Sums of LFSRs

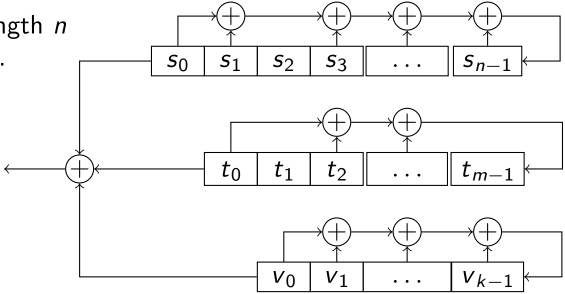
Tanja Lange

Eindhoven University of Technology

2WF80: Introduction to Cryptology

Sums of LFSRs

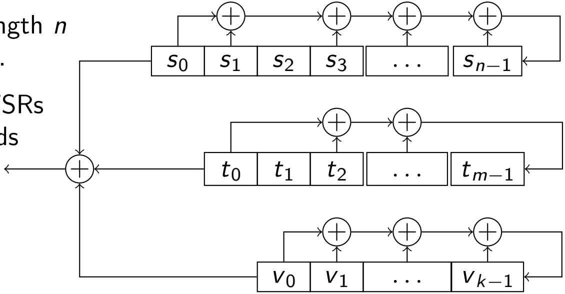
LFSR with state of length n has period at most 2^n.



Sums of LFSRs

LFSR with state of length n has period at most 2^n.

Can combine short LFSRs to create longer periods

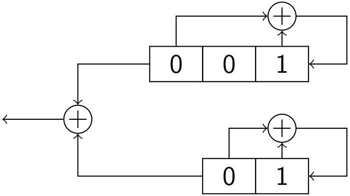


Sums of LFSRs

LFSR with state of length n has period at most 2^n.

Can combine short LFSRs to create longer periods

Concrete example:
$\overline{0011101} + \overline{011}$



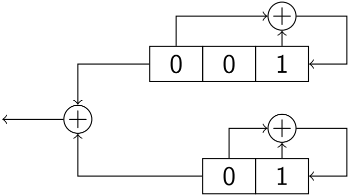
Sums of LFSRs

LFSR with state of length n has period at most 2^n.

Can combine short LFSRs to create longer periods

Concrete example:
$\overline{0011101} + \overline{011}$

```
  0 0 1 1 1 0 1
+ 0 1 1
---------------
```



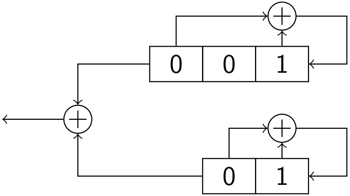
Sums of LFSRs

LFSR with state of length n has period at most 2^n.

Can combine short LFSRs to create longer periods

Concrete example:
$\overline{0011101} + \overline{011}$

```
   0  0  1  1  1  0  1
+  0  1  1
---------------
   0  1  0
```



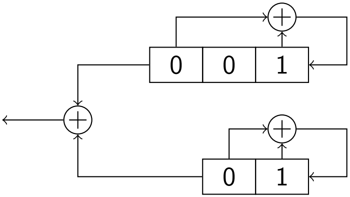
Sums of LFSRs

LFSR with state of length *n* has period at most 2^n.

Can combine short LFSRs to create longer periods

Concrete example:
$\overline{0011101} + \overline{011}$

```
  0 0 1 1 1 0 1
+ 0 1 1 0 1 1 0 1 1
-------------------
  0 1 0 1 0 1 1
```



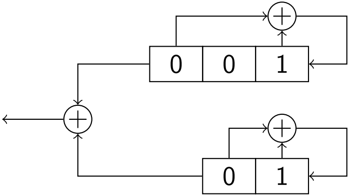
Sums of LFSRs

LFSR with state of length n
has period at most 2^n.

Can combine short LFSRs
to create longer periods

Concrete example:
$\overline{0011101} + \overline{011}$

```
  0 0 1 1 1 0 1 0 0 1 1 1 0 1
+ 0 1 1 0 1 1 0 1 1
-----------------------------
  0 1 0 1 0 1 1 1 1
```



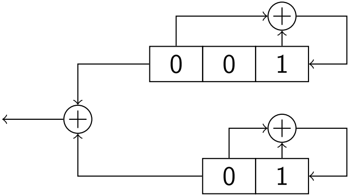
Sums of LFSRs

LFSR with state of length n
has period at most 2^n.

Can combine short LFSRs
to create longer periods

Concrete example:
$\overline{0011101} + \overline{011}$

```
  0 0 1 1 1 0 1 0 0 1 1 1 0 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
-------------------------------
  0 1 0 1 0 1 1 1 1 1 0 0 0 0
```

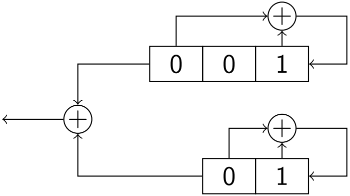


Sums of LFSRs

LFSR with state of length n
has period at most 2^n.

Can combine short LFSRs
to create longer periods

Concrete example:
$\overline{0011101} + \overline{011}$

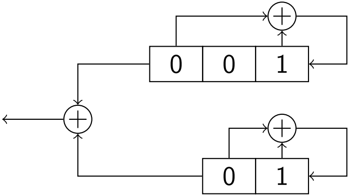



```
  0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
-------------------------------------------
  0 1 0 1 0 1 1 1 1 1 0 0 0 0 1
```

Sums of LFSRs

LFSR with state of length n has period at most 2^n.

Can combine short LFSRs to create longer periods



Concrete example:
$\overline{0011101} + \overline{011}$

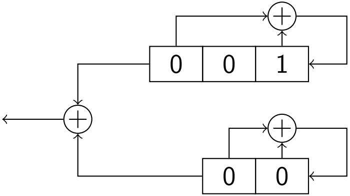
```
  0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
-------------------------------------------
  0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0 0 1 1 0
```

These LFSRs of periods 3 and 7 combine to period $3 \cdot 7 = 21$

Sums of LFSRs

LFSR with state of length n has period at most 2^n.

Can combine short LFSRs to create longer periods



Concrete example:
$\overline{0011101} + \overline{011}$

```
  0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
--------------------------------------------
  0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0 0 1 1 0
```

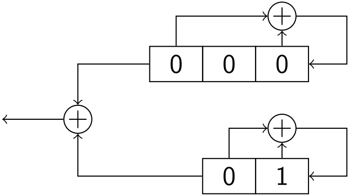
These LFSRs of periods 3 and 7 combine to period $3 \cdot 7 = 21$, 7

```
  0 0 1 1 1 0 1
+ 0 0 0 0 0 0 0
----------------
  0 0 1 1 1 0 1
```

Sums of LFSRs

LFSR with state of length n has period at most 2^n.

Can combine short LFSRs to create longer periods



Concrete example:
$\overline{0011101} + \overline{011}$

```
  0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
--------------------------------------------
  0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0 0 1 1 0
```

These LFSRs of periods 3 and 7 combine to period $3 \cdot 7 = 21$, 7, 3

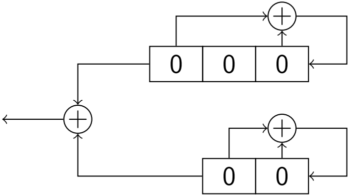
```
  0 0 1 1 1 0 1          0 0 0
+ 0 0 0 0 0 0 0        + 0 1 1
---------------        -------
  0 0 1 1 1 0 1          0 1 1
```

Sums of LFSRs

LFSR with state of length n
has period at most 2^n.

Can combine short LFSRs
to create longer periods

Concrete example:
$\overline{0011101} + \overline{011}$



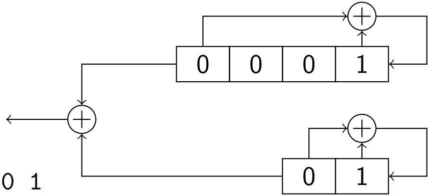

```
  0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
-------------------------------------------
  0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0 0 1 1 0
```

These LFSRs of periods 3 and 7 combine to period $3 \cdot 7 = 21$, 7, 3, 1.

```
  0 0 1 1 1 0 1            0 0 0          0
+ 0 0 0 0 0 0 0          + 0 1 1        + 0
---------------          -------        ---
  0 0 1 1 1 0 1            0 1 1          0
```

Another example

These LFSRs produce
$\overline{000111101011001}$ and $\overline{011}$
of periods 15 and 3.



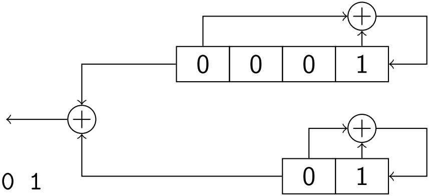
Their sum gives

	0	0	0	1	1	1	1	0	1	0	1	1	0	0	1
+	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
	0	1	1	1	0	0	1	1	0	0	0	0	0	1	0

of period 15.

Another example

These LFSRs produce $\overline{000111101011001}$ and $\overline{011}$ of periods 15 and 3.



Their sum gives

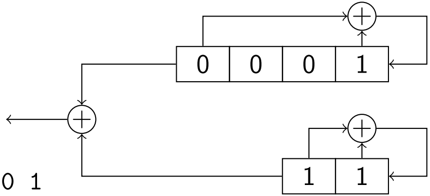
	0	0	0	1	1	1	1	0	1	0	1	1	0	0	1
+	0	1	1	0	1	1	0	1	1	0	1	1	0	1	1
	0	1	1	1	0	0	1	1	0	0	0	0	0	1	0

of period 15.

Initializing one or both LFSRs with all-zero state gives 15, 3, 1 – but we expect $2^6 = 64$ states.

Another example

These LFSRs produce $\overline{000111101011001}$ and $\overline{011}$ of periods 15 and 3.



Their sum gives

```
  0 0 0 1 1 1 1 0 1 0 1 1 0 0 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
---------------------------------
  0 1 1 1 0 0 1 1 0 0 0 0 0 1 0
```

of period 15.

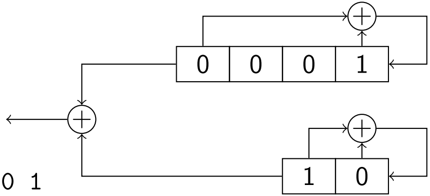
Initializing one or both LFSRs with all-zero state gives 15, 3, 1 – but we expect $2^6 = 64$ states.

```
  0 0 0 1 1 1 1 0 1 0 1 1 0 0 1
+ 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0
---------------------------------
  1 1 0 0 0 1 0 1 1 1 0 1 1 1 1
```

Starting at different offsets gives periods 15

Another example

These LFSRs produce
$\overline{000111101011001}$ and $\overline{011}$
of periods 15 and 3.



Their sum gives

```
  0 0 0 1 1 1 1 0 1 0 1 1 0 0 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
--------------------------------
  0 1 1 1 0 0 1 1 0 0 0 0 0 1 0
```

of period 15.

Initializing one or both LFSRs with all-zero state gives 15, 3, 1 –
but we expect $2^6 = 64$ states.

```
  0 0 0 1 1 1 1 0 1 0 1 1 0 0 1
+ 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1
--------------------------------
  1 0 1 0 1 0 0 0 0 1 1 0 1 0 0
```

Starting at different offsets gives periods 15 and 15.

For a total of periods
15, 15, 15, 15, 3, 1,
summing up to 64.

First hypotheses

- Adding LFSRs of max periods p and r gives period $\text{lcm}(p, r)$.

First hypotheses

- Adding LFSRs of max periods p and r gives period $\mathrm{lcm}(p, r)$.
- If the first LFSR has periods $p = 2^m - 1$ and 1 and the second LFSR has periods $r = 2^n - 1$ and 1, then
  - their sum has $\gcd(p, r)$ sequences of period $\mathrm{lcm}(p, r)$ (resulting from the $\gcd(p, r)$ different offsets)

First hypotheses

- Adding LFSRs of max periods p and r gives period $\operatorname{lcm}(p, r)$.
- If the first LFSR has periods $p = 2^m - 1$ and 1 and the second LFSR has periods $r = 2^n - 1$ and 1, then
  - their sum has $\gcd(p, r)$ sequences of period $\operatorname{lcm}(p, r)$ (resulting from the $\gcd(p, r)$ different offsets)
  - and sequences of period p, r, and 1, from initializing one or both in the all-zero state.
  - These sum up to $\gcd(p, r) \cdot \operatorname{lcm}(p, r) + p + r + 1 = p \cdot r + p + r + 1$ $= (p + 1)(r + 1) = 2^m \cdot 2^n$, thus accounting for all 2^{m+n} states.

First hypotheses

- Adding LFSRs of max periods p and r gives period $\text{lcm}(p, r)$.
- If the first LFSR has periods $p = 2^m - 1$ and 1 and
  the second LFSR has periods $r = 2^n - 1$ and 1, then
  - their sum has $\gcd(p, r)$ sequences of period $\text{lcm}(p, r)$
    (resulting from the $\gcd(p, r)$ different offsets)
  - and sequences of period p, r, and 1,
    from initializing one or both in the all-zero state.
  - These sum up to $\gcd(p, r) \cdot \text{lcm}(p, r) + p + r + 1 = p \cdot r + p + r + 1$
    $= (p + 1)(r + 1) = 2^m \cdot 2^n$,
    thus accounting for all 2^{m+n} states.
- If one or both do not have maximal periods we expect
  - $\gcd(p, r)$ sequences of period $\text{lcm}(p, r)$
  - sequences of period p, r, and 1,
  - sequences from combinations of the other parts.

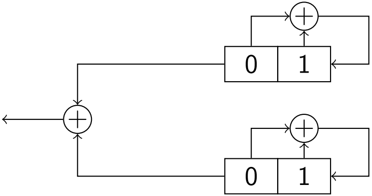
A third example

These LFSRs produce
$\overline{011}$ and $\overline{011}$
of periods 3 and 3.

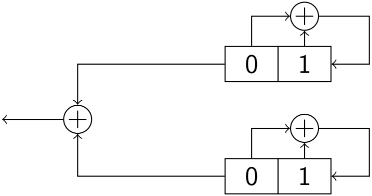
Their sum gives

```
  0 1 1
+ 0 1 1
-------
  0 0 0
```

of period 1.



A third example



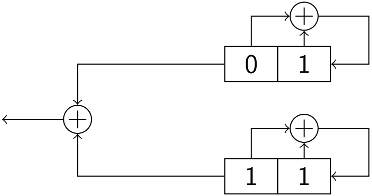
These LFSRs produce
$\overline{011}$ and $\overline{011}$
of periods 3 and 3.

Their sum gives

```
  0 1 1
+ 0 1 1
-------
  0 0 0
```

of period 1. The same will happen whenever the starting states are equal.

A third example



These LFSRs produce
$\overline{011}$ and $\overline{011}$
of periods 3 and 3.

Their sum gives

```
  0 1 1
+ 0 1 1
-------
  0 0 0
```

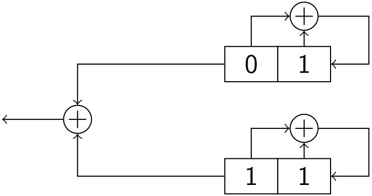
of period 1. The same will happen whenever the starting states are equal.

Shifting one starting state gives

```
  0 1 1
+ 1 1 0
-------
  1 0 1
```

of period 3.

A third example



These LFSRs produce
$\overline{011}$ and $\overline{011}$
of periods 3 and 3.

Their sum gives

```
  0 1 1
+ 0 1 1
-------
  0 0 0
```

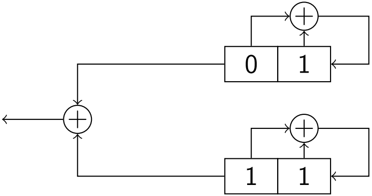
of period 1. The same will happen whenever the starting states are equal.

Shifting one starting state gives

```
  0 1 1
+ 1 1 0
-------
  1 0 1
```

of period 3. This is the same sequence as just one of them.

A third example



These LFSRs produce
$\overline{011}$ and $\overline{011}$
of periods 3 and 3.

Their sum gives

```
  0 1 1
+ 0 1 1
-------
  0 0 0
```

of period 1. The same will happen whenever the starting states are equal.

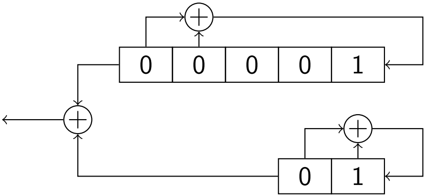
Shifting one starting state gives

```
  0 1 1
+ 1 1 0
-------
  1 0 1
```

of period 3. This is the same sequence as just one of them.

Not useful to combine identical LFSRs.

A fourth example



These LFSRs produce $\overline{000010001100101011111}$ and $\overline{011}$ of periods 21 and 3.

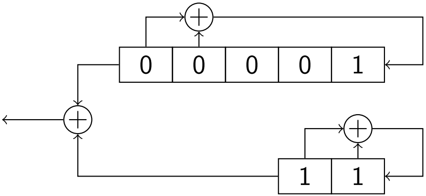
Their sum gives

```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
-------------------------------------------
  0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0
```

of period 21.

A fourth example

These LFSRs produce $\overline{000010001100101011111}$ and $\overline{011}$ of periods 21 and 3.



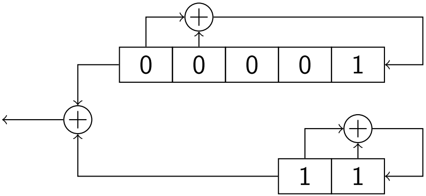
Their sum gives

```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
--------------------------------------------
  0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0
```

of period 21.

```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0
--------------------------------------------
  1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1
```

A fourth example



These LFSRs produce
$\overline{000010001100101011111}$ and $\overline{011}$
of periods 21 and 3.

Their sum gives

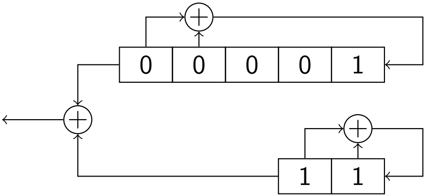
```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
-------------------------------------------
  0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0
```

of period 21.

```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0
-------------------------------------------
  1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1
```

A fourth example

These LFSRs produce $\overline{000010001100101011111}$ and $\overline{011}$ of periods 21 and 3.



Their sum gives

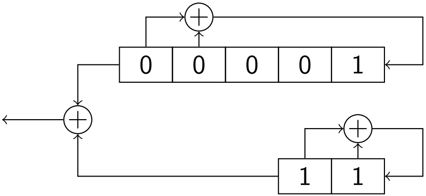
```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
-------------------------------------------
  0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0
```

of period 21.

```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0
-------------------------------------------
  1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1
```

of period 7?

A fourth example



These LFSRs produce $\overline{000010001100101011111}$ and $\overline{011}$ of periods 21 and 3.

Their sum gives

```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1
-------------------------------------------
  0 1 1 0 0 1 0 1 0 1 1 1 1 1 0 0 0 0 1 0 0
```

of period 21.

```
  0 0 0 0 1 0 0 0 1 1 0 0 1 0 1 0 1 1 1 1 1
+ 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0 1 1 0
-------------------------------------------
  1 1 0 1 0 0 1 1 1 0 1 0 0 1 1 1 0 1 0 0 1
```

of period 7?

Our hypotheses would have predicted: 21, 21, 21, 21, 3, 1 and some more for the $2^5 - 21 - 1 = 10$ missing states in the first. But we do not get the fourth 21.