Live session 30 Nov 2020

Tanja Lange

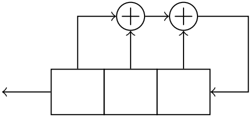
Eindhoven University of Technology

2WF80: Introduction to Cryptology

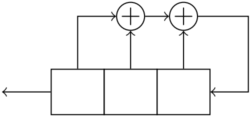
What does $P(C)$ mean?

This example has
$P(x) = x^3 + x^2 + x + 1$.

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



What does $P(C)$ mean?



This example has
$P(x) = x^3 + x^2 + x + 1$.

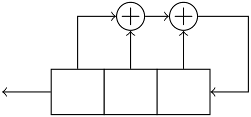
$$C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix},$$

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

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

$$P(C) = C^3 + C^2 + C + I =$$

What does $P(C)$ mean?



This example has
$P(x) = x^3 + x^2 + x + 1$.

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

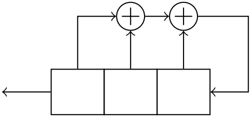
$$C^2 = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 & 1 \\ 0 & 1 & 0 \\ 1 & 1 & 0 \end{pmatrix},$$

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

$$P(C) = C^3 + C^2 + C + I =$$

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

What does $P(C)$ mean?



This example has
$P(x) = x^3 + x^2 + x + 1$.

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

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

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

$$P(C) = C^3 + C^2 + C + I =$$

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

Each position sums up to 0, thus $P(C) = 0$, the all-zero $n \times n$ matrix.

Another way to see the analogy of $x \bmod P(x)$ and C

We introduced C as the state-update matrix that takes a state vector
$S_i \quad = (s_i, s_{i+1}, s_{i+2}, \ldots, s_{i+n-1})$ to
$S_{i+1} = (s_{i+1}, s_{i+2}, s_{i+3}, \ldots, s_{i+n-1}, s_{i+n})$ via

$$S_{i+1} = S_i \cdot C.$$

Another way to see the analogy of x mod $P(x)$ and C

We introduced C as the state-update matrix that takes a state vector
$S_i \quad = (s_i, s_{i+1}, s_{i+2}, \dots, s_{i+n-1})$ to
$S_{i+1} = (s_{i+1}, s_{i+2}, s_{i+3}, \dots, s_{i+n-1}, s_{i+n})$ via

$$S_{i+1} = S_i \cdot C.$$

In the generating functions view we have

$$S(x) = s_0 + s_1 x + s_2 x^2 + \cdots + \underbrace{s_i x^i + s_{s+1} x^{i+1} + s_{i+2} x^{x+2} + \cdots + s_{i+n-1} x^{i+n-1}}_{\text{terms from } S_i} + s_{i+n} x^{i+n} + s_{i+n+1} x^{i+n+1} + \dots$$

Another way to see the analogy of x mod $P(x)$ and C

We introduced C as the state-update matrix that takes a state vector
$S_i \quad = (s_i, s_{i+1}, s_{i+2}, \dots, s_{i+n-1})$ to
$S_{i+1} = (s_{i+1}, s_{i+2}, s_{i+3}, \dots, s_{i+n-1}, s_{i+n})$ via

$$S_{i+1} = S_i \cdot C.$$

In the generating functions view we have

$$S(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_i x^i + \underbrace{s_{i+1}x^{i+1} + s_{i+2}x^{x+2} + \cdots + s_{i+n-1}x^{i+n-1} + s_{i+n}x^{i+n}}_{\text{terms from } S_{i+1}} + s_{i+n+1}x^{i+n+1} + \dots$$

Thus also here we see that multiplication by C corresponds to mulitplication by x mod $P(x)$.

Some notation

- Given an LFSR with state size n, characteristic polynomial $P(x)$.
- For a polynomial $f(x)$ denote by $f^*(x)$ its reciprocal

$$f^*(x) = \left(\sum_{i=0}^{n} f_i x^i\right)^* = x^n \sum_{i=0}^{n} f_i x^{-i} = \sum_{i=0}^{n} f_i x^{n-i} = \sum_{i=0}^{n} f_{n-i} x^i.$$

Some notation

- Given an LFSR with state size n, characteristic polynomial $P(x)$.
- For a polynomial $f(x)$ denote by $f^*(x)$ its reciprocal

$$f^*(x) = \left(\sum_{i=0}^{n} f_i x^i \right)^* = x^n \sum_{i=0}^{n} f_i x^{-i} = \sum_{i=0}^{n} f_i x^{n-i} = \sum_{i=0}^{n} f_{n-i} x^i.$$

- Examples: $(x^n + 1)^* = x^n(x^{-n} + 1) = 1 + x^n$; $(f^*(x))^* = f(x)$.

Some notation

- Given an LFSR with state size n, characteristic polynomial $P(x)$.
- For a polynomial $f(x)$ denote by $f^*(x)$ its reciprocal

$$f^*(x) = \left(\sum_{i=0}^{n} f_i x^i\right)^* = x^n \sum_{i=0}^{n} f_i x^{-i} = \sum_{i=0}^{n} f_i x^{n-i} = \sum_{i=0}^{n} f_{n-i} x^i.$$

- Examples: $(x^n + 1)^* = x^n(x^{-n} + 1) = 1 + x^n$; $(f^*(x))^* = f(x)$.
- The generating function of a sequence $\{s_i\}_i$ is given by

$$S(x) = \sum_{i=0}^{\infty} s_i x^i.$$

Note: S depends on the starting state; there are 2^n different generating functions for an LFSR with state size n.

Some notation and helpful results

- Given an LFSR with state size n, characteristic polynomial $P(x)$.
- For a polynomial $f(x)$ denote by $f^*(x)$ its reciprocal

$$f^*(x) = \left(\sum_{i=0}^{n} f_i x^i\right)^* = x^n \sum_{i=0}^{n} f_i x^{-i} = \sum_{i=0}^{n} f_i x^{n-i} = \sum_{i=0}^{n} f_{n-i} x^i.$$

- Examples: $(x^n + 1)^* = x^n(x^{-n} + 1) = 1 + x^n$; $(f^*(x))^* = f(x)$.
- The generating function of a sequence $\{s_i\}_i$ is given by

$$S(x) = \sum_{i=0}^{\infty} s_i x^i.$$

  Note: S depends on the starting state; there are 2^n different generating functions for an LFSR with state size n.
- Claims: $\deg(P^*(x)S(x)) < n$.

Claim: $\deg(P^*(x)S(x)) < n$

Proof.

$$P^*(x)S(x) = \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i$$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$P^*(x)S(x) = \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i$$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$\begin{aligned} P^*(x)S(x) &= \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i \\ &= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i \end{aligned}$$

□

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$P^*(x)S(x) = \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i$$

$$= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j}$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$\begin{aligned} P^*(x)S(x) &= \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right) \sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i \\ &= \sum_{i=0}^{n-1} \left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right) x^i + \sum_{i=n}^{\infty} \left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right) x^i \end{aligned}$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j} \Rightarrow 0 = \sum_{j=0}^{n} c_j s_{k+j}$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$
\begin{aligned}
P^*(x)S(x) &= \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i \\
&= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i
\end{aligned}
$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j} \Rightarrow 0 = \sum_{j=0}^{n} c_j s_{k+j}$

Change the order of summation: $0 = \sum_{j=0}^{n} c_{n-j} s_{k+n-j}$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$P^*(x)S(x) = \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i$$

$$= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j} \Rightarrow 0 = \sum_{j=0}^{n} c_j s_{k+j}$

Change the order of summation: $0 = \sum_{j=0}^{n} c_{n-j}s_{k+n-j}$
and rename $k + n = i$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$
\begin{aligned}
P^*(x)S(x) &= \left(1+\sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i \\
&= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i \\
&= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty} 0\cdot x^i
\end{aligned}
$$

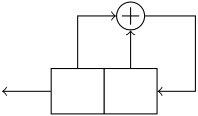
□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j} \Rightarrow 0 = \sum_{j=0}^{n} c_j s_{k+j}$

Change the order of summation: $0 = \sum_{j=0}^{n} c_{n-j} s_{k+n-j}$
and rename $k+n=i$

Example

Using
$P(x) = x^2 + x + 1$.



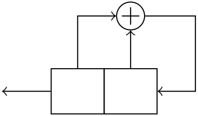
This LFSR produces output $\overline{011}$.

$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Example

Using
$P(x) = x^2 + x + 1.$



This LFSR produces output $\overline{011}$.

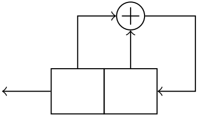
$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2).$
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0$

Example

Using
$P(x) = x^2 + x + 1$.



This LFSR produces output $\overline{011}$.

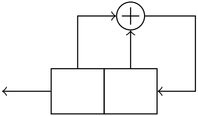
$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0 + 1) \cdot x$

Example

Using
$P(x) = x^2 + x + 1.$



This LFSR produces output $\overline{011}$.

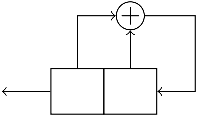
$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2).$
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0 + 1) \cdot x + (0 + 1 + 1) \cdot x^2$

Example

Using
$P(x) = x^2 + x + 1$.



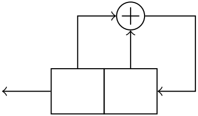
This LFSR produces output $\overline{011}$.

$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0 + 1) \cdot x + (0 + 1 + 1) \cdot x^2 + (1 + 1 + 0) \cdot x^3$

Example



Using
$P(x) = x^2 + x + 1$.

This LFSR produces output $\overline{011}$.

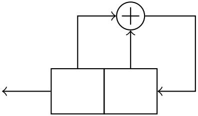
$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0+1) \cdot x + (0+1+1) \cdot x^2 + (1+1+0) \cdot x^3 + (1+0+1) \cdot x^4$

Example

Using
$P(x) = x^2 + x + 1$.



This LFSR produces output $\overline{011}$.

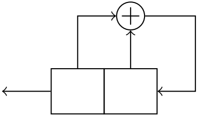
$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0+1) \cdot x + (0+1+1) \cdot x^2 + (1+1+0) \cdot x^3 + (1+0+1) \cdot x^4 + (0+1+1) \cdot x^5$

Example

Using
$P(x) = x^2 + x + 1$.



This LFSR produces output $\overline{011}$.

$P^*(x) = (x^2 + x + 1)^* = x^2(x^{-2} + x^{-1} + 1) = (1 + x + x^2)$.
This means the product on the previous slide is

$$(x^2 + x + 1) \cdot (x + x^2 + x^4 + x^5 + x^7 + x^8 + \cdots)$$

Crossmultiplying gives
$0 \cdot x^0 + (0+1) \cdot x + (0+1+1) \cdot x^2 + (1+1+0) \cdot x^3 + (1+0+1) \cdot x^4 + (0+1+1) \cdot x^5 + (1+1+0) \cdot x^6 \cdots$.

The coefficients of $x^2, x^3, \ldots$ match shifts of 011 because the coefficient vector of $P^*(x)$ is 111.
The coefficients of x^0 and x^1 have fewer terms because their degree is lower than $\deg(P)$.
That's why we need to treat them separately in

$$\sum_{i=0}^{n} c_{n-i} x^i \sum_{i=0}^{\infty} s_i x^i.$$

Claim: $\deg(P^*(x)S(x)) < n$

Simplify notation: put $c_n = 1$

Proof.

$$\begin{aligned} P^*(x)S(x) &= \left(1 + \sum_{i=1}^{n} c_{n-i}x^i\right)\sum_{i=0}^{\infty} s_i x^i = \sum_{i=0}^{n} c_{n-i}x^i \sum_{i=0}^{\infty} s_i x^i \\ &= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty}\left(\sum_{j=0}^{n} c_{n-j}s_{i-j}\right)x^i \\ &= \sum_{i=0}^{n-1}\left(\sum_{j=0}^{i} c_{n-j}s_{i-j}\right)x^i + \sum_{i=n}^{\infty} 0 \cdot x^i \end{aligned}$$

□

Definition of LFSR: $s_{k+n} = \sum_{j=0}^{n-1} c_j s_{k+j} \Rightarrow 0 = \sum_{j=0}^{n} c_j s_{k+j}$

Change the order of summation: $0 = \sum_{j=0}^{n} c_{n-j} s_{k+n-j}$
and rename $k + n = i$