УДК 681.325: 621.391.3:518.5:519.95
DOI 10.21685/2072-3059-2019-4-2

В. А. Песошин, В. М. Кузнецов, А. С. Кузнецова

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НЕМАКСИМАЛЬНОЙ ДЛИНЫ НА РЕГИСТРАХ СДВИГА С ЛИНЕЙНОЙ ОБРАТНОЙ СВЯЗЬЮ НА ОСНОВЕ ПРИМИТИВНОГО МНОГОЧЛЕНА В СТЕПЕНИ[1]

Аннотация.

Актуальность и цели. Современные методы организации машинных экспериментов в виде имитационных моделей основаны на использовании числовых последовательностей вероятностно-статистической природы, адекватных реальным процессам и явлениям. Цель статьи – продемонстрировать новые возможности генераторов двоичных последовательностей как псевдослучайных, не ограничиваясь реализацией бернуллиевской схемы независимых испытаний.

Материалы и методы. Предлагаются малоизученные методы аппаратного формирования двоичных рекуррентных последовательностей генераторами регистрового типа с линейной обратной связью. Математической основой генераторов выбран составной характеристический многочлен, состоящий из примитивных многочленов, один из которых возведен в целочисленную степень.

Результаты. Показано, что в однородном и неоднородном режимах работы генератора наблюдается многообразие формируемых последовательностей. Представлены в статистической и функциональной формах корреляционные связи элементов последовательностей. Решена задача инициализации генератора на формирование циклов немаксимальной длины данного порядка.

Выводы. Предложены аналитические условия и схемотехническая организация генераторов последовательностей немаксимальной длины с разнообразными вероятностными и корреляционными свойствами, расширяющими функциональные возможности имитационного эксперимента.

Ключевые слова: генератор псевдослучайных последовательностей, регистр сдвига, многообразие последовательностей, однородные и неоднородные последовательности, индикаторные последовательности, корреляционные функции.

V. A. Pesoshin, V. M. Kuznetsov, A. S. Kuznetsova

PSEUDO-RANDOM SEQUENCE GENERATORS OF NON-MAXIMUM LENGTH ON SHIFT REGISTERS WITH LINEAR FEEDBACK BASED ON A PRIMITIVE POLYNOMIAL OF SOME POWER

[1] Работа выполнена при финансовой поддержке РФФИ и Правительства Республики Татарстан в рамках научного проекта № 18-47-160001.

Abstract.

Background. Modern methods of organizing machine experiments in the form of simulation models are based on the use of numerical sequences of probabilistic-statistical nature, adequate to real processes and phenomena. The purpose of the article is to demonstrate the new possibilities of binary sequence generators as pseudo-random, not limited to the implementation of the Bernoulli scheme of independent tests.

Materials and methods. Poorly studied methods of hardware formation of binary recurrence sequences by register-type generators with linear feedback are proposed. The mathematical basis of the generators is a composite characteristic polynomial consisting of primitive polynomials, one of which is raised to an integer power.

Results. It is shown that in homogeneous and inhomogeneous operating modes of the generator, a variety of formed sequences is observed. Correlation relationships of sequence elements are presented in statistical and functional forms. The problem of initializing the generator to form cycles of non-maximum length of a given order is solved.

Conclusions. The proposed analytical conditions and circuit design of sequence generators of non-maximum length with various probabilistic and correlation properties that expand the functionality of a simulation experiment.

Keywords: pseudo-random sequence generator, shift register, sequence variety, homogeneous and heterogeneous sequences, indicator sequences, correlation functions.

Введение

Псевдослучайные числовые последовательности широко применяются в различных областях науки и техники. Общего или универсального определения таких последовательностей не существует. Однако их этимология указывает, что «псевдослучайные» – это «как бы случайные, но остающиеся детерминированными». Главное качество псевдослучайных последовательностей (ПСП) – это проявление случайности в рамках заданных ограничений по условиям решаемой задачи.

Наибольшее распространение получили последовательности, реализующие схему независимых испытаний Бернулли. Основные их ограничения оговорены в трех постулатах Голомба, исследованию которых посвящена бóльшая часть работ по ПСП. Элементарным представителем такого типа процессов выступают равновероятностные двоичные некоррелированные последовательности. Типичными сферами их применения являются методы статистических испытаний и алгоритмы защиты информации. Аппаратные формирователи или генераторы таких псевдослучайных последовательностей (ГПСП) эффективно реализуются на регистрах сдвига с линейной обратной связью, описываемой примитивными характеристическими многочленами [1–6].

Развитие методов имитационного моделирования, реализация тестовых, контрольно-измерительных, учебно-тренажерных, вибро-стендовых и других испытаний связано с необходимостью формирования последовательностей с неравновероятностным распределением и определенными корреляционными свойствами. Алгоритмы и аппаратура для их получения существенно сложнее, чем для широко распространенного бернуллиевского случая.

В данной статье предлагаются малоизученные методы построения ГПСП, способные формировать набор последовательностей с разными веро-

ятностными и корреляционными свойствами на периодах немаксимальной длины. При этом сохраняется возможность максимального использования хорошо отработанных в инженерной практике регистровых структур и линейной комбинационной логики. Оригинальным и новым является задание неоднородных режимов работы и использование приводимых характеристических многочленов.

1. Построение генераторов по схеме Фибоначчи и анализ последовательностей

Основой построения устройства выбран *n*-разрядный регистр сдвига с внешними линейными обратными связями, что образует характерную конфигурацию генератора по схеме Фибоначчи [2–6]. Его работа организована на следующем рекуррентном правиле формирования последовательности *a* с дискретным временны́м аргументом *t*:

$$a(t) = C_1\, a(t-1) \oplus C_2\, a(t-2) \oplus \ldots \oplus C_n\, a(t-n) \oplus \alpha, \qquad (1)$$

где для двоичного случая $a, C_i, \alpha \in \{0, 1\}$, $i = \overline{1,\ n}$.

Указанное рекуррентное правило устанавливается составным характеристическим многочленом, допускающим запись в следующей приводимой форме:

$$\varphi(x) = \varphi_0^m(x)\, \varphi_1(x), \qquad (2)$$

где $\varphi_0(x)$ и $\varphi_1(x)$ – примитивные многочлены степени m_0 и m_1 соответственно, причем $m m_0 + m_1 = n$. Свойство неоднородности задается коэффициентом $\alpha = 1$, выполняющим роль оператора инверсии в цепи обратной связи.

В работе [7] доказано, что при $\alpha = 0$ нахождение периодической структуры (ПС) многочлена $\varphi_0^m(x)$ сводится к последовательному нахождению ПС всех меньших степеней:

$$\varphi_0(x), \varphi_0^2(x), \ldots, \varphi_0^{j-1}(x), \varphi_0^j(x) \ldots, \varphi_0^{m-1}(x), \varphi_0^m(x).$$

Множество периодов многочлена $\varphi_0^j(x)$ состоит из элементов периодической структуры многочлена $\varphi_0^{j-1}(x)$, μ_j и дополнительных периодов длины

$$L_0 2^{k_j}, \qquad (3)$$

где L_0 – длина минимального периода неприводимого многочлена $\varphi_0(x)$; k_j – наименьшее целое число, для которого $2^{k_j} \geq j$. Тогда для любого неприводимого многочлена $\varphi_0(x)$ количество дополнительных циклов определится формулой $\mu_j = 2^{m_0(j-1)}(2^{m_0} - 1) \Big/ L_0 2^{k_j}$. Так как по условиям выражения (2) многочлен $\varphi_0(x)$ примитивный, то длина его минимального периода совпадает с максимальной длиной или длиной М-последовательности $L_0 = (2^{m_0} - 1)$, что упрощает формулу для количества циклов до выражения

$$\mu_j = 2^{(j-1)m_0 - k_j}. \quad (4)$$

Принимая для $j=0$ самый младший элемент ПС в виде моноцикла 1(1), справедливо утверждать, что рост степени многочлена $\varphi_0(x)$ порождает дополнения циклами к элементам ПС всех младших степеней согласно (3) и (4).

К аналогичному формированию ПС многочлена $\varphi_0^m(x)$ приходим и при $\alpha = 1$ [8].

Основой многообразия являются ПСП, содержащие в сложноорганизованном виде прямые М- и инверсные $\overline{\text{М}}$-последовательности (МП и $\overline{\text{М}}$П), для которых запрещенными являются моноциклы 0 и 1 соответственно [6].

Рассмотрим простые примеры ГПСП и формируемые ими ПСП при различных значениях m_0, m_1 и m.

1.1. Случай $m_0 = m = 2$, $m_1 = 0$

В генераторах Фибоначчи на всех выходах формируются одинаковые последовательности с точностью до начальной фазы в пределах своего периода.

Генератор на основе многочлена

$$\varphi_0(x) = x^2 \oplus x \oplus 1 \quad (5)$$

формирует последовательности с ПС {1(1),1(3)}, в которой второй элемент определен при значениях $j=1$, $L_0 = 2^{m_0} - 1 = 3$, $2^{k_1} \geq 1$ и $k_1 = 0$, параметрами $\mu_1 = 1$ и $2^{k_1} L_0 = 3$ согласно (3) и (4).

Для квадрата трехчлена (5) получаем

$$\varphi_0^2(x) = x^4 \oplus x^2 \oplus 1. \quad (6)$$

Степень трехчлена в форме функции $\varphi_0(x)$ возрастает на 1, т.е. $j=2$, а ПС дополняется двумя циклами длиной 6, так как выражения (3) и (4) при $L_0 = 2^{m_0} - 1 = 3$ и $2^{k_2} \geq 2$ определяют $k_2 = 1$, $\mu_2 = 2^{m_0 - 1} = 2$ и $2^{k_2} L_0 = 6$. Таким образом, ПС многочлена (6) равна {1(1),1(3),2(6)}.

Схема генератора на основе многочлена (6) представлена на рис. 1.

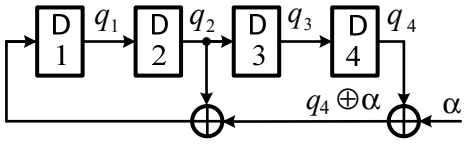

Рис. 1. Схема ГПСП на основе характеристического многочлена (6)

Моделирование при различных начальных состояниях (НС) регистра сдвига и $\alpha = 0$ позволяет получить следующие два дополнительных цикла:

$$0\,0\,0\,1\,0\,1 \quad (7)$$

и

$$0\,0\,1\,1\,1\,1, \tag{8}$$

соответствующих элементу 2(6) полной ПС.

Выявим связь этих последовательностей с МП, порождаемой исходным многочленом (5). Для этого получим по две последовательности таким образом, чтобы первая состояла из символов, стоящих на 1, 3, 5 позициях, вторая – на 2, 4, 6 позициях:

$$0\,0\,0\,1\,0\,1 \tag{7а}$$

$$0 - 0 - 0 -,$$

$$- 0 - 1 - 1,$$

$$0\,0\,1\,1\,1\,1 \tag{8а}$$

$$0 - 1 - 1 -,$$

$$- 0 - 1 - 1.$$

Из разложения видно, что последовательность (7) состоит из МП и константы 0, а последовательность (8) – из двух МП.

При $\alpha = 1$ формируются инверсные им последовательности (7а) и (8а), причем последовательность (7а) состоит из $\overline{\text{МП}}$ и константы 1, а (8а) – только из $\overline{\text{МП}}$.

Отметим, что ПСП содержат в сложно организованном виде не только МП и $\overline{\text{МП}}$, но и константы 0 и 1, которые, как увидим далее, вносят существенные особенности в формируемые последовательности.

1.2. Случай $m_0 = 2$, $m = 3$, $m_1 = 0$

Многочлен $\varphi_0^3(x) = (x^2 \oplus x \oplus 1)^3$ как куб квадратного трехчлена представим дополнительной степенью многочлена (6) из разд. 1.1:

$$(x^2 \oplus x \oplus 1)^3 = (x^2 \oplus x \oplus 1)^2 (x^2 \oplus x \oplus 1) = x^6 \oplus x^5 \oplus x^3 \oplus x \oplus 1, \tag{9}$$

которому соответствуют элементы ПС квадрата квадратного трехчлена {1(1), 1(3), 2(6)}. Тогда возникает дополнительный элемент 4(12), так как при $j = 3$ и $2^{k_3} \geq 3$ по (3) и (4) нетрудно определить $k_3 = 2$, $\mu_3 = 2^{2m_0 - 2} = 4$ и $2^{k_3} L_0 = 12$. Таким образом, полная ПС многочлена (9) выразится как {1(1),1(3),2(6),4(12)}.

Схема соответствующего генератора приведена на рис. 2.

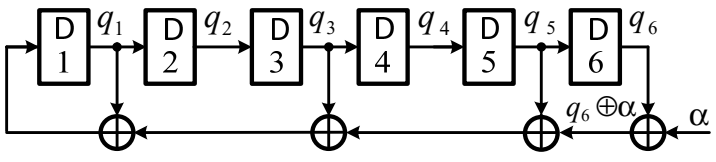

Рис. 2. Схема ГПСП на основе характеристического многочлена (9)

Рассмотрим связь четырех дополнительно сформированных при разных НС однородных ($\alpha = 0$) последовательностей с МП:

0 0 0 0 0 1 1 1 0 1 1 1 (10)

0 – – – 0 – – – 0 – – –,

– 0 – – – 1 – – – 1 – – ,

– – 0 – – – 1 – – – 1 – ,

– – – 0 – – – 1 – – – 1 ,

0 0 0 0 1 0 0 1 1 0 0 1 (11)

0 – – – 1 – – – 1 – – –,

– 0 – – – 0 – – – 0 – –,

– – 0 – – – 0 – – – 0 –,

– – – 0 – – – 1 – – – 1,

0 0 1 0 1 1 1 1 1 1 0 1 (12)

0 – – – 1 – – – 1 – – –,

– 0 – – – 1 – – – 1 – –,

– – 1 – – – 1 – – – 0 –,

– – – 0 – – – 1 – – – 1,

0 0 0 1 1 0 1 0 1 0 1 1 (13)

0 – – – 1 – – – 1 – – –,

– 0 – – – 0 – – – 0 – –.

– – 0 – – – 1 – – – 1 –,

– – – 1 – – – 0 – – – 1.

Как видим, формируются **равновероятностные** последовательности (10) и (13), **особенностью которых является содержание трех МП и одной константы 0**. Неравновероятностные последовательности (11) и (12) содержат две МП и две константы 0, и только МП соответственно.

При $\alpha = 1$ рассматриваемый генератор Фибоначчи формирует неоднородные последовательности, совпадающие в данном случае с инверсными (10)–(13), которые обозначим как (10а)–(13а). Отметим, что **равновероятностные** последовательности (10а) и (13а) **содержат три** $\overline{\text{МП}}$ **и одну константу 1**.

1.3. Случай $m_0 = 2$, $m = 4$, $m_1 = 0$

Заданный многочлен $\varphi_0^4(x)$, аналогично предыдущим случаям, запишем как дополнительную степень куба квадратного трехчлена вида

$$(x^2 \oplus x \oplus 1)^4 = (x^2 \oplus x \oplus 1)^3 (x^2 \oplus x \oplus 1) = x^8 \oplus x^4 \oplus 1. \quad (14)$$

Тогда дополнением к циклам $\varphi_0^3(x)$ с учетом $j=4$ и определением $2^{k_4} \geq 4$, $k_4=2$ по (3) и (4) будет $\mu_4 = 2^{3m_0-2} = 16$ и $2^{k_4} L_0 = 12$. С учетом этих дополнительных 16 последовательностей длиной 12 многочлен (14) приобретает полную ПС вида

$$\{1(1),1(3),2(6),4(12),16(12)\}=\{1(1),1(3),2(6),20(12)\}.$$

Соответствующая данному случаю схема ГПСП приведена на рис. 3.

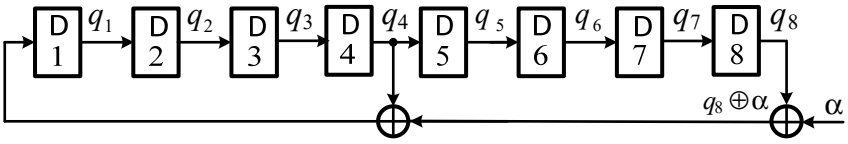

Рис. 3. Схема ГПСП на основе характеристического многочлена (14)

Формируемые неоднородным генератором последовательности для рассматриваемого случая вместе с предыдущими циклами представлены в табл. 1.

Таблица 1

Формируемые последовательности генератором при многочлене $\varphi_0^m(x) = (x^2 \oplus x \oplus 1)^m$ для $m = \overline{1,4}$ и $\alpha = 1$

Степень многочлена	ПС	Последовательности
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)000001101001, 3)000001001011, 4)000010000111, 5)000010100101, 6)**000100111101,** 7)**000101011011, 8)000100111101**, 9)**000110010111**, 10)**000110110101**, 11)**000111010011**, 12)**001001101011**, 13)001100111111, 14)001110110111, 15)010101011111, 16) 011101111111.

В табл. 1 последовательности при рассматриваемой степени многочлена, которые появились в дополнение к степени на единицу меньшей, пронумерованы со скобками. Равновероятностные циклы выделены жирным шрифтом.

По аналогии могут быть получены ПС и исследованы последовательности полноразмерного формата для практического применения за счет увеличения показателей степени m_0 и m_1.

2. ГПСП немаксимальной длины на основе приводимого характеристического многочлена, содержащего все ненулевые степени сомножителей

Рассмотрим генераторы, формирующие необходимое разнообразие ПСП на основе приводимого характеристического многочлена вида (2) с ненулевыми степенями, например, $\boldsymbol{m_0 = 2}$ и $\boldsymbol{m = m_1 = 3}$. Пусть многочлен $\varphi_0^3(x) = x^6 \oplus x^5 \oplus x^3 \oplus x \oplus 1$ имеет ПС $\{1(1),1(3),2(6),4(12)\}$, а $\varphi_1(x)$ степени $(n-6) \geq 2 - \left\{1(1),\ 1(2^{n-6}-1)\right\} = \{1(1),\ 1(7)\}$. Взаимодействие обеих ПС обеспечивают многочлену $\varphi(x)$ в целом следующую ПС:

$$\left\{1(1),1(3),2(6),4(12),1(2^{n-6}-1),1(3\cdot(2^{n-6}-1)),2(6\cdot(2^{n-6}-1)),4(12\cdot(2^{n-6}-1))\right\} =$$

$$= \{1(1),1(3),2(6),4(12),1(7),1(21)),2(42),4(84))\}. \quad (15)$$

Последовательности с ПС $\{1(1),1(3),2(6),4(12)\}$ образуют нерабочие (запрещенные) циклы и инициируют формирование рабочих ПСП с ПС:

$$\left\{1(2^{n-6}-1),1(3(2^{n-6}-1),2(6(2^{n-6}-1)),4(12(2^{n-6}-1))\right\}.$$

Рассмотрим случай, когда $\varphi_1(x) = x^3 \oplus x \oplus 1$. Тогда для ГПСП в форме (2):

$$\varphi(x) = (x^6 \oplus x^5 \oplus x^3 \oplus x \oplus 1)(x^3 \oplus x \oplus 1) = x^9 \oplus x^8 \oplus x^7 \oplus x^6 \oplus x^5 \oplus x^2 \oplus 1. \quad (16)$$

ПС рабочих последовательностей (РП) определим из (15) как

$$\{1(7),1(21),2(42),4(84)\} = \{1(7),1(3\cdot 7),2(6\cdot 7),4(12\cdot 7)\}.$$

Моделированием получены последовательности с периодами 21, 42 и 84 при $\alpha = 1$, которые приведены ниже (с периодами 42 и 84 по одной):

,010101100111011110000, (17)

,011110001101100100010000101010110111111001, (18)

,011001110011100011101110101101001001111110100000001010011010010111010100110000000111, (19)

Рассмотрим связь последовательности (17) с МП и $\bar{\text{М}}\text{П}$. Для этого определим три последовательности: первая из символов, стоящих на 1, 4, 7, … , вторая – на 2, 5, 8,…, третья – на 3, 6, 9, … и т.д. позициях:

,0 1 0 1 0 1 1 0 0 1 1 1 0 1 1 1 1 0 0 0 0,

,0 – – 1 – – 1 – – 1 – – 0 – – 1 – – 0 – –, МП

,– 1 – – 0 – – 0 – – 1 – – 1 – – 1 – – 0 –, МП

,– – 0 – – 1 – – 0 – – 1 – – 1 – – 0 – – 0, $\bar{\text{М}}\text{П}$

Последовательность (17) с периодом 21 организована и упорядочена из элементов двух МП и одной $\overline{\text{М}}\text{П}$, запрещенные последовательности в которых соответствуют циклу 1) 001 в табл. 1 при степени многочлена $m=1$. Для идентификации выходных последовательностей, не производя их потактное моделирование, целесообразно использовать запрещенные циклы в качестве индикаторных последовательностей (ИП) [3].

Для последовательности (18) с периодом 42 ИП являются 000011. Поэтому они содержат четыре МП и две $\overline{\text{М}}\,\text{П}$. Упорядоченность элементов МП и $\overline{\text{М}}\,\text{П}$ в формируемой равновероятностной последовательности с периодом 84 соответствует ИП 000100111101. Сложная упорядоченность МП и $\overline{\text{М}}\,\text{П}$ порождается многочленом $\varphi_1(x)=x^3\oplus x\oplus 1$ в форме (2).

3. Вероятностные и корреляционные свойства ПСП

Вероятностные свойства ПСП на выходах генераторов зависят от количества входящих в их состав МП и $\overline{\text{М}}\,\text{П}$, определяемого ЗС, которые порождаются многочленом $\varphi_1(x)$ степени m_1. Так, при ЗС 00…0 вероятность определяется МП, при 11…1 – вероятностью $\overline{\text{М}}\,\text{П}$. Если ЗС содержит равное количество 0 и 1, то выходные последовательности равновероятны.

Корреляционные свойства формируемых последовательностей также отличаются разнообразием. Периодические автокорреляционные функции (ПАКФ) $\mathbf{r}(\tau)$ последовательностей в общем случае вычисляются по следующей формуле [3]:

$$\mathbf{r}(\tau)=\frac{n_{\text{ц}}\,n_{11}(\tau)-n_1^2}{n_1(n_{\text{ц}}-n_1)}, \tag{20}$$

где τ – временной сдвиг как аргумент функции; n_1 и $n_{11}(\tau)$ – количество единиц и пар единиц на периоде $n_{\text{ц}}$.

Для равновероятностных последовательностей ПАКФ $\mathbf{r}(\tau)$ имеет вид [3]:

$$\mathbf{r}(\tau)=\frac{n_{\text{с}}(\tau)-n_{\text{н}}(\tau)}{n_{\text{ц}}}, \tag{21}$$

где $n_{\text{с}}(\tau)$ – количество совпадающих, а $n_{\text{н}}(\tau)$ – несовпадающих символов на периоде $n_{\text{ц}}$ при сдвиге τ.

В табл. 2 приведены малоразмерные примеры ПСП с максимальным периодом 12 из табл. 1 со значениями ПАКФ $\mathbf{r}(\tau)$, представленных на половине периода по оси аргумента τ. Вторая половина функций повторяет первую половину симметрично середине периода при $\tau=6$, соответствующему серому столбцу табл. 2. Строки таблицы обозначены комбинацией минимальной степени m многочлена $\varphi_0(x)$ и номером последовательности в табл. 1.

В табл. 3 приведены ПАКФ неравновероятностных последовательностей (17), (18) и равновероятностной (19), которые вычислялись по формулам (20) и (21) соответственно.

Таблица 2

ПАКФ $\mathbf{r}(\tau)$

m.№	Последовательности	Аргументы автокорреляционных функций						Вероят-ности
		τ = 1	τ = 2	τ = 3	τ = 4	τ = 5	τ = 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
4.5	000010100101	–0,5	0,25	–0,125	–0,5	0,625	–0,5	0,33
4.8	**000100111101**	0	0	0	0	–0,33	–0,33	**0,5**
4.9	**000110010111**	0	–0,33	–0,33	0	0	0,33	**0,5**
4.11	**000111010011**	–0,33	–0,33	0,33	0	–0,33	0,33	**0,5**
4.14	001110110111	–0,125	–0,5	–0,125	0,25	0,25	–0,5	0,67
4.16	011101111111	–0,2	–0,2	–0,2	0,4	–0,2	–0,2	0,83

Таблица 3

ПАКФ $\mathbf{r}(\tau)$ последовательностей (17) на полном периоде,
(18) – на половине периода и (19) – на четверти периода

τ	(17)	(16)	(17)
1	0,045	–0,050	0
2	0,045	0,045	0
3	–0,145	0,045	0
4	0,045	0,045	0
5	0,045	–0,050	0,048
6	–0,145	–0,145	0,048
7	–0,336	0,332	–0,333
8	0,045	0,045	0
9	–0,145	0,045	0
10	0,045	0,045	0
11	0,045	–0,050	0
12	–0,145	–0,145	–0,143
13	0,045	–0,050	0
14	–0,336	0,332	0
15	–0,145	0,045	0
16	0,045	0,045	0
17	0,045	–0,050	0,048
18	–0,145	–0,145	0,048
19	0,045	–0,050	0,048
20	0,045	0,045	0
21	1	0,332	0

Заключение

Исследованы однородные и неоднородные генераторы на регистре сдвига с внешними линейными обратными связями (генераторы Фибоначчи), формирующие псевдослучайные последовательности немаксимальной длины

на основе характеристического многочлена вида $\varphi(x) = \varphi_0^m(x)\,\varphi_1(x)$ степени n, где $\varphi_0(x)$ и $\varphi_1(x)$ – примитивные многочлены степени m_0 и m_1 соответственно, причем $m_0\, m + m_1 = n$. Определены периодические структуры многочленов $\varphi_0^m(x)$ и $\varphi(x)$.

Впервые показано, что ПСП на основе многочлена $\varphi_0^m(x)$ содержат в сложноорганизованном виде не только МП и $\overline{\text{МП}}$, но и константы 0 и 1, которые позволяют порождать последовательности как равновероятностного типа, так и не равновероятностного. На примерах малоразрядных генераторов представлены вероятностные и автокорреляционные свойства формируемых ПСП.

Рассмотрены генераторы Фибоначчи на основе приводимого характеристического многочлена $\varphi(x)$, содержащего все ненулевые степени сомножителей. Определены нерабочие (запрещенные) циклы, которые инициируют формирование рабочих ПСП. Эти циклы можно использовать в качестве индикаторных последовательностей для идентификации рабочих последовательностей. Разнообразие корреляционных и вероятностных свойств способствуют использованию рассмотренных последовательностей в имитационном моделировании.

Библиографический список

1. **Иванов, М. А.** Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – Москва : КУДИЦ-ОБРАЗ, 2003. – 240 с.
2. **Кузнецов, В. М.** Генераторы равновероятностных псевдослучайных последовательностей на регистрах сдвига / В. М. Кузнецов, В. А. Песошин // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2012. – № 1 (21). – С. 21–28.
3. **Кузнецов, В. М.** Генераторы случайных и псевдослучайных последовательностей на цифровых элементах задержки / В. М. Кузнецов, В. А. Песошин. – Казань : Изд-во Казан. гос. техн. ун-та, 2013. – 336 с.
4. **Песошин, В. А.** Генераторы равновероятностных псевдослучайных последовательностей немаксимальной длины на основе регистра сдвига / В. А. Песошин, В. М. Кузнецов, А. С. Кузнецова, А. Р. Шамеева // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2019. – № 1 (49). – С. 5–19.
5. **Pesoshin, V. A.** Generators of the equiprobable pseudorandom nonmaximal-length sequences based on linear-feedback shift registers / V. A. Pesoshin, V. M. Kuznetsov, D. V. Shirshova // Automation and Remote control. 2016. – Vol. 77, № 9. – P. 1622–1631.
6. **Pesoshin, V. A.** Pseudo-random sequences with nonmaximal length based on the shift register and reducible polynomial // V. A. Pesoshin, V. M. Kuznetsov, A. K. Rakhmatullin // MMPAM-2019. Journal of Physics: Conference Series. – Vol. 1352, № 1.
7. **Элспас, Б.** Теория автономных линейных последовательных сетей / Б. Элспас // Кибернетический сборник. – Вып. 7. – Москва : ИЛ, 1963. – С. 90–128.
8. **Кугураков, В. С.** Множество длин циклов взаимнооднозначных аффинных отображений пространства V^n (GF(p)) на себя / В. С. Кугураков, О. Б. Соколов // Ученые записки Казанского государственного университета. – 1969. – Т. 129, № 4. – С. 74–79.

References

1. Ivanov M. A., Chugunkov I. V. *Teoriya, primenenie i otsenka kachestva generatorov psevdosluchaynykh posledovatel'nostey* [Theory, application and quality assessment of pseudo-random sequence generators]. Moscow: KUDITs-OBRAZ, 2003, 240 p. [In Russian]
2. Kuznetsov V. M., Pesoshin V. A. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki* [University proceedings. Volga region. Engineering sciences]. 2012, no. 1 (21), pp. 21–28. [In Russian]
3. Kuznetsov V. M., Pesoshin V. A. *Generatory sluchaynykh i psevdosluchaynykh posledovatel'nostey na tsifrovykh elementakh zaderzhki* [Random and pseudo-random sequence generators on digital delay elements]. Kazan: Izd-vo Kazan. gos. tekhn. un-ta, 2013, 336 p. [In Russian]
4. Pesoshin V. A., Kuznetsov V. M., Kuznetsova A. S., Shameeva A. R. *Izvestiya vysshikh uchebnykh zavedeniy. Povolzhskiy region. Tekhnicheskie nauki* [University proceedings. Volga region. Engineering sciences]. 2019, no. 1 (49), pp. 5–19. [In Russian]
5. Pesoshin V. A., Kuznetsov V. M., Shirshova D. V. *Automation and Remote control*. 2016, vol. 77, no. 9, pp. 1622–1631.
6. Pesoshin V. A., Kuznetsov V. M., Rakhmatullin A. K. *MMPAM-2019. Journal of Physics: Conference Series*. Vol. 1352, no. 1.
7. Elspas B. *Kiberneticheskiy sbornik* [Cybernetic collection]. Issue 7. Moscow: IL, 1963, pp. 90–128. [In Russian]
8. Kugurakov V. S., Sokolov O. B. *Uchenye zapiski Kazanskogo gosudarstvennogo universiteta* [Proceedings of Kazan State University]. 1969, vol. 129, no. 4, pp. 74–79. [In Russian]

Песошин Валерий Андреевич
доктор технических наук, профессор, кафедра компьютерных систем, Казанский национальный исследовательский технический университет имени А. Н. Туполева–КАИ (Россия, г. Казань, ул. К. Маркса, 10)

E-mail: pesoshin-kai@mail.ru

Pesoshin Valeriy Andreevich
Doctor of engineering sciences, professor, sub-department of computer systems, Kazan National Research Technical University named after A. N. Tupolev – KAI (10 K. Marksa street, Kazan, Russia)

Кузнецов Валерий Михайлович
доктор технических наук, профессор, кафедра компьютерных систем, Казанский национальный исследовательский технический университет имени А. Н. Туполева–КАИ, (Россия, г. Казань, ул. К. Маркса, 10)

E-mail: kuznet_evm@mail.ru

Kuznetsov Valeriy Mikhaylovich
Doctor of engineering sciences, professor, sub-department of computer systems, Kazan National Research Technical University named after A. N. Tupolev – KAI (10 K. Marksa street, Kazan, Russia)

Кузнецова Александра Сергеевна
студент, Казанский национальный исследовательский технический университет имени А. Н. Туполева–КАИ, (Россия, г. Казань, ул. К. Маркса, 10)

E-mail: sasha_kzncv@mail.ru

Kuznetsova Aleksandra Sergeevna
Student, Kazan National Research Technical University named after A. N. Tupolev – KAI (10 K. Marksa street, Kazan, Russia)

Образец цитирования:

Песошин, В. А. Генераторы псевдослучайных последовательностей немаксимальной длины на регистрах сдвига с линейной обратной связью на основе примитивного многочлена в степени / В. А. Песошин, В. М. Кузнецов, А. С. Кузнецова // Известия высших учебных заведений. Поволжский регион. Технические науки. – 2019. – № 4 (52). – С. 14–26. – DOI 10.21685/2072-3059-2019-4-2.