Mathematics 124 (Winter 2009)
Feedback Shift Registers

Motivational Example: Four neighbours have established a pattern by which they leave their porch lights on at night.

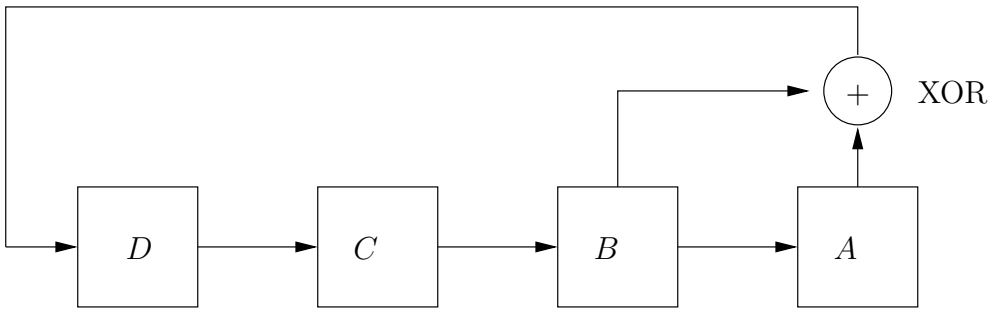
- Anne does what Barbara did the night before.
- Barbara does what Cathy did the night before.
- Cathy does what Denise did the night before.
- Denise leaves her light on if either Anne or Barbara (but not both) left theirs on the night before; otherwise she leaves it off.

On a particular night, Denise's light was on, Cathy's was off, Barbara's was off, and Anne's was off. Determine Anne's pattern of porch lighting on successive nights.

Denise, Cathy, Barbara, and Anne's porch-lighting scheme can be represented as

$$\begin{aligned} A' &\leftarrow B \\ B' &\leftarrow C \\ C' &\leftarrow D \\ D' &\leftarrow (B + A) \operatorname{MOD} 2 \end{aligned}$$

with initial assignments $D = 1$, $C = 0$, $B = 0$, $A = 0$.



t	D	C	B	A
0	1	0	0	0
1	0	1	0	0
2	0	0	1	0
3	1	0	0	1
4	1	1	0	0
5	0	1	1	0
6	1	0	1	1
7	0	1	0	1
8	1	0	1	0
9	1	1	0	1
10	1	1	1	0
11	1	1	1	1
12	0	1	1	1
13	0	0	1	1
14	0	0	0	1
15	1	0	0	0
16	0	1	0	0
17	0	0	1	0
18	1	0	0	1
19	1	1	0	0
20	0	1	1	0
21	1	0	1	1
22	0	1	0	1
23	1	0	1	0
24	1	1	0	1

The "random" pattern in column A begins repeating at $t = 15$.

Generic Linear Feedback Shift Register (LFSR)

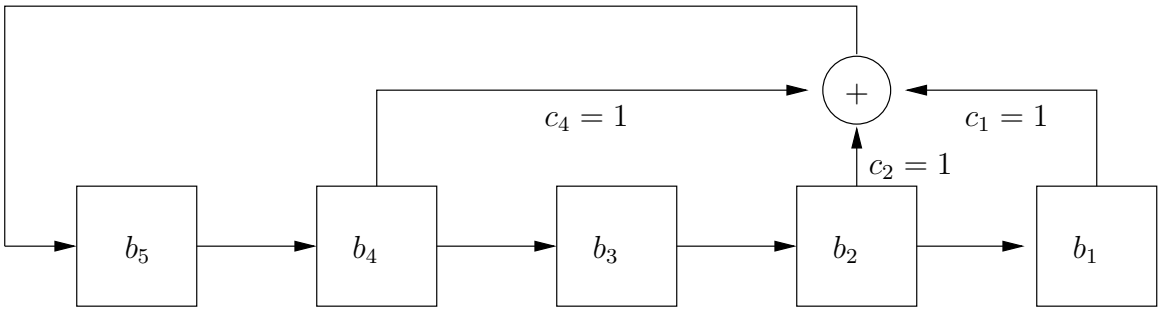
A **feedback shift register** is an electronic circuit that implements this sort of pattern. It is represented mathematically as several $(n-1)$ "shift equations" and one "feedback equation."

Suppose that $b_n, b_{n-1}, \ldots, b_3, b_2, b_1$ are the bits in the register at some given time. Then an n-bit linear feedback shift register is given by

$$\begin{aligned} b'_1 &\leftarrow b_2 \\ b'_2 &\leftarrow b_3 \\ &\vdots \\ b'_{n-1} &\leftarrow b_n \\ b'_n &\leftarrow (c_n b_n + c_{n-1} b_{n-1} + \cdots c_2 b_2 + c_1 b_1) \,\mathrm{MOD}\, 2 \end{aligned}$$

where

- $b_n, b_{n-1}, \ldots, b_2, b_1$ are variables taking the value 0 or 1,
- $c_n, c_{n-1}, \ldots, c_2, c_1$ are coefficients (constants, either 0 or 1) chosen in advance, and
- the prime notation ($'$) indicated the updated value of the variable.



Example: Consider the following 5-bit linear shift register with the feedback equations

$$
\begin{aligned}
b_1' &\leftarrow b_2 \\
b_2' &\leftarrow b_3 \\
b_3' &\leftarrow b_4 \\
b_4' &\leftarrow b_5 \\
b_5' &\leftarrow (0 \cdot b_5 + 1 \cdot b_4 + 0 \cdot b_3 + 1 \cdot b_2 + 1 \cdot b_1) \,\mathrm{MOD}\, 2
\end{aligned}
$$

and with initial values $b_5 = 1$, $b_4 = 0$, $b_3 = 1$, $b_2 = 0$, $b_1 = 0$.

The internal states of the LFSR are therefore given by

t	b_5	b_4	b_3	b_2	b_1
0	1	0	1	0	0
1	0	1	0	1	0
2	0	0	1	0	1
3	1	0	0	1	0
4	1	1	0	0	1
5	0	1	1	0	0
6	1	0	1	1	0
7	1	1	0	1	1
8	1	1	1	0	1
9	0	1	1	1	0
10	0	0	1	1	1
11	0	0	0	1	1
12	0	0	0	0	1
13	1	0	0	0	0
14	0	1	0	0	0
15	1	0	1	0	0
16	0	1	0	1	0

Notice that at time $t = 15$ the sequence has returned to its time $t = 0$ values. Thus, the pattern of b_1 will repeat itself every 15 times. This gives the following as output (sequence from b_1):

$$\boxed{001010011011100}0010100110111000\ldots$$

Uses in Cryptography: LFSRs have long been used as a pseudo-random number generator for use in stream ciphers (especially in military cryptography), due to the ease of construction from simple electromechanical or electronic circuits, long periods, and very uniformly distributed outputs. However the outputs of LFSRs are completely linear, leading to fairly easy cryptanalysis.

Three general methods are employed to reduce this problem in LFSR based stream ciphers:

- non-linear combination of several bits from the LFSR state;
- non-linear combination of the outputs of two or more LFSRs; or
- irregular clocking of the LFSR.

Important LFSR-based stream ciphers include **A5/1**, **A5/2** (a stream cipher used to provide over-the-air voice privacy in the GSM cellular telephone standard—reverse engineered and serious weaknesses identified—low end equipment can break it in real time), **E0** (used in Bluetooth protocol for wireless personal area networks—number of vulernabilites found—key recovered in 2^{38} computations), and the **shrinking generator** (introduced in 1993—limited cryptanalysis known only in very special cases).

Other Applications: LFSRs can be implemented in hardware, and this makes them useful in applications that require very fast generation of a pseudo-random sequence, such as direct-sequence spread spectrum (a modulation technique) radio.

The Global Positioning System uses a LFSR to rapidly transmit a sequence that indicates high-precision relative time offsets.

In order to keep digital transmissions from forming latent energy patterns that may disrupt other digital or analog transmissions – linear feedback registers are used to create more randomness in the outgoing digital bitstream (this technique is referred to as scrambling). Among the digital broadcasting systems that use linear feedback registers is ATSC, the North American standard for the HDTV transmission system.