ISSN 2320 - 2602
Volume 14 No. 9, September 2025
International Journal of Advances in Computer Science and Technology
Available Online at http://www.warse.org/IJACST/static/pdf/file/ijacst011492025.pdf
https://doi.org/10.30534/ijacst/2025/011492025

Entropy Analysis of Galois LFSR-Based Pseudorandom Binary Sequence Generators

Arsen Kovalchuk
State University "Kyiv Aviation Institute", Ukraine, kovalchuk.arsen1@gmail.com

Received Date : July 25, 2025 Accepted Date : August 27, 2025 Published Date : September 07, 2025

ABSTRACT

The problem of searching for aperiodic binary sequences with high entropy and uniform element distribution presents significant computational complexity, particularly as the sequence length increases. Such sequences are of crucial importance in communication engineering, radar systems[4], spectroscopy, quantum physics, chemistry, digital signal processing, and cryptography [3]. This paper examines the possibility of employing generators based on Galois fields, in particular linear feedback shift registers in Galois configuration (Galois LFSR), for constructing binary pseudorandom sequences and evaluating their entropic characteristics. A brief overview of the algebraic foundations of sequence generation in finite fields GF(2) through primitive polynomials is provided [2]. The obtained results can be applied to the design of signals with defined statistical properties, including high information density, which is critically important for spread spectrum systems and cryptographic protocols.

Key words: binary sequence, Galois fields, linear feedback shift registers, entropy, pseudorandom sequences, primitive polynomials.

1. INTRODUCTION

Binary sequences represent a class of pseudorandom sequences consisting of an ordered set of symbols, each of which can take the values 1 and –1 (or 1 and 0 in computer representation).

$$a_j \in \{0,1\} \text{ for } j = 0,1,...,N-1 \qquad (1)$$

The generation of such sequences is carried out using deterministic algorithms, finite automata, or linear feedback shift registers (LFSRs), which are hardware-efficient and exhibit statistical behavior close to randomness. Despite their deterministic nature, these sequences can be characterized by a high level of entropy, indicating unpredictability and the absence of excessive structure. This makes them valuable for noise modeling, data encryption, and the construction of test signals.

A special place among them is occupied by maximum-length sequences (m-sequences), which are generated by primitive polynomials over the Galois field GF(2). They are characterized by the maximum possible entropy for a given length, a uniform distribution of zeros and ones, and optimal statistical properties, including an almost ideal (two-valued) autocorrelation function. A defining feature of m-sequences is that for a register of length *r*, the sequence has a period of $2^r - 1$, traversing all possible nonzero states.

PRBS (Pseudorandom Binary Sequence) generators play a key role in telecommunications: in the conversion of analog signals into digital form, testing of communication channels, as well as in cryptographic schemes, time-of-flight spectroscopy, and statistical methods of signal analysis. Among the variants of LFSRs, the Galois configuration is considered more efficient in hardware implementation, as it enables sequence generation with reduced delays. Its operation is also based on finite fields GF(2^n), where the generator sequence is defined by a feedback polynomial, which must be primitive in order to achieve the maximum cycle length and the highest entropy of the output sequence.

In this work, the process of constructing binary sequences with predefined entropic characteristics based on Galois generators is analyzed, along with the computation of additional statistical parameters that determine the quality of the sequences both in randomness tests and in communication applications. The theoretical analysis is supported by simulation results.

2 . CONSTRUCTION OF GALOIS GENERATORS

Within the subset of classical generators of pseudorandom sequences with maximum period, we include those constructed on the basis of linear feedback shift registers (LFSRs) with a single feedback loop, defined exclusively by a primitive polynomial (PP), which serves as the generating polynomial of the generator. In number theory and Galois field theory, an irreducible polynomial f_n of degree *n* is called

primitive over *GF(p)* if and only if f_n is a monic polynomial, nonzero, and its order satisfies the required conditions [1].

$$ord(f_n) = p^n - 1 \qquad (2)$$

As register cells of LFSRs, D-type flip-flops are commonly used. These devices rewrite the input signal to the output at the moment of the clock pulse arrival. An example of a fourth-order Galois generator, in which the feedback is formed by a primitive polynomial of degree four $f = 1'0011$, is shown in Figure 1.

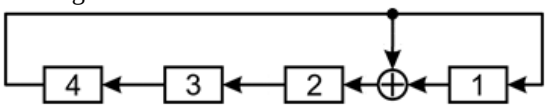

Figure 1: Structural diagram of a PRBS generator in Galois configuration

As follows from the structural diagram of the generator (Figure 1), the feedback connections in classical maximum-period Galois generators (registers) are uniquely determined by the chosen primitive polynomial f_n of degree n. They are constructed in the following way: the outputs of each register cell (D flip-flop) are connected to the inputs of the subsequent cells, serving as their excitation functions. In addition, the output of the most significant register cell is fed back (via an XOR scheme) to the inputs of those, and only those, register cells whose indices correspond to the indices of the nonzero monomials of the primitive polynomial. Here, the rightmost monomial of the polynomial f_n, as well as the least significant register cell, corresponds to index 1.

Using Figure 1, we can derive the monomial rule according to which structural diagrams of classical LFSRs in the Galois configuration are constructed. To do this, we augment the diagram with dashed lines placed in those parts of the lower row of D flip-flops where XOR operators are absent. Next, we assign the value "1" above solid vertical lines (feedback connections) and "0" above dashed lines. This procedure leads to Figure 2, which coincides structurally with Figure 1.

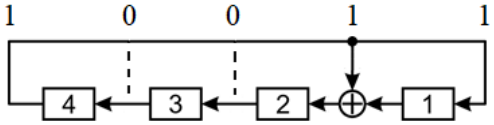

Figure 2: Construction of the structural diagram of a fourth-order Galois generator

As follows from Figure 2, the ones of the primitive polynomial in vector form determine the positions of the vertical lines in the single-loop feedback scheme of a classical Galois LFSR-based PRBS generator. To demonstrate the application of the formulated rule for constructing the structural diagram of a maximum-period pseudorandom sequence generator in the Galois configuration, let us illustrate it using the example of a generator defined by a primitive polynomial of degree eight $f = 1'0110'0101$. The solution of this task involves the implementation of the following two synthesis stages.

Stage 1. Construct an eight-bit ring shift register Figure 3, in which the nodes of the feedback line are marked equidistantly with the digits of the selected primitive polynomial:

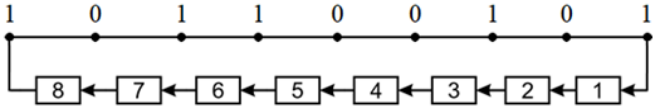

Figure 1: Basis diagram of an eight-bit Galois PRBS generator

Stage 2. By connecting the individual nodes of the feedback line through an XOR operator, as shown in Figure 4, we complete the construction of the classical Galois LFSR generator defined by the primitive polynomial of degree eight $f = 1'0110'0101$.

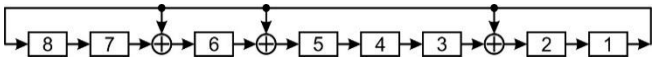

Figure 2: Structural diagram of the Galois PRBS generator

3 ENTROPY

One of the key metrics that determines the level of randomness in a binary sequence is Shannon entropy [5]. It estimates the average amount of information carried by a single bit of the sequence and reaches its maximum when the symbols 0 and 1 are equally probable. For a binary sequence of length N, consisting of zeros and ones, the entropy is defined as:

$$H = -p_0 \log_2(p_0) - p_1 \log_2(p_1) \qquad (3)$$

where p_0 and p_1 are the probabilities of occurrence of symbols 0 and 1, respectively.

In practice, these probabilities can be estimated using the relative frequencies:

$$p_1 = \frac{N_1}{N},\ p_0 = 1 - p_1 = \frac{N - N_1}{N}, \qquad (4)$$

where N_1 is the number of ones in the sequence.

In the case of maximum-length sequences (m-sequences) generated by LFSRs based on a primitive polynomial over GF(2), the period of the sequence is $L = 2^r - 1$, where r denotes the register length. It is known that m-sequences have the following symbol distribution:

$$N_1 = 2^{r-1},\ N_0 = 2^{r-1} - 1, \qquad (5)$$

that is, the ratio between the number of ones and zeros is maximally balanced for odd N, and the probabilities are given by:

$$p_1 = \frac{2^{r-1}}{2^r - 1},\ p_0 = \frac{2^{r-1} - 1}{2^{r-1}} \qquad (6)$$

Substituting these values into the entropy formula yields the analytical estimate:

$$H_r = -\frac{2^{r-1}}{2^r - 1}\log_2\left(\frac{2^{r-1} - 1}{2^{r-1}}\right) - \frac{2^{r-1}}{2^r - 1}\log_2\left(\frac{2^{r-1}}{2^r - 1}\right) \qquad (7)$$

The histogram of symbol distribution for a sequence of length $2^{32} - 1$ demonstrates an almost perfect balance: the probabilities of 0 and 1 are both close to 0.5 with minimal

deviation Figure 5. This visually confirms the bit-level balance, making the sequences suitable for noise modeling and basic cryptographic applications.

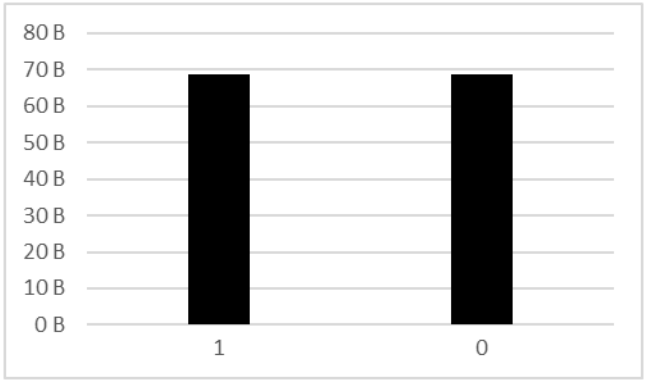

Figure 3 : Bit-level entropy $GF(2^{32})$

At the byte level, when grouping bits into blocks of 8, with 256 possible symbols, the histogram of distribution also demonstrates exceptionally high uniformity: all byte values occur with nearly equal probability and minimal deviations. This ensures entropy values approaching the theoretical maximum of 8 bits [5] Figure 6. Such a property makes m-sequences highly valuable for practical applications where strong unpredictability is critical: in cryptographic protocols, in the generation of test input data for system stress testing, in modeling noise characteristics of communication channels, as well as in spectral analysis and signal coding methods.

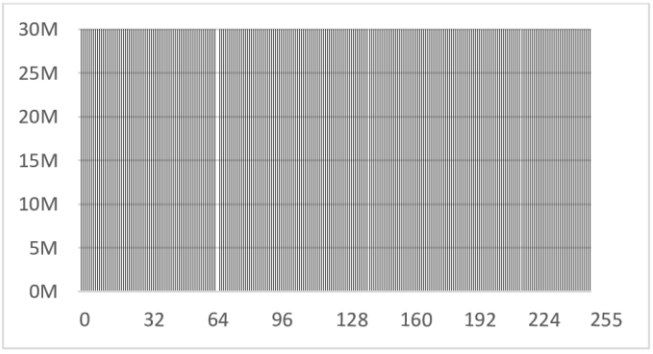

Figure 4: Byte-level entropy $GF(2^{32})$

4. CONCLUSION

This study investigated the application of linear feedback shift registers (LFSRs) in the Galois configuration, constructed on the basis of primitive polynomials over GF(2), for the generation of maximum-length pseudorandom binary sequences. It was demonstrated that the resulting m-sequences achieve the maximum possible period, defined by the register order r, and provide a uniform distribution of zeros of zeros and ones with minimal deviation.

Experimental evaluation confirmed a high level of Shannon entropy: at the bit level, values approach 1 bit per symbol, while at the byte level, they approach the theoretical maximum of 8. These results indicate strong statistical randomness of the generated sequences and uniform symbol distribution across multiple scales.

Overall, the findings confirm that Galois-based generators combine hardware efficiency with high-quality pseudorandom output streams, making them suitable for applications in telecommunications, cryptography, and measurement systems.

REFERENCES

1. Anatoly Beletsky, Alexander. Beletsky. **Synthesis of Primitive Matrices over Finite Galois Fields and Their Applications**, journal of Information Technologies in Education, No. 13, pp. 23-43, June 2012.
2. J. Espinosa García, G. Cotrina, P. Alberto, O. Andrés. **Security and Efficiency of Linear Feedback Shift Registers in GF(2ⁿ) Using n-Bit Grouped Operations,** Mathematics, vol. 10, no. 6, pp. 996-1017, March 2022.
3. T. Helleseth, C. Li. **An Updated Review on Crosscorrelation of m-Sequences**, arXiv:2407.16072, July 2024.
4. Y. Zhu, Y. Li, D. Li, L. Dong, X. Liu, A. Yan, Y. Liu, Z. Wang. **A Theoretical and Experimental Analysis of the Time-Domain Characteristics of a PRBS Phase-Modulated Laser System**, Applied Sciences, vol. 14, no. 20, p. 9198, October 2024
5. S. R. Davies, R. Macfarlane, W. J. Buchanan M. Sorell. **Comparison of Entropy Calculation Methods for Forensic and Security Applications**, Entropy, vol. 17, no. 10, p. 1503, October 2022.