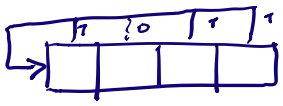
Polynomials and Constructing LFSRs

1. Construct a LFSR(of length 4) with generating polynomial $f(x) = x^4 + x^3 + x + 1$. Remark $f(x)$ is reducible. For different initial states generate sequences of states. Study the complete cyclic structure of that LFSR.
2. Recollect Euclidean Algorithm for polynomials modulo 2. Compute $\gcd(x^4 + x^2 + x + 1, x^3 + 1)$.
3. Recollect Extended Euclidean Algorithm for polynomials modulo 2. Compute polynomials $A = A(x)$ and $B = B(x)$ such that
$$A \times (x^4 + x^2 + x + 1) + B \times (x^3 + 1) = \gcd(x^4 + x^2 + x + 1, x^3 + 1).$$
4. Apply the first test(by computing gcd's) to prove $x^5 + x^3 + 1$ is irreducible.
5. Apply Berlekamp test to prove $x^5 + x^2 + 1$ is irreducible.
6. Apply Berlekamp test to factor the polynomial $x^5 + x + 1$.
7. Prove x^5+x^2+1, x^5+x^3+1 are primitive polynomials. Construct a maximum period LFSR of length 5.
8. If you like the topic, then prove $x^{127} + x + 1$ is primitive. That requires programming one of the tests.

1. LFSR



$f(x) = x^4 + 1 \cdot x^3 + 0 \cdot x^2 + 1 \cdot x + 1$

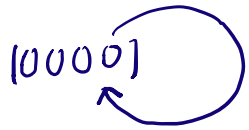
c_1 c_2 c_3 c_4

possible states is $2^4 = 16$

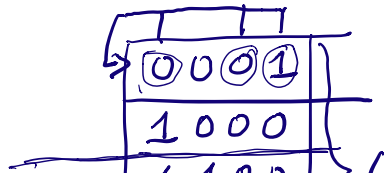
$f(x)$ reducible $= (x+1)(x^3+1) = (x+1)^2 \cdot (x^2+x+1)$

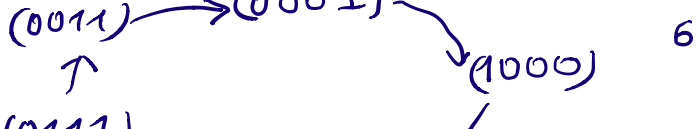
$\Rightarrow$ expect a lot of cycles of diff. length.

1



1





6

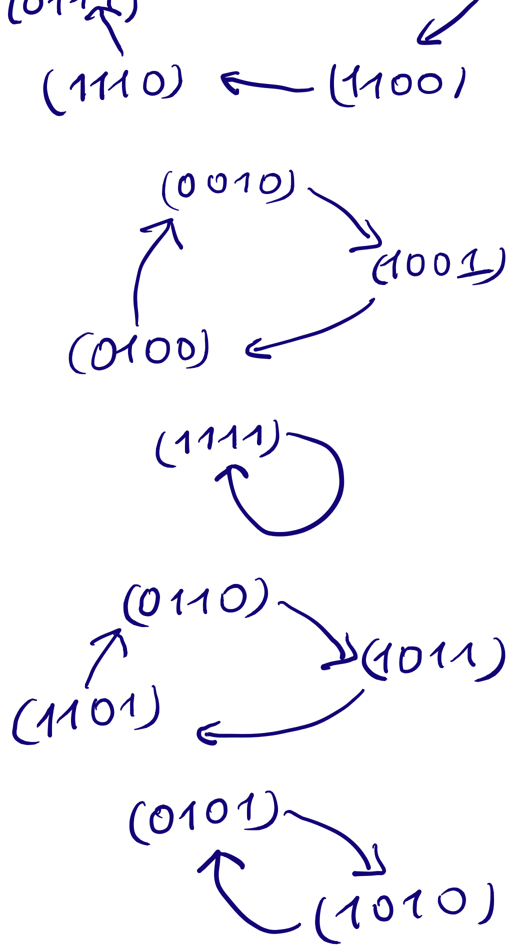
1 1 0 0
1 1 1 0
0 1 1 1
0 0 1 1 } 6
0 0 0 1

0 0 1 0
1 0 0 1 } 3
0 1 0 0
0 0 1 0

1 1 1 1 } 1
1 1 1 1

0 1 1 0
1 0 1 1 } 3
1 1 0 1
0 1 1 0

0 1 0 1 } 2
1 0 1 0
0 1 0 1



3

1

3

2

16

2. Euclid Algorithm for Polynomials.

$a_0 = a_0(x)$, $a_1 = a_1(x)$ $\quad gcd(a_0, a_1) = ?$

$a_0 = q_1 \cdot a_1 + a_2$, $\quad \deg a_2 < \deg a_1$.

(q_1 ↑ quotient, a_2 ↑ remainder)

$a_1 = q_2 \cdot a_2 + a_3$, $\quad \deg a_3 < \deg a_2$

...

$a_{s-1} = q_s \underline{\underline{a_s}} + a_{s+1}$ where $a_{s+1} = 0$

$\Rightarrow gcd(a_0, a_1) = a_s$

compute $gcd(x^4 + x^2 + x + 1, x^3 + 1)$, with $a_0 = x^4+x^2+x+1$, $a_1 = x^3+1$

$a_0 = x^4 + x^2 + x + 1 \;\; \lfloor\; x^3 + 1 = a_1$

$x^4 + x \qquad\qquad\qquad\;\; x$

$a_2 = x^2+1$

$x^3+1 \;\big|\; x^2+1$

$x^3+x \quad\quad x$

$a_3 = x+1$

$x^2+1 \;\big|\; x+1$

$x^2+x \quad\quad x+1$

$x+1$

$x+1$

$a_4 = 0$

$\Rightarrow \quad a_3 = x+1$ is gcd.

3. EEA $\quad a_0 = a_0(x)$, $a_1 = a_1(x)$

compute u, v s.t. $\boxed{u \cdot a_0 + v \cdot a_1 = \gcd(a_0, a_1)}$

i	u_i	v_i	a_i	q_i
0	1	0	a_0	—
1	0	1	a_1	$q_1 = \left\lfloor \frac{a_0}{a_1} \right\rfloor$
2	1	q_1	$a_0 + q_1 a_1 = a_2$	$q_2 = \left\lfloor \frac{a_1}{a_2} \right\rfloor$
3	q_2	$1 + q_1 \cdot q_2$	$a_1 + q_2 a_2 = a_3$	

$u_i a_0 + v_i \cdot a_1 = a_i$, $\quad i = s$

u_s	v_s	$a_s = \gcd$

$a_{s+1} = 0$

$\Rightarrow \quad \boxed{u_s \cdot a_0 + v_s \cdot a_1 = a_s = \gcd(a_0, a_1)}$

example 1) $a_0 = x^4+x^2+x+1$

$a_1 = x^3+1$

i	u_i	v_i	a_i	q_i
0	1	0	$a_0 = x^4+x^2+x+1$	—
1	0	1	$a_1 = x^3+1$	$q_1 = x$
2	1	x	$a_2 = x^2+1$	x
3	x	x^2+1	$a_3 = x+1$	$x+1$
4	x^2+x+1	x^3+x^2+1	$a_4 = 0$	

$a_4 = 0 \Rightarrow a_3 = x+1$

$$x\cdot(x^4+x^2+x+1)+(x^2+1)(x^3+1) = x+1$$

$\parallel$ u $\qquad$ $\parallel$ v

---

4. $p(x) = x^5+x^3+1$ irreducible ?

$n = 5$, a_1, q_0, $1 \le s \le 5/2 \Rightarrow s = 1, 2$

$\gcd(x^2+x,\ x^5+x^3+1)$

$x^5+x^3+1 \mid x^2+x$

$x^5+x^4 \qquad x^3+x^2$

x^4+x^3+1

x^4+x^3

$a_2 = 1 \Rightarrow \gcd = 1$

$\gcd(x^4+x,\ x^5+x^3+1)$

$q_0 = x^5+x^3+1 \mid x^4+x = a_1$

$x^5+x^2 \qquad x$

$a_2 = x^3+x^2+1$

$x^4+x \mid x^3+x^2+1$

$x^4+x^3+x \qquad x+1$

x^3

x^3+x^2+1

$a_3 = x^2+1$

$x^3+x^2+1 \mid x^2+1$

$x^3+x \qquad x+1$

x^2+x+1

x^2+1

$a_4 = x$

$x^2+1 \mid x$

$x^2 \qquad x$

$a_5 = 1 \Rightarrow \gcd = 1.$

$\Rightarrow$ $p(x)$ irreducible.

5. $f(x) = x^5 + x^2 + 1$

$\gcd(f, f') \stackrel{?}{=} 1$ $\quad f' = 5 \cdot x^4 + 2 \cdot x + 0 = x^4$

$\Rightarrow \gcd = 1 \Rightarrow f$ without multiple roots

B

$x^{2 \cdot 0} \equiv 1 \mod f$

$x^{2 \cdot 1} \equiv x^2$

$x^{2 \cdot 2} \equiv x^4$

$x^{2 \cdot 3} \equiv x^6 \equiv x^3 + x$

$x^{2 \cdot 4} \equiv x^5 + x^3 \equiv x^3 + x^2 + 1$

$B + I =$

x^0	x^1	x^2	x^3	x^4	
0	0	0	0	0	
0	1	1	0	0	lin. independent
0	0	1	0	1	
0	1	0	0	0	$(y_0 \dots y_4) \cdot (B + I) = 0$
1	0	1	1	1	

$\operatorname{rank}(B + I) = 4$ $\quad$ # solutions $2^{5-4} = 2$

$\Rightarrow$ only trivial solutions

(00000)

(10000)

$\Rightarrow f(x)$ irreducible.

6. $f = x^5 + x + 1$, $\quad f' = x^4 \quad \gcd(f, f') = 1$

$\Rightarrow f$ without multiple roots

B

$x^{2 \cdot 0} \equiv 1 \mod f$

$x^{2 \cdot 1} \equiv x^2$

$x^{2 \cdot 2} \equiv x^4$

$x^{2 \cdot 3} \equiv x^6 \equiv x^2 + x$

$x^{2 \cdot 4} \equiv x^4 + x^3$

$x^6 \mid x^5 + x + 1$

$x^6 + x^2 + x \quad x$

$x^2 + x$

$x^6 = x^5 \cdot x \equiv (x + 1) x \equiv x^2 + x$

$x^5 \equiv x + 1 \mod x^5 + x + 1$

$B+I = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix} \begin{matrix} \leftarrow \\ \\ \\ \leftarrow \\ \leftarrow \end{matrix}$

$(01011) \cdot (B+I) = (00000)$

solutions to $(y_0 \dots y_4) \cdot (B+I) = 0$

solution (non-trivial) is (01011)

$\Rightarrow$ polynomial $g = x + x^3 + x^4$

$\gcd(x^5+x+1, x^4+x^3+x) = x^3+x^2+1$

$f = (x^3+x^2+1)(x^2+x+1)$

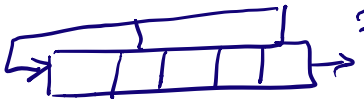
$= x^5 + x^4 + x^2$
$\quad x^4 + x^3 + x$
$\quad x^3 + x^2 + 1$

$= x^5 + x + 1 \Rightarrow$ f reducible
factorization is found.

7. $P_1 = x^5 + x^3 + 1$ irreducible

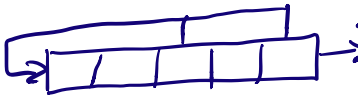
$P_2 = x^5 + x^2 + 1$ $\Rightarrow$ primitive

$2^5 - 1 = 31$ prime



min. period if initial state $\neq 0$.

P_1



P_2

8. $x^{127} + x + 1$ irred. $\Rightarrow$ prim.

$2^{127} - 1$ prime