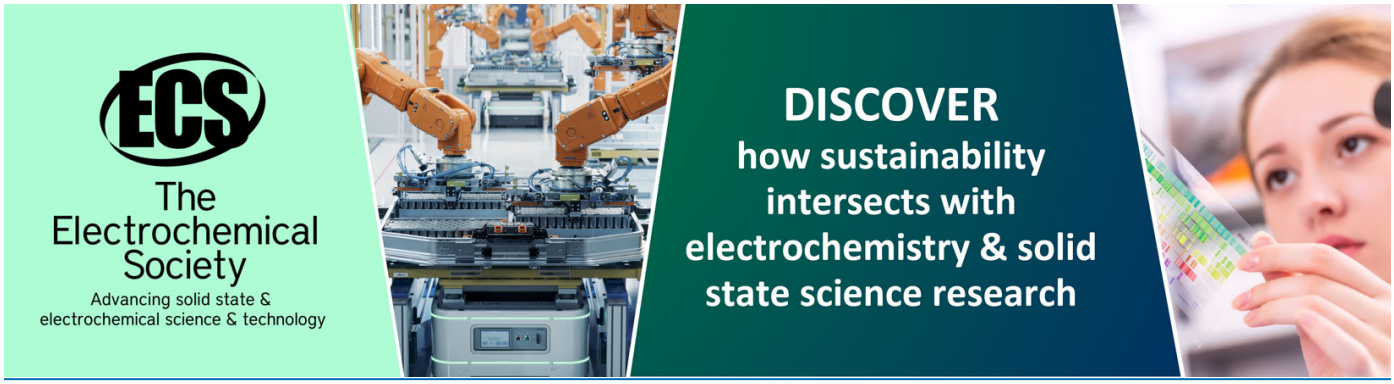
Pseudo-random sequences with nonmaximal length based on the shift register and reducible polynomial



IOP Conf. Series: Journal of Physics: Conf. Series **1352** (2019) 012035 doi:10.1088/1742-6596/1352/1/012035

Pseudo-random sequences with nonmaximal length based on the shift register and reducible polynomial

V A Pesoshin, V M Kuznetsov and A K Rakhmatullin

Kazan National Research Technical University named after A.N. Tupolev - KAI, Kazan, Russia

E-mail: pesoshin-kai@mail.ru

Abstract. We consider nonhomogeneous pseudorandom sequences of nonmaximal length formed by a shift register with linear feedback (Fibonacci generators), and with internal half-adders (Galois generators). As a basis, we consider characteristic polynomial raised to the power of n of a form $\varphi(x) = \varphi_0^m(x)\varphi_1(x)$, where $\varphi_0(x)$ and $\varphi_1(x)$ are primitive polynomials respectively raised to the power of m_1 and m_1, $m_0 \cdot m + m_1 = n$. We discovered periodic polynomial structures. Examples demonstrate a diversity of generated practical sequences, which are organized and ordered from elements of direct and inverse M-sequences. We investigated probabilistic properties of the formed sequences.

1. Introduction

It is necessary to generate pseudo-random sequences (PRS) with a variety of properties to solve problems by the method of statistical modeling [1]. Most of the time, PRSs are generated by PRS generators (pseudo-random number generator, PRNG) based on an n-bit shift register with linear feedbacks (Fibonacci generator) and with half-adders (Galois generator) [2, 3].

We propose underinvestigated methods based on a reducible characteristical polynomial raised to the power of n to produce nonhomogeneous PRSs with nonmaximal length.

$$\varphi(x) = \varphi_0^m(x)\varphi_1(x), \tag{1}$$

Where $\varphi_0(x)$ and $\varphi_1(x)$ are primitive polynomial respectively raised to the power of m_0 and m_1, $m_0 \cdot m + m_1 = n$. Coefficient $\alpha = 1$ parameterizes nonhomogeneous property as an inversion operator in the feedback circuit.

We proved that a problem of finding a periodic structure (PS) of the polynomial $\varphi_0^m(x)$is reducible to a problem of sequential finding a PS

$$\varphi_0(x), \varphi_0^2(x), \ldots, \varphi_0^j(x), \ldots, \varphi_0^m(x).$$

The set of periods of the polynomial $\varphi_0^j(x)$ consists of elements of the set of periods of the polynomial $\varphi_0^{j-1}(x)$ and μ_j periods of length $L_0 p^{k_j}$, where L_0 is the period length of the polynomial $\varphi_0(x)$, k_j is the smallest integer for which $p^{k_j} \geq j$, and μ_j is determined by the expression

$$\mu_j = \frac{p^{m_0(j-1)}(p^{m_0}-1)}{L_0 p^{k_j}}. \tag{2}$$

We reach the similar PS of the polynomial $\varphi_0^m(x)$ at $\alpha = 1$ [5].

A complexly organized form straight M- and inverse M̄- sequences (MS and M̄S) is the basis of the manifold of the PRS in which monocycles 0 and 1 are forbidden, respectively [6].

2. Pseudo-random sequences generated by the Fibonacci generator

The Fibonacci generator forms identical sequences on all outputs up to the initial phase within its period.
Example 1. Let $m = m_0 = 2$. Polynomial based PRNG

$$\varphi_0(x) = x^2 \oplus x \oplus 1 \tag{3}$$

forms MS 0 1 1 at α = 0 and M̄S 0 0 1 at α = 1 with PS {1 (1), 1 (3)}.
For polynomial

$$\varphi_0^2(x) = x^4 \oplus x^2 \oplus 1 \tag{4}$$

PS is {1 (1), 1 (3), 2 (6)}. We obtained the following PRS by simulating the operation of the Fibonacci generator based on a polynomial (4), for α = 1 (table 1).

Table 1. Generated polynomial sequences (4).

q_1	q_2	q_3	q_4	q_1	q_2	q_3	q_4	q_1	q_2	q_3	q_4	q_1	q_2	q_3	q_4
1	**1**	**1**	**1**	**0**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**1**	**0**	**1**
1	**1**	**1**	**1**	1	0	0	1	1	0	0	0	1	0	1	0
				0	1	0	0	1	1	0	0	1	1	0	1
				0	**0**	**1**	**0**	0	1	1	0	1	1	1	0
								0	0	1	1	0	1	1	1
								0	0	0	1	1	0	1	1
								0	**0**	**0**	**0**	**0**	**1**	**0**	**1**

The polynomial $\varphi_1(x)$raised to the power of $(n-4) \geq 2$has PS $\{1(1),\ \ 1(2^{n-4}-1)\}$.The interaction of both PS provides the polynomial$\varphi(x)$ with the following PS:

$$\{1(1),\ 1(3),2(6),1(2^{n-4}-1),1(3\cdot(2^{n-4}-1)),2(6\cdot(2^{n-4}-1))\}. \tag{5}$$

The sequences with PS {1 (1), 1 (3), 2 (6)} form non-working (forbidden) cycles and participate in the formation of working PRS with PS $\{1(2^{n-4}-1),1(3(2^{n-4}-1),2(6(2^{n-4}-1))\}$.
Consider the case when $\varphi_1(x) = x^3 \oplus x \oplus 1$, then for PRNG in the form of (1)

$$\varphi(x) = (x^3 \oplus x \oplus 1)(x^4 \oplus x^2 \oplus 1) = x^7 \oplus x^4 \oplus x^2 \oplus \mathrm{x} \oplus 1. \tag{6}$$

We define PS working sequences (WS) from (5) as $\{1(7),1(21),2(42)\} = \{1(7),1(3\cdot 7),2(6\cdot 7)\}$. Define the forbidden state (FS) of the shift register in tables for WS with a period of 21 (table 2a) and with periods of 42 (table 2b and table 2c).

Table 2. FS of shift register for Fibonacci generator.

(a)

q_1	q_2	q_3	q_4	q_5	q_6	q_7
0	**0**	**1**	**0**	**0**	**1**	**0**
1	0	0	1	0	0	1
0	1	0	0	1	0	0
0	**0**	**1**	**0**	**0**	**1**	**0**

(b)

q_1	q_2	q_3	q_4	q_5	q_6	q_7
0	**0**	**0**	**0**	**1**	**1**	**0**
1	0	0	0	0	1	1
1	1	0	0	0	0	1
0	1	1	0	0	0	0
0	0	1	1	0	0	0
0	0	0	1	1	0	0
0	**0**	**0**	**0**	**1**	**1**	**0**

(c)

q_1	q_2	q_3	q_4	q_5	q_6	q_7
0	**1**	**0**	**1**	**1**	**1**	**0**
1	0	1	0	1	1	1
1	1	0	1	0	1	1
1	1	1	0	1	0	1
0	1	1	1	0	1	0
1	0	1	1	1	0	1
0	**1**	**0**	**1**	**1**	**1**	**0**

The WS with period 21 (table 2a) is organized and ordered from the elements of two MS and one $\bar{M}S$ (note organization of the FS of the form 001). Similarly, a RP with a period of 42 combines four MS and two $\bar{M}S$ (table 2b), MS, $\bar{M}S$, MS and four $\bar{M}S$ (table 2c), which corresponds to WS 00011 and 01011. The characteristic polynomial $\varphi_1(x) = x^3 \oplus x \oplus 1$ generates complex ordered MS and $\bar{M}S$ in the form (1).

Table 3 shows the sequences generated by the nonhomogeneous Fibonacci generator with the polynomial $\varphi_0^m(x) = (x^2 \oplus x \oplus 1)^m$ for $m = \overline{1,\ 4}$.

Table 3. The Fibonacci generator produces the polynomial $\varphi_0^m(x) = (x^2 \oplus x \oplus 1)^m$ for $m = \overline{1,\ 4}$ and $\alpha = 1$.

Power of the polynomial	**PS**	**Sequences**
1	{1(1),1(3)}	1, 1)001
2	{1(1),1(3), 2(6)}	1, 001, 1)000011, 2)010111
3	{1(1),1(3), 2(6),4(12)}	1, 001, 000011, 010111, 1)000000101101, 2)**000100011111**, 3)**001010100111**, 4)001101111011
4	{1(1),1(3), 2(6),4(12),16(12)}	1, 001, 000011, 010111, 000000101101, **000100011111**, **001010100111**, 001101111011, 1)000000001111, 2)000010100101, 3)001110110111, 4)011101111111, 5)**000110010111**, 6)**000100111101**, ... 15)**000111010011**, 16) 000010100101,

The resulting sequence at the output of the PRNG is generated by a polynomial (1) and corresponds to the half-adder MS for the polynomial $\varphi_1(x)$ and the sequence generated by $\varphi_0^m(x)$.

Bold shows equiprobable sequences.

3. Pseudo-random sequences produced by a Galois generator

Nonhomogeneous Galois generators may produce different sequences as the outputs. Internal generators $\bar{M}S$ with half-adder, and MS with different shifts forms $\bar{M}S$, but the sum of two $\bar{M}S$ forms MS [2]. Nonhomogeneous Galois PRNG based on the polynomial (4) and different generated sequences are presented in table 4.

Table 4. Galois PRNG generated polynomial sequences (4).

q_1	q_2	q_3	q_4	q_1	q_2	q_3	q_4	q_1	q_2	q_3	q_4	q_1	q_2	q_3	q_4
0	**0**	**1**	**1**	**0**	**1**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**
0	**0**	**1**	**1**	1	0	1	0	1	0	0	0	0	0	1	0
				1	1	0	1	1	1	0	0	1	0	0	1
				0	**1**	**0**	**0**	1	1	1	0	0	1	1	0
								1	1	1	1	1	0	1	1
								0	1	0	1	0	1	1	1
								0	**0**	**0**	**0**	**0**	**0**	**0**	**1**

Let define the PRNG Galois FS for WS with a period of 21 (table 5a) and with periods of 42 for two sequences (table 5b and table 5c).

Table 5. FS of shift register for Galois generator.

(a)

q_1	q_2	q_3	q_4	q_5	q_6	q_7
0	**0**	**0**	**0**	**1**	**0**	**0**
1	0	0	0	0	1	0
1	1	0	0	0	0	1
0	**0**	**0**	**0**	**1**	**0**	**0**

(b)

q_1	q_2	q_3	q_4	q_5	q_6	q_7
0	**1**	**1**	**0**	**0**	**0**	**0**
1	0	1	1	0	0	0
1	1	0	1	1	0	0
1	1	1	0	1	1	0
1	1	1	1	0	1	1
0	0	0	1	0	0	1
0	**1**	**1**	**0**	**0**	**0**	**0**

(c)

q_1	q_2	q_3	q_4	q_5	q_6	q_7
0	**1**	**1**	**1**	**1**	**0**	**1**
0	1	0	1	0	1	0
1	0	1	0	1	0	1
0	0	1	1	1	1	0
1	0	0	1	1	1	1
0	0	1	0	0	1	1
0	**1**	**1**	**1**	**1**	**0**	**1**

WS with period 21 (table 4) at the output of register q_1 corresponds to FS 011, at output q_7 is the inverse state 001, at outputs q_3 and q_4 is 000, at outputs q_2, q_5 and q_6 is 001 with various shifts. Similarly, WS with a period of 42 (table 5) has at outputs q_1 equals 001111, at outputs q_5, q_6 and q_7 are inverse to this state 000011, at output q_2 is 010111, at outputs q_3 and q_4 are 011011. Difficultly ordered MS and M̄S correspond to the polynomial $\varphi_1(x) = x^3 \oplus x \oplus 1$.

The analysis of the PRS for illustrative purposes is considered on small-sized examples. Similarly, pseudo-random sequences can be investigated for other values of m_0, m and m_1.

4. Probability and correlation properties of pseudo-random sequences.

The probabilistic properties of pseudo-random sequences at the outputs of generators depend on the number of MS and M̄Scontained in them, which are defined by FS, which are generated by a polynomial $\varphi_1(x)$raised in power of m_1. Then FS is 00...0 the probability is determined by the MS, and by the probability of M̄Sin case of 11... 1. If the FS contains an equal number of 0 and 1, then the output sequences are equally probable.

The correlation properties of the generated sequences are also varied. In table 10 shows small-sized examples of PRS with a maximum period of 12 from table 5 with the values of the normalized periodic autocorrelation functions $\boldsymbol{r}(\tau)$ presented at half the period along the axis of the argumentτ. The second half of the functions repeats the first half symmetrically in the middle of the period $\tau = 6$, corresponding to the gray column of the table 6. The rows of the table are indicated by the combination of the minimum degree m of the polynomial $\varphi_0(x)$and the sequence number in the table 3.

Table 6. Normalized periodic autocorrelation functions.

m.#	Sequences with a period of 12	Arguments of autocorrelation functions						Probability
		$\tau=1$	$\tau=2$	$\tau=3$	$\tau=4$	$\tau=5$	$\tau=6$	
1.1	001(001001001)	-0,5	-0,5	1	-0,5	-0,5	1	0,33
2.1	000011(000011)	0,25	-0,5	-0,5	-0,5	-0,5	1	0,33
2.2	010111(010111)	-0,5	0,25	-0,5	0,25	-0,5	1	0,67
3.1	000000101101	-0,125	0,25	0,25	-0,5	-0,125	-0,5	0,33
3.3	**001010100111**	-0,33	0	-0,33	0	0,33	-0,33	**0,5**
4.1	000000001111	0,625	0,25	-0,125	-0,5	-0,5	-0,5	0,33
4.2	000010100101	-0,5	0,25	-0,125	-0,5	0,625	-0,5	0,33
4.3	001110110111	-0,125	-0,5	-0,125	0,25	0,25	-0,5	0,67
4.4	011101111111	-0,2	-0,2	-0,2	0,4	-0,2	-0,2	0,83
4.5	**000110010111**	0	-0,33	-0,33	0	0	0,33	**0,5**
4.6	**000100111101**	0	0	0	0	-0,33	-0,33	**0,5**

5. Conclusion

Pseudo-random sequences of nonmaximal length, formed by nonhomogeneous Fibonacci and Galois generators based on the characteristic polynomial of type $\varphi(x) = \varphi_0^m(x)\ \varphi_1(x)$ in power of n, where $\varphi_0(x)$ and $\varphi_1(x)$ are primitive polynomials of degree m_0 and m_1, respectively, are investigated, $m_0 m + m_1 = n$. Periodic polynomial structures are defined. Sequence analysis was performed on small-sized examples. A variety of correlation and probabilistic properties promotes the use of the considered sequences in simulation modeling. The material of the article is staged. Further elaboration of the topic is planned in the direction of searching for methods of identifying sequences at the outputs of the Galois generator and methods for initializing the required modes of binary sequences. Also relevant are the methods for specifying the required statistical properties of the memory bandwidth that simulate the external effects of the real environment for machine models.

Acknowledgments

This work was supported by Russian Foundation for Basic Research and the Government of the Republic of Tatarstan, project 18-47-160001.

References

[1] Ivanova V M 1984 *Random Numbers and Their Application* (Moscow: Finances and Statistics)
[2] Kuznetsov V M and Pesoshin V A 2013 *Generators of Random and Pseudorandom Sequences Based on Digital Delay Elements* (Kazan: Kazan. Gos. Tekhn. Univ.)
[3] Pesoshin V A and Kuznetsov V M and Shirshova D V 2016 Generators of the equiprobable pseudorandom nonmaximal-length sequences based on linear-feedback shift registers *Automation and Remote control* **779** 1622–1631
[4] Gill A 1966 *Linear Sequential Circuits; Analysis, Synthesis, and Applications* (New York: McGraw-Hill)
[5] Kugurakov V S and Sokolov O B 1969 Set of Cycle Lengths of One-to-One Affine Mappings of the Space Vn (GF(p)) on Itself *Proc. Kazan State Univ* Kazan: KGU **129 4** 74–79
[6] Pesoshin V A and Kuznetsov V M and Gumirov AI and Shirshova D V 2018 Generators of the binary inverse-segment pseudo-random sequences *Proceeding of IEEE East-west design & test symposium* 268–275