Linear-Feedback Shift Registers (LFSRs)

Hayden Gebhardt

August 23, 2023

Contents

1 Theory

A Linear Feedback Shift Register is a digital circuit or algorithm used to generate pseudorandom sequences of binary digits (bits). It is a shift register with feedback logic that produces a sequence of bits based on the current contents of the register and a predefined feedback polynomial. LFSRs are widely used in various applications, including cryptography, pseudorandom number generation, error detection and correction, digital signal processing, and more.

1.1 Structure

An LFSR comprises the following key components:

- **Shift Register:** A sequence of flip-flops, typically implemented using D-type or JK-type flip-flops, connected in series. Each flip-flop stores a single binary digit (bit).
- **Feedback Logic:** The feedback logic consists of XOR gates that combine specific bits from the shift register based on a feedback polynomial. This logic generates the new bit to enter the leftmost (or rightmost) flip-flop during each clock cycle.
- **Feedback Polynomial:** The feedback polynomial is a binary polynomial represented by its coefficients, which are either 0 or 1. The polynomial dictates the connections of the XOR gates in the feedback logic.

1.1.1 Feedback Polynomial

The feedback polynomial determines the arrangement of XOR gates and the taps (points from which bits are extracted) in the shift register. The taps are selected based on the non-zero coefficients of the feedback polynomial.

For example, if the feedback polynomial is x^4+x^3+1, the taps are usually located at the fourth and third flip-flops from the right. The XOR of the bit values at these taps, along with the XOR of other taps as defined by the polynomial, forms the feedback value.

1.2 Characteristics and Properties

- **Periodicity:** LFSRs generate pseudorandom sequences with a maximum period that depends on the number of bits in the shift register and the chosen feedback polynomial. The period is the number of clock cycles before the sequence repeats.

- **Linearity:** LFSRs are linear systems due to the XOR operations involved in the feedback logic.

- **Auto-Correlation:** Autocorrelation is a fundamental property of signals and sequences that describes the similarity between a signal and a delayed version of itself. In the context of Maximal Length Sequences (MLS), which are generated by Linear Feedback Shift Registers with specific properties, autocorrelation plays a significant role in various applications, particularly in fields like cryptography, communication systems, and signal processing. Autocorrelation measures the similarity between a signal and a delayed version of itself. Mathematically, the autocorrelation of a discrete signal or sequence $x[n]$ at a time offset k is given by:

$$R_x[k] = \sum_n x[n] * x[n-k] \tag{1}$$

  In the context of MLS, the autocorrelation function indicates how well a sequence matches with its delayed version, and it plays a crucial role in various practical applications. The autocorrelation (M) of an MLS is always calculated as follows:

$$M = 2^n - 1 \tag{2}$$

  Where "n" is the number of logical stages within the Linear Feedback Shift Register.

  Maximal Length Sequences (MLS) MLS are binary sequences generated by LFSRs with feedback polynomials that result in a maximum-length cycle before repetition. These sequences have desirable properties, including:

  – Long period before repetition.

- Balanced distribution of 1s and 0s.
- Low cross-correlation with shifted versions of themselves.

Importance of Autocorrelation in MLS

- Cryptography: In cryptographic applications, MLS with low autocorrelation are preferred. Low autocorrelation minimizes the likelihood of patterns in the sequence, making the MLS more suitable for use as pseudorandom keys in encryption algorithms.
- Spread Spectrum Communication: Autocorrelation properties are crucial in spread spectrum communication, where MLS are used for spreading signals over a wide bandwidth. Low autocorrelation helps minimize interference and enhances signal detection.
- Radar and Sonar: In radar and sonar systems, MLS with desirable autocorrelation properties are used for generating probing signals with good range resolution.

Autocorrelation Function Characteristics

The autocorrelation function of a maximal length sequence has some distinctive properties:

- Peak at Zero Delay: The autocorrelation function has a sharp peak at zero time delay, indicating that the MLS is very similar to itself without any delay.
- Low Sidelobes: The sidelobes (peaks away from zero delay) of the autocorrelation function are very small, indicating that the sequence has minimal correlation with its shifted versions.
- Dirac Comb Structure: The autocorrelation function resembles a Dirac comb structure, with impulses at integer multiples of the sequence length. This is a result of the maximal length property.

Cross-Correlation and Autocorrelation

MLS not only have low autocorrelation but also low cross-correlation with shifted versions of themselves. This property is essential in applications where multiple sequences need to be distinguishable, as in code-division multiple access (CDMA) communication systems.

2 Implementation

When implementing LFSRs in **microcontrollers**, the following considerations apply:

- Choosing Register Length: Select the register length based on the desired sequence length and available resources. Longer registers yield longer pseudorandom sequences but require more processing time.
- Clock Speed and Timing: LFSRs require a clock signal to operate. Ensure the clock speed and timing are appropriate for your application.
- Initialization: Initialize the LFSR with a nonzero seed value to avoid non-random outputs.
- Output Generation: Choose an appropriate tap for output generation, considering the desired characteristics of the pseudorandom sequence.
- Connecting to Other Components: LFSRs can be integrated with other microcontroller components to achieve specific functionality.

2.1 Common Structures

2.1.1 Fibonacci LFSR

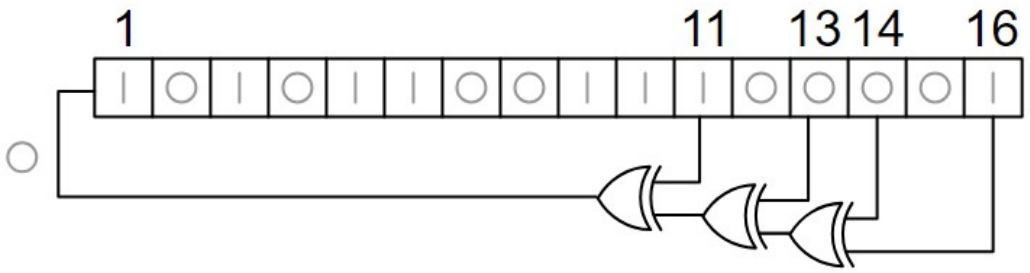

Figure 1: Fibonacci LFSR with combined XOR feedback. Source: Wikipedia

Feedback Polynomial

- In Fibonacci LFSRs, the feedback polynomial is typically chosen with fewer taps, which may lead to shorter periods compared to other LFSR structures. The selection of taps is often more straightforward, making these LFSRs easier to design and implement.

Characteristics

- Ease of Implementation: Fibonacci LFSRs can be simpler to design and implement due to the reduced number of taps in the feedback polynomial. This structure is particularly useful when precise and timely code execution is required.
- Reduced Hardware Complexity: The simplicity of Fibonacci LFSRs may lead to lower hardware complexity and reduced power consumption.

Applications

- Error Detection and Correction: Fibonacci LFSRs are used in error-detection codes like CRC (Cyclic Redundancy Check), where shorter periods are sufficient for checking data integrity.
- Digital Signal Processing: Fibonacci LFSRs find applications in signal processing tasks like signal modulation and generation of pseudorandom sequences for spread spectrum communication.

2.1.2 Gaussian LFSR

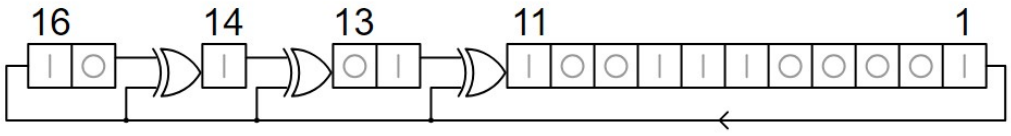

Figure 2: Gaussian LFSR with state sequential XOR feedback. Source: Wikipedia

Feedback Polynomial

- In Gaussian LFSRs, the feedback polynomial is chosen in a way that maximizes the length of the LFSR's period, resulting in a longer pseudorandom sequence before repetition occurs. This polynomial is often selected from a set of primitive polynomials over a finite field, such as Galois fields.

Characteristics

- Longer Periods: Gaussian LFSRs tend to produce longer pseudorandom sequences before cycling back to the initial state. This property is particularly useful in applications requiring extended sequences with minimal repetition.

Applications

- Cryptography: Gaussian LFSRs are used in stream ciphers where longer periods enhance security by reducing the predictability of the pseudorandom keystream.
- Random Number Generation: For applications demanding high-quality random numbers, Gaussian LFSRs can provide longer sequences before exhibiting repetition.

3 References

"Linear Feedback Shift Register.", Wikipedia, Wikimedia Foundation, 28 July 2023, https://en.wikipedia.org/wiki/Linear- feedback-shift-register.

Shift Register Sequences, Solomon W. Golomb, Holden-Day, 1967.