S_3 / Linear feedback shift registers (LFSR)

Un LFSR se asociază următorului sistem:

$$\begin{bmatrix} s_{j-L+1} \\ s_{j-L+2} \\ \vdots \\ s_{j-1} \\ s_j \end{bmatrix} = \underbrace{\begin{bmatrix} 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \ddots & \vdots \\ 0 & 0 & 0 & & 1 \\ c_L & c_{L-1} & c_{L-2} & \dots & c_1 \end{bmatrix}}_{L \times L} \begin{bmatrix} s_{j-L} \\ s_{j-L+1} \\ \vdots \\ s_{j-2} \\ s_{j-1} \end{bmatrix}$$

<u>Def.</u>: Polinomul caracteristic pt. un LFSR ca mai sus:

$$P(X) = 1 + c_1 X + c_2 X^2 + \dots + c_L X^L \in \mathbb{Z}_2[X]$$

<u>Def.</u>: Un polinom ireductibil $P(X)$ de $\deg(P) = n$ peste $\mathbb{Z}_2$ s.n. primitiv dacă cel mai mic nr. întreg λ a.î. $P(X)$ divide $X^\lambda + 1$ este:

$\lambda = 2^n - 1$

Pt. un LFSR distingem 4 cazuri:

1) Cazul singular: $c_L = 0$

↳ șirul format prin aplicarea lui M cuvintelor din alfabet devine periodic mai târziu, și nu de la început; avem șiruri periodice cu diferite perioade și dimensiuni

2) Reductibil: $c_L = 1$ și $P(X)$ reductibil peste $\mathbb{Z}_2$
↳ șirul este periodic de la început pt. toate stările inițiale dar are cicli disjuncți și de dim. diferite

3) Ireductibil și neprimitive: $c_L = 1$ și $P(X)$ ired. peste $\mathbb{Z}_2$, dar nu e primitive
↳ șir periodic pt. orice stare inițială
↳ cicli disjuncți, dar cu aceeași dim.

4) Ireductibil și primitiv: $c_L = 1$ și $P(X)$ primitiv
↳ un singur ciclu de lungime maximă $2^n - 1$

1. Cazul $\underline{IV}$
Arătați că polinomul $X^4 + X + 1$ este ired. peste $\mathbb{Z}_2$ și construind LFSR-ul asociat.

Dem.:

$f(x) = x^4 + x + 1 \mod 2$

$\rightarrow$ factori de grad 1: $\left.\begin{matrix} f(0) = 1 \\ f(1) = 1 \end{matrix}\right\}$ nu avem factori de grad 1

$\rightarrow$ factori de grad 2: $h = X^2 + X + 1$ ired.

f nu are factori de grad 2

$\Rightarrow f$ - ireductibil

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{bmatrix}$$

$$v = (a, b, c, d)^T$$

$$Mv = (b, c, d, a+d)$$

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 1 \xrightarrow{M} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = 8 \xrightarrow{M} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 1 \end{bmatrix} = 12 \xrightarrow{M}$$

$$\begin{bmatrix} 0 \\ 1 \\ 1 \\ 1 \end{bmatrix} = 14 \xrightarrow{M} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix} = 15 \xrightarrow{M} \begin{bmatrix} 1 \\ 1 \\ 1 \\ 0 \end{bmatrix} = 7$$

$$\xrightarrow{M} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 11 \xrightarrow{M} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 5 \xrightarrow{M} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 10$$

$$\xrightarrow{M} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 1 \end{bmatrix} = 13 \xrightarrow{M} \begin{bmatrix} 0 \\ 1 \\ 1 \\ 0 \end{bmatrix} = 6 \xrightarrow{M} \begin{bmatrix} 1 \\ 1 \\ 0 \\ 0 \end{bmatrix}$$

$$= 3 \xrightarrow{M} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 1 \end{bmatrix} = 9 \xrightarrow{M} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 4 \xrightarrow{M} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = 2 \xrightarrow{M} \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 1$$

3

2. Cazul II

Polinomul X^4+X^2+1 este red. peste $\mathbb{Z}_2$.
Constr. LFSR asociat.

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}$$

$v = [a, b, c, d]^T$

$Mv = (b, c, d, a+c)$

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix} = 1 \xrightarrow{M} \begin{bmatrix}0\\0\\0\\1\end{bmatrix} = 8 \xrightarrow{M} \begin{bmatrix}0\\0\\1\\0\end{bmatrix} = 4 \xrightarrow{M} \begin{bmatrix}0\\1\\0\\1\end{bmatrix} = 10 -$$

$$\xrightarrow{M} \begin{bmatrix}1\\0\\1\\0\end{bmatrix} = 5 \xrightarrow{M} \begin{bmatrix}0\\1\\0\\0\end{bmatrix} = 2 \xrightarrow{M} \begin{bmatrix}1\\0\\0\\0\end{bmatrix} = 1$$

$\rightarrow$ lungime 6

$$\begin{bmatrix}1\\1\\0\\0\end{bmatrix} = 3 \xrightarrow{M} \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = 9 \xrightarrow{M} \begin{bmatrix}0\\0\\1\\1\end{bmatrix} = 12 \xrightarrow{M} \begin{bmatrix}0\\1\\1\\1\end{bmatrix} = 14 -$$

$$\xrightarrow{M} \begin{bmatrix}1\\1\\1\\1\end{bmatrix} = 15 \xrightarrow{M} \begin{bmatrix}1\\1\\1\\0\end{bmatrix} = 7 \xrightarrow{M} \begin{bmatrix}1\\1\\0\\0\end{bmatrix} = 3$$