LFSRs: Mathematical properties

Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Order of C = longest period

Theorem

Let $ord(C) = \ell$ for C the state-update matrix of an LFSR.
The longest period generated by this LFSR is ℓ.
State $S_0 = (0\,0\,\ldots 0\,1)$ is a starting state of maximal period.

Proof.

Let S_i be the i-th state, starting from S_0, thus $S_i = (\underbrace{0\,0\,\ldots 0}_{n-1-i} 1 * \cdots *)$.

Order of C = longest period

Theorem

Let $ord(C) = \ell$ for C the state-update matrix of an LFSR.
The longest period generated by this LFSR is ℓ.
State $S_0 = (0\,0\,\ldots\,0\,1)$ is a starting state of maximal period.

Proof.

Let S_i be the i-th state, starting from S_0, thus $S_i = (\underbrace{0\,0\,\ldots\,0}_{n-1-i}1 * \cdots *)$.

Assume on the contrary that $S_i = S_{r+i}$ for all $i \geq 0$ and $0 < r < \ell$.
Then $S_i = S_{r+i} = S_i C^r$ and $C^r \neq I$ (by the definition of order).
Make an $n \times n$ matrix S of the starting states to get

$$S = \begin{pmatrix} \cdots & S_0 & \cdots \\ \cdots & S_1 & \cdots \\ & \vdots & \\ \cdots & S_{n-1} & \cdots \end{pmatrix} = \begin{pmatrix} \cdots & S_0 & \cdots \\ \cdots & S_1 & \cdots \\ & \vdots & \\ \cdots & S_{n-1} & \cdots \end{pmatrix} C^r = S \cdot C^r$$

Order of C = longest period

Theorem

Let $ord(C) = \ell$ for C the state-update matrix of an LFSR.
The longest period generated by this LFSR is ℓ.
State $S_0 = (0\,0\,\ldots 0\,1)$ is a starting state of maximal period.

Proof.

Let S_i be the i-th state, starting from S_0, thus $S_i = (\underbrace{0\,0\ldots 0}_{n-1-i}1 * \cdots *)$.

Assume on the contrary that $S_i = S_{r+i}$ for all $i \geq 0$ and $0 < r < \ell$.
Then $S_i = S_{r+i} = S_i C^r$ and $C^r \neq I$ (by the definition of order).
Make an $n \times n$ matrix S of the starting states to get

$$S = \begin{pmatrix} \cdots & S_0 & \cdots \\ \cdots & S_1 & \cdots \\ & \vdots & \\ \cdots & S_{n-1} & \cdots \end{pmatrix} = \begin{pmatrix} \cdots & S_0 & \cdots \\ \cdots & S_1 & \cdots \\ & \vdots & \\ \cdots & S_{n-1} & \cdots \end{pmatrix} C^r = S \cdot C^r$$

S is invertible (the S_i are linearly independent).

Order of C = longest period

Theorem

Let $ord(C) = \ell$ for C the state-update matrix of an LFSR.
The longest period generated by this LFSR is ℓ.
State $S_0 = (0\,0\,\ldots 0\,1)$ is a starting state of maximal period.

Proof.

Let S_i be the i-th state, starting from S_0, thus $S_i = (\underbrace{0\,0\,\ldots 0}_{n-1-i}\,1 * \cdots *)$.

Assume on the contrary that $S_i = S_{r+i}$ for all $i \geq 0$ and $0 < r < \ell$.
Then $S_i = S_{r+i} = S_i C^r$ and $C^r \neq I$ (by the definition of order).
Make an $n \times n$ matrix S of the starting states to get

$$S = \begin{pmatrix} \cdots & S_0 & \cdots \\ \cdots & S_1 & \cdots \\ & \vdots & \\ \cdots & S_{n-1} & \cdots \end{pmatrix} = \begin{pmatrix} \cdots & S_0 & \cdots \\ \cdots & S_1 & \cdots \\ & \vdots & \\ \cdots & S_{n-1} & \cdots \end{pmatrix} C^r = S \cdot C^r$$

S is invertible (the S_i are linearly independent).
Then $I = S^{-1}S = S^{-1}SC^r = C^r$ contradicting $r < \ell$. Thus $r = \ell$. □

Order of C = order of P

Let $P(x)$ be the characteristic polynomial of C.

By definition of the characteristic polynomials, $P(C) = 0$.

Thus x mod $P(x)$ satisfies the same equation as C and thus ord(C) =ord(P).

This matches our experiments

1. $s_{j+2} = s_j + s_{j+1}$ has order 3 for both C and P.
2. $s_{j+3} = s_j + s_{j+1}$ has order 7 for both C and P.

The other examples had reducible P, so we didn't compute ord(P).

Reminder:
$f(x)$ is irreducible if $f(x) = g(x) \cdot h(x)$ implies $\deg(g) = 0$ or $\deg(h) = 0$.
Else $f(x)$ is reducible.

Rabin's irreducibility test

A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is irreducible if and only if

1. $f(x) \mid \left(x^{q^n} - x\right)$,
2. $\gcd(f(x), x^{q^d} - x) = 1$ for all $d | n$ with $0 < d < n$.

Let $n = \prod p_i^{e_i}$ for p_i prime, $e_i \geq 1$. It is sufficient to check 2. for $d_i = n/p_i$.

Rabin's irreducibility test

A polynomial $f(x) \in \mathbb{F}_q[x]$ of degree n is irreducible if and only if

1. $f(x) \mid \left(x^{q^n} - x\right)$,
2. $\gcd(f(x), x^{q^d} - x) = 1$ for all $d|n$ with $0 < d < n$.

Let $n = \prod p_i^{e_i}$ for p_i prime, $e_i \geq 1$. It is sufficient to check 2. for $d_i = n/p_i$.

By 1. we have for f irreducible

$$x^{q^n} \equiv x \bmod f(x),$$

Thus $\mathrm{ord}(f) \,|(q^n - 1)$

Examples

This observation limits the orders we need to check

1. $s_{j+2} = s_j + s_{j+1}$ has $P(x) = x^2 + x + 1$ irreducible, $\deg(P) = 2$ and $2^2 - 1 = 3$ is prime, thus $\text{ord}(P) = 3$ without any computation.

Examples

This observation limits the orders we need to check

1. $s_{j+2} = s_j + s_{j+1}$ has $P(x) = x^2 + x + 1$ irreducible, $\deg(P) = 2$ and $2^2 - 1 = 3$ is prime, thus $\text{ord}(P) = 3$ without any computation.
2. $s_{j+3} = s_j + s_{j+1}$ has $P(x) = x^3 + x + 1$ irreducible, $\deg(P) = 3$ and $2^3 - 1 = 7$ is prime, thus $\text{ord}(P) = 7$ without any computation.

Examples

This observation limits the orders we need to check

1. $s_{j+2} = s_j + s_{j+1}$ has $P(x) = x^2 + x + 1$ irreducible, $\deg(P) = 2$ and $2^2 - 1 = 3$ is prime, thus $\mathrm{ord}(P) = 3$ without any computation.
2. $s_{j+3} = s_j + s_{j+1}$ has $P(x) = x^3 + x + 1$ irreducible, $\deg(P) = 3$ and $2^3 - 1 = 7$ is prime, thus $\mathrm{ord}(P) = 7$ without any computation.
3. $s_{j+4} = s_j + s_{j+1}$ has $P(x) = x^4 + x + 1$ irreducible, $\deg(P) = 4$ and $2^4 - 1 = 15 = 3 \cdot 5$. Thus we know $\mathrm{ord}(P) \in \{1, 3, 5, 15\}$.

Examples

This observation limits the orders we need to check

1. $s_{j+2} = s_j + s_{j+1}$ has $P(x) = x^2 + x + 1$ irreducible, $\deg(P) = 2$ and $2^2 - 1 = 3$ is prime, thus $\mathrm{ord}(P) = 3$ without any computation.
2. $s_{j+3} = s_j + s_{j+1}$ has $P(x) = x^3 + x + 1$ irreducible, $\deg(P) = 3$ and $2^3 - 1 = 7$ is prime, thus $\mathrm{ord}(P) = 7$ without any computation.
3. $s_{j+4} = s_j + s_{j+1}$ has $P(x) = x^4 + x + 1$ irreducible, $\deg(P) = 4$ and $2^4 - 1 = 15 = 3 \cdot 5$. Thus we know $\mathrm{ord}(P) \in \{1, 3, 5, 15\}$.
   Can exclude orders 1,3 without computation because of the degree.

$$x^5 = x \cdot x^4 \equiv x \cdot (x+1) = x^2 + x \neq 1 \bmod x^4 + x + 1.$$

Examples

This observation limits the orders we need to check

1. $s_{j+2} = s_j + s_{j+1}$ has $P(x) = x^2 + x + 1$ irreducible, $\deg(P) = 2$ and $2^2 - 1 = 3$ is prime, thus $\text{ord}(P) = 3$ without any computation.
2. $s_{j+3} = s_j + s_{j+1}$ has $P(x) = x^3 + x + 1$ irreducible, $\deg(P) = 3$ and $2^3 - 1 = 7$ is prime, thus $\text{ord}(P) = 7$ without any computation.
3. $s_{j+4} = s_j + s_{j+1}$ has $P(x) = x^4 + x + 1$ irreducible, $\deg(P) = 4$ and $2^4 - 1 = 15 = 3 \cdot 5$. Thus we know $\text{ord}(P) \in \{1, 3, 5, 15\}$.
   Can exclude orders 1,3 without computation because of the degree.

   $$x^5 = x \cdot x^4 \equiv x \cdot (x+1) = x^2 + x \neq 1 \bmod x^4 + x + 1.$$

   After excluding all small degrees we conclude that $\text{ord}(P) = 15$.

Examples

This observation limits the orders we need to check

1. $s_{j+2} = s_j + s_{j+1}$ has $P(x) = x^2 + x + 1$ irreducible, $\deg(P) = 2$ and $2^2 - 1 = 3$ is prime, thus $\mathrm{ord}(P) = 3$ without any computation.
2. $s_{j+3} = s_j + s_{j+1}$ has $P(x) = x^3 + x + 1$ irreducible, $\deg(P) = 3$ and $2^3 - 1 = 7$ is prime, thus $\mathrm{ord}(P) = 7$ without any computation.
3. $s_{j+4} = s_j + s_{j+1}$ has $P(x) = x^4 + x + 1$ irreducible, $\deg(P) = 4$ and $2^4 - 1 = 15 = 3 \cdot 5$. Thus we know $\mathrm{ord}(P) \in \{1, 3, 5, 15\}$.
   Can exclude orders 1,3 without computation because of the degree.

   $$x^5 = x \cdot x^4 \equiv x \cdot (x + 1) = x^2 + x \neq 1 \bmod x^4 + x + 1.$$

   After excluding all small degrees we conclude that $\mathrm{ord}(P) = 15$.
4. $s_{j+4} = s_j + s_{j+1} + s_{j+2} + s_{j+3}$ has $P(x) = x^4 + x^3 + x^2 + x + 1$ irreducible, $\deg(P) = 4$ and $2^4 - 1 = 15 = 3 \cdot 5$. Thus we know $\mathrm{ord}(P) \in \{1, 3, 5, 15\}$. Again can exclude orders 1,3.

Examples

This observation limits the orders we need to check

1. $s_{j+2} = s_j + s_{j+1}$ has $P(x) = x^2 + x + 1$ irreducible, $\deg(P) = 2$ and $2^2 - 1 = 3$ is prime, thus $\text{ord}(P) = 3$ without any computation.
2. $s_{j+3} = s_j + s_{j+1}$ has $P(x) = x^3 + x + 1$ irreducible, $\deg(P) = 3$ and $2^3 - 1 = 7$ is prime, thus $\text{ord}(P) = 7$ without any computation.
3. $s_{j+4} = s_j + s_{j+1}$ has $P(x) = x^4 + x + 1$ irreducible, $\deg(P) = 4$ and $2^4 - 1 = 15 = 3 \cdot 5$. Thus we know $\text{ord}(P) \in \{1, 3, 5, 15\}$.
   Can exclude orders 1,3 without computation because of the degree.
   $$x^5 = x \cdot x^4 \equiv x \cdot (x+1) = x^2 + x \neq 1 \bmod x^4 + x + 1.$$
   After excluding all small degrees we conclude that $\text{ord}(P) = 15$.
4. $s_{j+4} = s_j + s_{j+1} + s_{j+2} + s_{j+3}$ has $P(x) = x^4 + x^3 + x^2 + x + 1$ irreducible, $\deg(P) = 4$ and $2^4 - 1 = 15 = 3 \cdot 5$. Thus we know $\text{ord}(P) \in \{1, 3, 5, 15\}$. Again can exclude orders 1,3.
   $$\begin{aligned} x^5 &= x \cdot x^4 \equiv x \cdot (x^3 + x^2 + x + 1) = x^4 + x^3 + x^2 + x \\ &\equiv (x^3 + x^2 + x + 1) + x^3 + x^2 + x \equiv 1 \bmod x^4 + x^3 + x^2 + x + 1. \end{aligned}$$
   Thus the order is 5.

Primitive characteristic polynomial

Definition

The characteristic polynomial $P(x)$ of an LFSR is called *primitive* if P is irreducible and $\text{ord}(P) = 2^n - 1$, where n is the length of the state.

Primitive characteristic polynomial

Definition

The characteristic polynomial $P(x)$ of an LFSR is called *primitive* if P is irreducible and $\mathrm{ord}(P) = 2^n - 1$, where n is the length of the state.

This matches the definition of *primitive polynomial* in finite fields:

$\mathbb{F}_{2^k} \cong \mathbb{F}_2[x]/(P(x))$ has P primitive if P is irreducible and $\mathbb{F}_{2^k}^* = \langle x \rangle$, i.e. if x generates all $2^k - 1$ non-zero elements.

Primitive characteristic polynomial

Definition

The characteristic polynomial $P(x)$ of an LFSR is called *primitive* if P is irreducible and $\text{ord}(P) = 2^n - 1$, where n is the length of the state.

This matches the definition of *primitive polynomial* in finite fields:
$\mathbb{F}_{2^k} \cong \mathbb{F}_2[x]/(P(x))$ has P primitive if P is irreducible and $\mathbb{F}_{2^k}^* = \langle x \rangle$, i.e. if x generates all $2^k - 1$ non-zero elements.

Theorem

If P is irreducible then all non-zero starting states give the same period.

Proof in "LFSRs: Math vs. mystery" video.

Primitive characteristic polynomial

Definition

The characteristic polynomial $P(x)$ of an LFSR is called *primitive* if P is irreducible and $\text{ord}(P) = 2^n - 1$, where n is the length of the state.

This matches the definition of *primitive polynomial* in finite fields: $\mathbb{F}_{2^k} \cong \mathbb{F}_2[x]/(P(x))$ has P primitive if P is irreducible and $\mathbb{F}_{2^k}^* = \langle x \rangle$, i.e. if x generates all $2^k - 1$ non-zero elements.

Theorem

If P is irreducible then all non-zero starting states give the same period.

Proof in "LFSRs: Math vs. mystery" video.

This means that for irreducible P we know all periods by knowing $\text{ord}(P)$.

Example:
$s_{j+4} = s_j + s_{j+1}s_{j+2} + s_{j+3}$ has $P(x) = x^4 + x^3 + x^2 + x + 1$ irreducible of order 5. Thus the periods are 5,5,5,1.