УДК 004.932 **doi: 10.20998/2522-9052.2018.3.12**

А. Н. Рысованый

Национальный технический университет «ХПИ», Харьков, Украина

МЕТОД СИНТЕЗА ГЕНЕРАТОРОВ В КОНЕЧНОМ ПОЛЕ GF(3) С УПРОЩЕНИЕМ БЛОКОВ УМНОЖЕНИЯ

Предметом исследования в данной статье является процесс синтеза генераторов нелинейной псевдослучайной последовательности в конечном поле GF(3) с упрощением блока умножения. **Цель –** разработать метод синтеза генераторов нелинейной псевдослучайной последовательности в конечном поле GF(3) с упрощением блока умножения, основанный на использовании матрицы связей в качестве основного элемента генерации. **Задача**: на основе анализа известных подходов к генерированию последовательностей разработать метод, который по сравнению с двоичным регистром сдвига позволяет увеличить длину последовательности и упростить схему генерации. Используемыми **подходами** являются: применение циклического кодирования состояний, который позволяет в качестве операции умножения применять перекрестные линии выходов триггеров соответствующего канала регистра, что позволяет существенно упростить блок умножения. Получены следующие **результаты**: метод синтеза генераторов в конечном поле GF(3) с упрощением блоков умножения на коэффициенты, основанный на использовании матрицы связей в качестве основного элемента генерации. Приведен математический аппарат описания функционирования регистра сдвига с нелинейными обратными связями и его функциональная схема. В работе показан пример формирования первого состояния нелинейного регистра сдвига в зависимости от свободного коэффициента образующего полинома. **Выводы**. Предложен метод синтеза генераторов нелинейной псевдослучайной последовательности в конечном поле GF(3) с упрощением блока умножения, показаны примеры построения матриц связей в конечном поле тройки.

Ключевые слова: генератор двоичной последовательности; псевдослучайная последовательность; регистр сдвига.

Введение

Генераторы псевдослучайных чисел находят широкое применение в различных областях науки и техники. Такими областями можно считать и научные исследования, и моделирование, и криптографию, и статистику, и различные игры, и развлечения, экспертные системы принятия решений и т.д. [1, 2].

При выборе схем генераторов немаловажное значение имеет длина генерируемой последовательности и простота схемы [3-8]. При этом, генерируемые псевдослучайные последовательности обладают рядом существенных недостатков. Один из главных недостатков – достаточно короткий период генерации таких двоичных последовательностей. Наиболее просто реализуются такие генераторы с использованием сумматоров по mod2. В этом случае длина генерируемой последовательности ограничивается основанием двоичной системы счисления. Кроме того, существенным недостатком является очевидная зависимость генерирования последующей последовательности от предыдущей. Такой недостаток характерен всем алгоритмическим методам генерации последовательностей, но этот недостаток позволяет существенно упростить схему самого генератора.

До настоящего времени проблема создания быстрого, эффективного генератора псевдослучайных чисел по-прежнему не решена. Существует очень большое количество методов и просто схем генераторов псевдослучайных последовательностей, отличающихся как законами их описания, так и простотой реализации. Однако, трудность создания генераторов, лишенных традиционных недостатков, на данный момент, оказалось очень сложной задачей.

Для увеличения длины цикла генерации предлагается использовать в цепи обратных связей регистров сдвига сумматоры по mod3. Такие регистры сдвига, в цепях обратных связей которых производятся нелинейные преобразования, называются нелинейными. Получение псевдослучайной последовательности в конечном поле GF(3), основанной на использовании проверочной матрицы и матрицы связей в качестве основного элемента генерации, а также замена блока умножения на коммутацию линий и является **целью статьи**.

Основные проблемы и решения

Рассмотрим математическую модель функционирования генератора псевдослучайных последовательностей. Предположим, что анализируется последовательность длиной n с помощью регистра сдвига, который имеет r элементов. Обозначим предыдущее состояние j-го элемента каа b_j, а следующее – b^1_j. Тогда предыдущее состояние регистра сдвига из 5 элементов, будет $B = \|b_1, b_2, \ldots, b_5\|$, а следующее — $B^1 = \|b_1^1, b_2^1, \ldots, b_5^1\|$.

Состояние каждого r_i зависит от состояния других r_j в соответствии с выражением:

$$b_j^1 = a_1 b_1 \oplus_3 a_2 b_2 \oplus_3 a_3 b_3 \oplus_3 a_4 b_4 \oplus_3 a_5 b_5,$$

где $a_j = \{0, 1, 2\}$.

Для n-разрядного регистра сдвига каждое новое состояние спаренных в группу триггеров равно

$$b_j^1 = a_1 b_1 \oplus a_2 b_2 \oplus a_3 b_3 \oplus \ldots \oplus a_j b_j \oplus \ldots \oplus a_{16} b_{16}.$$

Функциональная схема генератора псевдослучайной последовательности с использованием блока сложения по mod3 с полиномом $P(x) = 2x^5 \oplus_3 x \oplus_3 1$ приведена на рис. 1. Так как при старшей степени аргумента коэффициент 2, то его необходимо в схеме умножить по mod3. Генерируемая последовательность для $P(x) = 2x^5 \oplus_3 x \oplus_3 1$, приведенная в виде матрицы состояний, представлена на рис. 2.

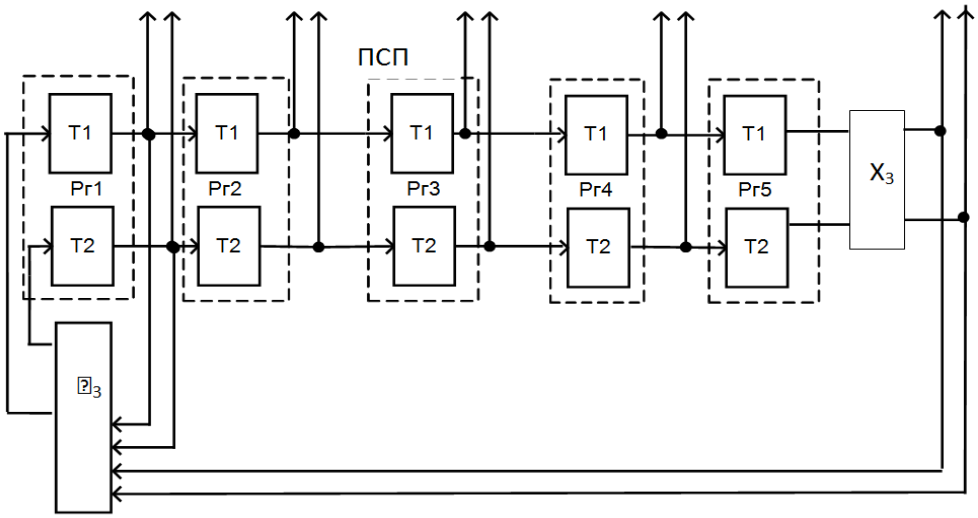

Рис. 1. Функциональная схема генератора псевдослучайных последовательностей с использованием блока сложения по mod3

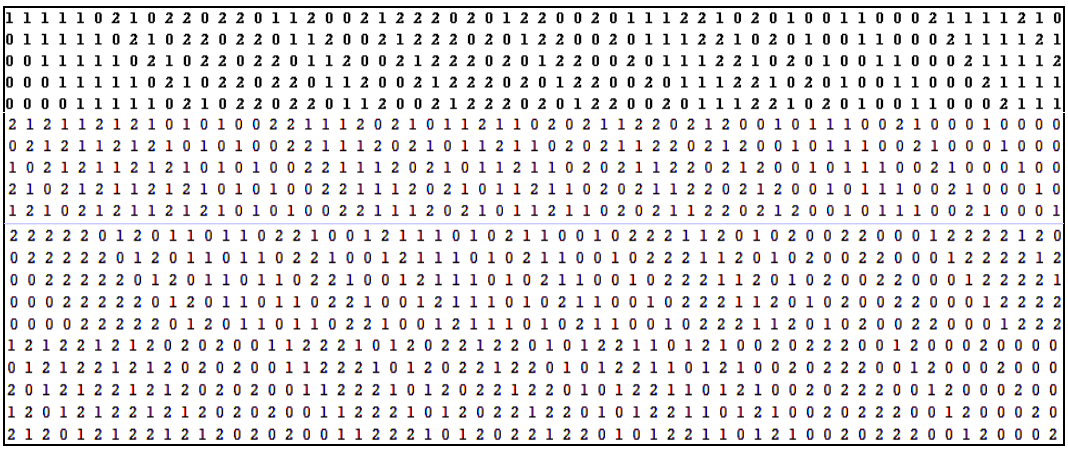

Рис. 2. Матрица состояний $P(x) = 2x^5 \oplus_3 x \oplus_3 1$

В связи с тем, что рассматриваемый полином генерирует максимальный период и его deg $P(X) = 5$:

$$T_{max} = 3^{\text{degP(x)}} - 1 = 242.$$

Таким образом, длина генерируемой этим полиномом $P(X)$ последовательности равняется 242.

Как следует из рис. 2, первое состояние генератора с $P(x) = 2x^5 \oplus_3 x \oplus_3 1$ $h_1 = \|10000\|$, второе – $h_2 = \|11000\|$, третье – $h_3 = \|11100\|$ и т.д.

Алгоритм формирования состояний нового столбца заключается в первоначальном сдвиге состояний предыдущего столбца и в формировании нового значения первого регистра. Это значение определяется как сумма по mod3 тех предыдущих значений регистров, номера которых соответствуют степеням образующего полинома, в соответствии с которыми и построена схема самого нелинейного генератора последовательности.

В связи с тем, что в нелинейном регистре кодируется двойной сигнал, то для хранения таких сигналом используются уже не отдельные триггера, а пары таких триггеров, которые принято называть каналом регистров. Связи выходов i-х каналов регистров со входами $i + 1$ каналов регистров описываются (описываются) матрицей связей S. В общем случае такая матрица имеет вид:

$$S = \begin{Vmatrix} a_1 & a_2 & a_3 & \dots & a_{r-1} & a_r \\ 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & 1 & 0 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & 0 & \dots & 1 & 0 \end{Vmatrix},$$

где a_i – коэффициенты образующего полинома, $r = degP(X)$ – максимальная степень регистра.

В качестве закона функционирования троичного кода используются выражения, которые соответствуют обычным правилам сложения двоичных чисел:

$$0 + 0 = 0 \rightarrow 00;$$
$$0 + 1 = 1 \rightarrow 01;$$
$$1 + 0 = 1 \rightarrow 01;$$
$$1 + 1 = 2 \rightarrow 10.$$

Важной особенностью этого правила является то, что сдвиг числа 1 на один разряд влево (то есть умножение на два) соответствует правильному значению – двойке (число 10).

Таким образом, образуется циклический сдвиг, который позволяет в качестве операции умножения применять перекрестные линии выходов триггеров соответствующего канала регистра, что позволяет существенно упростить блок умножения.

Таким образом, для построения генератора в конечном поле GF(3) необходимо выполнить действия:

определиться с длиной генерируемой последовательности;

определиться с максимальной степенью полинома;

выбрать исходное значение;

выбрать образующий полином с учетом предъявляемых к последовательности требований;

вычислить матрицу связей;

вычислить матрицу состояний;

определить длину цикла и сравнить с требуемой длиной;

построить схему с учетом обратных связей и блоков умножения на коэффициент 2 по модулю три.

На рис. 3 приведена схема генератора псевдослучайного последовательностей по модулю три.

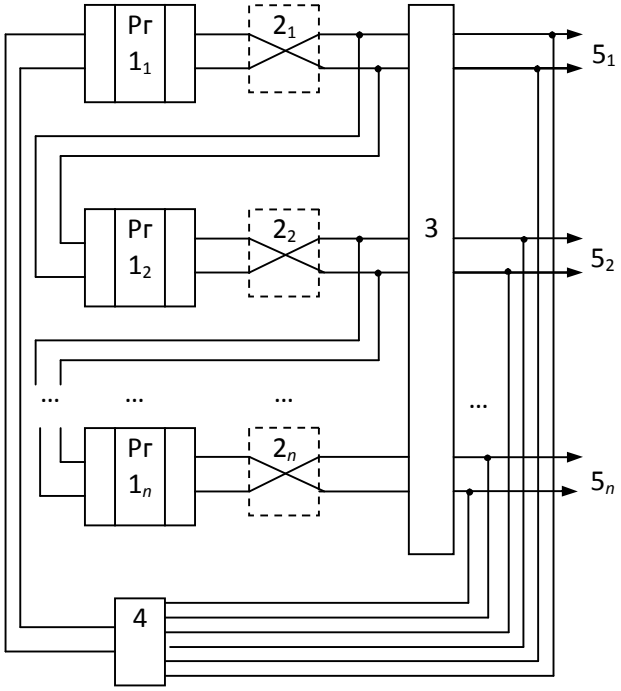

Рис. 3. Схема генератора в общем виде

На рис. 4 приведен пример реализации нелинейного генератора с $P(x) = 2x^4 \oplus_3 2x^4 \oplus_3 1$.

Устройство включает: группу блоков $1_1 - 1_n$ двухразрядных регистров; группу блоков $2_1 - 2_n$ умножения на два по модулю три, которые выполнены в виде перекрестных линий передачи данных; коммутатор 3, схему сумматора 4 по модулю три и пары выходных сигналов $5_1 - 5_n$ псевдослучайной последовательности. Генератор является схемой, которая осуществляет сдвиг содержимого регистра с учетом обратных связей, которые строятся в соответствии с образующим характеристическим полиномом $P(x) = a_r x^r \oplus_3 a_{r-1}x^{r-1} \oplus_3 \ldots \oplus_3 ax \oplus_3 a_0$, примитивного над конечным полем GF (3). Свободный член характеристического образующего полинома a_0 влияет на вид матрицы состояний и не зависит от связей регистра сдвига, которые задаются матрицей связей *S*.

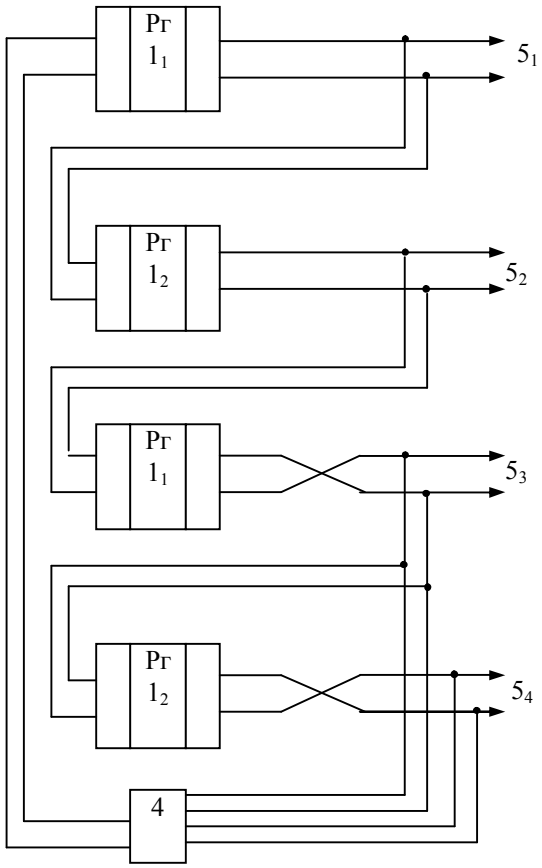

Рис. 4. Схема генератора $P(x) = 2x^4 \oplus_3 2x^4 \oplus_3 1$

На рис. 4 схема коммутатора 3 преобразовывается в цепи соединения выходов двухразрядного регистра со входами сумматора по модулю три с перекрестными линиями передачи данных в случае необходимости умножения на коэффициент 2. Это означает, что если у показателя степени полинома находится двойка, то вместо блока умножения на два по модулю три используется перекрестная передача сигналов, которая и выполняет умножение на два по модулю три.

Выводы

Предложен метод синтеза генераторов нелинейной псевдослучайной последовательности в конечном поле GF(3) с упрощением блока умножения. Такое упрощение возможно при определенном кодировании сигналов, что позволяет в качестве операции умножения применять перекрестные линии выходов триггеров соответствующего канала регистра.

СПИСОК ЛИТЕРАТУРЫ

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. / Р. Блейхут. – М.: Мир, 1986. – 576 с.
2. Муттер В. М. Основы помехоустойчивой телепередачи информации / В. М. Муттер. – Л.: Энергоатомиздат, 1990. – 288 с .

3. Рысованый А. Н. Выбор полиномов для нелинейных регистров сдвига с обратными связями по критерию формирования последовательности максимальной длины / А. Н. Рысованый, В. В. Гоготов // Системы управления, навигации и связи. – Киев.: Центральный научно-исследовательский институт навигации и управления, 2007. – Вып. 1.– С. 77-79.
4. Рысованый А. Н. Метод генерирования нелинейной псевдослучайной последовательности без использования обратных связей / А. Н. Рысованый // Системи управління, навігації та зв'язку. – Полтава : ПНТУ, 2018. – Вип. 4 (44). – С. 144-146.
5. Литиков И. П. Кольцевое тестирование цифровых устройств / И. П. Литиков. – М.: Энергоатомиздат, 1990. – 160 с.
6. Горяшко А. П. Синтез диагностируемых схем вычислительных устройств / А. П. Горяшко. – М.: Наука, 1987. – 288 с.
7. Ватолин Д. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео / Д. Ватолин, А. Ракушняк, М. Смирнов, В. Юкин. – М.: ДИАЛОГ-МИФИ, 2002. – 384 с.
8. Сорока Л. С. Способ получения псевдослучайной последовательности на основе использования матрицы связей в конечном поле GF(3) / Л. С. Сорока, А. Н. Рысованый, Б. И. Мороз // Патент Украины № u201109344. 2012. Бюл. № 5.

REFERENCE

1. Blehut, R. (1986), *Theory and Practice of Error Control Codes*, Mir, Moscow, 576 p.
2. Mutter, V.M. (1990), *Fundamentals of noise-free TV information*, Energoatomizdat, Leningrad, 288 p.
3. Rysovany, A.N. and Gogot, V.V. (2007), "Selection of polynomials for nonlinear shift registers with feedbacks on the criterion of forming a sequence of maximum length", *Control Systems, Navigation and Communications*, Central Research Institute of Navigation and Control, Kyiv, No. 1, pp. 77 - 79.
4. Rysovany, A.N. (2018), "Method of generating a nonlinear pseudorandom sequence without using feedbacks", *System Control, Navigation and Connection*, PNTU, Poltava, No. 4 (44), pp. 144-146.
5. Litikov, I.P. (1990), *Ring testing of digital devices*, Energoatomizdat, Moscow, 160 p.
6. Goryashko, A.P. (1987), *Synthesis of Diagnosed Computing Device Circuits*, Nauka, Moscow, 288 p.
7. Vatolin, D., Rakushnyak, A., Smirnov, M. and Yukin V. (2002), *Data Compression Methods. Device archivers, image and video compression*, DIALOG-MEPI, Moscow, 384 p.
8. Soroka, L.S., Rysovany, A.N. and Frost B.I. (2012), *A method of obtaining a pseudo-random sequence based on the use of a coupling matrix in the final field GF (3)*, Patent of Ukraine No. u201109344, Byul. No. 5.

Received (Надійшла) 28.06.2018
Accepted for publication (Прийнята до друку) 29.08.2018

Метод синтезу генераторів в кінцевому полі GF (3) зі спрощенням блоків множенняв

О. М. Рисований

Предметом дослідження в даній статті є процес синтезу генераторів нелінійної псевдовипадкової послідовності в кінцевому полі GF (3) зі спрощенням блоку множення. **Мета** - розробити метод синтезу генераторів нелінійної псевдовипадкової послідовності в кінцевому полі GF (3) зі спрощенням блоку множення, заснований на використанні матриці зв'язків в якості основного елемента генерації. **Завдання**: на основі аналізу відомих підходів до генерування послідовностей розробити метод, який в порівнянні з двійковим регістром зсуву дозволяє збільшити довжину послідовності і спростити схему генерації. Використовуваними **підходами** є: застосування циклічного кодування станів, який дозволяє в якості операції множення застосовувати перехресні лінії виходів тригерів відповідного каналу регістра, що дозволяє істотно спростити блок множення. Отримані наступні **результати**: метод синтезу генераторів в кінцевому полі GF (3) зі спрощенням блоків множення на коефіцієнти, заснований на використанні матриці зв'язків в якості основного елемента генерації. Наведено математичний апарат опису функціонування регістра зсуву з нелінійними зворотними зв'язками і його функціональна схема. У роботі показаний приклад формування першого стану нелінійного регістра зсуву залежно від вільного коефіцієнта утворюючого полінома. **Висновки**. Запропоновано метод синтезу генераторів нелінійної псевдовипадкової послідовності в кінцевому полі GF (3) зі спрощенням блоку множення, показані приклади побудови матриць зв'язків в кінцевому полі трійки.

Ключові слова: генератор двійковій послідовності; псевдовипадкова послідовність; регістр зсуву.

The method for the synthesis of generators in the terminal field of GF (3)

A. Rysovaniy

The subject of progress in this article is a process of synthesis of generators of independent pseudo-successive messages in the main field of GF (3) for the multiplication unit. The **problem**: develop a method for the synthesis of generators of non-first pseudo-disputable succession in the main field of the GF (3), which is based on a multiply basis based on victorious matrixes of words in the basic element of the generation. **The task:** based on the analysis of known approaches to the generation of sequences, develop a method that, as compared with the binary shift register, allows increasing the length of a sequence and simplifying the generation scheme. The approaches used are: the use of cyclic coding of states, which allows to apply the cross lines of the triggers of the corresponding channel of the register as the multiplication operation, which allows to significantly simplify the multiplication unit. The following results were obtained: a method for synthesizing generators in a finite field GF (3) with a simplification of the multiplication blocks for coefficients, based on the use of a coupling matrix as the main element of generation. The mathematical apparatus for describing the operation of a shift register with nonlinear feedbacks and its functional diagram are given. The paper shows an example of the formation of the first state of a nonlinear shift register, depending on the free coefficient of the generating polynomial. **Conclusions**. A method for synthesizing nonlinear pseudo-random sequence generators in a finite field GF (3) with simplification of the multiplication unit is proposed, examples of constructing a matrix of links in a finite triple field are shown.

Keywords: binary sequence generator; pseudo-random sequence; shift register.