SOCIETY FOR SCIENCE AND EDUCATION
UNITED KINGDOM

TNC TRANSACTIONS ON NETWORKS AND COMMUNICATIONS

VOLUME 7, NO. 2
ISSN: 2054 -7420

A New Type of NLFSR Functions with Maximum Periods

Ibraheem Al-Hejri, Talal Al-Kharobi
College of Computer Sciences and Engineering, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia
alhejri87@gmail.com; talalkh@kfupm.edu.sa

ABSTRACT

Nonlinear feedback shift registers (NLFSRs) have received much attention in designing various cryptographic algorithms such as stream ciphers and light weight block ciphers in the provision of high-level security in communication systems. The main purpose of NLFSRs is to generate pseudorandom sequences of bits. NLFSRs are known to be more secure than their linear counterparts. However, there is no mathematical foundation on how to construct an NLFSR with optimal period. In this paper, we propose a new type of NLFSR function of degree 2 with optimal periods. Using our construction method, we propose 639 new functions of this type with optimal periods.

Keywords: NLFSR; Stream Ciphers; Pseudorandom; Feedback Functions; Optimal Period.

1 Introduction

Feedback shift register (FSR) is a kind of implementation possessing the property of randomness. FSR is one of the most efficient ways to generate pseudorandom sequences. FSR has several applications such as authentication [1], cryptography [2], testing [3], and data compression [4]. FSR has mainly two types: Linear Feedback Shift Register (LFSR) and Non- Linear Feedback Shift Register (NLFSR). Notwithstanding the ease of implementation and speed of LFSR, it can be cryptanalyzed easily due to its linearity and the simplicity of its structure. LFSRs are well studied in literature, with a well-established theory. It is easy to mathematically obtain an LSFR feedback function with an optimal period by using primitive generator polynomials.

An NLFSR is a generalization of LFSR in which the current state is a nonlinear transformation of the previous state. This feature gives NLFSRs the ability to generate a very secure pseudorandom sequence which is hard to break compared to the LFSRs. Thus, to determine the structure of NLFSR, we need at least $\Theta(2^n)$ bits, while we need just $2n$ bits in order to break an LFSR sequence. While the theory behind LFSR is well understood, NLFSRs still have many open fundamental problems. Probably one of the most important issues is to devise a systematic way to construct NLFSRs with optimal periods. Existing algorithms are either only applicable to small NLFSRs or consider certain special cases.

In this paper, we propose a new type of feedback functions of degree 2 that provides optimal periods. Our construction method constructs 639 functions of this type for NLFSRs of sizes $8 \le n \le 23$. The importance of this work lies in generating NLFSR functions that can significantly improve the cryptographic strength of the generators of stream cipher cryptosystems and pseudorandom number generators of many cryptographic algorithms. This paper is organized as follows. Section 2 presents the necessary preliminary information and related definitions.

DOI: 10.14738/tnc.72.6473
Publication Date: 30th April 2019
URL: http://dx.doi.org/10.14738/tnc.72.6473

Section 3 reviews the existing studies related to NLFSR functions with optimal periods. Section 4 describes the proposed construction method. Section 5 presents the new NLFSR feedback functions. Finally, Section 6 concludes the present study and offers recommendations for future work.

2 Preliminaries

An FSR has *n* binary storage cells; each of them can hold a single bit. Each cell $i \in \{0, 1, \ldots, n-1\}$ is linked with a state variable x_i that shows the current value of a cell *i* and the feedback function $f_i : \{0, 1\}^n \rightarrow \{0, 1\}$ which reveals the updated value of the bit *i*. The state of an FSR can be presented as a vector of values of its state variables $(x_0, x_1, \ldots, x_{n-1})$. The period of an FSR is defined as the length of longest repeated output sequence can be obtained. The value of the cell *0* determines the output of an FSR, while the input of an FSR is determined by the value of the cell $n-1$. Figure 1 shows an *n*-bit FSR general structure.

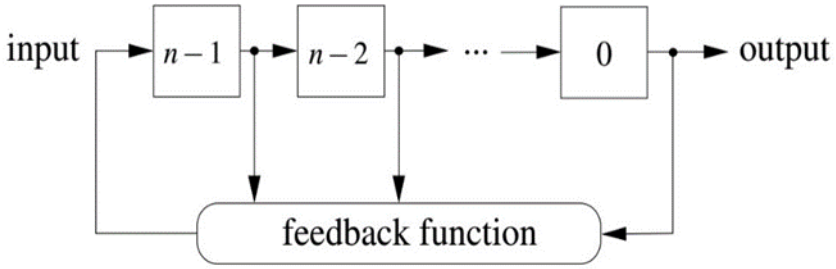

Fig. 1: An n-bit FSR general structure [14]

An FSR is called a Linear Feedback Shift Register (LFSR) when it has only linear feedback functions (i.e. of type $f(x_0, x_1, \ldots, x_{n-1}) = c_0 \cdot x_0 \oplus c_1 \cdot x_1 \oplus \ldots c_{n-1} \cdot x_{n-1}$ where $c_i \in \{0, 1\}$ for $i \in \{0, 1, \ldots, n-1\}$). Otherwise, it is called a Nonlinear Feedback Shift Register.

LFSR is one of the most common methods used to generate pseudo-random sequences. LFSRs are considered a well-known and mature area and most of the fundamental problems associated with LFSRs have been solved. The current state in LFSRs is a linear function of the previous state [5]. Unlike NLFSRs, LFSRs have a unique transformation between Galois and Fibonacci configurations [6] [7] [8].

In LFSRs, de Bruijn sequences can be produced using primitive polynomials and the theory of such sequences is well-understood [9]. The primitive sequence is an important component in cryptography applications. In [10], [11] and [12], it has been proved that the number of sequences which are cyclic equivalent equals:

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

The number of primitive sequences together is B_n as defined in (1). There are $\frac{\varphi(2^n-1)}{n}$ primitive LFSRs, where φ refers to the Euler phi function.

To determine the structure of NLFSR, we need at least $\Theta(2^n)$ bits [13], while we need just $2n$ bits in order to break an LFSR sequence. Figure 2 shows a *4*-bit NLFSR with its feedback function.

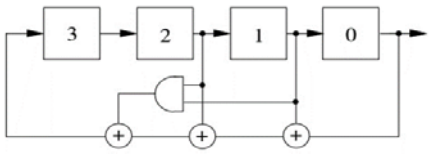

Fig. 2: A 4-bit NLFSR example [14].

There are various functions of $2^{2^{n-1}}$ on (n-1) variables. Therefore, the probability of choosing a primitive NLFSR function of the following FSR form (Where g denotes to a Boolean function on (n-1) variables):

$$f(x_0, x_1, \dots, x_{n-1}) = x_0 + g(x_1, x_2, \dots, x_{n-1}) \quad (2)$$

is given by:

$$\frac{2^{2^{n-1}-n}}{2^{2^{n-1}}} = \frac{1}{2^n} \quad (3)$$

3 Related Work

Non-linear feedback shift register functions have been in the focus of many researchers. For example, in [15] the authors proposed an approach based on heuristic algorithm to find the period of NLFSRs with $n \leq 6$, and used their feedback functions to generate pseudo-random sequences. Although this approach is efficient. However, it is only applicable to small NLFSR feedback functions. In [14] Dubrova presented a list of n-bit NLFSRs with the optimal period 2^{n-1}; *for n < 25*. The study used the following three types of feedback functions with the algebraic degree two.

- Type 1: $f(x_0, x_1, \dots, x_{n-1}) = x_0 \oplus x_a \oplus x_b \oplus x_c \cdot x_d$ (4)
- Type 2: $f(x_0, x_1, \dots, x_{n-1}) = x_0 \oplus x_a \oplus x_b \cdot x_c \oplus x_d \cdot x_e$ (5)
- Type 3: $f(x_0, x_1, \dots, x_{n-1}) = x_0 \oplus x_a \oplus x_b \oplus x_c \oplus x_d \oplus x_e \cdot x_h$ (6)

Where $a, b, c, d, e, h \in \{1, 2, \dots, n-1\}$, $x_i \in \{0, 1\}$, and the addition and multiplication operations are in *mod 2*. However, Dubrova's work did not list all the feedback functions having optimal periods. Almuhammadi et al. [16] proposed a new and efficient construction method. The authors used this method to construct the missing NLFSR feedback functions of the three types given in [14]. They presented complete lists of these types for all sizes n = 4, 5, …, 19. These functions were of degree 2.

On the other hand, several studies did not focus mainly on exploring NLFSR feedback functions with optimal periods. However, they made use of one or more of NLFSR feedback functions as building blocks in different cryptography applications. For instance, Rachwalik et.al. [17] implemented NLFSRs in Field Programmable Gate Arrays (FPGA) in order to construct NLFSR feedback functions with maximum period. The study also showed the statistical properties of the binary sequences of order of *n = 25* and *27*.

Mandal and Gong [18] proposed NLFSRs with optimal period to generate de Bruijn sequences of order *n=23*, *24* and *27*. In [19] an efficient way is proposed to generate a De Bruijn sequence by extending a maximal-length LFSR with *n* stages. The proposed approach could be also used to encrypt images based on chaotic maps [20]. Poluyanenko [21] proposed an approach based on FPGA. This approach proved the ability of FPGAs to generate NLFSR-based sequences of large sizes. The author successfully generated some sequences for sizes n = 26; 27; 28 and 29, without providing any complete list of these sizes.

4 The Construction Method

In this work, we used a sequential construction method similar to the one introduced in [16]. In this method, all NLFSR functions of a specific type are enumerated. Then, an NLFSR period verifier system is implemented to verify the optimality of the generated NLFSR feedback functions. The construction method consists of two steps: the enumeration step and the period-testing step. The enumeration step uses Sequential Function Generator (SFG) method, which enumerates feedback functions by incrementing the subscripts of a given feedback function. Then,

the period-testing algorithm selects a start point of the states of the NLFSRs and determines the period of the sequence by state transforming operations until the start point appears again. Finally, it keeps all the *n*-stage feedback functions generating sequences whose periods achieve 2^{n-1}. The reader may refer to [16] for details about this method and its proof of correctness. The reader may refer to [16] for more details about this method and its proof of correctness.

This work mainly proposes a new type of NLFSR feedback function of degree 2 with optimal periods for $n \leq 23$ as defined in Equation (7).

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0 \oplus x_a \oplus x_b \oplus x_c \oplus x_d \oplus x_e \oplus x_h \oplus x_w \cdot x_z \tag{7}$$

Where $a, b, c, d, e, h, w, z \in \{1, 2, \ldots, n-1\}$, $x_i \in \{0, 1\}$, and the addition (XOR) and multiplication (AND) operations are in *modulo 2*. The feedback function defined in Equation (7) is of algebraic degree2 because the number of variables in the largest product term are two variables. This type of feedback function generates the primitive NLFSRs for which the algebraic normal form of the Boolean function *g* defined in Equation (2) is quite simple.

5 The Proposed Feedback Functions

In this section, the complete list of all proposed NLFSR feedback functions of degree 2 having optimal periods as defined in Equation (7) are given. Table 1 shows a summary of these new functions for $8 \leq n \leq 23$.

Table 1. Summary of the New Feedback Functions of NLFSRs with Optimal Periods for ($8 \leq n \leq 23$).

n	# of Functions	n	# of Functions
8	12	16	84
9	12	17	70
10	34	18	44
11	26	19	23
12	64	20	24
13	64	21	17
14	76	22	12
15	70	23	7
Total	**639**		

A total of (639) new NLFSR functions with optimal periods for $8 \leq n \leq 23$ have been proposed. The new NLFSR feedback functions of this type are listed below. Each entry is of the form *n (0, a, b, c, d, e, h, w, z)* where *n* is the size of NLFSR function, and *a, b, c, d, e, h, w* and *z* are the indices of the variables defined in Equation (7). For example: $f(x_0, x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8) = x_0 \oplus x_2 \oplus x_3 \oplus x_4 \oplus x_5 \oplus x_6 \oplus x_7 \oplus x_1 \cdot x_5$ is an NLFSR function with register size $n = 8$, and it is represented below by the following entry: [8 (0, 2, 3, 4, 5, 6, 7, 1, 5)].

NLFSR Functions, n=8:

(0, 1, 2, 3, 4, 5, 6, 2, 4)
(0, 1, 2, 3, 4, 5, 6, 2, 7)
(0, 1, 2, 3, 4, 5, 6, 3, 7)
(0, 1, 2, 3, 4, 5, 6, 4, 6)
(0, 1, 2, 3, 4, 6, 7, 2, 6)
(0, 1, 2, 3, 4, 6, 7, 5, 7)
(0, 1, 2, 4, 5, 6, 7, 1, 3)
(0, 1, 2, 4, 5, 6, 7, 2, 6)
(0, 2, 3, 4, 5, 6, 7, 1, 5)
(0, 2, 3, 4, 5, 6, 7, 1, 6)
(0, 2, 3, 4, 5, 6, 7, 2, 4)
(0, 2, 3, 4, 5, 6, 7, 4, 6)

NLFSR Functions, n=9:

(0, 1, 2, 3, 4, 5, 7, 1, 7)
(0, 1, 2, 3, 5, 6, 8, 5, 7)
(0, 1, 2, 3, 5, 7, 8, 6, 8)
(0, 1, 2, 4, 5, 6, 8, 1, 6)
(0, 1, 2, 4, 5, 6, 8, 5, 7)
(0, 1, 2, 4, 6, 7, 8, 1, 3)
(0, 1, 3, 4, 5, 6, 7, 2, 3)
(0, 1, 3, 4, 5, 7, 8, 2, 4)
(0, 1, 3, 4, 5, 7, 8, 3, 8)
(0, 1, 3, 4, 6, 7, 8, 2, 4)
(0, 2, 3, 4, 5, 6, 8, 6, 7)
(0, 2, 4, 5, 6, 7, 8, 2, 8)

NLFSR Functions, n=10:

(0, 1, 2, 3, 4, 5, 6, 1, 3)
(0, 1, 2, 3, 4, 5, 6, 1, 7)
(0, 1, 2, 3, 4, 5, 6, 4, 7)
(0, 1, 2, 3, 4, 5, 6, 6, 8)
(0, 1, 2, 3, 4, 5, 8, 1, 3)
(0, 1, 2, 3, 4, 5, 8, 1, 7)
(0, 1, 2, 3, 4, 5, 9, 1, 3)
(0, 1, 2, 3, 4, 6, 7, 6, 8)
(0, 1, 2, 3, 4, 8, 9, 4, 7)
(0, 1, 2, 3, 5, 6, 7, 1, 5)
(0, 1, 2, 3, 6, 7, 9, 2, 4)
(0, 1, 2, 6, 7, 8, 9, 3, 6)
(0, 1, 3, 4, 5, 7, 9, 2, 8)
(0, 1, 3, 4, 5, 7, 9, 3, 6)
(0, 1, 3, 4, 5, 7, 9, 3, 7)
(0, 1, 3, 4, 5, 7, 9, 5, 6)
(0, 1, 3, 4, 6, 7, 8, 1, 3)
(0, 1, 3, 4, 7, 8, 9, 6, 8)
(0, 1, 3, 5, 6, 7, 9, 2, 8)
(0, 1, 3, 5, 6, 7, 9, 3, 7)
(0, 1, 3, 5, 6, 7, 9, 4, 5)
(0, 1, 3, 5, 6, 7, 9, 4, 7)
(0, 1, 5, 6, 7, 8, 9, 7, 9)
(0, 2, 3, 4, 5, 6, 7, 6, 9)
(0, 2, 3, 4, 6, 7, 9, 7, 9)
(0, 2, 5, 6, 7, 8, 9, 3, 9)
(0, 2, 5, 6, 7, 8, 9, 7, 9)
(0, 3, 4, 5, 6, 7, 8, 1, 4)
(0, 3, 4, 5, 7, 8, 9, 5, 9)
(0, 3, 4, 6, 7, 8, 9, 2, 4)
(0, 4, 5, 6, 7, 8, 9, 2, 4)
(0, 4, 5, 6, 7, 8, 9, 3, 6)
(0, 4, 5, 6, 7, 8, 9, 3, 9)
(0, 4, 5, 6, 7, 8, 9, 7, 9)

NLFSR Functions, n=11:

(0, 1, 2, 3, 4, 5, 7, 6, 10)
(0, 1, 2, 3, 5, 8, 9, 2, 9)
(0, 1, 2, 3, 6, 7, 9, 5, 8)
(0, 1, 2, 4, 6, 7, 8, 2, 6)
(0, 1, 2, 4, 7, 8, 10, 9, 10)
(0, 1, 2, 5, 6, 7, 9, 1, 6)
(0, 1, 2, 6, 7, 8, 10, 6, 7)
(0, 1, 3, 4, 5, 9, 10, 4, 5)
(0, 1, 3, 4, 7, 8, 9, 5, 9)
(0, 1, 3, 4, 7, 9, 10, 1, 2)
(0, 1, 3, 5, 7, 8, 9, 3, 5)
(0, 2, 3, 4, 5, 6, 8, 5, 6)
(0, 2, 3, 4, 6, 8, 9, 1, 3)
(0, 2, 3, 4, 6, 8, 9, 2, 10)
(0, 2, 3, 4, 6, 8, 10, 6, 8)
(0, 2, 3, 4, 7, 8, 10, 2, 6)
(0, 2, 3, 5, 6, 7, 9, 4, 9)
(0, 2, 3, 5, 7, 8, 9, 1, 9)
(0, 2, 3, 5, 7, 8, 9, 8, 10)
(0, 2, 3, 6, 8, 9, 10, 2, 9)
(0, 2, 4, 5, 6, 8, 9, 2, 7)
(0, 2, 4, 5, 6, 9, 10, 5, 10)
(0, 2, 4, 5, 8, 9, 10, 3, 6)
(0, 3, 4, 5, 7, 9, 10, 5, 9)
(0, 3, 5, 6, 7, 8, 9, 5, 6)
(0, 4, 6, 7, 8, 9, 10, 1, 5)

NLFSR Functions, n=12:

(0, 1, 2, 3, 4, 6, 9, 3, 9)
(0, 1, 2, 3, 4, 6, 9, 5, 11)
(0, 1, 2, 3, 4, 7, 8, 4, 10)
(0, 1, 2, 3, 4, 8, 9, 3, 9)
(0, 1, 2, 3, 5, 7, 11, 2, 3)
(0, 1, 2, 3, 5, 9, 11, 8, 9)
(0, 1, 2, 3, 6, 8, 9, 1, 5)
(0, 1, 2, 3, 6, 9, 10, 4, 11)
(0, 1, 2, 3, 6, 9, 10, 5, 6)
(0, 1, 2, 4, 5, 6, 11, 4, 9)
(0, 1, 2, 4, 5, 7, 8, 6, 10)
(0, 1, 2, 4, 5, 8, 9, 4, 5)
(0, 1, 2, 4, 7, 9, 10, 3, 11)
(0, 1, 2, 4, 8, 9, 11, 2, 5)
(0, 1, 2, 5, 6, 10, 11, 1, 6)
(0, 1, 2, 5, 7, 9, 10, 3, 5)

(0, 1, 2, 6, 7, 8, 11, 4, 6)
(0, 1, 2, 6, 7, 10, 11, 6, 11)
(0, 1, 3, 4, 5, 6, 10, 2, 8)
(0, 1, 3, 4, 5, 7, 11, 6, 11)
(0, 1, 3, 4, 5, 8, 9, 3, 9)
(0, 1, 3, 4, 7, 8, 10, 2, 8)
(0, 1, 3, 4, 8, 10, 11, 7, 10)
(0, 1, 3, 5, 7, 9, 10, 7, 11)
(0, 1, 3, 7, 9, 10, 11, 3, 4)
(0, 1, 4, 5, 6, 7, 8, 2, 9)
(0, 1, 4, 5, 6, 9, 10, 1, 6)
(0, 1, 4, 5, 6, 10, 11, 6, 8)
(0, 1, 4, 6, 7, 8, 9, 5, 11)
(0, 1, 4, 7, 8, 9, 10, 2, 11)
(0, 1, 5, 7, 8, 9, 11, 1, 6)
(0, 1, 5, 7, 9, 10, 11, 9, 10)

(0, 1, 6, 7, 8, 9, 10, 6, 8)
(0, 1, 6, 7, 8, 10, 11, 3, 8)
(0, 2, 3, 4, 5, 6, 11, 4, 6)
(0, 2, 3, 4, 5, 7, 8, 5, 10)
(0, 2, 3, 4, 5, 8, 11, 1, 10)
(0, 2, 3, 5, 7, 8, 9, 2, 8)
(0, 2, 3, 5, 7, 8, 10, 3, 9)
(0, 2, 3, 5, 7, 9, 11, 1, 5)
(0, 2, 3, 5, 7, 10, 11, 7, 9)
(0, 2, 3, 5, 8, 10, 11, 1, 9)
(0, 2, 3, 6, 7, 8, 9, 9, 10)
(0, 2, 3, 6, 7, 8, 11, 6, 11)
(0, 2, 3, 6, 9, 10, 11, 1, 8)
(0, 2, 3, 6, 9, 10, 11, 6, 7)
(0, 2, 4, 5, 6, 7, 10, 4, 8)
(0, 2, 4, 5, 7, 9, 10, 3, 9)

(0, 2, 4, 5, 8, 9, 11, 4, 10)
(0, 2, 5, 6, 7, 8, 10, 4, 8)
(0, 2, 6, 7, 8, 9, 11, 4, 10)
(0, 3, 4, 5, 6, 8, 11, 1, 7)
(0, 3, 4, 5, 6, 9, 10, 2, 3)
(0, 3, 4, 5, 7, 9, 10, 4, 10)

(0, 3, 4, 6, 9, 10, 11, 7, 11)
(0, 3, 4, 7, 8, 9, 11, 3, 9)
(0, 3, 4, 7, 8, 10, 11, 7, 8)
(0, 3, 4, 8, 9, 10, 11, 3, 9)
(0, 3, 6, 8, 9, 10, 11, 1, 7)
(0, 3, 6, 8, 9, 10, 11, 3, 9)

(0, 4, 5, 6, 7, 8, 11, 3, 10)
(0, 4, 5, 7, 8, 9, 10, 2, 7)
(0, 4, 5, 7, 8, 10, 11, 2, 6)
(0, 4, 5, 8, 9, 10, 11, 2, 8)

NLFSR Functions, n=13:

(0, 1, 2, 3, 4, 8, 12, 7, 8)
(0, 1, 2, 3, 4, 9, 11, 4, 10)
(0, 1, 2, 3, 5, 7, 8, 8, 12)
(0, 1, 2, 3, 5, 10, 11, 2, 8)
(0, 1, 2, 3, 6, 9, 12, 4, 8)
(0, 1, 2, 3, 8, 10, 12, 3, 6)
(0, 1, 2, 3, 8, 11, 12, 3, 11)
(0, 1, 2, 3, 9, 10, 11, 4, 12)
(0, 1, 2, 4, 5, 7, 10, 1, 11)
(0, 1, 2, 4, 7, 9, 10, 1, 5)
(0, 1, 2, 5, 6, 8, 10, 10, 12)
(0, 1, 2, 5, 10, 11, 12, 2, 10)
(0, 1, 2, 6, 7, 8, 12, 1, 7)
(0, 1, 2, 6, 7, 9, 11, 1, 7)
(0, 1, 3, 4, 5, 6, 7, 2, 7)
(0, 1, 3, 4, 5, 8, 9, 3, 10)
(0, 1, 3, 4, 5, 9, 12, 7, 8)
(0, 1, 3, 4, 6, 8, 10, 4, 9)
(0, 1, 3, 4, 7, 8, 9, 5, 6)
(0, 1, 3, 4, 7, 8, 9, 7, 8)
(0, 1, 3, 5, 6, 9, 10, 9, 11)
(0, 1, 3, 5, 6, 10, 11, 2, 12)

(0, 1, 3, 5, 10, 11, 12, 7, 10)
(0, 1, 3, 7, 8, 9, 10, 7, 11)
(0, 1, 3, 8, 9, 10, 11, 5, 6)
(0, 1, 4, 5, 6, 8, 12, 1, 6)
(0, 1, 4, 7, 10, 11, 12, 5, 9)
(0, 1, 4, 8, 9, 10, 12, 5, 6)
(0, 1, 5, 6, 7, 8, 9, 1, 10)
(0, 1, 5, 6, 7, 11, 12, 6, 12)
(0, 1, 5, 6, 9, 10, 11, 2, 6)
(0, 1, 5, 7, 8, 9, 12, 7, 12)
(0, 1, 5, 8, 9, 10, 11, 3, 5)
(0, 1, 5, 9, 10, 11, 12, 5, 6)
(0, 2, 3, 4, 5, 8, 10, 5, 8)
(0, 2, 3, 4, 5, 8, 12, 8, 10)
(0, 2, 3, 4, 5, 10, 12, 7, 8)
(0, 2, 3, 4, 7, 8, 12, 7, 11)
(0, 2, 3, 4, 10, 11, 12, 1, 9)
(0, 2, 3, 5, 7, 9, 10, 6, 8)
(0, 2, 3, 6, 7, 8, 10, 6, 8)
(0, 2, 3, 7, 8, 10, 12, 1, 11)
(0, 2, 3, 8, 10, 11, 12, 5, 11)
(0, 2, 4, 6, 7, 9, 10, 3, 12)

(0, 2, 4, 6, 7, 11, 12, 6, 12)
(0, 2, 4, 9, 10, 11, 12, 3, 9)
(0, 3, 4, 5, 6, 7, 9, 2, 3)
(0, 3, 4, 5, 6, 10, 12, 2, 6)
(0, 3, 4, 6, 7, 9, 11, 1, 10)
(0, 3, 4, 6, 8, 10, 11, 5, 7)
(0, 3, 4, 6, 9, 11, 12, 8, 12)
(0, 3, 4, 7, 8, 10, 12, 2, 4)
(0, 3, 5, 6, 7, 10, 11, 5, 7)
(0, 3, 5, 7, 8, 11, 12, 1, 3)
(0, 3, 5, 7, 9, 10, 12, 4, 9)
(0, 3, 5, 8, 9, 10, 11, 5, 8)
(0, 3, 6, 8, 9, 11, 12, 2, 12)
(0, 4, 5, 6, 7, 8, 12, 3, 12)
(0, 4, 5, 6, 9, 10, 12, 5, 6)
(0, 4, 5, 6, 9, 10, 12, 7, 8)
(0, 4, 5, 8, 9, 10, 12, 3, 10)
(0, 4, 6, 7, 8, 9, 10, 10, 11)
(0, 5, 6, 8, 10, 11, 12, 1, 5)
(0, 6, 7, 8, 9, 10, 12, 6, 11)

NLFSR Functions, n=14:

(0, 1, 2, 3, 4, 6, 13, 4, 6)
(0, 1, 2, 3, 4, 8, 9, 5, 8)
(0, 1, 2, 3, 5, 6, 12, 2, 6)
(0, 1, 2, 3, 5, 7, 13, 7, 13)
(0, 1, 2, 3, 6, 8, 9, 9, 10)
(0, 1, 2, 3, 8, 9, 12, 5, 11)
(0, 1, 2, 4, 7, 8, 11, 1, 6)
(0, 1, 2, 4, 8, 10, 12, 9, 11)
(0, 1, 2, 5, 6, 11, 12, 8, 10)
(0, 1, 2, 5, 7, 8, 10, 2, 6)
(0, 1, 2, 5, 7, 12, 13, 2, 10)
(0, 1, 2, 6, 8, 9, 12, 4, 6)
(0, 1, 2, 7, 8, 9, 10, 1, 3)
(0, 1, 2, 7, 8, 9, 10, 3, 13)
(0, 1, 2, 7, 9, 12, 13, 4, 12)
(0, 1, 2, 7, 10, 11, 12, 4, 5)
(0, 1, 3, 4, 5, 7, 11, 1, 2)
(0, 1, 3, 4, 9, 11, 13, 2, 7)
(0, 1, 3, 4, 10, 11, 12, 7, 8)
(0, 1, 3, 5, 6, 10, 13, 4, 12)
(0, 1, 3, 5, 10, 11, 13, 7, 12)
(0, 1, 3, 6, 7, 11, 13, 6, 7)
(0, 1, 3, 6, 8, 11, 12, 1, 3)
(0, 1, 3, 7, 8, 11, 13, 7, 8)
(0, 1, 3, 8, 9, 10, 12, 5, 11)
(0, 1, 4, 5, 6, 7, 8, 8, 13)
(0, 1, 4, 5, 7, 8, 13, 4, 12)
(0, 1, 4, 6, 7, 9, 12, 8, 13)
(0, 1, 4, 6, 7, 11, 12, 6, 8)
(0, 1, 4, 7, 8, 11, 12, 2, 7)
(0, 1, 4, 8, 9, 11, 13, 2, 10)
(0, 1, 5, 6, 7, 11, 12, 3, 11)
(0, 1, 5, 7, 8, 9, 10, 3, 11)
(0, 1, 5, 7, 9, 10, 11, 2, 5)
(0, 1, 6, 7, 8, 10, 11, 2, 9)
(0, 1, 6, 7, 9, 10, 13, 2, 10)
(0, 1, 7, 9, 11, 12, 13, 1, 7)
(0, 1, 8, 10, 11, 12, 13, 8, 10)
(0, 2, 3, 4, 6, 8, 12, 2, 3)
(0, 2, 3, 4, 7, 12, 13, 9, 10)
(0, 2, 3, 4, 10, 11, 13, 6, 7)
(0, 2, 3, 5, 7, 8, 12, 11, 12)
(0, 2, 3, 6, 7, 10, 11, 8, 9)
(0, 2, 3, 6, 7, 10, 13, 7, 12)
(0, 2, 3, 6, 8, 11, 13, 11, 13)
(0, 2, 3, 7, 8, 9, 13, 3, 11)
(0, 2, 3, 7, 8, 10, 13, 6, 8)
(0, 2, 3, 8, 9, 12, 13, 4, 6)
(0, 2, 4, 5, 6, 11, 13, 3, 9)
(0, 2, 4, 6, 10, 12, 13, 3, 5)
(0, 2, 5, 6, 7, 9, 12, 10, 13)
(0, 2, 5, 6, 8, 12, 13, 8, 10)
(0, 2, 5, 6, 11, 12, 13, 3, 9)
(0, 2, 5, 7, 8, 9, 12, 1, 4)
(0, 2, 5, 7, 8, 10, 13, 1, 6)
(0, 2, 6, 7, 9, 11, 12, 2, 3)
(0, 2, 6, 8, 10, 11, 12, 11, 12)
(0, 2, 8, 9, 11, 12, 13, 8, 12)
(0, 3, 4, 5, 6, 8, 10, 5, 13)
(0, 3, 4, 5, 7, 9, 13, 9, 12)
(0, 3, 4, 5, 7, 10, 11, 1, 5)
(0, 3, 4, 6, 7, 8, 10, 1, 9)
(0, 3, 4, 6, 7, 8, 13, 5, 12)
(0, 3, 4, 7, 8, 11, 12, 5, 6)
(0, 3, 4, 7, 9, 10, 11, 9, 13)
(0, 3, 6, 7, 10, 12, 13, 8, 13)
(0, 3, 7, 9, 10, 11, 13, 12, 13)
(0, 4, 5, 6, 7, 9, 13, 3, 11)
(0, 4, 5, 6, 7, 12, 13, 1, 11)
(0, 4, 5, 6, 7, 12, 13, 11, 13)
(0, 4, 6, 7, 8, 10, 11, 5, 13)
(0, 4, 6, 7, 9, 12, 13, 8, 12)
(0, 4, 6, 8, 9, 10, 11, 1, 9)
(0, 5, 6, 8, 11, 12, 13, 4, 5)
(0, 5, 6, 10, 11, 12, 13, 6, 9)
(0, 6, 7, 8, 9, 10, 13, 1, 6)

NLFSR Functions, n=15:

(0, 1, 2, 3, 5, 7, 10, 12, 14)
(0, 1, 2, 3, 5, 9, 14, 8, 11)
(0, 1, 2, 3, 5, 11, 12, 3, 13)
(0, 1, 2, 3, 6, 8, 10, 7, 13)
(0, 1, 2, 4, 5, 6, 10, 6, 14)
(0, 1, 2, 4, 6, 8, 13, 7, 13)
(0, 1, 2, 4, 7, 8, 14, 10, 13)
(0, 1, 2, 4, 9, 10, 12, 5, 7)
(0, 1, 2, 5, 6, 9, 11, 10, 12)
(0, 1, 2, 5, 7, 9, 10, 8, 13)
(0, 1, 2, 6, 7, 8, 14, 1, 14)
(0, 1, 2, 6, 7, 11, 13, 10, 11)
(0, 1, 2, 6, 8, 9, 12, 3, 10)
(0, 1, 2, 6, 9, 11, 14, 6, 14)
(0, 1, 2, 7, 8, 10, 11, 5, 11)
(0, 1, 2, 8, 9, 11, 12, 2, 6)
(0, 1, 3, 4, 5, 7, 13, 7, 11)
(0, 1, 3, 4, 5, 8, 13, 1, 6)
(0, 1, 3, 5, 8, 10, 13, 2, 3)
(0, 1, 3, 6, 7, 10, 12, 1, 13)
(0, 1, 3, 8, 9, 10, 13, 1, 6)
(0, 1, 4, 5, 8, 9, 11, 1, 14)
(0, 1, 4, 5, 8, 9, 14, 4, 12)
(0, 1, 4, 6, 7, 8, 14, 2, 13)
(0, 1, 4, 6, 8, 10, 13, 4, 9)
(0, 1, 4, 6, 9, 10, 12, 2, 7)
(0, 1, 4, 6, 9, 13, 14, 1, 9)
(0, 1, 4, 7, 9, 10, 11, 4, 12)
(0, 1, 6, 7, 10, 11, 14, 3, 11)
(0, 1, 6, 8, 9, 10, 13, 1, 7)
(0, 1, 6, 10, 12, 13, 14, 4, 7)
(0, 1, 7, 8, 9, 11, 14, 2, 13)
(0, 1, 7, 8, 9, 13, 14, 1, 14)
(0, 1, 7, 8, 11, 13, 14, 2, 5)
(0, 2, 3, 4, 5, 6, 8, 2, 13)
(0, 2, 3, 6, 8, 10, 11, 3, 13)
(0, 2, 3, 6, 9, 11, 13, 1, 5)
(0, 2, 4, 6, 9, 12, 13, 10, 14)
(0, 2, 4, 7, 9, 10, 12, 2, 13)
(0, 2, 4, 8, 9, 13, 14, 4, 5)
(0, 2, 5, 6, 7, 9, 14, 8, 14)
(0, 2, 5, 6, 7, 12, 14, 9, 14)
(0, 2, 5, 6, 8, 9, 12, 2, 10)
(0, 2, 5, 7, 9, 11, 14, 6, 11)
(0, 2, 5, 7, 10, 12, 14, 12, 13)
(0, 2, 7, 8, 9, 11, 12, 4, 8)
(0, 2, 7, 9, 11, 13, 14, 2, 8)
(0, 2, 7, 10, 11, 12, 14, 9, 14)
(0, 2, 8, 10, 11, 12, 14, 4, 8)
(0, 3, 4, 6, 7, 8, 13, 7, 11)
(0, 3, 4, 6, 7, 13, 14, 9, 13)
(0, 3, 4, 10, 12, 13, 14, 2, 12)
(0, 3, 5, 6, 8, 11, 13, 2, 13)
(0, 3, 5, 6, 9, 10, 11, 9, 12)
(0, 3, 5, 6, 9, 11, 14, 8, 13)
(0, 3, 5, 6, 11, 13, 14, 8, 10)
(0, 3, 5, 8, 9, 12, 14, 2, 14)
(0, 3, 6, 7, 9, 10, 13, 5, 13)
(0, 3, 6, 7, 9, 13, 14, 5, 12)
(0, 4, 5, 6, 8, 11, 14, 3, 11)
(0, 4, 5, 6, 9, 10, 12, 3, 6)
(0, 4, 5, 7, 8, 13, 14, 4, 10)
(0, 4, 5, 7, 9, 12, 13, 2, 12)
(0, 4, 6, 7, 10, 11, 14, 1, 14)
(0, 4, 6, 9, 10, 13, 14, 3, 5)
(0, 5, 6, 8, 10, 13, 14, 2, 7)
(0, 5, 7, 9, 12, 13, 14, 2, 8)
(0, 5, 8, 10, 12, 13, 14, 1, 3)
(0, 5, 9, 10, 11, 13, 14, 1, 9)
(0, 7, 9, 10, 11, 12, 13, 2, 13)

NLFSR Functions, n=16:

(0, 1, 2, 3, 4, 6, 13, 6, 8)
(0, 1, 2, 3, 5, 11, 13, 1, 8)
(0, 1, 2, 3, 6, 7, 10, 8, 13)
(0, 1, 2, 4, 6, 7, 13, 4, 13)
(0, 1, 2, 4, 7, 10, 15, 4, 13)
(0, 1, 2, 5, 10, 12, 14, 2, 12)
(0, 1, 2, 6, 9, 11, 12, 7, 13)
(0, 1, 2, 7, 9, 11, 15, 4, 8)
(0, 1, 2, 9, 11, 12, 14, 4, 11)
(0, 1, 2, 10, 11, 13, 14, 2, 14)
(0, 1, 3, 4, 5, 9, 14, 7, 15)
(0, 1, 3, 4, 7, 8, 15, 1, 5)
(0, 1, 3, 5, 9, 10, 11, 7, 11)
(0, 1, 3, 6, 8, 9, 10, 2, 10)
(0, 1, 3, 6, 11, 13, 14, 9, 13)
(0, 1, 3, 8, 10, 12, 15, 5, 11)
(0, 1, 3, 8, 10, 12, 15, 8, 13)
(0, 1, 4, 5, 8, 12, 14, 2, 8)
(0, 1, 4, 6, 8, 13, 15, 3, 8)
(0, 1, 4, 6, 8, 13, 15, 5, 11)
(0, 1, 4, 10, 11, 12, 13, 7, 9)
(0, 1, 4, 10, 11, 13, 14, 7, 12)
(0, 1, 5, 7, 9, 11, 12, 9, 14)
(0, 1, 5, 7, 9, 14, 15, 8, 12)
(0, 1, 6, 7, 10, 12, 13, 2, 4)
(0, 1, 6, 7, 10, 13, 14, 8, 11)
(0, 1, 6, 9, 10, 12, 14, 8, 10)
(0, 1, 6, 9, 12, 14, 15, 3, 12)
(0, 1, 8, 9, 12, 13, 15, 11, 15)

(0, 2, 3, 4, 5, 6, 7, 6, 9)
(0, 2, 3, 4, 6, 13, 14, 6, 14)
(0, 2, 3, 4, 8, 10, 14, 1, 3)
(0, 2, 3, 5, 6, 10, 14, 3, 15)
(0, 2, 3, 5, 6, 12, 15, 4, 9)
(0, 2, 3, 5, 6, 14, 15, 2, 14)
(0, 2, 3, 5, 10, 12, 13, 1, 7)
(0, 2, 3, 5, 10, 13, 15, 3, 7)
(0, 2, 3, 6, 7, 13, 14, 3, 9)
(0, 2, 3, 6, 9, 10, 15, 5, 8)
(0, 2, 3, 8, 9, 10, 11, 3, 15)
(0, 2, 3, 8, 9, 11, 14, 8, 15)
(0, 2, 3, 8, 10, 11, 13, 7, 13)
(0, 2, 3, 9, 10, 13, 14, 7, 13)
(0, 2, 3, 10, 12, 13, 14, 2, 10)
(0, 2, 4, 5, 7, 14, 15, 5, 12)
(0, 2, 4, 5, 9, 12, 13, 3, 6)
(0, 2, 4, 6, 7, 10, 15, 6, 8)
(0, 2, 4, 6, 11, 14, 15, 4, 14)
(0, 2, 4, 7, 8, 11, 12, 3, 11)
(0, 2, 4, 8, 11, 12, 15, 8, 14)
(0, 2, 5, 7, 8, 13, 14, 1, 8)
(0, 2, 6, 8, 12, 13, 14, 13, 15)
(0, 2, 6, 10, 11, 13, 14, 1, 13)
(0, 2, 7, 9, 10, 11, 12, 1, 14)
(0, 2, 7, 11, 12, 13, 15, 1, 9)
(0, 2, 9, 10, 11, 12, 13, 4, 13)
(0, 3, 4, 5, 6, 7, 14, 3, 12)
(0, 3, 4, 5, 6, 12, 15, 7, 9)

(0, 3, 4, 5, 7, 8, 12, 7, 8)
(0, 3, 4, 5, 8, 12, 13, 6, 8)
(0, 3, 4, 6, 9, 10, 15, 12, 14)
(0, 3, 4, 6, 11, 13, 14, 9, 15)
(0, 3, 4, 7, 11, 12, 14, 10, 13)
(0, 3, 4, 8, 11, 12, 13, 8, 10)
(0, 3, 5, 6, 7, 10, 12, 6, 13)
(0, 3, 5, 6, 8, 13, 14, 3, 9)
(0, 3, 5, 7, 8, 9, 13, 4, 8)
(0, 3, 5, 11, 13, 14, 15, 8, 15)
(0, 3, 7, 8, 9, 10, 12, 4, 6)
(0, 3, 7, 8, 9, 11, 13, 8, 12)
(0, 3, 9, 10, 12, 14, 15, 3, 12)
(0, 3, 10, 12, 13, 14, 15, 8, 10)
(0, 4, 5, 6, 7, 9, 14, 2, 15)
(0, 4, 5, 7, 9, 11, 15, 2, 7)
(0, 4, 5, 7, 10, 14, 15, 3, 9)
(0, 4, 5, 8, 9, 12, 14, 5, 13)
(0, 4, 6, 7, 8, 9, 13, 10, 12)
(0, 4, 6, 9, 10, 11, 13, 3, 10)
(0, 4, 8, 9, 11, 12, 13, 8, 9)
(0, 5, 6, 7, 8, 13, 14, 1, 13)
(0, 5, 6, 7, 11, 13, 15, 5, 9)
(0, 6, 7, 8, 10, 13, 15, 6, 14)
(0, 6, 9, 10, 13, 14, 15, 3, 8)
(0, 9, 10, 11, 12, 13, 14, 7, 10)

NLFSR Functions, n=17:

(0, 1, 2, 3, 8, 9, 11, 6, 15)
(0, 1, 2, 3, 10, 15, 16, 5, 13)
(0, 1, 2, 4, 8, 10, 14, 8, 16)
(0, 1, 2, 6, 7, 8, 12, 1, 8)
(0, 1, 2, 6, 7, 12, 16, 3, 8)
(0, 1, 2, 7, 8, 13, 15, 8, 13)
(0, 1, 2, 7, 14, 15, 16, 4, 12)
(0, 1, 2, 9, 11, 12, 13, 8, 11)
(0, 1, 2, 11, 12, 13, 15, 3, 13)
(0, 1, 3, 5, 6, 7, 16, 9, 11)
(0, 1, 3, 5, 7, 8, 10, 3, 13)
(0, 1, 3, 8, 12, 14, 15, 6, 8)
(0, 1, 4, 6, 7, 8, 10, 3, 9)
(0, 1, 4, 6, 11, 13, 14, 8, 16)
(0, 1, 4, 7, 9, 13, 16, 1, 5)
(0, 1, 4, 8, 9, 11, 16, 1, 9)
(0, 1, 4, 8, 10, 13, 16, 12, 16)
(0, 1, 5, 7, 8, 10, 11, 2, 13)
(0, 1, 5, 7, 9, 12, 16, 3, 15)
(0, 1, 5, 8, 10, 12, 16, 2, 14)
(0, 1, 5, 10, 11, 15, 16, 9, 14)
(0, 1, 5, 12, 13, 14, 15, 5, 15)
(0, 1, 6, 8, 9, 13, 16, 8, 16)
(0, 1, 6, 9, 10, 13, 15, 4, 9)

(0, 1, 7, 9, 10, 14, 15, 5, 15)
(0, 1, 7, 10, 11, 14, 15, 1, 12)
(0, 1, 7, 10, 12, 13, 15, 3, 7)
(0, 1, 10, 11, 12, 14, 16, 6, 8)
(0, 1, 11, 12, 13, 14, 15, 9, 11)
(0, 2, 3, 4, 5, 6, 16, 6, 8)
(0, 2, 3, 4, 5, 12, 16, 2, 12)
(0, 2, 3, 5, 9, 14, 16, 9, 11)
(0, 2, 3, 6, 7, 10, 16, 5, 16)
(0, 2, 3, 7, 8, 10, 16, 2, 12)
(0, 2, 3, 8, 12, 13, 14, 1, 4)
(0, 2, 3, 9, 12, 13, 14, 9, 11)
(0, 2, 4, 5, 6, 15, 16, 4, 14)
(0, 2, 4, 5, 7, 10, 16, 10, 14)
(0, 2, 4, 7, 8, 11, 16, 8, 13)
(0, 2, 4, 7, 8, 12, 15, 8, 14)
(0, 2, 4, 9, 10, 15, 16, 4, 9)
(0, 2, 5, 6, 7, 11, 15, 6, 14)
(0, 2, 5, 6, 8, 12, 13, 2, 13)
(0, 2, 5, 9, 10, 13, 15, 3, 9)
(0, 2, 6, 7, 8, 11, 12, 6, 16)
(0, 2, 6, 7, 12, 13, 14, 1, 14)
(0, 2, 6, 10, 11, 12, 15, 3, 11)
(0, 2, 9, 10, 12, 13, 14, 3, 6)

(0, 3, 4, 5, 7, 8, 15, 11, 14)
(0, 3, 4, 5, 8, 9, 10, 1, 9)
(0, 3, 4, 5, 8, 14, 15, 6, 8)
(0, 3, 4, 5, 9, 14, 15, 13, 16)
(0, 3, 4, 5, 10, 11, 15, 3, 16)
(0, 3, 4, 6, 11, 13, 16, 1, 9)
(0, 3, 4, 9, 11, 12, 14, 2, 6)
(0, 3, 5, 6, 8, 13, 14, 11, 15)
(0, 3, 7, 8, 10, 12, 13, 8, 10)
(0, 3, 7, 9, 13, 15, 16, 1, 9)
(0, 4, 5, 6, 7, 8, 12, 9, 13)
(0, 4, 5, 6, 8, 15, 16, 6, 9)
(0, 4, 5, 7, 9, 10, 14, 7, 9)
(0, 4, 5, 9, 11, 12, 15, 4, 15)
(0, 5, 6, 9, 10, 11, 15, 1, 11)
(0, 5, 9, 10, 11, 12, 13, 4, 8)
(0, 5, 9, 10, 11, 15, 16, 9, 16)
(0, 6, 7, 9, 10, 12, 16, 4, 15)
(0, 6, 8, 9, 14, 15, 16, 2, 11)
(0, 7, 8, 9, 12, 13, 14, 8, 16)
(0, 7, 9, 10, 11, 13, 16, 8, 14)
(0, 7, 9, 10, 12, 14, 16, 4, 14)

NLFSR Functions, n=18:

(0, 1, 2, 3, 7, 13, 14, 3, 15)
(0, 1, 2, 7, 9, 10, 13, 3, 15)
(0, 1, 2, 11, 13, 14, 15, 8, 10)
(0, 1, 3, 4, 5, 6, 10, 13, 15)
(0, 1, 3, 4, 6, 12, 16, 9, 15)
(0, 1, 3, 4, 8, 10, 15, 13, 17)
(0, 1, 3, 4, 9, 11, 13, 3, 13)
(0, 1, 3, 5, 11, 14, 17, 4, 10)
(0, 1, 4, 5, 7, 10, 14, 11, 14)
(0, 1, 4, 7, 11, 13, 17, 8, 14)
(0, 1, 4, 7, 13, 15, 17, 8, 14)
(0, 1, 4, 8, 10, 13, 15, 10, 12)
(0, 1, 5, 6, 8, 12, 15, 5, 15)
(0, 1, 5, 7, 11, 14, 17, 4, 10)
(0, 1, 8, 9, 12, 14, 15, 1, 7)

(0, 2, 3, 4, 6, 7, 13, 14, 16)
(0, 2, 3, 6, 12, 13, 15, 2, 15)
(0, 2, 3, 7, 9, 12, 14, 1, 13)
(0, 2, 4, 10, 12, 14, 15, 1, 7)
(0, 2, 5, 6, 8, 11, 14, 6, 14)
(0, 2, 6, 7, 8, 9, 15, 1, 4)
(0, 2, 6, 12, 14, 15, 17, 3, 9)
(0, 3, 4, 5, 7, 16, 17, 8, 10)
(0, 3, 4, 6, 8, 12, 13, 11, 13)
(0, 3, 4, 6, 8, 14, 16, 11, 17)
(0, 3, 4, 6, 9, 10, 17, 11, 17)
(0, 3, 5, 6, 12, 15, 16, 3, 16)
(0, 3, 5, 8, 10, 14, 17, 6, 8)
(0, 3, 6, 9, 12, 13, 14, 4, 15)
(0, 3, 6, 10, 11, 12, 13, 8, 14)

(0, 3, 6, 10, 12, 13, 17, 3, 13)
(0, 3, 8, 10, 14, 15, 17, 1, 5)
(0, 3, 9, 10, 11, 12, 16, 14, 17)
(0, 4, 5, 6, 9, 12, 15, 3, 14)
(0, 4, 5, 11, 15, 16, 17, 3, 15)
(0, 4, 6, 9, 11, 15, 16, 5, 17)
(0, 4, 7, 10, 12, 13, 16, 4, 12)
(0, 4, 8, 11, 13, 14, 17, 4, 7)
(0, 5, 6, 7, 8, 12, 15, 4, 10)
(0, 5, 6, 10, 12, 14, 15, 5, 7)
(0, 5, 7, 9, 14, 15, 17, 5, 15)
(0, 5, 8, 9, 11, 16, 17, 3, 15)
(0, 5, 11, 12, 14, 15, 16, 2, 4)
(0, 8, 12, 13, 14, 15, 17, 3, 5)

NLFSR Functions, n=19:

(0, 1, 2, 3, 5, 13, 17, 1, 13)
(0, 1, 2, 4, 6, 15, 18, 5, 6)
(0, 1, 2, 4, 9, 10, 16, 10, 14)
(0, 1, 2, 4, 12, 15, 18, 3, 11)
(0, 1, 2, 5, 6, 14, 16, 8, 18)
(0, 1, 2, 6, 7, 15, 17, 9, 12)
(0, 1, 3, 4, 5, 14, 17, 11, 18)
(0, 1, 3, 4, 8, 11, 17, 1, 3)

(0, 1, 3, 5, 6, 7, 11, 8, 10)
(0, 1, 3, 5, 6, 9, 12, 14, 16)
(0, 1, 3, 6, 9, 10, 17, 7, 13)
(0, 1, 4, 5, 7, 11, 16, 7, 15)
(0, 1, 4, 5, 14, 15, 17, 13, 16)
(0, 1, 4, 9, 12, 13, 14, 14, 18)
(0, 1, 7, 8, 9, 11, 14, 3, 11)
(0, 2, 3, 5, 9, 11, 12, 8, 18)

(0, 2, 3, 5, 11, 12, 16, 9, 13)
(0, 2, 4, 5, 6, 12, 13, 3, 8)
(0, 2, 4, 5, 10, 11, 16, 15, 16)
(0, 2, 4, 6, 7, 8, 17, 14, 17)
(0, 2, 4, 7, 10, 14, 17, 14, 16)
(0, 3, 5, 7, 8, 9, 14, 5, 10)
(0, 5, 6, 8, 9, 10, 14, 2, 4)

NLFSR Functions, n=20:

(0, 1, 2, 3, 5, 17, 19, 5, 11)
(0, 1, 2, 3, 8, 16, 18, 7, 17)
(0, 1, 2, 4, 10, 15, 17, 2, 3)
(0, 1, 2, 6, 11, 15, 19, 11, 17)
(0, 1, 2, 11, 12, 13, 16, 7, 14)
(0, 1, 3, 4, 8, 13, 18, 13, 15)
(0, 1, 3, 4, 9, 13, 15, 7, 13)
(0, 1, 4, 5, 7, 11, 18, 11, 15)
(0, 1, 4, 7, 9, 13, 15, 7, 8)

(0, 1, 6, 7, 8, 16, 17, 4, 18)
(0, 1, 6, 7, 12, 13, 16, 4, 8)
(0, 1, 6, 8, 9, 11, 18, 12, 14)
(0, 1, 6, 8, 15, 17, 18, 4, 16)
(0, 1, 7, 9, 12, 16, 18, 4, 6)
(0, 1, 8, 10, 12, 13, 17, 13, 17)
(0, 2, 4, 6, 11, 12, 16, 9, 19)
(0, 2, 4, 7, 15, 16, 17, 4, 9)
(0, 2, 4, 8, 13, 16, 17, 6, 14)

(0, 2, 5, 9, 12, 13, 15, 11, 19)
(0, 2, 5, 11, 13, 15, 17, 2, 14)
(0, 2, 6, 8, 9, 14, 17, 14, 18)
(0, 2, 6, 12, 13, 15, 17, 14, 18)
(0, 2, 7, 13, 14, 15, 16, 2, 10)
(0, 3, 6, 7, 12, 15, 16, 1, 3)

NLFSR Functions, n=21:

(0, 1, 2, 3, 4, 12, 18, 6, 18)
(0, 1, 2, 3, 5, 6, 17, 8, 9)
(0, 1, 2, 5, 9, 14, 19, 2, 4)
(0, 1, 3, 4, 6, 8, 16, 1, 6)
(0, 1, 3, 4, 10, 17, 19, 7, 15)
(0, 1, 7, 8, 13, 14, 15, 8, 10)

(0, 1, 7, 11, 12, 15, 18, 14, 20)
(0, 1, 9, 11, 12, 16, 19, 5, 8)
(0, 2, 3, 4, 7, 11, 19, 1, 10)
(0, 2, 3, 8, 10, 13, 16, 3, 19)
(0, 2, 4, 5, 7, 10, 14, 7, 13)
(0, 2, 4, 12, 15, 16, 18, 1, 15)

(0, 2, 10, 11, 12, 15, 18, 10, 19)
(0, 3, 4, 5, 6, 15, 17, 12, 16)
(0, 3, 8, 10, 13, 14, 16, 3, 16)
(0, 4, 5, 7, 9, 12, 13, 3, 5)
(0, 4, 5, 9, 10, 12, 16, 2, 7)

NLFSR Functions, n=22:

(0, 1, 2, 3, 9, 11, 13, 3, 15)
(0, 1, 2, 3, 9, 12, 20, 1, 13)
(0, 1, 3, 5, 8, 9, 20, 10, 18)
(0, 1, 3, 6, 11, 13, 17, 7, 17)
(0, 1, 6, 7, 12, 13, 20, 3, 19)

(0, 1, 9, 10, 11, 14, 18, 13, 16)
(0, 2, 6, 9, 10, 11, 17, 5, 7)
(0, 2, 9, 10, 15, 16, 21, 3, 19)
(0, 2, 10, 13, 19, 20, 21, 9, 21)
(0, 2, 13, 14, 17, 19, 21, 4, 12)

(0, 3, 5, 6, 7, 14, 16, 4, 10)
(0, 3, 5, 9, 10, 11, 17, 4, 17)

NLFSR Functions, n=23:

(0, 1, 2, 7, 18, 20, 22, 1, 5)
(0, 1, 2, 12, 13, 17, 19, 2, 3)
(0, 1, 3, 5, 8, 10, 13, 2, 22)

(0, 1, 3, 5, 16, 21, 22, 18, 22)
(0, 1, 3, 11, 12, 13, 22, 3, 13)
(0, 1, 4, 5, 10, 13, 14, 4, 8)

(0, 1, 7, 15, 16, 19, 21, 3, 19)

6 Conclusion and Future Work

The pseudo-random generators for stream ciphers can be generated using NLFSRs. There is no mathematical foundation on how to construct an NLFSR with optimal period. In this paper, we constructed a new type of NLFSR feedback functions of degree 2 with optimal periods. A total of (639) new NLFSR functions for $8 \leq n \leq 23$ are proposed. We ensured that these functions are the only ones existing within this range. The construction method generating NLFSR functions is briefly described. For future work, we suggest extending this work by generating more feedback functions having optimal periods with larger values of n. Furthermore, this work can be extended to include NLFSR feedback functions of degree 3 and higher that can generate more secure pseudorandom bit sequences capable of resisting the low-order approximation attack.

REFERENCES

[1]. Zhou, Liang, and Shantanu Chakrabartty. "Secure dynamic authentication of passive assets and passive iots using self-powered timers." *2017 IEEE International Symposium on Circuits and Systems (ISCAS)*. IEEE, 2017.

[2]. Zeng, Kencheng, et al. "Pseudorandom bit generators in stream-cipher cryptography." *Computer* 24.2 (1991): 8-17.

[3]. Ahmad, A. "Achievement of higher testability goals through the modification of shift registers in LFSR-based testing." *International journal of electronics* 82.3 (1997): 249-260.

[4]. Mrugalski, Grzegorz, Janusz Rajski, and Jerzy Tyszer. "Ring generators-new devices for embedded test applications." *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems* 23.9 (2004): 1306-1320.

[5]. Zhang, Jia-Min, et al. "Further Results on the Decomposition of an NFSR Into the Cascade Connection of an NFSR Into an LFSR." *IEEE Trans. Information Theory* 61.1 (2015): 645-654.

[6]. Dubrova, Elena, and Martin Hell. "Espresso: A stream cipher for 5G wireless communication systems." *Cryptography and Communications* 9.2 (2017): 273-289.

[7]. Chabloz, Jean-Michel, Shohreh Sharif Mansouri, and Elena Dubrova. "An algorithm for constructing a fastest Galois NLFSR generating a given sequence." *International Conference on Sequences and Their Applications*. Springer, Berlin, Heidelberg, 2010.

[8]. Dubrova, Elena. "An equivalence-preserving transformation of shift registers." *International Conference on Sequences and Their Applications*. Springer, Cham, 2014.

[9]. Lidl, Rudolf, and Harald Niederreiter. *Introduction to finite fields and their applications*. Cambridge university press, 1994.

[10]. Kaashoek, M. Frans, and David R. Karger. "Koorde: A simple degree-optimal distributed hash table." *International Workshop on Peer-to-Peer Systems*. Springer, Berlin, Heidelberg, 2003.

[11]. Mayhew, Gregory L., and Solomon W. Golomb. "Linear spans of modified de Bruijn sequences." *IEEE transactions on information theory* 36.5 (1990): 1166-1167.

[12]. Champness, Neil R. "Coordination polymers: from metal–organic frameworks to spheres." *Angewandte Chemie International Edition* 48.13 (2009): 2274-2275.

[13]. Dubrova, Elena. "Generation of full cycles by a composition of NLFSRs." *Designs, codes and cryptography* 73.2 (2014): 469-486.

[14]. Dubrova, Elena. "A list of maximum-period NLFSRs." (2012).

[15]. Janicka-Lipska, Izabela, and Janusz Stokłosa. "Boolean feedback functions for full-length nonlinear shift registers." *Journal of Telecommunications and Information Technology* (2004): 28-30.

[16]. Almuhammadi, Sultan, et al. "NLFSR Functions with Optimal Periods." *International Conference on Computational Science and Its Applications*. Springer, Cham, 2018.

[17]. Rachwalik, Tomasz, et al. "Generation of Nonlinear Feedback Shift Registers with special-purpose hardware." *Communications and Information Systems Conference (MCC), 2012 Military*. IEEE, 2012.

[18]. Mandal, Kalikinkar, and Guang Gong. *Cryptographic D-morphic analysis and fast implementations of composited de Bruijn sequences*. Technical Report CACR 2012-27, University of Waterloo, 2012.

[19]. Günther, Christoph G. "Alternating step generators controlled by de Bruijn sequences." *Workshop on the Theory and Application of of Cryptographic Techniques*. Springer, Berlin, Heidelberg, 1987.

[20]. Ghebleh, Mohammad, Ali Kanso, and Hassan Noura. "An image encryption scheme based on irregularly decimated chaotic maps." *Signal Processing: Image Communication* 29.5 (2014): 618-627.

[21]. Poluyanenko, Nikolay. "Development of the search method for non-linear shift registers using hardware, implemented on field programmable gate arrays." *EUREKA: Physics and Engineering* 1 (2017): 53-60.