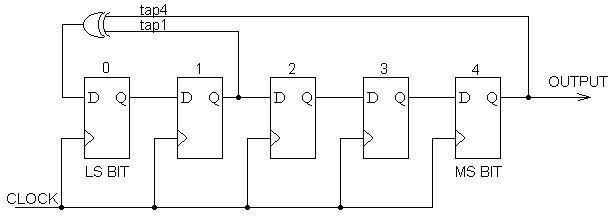
**Introduction**

A **linear feedback shift register** (LFSR) is a [shift register](http://en.wikipedia.org/wiki/Shift_register) whose input bit is a [linear](http://en.wikipedia.org/wiki/Linear_transformation) function of its previous state. The only linear function of single bits is xor, thus it is a shift register whose input bit is driven by the [exclusive-or](http://en.wikipedia.org/wiki/Exclusive-or) (xor) of some bits of the overall shift register value.

The initial value of the LFSR is called the seed, and because the operation of the register is deterministic, the stream of values produced by the register is completely determined by its current (or previous) state. Likewise, because the register has a finite number of possible states, it must eventually enter a repeating cycle. However, an LFSR with a well-chosen feedback function can produce a sequence of bits which appears random and which has a very long cycle.

A n-bit LFSR is a n-bit length shift register with feedback to its input. The feedback is formed by XORing or XNORing the outputs of selected stages of the shift register - referred to as 'taps' - and then inputting this to the least significant bit (stage 0). Each stage has a common clock. The 'linear' part of the term 'LFSR' derives from the fact that XOR and XNOR are linear functions. An example of a 5-bit LFSR is shown below:

[](http://reocities.com/siliconvalley/screen/2257/vhdl/lfsr/lfsrfig1.gif)

5-bit LFSR

This has taps at stages 1 and 4 with XOR feedback. Here, the LS bit of the shift register is, by convention, shown at the left hand side of the shift register, with output being taken from the MS bit at the right hand side. It will produce a pseudorandom sequence of length 2n-1 states (where n is the number of stages) if the LFSR is of [maximal length](http://reocities.com/siliconvalley/screen/2257/vhdl/lfsr/lfsr.html#maxlen). The sequence will then repeat from the initial state for as long as the LFSR is clocked.

**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](http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum) radio. LFSRs have also been used for generating an approximation of [white noise](http://en.wikipedia.org/wiki/White_noise) in various [programmable sound generators](http://en.wikipedia.org/wiki/Programmable_sound_generator).

The [Global Positioning System](http://en.wikipedia.org/wiki/Global_Positioning_System) uses an LFSR to rapidly transmit a sequence that indicates high-precision relative time offsets.

### Uses as counters

The repeating sequence of states of an LFSR allows it to be used as a [clock divider](http://en.wikipedia.org/wiki/Clock_divider), or as a counter when a non-binary sequence is acceptable as is often the case where computer index or framing locations need to be machine-readable. LFSR [counters](http://en.wikipedia.org/wiki/Counter) have simpler feedback logic than natural binary counters or [Gray code](http://en.wikipedia.org/wiki/Gray_code) counters, and therefore can operate at higher clock rates. However it is necessary to ensure that the LFSR never enters an all-zeros state, for example by presetting it at start-up to any other state in the sequence.

### Uses in cryptography

LFSRs have long been used as [pseudo-random number generators](http://en.wikipedia.org/wiki/Pseudo-random_number_generator) for use in [stream ciphers](http://en.wikipedia.org/wiki/Stream_cipher) (especially in [military](http://en.wikipedia.org/wiki/Military) [cryptography](http://en.wikipedia.org/wiki/Cryptography)), due to the ease of construction from simple [electro-mechanical](http://en.wikipedia.org/wiki/Electromechanical) or [electronic circuits](http://en.wikipedia.org/wiki/Electronic_circuits), long [periods](http://en.wikipedia.org/wiki/Periodic_function), and very uniformly [distributed](http://en.wikipedia.org/wiki/Probability_distribution) output streams. However, an LFSR is a linear system, leading to fairly easy [cryptanalysis](http://en.wikipedia.org/wiki/Cryptanalysis). For example, given a stretch of known plaintext and corresponding ciphertext, an attacker can intercept and recover a stretch of LFSR output stream used in the system described, and from that stretch of the output stream can construct an LFSR of minimal size that simulates the intended receiver. This LFSR can then be fed the intercepted stretch of output stream to recover the remaining plaintext.

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

* [Non-linear](http://en.wikipedia.org/wiki/Non-linear) combination of several [bits](http://en.wikipedia.org/wiki/Bit) from the LFSR [state](http://en.wikipedia.org/wiki/State_%28computer_science%29).
* Non-linear combination of the output bits of two or more LFSRs.
* Irregular clocking of the LFSR, as in the [alternating step generator](http://en.wikipedia.org/wiki/Alternating_step_generator).

### Uses in digital broadcasting and communications

To prevent short repeating sequences (e.g., runs of 0's or 1's) from forming spectral lines that may complicate symbol tracking at the receiver or interfere with other transmissions, linear feedback registers are often used to "randomize" the transmitted bit stream. This randomization is removed at the receiver after demodulation. When the LFSR runs at the same rate as the transmitted symbol stream, this technique is referred to as [scrambling](http://en.wikipedia.org/wiki/Scrambler_%28randomizer%29). When the LFSR runs considerably faster than the symbol stream, expanding the bandwidth of the transmitted signal, this is [direct-sequence spread spectrum](http://en.wikipedia.org/wiki/Direct-sequence_spread_spectrum).

Digital broadcasting systems that use linear feedback registers:

* [ATSC Standards](http://en.wikipedia.org/wiki/ATSC_Standards) (digital TV transmission system – North America)
* [DAB](http://en.wikipedia.org/wiki/Digital_Audio_Broadcasting) ([Digital Audio Broadcasting](http://en.wikipedia.org/wiki/Digital_Audio_Broadcasting) system – for radio)
* [DVB-T](http://en.wikipedia.org/wiki/DVB-T) (digital TV transmission system – Europe, Australia, parts of Asia)
* [NICAM](http://en.wikipedia.org/wiki/NICAM) (digital audio system for television)

Other digital communications systems using LFSRs:

* [IBS](http://en.wikipedia.org/w/index.php?title=INTELSAT_business_service&action=edit&redlink=1) (INTELSAT business service)
* [IDR](http://en.wikipedia.org/w/index.php?title=Intermediate_data_rate&action=edit&redlink=1) (Intermediate Data Rate service)
* [SDI](http://en.wikipedia.org/wiki/Serial_digital_interface) (Serial Digital Interface transmission)
* Data transfer over [PSTN](http://en.wikipedia.org/wiki/PSTN) (according to the [ITU-T](http://en.wikipedia.org/wiki/ITU-T) V-series recommendations)
* [CDMA](http://en.wikipedia.org/wiki/CDMA) (Code Division Multiple Access) cellular telephony
* [100BASE-T2 "fast" Ethernet](http://en.wikipedia.org/wiki/Fast_Ethernet#100BASE-T2) scrambles bits using an LFSR
* [1000BASE-T Ethernet](http://en.wikipedia.org/wiki/Gigabit_Ethernet#1000BASE-T), the most common form of Gigabit Ethernet, scrambles bits using an LFSR
* [PCI Express](http://en.wikipedia.org/wiki/PCI_Express) 3.0
* [USB 3.0](http://en.wikipedia.org/wiki/USB_3.0)
* [IEEE 802.11a](http://en.wikipedia.org/wiki/IEEE_802.11a) scrambles bits using an LFSR