LFSRs: matrix and characteristic polynomial

Tanja Lange

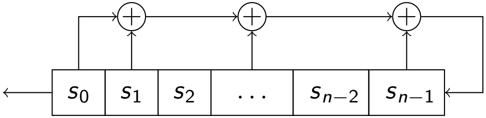
Eindhoven University of Technology

2WF80: Introduction to Cryptology

Status update as matrix multiplication

Express state $S_j \in \mathbb{F}_2^n$,
as function of S_{j-1}.

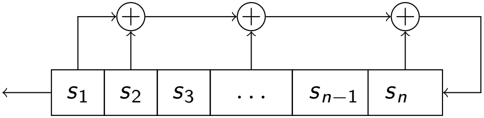
$S_0 = (s_0\, s_1\, s_2\, \ldots\, s_{n-2}\, s_{n-1})$.



Status update as matrix multiplication

Express state $S_j \in \mathbb{F}_2^n$,
as function of S_{j-1}.

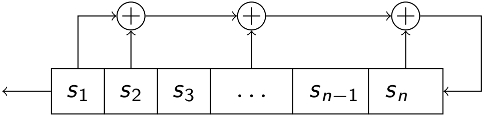
$S_0 = (s_0\, s_1\, s_2\, \ldots\, s_{n-2}\, s_{n-1})$.
$S_1 = (s_1\, s_2\, s_3\, \ldots\, s_{n-1}\, s_n)$,
with $s_n = \sum c_i s_i$.



Status update as matrix multiplication

Express state $S_j \in \mathbb{F}_2^n$,
as function of S_{j-1}.

$S_0 = (s_0\, s_1\, s_2\, \ldots\, s_{n-2}\, s_{n-1})$.
$S_1 = (s_1\, s_2\, s_3\, \ldots\, s_{n-1}\, s_n)$,
with $s_n = \sum c_i s_i$.

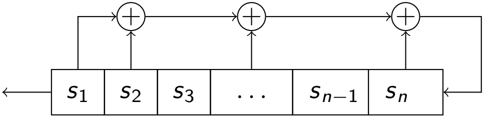


$$
\begin{aligned}
S_1 &= (s_1\, s_2\, s_3\, \ldots\, s_{n-1}\, s_n) \\
&= (s_0\, s_1\, s_2\, \ldots\, s_{n-2}\, s_{n-1}) \underbrace{\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \cdots & 0 & \vdots \\ 0 & 0 & 0 & \ddots & 0 & c_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}}_{C} \\
&= S_0 \cdot C.
\end{aligned}
$$

Status update as matrix multiplication

Express state $S_j \in \mathbb{F}_2^n$,
as function of S_{j-1}.

$S_0 = (s_0\, s_1\, s_2\, \ldots\, s_{n-2}\, s_{n-1})$.
$S_1 = (s_1\, s_2\, s_3\, \ldots\, s_{n-1}\, s_n)$,
with $s_n = \sum c_i s_i$.



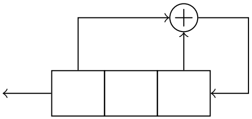
$$\begin{aligned} S_1 &= (s_1\, s_2\, s_3\, \ldots\, s_{n-1}\, s_n) \\ &= (s_0\, s_1\, s_2\, \ldots\, s_{n-2}\, s_{n-1}) \underbrace{\begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & c_0 \\ 1 & 0 & 0 & \cdots & 0 & c_1 \\ 0 & 1 & 0 & \cdots & 0 & c_2 \\ \vdots & \vdots & \ddots & \cdots & 0 & \vdots \\ 0 & 0 & 0 & \ddots & 0 & c_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & c_{n-1} \end{pmatrix}}_{C} \\ &= S_0 \cdot C. \end{aligned}$$

$(n-1) \times (n-1)$ identity matrix

coefficients

Examples

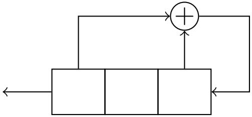
State update matrix C is an $n \times n$ matrix,
where n is the length of the register.



Examples

State update matrix C is an $n \times n$ matrix,
where n is the length of the register.

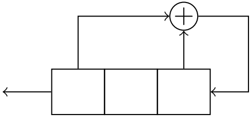
$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix}$$

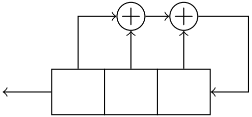


Examples

State update matrix C is an $n \times n$ matrix, where n is the length of the register.

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

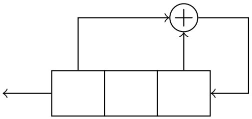




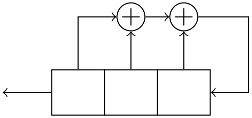
Examples

State update matrix C is an $n \times n$ matrix, where n is the length of the register.

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



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



What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.

What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.
- $S_2 = S_1 \cdot C = (S_0 \cdot C) \cdot C = S_0 \cdot C^2$.

What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.
- $S_2 = S_1 \cdot C = (S_0 \cdot C) \cdot C = S_0 \cdot C^2$.
- In general $S_j = S_0 \cdot C^j$.

What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.
- $S_2 = S_1 \cdot C = (S_0 \cdot C) \cdot C = S_0 \cdot C^2$.
- In general $S_j = S_0 \cdot C^j$.
- There are only 2^{n^2} $n \times n$ matrices over $\mathbb{F}_2$, so eventually

$$C^i = C^j$$

What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.
- $S_2 = S_1 \cdot C = (S_0 \cdot C) \cdot C = S_0 \cdot C^2$.
- In general $S_j = S_0 \cdot C^j$.
- There are only 2^{n^2} $n \times n$ matrices over $\mathbb{F}_2$, so eventually

$$C^i = C^j \Rightarrow S_i = S_0 C^i$$

What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.
- $S_2 = S_1 \cdot C = (S_0 \cdot C) \cdot C = S_0 \cdot C^2$.
- In general $S_j = S_0 \cdot C^j$.
- There are only 2^{n^2} $n \times n$ matrices over $\mathbb{F}_2$, so eventually

$$C^i = C^j \Rightarrow S_i = S_0 C^i = S_0 C^j = S_j.$$

What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.
- $S_2 = S_1 \cdot C = (S_0 \cdot C) \cdot C = S_0 \cdot C^2$.
- In general $S_j = S_0 \cdot C^j$.
- There are only 2^{n^2} $n \times n$ matrices over $\mathbb{F}_2$, so eventually

  $$C^i = C^j \Rightarrow S_i = S_0 C^i = S_0 C^j = S_j.$$

  The output is ultimately periodic as also $C^{i+1} = C^{j+1} etc.$
- This is independent of the starting state.

What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.
- $S_2 = S_1 \cdot C = (S_0 \cdot C) \cdot C = S_0 \cdot C^2$.
- In general $S_j = S_0 \cdot C^j$.
- There are only 2^{n^2} $n \times n$ matrices over $\mathbb{F}_2$, so eventually

  $$C^i = C^j \Rightarrow S_i = S_0 C^i = S_0 C^j = S_j.$$

  The output is ultimately periodic as also $C^{i+1} = C^{j+1} etc.$
- This is independent of the starting state.
- If C is invertible

  $$C^i = C^j \overset{i \geq j}{\Leftrightarrow} C^{i-j} = I,$$

  where I is the $n \times n$ identity matrix.

What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.
- $S_2 = S_1 \cdot C = (S_0 \cdot C) \cdot C = S_0 \cdot C^2$.
- In general $S_j = S_0 \cdot C^j$.
- There are only 2^{n^2} $n \times n$ matrices over $\mathbb{F}_2$, so eventually

$$C^i = C^j \Rightarrow S_i = S_0 C^i = S_0 C^j = S_j.$$

  The output is ultimately periodic as also $C^{i+1} = C^{j+1} etc.$
- This is independent of the starting state.
- If C is invertible

$$C^i = C^j \overset{i>j}{\Leftrightarrow} C^{i-j} = I,$$

  where I is the $n \times n$ identity matrix.
  Thus $S_{i-j} = S_0$ and the output is periodic;
  by the lemma, the period divides $i - j$.
- This is independent of the starting state.

What can we learn from the state-update matrix?

- $S_1 = S_0 \cdot C$.
- $S_2 = S_1 \cdot C = (S_0 \cdot C) \cdot C = S_0 \cdot C^2$.
- In general $S_j = S_0 \cdot C^j$.
- There are only 2^{n^2} $n \times n$ matrices over $\mathbb{F}_2$, so eventually

  $$C^i = C^j \Rightarrow S_i = S_0 C^i = S_0 C^j = S_j.$$

  The output is ultimately periodic as also $C^{i+1} = C^{j+1} etc.$
- This is independent of the starting state.
- If C is invertible

  $$C^i = C^j \overset{i>j}{\Leftrightarrow} C^{i-j} = I,$$

  where I is the $n \times n$ identity matrix.
  Thus $S_{i-j} = S_0$ and the output is periodic;
  by the lemma, the period divides $i - j$.
- This is independent of the starting state.
- If $c_0 = 1$ the determinant of C is 1 and C is invertible.

Order of C

The order of C, $\text{ord}(C)$, is the smallest integer $\ell > 0$ such that $C^\ell = I$, if such an ℓ exists.

Order of C

The order of C, ord(C), is the smallest integer $\ell > 0$ such that $C^\ell = I$, if such an ℓ exists.

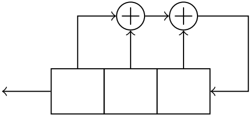
If the state-update matrix of an LFSR has order ℓ then all the periods for all starting states divide ℓ.

$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

Order of C

The order of C, ord(C), is the smallest integer $\ell > 0$ such that $C^\ell = I$, if such an ℓ exists.

If the state-update matrix of an LFSR has order ℓ then all the periods for all starting states divide ℓ.



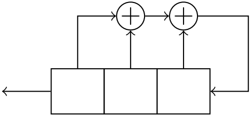
$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

$$C^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & & \\ & & \\ & & \end{pmatrix} \quad (0\,0\,1) \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

Order of C

The order of C, $\mathrm{ord}(C)$, is the smallest integer $\ell > 0$ such that $C^\ell = I$, if such an ℓ exists.

If the state-update matrix of an LFSR has order ℓ then all the periods for all starting states divide ℓ.



$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

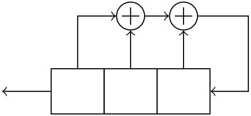
$$C^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$

$$C^3 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

Order of C

The order of C, $\mathrm{ord}(C)$, is the smallest integer $\ell > 0$ such that $C^\ell = I$, if such an ℓ exists.

If the state-update matrix of an LFSR has order ℓ then all the periods for all starting states divide ℓ.



$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

$$C^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$

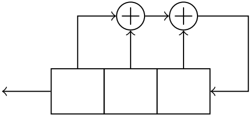
$$C^3 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$C^4 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I.$$

Order of C

The order of C, $\text{ord}(C)$, is the smallest integer $\ell > 0$ such that $C^\ell = I$, if such an ℓ exists.

If the state-update matrix of an LFSR has order ℓ then all the periods for all starting states divide ℓ.



$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

$$C^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$

$$C^3 = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix},$$

$$C^4 = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = I.$$

$\text{ord}(C) = 4$; indeed the periods we found, 4, 2, 1, 1, all divide 4.

Characteristic polynomial of C

Doing this one for general fields; over $\mathbb{F}_2 : + = -$.

$$\det(xI - C) = \begin{vmatrix} x & 0 & 0 & \cdots & 0 & -c_0 \\ -1 & x & 0 & \cdots & 0 & -c_1 \\ 0 & -1 & x & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \cdots & 0 & \vdots \\ 0 & 0 & 0 & \ddots & x & -c_{n-2} \\ 0 & 0 & 0 & \cdots & -1 & x - c_{n-1} \end{vmatrix} =$$

Characteristic polynomial of C

Doing this one for general fields; over $\mathbb{F}_2 : + = -$.

$$\det(xI - C) = \begin{vmatrix} x & 0 & 0 & \cdots & 0 & -c_0 \\ -1 & x & 0 & \cdots & 0 & -c_1 \\ 0 & -1 & x & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \cdots & 0 & \vdots \\ 0 & 0 & 0 & \ddots & x & -c_{n-2} \\ 0 & 0 & 0 & \cdots & -1 & x - c_{n-1} \end{vmatrix} =$$

$$x \begin{vmatrix} x & 0 & \cdots & 0 & -c_1 \\ -1 & x & \cdots & 0 & -c_2 \\ \vdots & \ddots & \cdots & 0 & \vdots \\ 0 & 0 & \ddots & x & -c_{n-2} \\ 0 & 0 & \cdots & -1 & x - c_{n-1} \end{vmatrix} + (-1)^{n+1} c_0 \begin{vmatrix} -1 & x & 0 & \cdots & 0 \\ 0 & -1 & x & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & 0 \\ 0 & 0 & 0 & \ddots & x \\ 0 & 0 & 0 & \cdots & -1 \end{vmatrix}$$

$= x\cdot$ determinant of same type matrix $+(-1)^{n-1+1} c_0 (-1)^{n-1}$

Characteristic polynomial of C

Doing this one for general fields; over $\mathbb{F}_2 : + = -$.

$$\det(xI - C) = \begin{vmatrix} x & 0 & 0 & \cdots & 0 & -c_0 \\ -1 & x & 0 & \cdots & 0 & -c_1 \\ 0 & -1 & x & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \cdots & 0 & \vdots \\ 0 & 0 & 0 & \ddots & x & -c_{n-2} \\ 0 & 0 & 0 & \cdots & -1 & x - c_{n-1} \end{vmatrix} =$$

$$x \begin{vmatrix} x & 0 & \cdots & 0 & -c_1 \\ -1 & x & \cdots & 0 & -c_2 \\ \vdots & \ddots & \cdots & 0 & \vdots \\ 0 & 0 & \ddots & x & -c_{n-2} \\ 0 & 0 & \cdots & -1 & x - c_{n-1} \end{vmatrix} + (-1)^{n+1} c_0 \begin{vmatrix} -1 & x & 0 & \cdots & 0 \\ 0 & -1 & x & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & 0 \\ 0 & 0 & 0 & \ddots & x \\ 0 & 0 & 0 & \cdots & -1 \end{vmatrix}$$

$= x\cdot$ determinant of same type matrix $+(-1)^{n-1+1} c_0 (-1)^{n-1}$
$= x(x(\cdots x(x(x - c_{n-1}) - c_{n-2}) - \cdots - c_2) - c_1) - c_0$

Characteristic polynomial of C

Doing this one for general fields; over $\mathbb{F}_2: + = -$.

$$\det(xI - C) = \begin{vmatrix} x & 0 & 0 & \cdots & 0 & -c_0 \\ -1 & x & 0 & \cdots & 0 & -c_1 \\ 0 & -1 & x & \cdots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \cdots & 0 & \vdots \\ 0 & 0 & 0 & \ddots & x & -c_{n-2} \\ 0 & 0 & 0 & \cdots & -1 & x - c_{n-1} \end{vmatrix} =$$

$$x \begin{vmatrix} x & 0 & \cdots & 0 & -c_1 \\ -1 & x & \cdots & 0 & -c_2 \\ \vdots & \ddots & \cdots & 0 & \vdots \\ 0 & 0 & \ddots & x & -c_{n-2} \\ 0 & 0 & \cdots & -1 & x - c_{n-1} \end{vmatrix} + (-1)^{n+1} c_0 \begin{vmatrix} -1 & x & 0 & \cdots & 0 \\ 0 & -1 & x & \cdots & 0 \\ \vdots & \vdots & \ddots & \cdots & 0 \\ 0 & 0 & 0 & \ddots & x \\ 0 & 0 & 0 & \cdots & -1 \end{vmatrix}$$

$= x\cdot$ determinant of same type matrix $+(-1)^{n-1+1} c_0 (-1)^{n-1}$
$= x(x(\cdots x(x(x - c_{n-1}) - c_{n-2}) - \cdots - c_2) - c_1) - c_0 = x^n - \sum c_i x^i$.