Seminar 3 – 12 martie 2024

Ex #1 Arătați că polinomul X^4+X+1 este ireductibil peste $\mathbb{F}_2$ și primitiv construind circuitul liniar asociat (LFSR).

Cazul IV din Curs în care polinomul este primitiv

Dem

Primul lucru pe care îl facem este să verificăm că polinomul este ireductibil. Deoarece lucrăm în $\mathbb{F}_2$ și gradul polinomului este 4, putem face această verificare direct, fără a apela la algoritmi de verificare a ireductibilității.

Dacă notăm $f(x)=x^4+x+1$, observăm că $f(0)=1$, iar $f(1)=0$. Prin urmare, polinomul nu are soluții în $\mathbb{F}_2$, deci nu există factori de gradul 1.

Verificăm dacă avem factori de gradul 2. Știm că singurul polinom ireductibil de grad 2, în $\mathbb{F}_2$, este X^2+X+1. Atunci avem

$$\begin{array}{l|l} X^4+X+1 & X^2+X+1 \\ \cline{2-2} -X^4-X^3-X^2 & X^2-X \\ \hline -X^3-X^2+X+1 & \\ X^3+X^2+X & \\ \hline 2X+1 & \end{array}$$

Deoarece lucrăm în $\mathbb{F}_2$, avem $X^2-X=X^2+X$, iar $2X+1=1$.
Așadar, putem scrie $X^4+X+1=(X^2+X)(X^2+X+1)+1$ sau, altfel, $X^4+X+1=X(X+1)(X^2+X+1)+1$.

Concluzionăm, deci, că polinomul este ireductibil.

Verificăm acum că este primitiv.

Construim matricea asociată:

Din teorie știm că, având polinomul

$$C(X)=1+c_1X+c_2X^2+\ldots+c_LX^L\in\mathbb{F}_2[X]$$

matricea asociată $M\in\mathcal{M}(L;\mathbb{F}_2)$ este dată de

$$M=\begin{bmatrix} 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & 1 \\ c_L & c_{L-1} & c_{L-2} & \cdots & c_1 \end{bmatrix}$$

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

Considerăm un vector $v=(a,b,c,d)^T$ și vedem cum se comportă M atunci când îl aplicăm lui v. Calculăm

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

Cu această acțiune a lui M, considerăm, de exemplu, vectorul $(1,0,0,0)^T$ și vedem cum se comportă la aplicații repetate ale lui M.

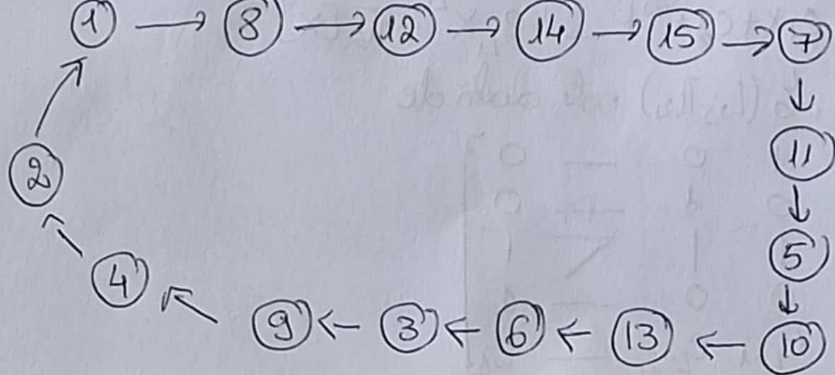
$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=1 \xrightarrow{M} \begin{bmatrix}0\\0\\0\\1\end{bmatrix}=8 \xrightarrow{M} \begin{bmatrix}0\\0\\1\\1\end{bmatrix}=12 \xrightarrow{M} \begin{bmatrix}0\\1\\1\\1\end{bmatrix}=14 \xrightarrow{M} \begin{bmatrix}1\\1\\1\\1\end{bmatrix}=15 \xrightarrow{M}$$

$$\rightarrow \begin{bmatrix}1\\1\\1\\0\end{bmatrix}=7 \xrightarrow{M} \begin{bmatrix}1\\1\\0\\1\end{bmatrix}=11 \xrightarrow{M} \begin{bmatrix}1\\0\\1\\0\end{bmatrix}=5 \xrightarrow{M} \begin{bmatrix}0\\1\\0\\1\end{bmatrix}=10 \xrightarrow{M}$$

$$\rightarrow \begin{bmatrix}1\\0\\1\\1\end{bmatrix}=13 \xrightarrow{M} \begin{bmatrix}0\\1\\1\\0\end{bmatrix}=6 \xrightarrow{M} \begin{bmatrix}1\\1\\0\\0\end{bmatrix}=3 \xrightarrow{M} \begin{bmatrix}1\\0\\0\\1\end{bmatrix}=9 \xrightarrow{M} \begin{bmatrix}0\\0\\1\\0\end{bmatrix}=4 \xrightarrow{M}$$

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

Graful asociat



Observăm că s-a obținut un singur ciclu de lungime maximă $2^4 - 1 = 15$. Așadar putem trage concluzia că polinomul este primitiv.

<u>OBS</u>: Starea zero se duce în ea însăși.

$\square$

$\boxed{\text{Ex \#2}}$ Polinomul $X^4 + X^2 + 1$ este reductibil peste $\mathbb{F}_2$. Construiți circuitul liniar asociat.

Cazul II de la curs.
Polinomul este reductibil

Dem

Prima dată vom verifica că $X^4 + X^2 + 1$ este într-adevăr reductibil. La fel ca în cazul problemei anterioare, se observă ușor că polinomul nu are factori de grad 1.

Calculăm

$$\begin{array}{l|l} X^4 + X^2 + 1 & X^2 + X + 1 \\ \cline{2-2} -X^4 - X^3 - X^2 & X^2 - X + 1 \\ \cline{1-1} -X^3 + 1 & \\ \quad X^3 + X^2 + X & \\ \cline{1-1} \quad X^2 + X + 1 & \\ -X^2 - X - 1 & \\ \cline{1-1} / \quad / \quad / & \end{array}$$

$\overset{\mathbb{F}_2}{\rightsquigarrow} X^2 + X + 1$

Deci $X^4 + X^2 + 1 = (X^2 + X + 1)^2$. Reductibil.

Conform teoriei, construim matricea asociată M. Astfel

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

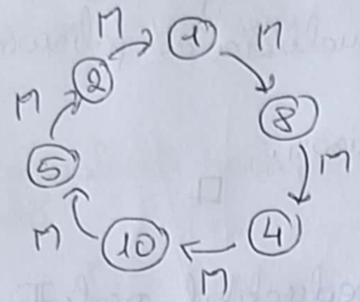
Pe un vector $v = (a, b, c, d)^T$, M acționează astfel

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

Calculăm

$$\begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} = 1 \xrightarrow{M} \begin{bmatrix} 0 \\ 0 \\ 0 \\ 1 \end{bmatrix} = 8 \xrightarrow{M} \begin{bmatrix} 0 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 4 \xrightarrow{M} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 1 \end{bmatrix} = 10 \xrightarrow{M} \begin{bmatrix} 1 \\ 0 \\ 1 \\ 0 \end{bmatrix} = 5 \xrightarrow{M} \begin{bmatrix} 0 \\ 1 \\ 0 \\ 0 \end{bmatrix} = 2 \xrightarrow{M} 1$$

Graful asociat

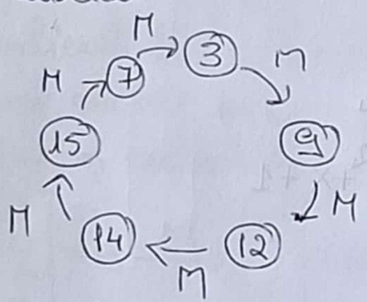


Am găsit un ciclu de lungime 6 descris de $(1,8,4,10,5,2)$.

Luăm acum cel mai mic vector care nu a apărut în ciclul anterior și vedem cum se comportă sub acțiunea lui M. (Mai exact 3).

$$\begin{bmatrix}1\\1\\0\\0\end{bmatrix}=3 \xrightarrow{M} \begin{bmatrix}1\\0\\0\\1\end{bmatrix}=9 \xrightarrow{M} \begin{bmatrix}0\\0\\1\\1\end{bmatrix}=12 \xrightarrow{M} \begin{bmatrix}0\\1\\1\\1\end{bmatrix}=14 \xrightarrow{M} \begin{bmatrix}1\\1\\1\\1\end{bmatrix}=15 \xrightarrow{M} \begin{bmatrix}1\\1\\1\\0\end{bmatrix}=7 \xrightarrow{M} 3$$

Graful asociat

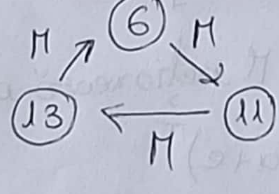


Am mai găsit încă un ciclu de lungime 6 descris, de data aceasta de $(3,9,12,14,15,7)$.

Trecem la următorul cel mai mic vector, adică 6.

$$\begin{bmatrix}0\\1\\1\\0\end{bmatrix}=6 \xrightarrow{M} \begin{bmatrix}1\\1\\0\\1\end{bmatrix}=11 \xrightarrow{M} \begin{bmatrix}1\\0\\1\\1\end{bmatrix}=13 \longrightarrow \begin{bmatrix}0\\1\\1\\0\end{bmatrix}=6$$

Graful asociat



Avem un ciclu de lungime 3 dat de $(6,11,13)$.

Clar, 0 își creează propriul ciclu.

Se poate observa că:

a) am obținut cicli disjuncți de lungimi diferite

b) secvențele sunt periodice de la început pt toate stările inițiale. $\blacksquare$

Ex #3 Construiți graful pentru circuitul liniar dat de polinomul X^3+X+1 pe cuvinte de lungime 4 peste $\mathbb{F}_2$.

Cazul I din curs
Cazul singular când
coef. $c_4 = 0$

Dem

Evident, polinomul este ireductibil. Construim matricea asociată

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

Aplicația lui M pe un vector $v = (a,b,c,d)^T$ este

$$Mv = (b, c, d, b+d)^T$$

Să vedem ce se întâmplă aplicând M pe cuvintele din spațiul nostru:

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

Deci M aplicat lui 1 ne duce în 0, iar din 0 găsim un ciclu care ne va duce mereu în 0.

Continuăm și calculăm

$$\begin{bmatrix}0\\1\\0\\0\end{bmatrix} = 2 \xrightarrow{M} \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = 9 \xrightarrow{M} \begin{bmatrix}0\\0\\1\\1\end{bmatrix} = 12 \xrightarrow{M} \begin{bmatrix}0\\1\\1\\1\end{bmatrix} = 14 \xrightarrow{M} \begin{bmatrix}1\\1\\1\\0\end{bmatrix} = 7 \xrightarrow{M} \begin{bmatrix}1\\1\\0\\1\end{bmatrix} = 11 \xrightarrow{M} \begin{bmatrix}1\\0\\1\\0\end{bmatrix} = 5 \xrightarrow{M} \begin{bmatrix}0\\1\\0\\0\end{bmatrix} = 2$$

Obținem un ciclu de lungime 7 dat de $(2, 9, 12, 14, 7, 11, 5)$.

Mai departe

$$\begin{bmatrix}1\\1\\0\\0\end{bmatrix} = 3 \xrightarrow{M} \begin{bmatrix}1\\0\\0\\1\end{bmatrix} = 9$$ ← mă opresc pentru că 9 este în ciclu

$$\begin{bmatrix}0\\0\\1\\0\end{bmatrix} = 4 \xrightarrow{M} \begin{bmatrix}0\\1\\0\\0\end{bmatrix} = 2$$ ← mă opresc pentru că 2 este în ciclu

$$\begin{bmatrix}0\\1\\1\\0\end{bmatrix} = 6 \xrightarrow{M} \begin{bmatrix}1\\1\\0\\1\end{bmatrix} = 11$$ ← mă opresc pentru că 11 este în ciclu

$\begin{bmatrix}0\\0\\0\\1\end{bmatrix}=8 \xrightarrow{M} \begin{bmatrix}0\\0\\1\\1\end{bmatrix}=12$ ← mă opresc pt că 12 este în ciclu

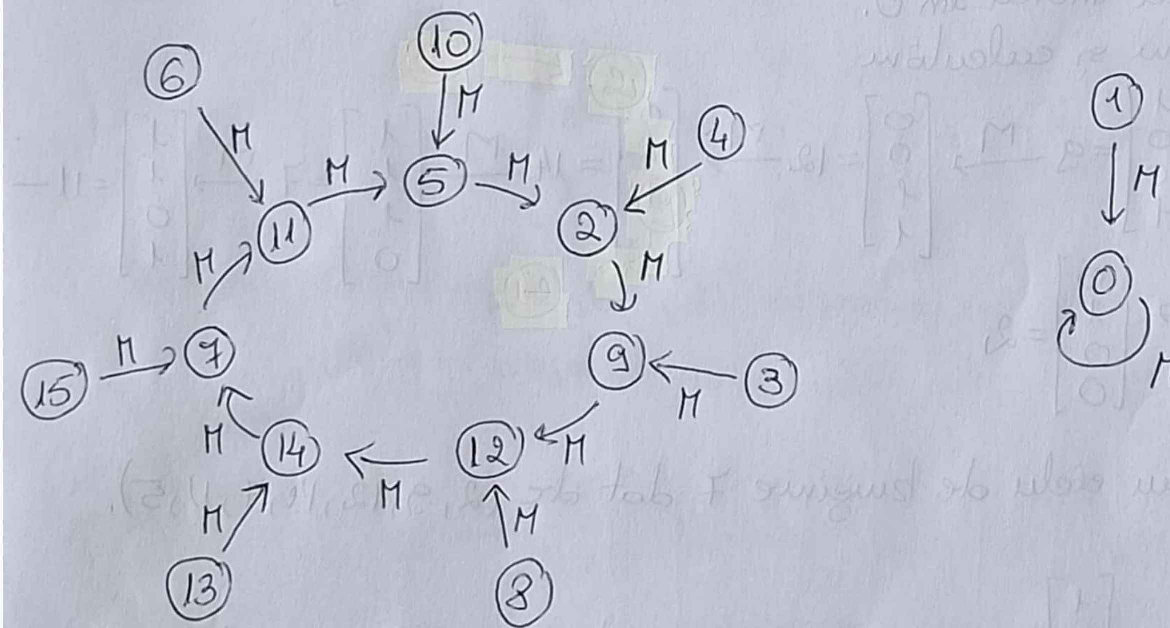
$\begin{bmatrix}0\\1\\0\\1\end{bmatrix}=10 \xrightarrow{M} \begin{bmatrix}1\\0\\1\\0\end{bmatrix}=5$ ← mă opresc pt că 5 este în ciclu

$\begin{bmatrix}1\\0\\1\\1\end{bmatrix}=13 \xrightarrow{M} \begin{bmatrix}0\\1\\1\\1\end{bmatrix}=14$ ← mă opresc pt că 14 este în ciclu

$\begin{bmatrix}1\\1\\1\\1\end{bmatrix}=15 \xrightarrow{M} \begin{bmatrix}1\\1\\1\\0\end{bmatrix}=7$ ← mă opresc pt că 7 este în ciclu

Observăm că pe lângă ciclul de lungime 7 am mai găsit alte 7 extremități care se duc în nodurile grafului nostru ciclic.

Graful asociat este



Ce se poate vedea este că secvența nu devine periodică de la început, ci mai târziu. Mai mult, există secvențe periodice cu perioade diferite și dimensiuni diferite.

□

Cazul III din curs
Polinom ireductibil, dar care NU este primitiv

Ex #4 Construiți graful circuitului liniar dat de polinomul $x^4+x^3+x^2+1$ pe cuvinte de lungime 4 peste $\mathbb{F}_2$. Observați că polinomul este ireductibil, dar nu este primitiv

Dem

Verificăm, prima dată, ireductibilitatea.

Considerăm funcția polinomială $f(x)=x^4+x^3+x^2+1$. Evident, cum $f(0)=f(1)=1\neq 0$, deducem că f nu are factori de gradul 1.

Calculăm

$$\begin{array}{l|l} x^4+x^3+x^2+1 & x^2+x+1 \\ \cline{2-2} -x^4-x^3-x^2 & x^2 \\ \hline \quad = \quad = \quad = \quad 1 & \end{array}$$

Deci $f(x)=x^4+x^3+x^2+1=x^2(x^2+x+1)+1$, de unde rezultă că nu avem factori de gradul 2 și, deci, polinomul este ireductibil.

Pentru a verifica dacă f este primitiv, vom rula circuitul liniar. Am văzut, într-o problemă anterioară, că dacă f ar fi primitiv, ar trebui să obținem un ciclu de lungime maximă $2^4-1=15$.

Construim întâi matricea asociată.

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

Aplicăm M lui $v=(a,b,c,d)^T$ și avem

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

Calculăm

$$\begin{bmatrix}1\\0\\0\\0\end{bmatrix}=1 \xrightarrow{M} \begin{bmatrix}0\\0\\0\\1\end{bmatrix}=8 \xrightarrow{M} \begin{bmatrix}0\\0\\1\\1\end{bmatrix}=12 \xrightarrow{M} \begin{bmatrix}0\\1\\1\\0\end{bmatrix}=6 \xrightarrow{M} \begin{bmatrix}1\\1\\0\\0\end{bmatrix}=3 \xrightarrow{M} \begin{bmatrix}1\\0\\0\\0\end{bmatrix}=1$$

1) Ciclu de lungime 5 dat de $(1,8,12,6,3)$

$$\begin{bmatrix}0\\1\\0\\0\end{bmatrix}=2 \xrightarrow{M} \begin{bmatrix}1\\0\\0\\1\end{bmatrix}=9 \xrightarrow{M} \begin{bmatrix}0\\0\\1\\0\end{bmatrix}=4 \xrightarrow{M} \begin{bmatrix}0\\1\\0\\1\end{bmatrix}=10 \xrightarrow{M} \begin{bmatrix}1\\0\\1\\0\end{bmatrix}=5 \xrightarrow{M} \begin{bmatrix}0\\1\\0\\0\end{bmatrix}=2$$

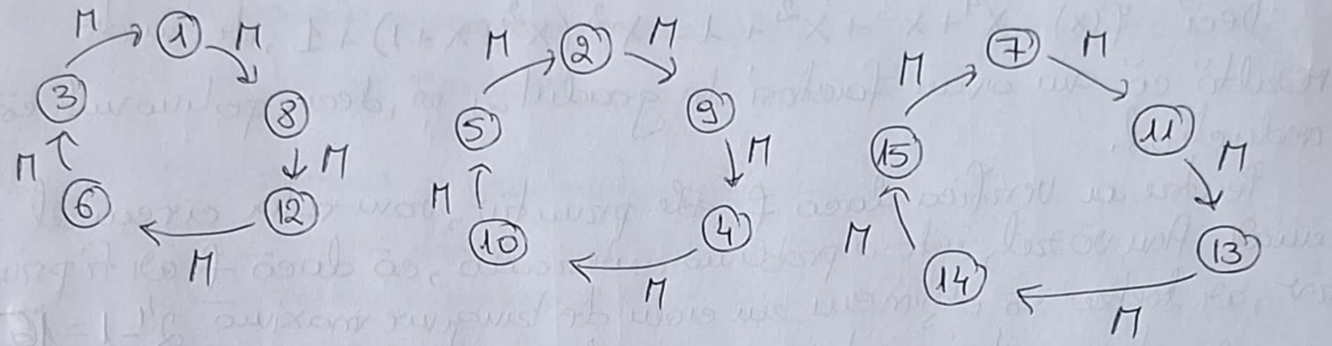
2) Ciclu de lungime 5 dat de $(2,9,4,10,5)$.

$$\begin{bmatrix}1\\1\\1\\0\end{bmatrix}=7 \xrightarrow{M} \begin{bmatrix}1\\1\\0\\1\end{bmatrix}=11 \xrightarrow{M} \begin{bmatrix}1\\0\\1\\1\end{bmatrix}=13 \xrightarrow{M} \begin{bmatrix}0\\1\\1\\1\end{bmatrix}=14 \xrightarrow{M} \begin{bmatrix}1\\1\\1\\1\end{bmatrix}=15 \xrightarrow{M} \begin{bmatrix}1\\1\\1\\0\end{bmatrix}=7$$

3) Ciclu de lungime 5 dat de $(7, 11, 13, 14, 15)$.

Observăm că s-au creat cicli disjuncți de aceeași lungime. Așadar, concluzionăm că polinomul NU este primitiv.

Evident, mai avem și ciclul trivial de lungime 1 dat de 0.



$\square$

Q: De ce mergem până la $15 = 1111_{(2)}$?
A: Deoarece lucrăm cu cuvinte/vectori de lungime 4 cu intrări în $\{0,1\}$. Câți astfel de vectori avem? R: 15
Avem 15 vectori nenuli $(2^4 - 1)$ (16 cu cel nul)

Avem n variabile de stare. Dacă luăm valori binare, numărul tuturor stărilor posibile este 2^n.

<u>OBS</u> LFSR poate avea cel mult $2^n - 1$ stări unice deoarece starea nulă se exclude.

Q: De ce alegem 1 ca vector de start?
A: Pt că 0 nu ne dă nimic interesant, așa că îl luăm pe primul nenul pentru a vedea ce se întâmplă. Evident, puteți începe de unde vreți. Important este să trataţi toate cazurile.

Q: De ce alegem, la următorul pas, următorul cel mai mic vector?
A: Alegere personală. Pentru ușurință și ordine.

Q: De ce vrem să fie ireductibil și primitiv?
A: Ca LFSR să fie maxim.

Q: Pt ce avem nevoie de LFSR?
A: Pt a genera șiruri de biți pseudo-aleatoare.
„Because of this, we would ideally not want this repeating cycle behaviour to occur."