УДК 519.711.4 (075.8)

АЛГЕБРАИЧЕСКИЕ БАЗИСНЫЕ МЕТОДЫ ФОРМИРОВАНИЯ И ОБРАБОТКИ КОДОВЫХ ПОСЛЕДОВАТЕЛЬНОСТЕЙ

Н.В. ЧЕСАЛИН

Белорусский государственный университет информатики и радиоэлектроники
П. Бровки, 6 Минск 220013, Беларусь

Поступила в редакцию 26 октября 2009

Сделан краткий обзор по проблемам генерации и обработки периодических кодовых последовательностей. Предложен новый подход к формированию последовательностей и исследованию их свойств. Методы связаны с построением нормальных базисов в полях Галуа.

Ключевые слова: кодовая последовательность, поле Галуа, нормальный базис, регистр сдвига.

Введение

Периодические кодовые последовательности в настоящее время имеют большое научное и прикладное значение. Они используются, прежде всего, в радиолокационных и навигационных системах, системах мобильной связи и криптографии.

Изучению свойств различных классов периодических последовательностей посвящены, например, монографии [1, 2], в которых, в частности, была приведена классификация периодических последовательностей по некоторым выделенным свойствам. Однако до сих пор остаются нерешенными многие проблемы данной теории, которые сформулированы в виде гипотез [3]. Это, прежде всего, гипотеза о существовании бесконечного числа примитивных трехчленов, о циклических разностных множествах Адамара, о совпадении класса двоичных M-последовательностей с классом периодических последовательностей сдвигового регистра линейной сложности n, обладающих идеальной автокорреляционной функцией и многие другие.

В ряде ситуаций, возникающих в работе компьютеров, в криптографии и многочисленных других областях появляется необходимость использования случайных последовательностей из нулей и единиц. Здесь под случайностью понимается непредсказуемость последовательности. Более точно, требуются последовательности, которые бы выглядели как случайные, но при более глубоком анализе можно было бы найти определенную регулярность. Первоначально были выделены три характеристических свойства двоичных последовательностей над полем Галуа $GF(2)$, характеризующих их случайность. Это сбалансированность, определенное соотношение для числа идущих подряд 1 и 0 и свойство автокорреляции. Затем эти свойства были обобщены на случай последовательностей над произвольным полем Галуа $GF(q)$. Всестороннее изучение M– последовательностей привело к открытию ряда новых свойств, которые продолжили аксиоматику случайных последовательностей.

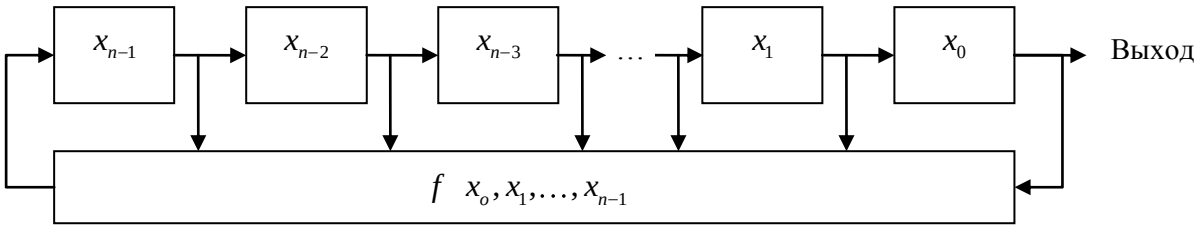

Рис. 1. Блок-схема n-уровневого регистра сдвига с обратной связью конфигурации Фибоначчи

Одним из классических методов задания периодических последовательностей является рекурсия. Физическая реализация процесса построения периодических последовательностей осуществляется с помощью n-уровневого регистра сдвига на триггерах [4]. В настоящее время используются два основных типа регистров сдвига с обратной связью: либо с конфигурацией Фибоначчи, либо с конфигурацией Галуа. На рис. 1 рассмотрена блоковая диаграмма первого процесса. Таким образом, задается линейный регистр сдвига с обратной связью (LFSR), если булева функция $f\ x_0, x_1, ..., x_{n-1}$ является линейным отображением из $0,1^{\ n}$ в $0,1$, и задается нелинейный регистр сдвига с обратной связью (NLFSR) в противном случае. Блоковая диаграмма второго процесса представлена на рис. 2.

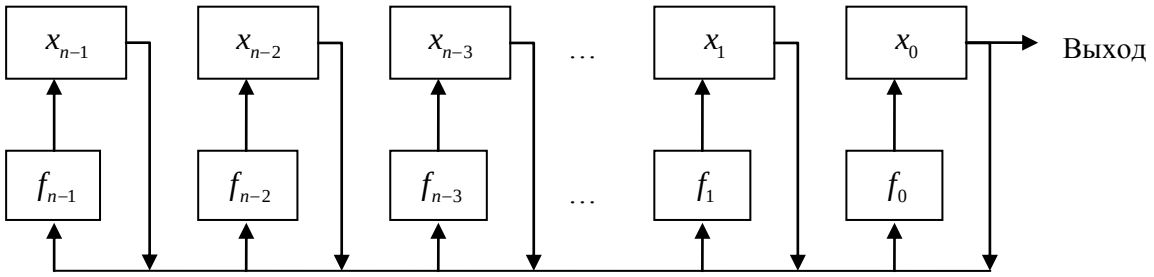

Рис. 2. Блок-схема n-уровневого регистра сдвига с обратной связью конфигурации Галуа

Как видно из приведенных блок-схем конфигурация Галуа концептуально значительно сложнее конфигурации Фибоначчи. В работе [5] было установлено, что для любого NLFSR конфигурации Фибоначчи существует класс соответствующих эквивалентных регистров сдвига конфигурации Галуа. Вопрос обратного соответствия остается открытым, как и построение систематических алгоритмов для синтеза NLFSR, обеспечивающих заданные длинные периоды генерируемых последовательностей. Следует отметить, что для генерации последовательностей также используются конфигурации регистров с обратной связью более общего вида (не обязательно регистры сдвига) [6]. Пример такой конфигурации схематически изображен на рис. 3.

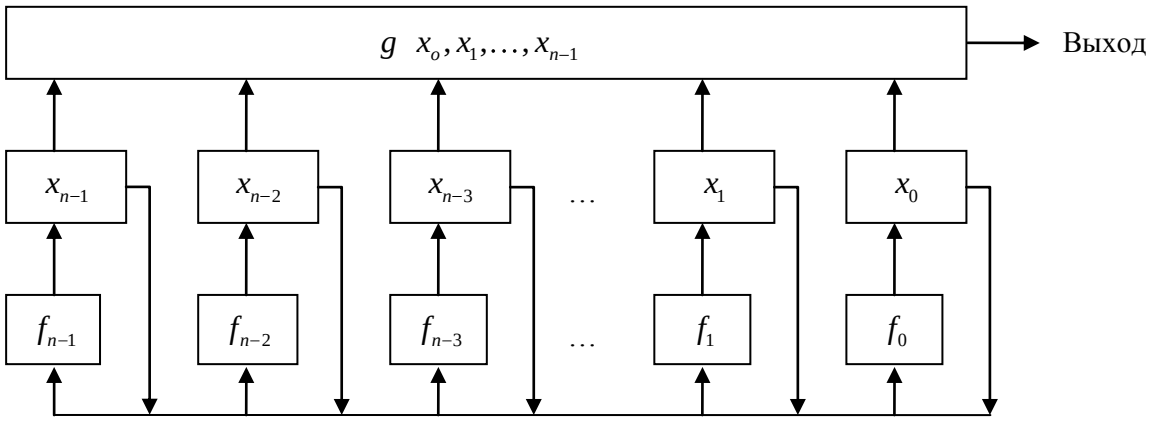

Рис. 3. Блок-схема n-уровневого регистра с обратной связью общей конфигурации

На последних двух блок-схемах g и f_i – булевы функции, действующие из $0,1^n$ в $0,1$, $0 \le i \le n-1$.

Одной из важнейших характеристик генерируемых последовательностей является их линейная сложность (Linear Complexity). Она характеризует степень сложности процесса генерации и криптографические свойства последовательности.

В настоящей работе, используя анализ различных методов формирования кодовых последовательностей, разрабатываются некоторые новые подходы к формированию и изучению важнейших свойств кодовых последовательностей. Основу здесь составляет представление периодических последовательностей элементами подходящего поля Галуа в нормальном базисе и использование базисов Гребнера для линеаризации систем булевых функций и исследования линейной сложности.

Периодические последовательности и нормальные базисы

В поле $GF\ q^n$, рассматриваемом как n-мерное векторное пространство над полем $GF\ q$, где q – степень некоторого простого числа, всегда можно ввести базис вида

$$N = \alpha, \alpha^q, \alpha^{q^2}, ..., \alpha^{q^{n-1}} , \qquad 0 \ne \alpha \in GF\ q^n .$$

Данный базис называется нормальным. Далее, через $T = t_{ij}$ обозначим квадратную матрицу $n \times n$, определенную равенствами

$$\alpha\alpha_i = \sum_{j=0}^{n-1} t_{ij}\alpha_j, \quad 0 \le i \le n-1, \qquad t_{ij} \in GF\ q , \qquad \alpha_i = \alpha^{q^i}.$$

Число ненулевых элементов матрицы T называется сложностью нормального базиса N и обозначается через c_N. Имеет место оценка $c_N \ge 2n-1$. если $c_N = 2n-1$, то базис N называется оптимальным нормальным базисом. Заметим, что для $a \in GF\ q^n$, $a \ne 0$, $aN = a\alpha_0, a\alpha_1, ..., a\alpha_{n-1}$ – также нормальный базис; базисы N и aN называются эквивалентными. Как известно, нормальный базис N эквивалентен своему двойственному базису (совпадает со своим двойственным базисом) тогда и только тогда, когда матрица T – симметрическая (и след $Tr_n\ \alpha^2 = 1$, где α – элемент, порождающий базис N). Оптимальные нормальные базисы были открыты Mullin, Onyszchuk, Vanstone и Wilson [7]. Имеют место следующие результаты.

Теорема 1. (Тип 1 оптимальных нормальных базисов) Предположим, что число $n+1$ – простое и число q является примитивным элементом в $\mathbf{Z}_{n+1}$. Тогда n корней степени $n+1$ из единицы (кроме 1) образуют оптимальный нормальный базис в $GF\ q^n$ над полем $GF\ q$.

Теорема 2. (Тип 2 оптимальных нормальных базисов) Пусть число $2n+1$ – простое и либо число 2 является примитивным элементом в $\mathbf{Z}_{2n+1}$, либо число 2 порождает квадратичные вычеты в $\mathbf{Z}_{2n+1}$ и $2n+1 \equiv 3 \bmod 4$. Тогда $\alpha = \gamma + \gamma^{-1}$ порождает оптимальный нормальный базис в $GF\ 2^n$ над полем $GF\ 2$, где γ – примитивный корень степени $2n+1$ из 1.

В 1992 году Gao и Lenstra доказали, что каждый оптимальный нормальный базис в $GF\ q^n$ над полем $GF\ q$ эквивалентен одному из базисов теорем 1 либо 2. Кроме того, оптимальный нормальный базис N является самодвойственным тогда и только тогда, когда N – оптимальный нормальный базис первого типа и $q = n = 2$ либо N – оптимальный нормальный базис второго типа [8].

Для аналитического описания и исследования свойств периодических функций будем использовать функцию следа $Tr_n\ x = x + x^p + x^{p^2} + \ldots + x^{p^{n-1}}, x \in GF\ p^n$, которая является линейным оператором из $GF\ p^n$ в $GF\ p$, p – простое число.

Для получения различных представлений периодических последовательностей с использованием функции следа оказалось эффективным введение на множестве $\mathbf{Z}_T$ специального отношения эквивалентности, которое разбивает это множество на циклотомические классы C_s, где

$$C_s = s, sq, sq^2, \ldots, sq^{n_s-1}, \qquad sq^{n_s} \equiv s \bmod T,$$

n_s – наименьшее такое натуральное число, T делит $q^n - 1$ и q – степень простого числа. В качестве индекса s циклотомического класса C_s удобно выбирать наименьшее положительное число из данного класса, называемое лидером циклотомического класса. Множество всех лидеров циклотомических классов по модулю T обозначим через L.

Пусть S_T – множество всех T – периодических последовательностей над полем $GF\ p$ и F – множество всех функций из $GF\ p^n$ в $GF\ p$. След-представление периодических последовательностей выражает следующая теорема [2].

Теорема 3. Для любой последовательности $u = u_0, u_1, \ldots, u_{T-1} \in S_T$, T делит $p^n - 1$, существует функция $f\ x \in F$ такая, что

$$f\ x = \sum_{i=1}^{r} Tr_{n_i}\ a_i x^{s_i}, \qquad a_i \in GF\ p^{n_i}, \qquad u_i = f\ \alpha^i,$$

где α – примитивный элемент поля $GF\ p^n$, s_i – лидер циклотомического класса по модулю $p^{n_i} - 1$, n_i – размер циклотомического класса, содержащего s_i, n_i делит n.

Функцию $f\ x$ называют след-представлением r – членной последовательности u. В частности, при $r = 1$ получаем представление M-последовательностей. Однако, следует заметить, что для применения записанной выше формулы на практике требуется описание всех промежуточных полей Галуа и полное описание соответствующих циклотомических классов, что при больших значениях составного числа n является весьма сложной вычислительной задачей.

В данной работе предлагается следующий способ формирования и последующего изучения свойств периодических последовательностей. Для простоты изложения будем рассматривать T – периодические последовательности над полем $GF\ 2$.

Рассмотрим в поле $GF\ 2^T$ нормальный оптимальный базис N, порожденный элементом $\alpha \in GF\ 2^T$. Тогда для любого элемента $u \in GF\ 2^T$ разложение по базису N имеет вид

$$u = u_0\alpha_0 + u_1\alpha_1 + \ldots + u_{T-1}\alpha_{T-1}, \qquad Tr_T\ u = u_0 + u_1 + \ldots + u_{T-1}.$$

Согласно [8] можно выбрать другой нормальный оптимальный базис $M = \beta, \beta^2, \beta^{2^2}, \ldots, \beta^{2^{T-1}}$, $0 \neq \beta \in GF\ 2^T$, являющийся двойственным к N. Как и ранее, вводя обозначение $\beta_i = \beta^{2^i}$, элемент u может быть записан в виде $u = \sum_{i=0}^{T-1} Tr_T\ u\beta_i\ \alpha_i = \sum_{i=0}^{T-1} Tr_T\ u\alpha_i\ \beta_i$.

Каждую последовательность из множества S_T можно рассматривать как последовательность коэффициентов разложения по нормальному базису. Следовательно, таким образом, строится взаимно-однозначное соответствие множества S_T и поля $GF\ 2^T$. С другой стороны, элементы поля $GF\ 2^T$ допускают стандартную запись с помощью некоторого

примитивного многочлена $p\ x$ в виде многочленов степени не выше $T-1$ с коэффициентами из $GF\ 2$. Обозначая через $\tilde{S}_{T,p\ x}$ множество всевозможных последовательностей, образованных коэффициентами описанных выше многочленов, получаем отображение $G: S_T \to \tilde{S}_{T,p\ x}$, которое устанавливает аналитическую связь между основными параметрами данной модели и инвариантные свойства которого позволяют проводить соответствующую классификацию T-периодических последовательностей. Особый интерес представляют спектральные последовательности, полученные применением дискретного преобразования Фурье и их инвариантные свойства, такие как, например, циклотомическая инвариантность [9], постоянство числа ненулевых компонент спектральных последовательностей, исходные последовательности которых имеют фиксированную линейную сложность и др.

Кроме того, имеет место цепочка включений

$$GF\ 2\ \subset GF\ 2^T\ \subset GF\ 2^{2^n-1}$$

при условии, что $2^n-1=Tm$. Это позволяет рассматривать поле $GF\ 2^{2^n-1}$ как m-мерное векторное пространство над полем $GF\ 2^T$ и моделировать двумерные массивы двоичных последовательностей (типа GMW последовательностей и их обобщений).

Как известно, периоды последовательностей, генерируемых нелинейными регистрами, удовлетворяют оценке $T \le 2^n$. Следовательно, минимальным расширением поля $GF\ 2$, необходимым для полного описания генерируемых последовательностей по аналогичной схеме, является поле $GF\ 2^{2^n}$. Задача точного вычисления либо оценки сверху линейной сложности последовательностей в нелинейном случае решается с помощью базисов Гребнера [10] идеалов полиномиальных колец, порожденных нелинейными функциями f, g и f_i, $0 \le i \le n-1$.

Заключение

Данная работа содержит как краткий обзор по проблемам генерации и обработки периодических кодовых последовательностей, так и новый концептуальный подход к формированию и исследованию свойств периодических последовательностей, основанный, прежде всего, на использовании специальных алгебраических базисов в полях Галуа и полиномиальных кольцах. Статистический материал, полученный на основе численного компьютерного анализа примеров по описанной схеме для различных значений числа n занимает достаточно большой объем и ему будет посвящена отдельная публикация.

ALGEBRAIC BASE METHODS OF GENERATION AND PROCESSING OF CODE SEQUENCES

N.V. CHESALIN

Abstract

Different problems of periodic code sequences in finite fields are considered. A new mode of investigation such sequences is developed. In this research normal bases of Galois fields are applied.

Литература

1. *Golomb S.W.* // Shift Register Sequences. 1982. P. 247.
2. *Golomb S.W., Gong G.* // Signal Design for Good Correlation – Wireless Communication, Cryptography, and Radar. 2005. P. 438.
3. *Golomb S.W.* // Solved and Unsolved Problems Springer-Verlag Berlin Heidelberg. 2007. P.1-8.
4. *Биркгоф Г., Барти Т.* Современная прикладная алгебра. М., 1976.
5. *Dubrova E.* // An Equivalence Preserving Transformation from the Fiibonacci to the Galois NLFSRs.2008. P. 1-14.
6. *Chan A.H., Goresky M., Klapper A.* // On the Linear Complexity of Feedback Registers. 1990. Vol. 36, №3. P.640-644.
7. *Mullin R.C., Onyszchuk I.M., Vanstone S.A., Wilson R.M.* // Optimal Normal Bases of $GF(p^n)$ 1989. P.149-161.
8. *Liao Q.Y., Sun Q.* // Normal Bases and Their Dual-Bases over Finite Fields. Vol. 22, № 3. 2006. P.845-848.
9. *Липницкий В.А., Чесалин Н.В.* // 10 БМК. М., 2008.
10. *Кокс Д., Литл Дж., О`Ши Д.* Идеалы, многообразия и алгоритмы. Введение в вычислительные аспекты алгебраической геометрии и коммутативной алгебры. М., 2000.