ИНФОРМАТИКА, ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА И УПРАВЛЕНИЕ

УДК 681.325: 621.391.3:518.5:519.95
DOI 10.21685/2072-3059-2019-1-1

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

ГЕНЕРАТОРЫ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ НЕМАКСИМАЛЬНОЙ ДЛИНЫ НА РЕГИСТРАХ СДВИГА[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 многоканальных генераторов двоичных последовательностей как псевдослучайных в условиях формирования циклов немаксимальной длины.

Материалы и методы. Предлагаются малоизученные методы аппаратного формирования двоичных рекуррентных последовательностей генераторами регистрового типа с линейной обратной связью и с внутренними сумматорами по модулю два. Математической основой генераторов выбран составной характеристический многочлен, одним из множителей которого является целочисленная степень двучлена первой степени.

Результаты. Показано, что в случае неоднородного режима работы генератора наблюдается многообразие одновременно формируемых последовательностей. Представлены в статистической и функциональной формах корреляционные связи элементов последовательностей как внутри, так и между ними. Решены задачи идентификации последовательностей по разрядным выходам и инициализации генераторов на заданный набор циклов немаксимальной длины данного порядка.

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

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

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

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

THE GENERATORS OF PSEUDORANDOM SEQUENCES OF A NAMAXIMUM LENGTH ON SHIFT REGISTERS

Abstract.

Background. Modern methods of organization of machine experiments in the simulation models form are based on the use of numerical sequences of probabilistic and statistical nature, which are adequate to real processes and phenomena. The purpose of the article is to demonstrate the new capabilities of multichannel pseudo – random binary sequence generators in the conditions of non-maximum length cycles formation.

Materials and methods. Insufficiently studied methods of binary recurrent sequences hardware formation by register-type generators with linear feedback and with internal adders by modulo two are proposed. A composite characteristic polynomial is chosen as the mathematical basis of the generators, one of the multipliers of which is the integer power of the first-degree two-term.

Results. It is shown that in the case of inhomogeneous mode of operation of the generator the diversity of the simultaneously generated sequences is observed. Correlation connections of elements of sequences both inside and between them in statistical and functional forms are presented. The problem of the sequence identification at the bit outputs, and the problem of initialization of the generators to a specified set of cycles of the non-maximum length of definite order are solved.

Conclusions. The proposed analytical conditions and schematic organization of sequence generators of non-maximum length allow us to form sets with a variety of probabilistic and correlation properties that extend the functionality of the simulation experiment.

Keywords: pseudorandom sequence generator, shift register, diversity of sequences, heterogeneous sequences, indicator sequences, correlation function.

Введение

Для решения задач методом статистического моделирования необходимо вырабатывать большие объемы случайных чисел с разнообразными свойствами [1]. При аппаратной реализации широкое распространение получили генераторы псевдослучайных последовательностей (ГПСП) Фибоначчи (на основе *n*-разрядного регистра сдвига с линейными обратными связями) и Галуа (с внутренними сумматорами по модулю два) [2–5].

В работах [6–10] рассмотрены генераторы, формирующие неоднородные последовательности немаксимальной длины. В качестве математической основы использован характеристический многочлен степени *n* вида

$$\varphi(x) = \varphi_0(x)\varphi_1(x), \quad (1)$$

где

$$\varphi_0(x) = (x \oplus 1)^{m_0}, \quad (2)$$

$m_0 = 2^k$ (k – целое положительное число), многочлен $\varphi_1(x)$ степени m_1 примитивен ($n = m_0 + m_1$). Неоднородность задается коэффициентом $\alpha = 1$.

Для многочлена (2) при $\alpha = 1$ периодическая структура (ПС) [11] определится в форме множества $\{\mu_{m_0}(L_{m_0})\}$, где длина периода

$L_{m_0} = 2^{]\log_2(m_0+1)[}$, количество периодов $\mu_{m_0} = 2^{m_0-]\log_2(m_0+1)[}$, $]z[$ означает ближайшее большее целое число или равное z, если z целое. В табл. 1 приведены ПС многочлена $(x \oplus 1)^{m_0}$ для $m_0 = \overline{1,16}$.

Таблица 1

ПС многочлена (2) для $m_0 = \overline{1,16}$

m_0	ПС	m_0	ПС
1	{1(2)}	**9**	**{32(16)}**
2	{1(4)}	**10**	**{64(16)}**
3	**{2(4)}**	**11**	**{128(16)}**
4	{2(8)}	**12**	**{256(16)}**
5	**{4(8)}**	**13**	**{512(16)}**
6	**{8(8)}**	**14**	**{1024(16)}**
7	**{16(8)}**	**15**	**{2048(16)}**
8	{16(16)}	16	{2048(32)}

Жирным шрифтом выделены строки таблицы с числовыми данными, впервые рассматриваемые в данной работе.

Вначале представим простейшие малоразмерные случаи.

1. Анализ последовательностей на выходах регистра при $m_0 \neq 2^k$

Случай $m_0 = 3$. Двучлен вида $\varphi_0(x) = (x \oplus 1)^3 = x^3 \oplus x^2 \oplus x \oplus 1$ с ПС {2(4)} порождает в неоднородном режиме две последовательности: ,0001, и ,0111,. В качестве многочлена $\varphi_1(x)$ степени $m_1 = n - 3 \geq 2$ выбирается примитивный полином с ПС $\{1(1), 1(2^{n-3} - 1)\}$. Тогда аналогичная структура ГПСП и его многочлена $\varphi(x)$ в целом определяется как формальное произведение членов [11]:

$$\{2(4), 2(2^{n-1} - 4)\} = \{2(4), 2((2^{n-1} - 1) - 3)\}, \quad (3)$$

т.е. формируются два нерабочих цикла с периодом 4 и две рабочие последовательности n-го порядка с периодом $(2^{n-1} - 1) - 3$.

Пример 1. Пусть

$$\varphi_1(x) = x^3 \oplus x \oplus 1, \quad (4)$$

тогда

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

Многочлен (4) порождает М-последовательность (МП) с периодом 7 вида

$$,0\ 0\ 1\ 0\ 1\ 1\ 1,. \quad (6)$$

ПС $\{2(4),\ 2(28)\} = \{2(4), 2(31-3)\}$ многочлена (5) соответствует общей форме (3), в которой второй элемент свидетельствует о двух рабочих последовательностях с периодами $(2^{n-1} - 1) - 3 = 28$.

По многочлену (5) можно построить генераторы Фибоначчи (рис. 1) и Галуа (рис. 2).

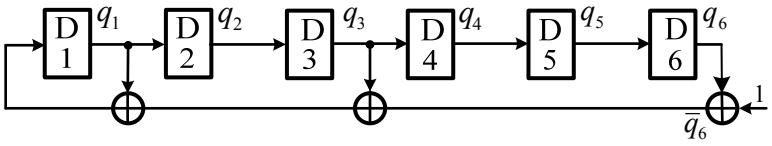

Рис. 1. ГПСП по схеме Фибоначчи на основе многочлена (5)

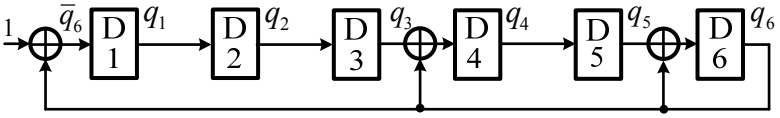

Рис. 2. ГПСП по схеме Галуа на основе многочлена (5)

Структуры схем ГПСП полностью описываются квадратными матрицами $\mathbf{C}_\alpha$ $(n+1)$-го порядка соответственно для Фибоначчи и Галуа:

$$\begin{Vmatrix} 1 & 0 & 1 & 0 & 0 & 1 & \alpha \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{Vmatrix} \text{ и } \begin{Vmatrix} 0 & 0 & 0 & 0 & 0 & 1 & \alpha \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{Vmatrix}.$$

Верхняя строка первой матрицы и предпоследний столбец второй матрицы определяют вид обратной связи соответствующего генератора. Наличие единицы в последнем столбце на главной диагонали и задание константы $\alpha \in \{0,1\}$ позволяют реализовать свойства однородности-неоднородности формируемой линейной рекуррентной последовательности. Остальные единичные элементы матриц, находящиеся на диагонали ниже главной, задают связи D-триггеров между собой, определяющие операцию сдвига в регистре.

Порожденные многочленом (5) две рабочие последовательности

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

$$...,1\,1\,1\,1\,0\,0\,1\,1\,1\,0\,0\,0\,0\,0\,0\,1\,0\,1\,1\,0\,0\,1\,0\,0\,1\,0\,1\,0,\ldots$$

взаимоинверсны, но не инверсно-сегментные. Однако их период совпадает с (М – 3)-последовательностью (кратко обозначим $(\mathrm{M}-3)\,\mathrm{П}$). Поэтому назовем их (М – 3)-подобными последовательностями и обозначим как (М – 3)ПП.

Выявим связь полученных последовательностей на основе (6) с МП, определяемой многочленом (4). Для этого выделим, например, из (7) по четыре последовательности таким образом, чтобы первая состояла из символов, стоящих на 1, 5, 9, … позициях, вторая – на 2, 6, 10, …, третья – на 3, 7, 11, … и четвертая – на 4, 8, 12, … позициях:

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

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

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

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

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

Как видим, последовательность (7) содержит в сложно организованном виде три МП (6) и одну инверсную $\overline{M}$ П, определяемые многочленом (4). Об этом же свидетельствует нерабочий цикл 0 0 0 1. Аналогичные выделения МП и $\overline{M}$ П из инверсной последовательности (7) позволяют ставить в соответствие запрещенный цикл 1 1 1 0.

Генератор по схеме Галуа на выходах своего регистра позволяет получить существенно отличающиеся последовательности. Так, на выходах триггеров $q_1 - q_3$ также формируются новые последовательности (7), на выходе q_6 – инверсная им последовательность. Однако за счет внутреннего суммирования по модулю два на выходах q_4 и q_5 формируются две ранее известные инверсно-сегментные последовательности (ИСП), совпадающие друг с другом с точностью циклического сдвига на величину полпериода вида

…,0 0 0 0 1 1 1 0 1 0 1 1 0 1 1 1 1 1 0 0 0 1 0 1 0 0 1 0,…

Таким образом, на выходах одного ГПСП получаются одновременно и (М – 3)П и (М – 3)ПП, существенно отличающиеся как структурой, так и корреляционными связями. Отмеченное многообразие формируемых последовательностей делает актуальной задачу идентификации.

2. Идентификация последовательностей на выходах регистра

Рассмотрим метод идентификации последовательностей на выходах генератора Галуа без моделирования на полных периодах. Для этого используется уникальность коротких нерабочих циклов в качестве индикаторных последовательностей (ИП).

В неоднородных генераторах Галуа с n-разрядным регистром сдвига справедливо соотношение $q_1(t+1) = \overline{q}_n(t)$. Тогда, зная сигналы на выходах триггера q_1 (или q_n) и алгоритм работы ГПСП, нетрудно последовательно найти состояния триггеров q_2, затем q_3 и т.д. до q_{n-1}, по которым выявляются нерабочие циклы, образующие ИП.

Например, для ГПСП по схеме Галуа (рис. 2) на основе многочлена $\varphi(x) = x^6 \oplus x^5 \oplus x^3 \oplus 1$ с выходов триггеров $q_1 - q_3$ (табл. 2), моделированием воспроизводятся нерабочие циклы 0 0 0 1 (с точностью до циклического сдвига), индицирующие рабочие последовательности вида (М – 3)ПП (7).

На выходах q_4, q_5 индикаторными являются последовательности 0 0 1 1. Соответствующие им рабочие ИСП содержат две МП и две $\overline{\text{М}}$П, которые определяют $(\text{М}-3)\,\text{П}$. На выходе q_6 ИП 0 1 1 1, следовательно, формируется последовательность, инверсная (7) вида $\overline{(\text{М}-3)}\,\text{ПП}$.

Предложенным образом решается задача анализа генератора как готового технического средства. Инженерная разработка нового ГПСП требует

постановки задачи синтеза, основой решения которой является инициализация регистровой части устройства в классе конечных автоматов путем задания необходимых начальных состояний.

Таблица 2

Нерабочие состояния регистра

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

3. Инициализация рабочих режимов генератора

Для формирования конкретных рабочих последовательностей требуется определить соответствующее начальное состояние регистра. Рассмотрим метод инициализации линейных генераторов Галуа на основе доопределения не полностью известного начального состояния по заданным ИП и МП. Он позволяет сократить количество шагов имитации работы регистровой структуры до n. Сущность разработанной процедуры метода поясним на малоразмерном примере.

Так, например, для формирования $(\mathrm{M}-3)$ ПП на основе МП вида (6) задаем ИП 0 0 0 1, тогда

$$\begin{array}{l} ,0\,0\,1\,0\,1\,1\,1,0\,0\,1\,0\,1\,1\,1, \\ \oplus \\ \underline{,0\,0\,0\,1,0\,0\,0\,1,.} \\ 0\,1\,1\,0\,0\,0 \end{array} \qquad (8)$$

Используя полученный фрагмент как последовательность состояний разряда регистра q_1, из соотношения $q_1(t+1)=\overline{q}_6(t)$ обратной по времени экстраполяцией находим q_6. При известном алгоритме работы ГПСП становится возможным доопределение состояний регистра, представленного в табл. 3. Полученная комбинация полностью определенных состояний в строке $t+5$ табл. 3 является достаточной для инициализации генератора Галуа на формирование $(\mathrm{M}-3)$ ПП с выхода q_1.

Таблица 3

Определение начального состояния регистра для ИП 0 0 0 1

$t+$	q_1 q_2 q_3 q_4 q_5 q_6
t	* * * * * 1
$t+1$	**0** * * * * 0
$t+2$	**1** 0 * * * 0
$t+3$	**1** 1 0 * * 1
$t+4$	**0** 1 1 1 * 1 **0** 0 1 0 1 **1**
$t+5$	0 – – – – – инверсия – – – – – ↑
$t+6$	

4. Многообразие последовательностей, формируемых ГПСП на основе многочлена $(x \oplus 1)^{m_0}$

Аналогично рассмотренному случаю $m_0 = 3$ можно исследовать псевдослучайные последовательности немаксимальной длины, порождаемые многочленом $\varphi_0(x)$ степени $m_0 > 3$, акцентировав внимание на степени $m_0 \neq 2^k$. В табл. 4 представлены последовательности, формируемые генератором Фибоначчи на основе многочлена $\varphi_0(x) = (x \oplus 1)^{m_0}$ при $\alpha = 1$. Многочлены $\varphi_0(x)$ записаны в восьмеричном представлении.

(М – 3)

Таблица 4

Последовательности, формируемые генератором Фибоначчи на основе многочлена $(x \oplus 1)^{m_0}$ для $m_0 = \overline{1, 7}$

m_0	1	2	**3**	4	**5**	**6**	**7**
$\varphi_0(x)$	3	5	17	21	63	125	377
ПС	{1(2)}	{1(4)}	{2(4)}	{2(8)}	{4(8)}	{8(8)}	{16(8)}
Генераторы Фибоначчи	(М – 1): **01**	(М – 3): **0011**	(М – 3) П: 0001, 0111	(М – 7) П: **00001111**, **01011010**	(М – 7) П: 00000101, **00011011, 00100111**, 01011111	(М – 7) П: 00000011, 00001001, **00010111, 00011101, 00101011, 00110101,** 00111111, 01101111	(М – 7) П: 00000001, 00000111, 00001011, 00001101, 00010011, 00010101, 00011001, 00011111, 00100101, 00101111, 00110111, 00111011, 00111101, 01010111, 01011011, 01111111

Необходимо отметить, что при $m_0 = \overline{5, 7}$ для ПС {4(8)}–{16(8)} все (М – 7) ПП различные, причем половина из них инверсные. Жирным шрифтом выделены равновероятностные последовательности, из которых **01, 0011, 00010111** и **00011101** являются последовательностями де Брейна.

В работах [4, 5] установлено, что при данных условиях генератор Галуа способен формировать одновременно разные последовательности:

– при $\varphi_0(x) = x \oplus 1$: М-, $\overline{\text{М}}$ - и (М – 1) -,

– при $\varphi_0(x) = (x \oplus 1)^2$: М-, $\overline{\text{М}}$ -, (М – 1) - и (М – 3) -последовательности.

Однако есть предположение, что чем больше степень многочлена и плотнее его структура (больше членов), тем шире многообразие формируемых последовательностей одним генератором.

Предлагается простой способ нахождения возможных индикаторных циклов. Суть способа заключается в том, что проверяется возможность появления каждого индикаторного цикла в отдельности и возможность выхода из него.

Пример 2. Рассмотрим *n*-разрядный регистр, в котором между *i*-м и $(i+1)$-м триггерами с состояниями q_i и q_{i+1} включен сумматор по модулю два, $\varphi_0(x)=(x\oplus 1)^3$, на выходе $q_1(t)$ формируется ИП вида 0 0 0 1 и $q_1(t+1)=\overline{q}_n(t)$. В табл. 5–12 показаны ИП на выходах триггеров.

Таблицы 5–12

ИП на выходах триггеров

$q_1 \dots q_i\ q_{i+1} \dots q_n$	$q_1 \dots q_i\ q_{i+1} \dots q_n$	$q_1 \dots q_i\ q_{i+1} \dots q_n$	$q_1 \dots q_i\ q_{i+1} \dots q_n$
0 … 0 1 … 1	0 … 1 0 … 1	0 … 1 0 … 1	0 … 0 1 … 1
0 … 0 1 … 1	0 … 1 0 … 1	0 … 1 0 … 1	0 … 0 1 … 1
0 … 0 1 … 0	0 … 0 0 … 0	0 … 1 0 … 0	0 … 1 1 … 0
1 … 0 0 … 1	1 … 1 0 … 1	1 … 1 1 … 1	1 … 0 1 … 1
0 … 0 1 … 1	**0 … 0 0 … 1**	**0 … 1 0 … 1**	**0 … 0 1 … 1**

$q_1 \dots q_i\ q_{i+1} \dots q_n$	$q_1 \dots q_i\ q_{i+1} \dots q_n$	$q_1 \dots q_i\ q_{i+1} \dots q_n$	$q_1 \dots q_i\ q_{i+1} \dots q_n$
0 … 0 0 … 1	0 … 0 0 … 1	0 … 0 0 … 1	0 … 1 0 … 1
0 … 1 1 … 1	0 … 1 0 … 1	0 … 0 1 … 1	0 … 0 0 … 1
0 … 1 0 … 0	0 … 0 0 … 0	0 … 1 1 … 0	0 … 1 1 … 0
1 … 1 1 … 1	1 … 1 0 … 1	1 … 1 1 … 1	1 … 1 1 … 1
0 … 0 0 … 1	**0 … 0 0 … 1**	**0 … 0 0 … 1**	**0 … 0 0 … 1**

Из таблиц 5–12 следует, что генератор в рабочем режиме формирует на выходах q_1 и q_n $(\text{M}-3)$ ПП, согласно ИП 0000, 1111, 0101 и 0011 на выходах q_i или q_{i+1} – M-, $\overline{\text{M}}$-, $(\text{M}-1)$- и $(\text{M}-3)$-последовательности соответственно. Подобным образом могут определяться ИП и при других значениях m_0.

5. Условия взаимно корреляционной независимости

Для случая одновременного формирования множества различных периодических последовательностей как псевдослучайных предлагается теоретико-числовой метод установления некоррелированных пар из этого множества без применения расчетных процедур корреляционного анализа.

Обозначим для двух последовательностей двоичных символов *x* и *y* отсутствие взаимно корреляционной зависимости условием [4]:

$$\mathbf{k}_{xy}(\tau)=p_{xy}(\tau)-p_x p_y=0,$$

выразим вероятности появления единиц в $\langle x(t)\rangle$, $\langle y(t)\rangle$ и совпадения двух единиц в $\langle x(t)\rangle$ и $\langle y(t+\tau)\rangle$ через отношения целочисленных переменных

$$p_x=n_x/T_x,\ p_y=n_y/T_y \text{ и } p_{xy}(\tau)=n_{xy}(\tau)/T_{xy},$$

где n_x, n_y – число единиц в $\langle x(t)\rangle$, $\langle y(t)\rangle$ на периоде T_x, T_y соответственно; $n_{xy}(\tau)$ – количество совпадений единиц в $\langle x(t)\rangle$ и $\langle y(t+\tau)\rangle$ на общем периоде $T_{xy}=\mathbf{k}\left(T_x, T_y\right)$, определенном как наименьшее общее кратное. Тогда равенство

$$n_{xy}(\tau)=\frac{n_x\, n_y}{\mathbf{d}\left(T_x, T_y\right)}, \tag{9}$$

справедливость которого соблюдается только для целых чисел, является необходимым и достаточным условием отсутствия взаимной корреляционной связи между двоичными последовательностями при области определения по аргументу τ размером, не превышающим наибольший общий делитель циклов $\mathbf{d}\left(T_x, T_y\right)$ [7].

Частным случаем (9) является условие отсутствия взаимной корреляции для любых периодических последовательностей с взаимно простыми минимальными периодами T_x и T_y. Действительно, выражая взаимную простоту чисел через наибольший общий делитель тождеством $\mathbf{d}\left(T_x, T_y\right)=1$, обеспечиваем в (9) очевидную целочисленность левой части через произведение целых чисел в правой, т.е. $n_{xy}(\tau)\equiv n_x\, n_y$.

Применительно к неоднородным ГПСП по схеме Галуа, одновременно формирующим различные последовательности, среди которых значительная часть ИСП, сформулирован еще один частный случай теоретико-числового условия некоррелированности (9). Оно получено в виде дробно-рационального соотношения

$$\frac{2k-1}{2l}=\frac{T_v}{T_{w\bar{w}}} \tag{10}$$

целочисленных периодов любых рекуррентных последовательностей T_v и только инверсно-сегментных $T_{w\bar{w}}$, где k и l – натуральные числа. Выявлена исключительная особенность генератора Галуа – одновременно формировать взаимно некоррелированные пары ПСП, когда по крайней мере одна из них является ИСП и выполняется условие (10).

6. Периодические автокорреляционные функции

Внутренние связи элементов рассмотренных двоичных последовательностей во временной области характеризуются периодическими автокорреляционными функциями (ПАКФ). Знания структурных особенностей этих двоичных последовательностей на минимальном периоде T позволяют вычислить ПАКФ в нормированном виде по следующей формуле [4]:

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

где τ – временной сдвиг как аргумент функции; n_1 и $n_{11}(\tau)$ – количество единиц и пар единиц, разнесенных по времени на τ, в пределах периода T.

Для равновероятностных последовательностей на периоде характерно равенство $n_1 = T - n_1$, упрощающее формулу (11) до выражения

$$\mathbf{r}(\tau) = \frac{n_{\text{с}}(\tau) - n_{\text{н}}(\tau)}{T}, \qquad (12)$$

где $n_{\text{с}}(\tau)$ и $n_{\text{н}}(\tau)$ – количество совпадающих и несовпадающих символов 0 и 1 на периоде n при сдвиге τ.

Учитывая симметрию графика ПАКФ не только относительно осей ординат в нулевых, но и в половинных от периода T точках аргумента τ по модулю n, достаточно производить вычисления только на половине периода.

Пример 3. Пусть $m_0 = 5$, т.е. $\varphi_0(x) = (x \oplus 1)^5$. Как видно из табл. 4, этот многочлен порождает две пары (М – 7) ПП:

$$00000101 \quad (11111010), \qquad (13)$$

$$\mathbf{00011011} \quad \mathbf{(11100100)}. \qquad (14)$$

Нормированные ПАКФ этих последовательностей в пределах τ от 0 до $0{,}5T = 4$ представлены в табл. 13 и 14.

Таблица 13

ПАКФ последовательностей 00000101 (11111010)

τ	1	2	3	4
$\mathbf{r}_0(\tau)$	– 1/3	+ 1/3	– 1/3	– 1/3

Таблица 14

ПАКФ последовательностей **00011011 (11100100)**

τ	1	2	3	4
$\mathbf{r}_0(\tau)$	0	–0,5	0	0

Для двоичной последовательности, полученной суммой по модулю два от двух независимых исходных последовательностей, известно аналитическое соотношение для автокорреляционных функций вида [5]:

$$\mathbf{r}(\tau) = \frac{\delta_0^2\left(1-\delta_1^2\right)\mathbf{r}_1(\tau) + \delta_1^2\left(1-\delta_0^2\right)\mathbf{r}_0(\tau) + \left(1-\delta_0^2\right)\left(1-\delta_1^2\right)\mathbf{r}_0(\tau)\,\mathbf{r}_1(\tau)}{1-\delta_0^2\,\delta_1^2}, \qquad (15)$$

где $\delta_0 = (P_0 - 0{,}5)/0{,}5 = 2P_0 - 1$ и $\delta_1 = (P_1 - 0{,}5)/0{,}5 = 2P_1 - 1$ – относительные погрешности по равновероятности исходных последовательностей с вероятностями появления 1 и нормированными ПАКФ P_0, P_1 и $\mathbf{r}_0(\tau)$, $\mathbf{r}_1(\tau)$ соответственно.

Примем, что индексы 0 и 1 у переменных (15) имеют отношение к многочленам $\varphi_0(x)$ и $\varphi_1(x)$ как сомножителям характеристического многочлена

вида (1), порождающих исходные последовательности. Пусть периоды исходных последовательностей выбраны взаимно простыми. Это означает отсутствие их взаимной корреляции [4], что позволяет применить формулу (15). Учитывая неопределенно разнообразное множество структурных и вероятностных свойств нерабочих последовательностей (в первую очередь P_0 и $\mathbf{r}_0(\tau)$), порождаемых $\varphi_0(x)$, выразим инвариантные свойства последовательностей на основе $\varphi_1(x)$. Так как речь идет о М-последовательностях m_1-го порядка, то известно выражение для вероятности $P_1 = 2^{m_1-1}\Big/\left(2^{m_1}-1\right)$ и относительной погрешности по равновероятности

$$\delta_1 = 2P_1 - 1 = 2^{m_1}\Big/\left(2^{m_1}-1\right) - 1 = 1/M_1 \text{, где } M_1 = 2^{m_1}-1.$$

Это позволяет ориентировать (15) на использование параметра M_1 в следующей форме:

$$\mathbf{r}(\tau) = \frac{1}{M_1^2 - \delta_0^2}\Big[\left(1-\delta_0^2\right)\left(M_1^2-1\right)\mathbf{r}_0(\tau)\mathbf{r}_1(\tau) + \left(1-\delta_0^2\right)\mathbf{r}_0(\tau) + \delta_0^2\left(M_1^2-1\right)\mathbf{r}_1(\tau)\Big]. \quad (16)$$

Пример 4. Рассмотрим многочлен ГПСП $\varphi(x)$ 7-й степени:

$$\varphi(x) = (x^2 \oplus x \oplus 1)(x \oplus 1)^5 = x^7 \oplus x^4 \oplus x^3 \oplus 1. \quad (17)$$

ПС многочлена (17) определится как $\{1(1),1(3)\}\{4(8)\} = \{4(8),4(24)\}$.

Моделированием ГПСП получим две пары взаимно инверсных рабочих последовательностей с периодом 24:

…,0 1 1 0 1 0 0 0 1 0 1 1 0 0 1 1 1 1 0 1 1 1 1 0,… (18)

…,1 0 0 1 0 1 1 1 0 1 0 0 1 1 0 0 0 0 1 0 0 0 0 1,

…,0 1 0 0 1 0 1 0 1 0 0 1 0 0 0 1 1 1 1 1 1 1 1 0 0…., (19)

…,1 0 1 1 0 1 0 1 0 1 1 0 1 1 1 0 0 0 0 0 0 0 1 1.

Причем последовательности первой пары неравновероятностные, а второй – равновероятностные, образованные от нерабочих (13) и (14) соответственно.

Степень равновероятности (13) и М-последовательности из (17) выражается погрешностями $\delta_0 = -1/2$ и $\delta_1 = 1/3$, определенными на своих периодах или общем $T = 24$. Так как периоды (13) и МП из (17) как исходных равны 8 и 3, то их взаимная простота позволяет применить формулы (15) и (16). Используя значения $\mathbf{r}_0(\tau)$ из табл. 13 и известные значения $\mathbf{r}_1(\tau)$ нормированной ПАКФ МП 2-го порядка, получаем результирующую ПАКФ $\mathbf{r}(\tau)$, представленную в табл. 15. Расчет и числовые значения определены в пределах τ от 0 до 0,5 $T = 12$.

Таблица 15

ПАКФ (13), МП из (17) и результирующей последовательности (18)

τ	0	1	2	3	4	5	6	7	8	9	10	11	12
$3\,\mathbf{r}_0(\tau)$	3	−1	1	−1	−1	−1	1	−1	3	−1	1	−1	−1
$2\,\mathbf{r}_1(\tau)$	2	−1	−1	2	−1	−1	2	−1	−1	2	−1	−1	2
$35\,\mathbf{r}(\tau)$	35	−1	−7	−1	−1	−1	17	−1	−13	−1	−7	−1	−1

Нетрудно убедиться, что подсчет $\mathbf{r}(\tau)$ по формуле (15), выполненный на периоде $T = 24$ при условии полного знания структуры (14), дает точно такой же результат.

Аналогичным образом можно повторить расчеты для равновероятностных последовательностей (14) и (19), но значение $\delta_0 = 0$ позволяет получить и использовать упрощенную форму выражения (12):

$$\mathbf{r}(\tau) = \frac{1}{M_1^2}\left[\left(M_1^2 - 1\right)\mathbf{r}_0(\tau)\mathbf{r}_1(\tau) + \mathbf{r}_0(\tau)\right] = \mathbf{r}_0(\tau)\mathbf{r}_1'(\tau), \qquad (20)$$

где

$$\mathbf{r}_1'(\tau) = \begin{cases} 1 & \text{при} \quad \tau = 0 \ (\mathrm{mod}\ M_1), \\ -\dfrac{1}{M_1} & \text{при} \quad \tau \neq 0 \ (\mathrm{mod}\ M_1), \end{cases} \qquad (21)$$

значения приведенной ПАКФ МП m_1-го порядка и M_1 – ее период [10].

Умножая значения $\mathbf{r}_0(\tau)$ из табл. 14 на отсчеты $\mathbf{r}_1'(\tau)$ приведенной ПАКФ МП 2-го порядка (фоновые уровни $-1/3$, так как $M_1 = 3$), получаем результирующую ПАКФ $\mathbf{r}(\tau)$, представленную в табл. 16 также на половине периода.

Таблица 16

ПАКФ (14), приведенная ПАКФ МП из (17)
и ПАКФ результирующей последовательности (19)

τ	0	1	2	3	4	5	6	7	8	9	10	11	12
$2\,\mathbf{r}_0(\tau)$	2	0	−1	0	0	0	−1	0	2	0	−1	0	0
$3\,\mathbf{r}_1'(\tau)$	3	−1	−1	3	−1	−1	3	−1	−1	3	−1	−1	3
$6\,\mathbf{r}(\tau)$	6	0	1	0	0	0	−3	0	−2	0	1	0	0

Подсчет $\mathbf{r}(\tau)$ по формуле (12), выполненный на периоде $T = 24$ при условии полного знания структуры (19), приводит к такому же результату.

Заключение

Представлен класс линейных генераторов, формирующих псевдослучайные последовательности, минимальные периоды которых меньше длин

М-последовательностей того же порядка. Оставляя без изменений известные технические решения генераторов (схемы Фибоначчи и Галуа), найдем формальные условия их работы и исследуем свойства формируемых последовательностей. Примечательной особенностью линейных рекуррентных последовательностей немаксимальной длины является их неоднородность, породившая многообразие циклических, структурных и статистических свойств.

Режим неоднородности работы генераторов позволил образовать специфичный вид двоичных псевдослучайных последовательностей, между элементами которых установлен взаимно инверсный характер следования в пределах половины минимального периода. Такие инверсно-сегментные последовательности, наряду с равновероятностью, обладают рядом корреляционных свойств, способствующих образованию многофункционального сервисного набора имитирующих сигналов для организации машинного эксперимента.

Реализация многоканального генератора Галуа в неоднородном режиме позволяет получить одновременно несколько пар разных псевдослучайных сигналов с нулевой периодической взаимно корреляционной функцией. Для этой цели решены задачи идентификации последовательностей и инициализации генератора в классе автоматных моделей.

Высокое быстродействие рассмотренных генераторов, малые аппаратные издержки при наличии многофункциональных свойств вероятностно-статистического характера актуальны в прикладных областях машинного моделирования, защиты информации и широкополосных систем связи.

Библиографический список

1. **Иванова, В. М.** Случайные числа и их применение / В. М. Иванова. – Москва : Финансы и статистика, 1984. – 111 с.
2. **Иванов, М. А.** Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков. – Москва : КУДИЦ-ОБРАЗ, 2003. – 240 с.
3. **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.
4. **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.
5. **Песошин, В. А.** Генераторы псевдослучайных и случайных чисел на регистрах сдвига / В. А. Песошин, В. М. Кузнецов. – Казань : Изд-во Казан. гос. техн. ун-та, 2007. – 296 с.
6. **Песошин, В. А.** Генераторы псевдослучайных последовательностей немаксимальной длины на основе регистра с внутренними сумматорами по модулю два (Часть 1) / В. А. Песошин, В. М. Кузнецов, А. И. Гумиров // Вестник Чувашского университета. – 2017. – № 1. – С. 263–272.
7. **Песошин, В. А.** Генераторы псевдослучайных последовательностей немаксимальной длины на основе регистра с внутренними сумматорами по модулю два (Часть 2) / В. А. Песошин, В. М. Кузнецов, А. И. Гумиров // Вестник Чувашского университета. – 2017. – № 1. – С. 273–284.
8. **Песошин, В. А.** Генераторы псевдослучайных последовательностей немаксимальной длины на основе регистра с внутренними сумматорами по модулю два

(Часть 3) / В. А. Песошин, В. М. Кузнецов, А. Х. Рахматуллин // Вестник Чувашского университета. – 2017. – № 3. – С. 251–261.
9. Генераторы псевдослучайных последовательностей немаксимальной длины на основе регистра с внутренними сумматорами по модулю два (Часть 4) / В. А. Песошин, В. М. Кузнецов, А. Х. Рахматуллин, Р. Р. Галимов, А. Д. Ямщикова // Вестник Чувашского университета. – 2018. – № 3. – С. 224–234.
10. **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.
11. **Элспас, Б.** Теория автономных линейных последовательных сетей / Б. Элспас // Кибернетический сборник. – Москва : ИЛ, 1963. – № 7. – С. 90–128.

References

1. Ivanova V. M. *Sluchaynye chisla i ikh primenenie* [Random numbers and their use]. Moscow: Finansy i statistika, 1984, 111 p. [In Russian]
2. 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]
3. 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]
4. 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]
5. Pesoshin V. A., Kuznetsov V. M. *Generatory psevdosluchaynykh i sluchaynykh chisel na registrakh sdviga* [Pseudo-random and random number generators on shift registers]. Kazan: Izd-vo Kazan. gos. tekhn. un-ta, 2007, 296 p. [In Russian]
6. Pesoshin V. A., Kuznetsov V. M., Gumirov A. I. *Vestnik Chuvashskogo universiteta* [Bulletin of Chuvash State University]. 2017, no. 1, pp. 263–272. [In Russian]
7. Pesoshin V. A., Kuznetsov V. M., Gumirov A. I. *Vestnik Chuvashskogo universiteta* [Bulletin of Chuvash State University]. 2017, no. 1, pp. 273–284. [In Russian]
8. Pesoshin V. A., Kuznetsov V. M., Rakhmatullin A. Kh. *Vestnik Chuvashskogo universiteta* [Bulletin of Chuvash State University]. 2017, no. 3, pp. 251–261. [In Russian]
9. Pesoshin V. A., Kuznetsov V. M., Rakhmatullin A. Kh., Galimov R. R., Yamshchikova A. D. *Vestnik Chuvashskogo universiteta* [Bulletin of Chuvash State University]. 2018, no. 3, pp. 224–234. [In Russian]
10. Pesoshin V. A., Kuznetsov V. M., Shirshova D. V. *Automation and Remote control*. 2016, vol. 77, no. 9, pp. 1622–1631.
11. Elspas B. *Kiberneticheskiy sbornik* [Cybernetic collection]. Moscow: IL, 1963, no. 7, pp. 90–128. [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 (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 (10 K. Marksa street, Kazan, Russia)

Кузнецова Александра Сергеева
студентка, 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 Sergeeva
Student, Kazan National Research Technical University named after A. N. Tupolev (10 K. Marksa street, Kazan, Russia)

Шамеева Алсу Рафиковна
студентка, Казанский национальный исследовательский технический университет имени А. Н. Туполева (КАИ), (Россия, г. Казань, ул. К. Маркса, 10)

E-mail: snameevaa@mail.ru

Shameeva Alsu Rafikovna
Student, Kazan National Research Technical University named after A. N. Tupolev (10 K. Marksa street, Kazan, Russia)

Образец цитирования:

Песошин, В. А. Генераторы псевдослучайных последовательностей немаксимальной длины на регистрах 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. 3–17. – DOI 10.21685/2072-3059-2019-1-1.