(x) \in C : c(x) = u(x) g(x)$
- $g(x) \mid x^n - 1$ ($g(x)$ can be divided by $(x^n - 1)$ without remainder)