УДК 004.4’415 (045)

Р. Ю. Кандыба

ПРОГРАММНО-МОДЕЛИРУЮЩИЙ КОМПЛЕКС ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Інститут аэрокосмических систем управления НАУ, e-mail: iesy@nau.edu.ua

Разработан на алгоритмическом языке С++ программный продукт, обеспечивающий возможность построения генераторов псевдослучайной последовательности по схемам Галуа и Фибоначчи над образующими полиномами 4 – 8 степеней.

Ключевые слова: программный комплекс, генератор псевдослучайной последовательности, регистр сдвига с линейной обратной связью.

Введение и постановка задачи. Генераторы псевдослучайных последовательностей (ПСП) строятся на основе линейных регистров сдвига (ЛРС) с линейными обратными связями. Длина периода последовательности будет максимальной, если обратные связи в ЛРС создаются примитивными неприводимыми полиномами *n*-й степени. Неприводимый полином φ_n является примитивным (ПрП), если минимальное значение показателя e, при котором выполняется условие

$$x^e \equiv 1 \bmod \varphi_n \tag{1}$$

составляет величину

$$e = L_n = 2^n - 1. \tag{2}$$

Сравнение (1) означает, что степени образующего элемента $x = 10$ (являющегося полиномом первой степени с минимальным весом, равным 1) в кольце вычетов по модулю φ_n формируют последовательность длины (2).

Известны два типа ЛРС генераторов ПСП над ПрП: генераторы по схемам Галуа и Фибоначчи [1]. Обратные связи в регистрах этих генераторов задаются матрицами преобразований, посредством которых формируются функции возбуждения *D*-триггеров ЛРС. Обозначим эти матрицы как **G** и **F** для генераторов Галуа и Фибоначчи соответственно. Матрицы **G** и **F** связаны оператором правостороннего транспонирования (транспонирования относительно вспомогательной диагонали матрицы), для которого введем обозначение $\perp$. Следовательно,

$$\mathbf{G} \longleftrightarrow^{\perp} \mathbf{F}, \text{ т. е. } \mathbf{F} = \mathbf{G}^{\perp} \text{ и } \mathbf{G} = \mathbf{F}^{\perp}. \tag{3}$$

Пусть $\varphi_n = a_n a_{n-1} a_{n-2} \cdots a_1 a_0$ есть ПрП *n*-й степени, $a_i \in \{0, 1\}$, $i = \overline{1, n-1}$. Поскольку в двоичном неприводимом полиноме $\varphi_n = \varphi_0 = 1$, то $\varphi_n = 1\, a_{n-1} a_{n-2} \cdots a_1 1$.

Матрицы Галуа $\mathbf{G}_{\varphi_n}^{(10)}$ составляются по схеме, представленной соотношением

$$\mathbf{G}_{\varphi_n}^{(10)} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ \dots \\ n-1 \\ n \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & \dots & n-1 & n \end{array} \\ \begin{bmatrix} 0 & 0 & 0 & \dots & 0 & 1 \\ 1 & 0 & 0 & \dots & 0 & \grave{a}_1 \\ 0 & 1 & 0 & \dots & 0 & \grave{a}_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & \grave{a}_{n-2} \\ 0 & 0 & 0 & \dots & 1 & \grave{a}_{n-1} \end{bmatrix} \end{array}. \tag{4}$$

Пусть $D = (D_1, D_2, \cdots D_n)^T$ – вектор-столбец функций возбуждения D-триггеров n-разрядного ЛРС, а $U = (1, 2, \cdots n)$ – вектор-столбец состояний соответствующих разрядов регистра. Имеем

$$D = G \otimes U. \tag{5}$$

На основании выражения (5) легко приходим к выражению D_k для функций возбуждения k-го триггера ЛРС-генератора Галуа:

$$D_k = (k-1) \oplus n \cdot a_{k-1}, \quad k = \overline{1, n}. \tag{6}$$

В соотношениях (5) и (6) операторы $\otimes$ и $\oplus$ представляют собой операторы умноження и порозрядного сложения в кольце вычетов по $\bmod 2$. В правой части равенства (6) компоненты $(k-1)$ и n представляют собой отклики $(k-1)$-го и n-го разрядов ЛРС соответственно.

Структурная схема восьмиразрядного ЛРС генераторов ПСП над примитивный неприводимый полином (ПНП) $\varphi_8 = 101001101$ показана на рис. 1.

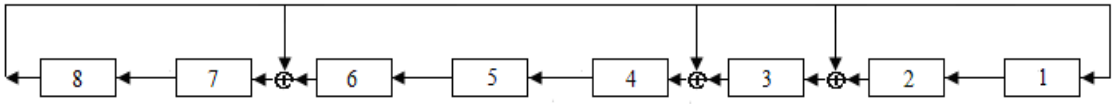


Рис. 1. Галуа ЛРС – генератор ПСП ($\omega = 10$)

В соответствии с преобразованием (3) от матрицы Галуа (4) приходим к матрице Фибоначчи

$$F_{\varphi_n}^{(10)} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ \dots \\ n-1 \\ n \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & \dots & n-1 & n \end{array} \\ \begin{bmatrix} a_{n-1} & a_{n-2} & a_{n-3} & \dots & a_1 & 1 \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 0 & 0 \\ 0 & 0 & 0 & \dots & 1 & 0 \end{bmatrix} \end{array}. \tag{7}$$

Верхний индекс в обозначениях матриц (4) и (7) соответствует классическому минимальному (по весу) образующему полиному первой степени $x = 10$.

Функции возбуждения D-триггеров ЛРС – генератора ПСП по схеме Фибоначчи получим на основании выражения (5), заменив в нем матрицу **G** матрицей **F**.

Основная идея обобщения методов синтеза генераторов ПСП на линейных регистрах сдвига состоит в замене в матрицах **G** и **F** образующих полиномов x первой степени $x = 10$ образующими полиномами ω произвольной степени, т. е.

$$M_{\varphi_n}^{(x)} \Rightarrow M_{\varphi_n}^{(\omega)}, \quad M = G \ \text{ или } \ M = F,$$

причем

$$\omega = 1\omega_{k-1}\omega_{k-2}\cdots\omega_0, \quad \omega_i \in \{0, 1\}, \quad i = \overline{0, k-1},$$

где k – степень образующего полинома.

Ограничимся в дальнейшем рассмотрением ЛРС – генераторов ПСП только по схеме Галуа. Как показали результаты компьютерных вычислений, замена образующего полинома

$\omega = 10$ полиномом $\omega = 11$ приводит к тому, что все разряды регистра оказываются охваченными обратными связями, при которых выход каждого *D*-триггера подается на вход того же триггера. Математически переход от матрицы $\mathbf{G}_{\varphi_n}^{(10)}$ к матрице $\mathbf{G}_{\varphi_n}^{(11)}$ отображается элементарной операцией

$$\mathbf{G}_{\varphi_n}^{(11)} = \mathbf{G}_{\varphi_n}^{(10)} \oplus E .$$

Имеем

$$\mathbf{G}_{\varphi_n}^{(11)} = \begin{array}{c} \\ 1 \\ 2 \\ 3 \\ \dots \\ n-1 \\ n \end{array} \begin{array}{c} \begin{array}{cccccc} 1 & 2 & 3 & \cdots & n-1 & n \end{array} \\ \begin{bmatrix} 1 & 0 & 0 & \dots & 0 & 1 \\ 1 & 1 & 0 & \dots & 0 & \grave{a}_1 \\ 0 & 1 & 1 & \dots & 0 & \grave{a}_2 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & \grave{a}_{n-2} \\ 0 & 0 & 0 & \dots & 1 & 1 \oplus \grave{a}_{n-1} \end{bmatrix} \end{array}. \qquad (8)$$

На основании соотношений (5) и (8) приходим к следующим значениям функций возбуждения *k*-го разряда ЛРС над ПрП φ_n и образующего полинома $\omega = 11$.

$$D_k = (k-1) \oplus k \oplus n a_{k-1}, \quad k = \overline{1, n}.$$

Структурная схема восьмиразрядного ЛРС – генераторов ПСП над ПрП $\varphi_8 = 101001101$ приведена на рис. 2.

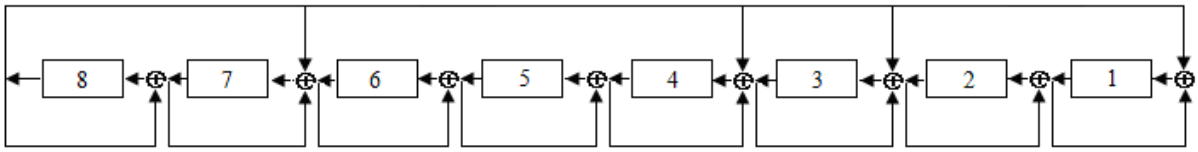


Рис. 2. Галуа ЛРС – генератор ПСП ($\omega = 11$)

В этой работе ставится задача разработать универсальный программный стенд, обеспечивающий возможность построения генераторов псевдослучайной последовательности на схемах Галуа и Фибоначчи над образующими полиномами 4 – 8 степеней.

Базовый интерфейс программного комплекса. Интерфейс базового моделирующего комплекса изображен на рис. 3.

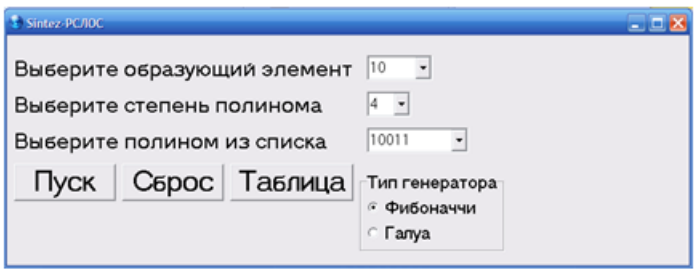


Рис 3. Базовый интерфейс моделирующего комплекса

Компоненты, показанные на рис. 1, позволяют параметризовать характеристики регистра сдвига с линейными обратными связями. Интерфейс допускает возможность выбора схемы построения сдвигового регистра.

После выбора всех параметров, нажав кнопку ПУСК, и если выбранный полином является примитивным для выбранного образующего элемента, то выводится на экран структурная схема ЛРС (рис. 4).

Рис. 4. Построение регистра сдвига с линейной обратной связью

Показатели ряда образующих элементов для всех 30 неприводимых полиномов восьмой степени сведены в таблицу.

Порядок образующих элементов двоичных неприводимых многочленов восьмой степени

Номер полинома	Неприводимый полином	Образующий элемент		Номер полинома	Неприводимый полином	Образующий элемент	
		10	11			10	11
1	100011011	51	255	16	110001011	85	51
2	100011101	255	51	17	110001101	255	255
3	100101011	255	85	18	110011111	51	255
4	100101101	255	17	19	110100011	85	85
5	100111001	17	255	20	110101001	255	255
6	100111111	85	255	21	110110001	51	85
7	101001101	255	255	22	110111101	85	17
8	101011111	255	255	23	111000011	255	255
9	101100011	255	255	24	111001111	255	85
10	101100101	255	255	25	111010111	17	85
11	101101001	255	255	26	111011101	85	51
12	101110001	255	85	27	111100111	255	51
13	101110111	85	255	28	111110011	51	85
14	101111011	85	85	29	111110101	255	255
15	110000111	255	85	30	111111001	85	255

Как видно из таблицы, только 16 из 30 неприводимых полиномов восьмой степени являются *примитивными*, т. е. такими, для которых образующий элемент 10 обладает максимальным порядком, равным 255.

Формирование таблицы. Полное множество ненулевых элементов поля $GF(2^n)$ над неприводимым полиномом φ можна выразить в виде степеней ω^k примитивного элемента

ω, вычисляемых по mod φ. Это означает, что ненулевые компоненты $GF(2^n)$ образуют циклическую группу относительно операции умножения.

Пусть $L = 2^n - 1$. Тогда

$$\omega^L \bmod \varphi \equiv 1.$$

Рассмотрим методику вычисления степеней образующего элемента $\omega = 11$ по заданному модулю неприводимого многочлена $\varphi = 100111001$. Имеем $\omega^0 = 1$, $\omega^1 = 11$.

Последующие *k*-е степени, $k \geq 2$, элемента ω будем формировать по правилу

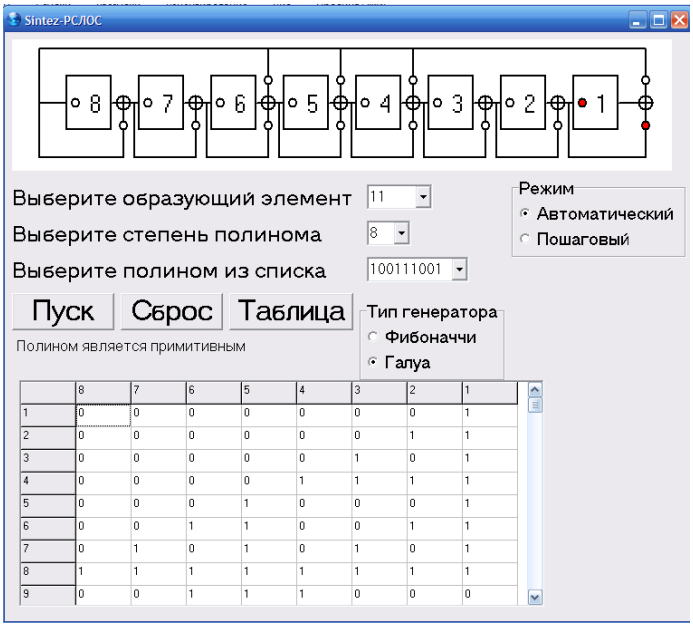
$$\omega^k = \omega^{k-1}\omega^1. \qquad (9)$$

Вычисления в соотношении (9) для $\omega = 11$ сводятся к поразрядному сложению по mod 2 многочлена ω^{k-1} и его копии, сдвинутой на один разряд влево. Следуя этому алгоритму, получим

$$\omega^2 = 101, \quad \omega^3 = 1111, \quad \omega^4 = 10001, \quad \omega^5 = 110011, \quad \omega^6 = 1010101, \quad \omega^7 = 11111111.$$

Восьмая степень (ω^8) примитивного образующего элемента $\omega = 11$, равная 100000001, оказывается девятиразрядной и, следовательно, должна быть приведена к остатку по модулю φ. В двоичной модулярной арифметике операция поразрядного вычитания, которая появляется на этапе вычисления остатков, эквивалентна операции поразрядного сложения.

Продолжая вычисления степеней элемента ω по модулю выбранного неприводимого полинома φ, приходим (определяя, в случае необходимости, остатки по модулю неприводимого полинома) к результатам, которые показаны на рис. 5 (прокруткой можно просмотреть всю таблицу).



	8	7	6	5	4	3	2	1
1	0	0	0	0	0	0	0	1
2	0	0	0	0	0	0	1	1
3	0	0	0	0	0	1	0	1
4	0	0	0	0	1	1	1	1
5	0	0	0	1	0	0	0	1
6	0	0	1	1	0	0	1	1
7	0	1	0	1	0	1	0	1
8	1	1	1	1	1	1	1	1
9	0	0	1	1	1	0	0	0

Рис. 5. Таблица степеней ПСП для $\omega = 11$ и $\varphi = 100111001$

Таблица, показанная на рис. 5, выводится на экран монитора при нажатии на кнопку ТАБЛИЦА. Роль осей координат таблицы выполняют ее затемненные верхняя строка и левый столбец. На оси абсцисс отложены значения двоичных разрядов, а на оси ординат – номер восьмибитных входных величин.

Также допускается возможность заполнения таблицы в пошаговом режиме. В этом случае каждая строка заполняется после нажатия на кнопку ТАКТ, а индикаторы

показывают состояния регистров (закрашенный – 1, белый – 0), соответствующий данному такту, как показано на рис. 6.

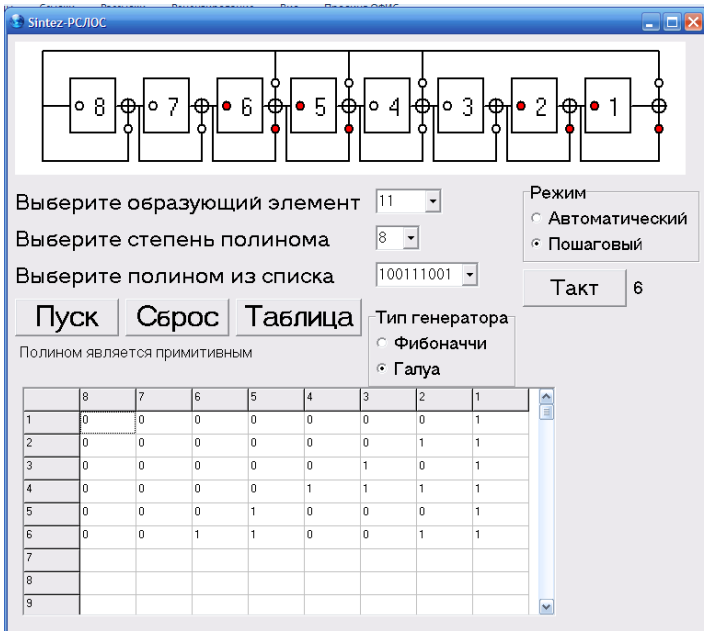


Рис. 6. Таблица степеней ПСП для $\omega = 11$ и φ = 100111001 в пошаговом режиме

Выводы. Разработанная на языке C++ программа синтеза регистров сдвига с линейной обратной связью позволяет строить генраторы псевдослучайной последовательности максимального порядка. Параметрами ЛРС являются неприводимые полиномы 4 – 8 степеней φ и образующие элементы ω = 10 и ω = 11. Интерфейс программы достаточно прост и может использоваться как в научных, так и в учебных целях.

Список литературы

1. *Иванов М. А. В.* Теория, применение и оценка качества генераторов псевдослучайных последовательностей / М. А. Иванов, И. В. Чугунков – М. КУДИЦ-ОБРАЗ, 2003. – 240 с.
2. *Блейхут Р.* Теория и практика кодов, контролирующих ошибки / Р. Блейхут – М.: Мир, 1986. – 576 с.
3. *Лидл Р.* Конечные поля: в 2 т. / Р. Лидл, Г. Нидеррайтер // пер. с англ. – М.: Мир, 1988. – Т.1. – 430 с.

Р. Ю. Кандиба

Програмно-моделювальний комплекс генераторів псевдовипадкових послідовностей

Розроблено алгоритмічною мовою C++ програмний продукт, що забезпечує можливість побудови генераторів псевдовипадкової послідовності за схемами Галуа й Фибоначчі над твірними поліномами 4 – 8 степенів.

R. U. Kandyba

Software-simulated complex for generators of pseudorandom sequences

Designed by algorithmic language C++ software, enables construction of pseudorandom sequence generators for Galois and Fibonacci schemes over polynomials forming 4 – 8 degrees.