LFSR cyclic structure

Theorem.

1. A $n \times n$ matrix and its characteristic polynomial $f_A(x)$ is irreducible

$$\Rightarrow \quad m_{z,A}(x) = m_A(x) = f_A(x)$$

(z: non-zero n-bit vector)

2. LFSR defined by polynomial $f(x)$ irreducible, $f(x) \neq x$.
$\deg f = n$

z any non-zero initial state of the LFSR

$\Rightarrow$ LFSR generates a pure periodic sequence of min. period N
= period of $f(x)$

3. $f(x)$ irreducible polynomial of degree n
$f(x) \neq x$ of period N. Then

$$N \mid 2^n - 1.$$

Proof.

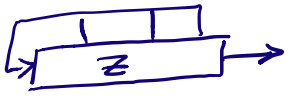
1. $m_{z,A}(x) \mid m_A(x) \mid f_A(x)$

if $f_A(x)$ irreducible $\Rightarrow$

$$m_{z,A}(x) = m_A(x) = f_A(x).$$

2. z non-zero initial state of the LFSR.

LFSR sequence on this state is of minimum period t.



$\Leftrightarrow \quad z \cdot A^t = z$, A companion matrix to $f(x)$
t min.

$\Leftrightarrow \quad z(A^t + \underset{\uparrow}{I}) = 0$ - matrix

unity matrix of size $n \times n$

t min.

$\Leftrightarrow \quad m_{z,A}^{(x)} \,/\, x^t + 1 \quad \Leftrightarrow \quad m_{z,A} = m_A = p_A = p$

t min.

$p(x) \,/\, x^t + 1$, t min.

$\Leftrightarrow$ $t = N$ period of $p(x)$.

3. all non-zero n-bit vectors $2^n - 1$

split into subsets

$\{z_1, z_1 \cdot A, \dots, z_1 \cdot A^{N-1}\} \cup \{z_2, z_2 A, \dots, z_2 \cdot A^{N-1}\} \cup \dots$

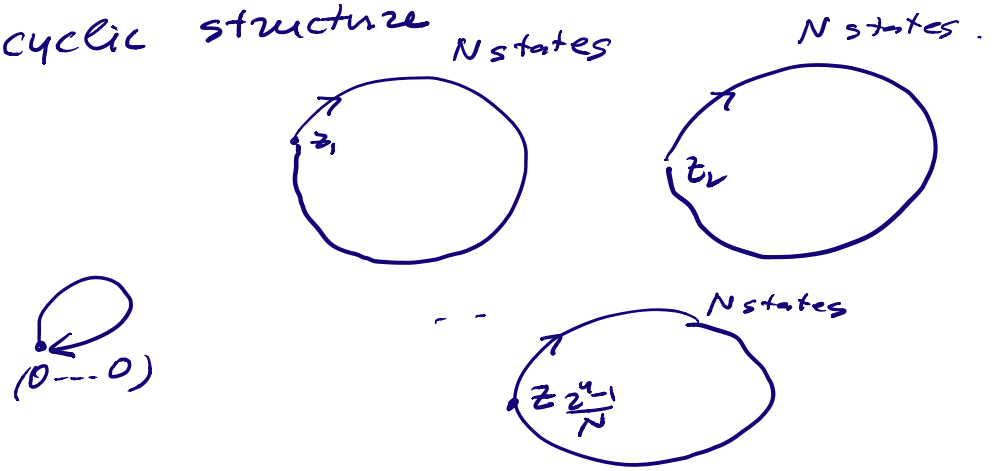
all such subsets are disjoint

$z_2 A^i = z_1 \cdot A^j \Rightarrow z_2 = z_1 A^{j-i} \Rightarrow z_2$ in the first set.

$\Rightarrow \quad N \,/\, 2^n - 1$

LFSR with irreducible polynomial of period N

cyclic structure



Important definition.

irreducible polynomial $p(x) \neq x$ of period $2^n - 1$

$\Rightarrow$ $p(x)$ is called primitive

primitive polynomials really exist.

How to find irreducible and primitive polynomials.

take a polynomial and test it if irreducible (primitive)

GCD-test

TH. $f(x)$ polynomial of degree n.
Then $f(x)$ irreducible
$\Leftrightarrow \gcd(f(x), x^{2^s}+x) = 1$
for every $1 \le s \le n/2$

based on Lemma.

$$x^{2^s}+x = \prod g(x)$$

$g(x)$ irreducible
$\deg g(x) \mid s$.

e.g. $s = 1, 2, 3$

$x^2+x = x(x+1)$ over poly. irreducible of degree 1.

$x^4+x = x(x+1)(x^2+x+1)$
↑ over irr. of degree 2.

$x^8+x = x(x+1)(x^3+x+1)(x^3+x^2+1)$
↑ over irr. of degree 3.

Examples. $f(x) = x^5+x+1$, $n=5$

$1 \le s \le 5/2 \Rightarrow s = 1, 2$.

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

Euclidean algorithm

apply Euclid Algorithm:

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

x^5+x^4 — x^3+x^2+x+1

x^4+x+1

x^4+x^3

x^3+x+1

x^3+x^2

x^2+x+1

x^2+x

1 remainder

$\Rightarrow$ gcd = 1.

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

$x^5+x+1 \mid x^4+x$

x^5+x^2 — x

x^2+x+1 remainder

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

$x^4+x^3+x^2$ — x^2+x

x^3+x^2+x

x^3+x^2+x

0 remainder

$\Rightarrow$ gcd $= x^2+x+1$ $\Rightarrow$ 1) x^5+x+1 reducible

2) $x^5+x+1 = (x^2+x+1)(x^3+x^2+1)$ factorization.

apply the test to

$$P(x) = x^6+x^5+x^4+x^3+x^2+x+1$$

$n=6 \Rightarrow s=1,2,3$

$\gcd(x^2+x, P) = 1$

$\gcd(x^4+x, P) = 1$

$\gcd(x^8+x, P) = P$

$\Rightarrow$ $P(x)$ is reducible

the factorization is not provided.

Efficiency of the test.

need to compute $\gcd(x^{2^s}+x, P(x))$

↑ of degree $2^s \le 2^{n/2}$

use two tricks

1) $\gcd(g, f) = \gcd(g \bmod f, f)$

2) $x^{2^s} + x \equiv u_s \bmod f(x)$

identity

$$x^{2^j} + x = (x^{2^{j-1}} + x)^2 + x^2 + x$$

then consider mod $f(x)$

$$u_s \equiv u_{s-1}^2 + x^2 + x \bmod f.$$

$\Rightarrow$ in order to compute $\gcd(x^{2^s} + x, f) =$
$= \gcd(u_s, f)$ By using

$\Rightarrow$ test is efficient.

Another test

$f(x)$ polynomial of degree n

$$f(x) = g_1^{\ell_1} \cdots g_r^{\ell_r}$$

where $g_1, \ldots, g_r$ distinct irreducible polynomials and $\ell_1 \geq 1, \ldots, \ell_r \geq 1$.

say $f(x)$ is without multiple roots if $\ell_1 = \ldots = \ell_r = 1$.

Lemma. $f(x)$ is without multiple roots $\Leftrightarrow \gcd(f, f') = 1$.

f' ↑ formal derivative of f.

$$f(x) = x^n + c_1 x^{n-1} + \ldots + c_n$$
$$f'(x) = n \cdot x^{n-1} + c_1(n-1) \cdot x^{n-2} + \ldots + c_{n-1}$$

Theorem (Berlekamp test)

$f(x)$ polynomial of degree n without multiple roots. Consider the equation

$$g^2+g \equiv 0 \bmod f(x) \qquad (*)$$

in polynomials $g(x)$ of degree $< n$. Then

1. $f(x)$ irreducible $\Leftrightarrow$ $g = 0, 1$ only solutions to $(*)$.

2. $g \neq 0, 1$ solution to $(*)$, then $R = \gcd(f, g)$ is non-trivial factor ($\neq 1, R$) of $f(x)$.

Proof in the Lecture Notes.

$(*)$ equivalent to a system of linear equations.

$$g(x) = \sum_{i=0}^{n-1} y_i x^i, \quad y_i \text{ unknowns}$$

Let $$x^{2i} \equiv \sum_{j=0}^{n-1} b_{ij} x^j \bmod f(x)$$

$i = 0, \dots, n-1$.

matrix $B = (b_{ij})_{0 \le i,j \le n-1}$

$$(a+b)^2 = a^2 + b^2 \bmod 2$$

$y_i = 0$ or 1, $y_i^2 = y_i$

$$g^2+g = \left(\sum_i y_i x^i\right)^2 + \left(\sum_i y_i x^i\right) =$$

$$= \sum_i y_i x^{2i} + \sum_i y_i x^i$$

$$\equiv \sum_i y_i \sum_j b_{ij} x^j + \sum_j y_j x^j \bmod f(x)$$

$$\equiv \sum_{j=0}^{n-1} \left(y_j + \sum_{i=0}^{n-1} y_i b_{ij}\right) x^j \equiv 0$$

$\deg \le n-1$

$\deg f = n$

$\Leftrightarrow \quad y_j + \sum_{i=0}^{n-1} y_i b_{ij} = 0 \qquad j = 0, 1, \ldots, n-1$

in matrix form

$$(y_0\, y_1 \ldots y_{n-1}) \left(B + \underset{\uparrow}{I} \right) = 0$$

unity matrix of size $n \times n$ $\begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix}$

system of linear equations.

two solutions are $(00\ldots0)$, $g=0$; $(10\ldots0)$, $g=1$

according to the Theorem

$f(x)$ is irred. $\Leftrightarrow$ only two solutions.

Example. $f(x) = x^4 + x^3 + 1$.

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

$\gcd(x^2, x^4 + x^3 + 1) \overset{\text{mod } 2}{=} 1 \Rightarrow f(x)$ without multiple roots.

construct matrix B:

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

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

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

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

$$B = \begin{array}{c} \begin{matrix} x^0 & x^1 & x^2 & x^3 \end{matrix} \\ \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 \end{pmatrix} \end{array}$$

$$B + I = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \end{pmatrix} \Big\} \text{ lin. indep. rows}$$

$\begin{pmatrix} 1 & 1 & 1 & 0 \end{pmatrix}$

$\text{rank}(B+I) = 3$ $\quad (y_0 y_1 y_2 y_3)(B+I) = (0000)$

solutions is $2^{4-\text{rank}} = 2$ $\quad \begin{matrix}(0000)\\(1000)\end{matrix}$ trivial sol.

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

For factoring $p = x^6+x^5+x^4+x^3+x^2+x+1$ reducible

construct B

$x^{2\cdot 0} \bmod p \equiv 1$

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

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

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

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

$x^{2\cdot 5} \equiv x^3$

x^8 by p / x^7+1

$x^8 \equiv x \bmod p$

$x^8 \,|\, x^6+x^5+x^4+\cdots+1$

$x^8 + \cdots x^2$

x^2

$x^0\ x^1\ x^2\ x^3\ x^4\ x^5$

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

$\text{rank}(B+I) = 4$ $\quad$ # solutions to $y_0 y_1 \cdots y_5$ is $2^{6-\text{rank}} = 2^2 = 4$

there are non-trivial solutions.

$y_0 y_1 \cdots y_5 = 011010$

$\Rightarrow$ $g = x+x^2+x^4$

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

factor $p = (x^3+x+1)(x^3+x^2+1)$

Test for a primitive polynomial.

Lemma. $2^n - 1 = \prod_{i=1}^{z} q_i^{\ell_i}$

$q_1, \dots, q_z$ distinct primes

$\ell_i \geq 1$.

$P(x)$ irreducible polynomial of degree n.

$P(x)$ is primitive

$\Leftrightarrow \quad x^{\frac{2^n-1}{q_i}} \not\equiv 1 \bmod P(x)$

$i = 1, \dots, z$.

Example. $P(x) = x^4 + x^3 + 1$ irreducible

$2^4 - 1 = 15 = 3 \cdot 5$

$$x^{\frac{2^4-1}{3}} \equiv x^5 \equiv x^3 + x + 1 \not\equiv 1 \bmod P(x).$$

$$x^5 \equiv x^4 \cdot x = (x^3+1) \cdot x \equiv x^4 + x \equiv x^3 + x + 1$$

$$x^{\frac{2^4-1}{5}} \equiv x^3 \not\equiv 1 \bmod P(x)$$

$\Rightarrow P(x)$ primitive.

To implement the test compute

$x^a \bmod P(x)$ a may be very large.

$= \underbrace{x \cdot x \cdots x}_{a \text{ times}}$

Binary exponentiation method.

$a = 2^e + a_{e-1} 2^{e-1} + \dots + a_0 \qquad a_i \in \{0, 2\}$

Binary expansion of a.

$$x^a \equiv \left(\dots \left(\left(x^2 \cdot x^{a_{e-1}} \right)^2 \cdot x^{a_{e-2}} \right)^2 \dots \right)^2 \cdot x^{a_0}$$

x^2 if $a_{l-1}=0$

$x^2 \cdot x$ $\quad a_{l-1}=1$

squarings mod $P(x)$ is $\quad l \approx \log_2 a$

multipl. by x mod $P(x)$ is at most l
(on the average $\approx \frac{l}{2}$)

2^n-1 prime itself. Mersenne prime.

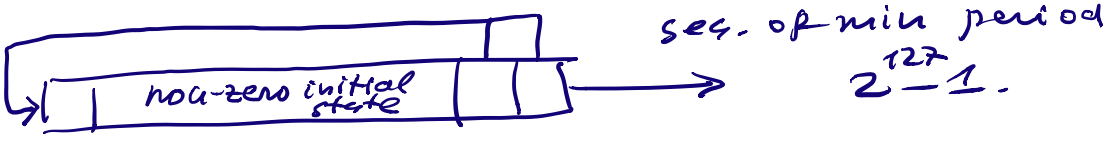
$n = 3, 7, 31, 127, \ldots$

2^n-1 Mersenne prime and $P(x)$ of degree n irreducible, then $P(x)$ is primitive.

$$x^{\frac{2^n-1}{2^n-1}} \equiv x \not\equiv 1 \bmod P(x)$$

e.g. $2^{127}-1$ prime, $x^{127}+x+1$ irr.

$\Rightarrow$ primitive.



Boolean Functions.

$$f : \{0, 1, \ldots, 2^n-1\} \to \{0,1\}$$

$$X = x_1 \cdot 2^{n-1} + x_2 \cdot 2^{n-2} + \ldots + x_n \qquad x_i \in \{0,1\}$$

$$f(X) = f(x_1 x_2 \ldots x_n)$$

$X \le 2^n-1$

$X \ge 0$

Truth table (table of values of $P(x)$), $n=3$

X	$x_1\ x_2\ x_3$	$f(x_1x_2x_3)=P(x)$

0	0	0	0	0
1	0	0	1	0
2	0	1	0	0
3	0	1	1	1
4	1	0	0	1
5	1	0	1	0
6	1	1	0	0
7	1	1	1	1

ANF (Algebraic Normal Form)

$$f(x_1 x_2 \cdots x_n) = \sum_{\{i_1 i_2 \cdots i_t\} \subseteq \{12\cdots n\}} c_{\{i_1 i_2 \cdots i_t\}} \, x_{i_1} x_{i_2} \cdots x_{i_t}, \quad c \in \{0,1\}$$

including $c_\emptyset$

e.g. $f(x_1 x_2 x_3) = x_1 x_2 x_3 + x_1 x_2 + x_1 x_3 + x_2 x_3 + x_1$

$f(000) = 0$

$\vdots$

$f(111) = 1$