Linear Feedback Shift Register Megafunction

Target Application:
Digital Signal Processing
Wireless Communications

Family:
FLEX 10K and FLEX 8000

Vendor:

NOVA
E N G I N E E R I N G

Nova Engineering, Inc.
5 Circle Freeway Drive
Cincinnati, OH 45246
Tel.   (513) 860-3456
Fax   (513) 860-3535
E-mail   sales@nova-eng.com
WWW   http://www.nova-eng.com

Features

■ Programmable pattern length
■ Automatic resizing and feedback selection
■ Programmable initial value (IV)
■ Optimized for the Altera FLEX® 10K and FLEX 8000 device architectures
■ Applications
– Encryption/decryption
– Direct sequence spread spectrum
– Pseudo-random number (PN) generation
– Scrambler/de-scrambler
– Built-in self test

General Description

A linear feedback shift register (LFSR) megafunction is based on linear XOR or XNOR feedback logic in which the initial value of the shift register, shift register taps, and feedback logic determines the output sequence. This scheme allows the user to load the shift register with an initialization sequence. The shift register taps are combined with XOR or XNOR logic and then fed back into the shift register input.

The LFSR megafunction is designed for applications in digital signal processing (DSP) and wireless telecommunication systems. Figure 1 shows a block diagram of the LFSR megafunction.

Figure 1. LFSR Megafunction Block Diagram
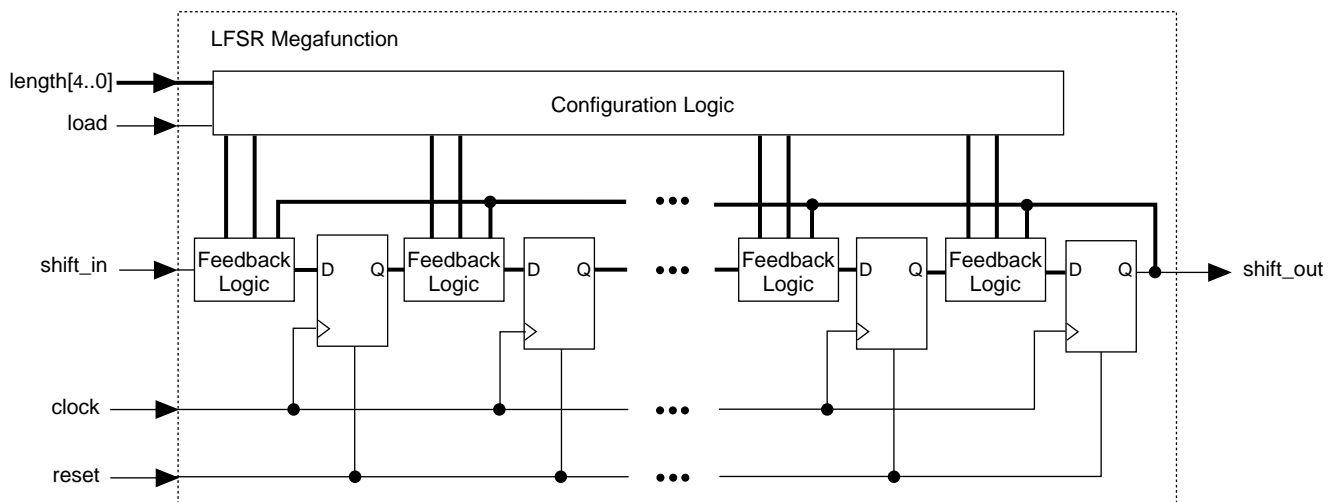
Functional Description

The shift register size (m) is equal to length + 1, where length is an integer between 1 and 31. The shift register produces a sequence of $2^m - 1$ bits. For example, a shift register size of 32 produces a shift register sequence of $2^{32} - 1$ bits and is specified by setting the length input to 31. The length input is synchronous to the rising edge of the clock. When a clock edge loads the length input, the megafunction will automatically reconfigure the shift register's size.

The load input initializes the contents of the shift register. Whenever load is asserted, the megafunction configures itself to a normal shift register size of 32. The desired initial value will be loaded through the shift_in input using 32 clock cycles. Because the length value is ignored when load is asserted, length can be asserted any time before load de-asserts. The load input can be de-asserted after the 32nd rising clock edge. The next rising edge of the clock would then configure the shift register size and feedback logic and initialize the length sequence.

Ports

Table 1 describes the ports for the LFSR megafunction.

Name	Type	Description
length[4..0]	Input	A 5-bit word that determines the shift register size (length + 1).
load	Input	Asserted high to serially shift in user data.
shift_in	Input	Serial input data to the shift register when load is asserted. Otherwise, it is ignored.
clock	Input	System clock.
reset	Input	Asynchronous reset, active high.
shift_out	Output	Serial data output.

Table 1. LFSR Megafunction Ports

Parameters

Nova Engineering will customize the LFSR megafunction's shift register size and the feedback configuration to meet user specifications. This customization reduces logic usage and optimizes area and performance. Table 2 describes these parameters.

Name	Typical Values	Description
Shift register size(s)	2 to 32 bits	Specified by user.
Feedback logic configuration	XOR	Can be customized for either XOR or XNOR applications.

Table 2. LFSR Megafunction Parameters

Performance

The LFSR megafunction is designed for both FLEX 10K and FLEX 8000 device architectures. In FLEX 10K devices, the megafunction are designed for maximum performance, and does not use embedded array blocks (EABs).

Table 3 illustrates the typical device utilization and maximum clock frequency for the LFSR megafunction in an EPF10K10-3 device. Custom configurations differ in logic cell usage, but generally maintain the same speed performance.

Table 3. Typical Device Utilization for the LFSR Megafunction in an EPF10K10-3 Device			
Implementation	**Clock (f_{MAX})**	**Logic Cells**	**EABs**
Shift register size = 32 bits	78 MHz	325	0

Applications

The megafunction's use in encryption/decryption, direct sequence spread spectrum, and data scrambling/descrambling applications are described below.

Encryption/Decryption

The user can encrypt and decrypt serial data streams by initializing the transmitting LFSR megafunction with a desired sequence or key. The serial data stream to be encrypted is simply combined with the LFSR output using an exclusive-OR gate. To decrypt the data, the receiving LFSR megafunction performs the same operation. It is initialized with the same key used by the transmitting megafunction. The encrypted data is then combined with the LFSR output using an exclusive-OR gate. The received data stream must be aligned with the LFSR output sequence. Moreover, synchronized pattern is used to detect the first bit. Normally, the synchronization pattern is not encrypted, which makes detecting the first data bit and performing the PN code alignment much easier.

In addition, an LFSR megafunction can generate long sequences of nearly random data. A 50-bit LFSR megafunction has a repetition period of $2^{50} - 1$ clock periods. Longer bit lengths will cause longer repetition cycles. For example, when clocking at the maximum rate of 75 MHz, a 50-bit pattern in continuous operation would not repeat for six months.

Direct Sequence Spread Spectrum

Direct sequence spread spectrum is a modulation technique used to "spread" the energy of a transmitted signal over a wide band of frequencies. The wide band spreading causes the modulated signal to appear spectrally as random noise. The clock rate of the PN generator is usually much higher than the data rate. A long PN sequence operating at a high frequency produces a wide band signal. The high frequencies are produced when the PN generator sequences through a series of alternating 1s and 0s (e.g., 101010101). In contrast, low frequencies are produced when the PN generator sequences through long patterns of 1s and 0s (e.g., 1111111. . . 0000000. . .).

In direct sequence spread spectrum, the transmitted signal is immune to continuous wave (CW) interference from either intentional or unintentional sources. A CW tone appears in the frequency domain as a narrow band signal. During transmission, CW tones are imposed onto the wide band signal. The signal plus interference are despread at the receiver. The despreading causes the wide band signal to revert to a narrow band signal. The CW interference appears as wide band noise after despreading and can be attenuated by narrow band filtering.

In addition, direct sequence spread spectrum is inherently secure. That is, the transmitted energy is spread over a wide band and appears as noise to an unauthorized listener. An intended receiver, however, knows the exact PN sequence that was used to spread the data signal and can despread the signal by reapplying the same PN sequence. It is important to align the PN sequence applied at the receiver with the PN sequence applied at the transmitter; this procedure is usually accomplished during the acquisition process.

XOR logic is configured on the received data stream with the various PN sequence phases until the PN sequence phase embedded in the receive stream matches the PN sequence being evaluated. Once a match occurs, the data "collapses" back into a narrow band signal. The increased energy within the expected data bandwidth is used to detect the matching PN sequence phase. This process is commonly referred to as "autocorrelation" because the PN sequence is being correlated to itself. In addition, multiple PN generators can be combined to build specific codes (i.e., gold codes) for applications like CDMA.

Scrambler/Descrambler

A scrambler/descrambler limits the DC component of a digital data stream. A data stream containing long consecutive strings of 1s or 0s—such as in transmitting constant 0s—will produce spectral components at DC. Usually, this format is not desirable because most systems need to ensure that sufficient transitions are minimized for both time tracking and spectral peak detection. Minimizing sufficient transitions prevent interference with co-channel users. Another application requiring a scrambler/descrambler is an AC coupled system that droops to its zero-value if the data does not contain some minimum transition density.

The LFSR megafunction can be configured to generate a maximal length sequence that has a short repetition period. The data stream is then combined with the LFSR megafunction's output using XOR logic. Combining the data stream with the megafunction's output ensures that the transitions at the XOR logic gate output are not longer than 2^m bits.