Feedback shift registers

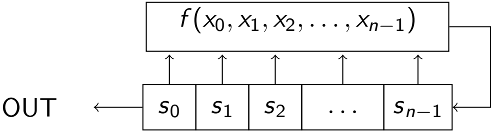
Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

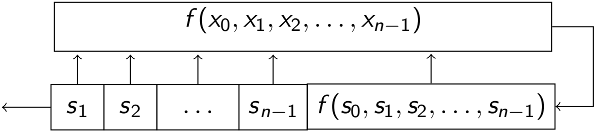
Feedback shift registers

Typically $s_i \in \mathbb{F}_2$
Starting state:
$(s_0\, s_1\, s_2\, \ldots\, s_{n-1})$



Feedback shift registers

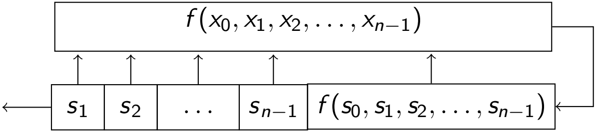
Typically $s_i \in \mathbb{F}_2$
Starting state:
$(s_0\, s_1\, s_2\, \dots\, s_{n-1})$



First output:
s_0
Second state:
$(s_1\, s_2\, \dots\, s_{n-1}\, f(s_0, s_1, s_2, \dots, s_{n-1}))$

Feedback shift registers

Typically $s_i \in \mathbb{F}_2$
Starting state:
$(s_0\ s_1\ s_2\ \ldots\ s_{n-1})$



First output:
s_0
Second state:
$(s_1\ s_2\ \ldots\ s_{n-1}\ f(s_0, s_1, s_2, \ldots, s_{n-1}))$

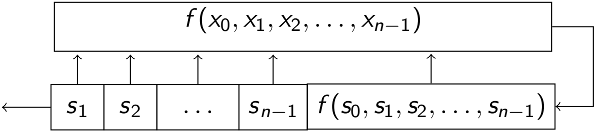
First $n + 2$ outputs:
$s_0\ s_1\ s_2\ \ldots s_{n-1}\ f(s_0, s_1, s_2, \ldots, s_{n-1})\ f(s_1, s_2, \ldots, s_{n-1}, f(s_0, s_1, s_2, \ldots, s_{n-1}))$

Feedback shift registers

Typically $s_i \in \mathbb{F}_2$

Starting state:

$(s_0\ s_1\ s_2\ \ldots\ s_{n-1})$



First output:

s_0

Second state:

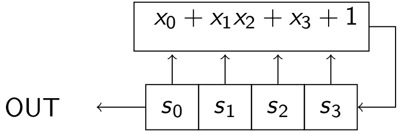
$(s_1\ s_2\ \ldots\ s_{n-1}\ f(s_0, s_1, s_2, \ldots, s_{n-1}))$

First $n+2$ outputs:

$s_0\ s_1\ s_2\ \ldots s_{n-1}\ f(s_0, s_1, s_2, \ldots, s_{n-1})\ f(s_1, s_2, \ldots, s_{n-1}, f(s_0, s_1, s_2, \ldots, s_{n-1}))$

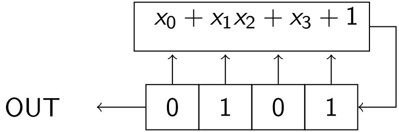
To use an FSR as a stream cipher, make $f = f_k$ a function of the key k, put $IV = (s_0\ s_1\ s_2\ \ldots\ s_{n-1})$, and discard the first n output bits.

Example



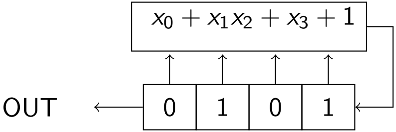
Output:

Example



Output:

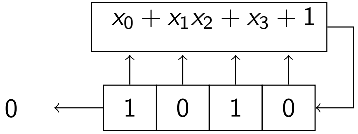
Example



$0 + 1 \cdot 0 + 1 + 1 = 0$

Output:

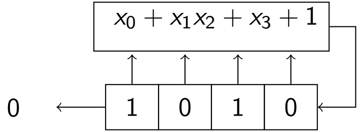
Example



$0 + 1 \cdot 0 + 1 + 1 = 0$

Output:
0

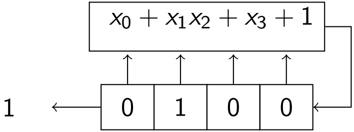
Example



$1 + 0 \cdot 1 + 0 + 1 = 0$

Output:
0

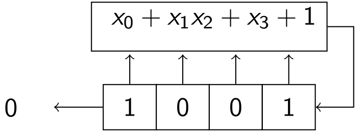
Example



$0 + 1 \cdot 0 + 0 + 1 = 1$

Output:
0 1

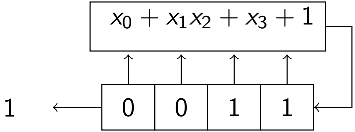
Example



$1 + 0 \cdot 0 + 1 + 1 = 1$

Output:
0 1 0

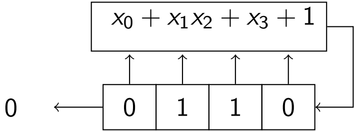
Example



$0 + 0 \cdot 1 + 1 + 1 = 0$

Output:
0 1 0 1

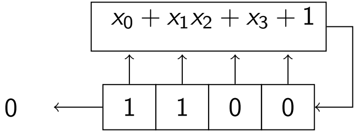
Example



$0 + 1 \cdot 1 + 0 + 1 = 0$

Output:
0 1 0 1 0

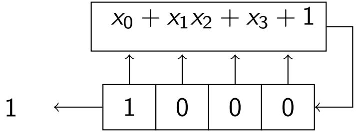
Example



$1 + 1 \cdot 0 + 0 + 1 = 0$

Output:
0 1 0 1 0 0

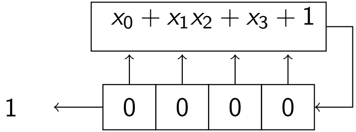
Example



$$1 + 0 \cdot 0 + 0 + 1 = 0$$

Output:
0 1 0 1 0 0 1

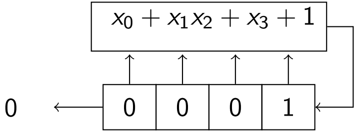
Example



$0 + 0 \cdot 0 + 0 + 1 = 1$

Output:
0 1 0 1 0 0 1 1

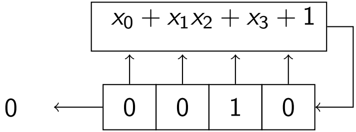
Example



$0 + 0 \cdot 0 + 1 + 1 = 0$

Output:
0 1 0 1 0 0 1 1 0

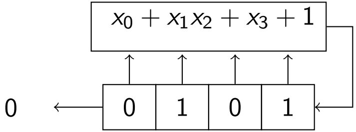
Example



$0 + 0 \cdot 1 + 0 + 1 = 1$

Output:
0 1 0 1 0 0 1 1 0 0

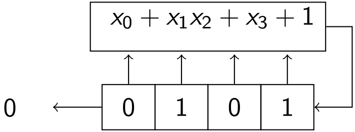
Example



$0 + 1 \cdot 0 + 1 + 1 = 0$

Output:
0 1 0 1 0 0 1 1 0 0 0

Example

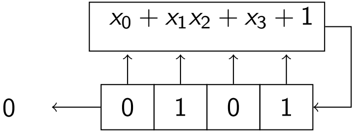


$0 + 1 \cdot 0 + 1 + 1 = 0$

Output:
0 1 0 1 0 0 1 1 0 0 0

This is equal to our starting state!

Example



$0 + 1 \cdot 0 + 1 + 1 = 0$

Output:
0 1 0 1 0 0 1 1 0 0 0

This is equal to our starting state!

This FSR outputs

$$\overline{0\,1\,0\,1\,0\,0\,1\,1\,0\,0\,0},$$

i.e., the output is periodic with period length 11.

Repetition is unavoidable as there are only $2^4 = 16$ possible states.

Not all need to appear in the same run.

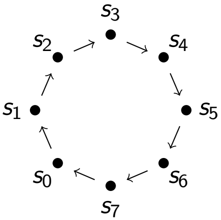
Exercise: Here we miss state $(1\,1\,1\,1)$.
Determine the output sequence resulting from this state.

Definition periods

A sequence $\{s_i\}_i$ is called *periodic* if there exists an integer $r > 0$ so that

$$s_{r+i} = s_i$$

for all $i \geq 0$.
The *period* is the smallest such r.

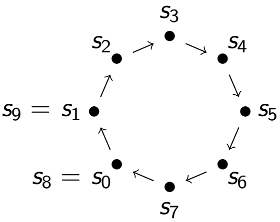


Definition periods

A sequence $\{s_i\}_i$ is called *periodic* if there exists an integer $r > 0$ so that

$$s_{r+i} = s_i$$

for all $i \geq 0$.
The *period* is the smallest such r.

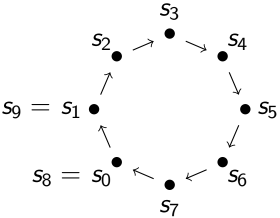


Definition periods

A sequence $\{s_i\}_i$ is called *periodic* if there exists an integer $r > 0$ so that

$$s_{r+i} = s_i$$

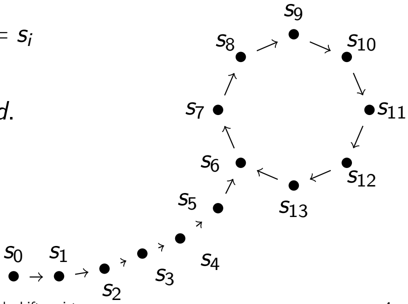
for all $i \geq 0$.
The *period* is the smallest such r.



It is called *ultimately periodic* if there exist integers $r > 0$ and $i_0 \geq 0$ so that

$$s_{r+i} = s_i$$

for all $i \geq i_0$.
The smallest i_0 is called the *pre-period*.

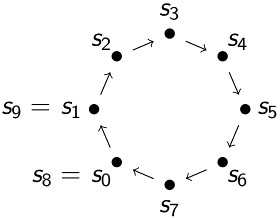


Definition periods

A sequence $\{s_i\}_i$ is called *periodic* if there exists an integer $r > 0$ so that

$$s_{r+i} = s_i$$

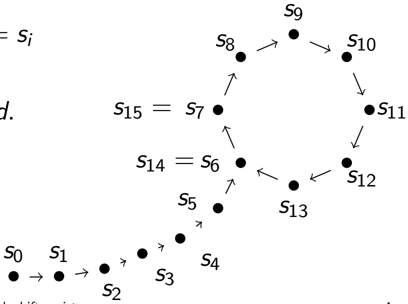
for all $i \geq 0$.
The *period* is the smallest such r.



It is called *ultimately periodic* if there exist integers $r > 0$ and $i_0 \geq 0$ so that

$$s_{r+i} = s_i$$

for all $i \geq i_0$.
The smallest i_0 is called the *pre-period*.



Divisibility property

Lemma

If $\{s_i\}_i$ is periodic with period r and if for some $\ell > 0$ it holds that

$$s_i = s_{i+\ell}$$

for all $i \geq 0$, then

$$r | \ell.$$

Divisibility property

Lemma

If $\{s_i\}_i$ is periodic with period r and if for some $\ell > 0$ it holds that

$$s_i = s_{i+\ell}$$

for all $i \geq 0$, then

$$r|\ell.$$

Proof.

Assume on the contrary that $\ell = qr + r_0$ with $0 < r_0 < r$.
Then

$$s_i = s_{i+\ell} = s_{i+qr+r_0} = s_{qr+(i+r_0)} = s_{i+r_0}.$$

Divisibility property

Lemma

If $\{s_i\}_i$ is periodic with period r and if for some $\ell > 0$ it holds that

$$s_i = s_{i+\ell}$$

for all $i \geq 0$, then

$$r | \ell.$$

Proof.

Assume on the contrary that $\ell = qr + r_0$ with $0 < r_0 < r$.
Then

$$s_i = s_{i+\ell} = s_{i+qr+r_0} = s_{qr+(i+r_0)} = s_{i+r_0}.$$

Divisibility property

Lemma

If $\{s_i\}_i$ is periodic with period r and if for some $\ell > 0$ it holds that

$$s_i = s_{i+\ell}$$

for all $i \geq 0$, then

$$r | \ell.$$

Proof.

Assume on the contrary that $\ell = qr + r_0$ with $0 < r_0 < r$.
Then

$$s_i = s_{i+\ell} = s_{i+qr+r_0} = s_{qr+(i+r_0)} = s_{i+r_0}.$$

period definition

Divisibility property

Lemma

If $\{s_i\}_i$ is periodic with period r and if for some $\ell > 0$ it holds that

$$s_i = s_{i+\ell}$$

for all $i \geq 0$, then

$$r|\ell.$$

Proof.

Assume on the contrary that $\ell = qr + r_0$ with $0 < r_0 < r$.
Then

$$s_i = s_{i+\ell} = s_{i+qr+r_0} = s_{qr+(i+r_0)} = s_{i+r_0}.$$

period definition

Thus $s_i = s_{i+r_0}$ or all $i \geq 0$.

This contradicts the minimality of the period as $0 < r_0 < r$.

Thus $r_0 = 0$ and $r|\ell$.

□