УДК 004.932 **doi: 10.26906/SUNZ.2018.6.079**

А. Н. Рысованый

Национальный технический университет «ХПИ», Харьков, Украина

МЕТОД СИНТЕЗА НЕЛИНЕЙНЫХ ГЕНЕРАТОРОВ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ НА ОСНОВЕ ИСПОЛЬЗОВАНИЯ ПЕРВОГО СОСТОЯНИЯ МАТРИЦЫ СОСТОЯНИЙ В КОНЕЧНОМ ПОЛЕ GF(3)

Предметом исследования в данной статье является процесс синтеза нелинейных генераторов псевдослучайной последовательности в конечном поле *GF*(3) на основе использования первого состояния матрицы состояний. **Цель –** разработать метод синтеза нелинейных генераторов псевдослучайной последовательности в конечном поле *GF*(3), основанный на использовании первого столбца матрицы состояний в качестве основного элемента генерации. **Задача**: создание математического описания нелинейных генераторов псевдослучайной последовательности в конечном поле *GF*(3), основанный на использовании взаимодействия первого столбца матрицы состояний и матрицы связей различных степеней. Поставленная задача решается за счет того, что в известном способе описания нелинейных генераторов псевдослучайной последовательности при использовании полиномов, которые генерируют максимальный период, связи выходов и входов триггеров описываются при помощи матрицы связей. А сдвиг предыдущего состояния на один разряд есть операция умножения этой матрицы на начальное, исходное, состояние регистра. Получены следующие **результаты**: метод синтеза генераторов в конечном поле *GF*(3), основанный на использовании первого, начального, состояния генератора в качестве основного элемента генерации. Приведен математический аппарат описания функционирования регистра сдвига с нелинейными обратными связями. В работе показаны примеры формирования различных степеней матрицы связей, показана роль свободного члена полинома в формировании проверочной матрицы. **Выводы:** в работе впервые приведено и доказано утверждение о нахождении любого состояния генератора на основе его первого состояния для конечного поля *GF*(3) для двух полупериодов цикла генерации. Приведенные формулы нахождения состояний генератора могут быть использованы при построении схемы генератора без использования обратных связей.

Ключевые слова: Генератор последовательности, генератор псевдослучайной последовательности в поле *GF*(3), псевдослучайная последовательность, регистр сдвига.

Введение

Во многих областях науки и техники широкое применение находят регистры сдвига и устройства на их основе [1-6]. Нельзя обойти вниманием и военную технику, в качестве одного из примеров можно привести передачу пакетов данных, передаваемых операторами противолодочного самолёта P-8A «Poseidon» по кодированному радиоканалу связи на соответствующий командный пункт. Для этого используется радиоканал тактической сети обмена данными «Link-16», который защищен методом псевдослучайной выборки рабочей частоты с громадной скоростью изменения этой частоты (77,8 кГц – это 77800 скачков/с). И в это же время для перестройки имеются большое число фиксированных частотных ячеек памяти в диапазоне от 0,96 до 1,215 ГГц (51 ячейка).

Естественно, что и число ячеек может быть в следующих разработках увеличено, а если использовать динамически изменяемый вид полиномов, которые являются закрытой информацией, то расшифровать такой сигнал в реальном масштабе времени, даже теоретически, не представляется возможным.

Можно в качестве примера привести и систему глобального позиционирования GPS, сигналы в которой подвергаются модулированию псевдослучайной последовательностью (ПСП) двух типов: первый тип – *P*-код и второй тип – *C*/*A*-код. *C*/*A*-код представляет собой код с циклом повторения 1023 состояния, частотой 1,023 МГц и, естественно, полиномом с $degP(x) = 10$, что является достаточно слабой характеристикой. На этой частоте и с такой ПСП работают GPS-приёмники гражданского назначения. А вот *P*-код используется в системах ответственного (военного) применения. Здесь применяется полином с циклом повторения $2 \cdot 10^{14}$ состояний.

Сигналы, которые модулированы *P*-кодом, передаются на двух разных частотах: F1 = 1575,42 МГц и F2 = 1227,6 МГц. А несущая частота еще модулируется и навигационным сообщением. Для надежной защиты БПЛА от перехвата управления можно считать двойное применения ПСП для переброски частот и для модулирования сигнала. Причем, если использовать при этом редко используемые и не до конца исследованные полиномы из конечных или расширенных полей Галуа (из-за нелинейности преобразований), то в настоящее время перехват управления можно считать невозможным.

Актуальность применения ПСП не сколько не ограничивается приведенными примерами. Можно привести еще множество примеров применения ПСП в защищенных системах, таких как, криптографические системы, радиолокационные станции, средства моделирования, системы имитации, защита банковской информации и др.

При анализе известных характеристик приведенных современных систем (например, в «Link-16» может применяться полином с циклом повторения 2^{17}) однозначно делается вывод, что для надежной защиты от посягательства на чужую информацию одним из критериев является критерий выбора полинома с очень большим циклом повто-

рения. Увеличение цикла генерации возможно как путем применения полиномов с большей степенью полинома так и применение полиномов из конечных или расширенных полей Галуа. Конечно, каждый из способов имеет свои достоинства и недостатки.

Нахождение любого состояния нелинейного генератора на основе его первого состояния для конечного поля $GF(3)$ и является **целью статьи**.

Основные проблемы и решения

В зависимости от требований к генераторам псевдослучайных последовательностей существуют различные методы их построения и, как следствие, большое многообразие таких схем [7-9]. Но одно требование остается всегда актуальным – должен существовать достаточно большой цикл генерации. В противном случае – это уже не псевдослучайная, а случайная последовательность с непредсказуемыми характеристиками. Причем, в большинстве случаев цикл генерации должен быть максимальным. Максимальность предполагает не только наличие всех возможных состояний в гамме, но и возможность применения математического анализа всех этих состояний [7, 8]. В зависимости от конкретных требований, таких как сложность технической реализации всего устройства или отдельных его частей, выдача воздействий для выявления не только ошибок, но и определенного вида ошибок исследуемой схемы, подчинение определенным законам распределения и т.д., то последнее условие может и не выполняться.

Основная проблема генераторов псевдослучайных последовательностей – это получение математических выражений, которые описывают не только предыдущие состояния, но и дают возможность вычисления и любых других, и не только предыдущих. Это позволяет рассчитать как весь цикл генерации, так и его часть с любой позиции генерации и построить при этом различные варианты схем, которые позволяют получить один и тот же результат. Для увеличения длины цикла рассмотрим полиномы конечного поля $GF(3)$, которые позволяют достаточно резко увеличить цикл генерации. Классический генератор псевдослучайных последовательностей представляет собой регистр сдвига, в цепи обратных связей которого располагается сумматор по модулю поля.

Короткий период генерации является «узким» местом генераторов псевдослучайных последовательностей. Увеличить этот период генерации наиболее просто, если применить полиномы в конечном поле, например, $GF(3)$.

Суть предлагаемого способа заключается в следующем. Сначала строится матрица связей S первой степени в конечном поле $GF(3)$, которая описывает связи входов и выходов регистра сдвига с обратными связями согласно виду образующего полинома.

Для сокращения записи будем учитывать только коэффициенты полинома, например, для $P(X)$ = 1221202 матрица связей имеет вид:

$$S = \begin{Vmatrix} 0 & 2 & 1 & 2 & 2 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{Vmatrix}.$$

Свободный член полинома $P(X)$ не находит отражения в матрице связей S первой степени. Однако он определяет самое главное состояние – это начальное (первое) состояние $h_1 = \| a_0 00000 \|$ матрицы состояний H, которое никогда не входит в матрицу S первой степени.

Но от его значения по правилу выбранного полинома формируются все остальные столбцы матрицы H.

Выходные состояния генератора в конечном итоге сводятся в матрицу состояний H:

$$H = \|h_1 h_2 h_3 ... h_n\|, \text{ где } n \text{ – длина гаммы.}$$

Рассмотрим распределение столбцов в матрице S различных степеней в зависимости от их значений. В связи с тем, что рассматриваются $P(X)$, которые имеют только $T_{\max}$, то, естественно в ПСП присутствуют все значения переборов. Так, например, для $P(X)$ = 1221202:

$$S^1 = \|h_{366}, h_{367}, h_{297}, h_{422}, h_{81}, h_{365}\|;$$

$$S^2 = \|h_{367}, h_{368}, h_{298}, h_{423}, h_{82}, h_{366}\|;$$

$$S^3 = \|h_{368}, h_{369}, h_{299}, h_{424}, h_{83}, h_{367}\|.$$

Примечательно, что когда номер одного из столбцов h_i достигает $T_{\max}$, то нумерация начинается с h_1:

$$S^{308} = \|h_{673}, h_{674}, h_{604}, h_1, h_{388}, h_{672}\|;$$

$$S^{365} = \|h_2, h_3, h_{661}, h_{58}, h_{445}, h_1\|.$$

Последняя запись представляет особый интерес для анализа наполняемости матрицы S столбцами h_i, т.к. в матрице присутствует первый столбец h_1, который всегда является исходным для матрицы H, а в матрице S располагается в последнем столбце.

Но степень матрицы S, у которой, наконец, появился h_1, свидетельствует о том, что $a_0 = 2$. Наиболее просто исследовать $P(X)$ с $a_0 = 1$. В последнем случае для $P(X)$ = 1221202:

$$S_{.6} = \|h_1\|; S_{.2} = \|h_2\|; S_{.3} = \|h_3\|.$$

Обобщенная запись S_i для $P(X)$ = 1221202:

$$S^i = \|h_{i+365}, h_{i+366}, h_{i+296}, h_{i+421}, h_{i+80}, h_{i+364}\|.$$

Из анализа полученных результатов и на основании ранее полученных исследований [7-9] можно сделать вывод, что распределение номеров столбцов

в матрице S подчиняется правилу: последний столбец всегда равен h_1, если свободный коэффициент полинома $a_0 = 1$ или первому столбцу второго полупериода, который всегда в $GF(3)$ инверсен в действующих значениях 1 и 2 друг другу.

Например, если $a_0 = 1$, то $h_1 = \|100\ldots00\|$, а $h_{P/2} = \|200\ldots00\|$, где P – период $P(X)$. Для каждого $P(X)$ существует свое распределение столбцов h_i в матрице S.

Утверждение. Каждый i-й столбец матрицы состояний H определяется путем перемножения по модулю поля первого столбца h_1 матрицы состояний H на матрицу связей S^{i-1} степени предыдущего столбца регистра сдвига с обратными связями.

Доказательство. Анализу будут подвергаться полиномы, которые имеют $T_{\max}$ [7-9].

В связи с тем, что матрица связей S всегда квадратная и ее размер $r \times r$ определяется только видом полинома $P(X)$, то любой ее i-й столбец должен соответствовать определенному столбцу h_i матрицы состояний H.

Вначале рассмотрим полином, у которого свободный член $a_0 = 1$, например, $P(X) = 1000011$.

Для $P(X)$ с $a_0 = 1$ начальное $h_1 = \|100000\|$. Обозначим предыдущее состояние k-того регистра как b, а текущее как b'.

При сдвиге этого состояния в регистре сдвигов с выбранными обратными связями будет получено $h_2 = \|b_1 10000\|$, где

$$b_1 = b_1' \oplus_3 b_5';\ b_2 = b_1';$$

$$b_3 = b_2';\ b_4 = b_3';$$

$$b_5 = b_4';\ b_6 = b_5'.$$

Полученное выражение обозначает, что вначале происходит сдвиг всех триггеров регистра, а затем формирование значения первого триггера с учетом обратных связей по правилу выбранного полинома.

Но такие взаимосвязи входов и выходов триггеров регистра описывает и матрица S, которая для этого $P(X)$= 1000011 имеет вид:

$$S = \begin{Vmatrix} 1 & 0 & 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \end{Vmatrix}$$

Поэтому, если первое состояние умножить по модулю поля на матрицу S, то будет получено второе состояние, например

$$h_2 = h_1 \otimes_3 S^1.$$

Применим метод подстановки для получения других значений h_i:

$$h_3 = h_2 \otimes_3 S^1 = (h_1 \otimes_3 S^1) \otimes_3 S^1 = h_1 \otimes_3 S^2;$$

$$h_4 = h_3 \otimes_3 S^1 =$$

$$= (h_2 \otimes_3 S^1) \otimes_3 S^1 =$$

$$= (h_1 \otimes_3 S^1) \otimes_3 S^1 \otimes_3 S^1 = h_1 \otimes_3 S^3;$$

$$h_5 = h_4 \otimes_3 S^1 =$$

$$= (h_3 \otimes_3 S^1) \otimes_3 S^1 =$$

$$= (h_2 \otimes_3 S^1) \otimes_3 S^1 \otimes_3 S^1 \otimes_3 S^1 = h_1 \otimes_3 S^4$$

и т.д.

Следовательно, обобщенная формула получения i-го состояния h_i при условии, $a_0 = 1$ будет такой:

$$h_i = h_1 \otimes_3 S^{i-1} \mid a_0 = 1.$$

Рассмотрим $P(X)$ = 1221202, у которого $a_0 = 2$. Из проведенных исследований [7-9] известно, что в поле $GF(3)$ формируется период, состояний из двух полупериодов.

А так как полупериоды инверсны значениями 1 и 2 друг другу, то это свойство необходимо учитывать.

Результирующая формула получения i-того состояния h_i при условии, что $a_0 = 2$ будет такой:

$$h_i = h_1 \otimes_3 S^{i-1+P/2} \mid a_0 = 2.$$

Для $P(X) \in \deg P(X) = 6$ с $T_{max} = 728$ насчитывается 96 полиномов:

1000011 ;1000021 ;1001011 ;1002021 ;1010211 ;1010221;
1011021 ;1011121 ;1012011 ;1012111 ;1020111 ;1020121;
1021111 ;1022121 ;1100001 ;1101001 ;1101111 ;1101211;
1102201 ;1110121 ;1110201 ;1111011 ;1111111 ;1111221;
1112221 ;1120101 ;1120221 ;1121011 ;1121101 ;1121211;
1122201 ;1200001 ;1201201 ;1202001 ;1202121 ;1202221;
1210111 ;1210201 ;1211211 ;1212021 ;1212121 ;1212211;
1220101 ;1220211 ;1221201 ;1222021 ;1222101 ;1222221;
1000012 ;1000022 ;1001012 ;1002022 ;1010212 ;1010222;
1011022 ;1011122 ;1012012 ;1012112 ;1020112 ;1020122;
1021112 ;1022122 ;1100002 ;1101002 ;1101112 ;1101212;
1102202 ;1110122 ;1110202 ;1111012 ;1111112 ;1111222;
1112222 ;1120102 ;1120222 ;1121012 ;1121102 ;1121212;
1122202 ;1200002 ;1201202 ;1202002 ;1202122 ;1202222;
1210112 ;1210202 ;1211212 ;1212022 ;1212122 ;1212212;
1220102 ;1220212 ;1221202 ;1222022 ;1222102 ;1222222.

Выводы

В работе впервые приведено и доказано утверждение о нахождении любого состояния генератора на основе его первого состояния для конечного поля $GF(3)$ для двух полупериодов цикла генерации.

Приведенные формулы нахождения состояний генератора могут быть использованы при построения схемы генератора без использования обратных связей.

СПИСОК ЛИТЕРАТУРЫ

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.
2. Ватолин Д., Ракушняк А., Смирнов М., Юкин В. Методы сжатия данных. Устройство архиваторов, сжатие изображений и видео. – М.: ДИАЛОГ-МИФИ. – 2002. – 384 с.
3. Горяшко А.П. Синтез диагностируемых схем вычислительных устройств. – М.: Наука. Гл. ред. физ.-мат. лит. – 1987. – 288 с
4. Кларк Дж., мл., Кейн Дж. Кодирование с исправлением ошибок в системах цифровой связи: Пер. с англ. — М.: Радио и связь, 1987. — 392 с.
5. Литиков И. П. Кольцевое тестирование цифровых устройств. – М.: Энергоатомиздат, 1990. – 160 с.
6. Муттер В. М. Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат, 1990. – 288 с .
7. Рысованый А. Н. Метод генерирования нелинейной псевдослучайной последовательности без использования обратных связей/ А. Н. Рысованый // Системи управління, навігації та зв'язку. – Полтава : ПНТУ ім. Ю. Кондратюка. –2 018. – №4(50).– С. 144-146.
8. Рысованый А. Н. Метод синтеза генераторов в конечном поле *GF*(3) с упрощением блоков умножения / А. Н. Рысованый // Сучасні інформаційні системи . – Харків: НТУ «ХПІ» – 2018. – Том 2, №3. – С. 76-79.
9. Сорока Л. С., Рысованый А. Н., Мороз Б. И. Способ получения псевдослучайной последовательности на основе использования матрицы связей в конечном поле GF(3) // Патент Украины № u201109344. 2012. Бюл. № 5.

Рецензент: д-р техн. наук, проф. С. В. Козелков,
Державний університет телекомунікацій, Київ
Received (Надійшла) 28.09.2018
Accepted for publication (Прийнята до друку) 29.11.2018

Метод синтезу нелінійних генераторів псевдовипадкової послідовності на основі використання першого стану матриці станів в кінцевому полі GF (3)

О. М. Рисований

Предметом дослідження в даній статті є процес синтезу нелінійних генераторів псевдовипадкової послідовності в кінцевому полі *GF* (3) на основі використання першого стану матриці станів. **Мета** - розробити метод синтезу нелінійних генераторів псевдовипадкової послідовності в кінцевому полі *GF* (3), заснований на використанні першого стовпчика матриці станів в якості основного елемента генерації. **Завдання**: створення математичного опису нелінійних генераторів псевдовипадкової послідовності в кінцевому полі GF (3), заснований на використанні взаємодії першого стовпчика матриці станів і матриці зв'язків різних ступенів. Задача, що поставлена вирішується за рахунок того, що у відомому способі опису нелінійних генераторів псевдовипадкової послідовності при використанні поліномів, які генерують максимальний період, зв'язки виходів і входів тригерів описуються за допомогою матриці зв'язків. А зрушення попереднього стану на один розряд є операція множення цієї матриці на початковий стан регістра. Отримані наступні **результати**: метод синтезу генераторів в кінцевому полі *GF* (3), заснований на використанні першого, вихідного, стану генератора в якості основного елемента генерації. Наведено математичний апарат опису функціонування регістра зсуву з нелінійними зворотними зв'язками. У роботі показані приклади формування різних ступенів матриці зв'язків, показана роль вільного члена полінома в формуванні перевірочної матриці. **Висновки:** в роботі вперше наведено і доведено твердження про знаходження будь-якого стану генератора на основі його першого стану для кінцевого поля *GF* (3) для двох напівперіодів циклу генерації. Наведені формули знаходження станів генератора можуть бути використані при побудові схеми генератора без використання зворотних зв'язків.

Ключові слова: Генератор двійковій послідовності, псевдовипадкова послідовність, регістр зсуву.

Synthesis method of nonlinear generators Pseudocasual sequence based on first use condition of the state matrix in the final field GF (3)

A. Rysovaniy

The subject of research in this article is the process of synthesis of nonlinear Pseudocasual sequence generators in a finite field GF (3) based on the use of the first state of the state matrix. The goal is to develop a method for synthesizing nonlinear generators of a Pseudocasual sequence in a finite field GF (3), based on using the first column of the state matrix as the main generation element. **Task:** creating a mathematical description of nonlinear Pseudocasual sequence generators in a finite field GF (3), based on the interaction of the first column of the state matrix and the matrix of relations of different degrees. The problem is solved due to the fact that in the well-known method of describing nonlinear Pseudocasual sequence generators using polynomials that generate the maximum period, the connections of the outputs and inputs of the triggers are described using a matrix of relations. And the shift of the previous state by one digit is the operation of multiplying this matrix by the initial, initial, state of the register. The following results were obtained: a method for synthesizing generators in a finite field GF (3), based on using the first, initial, state of the generator as the main element of generation. The mathematical apparatus for describing the operation of the shift register with nonlinear feedback is given. The paper shows examples of the formation of various degrees of the matrix of relations, shows the role of the free member of a polynomial in the formation of a test matrix. **Conclusions:** in this paper, for the first time, the statement about finding any state of the generator based on its first state for a finite field *GF* (3) for two half cycles of the generation cycle is given and proved. The above formulas for finding the states of a generator can be used to construct a generator circuit without using feedback.

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