Digitalteknik EITF65

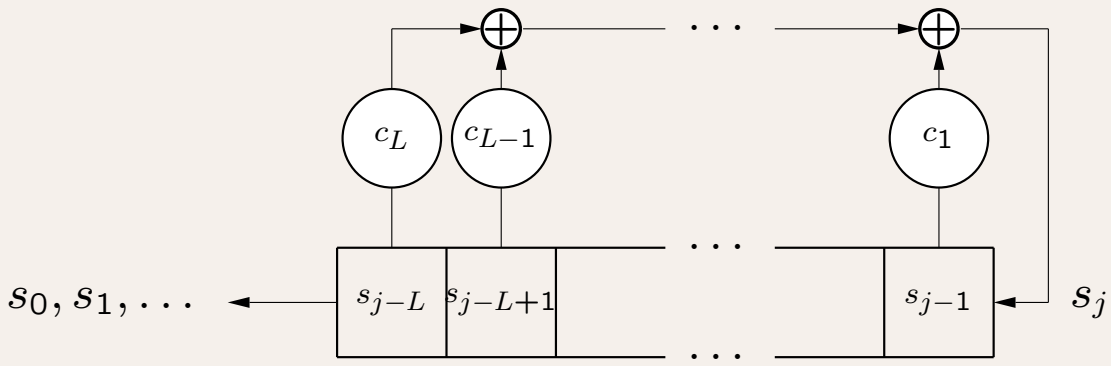
Lecture 14: Linear Sequential Circuits, Part 2

August 27, 2020

LFSR

Definition

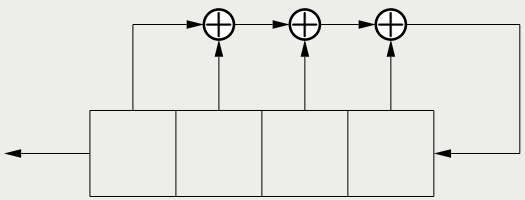
A linear feedback shift register (LFSR) is a cascade of D-elements where the input is a linear function of the state variables.

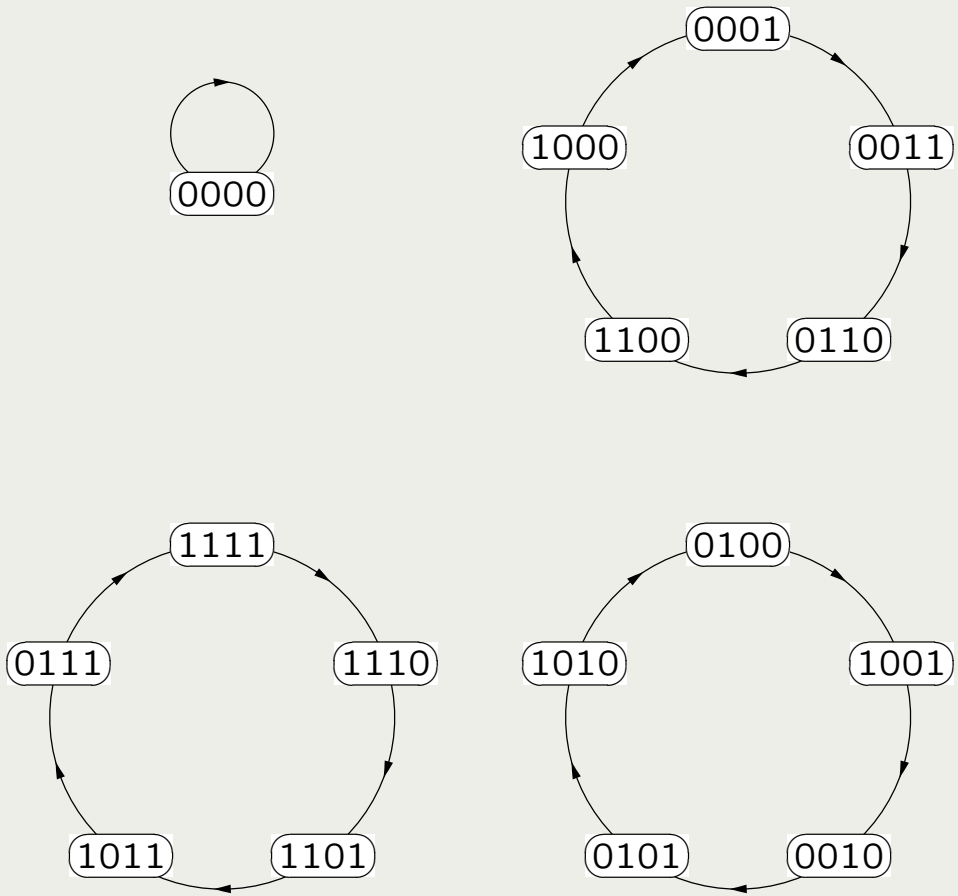


LFSR

Example

The following LFSR gives the state transition graph below.

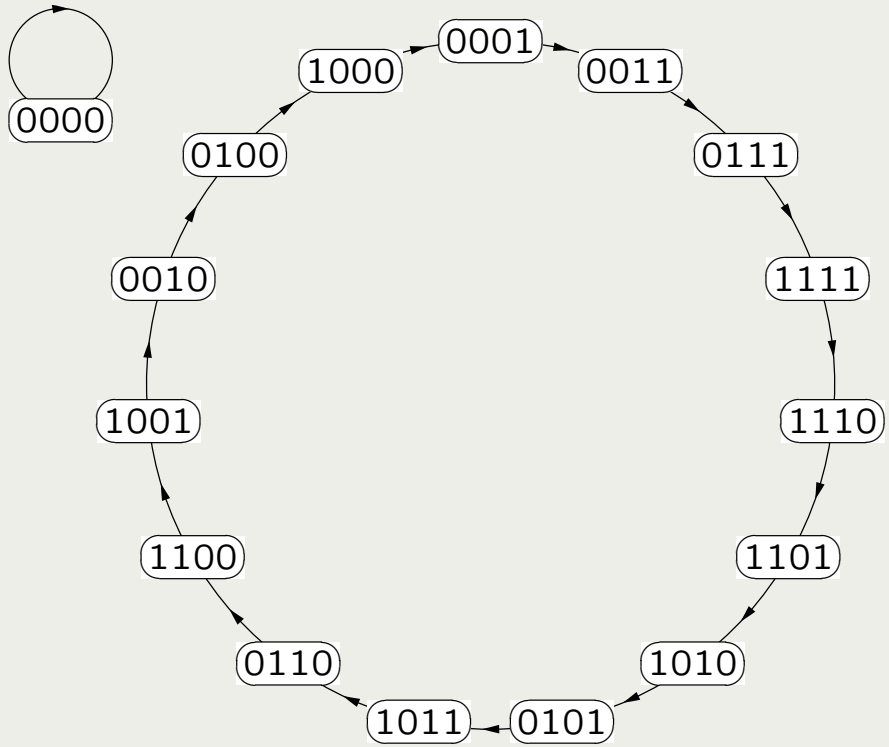




LFSR

Example

The following LFSR gives the state transition graph below.



Maximal Length Sequence

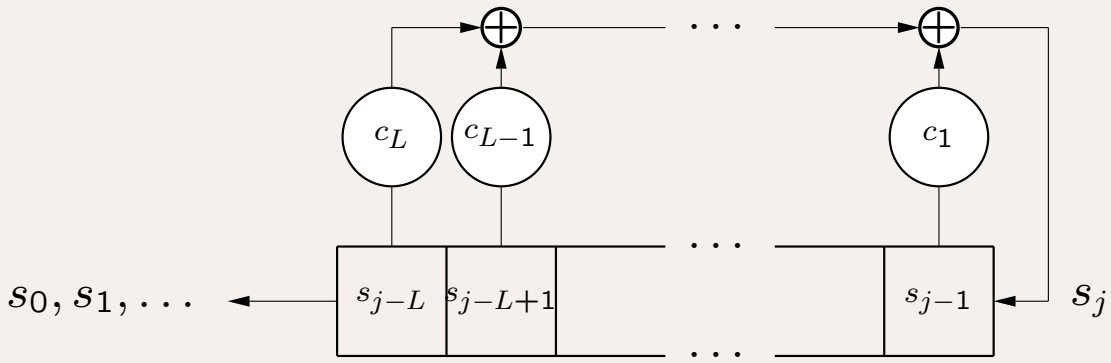
Definition

All LFSRs give separate cycles in the state transition graph. If all nonzero states are included in one cycle the output is called a maximal length sequence.

LFSR

Definition (Connection Polynomial)

The general form of an LFSR is given by:



It is determined by $\mathbf{c} = (1, c_1, \ldots, c_L)$. The $\mathcal{D}$-transform of $\mathbf{c}$

$$C(D) = 1 \oplus \sum_{i=1}^{L} c_i D^i \overset{c_0=1}{\downarrow} \sum_{i=0}^{L} c_i D^i$$

is called the connection polynomial of the LFSR.

Shift register recursion

Theorem

The shift register recursion can be written as

$$\sum_{i=0}^{L} c_i s_{j-i} = 0, \quad j \geq L$$

where $c_0 = 1$.

Shift register recursion

Proof.

For $j \geq L$

$$s_j = c_L s_{j-L} \oplus c_{L-1} s_{j-L+1} \oplus \cdots \oplus c_1 s_{j-1} = \sum_{i=1}^{L} c_i s_{j-i}$$

or, equivalently,

$$s_j \oplus \sum_{i=1}^{L} c_i s_{j-i} = 0$$

With $c_0 = 1$

$$c_0 s_j \oplus \sum_{i=1}^{L} c_i s_{j-i} = 0$$

The LFSR theorem

Theorem

An LFSR with connection polynomial $C(D)$, $\deg C(D) = L$, *can generate the sequence* $\mathbf{s}$ *if and only if* $S(D)$ *can be written as*

$$S(D) = \frac{P(D)}{C(D)}$$

where $\deg P(D) < \deg C(D)$.

See proof in course book.

Euclid's algorithm

To find the shortest LFSR that generates a sequence $\mathbf{s}$ we delete common factors in the numerator and the denominator of the D transform $S(D)$.

Therefore, we need to find the greatest common divisor (gcd) of two polynomials. This can be done with Euclid's algorithm.

$\mathbf{s} = [1101001]^{\infty}$

Example

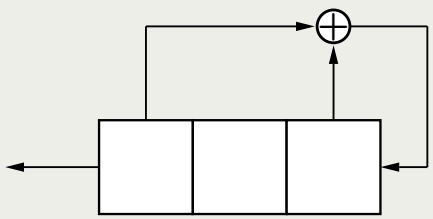
To find a minimal LFSR that generates $\mathbf{s} = [1101001]^{\infty}$, consider the $\mathcal{D}$-transform

$$s(D) = \frac{1 \oplus D \oplus D^3 \oplus D^6}{1 \oplus D^7}$$

Use Euclid's algrithm to find common factors gives
$\gcd(D^7 \oplus 1, D^6 \oplus D^3 \oplus D \oplus 1) = D^4 \oplus D^2 \oplus D \oplus 1$
We get

$$s(D) = \frac{(1 \oplus D^2)(1 \oplus D \oplus D^2 \oplus D^4)}{(1 \oplus D \oplus D^3)(1 \oplus D \oplus D^2 \oplus D^4)} = \frac{1 \oplus D^2}{1 \oplus D \oplus D^3}$$

A minimal length LFSR:



Starting state ($P(D) \rightarrow \mathbf{s}$)

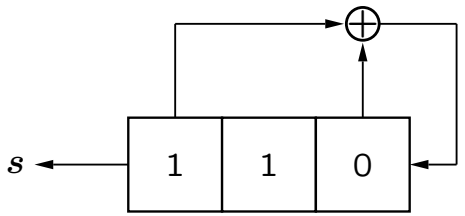
To get the starting state we can also perform long division (series expansion) of (se next slide for derivation)

$$s(D) = \frac{1 \oplus D^2}{1 \oplus D \oplus D^3} = 1 \oplus D \oplus D^3 \oplus D^6 \oplus \cdots$$

Hence,

$$s(D) = 1 \oplus D \oplus D^3 \oplus D^6 \oplus \cdots \xrightarrow{\mathcal{D}^{-1}} \underbrace{110}_{\text{starting state}} 1001 \ldots$$

The starting state is the first bits that are shifted out.



Starting state ($P(D) \rightarrow \mathbf{s}$)

Derivation of long division of $S(D)$.

$$
\begin{array}{r|l}
 & 1 \oplus D \quad \oplus D^3 \quad \oplus D^6 \oplus \cdots \\
\cline{2-2}
1 \oplus D \oplus D^3 & 1 \quad \oplus D^2 \\
 & \underline{1 \oplus D \quad \oplus D^3} \\
 & \quad D \oplus D^2 \oplus D^3 \\
 & \quad \underline{D \oplus D^2 \quad \oplus D^4} \\
 & \qquad D^3 \oplus D^4 \\
 & \qquad \underline{D^3 \oplus D^4 \oplus D^6} \\
 & \qquad\quad D^6 \\
 & \qquad\quad \underline{D^6 \oplus D^7 \oplus D^9} \\
 & \qquad\qquad D^7 \oplus D^9 \\
 & \qquad\qquad\quad \ddots
\end{array}
$$

Starting state ($\mathbf{s} \rightarrow P(D)$)

We can also derive $P(D)$ from the starting state.
We know that

$$P(D) = S(D)C(D)$$

and if we know

$$C(D) = 1 \oplus D \oplus D^3$$
$$S(D) = 1 \oplus D \oplus \mathcal{O}(D^3)$$

where $\mathcal{O}(D^3)$ represents all terms with degree 3 and higher.
Combining, we get

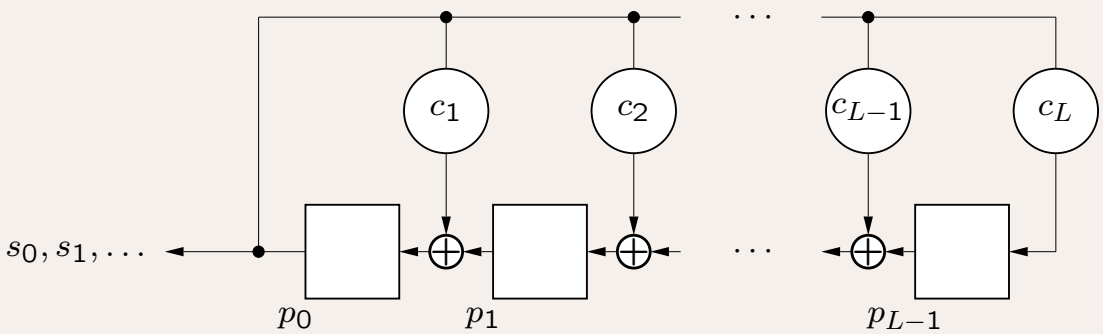
$$\begin{aligned} P(D) &= (1 \oplus D \oplus \mathcal{O}(D^3))(1 \oplus D \oplus D^3) \\ &= \underbrace{1 \oplus D^2}_{P(D)} \oplus \underbrace{\mathcal{O}(D^3)}_{=0} \end{aligned}$$

since $\deg\big(P(D)\big) < \deg\big(C(D)\big)$.

Observer canonical form

OCF of LFSR

An LFSR is a linear sequential circuit in pseudo-controller canonical form. It can also be realized in observer canonical form.



To realize the sequence $S(D)$ the starting state is

$$P(D) = S(D)C(D)$$

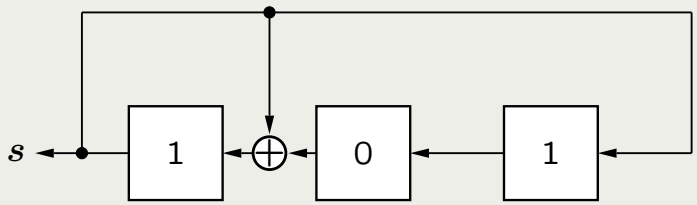
$$s(D) = \frac{1 \oplus D^2}{1 \oplus D \oplus D^3}$$

Example

To genetrate the sequence **s** with $\mathcal{D}$-transform

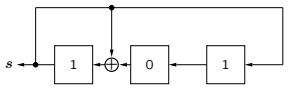
$$s(D) = \frac{1 \oplus D^2}{1 \oplus D \oplus D^3}$$

we can use the circuit



State value

In this form the state is directly the reminder in the (long) division.



1	0	$1 = 1 \oplus D^2$
1	1	$1 = 1 \oplus D \oplus D^2$
0	1	$1 = D \oplus D^2$
1	1	$0 = 1 \oplus D$
0	0	$1 = D^2$
0	1	$0 = D$
1	0	$0 = 1$
1	0	$1 = 1 \oplus D^2$

$$
\begin{array}{r|l}
 & 1 \oplus D \oplus D^3 \oplus D^6 \oplus \cdots \\
1 \oplus D \oplus D^3 & \overline{1 \oplus D^2} \\
 & \underline{1 \oplus D \oplus D^3} \\
 & \overline{D \oplus D^2 \oplus D^3} \quad = D(1 \oplus D \oplus D^2) \\
 & \underline{D \oplus D^2 \oplus D^4} \\
 & \overline{D^3 \oplus D^4} \quad = D^2(D \oplus D^2) = D^3(1 \oplus D) \\
 & \underline{D^3 \oplus D^4 \oplus D^6} \\
 & \overline{D^6} \quad = D^4(D^2) = D^5(D) = D^6(1) \\
 & \underline{D^6 \oplus D^7 \oplus D^9} \\
 & \overline{D^7 \oplus D^9} \quad = D^7(1 \oplus D^2)
\end{array}
$$

The period

The period T for a connection polynomial $C(D)$ is defined as the smallest $T > 0$ for which $C(D)$ divides $1 + D^T$.

Theorem

The period for connection polynomial $C(D)$ can be derived by the long division (series expansion) of $\frac{1}{C(D)}$. At the first occasion the reminder is D^k we get the period as $T = k$.

Period

Example 7.7

To calculate the period for the connection polynomial

$$C(D) = 1 \oplus D \oplus D^3$$

we derive $\frac{1}{C(D)}$:

$$\begin{array}{r|l}
 & 1 \oplus D \oplus D^2 \qquad \oplus D^4 \oplus \cdots \\
\hline
1 \oplus D \oplus D^3 & 1 \\
 & \underline{1 \oplus D \qquad \oplus D^3} \\
 & \quad D \qquad \oplus D^3 \\
 & \quad \underline{D \oplus D^2 \qquad \oplus D^4} \\
 & \qquad D^2 \oplus D^3 \oplus D^4 \\
 & \qquad \underline{D^2 \oplus D^3 \qquad \oplus D^5} \\
 & \qquad\qquad D^4 \oplus D^5 \\
 & \qquad\qquad \underline{D^4 \oplus D^5 \oplus D^7} \\
 & \qquad\qquad\qquad D^7
\end{array}$$

Hence, the period is $T = 7$.

The period

Theorem

The period for connection polynomial $C(D)$ and the period of the sequence $\mathbf{s}$ *with D-transform*

$$S(D) = \frac{P(D)}{C(D)}, \quad \textit{where } \deg(P(D)) < \deg(C(D)),$$

is the same if $gcd(P(D), C(D)) = 1$.