УДК 004.932 **doi: 10.26906/SUNZ.2018.4.144**

А. Н. Рысованый

Национальный технический университет «ХПИ», Харьков, Украина

МЕТОД ГЕНЕРИРОВАНИЯ НЕЛИНЕЙНОЙ ПСЕВДОСЛУЧАЙНОЙ ПОСЛЕДОВАТЕЛЬНОСТИ БЕЗ ИСПОЛЬЗОВАНИЯ ОБРАТНЫХ СВЯЗЕЙ

Предметом исследования в данной статье является процесс получения нелинейной псевдослучайной последовательности на основе использования матрицы связей в конечном поле GF(3). **Цель –** разработать метод получения нелинейной псевдослучайной последовательности в конечном поле GF(3), 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. Используемыми **подходами** являются: получение математической закономерности генерирования нового состояния на основе полученного ранее и получение схемы генератора, который реализовывает эти закономерности. Получены следующие **результаты**: метод получения псевдослучайной последовательности в конечном поле GF(3), 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 регистра. Кроме того, приведен пример закономерности кольцевого расположения столбцов матриц связи. В результате чего предложена схема генерирования последовательности без применения обратных связей, как у классического регистра сдвигов. Это позволяет генерировать последовательности для любого выбранного полинома, который удовлетворяет условию получения максимального периода генерации. **Выводы**. Предложен метод, представленный в виде полученного выражения, позволяет определить все столбцы матрицы состояний H без выполнения расчетов и быть применимым для определения ПСП с использованием примитивного неприведенного характеристического полинома. В предложенном методе отсутствуют обратные связи, как у классического регистра сдвига, и, поэтому, могут генерироваться ПСП для любого выбранного полинома, который удовлетворяет условию получения максимального периода генерации.

Ключевые слова: псевдослучайная последовательность, регистр сдвига.

Введение

В системах диагностирования цифровых объектов одно из значительных мест отводится генераторам псевдослучайных последовательностей (ПСП), от качества которых зависит глубина тестов. Например, при диагностировании шинных формирователей, контроллеров шин, микросхем памяти становится неэффективным псевдослучайный тест с линейного регистра сдвига с обратными связями, так как эти схемы имеют три состояния (0, 1 и R – высокий импеданс).

Кроме того, для диагностирования линий передачи данных, по которым передаются двуполярные сигналы (V+, V–, V0) предпочтительнее использовать устройства, предназначенные именно для решения таких задач. В этих случаях третьи состояния не диагностируются. Регистры сдвига с нелинейными обратными связями являются основой таких устройств. В работе [1, с. 61] сказано, что:"… в настоящее время мы располагаем весьма скудной информацией о построении нелинейных кодеров". Перекликается с этим высказыванием и работа [2, с. 3]: "… разрыв между практикой и математической теорией недвоичного помехоустойчивого кодирования не сокращается или сокращается недостаточно быстрыми темпами". Кроме того, не снимается задача увеличения длины генерируемой последовательности при ограничении на применяемую максимальную степень полинома [3].

Получение псевдослучайной последовательности в конечном поле GF(3), основанный на использовании матрицы связей в качестве основного элемента генерации и является **целью статьи**.

Основные проблемы и решения

Основная проблема при диагностировании сложных цифровых устройств заключается в отсутствии средств, которые способны диагностировать третье выходное состояние различных микросхем. Такими устройствами диагностирования могли бы служить сигнатурные анализаторы (СА), основой которых являются регистры сдвига с нелинейными обратными связями, построенными по правилу выбранного полинома.

Но в этом случае связи между регистрами и между сумматорами по модулю три должны быть выполнены с учетом выбранного полинома из конечного поля тройки. Такие регистры принято называть нелинейными, т.е. такие, в цепях обратной связи которых происходят нелинейные преобразования.

Но если для генераторов ПСП с нелинейными связями считается приемлемым применение регистра сдвига, то для многоканального СА [4] по временному критерию такое применение уже считается неприемлемым. Однако для того, чтобы результаты были одинаковыми при одинаковых начальных условиях, и первые, и вторые должны использовать одну и туже теорию – теорию линейных последовательных машин [5-7]. В работе рассматривается разработка математического аппарата функционирования регистров сдвига с нелинейными обратными связями в конечном поле GF(3) и метода получения ПСП на основе использования матрицы связей, применимого в дальнейшем для описания функционирования многоканальных структур, которые в основном являются нелинейными. Для генерирования ПСП в поле GF(3)применяется регистр сдвига с

нелинейными обратными связями, которые принято определять в виде полинома:

$$P(x) = a_n x^n \oplus a_{n-1} x^{n-1} \oplus ... \oplus a_0 x^0$$

где $a_n, a_{n-1}, ..., a_0$ – коэффициенты при аргументах в полиноме; $a_i|_{i=1-n-1} \in \{0, 1, 2\}$; $a_0, a_n \in \{1, 2\}$.

Правила сложения и умножения в конечном поле GF(3) = {0, 1, 2} имеют такой вид (рис. 1):

$\oplus_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$\otimes_3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

Рис. 1. Правила сложения и умножения в конечном поле GF(3)

Матрица связей [3] регистра сдвига определяет связи между разрядами регистра сдвига и изменяется в зависимости от выбранного образующего полинома $P(x)$. В общем случае матрица S связей регистра сдвига имеет вид:

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

Например, для $P(x) = x^5 \oplus_3 x^4 \oplus_3 x^3 \oplus_3 1$

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

При подаче на вход регистра с образующим полиномом $P(x) = x^5 \oplus_3 x^4 \oplus_3 x^3 \oplus_3 1$ логической 1 и последующих сдвигах в регистрах сдвига получится матрица состояний H:

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

Функциональная схема такого классического нелинейного генератора ПСП приведена на рис. 2.

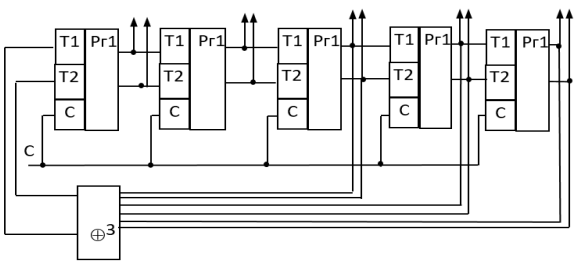

Рис. 2. Функциональная схема НСА с $P(x) = x^5 \oplus_3 x^4 \oplus_3 x^3 \oplus_3 1$

Свободный член a_0 образующего характеристического полинома $P(x) = a_r x^r \oplus_3 a_{r-1} x^{r-1} \oplus_3 \ldots \oplus_3 ax \oplus_3 a_0$ описывает первое состояние h_1 матрицы состояний H [3] и всегда равняется: $h_1 = \|a_0 0 \ldots 0\|$. Например, для $P_1(x) = x^4 \oplus_3 2x^3 \oplus_3 1$ первое состояние $h_1 = \|1000\|$, а для $P_2(x) = x^4 \oplus_3 2x^3 \oplus_3 2$ первое состояние $h_1 = \|2000\|$, в матрице состояний H каждый столбец матрицы связей S всегда представляет один из столбцов матрицы H регистра ПСП.

Практическое применение почти во всех случаях имеют полиномы с максимальным периодом генерации. В этом случае раскрываются все свойства такого генератора. Однако в случае, когда требуется получить последовательность с конкретной усеченной последовательностью могут применяться и полиномы с не максимальным периодом. Для каждого полинома только с максимальным периодом генерации [7] есть своя закономерность кольцевого расположения столбцов матриц связи.

Каждый $S^i = h^k$, т.е. $S^1 = \|h_2\ h_{119}, h_{120}\ h_{121}\ h_{122}\|$.

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

Такая запись соответствует $S^2 = \|h_2\ h_{120}, h_{121}\ h_{121}\ h_{123}\|$ и т.д. Можно практически проверить, что для $P(X)$ = 200011 результирующая формула определения степеней матрицы связей имеет вид:

$$S^i = h_{i+118} h_{i+119} h_{i+120} h_{i+121} h_{i+122}.$$

Для $P(X) \in$ degP(X) =5 с $T = 3^{\text{degP(x)}} - 1$ насчитывается 44 полинома с такими коэффициентами:

200011; 210021; 221001; 201122; 211012; 221222; 200121; 210111; 221101; 201202; 211202; 222022; 201121; 211011; 221221; 202022; 212222; 222122; 201201; 211201; 222021; 202102; 220012; 222212, 202021; 212221; 222121; 202112; 220202; 202101; 220011; 222211; 210002; 220222; 202111; 220201; 200012; 210022; 221002; 210001; 220221; 200122; 210112; 221102;

Для каждого из приведенных полиномов существует своя закономерность размещения столбцов проверочной матрицы H в матрице связей S^i, которые можно использовать для генерирования нелинейной псевдослучайной последовательности. Особый интерес представляет исследование полиномов, у которых свободный член полинома равняется 2 и коэффициенты при аргументах, кроме самого старшего так же равняются 2. В противном случае столбцы матрицы связей получаются путем соответствующего сдвига последнего столбца в нелинейном регистре сдвига с обратными связями. Полученные обобщенные формулы позволяют найти все другие столбцы на основе известного одного путем его сдвига.

Способ, который предлагается [8], может быть реализован, например, с помощью устройства, который включает: блок управления выдачей ПСП; группу из n блоков регистров хранения матриц связей разных степеней и группу r- разрядных выходных состояний. Блок регистров предназначен для

хранения матриц связей. В них занесены матрицы связей соответствующих степеней, каждый столбец которой является одним из состояний матрицы *H*. Блок управления последовательно, за избранным для каждого полинома алгоритмом подает сигналы считывания. В результате чего *r*- разрядные состояния передаются на выход схемы. Каждый блок выдает свои состояния, которые не должны быть повторены, чтобы не нарушить последовательность генерирования ПСП. Блок управления обеспечивает выдачу соответствующих к избранному алгоритму данных. Причем, начинать выдавать r- разрядные данные можно из какого угодно состояния.

Выводы

Предложен метод, представленный в виде полученного выражения, позволяет определить все столбцы матрицы состояний *H* без выполнения расчетов и быть применимым для определения ПСП с использованием примитивного неприведенного характеристического полинома. В предложенном методе отсутствуют обратные связи, как у классического регистра сдвига, и, поэтому, могут генерироваться ПСП для любого выбранного полинома, который удовлетворяет условию получения максимального периода генерации.

СПИСОК ЛІТЕРАТУРИ

1. Блейхут Р. Теория и практика кодов, контролирующих ошибки: Пер. с англ. – М.: Мир, 1986. – 576 с.
2. Муттер В.М. Основы помехоустойчивой телепередачи информации. – Л.: Энергоатомиздат, 1990. – 288 с .
3. Рысованый А.Н., Гоготов В.В. Выбор полиномов для нелинейных регистров сдвига с обратными связями по критерию формирования последовательности максимальной длины // СУНЗ. – Киев ЦНДИ, 2007. – Вып.1.– С. 77 – 79.
4. Ярмолик В.Н. Контроль и диагностика цифровых узлов ЭВМ. – Мн.: Наука и техника. 1988. – 240 с.: ил.
5. Литиков И.П. Кольцевое тестирование цифровых устройств. – М.: Энергоатомиздат, 1990. – 160 с.: ил.
6. Горяшко А.П. Синтез диагностируемых схем вычислительных устройств. – М.: Наука, 1987. – 288 с.
7. Ватолин Д., Ракушняк А., Смирнов М., Юкин В. Методы сжатия данных. – М.: ДИАЛОГ-МИФИ. – 2002. – 384 с.
8. 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. О. В. Козелков,
Державний університет телекомунікацій, Київ
Received (Надійшла) 28.04.2018
Accepted for publication (Прийнята до друку) 16.07.2018

Метод генерування нелінійної псевдовипадкової послідовності без використання зворотних зв'язків

О.М. Рисований

Предметом дослідження в даній статті є процес отримання псевдовипадкової послідовності на основі використання матриці зв'язків в кінцевому полі GF (3). **Мета** – розробити метод отримання псевдовипадкової послідовності в кінцевому полі GF (3), 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. Використовуваними **підходами** є: отримання математичної закономірності генерування нового стану на основі отриманого раніше і отримання схеми генератора, який реалізовує ці закономірності. Отримані наступні **результати**: метод отримання псевдовипадкової послідовності в кінцевому полі GF (3), 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 регістра. Крім того, наведено приклад закономірності кільцевого розташування стовпців матриць зв'язку. В результаті чого запропонована схема генерування послідовності без застосування зворотних зв'язків, як у класичного регістра зрушень. Це дозволяє генерувати послідовності для будь-якого обраного полінома, який задовольняє умові отримання максимального періоду генерації. **Висновки**. Запропоновано метод, представлений у вигляді отриманого виразу, дозволяє визначити всі стовпці матриці станів без виконання розрахунків і бути придатним для визначення ПВП з використанням примітивного неприведеного характеристичного полінома. У запропонованому методі відсутні зворотні зв'язки, як у класичного регістра зсуву, і, тому, можуть генерувати ПВП для будь-якого обраного полінома, який задовольняє умові отримання максимального період генерації.

Ключові слова: псевдовипадкова послідовність, регістр зсуву.

The method of generation of nonlinear Pseudocasual sequence without use of feedbacks

A.N. Rysovaniy

The subject of the research in this article is the process of obtaining a pseudocasual sequence based on the use of the coupling matrix in the finite field GF (3). The goal is to develop a method for obtaining a pseudocasual sequence in a finite field GF (3), based on the use of the coupling matrix as the main generation element. The task: based on the analysis of known approaches to sequence generation, develop a method that, in comparison with a binary shift register, allows increasing the length of the sequence. The approaches used are: obtaining a mathematical pattern for generating a new state on the basis of the previously obtained one and obtaining a generator circuit that implements these regularities. The following results are obtained: the method for obtaining a pseudo-random sequence in a finite field GF (3), based on the use of the coupling matrix as the main generation element. A mathematical apparatus describing the functioning of the shift register with nonlinear feedbacks and its functional scheme is given. The paper shows an example of the formation of the first state of the register. In addition, an example of the regularity of the ring arrangement of columns of coupling matrices is given. As a result, a scheme for generating a sequence without the use of feedbacks is proposed, as in the classical shift register. This allows you to generate sequences for any chosen polynomial that satisfies the condition of obtaining the maximum generation period. Conclusions. The method presented in the form of the obtained expression is proposed, it makes it possible to determine all the columns of the state matrix H without performing calculations and to be applicable to the determination of the SRS using a primitive non-reduced characteristic polynomial. In the proposed method, there are no feedbacks, as in the classical shift register, and therefore, a PRSP can be generated for any chosen polynomial that satisfies the condition for obtaining the maximum generation period.

Keywords. pseudocasual sequence, shift register.