The Journal of Engineering Research, Vol. 11, No. 2 (2014) 1-14

On Sequence Lengths of Some Special External Exclusive OR Type LFSR Structures – Study and Analysis

A Ahmad* and A Al Maashri

Department of Electrical & Computer Engineering, College of Engineering, Sultan Qaboos University, P.O. Box 33, Postal Code 123, Sultanate of Oman

Received 14 February 2014; accepted 20 April 2014

Abstract: The study of the length of pseudo-random binary sequences generated by Linear-Feedback Shift Registers (LFSRs) plays an important role in the design approaches of built-in self-test, cryptosystems, and other applications. However, certain LFSR structures might not be appropriate in some situations. Given that determining the length of generated pseudo-random binary sequence is a complex task, therefore, before using an LFSR structure, it is essential to investigate the length and the properties of the sequence. This paper investigates some conditions and LFSR's structures, which restrict the pseudo-random binary sequences' generation to a certain fixed length. The outcomes of this paper are presented in the form of theorems, simulations, and analyses. We believe that these outcomes are of great importance to the designers of built-in self-test equipment, cryptosystems, and other applications such as radar, CDMA, error correction, and Monte Carlo simulation.

Keywords: LFSR, Pseudo-random binary sequence, Seed, Feedback connection, Periodicity, Exclusive OR.

أطوال متسلسلة بعض الحالات الخاصة من بنى LFSR - دراسة و تحليل

آفاق أحمد وأحمد المعشري

الملخص: هناك دور مهم لدراسة أطوال المتسلسلات الإثنانية شبه العشوائيةالتي ينتجها ال LFSR في تطبيقات مثل الفحص الذاتي المدمج و أنظمة التشفير وغيرها. وعلى الرغم من ذلك فهنالك بعض بنى ال LFSR التي قد لا تلائم تطبيقات بعينها. وإذا أخذ في الاعتبار مدى تعقيد عملية حساب أطوال المتسلسلات الإثنانية شبه العشوائية الناتجة عن ال LFSR، فإنه يجب معرفة أطوال وخصائص هذه المتسلسلات قبل استخدام بنى ال LFSR. تبحث هذه المقالة بعض الشروط وبنى ال LFSR التي قد تنتج متسلسلات إثنانية شبه عشوائية بأطوال محددة بعينها. مخرجات هذه المقالة تم تقديمها علي هيئة نظريات و نتائج محاكاة و تحاليل. المؤلفون على قناعة تامة بأن هذه المخرجات لها أهمية كبيرة لمصممي معدات الفحص الذاتي المدمج ونظم التشفير و غيرها من التطبيقات مثل أنظمة الرادار و CMDA و تصحيح الأخطاء و محاكاة مونتي كارلو.

مفاتيح الكلمات: LFSR، المتسلسلة الإثنانية شبه العشوائية، بذرة العشوائية، توصيل الراجع، الدوريات.

*Corresponding author's e-mail: afaq@squ.edu.om

1. Introduction

Pseudo-Random Binary Sequences (PRBSs) have been used for various applications. Some of the application areas are Built-In Self-Test (BIST) for Very Large Scale Integration (VLSI) circuits' design, cryptography applications like stream ciphers, and error correction and detection codes. In addition, PRBS have been commonly used in the fields of digital signal processing, wireless communications, direct sequence spread spectrum, scrambling &descrambling, encryption & decryption, steganography, and many more (Williams 1984; McCluskey 1985, Bardell *et al*. 1987; Nanda *et al*. 1989, Ahmad 1997; Jamil and Ahmad 2002; Ahmad 2005a, 2012, 2013a; Hell and Johansson 2008, Mukherjee *et al*. 2011 and Ayinala and Parhi2011).

Linear Feedback Shift Registers (LFSRs) are usually used for generating PRBSs (Peterson and Weldon 1984 and Golomb 1981). In fact, LFSRs have been employed in a wide range of applications. This is due to several reasons: 1) LFSRs are well-suited to hardware implementation, 2) LFSRs can produce PRBS with good statistical properties, 3) LFSRs can produce sequences of large periods with different frequencies, and 4) because of their structures; LFSRs can be readily analyzed using algebraic techniques. However, there are a number of design issues that need to be considered prior to integrating LFSR to a real application. Some of these issues include the size of LFSR '*n*', the seed '*s*' (*ie*. initial state of the LFSR), feedback connection (FB) in the LFSR, and the type of the LFSR (*ie*. internal or external) using exclusive-OR 'XOR' or exclusive-NOR 'XNOR'.

Some structures of LFSRs are constructed using internal XNOR model with respect to their periodicity, which have been analyzed in (Ahmad and Al-Maashri 2008) exploiting the state space model of XNOR structures of LFSR (Ahmad 2005b). In this paper, we consider internal XOR model of LFSR structures to study some of the conditions, which restrict the LFSR to a particular periodicity. Our study is based on a derived algebraic modeling of generated PRBSs by the LFSR. We further validate our results through simulation process. We also present a study on randomness criterion of those LFSR structures.

The rest of this paper is organized as appears in Sections 2 - 7. Section 2 introduces LFSR model. In Section 3 we present the derived algebraic model of an LFSR, whereas Section 4 presents the analytical study. Simulation model and runs are embodied in Section 5, while Section 6 presents a study on randomness criterion of PRBSs. Finally, Section 7 concludes the paper and discusses future work. Also, an appendix (Appendix A) is provided for the abbreviations and terminologies used in this paper.

2. LFSR – An Introduction

An LFSR is a special type of Serial-In Serial-Out (SISO) shift register that, when clocked, advances the signal through the register from one bit to the next most-significant bit. Figure 1 shows an *n*-bit SISO shift register. The key element of SISO shift register is D-type Flip-Flops (FFs). The $\{q_1, q_2, q_i, \ldots q_{n-1}, q_n\}$ are the states of the flip-flops $\{D_1, D_2, \ldots, D_i, \ldots D_{n-1}, D_n\}$, respectively.

SISO shift register has two special features: 1) some of the outputs are combined internally or externally in exclusive-NOR or exclusive-OR configuration to form a feedback mechanism and 2) it retains the autonomous nature of LFSR that is the last output should be part of feedback mechanism. Figure 2 shows an external type XOR structure of an n-bit LFSR. The $\{c_0, c_1, c_2, \ldots.., c_i,, \ldots., c_{n-1}, c_n\}$, are the possible feedback connections.

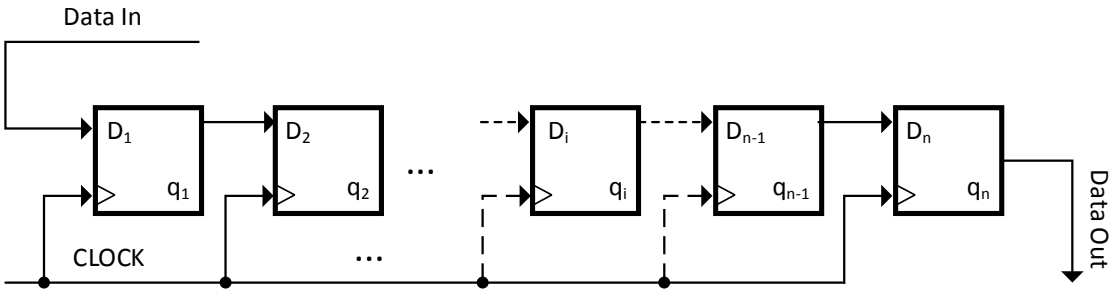

Figure 1. An n-bit SISO shift register.

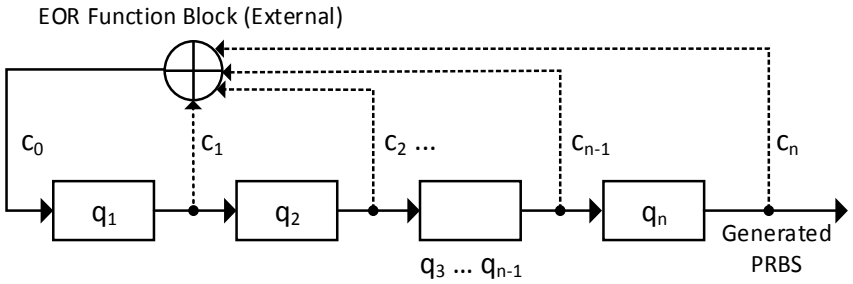

Figure 2. An n-bit LFSR (External XOR type).

Therefore, an LFSR can be formed by either performing exclusive-OR or exclusive-NOR operations on the combined outputs of two or more of the flip-flops. The model for exclusive-NOR has been presented in (Ahmad and Al-Maashri 2008; Ahmad 2005b). In this paper, however, our focus will be towards presenting an algebraic model for an n-bit external exclusive-OR type LFSR.

In an external exclusive-OR type LFSR, the output of the aforementioned operations on the combined outputs of two or more of the FFs and the result is fed to the least significant FF (*ie*. q_1) as shown in Fig. 2. Figure 3 shows an example of a 3-bit LFSR, which is constructed using external XOR functional block. Note how the feedback– which is fed as an input to the first FF – is the result of exclusive-OR operation of the outputs of the second and third FFs. Table 1 visualizes the operations of the LFSR depicted in Fig. 3. The table elaborates the next states (FF1_OUT, FF2_OUT, and FF3_OUT) and the output sequence S_i. The used seed to start the operation is considered as q_1 (0) = 1, q_2 (0) = 0, and q_3 (0) = 1.

It is this feedback function that causes the register to loop through repetitive sequences of PRBS value. The choice of feedback connections, the seed, and the value of 'n' determine the number of PRBS values in a given sequence before the sequence repeats - this length is known as periodicity 'p' of the LFSR (Williams 1984;McCluskey 1985; Nanda *et al*. 1989; Ahmad 1997; Hell and Johansson 2008; Mukherjee *et al*. 2011; Ayinala and Parhi2011; Peterson and

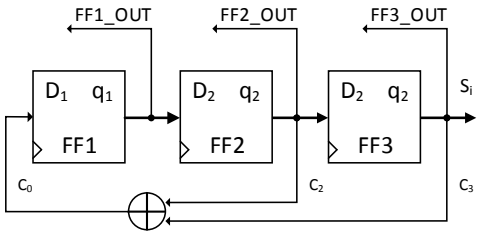

Figure 3. A 3-bit LFSR (External XOR type).

Weldon, Jr. 1984; Golomb 1981; Ahmad and Al-Maashri 2008; Ahmad 2005b; Williams *et al*. 1988; Ahmad 1990; Ahmad and Elabdalla 1997; Ahmad 1994; Knuth 1997; Ahmad *et al*. 2002; Ahmad 2002; Krishnaswamy and Pillai 2012, Peinado and Fuster-Sabater, 2013; Chunqiang *et al*. 2012; Ming-Hung 2013).

3. LFSR AS PRBS Generator – An Algebraic Modeling

In this section, we present a generalized algebraic model exclusively for an n-bit external exclusive-OR type LFSR based PRBS generator. Any binary data sequence can be represented in form of polynomial in GF(2). Therefore, the feedback connection vector for an LFSR can be represented in the form of a polynomial and is technically known as a characteristic polynomial. Eqn. (1) define a general form of a characteristic polynomial and let us call it $\mathcal{D}(x)$.

$$\mathcal{D}(x) = \sum_{i=0}^{n} c_i \times x^i \quad (1)$$

Let $\{a_m\}$= [a_0 , a_1 , . . , a_i, . .], represent the output sequence generated by the LFSR used as PRBS, where a_i= 0 or 1. Then this sequence can be represented as given in Eqn. (2).

$$G(x) = \sum_{m=0}^{n} a_m \times x^m \quad (2)$$

From the structure of the type of the LFSR shown in Fig. 2, it can be seen that if the current state of the i^{th} flip-flop is a_{m-i} , for i = 1, 2 , ... , n , then by the recurrence relation an equation can be given as depicted in Eqn. (3).

$$a_m = \sum_{i=1}^{n} c_i \times a_{m-1} \quad (3)$$

The generating function$G(x)$ associated with the PRBS can be mathematically defined as in Eqn. (4).

$$G(x) = \sum_{i=0}^{\infty} a_i \times x^i \quad (4)$$

or

$$G(x) = \frac{\sum_{i=0}^{n-1} x^i \sum_{k=0}^{i} c_k \times q_{(i+1-k)}}{\sum_{i=0}^{n} c_i \times x^i} \quad (5)$$

or, Eqn. (4) can be rewritten as:

$$s(x) = G(x) = \frac{\mathcal{N}(x)}{\mathcal{D}(x)} \quad (6)$$

The $\mathcal{D}(x)$ and$\mathcal{N}(x)$ can be written in an expanded form as described by Eqns. (8) and (10), respectively.

$$(x) = \sum_{i=0}^{n} c_i \times x^i \quad (7)$$

$$\mathcal{D}(x) = (c_0 \times x^0) + (c_1 \times x^1) + \cdots + (c_n \times x^n) \quad (8)$$

Table 1. Next state sequences (PRBS) for the structure of LFSR of Figure 3.

Clock	q_1 (FF1_OUT)	q_2 (FF2_OUT)	q_3 (FF3_OUT)	S_i
0	1	0	1	
1	1	1	0	
2	1	1	1	
3	0	1	1	…11101001110
4	0	0	1	
5	1	0	0	
6	0	1	0	
7	1	0	1	Repeats

or,

$$\mathcal{D}(x) = 1 + (c_1 \times x^1) + \cdots + (c_n \times x^n) \quad (9)$$

$$\mathcal{N}(x) = (x^0 \times c_0 \times q_1) + (x^1 \times c_0 \times q_2) + (x^1 \times c_1 \times q_1) + (x^2 \times c_0 \times q_3) + (x^2 \times c_1 \times q_2) + (x^2 \times c_2 \times q_1) + \cdots + (x^{n-1} \times c_0 \times q_n) + \cdots + (x^{n-1} \times c_{n-2} \times q_2) + (x^{n-1} \times c_{n-1} q_1) \quad (10)$$

As an example, let us consider the LFSR structure shown in Fig. 3. In this structure, n = 1, q_1 (0) = 1, q_2 (0) = 0, q_3 (0) = 1, c_0 = 1, c_1 = 0, c_2 = 1and c_3 = 1. Hence,$\mathcal{N}(x)$ and $\mathcal{D}(x)$can be derived in the forms of polynomials as given in Eqns. (11) and (12) respectively.

$$\mathcal{D}(x) = 1 + (x^2) + (x^3) \quad (11)$$

$$\mathcal{N}(x) = 1 + (x^2) + (x^2) = 1 \quad (12)$$

Computing$s(x) = \mathcal{N}(x)/\mathcal{D}(x)$, we get the result as shown in Fig. 4. The quotient of this long division process is PRBS in a polynomial form. This result is validated by crosschecking with those presented in Table 1.

$$
\begin{array}{r|l}
 & 1 + x^2 + x^3 + x^4 + x^7 + x^9 + x^{10} + \cdots \\
1 + x^2 + x^3 & \\
\hline
 & 1 \\
 & 1 + x^2 + x^3 \\
\hline
 & x^2 + x^3 \\
 & x^2 \quad + x^4 + x^5 \\
\hline
 & x^3 + x^4 + x^5 \\
 & x^3 \quad + x^5 + x^6 \\
\hline
 & x^4 + x^6 \\
 & x^4 + x^6 + x^7 \\
\hline
 & + x^7 \\
 & + x^7 + x^9 + x^{10} \\
\hline
 & x^9 + x^{10} \\
 & x^9 \quad + x^{11} + x^{12} \\
\hline
 & x^{10} + x^{11} + x^{12} \\
 & x^{10} \quad + x^{12} + x^{13} \\
\hline
 & x^{11} \quad + x^{13} \\
 & \cdots\cdots\cdots
\end{array}
$$

Figure 4. Long-division computation of $s(x) = \mathcal{N}(x)/\mathcal{D}(x)$.

4. Analytical Study

This section presents a study on some special cases where the LFSRs are restricted to generate PRBSs of limited periodicity. The study covers the roles of all parameters related to the LFSR generating the PRBSs. These parameters are '*n*', '*seed*' and the feedback connection function ('*FB*'). The value of *n* may be either even or odd, *seed* may vary from $(0)_{10}$to $(2^n\text{-}1)_{10}$.The FB function depends on input connections coming from c_1, c_2, ….., c_i,, …., $c_{n\text{-}1}$, c_n links to the XOR function block. We present the results of our study in the forms of theorems supported with proofs using algebraic model of LFSR presented in Section 2.Throughout the study, we consider an n-bit XOR structure of LFSR.

Theorem 1:

"If the seed value in the LFSR is 0 ($\mathcal{s} = (0)_{10}$), then for any value of n and for any FB function the period 'p' of generated PRBS by the LFSR will be 1 (p = 1)."

Proof:

Since by substituting *($\mathcal{s} = (0)_{10}$)*, in Eqn. (5), the equation reduces to a Reduction Modular (MOD) equation as given below.

$$0 \; mod \sum_{i=0}^{n} c_i \times x^i = 0 \qquad (13)$$

Hence the generated PRBS is , $\mathcal{s} = 0$ which is the seed value. Hence this proves that the period '*p*' of generated PRBS by the LFSR is 1.

Theorem 2:

"If the seed value in the LFSR is all ones, $\mathcal{s} = (2^n\text{-}1)_{10}$, where n is odd and FB function is considered from all the links [c_1, c_2, ….., c_i,, …., $c_{n\text{-}1}$, c_n], then the period 'p' of generated PRBS by the LFSR will be 1 (p = 1)."

Proof:

Using Eqns. (8) and (9) we can write

$$\mathcal{D}(x) = 1 + (c_1 \times x^1) + \cdots + (c_n \times x^n),$$

$$\mathcal{N}(x) = (x^0) + (x^1) + (x^2) + \cdots + (x^{n-1}).$$

The result of the long division process of Eqn. (14) or Eqn. 15 produces $\mathcal{s}(x) = (2^n\text{-}1)_{10}$, which proves that the '*p*' of $\mathcal{s}(x)$ can be given as:

$$\mathcal{s}(x) = \frac{1 + x + \cdots + x^{n-1}}{1 + x + \cdots + x^n} \qquad (14)$$

or,

$$\sum_{i=0}^{n-1} c_i \times x^i \; mod \sum_{i=0}^{n} c_i \times x^i = \sum_{i=0}^{n-1} x^i \qquad (15)$$

The value $\sum_{i=0}^{n-1} x^i$ implicates that the generated PRBS by the LFSR structure set in Theorem 2 is 1.

Theorem 3:

"If the seed value in the LFSR is all ones, $\mathcal{s} = (2^n\text{-}1)_{10}$, and in the total number of considered links in the FB function from the [c_1, c_2, ….., c_i, …., $c_{n\text{-}1}$, c_n] is odd, then the period 'p' of generated PRBS by the LFSR will be 1 (p = 1)."

Proof:

By substituting the seed value $\mathcal{s} = (2^n\text{-}1)_{10}$, and inserting FB function for the said structure in Theorem 3 in Eqns. (8) and (9) we get:

$$\sum_{i=0}^{n-1} x^i \; mod \; (1 + x^n) = \sum_{i=0}^{n-1} x^i \qquad (16)$$

Therefore, the next state of the LFSR will be the same as the seed and hence it proves that the period of the generated PRBS by the LFSR structure of Theorem 3 will be 1, *ie*. (p = 1).

Theorem 4:

"If the FB function is considered only from the link [c_n] and the seed value in the LFSR is any value except all zeros, $\mathcal{s} = (0)_{10}$ or all ones, $\mathcal{s} = (2^n\text{-}1)_{10}$, then the period 'p' of generated PRBS by the LFSR will be n (p = n)."

Proof:

Let n = 3 and q_1 (0) = 1, q_2 (0) = 1, and q_3 (0) = 0. Using Equation (9), the numerator$\mathcal{N}(x)$ can be computed as $\mathcal{N}(x) = 1 + x$.

Therefore, dividing $\mathcal{N}(x)$ by$\mathcal{D}(x)$, $[\mathcal{D}(x) = 1 + x^3]$ we get:

$\mathcal{s}(x) = 1 + x + x^3 + x^4 + x^6 + x^7 + \cdots = (((1 + x) \times x^3) \times x^3)$.

This demonstrate that the period 'p' of generated PRBS by the LFSR is 3 (i.e. $p = n$). We can consider any value of n, resulting$\mathcal{s}(x) = (((1 + x) \times x^n) \times x^n))$.

Theorem 5:

"If FB function is considered from all the links [c_1, c_2, ….., c_i,, …., $c_{n\text{-}1}$, c_n], and the seed value in the LFSR is any value except all zeros, $\mathcal{s} = (0)_{10}$ or all ones, $\mathcal{s} = (2^n\text{-}1)_{10}$, then the period 'p' of generated PRBS by the LFSR will be n +1 (p = n +1)."

Proof:

Let n = 3 and q_1 (0) = 1, q_2 (0) = 1, and q_3 (0) = 0. Using Eqn. (9) the numerator $\mathcal{N}(x)$ can be computed as$\mathcal{N}(x) = 1$. Therefore, dividing$\mathcal{N}(x)$ by$\mathcal{D}(x)$, $[\mathcal{D}(x) = 1 + x + x^2 + x^3]$ We get$\mathcal{s}(x) = 1 + x + x^4 + x^5 + x^8 + x^9 + \cdots = (((1 + x) \times x^4) \times x^4))$.

This demonstrates that the period 'p' of generated PRBS by the LFSR is 3 (*ie*. $p = n$). We can consider any value of n, resulting $\mathcal{s}(x) = (((1 + x) \times x^{n+1}) \times x^{n+1}$.

Theorems 1-5 presented in Section 4 have great values. Firstly, from point of view of applications of LFSRs and secondly, the described theorems shall help in deducing the LFSR structures of maximal length sequences. Considering the interests of practicing engineers, we present Table 2 to demonstrate how guidelines and restrictions can be ascertained while using LFSRs for its practical usage. For demonstrating the applicability of Theorems 1 and 3-5, all possible LFSR's structures of order n = 4 are considered. Also, the applicability of the study helps in searching the generator for maximal length sequences. As can be visualized from Table 2, for n = 4, there exist 8 possible FB functions, out of those 8, 5 of them have restrictions. Hence, the search set is reduced to 3 as $(1 + x + x^4)$, $(1 + x^2 + x^4)$, and $(1 + x^3 + x^4)$.

5. Simulation Model

A simulation model was developed to validate the analytical study presented in Section 3. The model was developed in MATLAB to simulate the behavior of LFSR structures. Figure 5 illustrates the two simulation models that were developed to validate the theorems. Figure 5a depicts the model "*prb_single_seed*", which is capable of generating PRBS '*prbs*' as function of feedback connection '*fb*' and seed's'. In simulation, the length of the generated sequence is controlled by a set length '*l*', computed as follows: $l = 2^*(2^n\text{-}1)$.

Table 2. Demonstrating guideline and restrictions based on Theorem 1–5.

Study	Possible feedback connection functions of order 4 (n = 4)								Comment
	$1+x^4$	$1+x+x^4$	$1+x^2+x^4$	$1+x+x^2+x^4$	$1+x^3+x^4$	$1+x+x^3+x^4$	$1+x^2+x^3+x^4$	$1+x+x^2+x^3+x^4$	
Theorem 1	*G1	*G1	*G1	*G1	*G1	*G1	*G1	*G1	*G1: Guideline Do not use $\mathcal{s} = (0)_{10}$
Theorem 3	*R3			*R3		*R3	*R3		*R3: Restriction Do not use $\mathcal{s} = (2^n\text{-}1)_{10}$
Theorem 4	*R4								*R4: Restriction Restricts p to $p = n$ for any value of$\mathcal{s}$ except as restricted by Theorems 1 and 3
Theorem 5								*R5	*R5: Restriction Restricts p as: $p = n + 1$ for any value of$\mathcal{s}$ except as restricted by Theorems 1 and 3
Theorem 2	n = 5; $1+x+x^2+x^3+x^4+x^5$								*R2: Restriction Restricts p as p = 1 for a value of$\mathcal{s}$, as $\mathcal{s} = (2^n\text{-}1)_{10}$
	n = 7; $1+x+x^2+x^3+x^4+x^5+x^6+x^7$								
	n = 9; $1+x+x^2+x^3+x^4+x^5+x^6+x^7+x^8+x^9$								

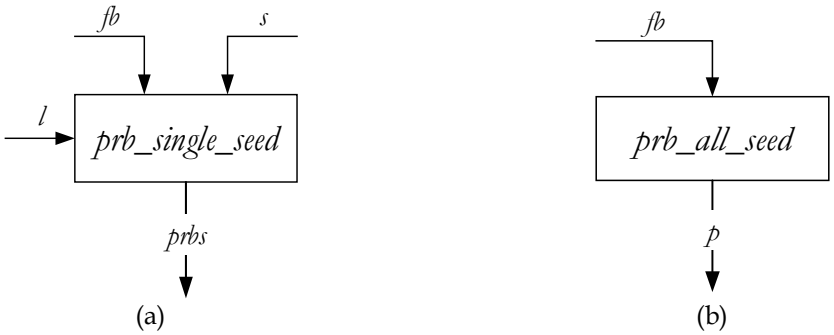

Figure 5. The two simulation models that are used to validate the theorems presented in analytical study. (a) Used to validate the Theorems 1, 2, and 3 (b) Used to validate the Theorems 4 & 5.The model "*prb_single_seed*" is used to validate the theorems 1, 2, and 3.

Table 3 shows a representative result set out of the simulation results when running the model to validate Theorem 1. The table demonstrates that for any possible '*fb*' the period of '*prbs*' is 1. Similarly, Table 4 shows the simulation results for validating Theorems 2 and 3.

To validate Theorems 4 and 5, we use another simulation model called "*prb_all_seed*" (see Figure 5b). Unlike the model above, "*prb_all_seed*" examines the LFSR structures by generating all possible seeds, while requiring only '*fb*' to compute the output *p* of the function. The sample results for the runs are given in Tables 5 and 6 for validations of Theorems 4 and 5, respectively.

6. Justification of the Study

Due to their good statistical properties, the LFSRs generating maximal length PRBSs are widely used in stream ciphers (Knuth 1997; Ahmad *et al*. 2001). The maximal length PRBSs are popularly known as m-sequence or Pseudo Noise (PN) sequence. The maximal length PRBSs have period length of 2^n-*1* (where *n* is the length of the LFSR). Such LFSRs, which generates m-sequence, are realized when the corresponding FB to the LFSR is primitive **(**Peterson and Weldon, Jr. 1984; Golomb 1981; Ahmad *et al*. 1990; Ahmad and Elabdalla1997; Knuth 1997; Chunqiang *et al*. 2012; Ahmad *et. al* 2013b; Ming-Hung 2013). It is imperative for the designers of crypto systems to consider suitable criteria

Table 3. Results of simulation runs for Theorem 1.

Theorem	n		p

Theorem 1	2	*Case 1:*
		fb=[1,1,1]; s=[0,0];
		prbs =
		0 0 0 0 0 0
		
		Case 2:
		fb=[1,0,1]; s=[0,0];
		prbs=
		0 0 0 0 0 0
			$p = 1$ for all the cases

	3	*Case 1:*
		fb=[1,1,1,1]; s=[0,0,0];
		prbs =
		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
		
		Case 2:
		fb=[1,0,0,1]; s=[0,0,0];
		prbs =
		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
		
		Case 3:
		fb=[1,0,1,1]; s=[0,0,0];
		prbs=
		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0
		
		Case 4:
		fb=[1,1,0,1]; s=[0,0,0];
		prbs =
		0 0 0 0 0 0 0 0 0 0 0 0 0 0 0	

Table 4. Results of simulation runs for Theorems 2 and 3.

Theorem	n		p
Theorem 2	3	FB = [1,1,1,1]; *s* = [1,1,1]; PRBS = 1 1 1 1 1 1 1 1 1 1 1 1 1 1	*p* = 1 for all the cases
	5	FB = [1,1,1,1,1,1]; *s* = [1,1,1,1,1]; PRBS = 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	
Theorem 3	4	FB = [1,0,1,1,1]; *s* = [1,1,1,1]; PRBS = 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	

FB = feedback connection; s = seed; PRBS = pseudorandom binary sequence

Table 5. Results of simulation runs for Theorem 4.

Theorem	n		p
Theorem 4	2	FB = [1,0,1]; *p* = 2	*p* = n for all the cases
	3	FB =[1,0,0,1]; *p* = 3	
	5	FB = [1,0,0,0,0,1]; *p* = 5	
	21	FB = [1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,1]; *p* = 21	
	41	FB = [1,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0,0, 0,0,0,0,1]; *p* = 41	

FB = feedback connection; p = periodicity

Table 6. Results of simulation runs for Theorem 5.

Theorem	n		p
Theorem 5	16	FB = [1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]; *p* = 17	*p* = n + 1 for all the cases
	32	FB = [1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]; p = 33	
	64	FB = [1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1, 1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1,1]; *p* = 65	

FB = feedback connection; p = periodicity

for the selection of a key stream generator in the design. Some of these design criteria are statistical measures, period and linear complexity. Acceptable PRBSs should exhibit no statistical bias in occurrence of individual symbols or small block of symbols. In this regard, Golomb's postulates defined in (Ahmad *et al*. 2002; Ahmad *et al*. 2013c; Golomb 1981)suggest that a PRBS that passes the tests for randomness will be acceptable for the use of cryptosystems and other applications like radar, Code Division Multiple Access (CDMA), error correction and Monte Carlo simulation. For the sake of completeness, we list the postulates outlined in (Ahmad *et al*. 2002; Ahmad *et al*, 2013c;Golomb 1981); namely, 1) PRBS Length, 2) Balance of 1's and 0's, 3) Run property, and 4) Ideal autocorrelation.
In this paper, the study of the Theorems 1, 2 and 3 provide the boundary situations where LFSRs lock and fail to generate PRBSs of sufficient length. Also LFSR structures and seed combinations are to be avoided in length. Because of this, LFSR structures and applications of BIST as test pattern generators, and in cryptography as key generators.

To demonstrate the level of prohibitions and utilizations of the LFSR structures defined in Theorems 4 and 5, we considered the criterions of Golomb's postulates. The ratios of the lengths of generated PRBS using the generators defined in Theorems 4 and 5 with respect to the maximal length PRBS of 2^n-1 (where n is the length of the LFSR) are shown in Table 7 for n = {*2, 3, 4, 5, 6, 7, 8, 16, 32, 64, 128*}. In the table, R_{4ml} and R_{5ml} represent the ratios due to the described PRBS generators of Theorems 4 and 5, respectively. In addition, Table 7 demonstrates the balance properties of the LFSR structures defined via Theorems 4 and 5. Moreover, R_{4mo} and R_{5mo} represent the ratios due to the described PRBS generators of Theorems 4 and 5, respectively, of maximum possible number of 1's. Whereas, R_{4mz} and R_{5mz} represent the ratios due to the described PRBS generators of Theorems 4 and 5, respectively, of maximum possible number of zeroes.

7. Conclusion and Future Work

PRBS serves an important role in a diversified collection of application domains; including cryptography and fault tolerance. This work has investigated the properties of LFSR circuits used for generating PRBS periods and highlighted the behavior of some of the LFSR structures. The study has employed the recurrence relations to describe the PRBS periods generated by the LFSR structures. A number of theorems have been presented in this paper. These theorems summarize the observations that were outlined throughout the discussion of the analytical model. These observations add some knowledge towards the generation of maximal length PRBS. The theorems and their subsequent outcomes were validated using a simulation model.

The focus of this study was on PRBS generation; however, LFSRs could also be the building block of other correlation functions. As future work, it would be interesting to investigate further properties and observations on the LFSR circuits that could be of use in other application domains and functions.

Acknowledgments

The authors would like to express their great appreciations and gratitude to Sultan Qaboos University, Sultanate of Oman for providing research facilities, technical supports and research environment.

References

Ahmad A (1994), Critical role of polynomial seeds on the effectiveness of an LFSR-based testing technique. International Journal of Electronics 77:127–137.

Ahmad A (1997), Achievement of higher testability goals through the modification of shift register in LFSR based testing. International Journal of Electronics 82:249–260.

Ahmad A (2002), Constant error masking behavior of an internal XOR type signature analyzer due to the changed polynomial seeds. Journal of Computers & Electrical Engineering 28:577–589.

Ahmad A (2005a), Testing of complex integrated circuits (ICs)–The bottlenecks and solutions. Asian Journal of Information Technology4:816–822.

Ahmad A (2005b), Development of state model theory for external exclusive-NOR type LFSR structures. World Enformatika Society-Transactions on Engineering, Computing and Technology 10:12–19.

Ahmad A (2012), Better PN generators for CDMA application–A Verilog-HDL implementation approach. International Journal of Information Engineering 2:6–11.

Ahmad A (2013a), Development realization of a better signature analysis scheme by adding a bit to the size of 8k. International Journal of Information Engineering 3:122–128.

Ahmad A, Al-Busaidi SS, Al-Maashri A, Awadalla M, Rizvi MAK, Mohanan N (2013b), Computing and listing of possible number of m-sequence generators of order n. Indian Journal of Science and Technology10:5359–5369.

Ahmad A, Al-Busaidi SS, Al-Mushrafi MJ (2013c), On properties of PN sequences generated by LFSR—A generalized study and simulation modeling. Indian Journal of Science and Technology10:5351–5358.

Ahmad A, Al-Maashri A (2008), Investigating some special sequence lengths generated in an external exclusive-NOR type LFSR. Journal of Computers and Electrical Engineering 34:270–280.

Ahmad A, Al-Musharafi MJ, Al-Busaidi S (2002), Study and implementation of properties of m-sequences in MATLAB-SIMULINK—A pass/fail test tool for designs of random generators. SQU Journal of Scientific Research–Science and Technology 7:147–156.

Ahmad A, Al-Musharafi MJ, Al-Busaidi S, Al-Naamany A, Jervase JA (2001), An NLFSR based sequence generation for stream ciphers. Proceeding International Conference on Sequences and their Applications, Bergen, Norway, May 13-17, 11–12.

Ahmad A, Elabdalla AM (1997), An efficient method to determine linear feedback connections in shift registers that generate maximal length pseudo-random up and down binary sequences. Computer & Electrical Engineering—An International Journal 23:33–39.

Ahmad A, Nanda NK, Garg K (1997), Are primitive polynomials always best in signature analysis? IEEE Design & Test of Computers 7:36–38.

Ayinala M, Parhi K (2011), High-speed parallel architectures for linear feedback shift registers. IEEE Transactions on Signal Processing 59(9):4459–4469.

Bardell PH, McAnney WH, Savir J (1987), Built-in-test for VLSI. New York: John Wiley.

Chunqiang H, Xiaofeng L, Xiuzhen (2012), Verifiable multi-secret sharing based on LRSR sequences. Journal of Theoretical Computer Science 445:52-62.

Golomb SW (1981), Shift register sequence. Walnut Creek, CA: Aegean Park Press.

Hell M, Johansson T, Maximov A, Meier W (2008), New stream cipher designs—The eSTREAM finalists, Springer 4986:179–190.

Hu CQ, Liao XF, Cheng XH (2012), Verifiable multi-secret sharing based on LFSR sequences. Journal of Theoretical Computer Science (Elsevier) 45:52–62.

Jamil T, Ahmad A (2002), An Investigation into the Application of Linear Feedback Shift Registers for Steganography. Proceeding IEEE Southeast Con, SC, USA. April 2002.

Kao MH (2013), On the optimality of extended maximal length linear feedback shift register sequences. Journal Statistics & Probability Letters 83:1479–1483.

Knuth D (1997), The art of computer programming, Semi numerical algorithms. Reading, MA: Addison-Wesley 2.

Krishnaswamy S, Pillai HK (2012), On the number of linear feedback shift registers with a special structure. IEEE Transactions on Information Theory 58(3):1783–1790.

McCluskey EJ (1985), Built-in self-test techniques. IEEE Design & Test of Computers 2(2):21–28.

Ming-Hung K (2013), On the optimality of extended maximal length linear feedback shift register sequences. Journal of Statistics and Probability Letters 83(6):1479-1483.

Mukherjee N, Rajski J, Mrugalski G, Pogiel A (2011), Ring generator: An ultimate linear feedback shift register. IEEE Computer 44(6):64–71.

Nanda NK, Ahmad A, Gaindhar VC (1989), Shift register modification for multipurpose use in combinational circuit testing. International Journal of Electronics 66(6):875–878.

Peinado A, Fuster-Sabater A (2013), Generation of pseudorandom binary sequences by means of linear feedback shift registers (LFSRs) with dynamic feedback. Mathematical and Computer Modeling 57(6): 2596–2604.

Peterson WW, Weldon EJ Jr (1984), Error-correcting codes. 2nd ed., Cambridge, MA: Massachusetts Institute of Technology Press.

Williams TW (1984), VLSI testing. IEEE Computer C-17(10):126–136.

Williams TW, Daehn W, Gruetzner M, Starke CW (1988), Bounds and analysis of aliasing errors in linear feedback shift registers. IEEE Trans. Computer Aided-Design CAD-7(1):75–83.

Appendix A

List of abbreviations and terminology used in the paper

PRBS	Pseudorandom binary sequence
BIST	Built-in self-test
VLSI	Very-large-scale integration
LFSR	Linear feedback shift register
XOR	Exclusive-OR
XNOR	Exclusive-NOR
SISO	Serial-in serial-out
n	LFSR size
c_i	The i^{th} feedback connection
FF	Flip-flop
q_i	The state of the i^{th} FF
D_i	The input to the i^{th} FF
GF(2)	Galois Field mod 2
D(x)	Characteristic polynomial of LFSR
s	Generated PRBS
Seed	Initial state of LFSR