Math-Net.Ru

Общероссийский математический портал

О. А. Козлитин, Генераторы псевдослучайных последовательностей, использующие регистровые преобразования конечных цепных колец, *Матем. вопр. криптогр.*, 2019, том 10, выпуск 3, 49–65

DOI: <https://doi.org/10.4213/mvk299>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 18.209.158.208

26 апреля 2023 г., 17:54:22

**Генераторы псевдослучайных последовательностей,
использующие регистровые преобразования
конечных цепных колец**

О. А. Козлитин

ООО «Центр сертификационных исследований», Москва

Получено 11.VII.2019

Посвящается светлой памяти Михаила Михайловича Глухова

Аннотация. В основу статьи положен доклад, сделанный на конференции STCrypt'2018 и содержащий обзор работ автора, касающихся синтеза генераторов псевдослучайных последовательностей. В этих работах найден максимум $L_m(R)$ длин циклов в цикловых записях m -мерных полиномиальных подстановок над кольцом Галуа R , предложен алгоритм, строящий полиномиальные подстановки, в цикловой записи которых содержится цикл длины $L_m(R)$, а также получены оценки периодов, рангов и частот знаков на циклах выходных последовательностей самоуправляемых 2-линейных регистров сдвига. В статье анонсирован новый результат о периодических свойствах полиномиальных регистров сдвига над кольцом Галуа, а именно утверждается, что над кольцом R существуют полиномиальные регистры сдвига длины m , в графе переходов состояний которых содержится цикл длины $L_m(R)$.

Ключевые слова: полиномиальный генератор, полиномиальный регистр сдвига, полилинейный регистр сдвига, полилинейная рекуррентная последовательность

Pseudorandom sequence generators based on shift registers over finite chain rings

O. A. Kozlitin

Certification Research Center, LLC, Moscow

Abstract. This article is based on a report made at the conference CTCrypt'2018. The paper contains an overview of the author's results related to the synthesis of pseudorandom sequence generators. For arbitrary m and for Galois ring R the maximum length $L_m(R)$ of cycles of bijective polynomial transformations of module R^m is calculated. An algorithm is proposed that constructs polynomial transformations with a cycle of length $L_m(R)$. Some estimates of the periods and ranks of the output sequences of self-controlled 2-dimensional linear shift registers (2-LFSR) are obtained. The frequencies of occurrence of signs on the cycles of the output sequences of 2-LFSR are investigated. A new result is announced in the article, consisting of the fact that over Galois ring R there are polynomial shift registers of length m , the state transition graph of which contains a cycle of length $L_m(R)$.

The author devotes this article to the blessed memory of M. M. Glukhov.

Keywords: polynomial generator, polynomial shift register, multidimensional linear shift register, multidimensional linear recurrence sequence

1. Введение

Применение регистровых преобразований вектор-строк длины m над конечным коммутативным кольцом R (которые далее для краткости будут именоваться *регистровыми преобразованиями кольца R*) – один из возможных способов выработки псевдослучайных последовательностей (ПСП) с заданными криптографическими свойствами. Стандартным примером генератора, использующего регистровые преобразования, является линейный регистр сдвига (ЛРС) с нелинейной функцией выхода, называемый также *фильтрующим генератором* (см. рисунок). Существует ряд параметров и свойств фильтрующего генератора, характеризующих его криптографические качества. Среди них периодические свойства последовательности состояний, а также периодические, статистические и сложностные свойства (ранг) выходной последовательности. Изучению этих параметров и свойств посвящено большое количество статей. Не претендуя на полноту, упо-

Рис. Фильтрующий генератор

мянем в этой связи работы В.И. Нечаева, Н.М. Коробова, И.Е. Шпарлинского, А.А. Нечаева, В.Л. Куракина, А.С. Кузьмина, А.В. Михалева, О.В. Камловского, Д.Н. Былкова, Г.Б. Маршалко, Р. Рупшеля, Н. Цирлера, В. Миллса.

Целью настоящей работы является описание двух способов обобщения классического ЛРС. Первый способ состоит в использовании генератора с полиномиальной функцией обратной связи (*полиномиального генератора*). Частным случаем полиномиального генератора является так называемый *полиномиальный регистр сдвига*. Одномерный полиномиальный генератор (*полиномиальный конгруэнтный генератор*, ПКГ) над кольцом вычетов изучался в работах В.С. Анашина [14] и М.В. Ларина [12]. Основы математического аппарата, необходимого для исследования периодических свойств полиномиальных преобразований над произвольным конечным коммутативным кольцом с единицей, были разработаны В.Е. Викторенковым (см. [1, 2]). Цикловую структуру ПКГ над произвольным кольцом Галуа изучали Д.М. Ермилов и О.А. Козлитин (см. [4, 5]). В разделе 2 настоящей работы обсуждаются периодические свойства одномерного полиномиального генератора над конечным *цепным* кольцом (конечным коммутативным локальным кольцом главных идеалов), а также полиномиального регистра сдвига над кольцом Галуа.

Второй способ обобщения заключается в применении нескольких линейных функций обратной связи. Один из подходов к реализации этой идеи – использование многомерного (k -мерного) линейного регистра сдвига (k -ЛРС). Первоначально k -ЛРС был предложен японскими математиками Т. Номура и А. Фукуда как кодер и декодер рассмотренного этими авторами двумерного циклического кода [15].

Позже многомерный регистр сдвига изучался в работах А.А. Нечаева, А.В. Михалева, В.Л. Куракина и А.С. Кузьмина с точки зрения его возможного использования в качестве генератора ПСП (см., например, [11]). В 2003 г. вышла работа А.А. Нечаева [13], положившая начало исследованиям так называемого *самоуправляемого k -линейного регистра сдвига*. В разделе 3 настоящей работы рассматриваются некоторые криптографические свойства выходной последовательности самоуправляемого 2-линейного регистра сдвига над кольцом Галуа (период, ранг, ранги разрядных последовательностей, частотные характеристики). Обсуждаются способы выбора функции самоуправления и функции выхода, обеспечивающие оптимальные значения параметров выходной последовательности.

2. Полиномиальный генератор

Пусть R – конечное коммутативное кольцо с единицей e , $\mathbf{z} = (z_1, z_2, \dots, z_m)$ – строка переменных над кольцом R . Рассмотрим семейство полиномов

$$f_1(\mathbf{z}), \dots, f_m(\mathbf{z}) \in R[\mathbf{z}] \quad (1)$$

и преобразование $f : R^m \rightarrow R^m$, определенное равенством

$$f(\mathbf{z}) = (f_1(\mathbf{z}), \dots, f_m(\mathbf{z})). \quad (2)$$

В этой ситуации преобразование f будем называть *многомерным (m -мерным) полиномиальным преобразованием над кольцом R с координатными полиномами (1)*. Генератор, функция обратной связи которого задана равенством (2), будем называть *многомерным (m -мерным) полиномиальным генератором*.

Рассмотрим конечное цепное кольцо R и величину $L_m(R)$ – максимум длин циклов m -мерных биективных полиномиальных преобразований (*m -мерных полиномиальных подстановок*) над R . Для краткости вместо $L_1(R)$ будем писать $L(R)$. Оценим сверху величину $L(R)$.

Пусть J – нильрадикал кольца R , порожденный (как главный идеал) элементом π : $J = \pi R$, n – индекс нильпотентности кольца R , $f(z) \in R[z]$ – полином, задающий, вообще говоря, небиективное преобразование кольца R , G_f – граф этого полиномиального преобразования. Вершины графа G_f , принадлежащие циклам, будем называть *циклическими*. Следуя терминологии В.Е. Викторенкова [1], назовем циклическую вершину *особой*, если выполнено соотношение

$$f'(a) \equiv 0 \pmod{J},$$

и *неособой* в противном случае (здесь $f'(z)$ – введенная стандартным образом производная полинома f , см., например, [3]). Цикл называется *неособым*, если он не содержит особых вершин, и *особым* в противном случае.

Нормой элемента $r \in R$ называется максимальное значение $k \in \{0, 1, \dots, n\}$ со свойством $r \in \pi^k R$. Пусть p – характеристика поля $\bar{R} = R/J$, $\varepsilon = \|pe\|$. Величина ε называется *индексом ветвления* кольца R . Для колец Галуа $\varepsilon = 1$. Для конечных цепных колец простой характеристики $\varepsilon = n$. Для произвольного конечного цепного кольца $1 \leq \varepsilon \leq n$.

Обозначим через $\circ$ операцию *композиции* преобразований. Пусть $f^{[0]}$ – тождественное преобразование,

$$f^{[m]} = f \circ f \circ \dots \circ f,$$

где f повторяется m раз. Всюду далее будем считать, что вершина a принадлежит неособому циклу. Пусть $t_s(a)$ есть минимальное натуральное число t , обладающее свойством

$$f^{[t]}(a) \equiv a \pmod{J^s}.$$

Очевидно, что $t_s(a) \mid t_{s+1}(a)$ для всех $s \in \{1, \dots, n-1\}$.

Изучим строение последовательности

$$t_1(a), t_2(a), \dots, t_n(a).$$

Пусть φ – естественный эпиморфизм $R \rightarrow \bar{R} = R/J$, элемент $\bar{\alpha} \in \bar{R}$ (полином $\bar{f}(z) \in \bar{R}[z]$) – образ элемента $\alpha \in R$ (полинома $f(z) \in R[z]$) под действием φ . Введем обозначения

$$F_s = f^{[t_s(a)]}, \quad \alpha_s = F'_s(a) \in R^*, \quad s \in \{1, 2, \dots, n\},$$

$$d_s(a) = t_{s+1}(a)/t_s(a), \quad s \in \{1, 2, \dots, n-1\},$$

$$\sigma = \min\{s \in \{1, 2, \dots, n\} : \bar{\alpha}_s = \bar{e}\},$$

$$\delta_s(a) = \text{ord } \bar{\alpha}_s, \quad s \in \{1, 2, \dots, \sigma-1\},$$

где $\text{ord } \bar{\alpha}_s$ – мультипликативный порядок элемента $\bar{\alpha}_s \in \bar{R}^*$.

Теорема 1 ([8]). *Справедливы следующие утверждения:*

$$1) \quad d_1(a) \cdot d_2(a) \cdots d_{\sigma-1}(a) \mid \delta_1(a),$$

2) если $\epsilon = \min\{\epsilon, p-1\}$, то

$$d_\sigma(a) \cdot d_{\sigma+1}(a) \dots d_{n-1}(a) \mid p^{\nu(a)},$$

где $\nu(a) = \lceil (n - 2^\rho \sigma) / \epsilon \rceil + \rho$ и $\rho \in \mathbb{N}_0$ – минимальное число со свойством $2^\rho \sigma > \epsilon$. В частности,

$$t_n(a) \mid t_1(a) \cdot \delta_1(a) \cdot p^{\nu(a)}.$$

Пусть R – конечное цепное кольцо, отличное от кольца Галуа, $L(G_f)$ – максимум длин циклов в графе G_f , $\bar{R} = GF(q)$. Справедливы следующие утверждения.

Теорема 2 ([8]). Пусть $n \geq 4$. Если $q \neq p > 2$, то

$$L(G_f) \leq L(G_{\bar{f}}) \cdot (q-1) \cdot p^{\lfloor \frac{n}{2} \rfloor + 1}.$$

Если $q = p > 2$, то

$$L(G_f) \leq L(G_{\bar{f}}) \cdot p^{\lfloor \frac{n}{2} \rfloor + 2}.$$

Теорема 3 ([8]). Пусть $n \geq 5$, $\sigma \in \{1, 2\}$. Если $q = p = 2$, то

$$t_n(a) \leq 2^{n-\epsilon+1+\lfloor \log_2 \epsilon \rfloor}.$$

Если $q > p = 2$, то

$$t_n(a) \leq q \cdot (q-1) \cdot 2^{n-\epsilon+\lfloor \log_2(\epsilon-1) \rfloor}.$$

Напомним, что если $BP(R)$ есть множество всех биективных полиномиальных преобразований кольца R , то

$$L(R) = \max_{f \in BP(R)} L(G_f).$$

Пусть $n \geq 5$, $S = GR(q^n, p^n)$, R – конечное цепное кольцо мощности q^n со свойствами $\bar{R} = GF(q)$ и $\epsilon \geq 2$. В первом столбце приведенной ниже таблицы перечислены рассматриваемые случаи, во втором – точные значения величины $L(S)$, в третьем – верхние оценки величины $L(R)$.

	S	R
$p = 2, q = p$	2^n	2^{n-1}
$p = 2, q > p$	$q \cdot (q-1) \cdot 2^{n-2}$	$q \cdot (q-1) \cdot 2^{n-3}$
$p > 2, q = p$	p^n	$p^{\lfloor \frac{n}{2} \rfloor + 3}$
$p > 2, q > p$	$q \cdot (q-1) \cdot p^{n-2}$	$q \cdot (q-1) \cdot p^{\lfloor \frac{n}{2} \rfloor + 1}$

Суммируя сказанное, получаем следующее утверждение.

Теорема 4 ([8]). Пусть $n \geq 7$, $S = GR(q^n, p^n)$, R – конечное цепное кольцо мощности q^n со свойством $\bar{R} = GF(q)$. Тогда $L(R) \leq L(S)$. Равенство $L(R) = L(S)$ выполняется тогда и только тогда, когда $R \cong S$.

Теорему 4 можно сформулировать следующим образом: при переходе от кольца Галуа S к конечному цепному кольцу R той же мощности и с тем же индексом нильпотентности величина $L(\cdot)$ не возрастает. Это означает, что с точки зрения периодических свойств полиномиального генератора в классе конечных цепных колец рассматривать алгебраические структуры более сложные, чем кольца Галуа, нецелесообразно.

Для произвольного $m \in \mathbb{N}$ и кольца Галуа R доказана следующая теорема.

Теорема 5 ([9]). Для всякого собственного кольца Галуа $R = GR(q^n, p^n)$, т. е. кольца Галуа мощности q^n и характеристики p^n , отличного от конечного поля и от примарного кольца вычетов, верно равенство $L_m(R) = q^m(q^m - 1)p^{n-2}$.

Полиномиальные подстановки вида (2), обладающие циклом максимальной возможной длины $L_m(R) = q^m(q^m - 1)p^{n-2}$, назовем МДЦ-подстановками. В [9] в случае $p > 2$ построен и обоснован алгоритм, который порождает широкий класс МДЦ-подстановок. Аналогичный алгоритм удалось построить и в случае $p = 2$. Особенность предложенного алгоритма состоит в том, что он позволяет строить регистровые полиномиальные МДЦ-подстановки, т. е. МДЦ-подстановки вида

$$f(z_1, z_2, \dots, z_m) = (z_2, z_3, \dots, z_m, f_m(z_1, z_2, \dots, z_m)).$$

Таким образом, анонсируется следующий результат о полиномиальных регистрах сдвига над кольцом Галуа.

Теорема 6. Для всякого собственного кольца Галуа $R = GR(q^n, p^n)$ существует автономный полиномиальный регистр сдвига длины m , граф переходов состояний которого обладает циклом длины $L_m(R) = q^m(q^m - 1)p^{n-2}$.

Регистры сдвига, о которых идет речь в теореме 6, можно назвать полиномиальными регистрами сдвига максимального периода. В теории полиномиальных рекуррент эти регистры играют такую же роль, какую играют в теории линейных рекуррент линейные регистры сдвига максимального периода.

3. k -линейный регистр сдвига

В этом разделе обсуждаются свойства так называемого k -линейного регистра сдвига, $k \geq 2$, с точки зрения его возможного использования в качестве генератора ПСП. Сначала кратко охарактеризуем основные результаты, составляющие содержание раздела.

Пусть I – унитарный идеал кольца $R[x_0, x_1, \dots, x_{k-1}]$, т.е. идеал, порожденный унитарными многочленами $F_0(x_0), F_1(x_1), \dots, F_{k-1}(x_{k-1})$, а u есть k -линейная рекуррентная последовательность (k -ЛРП), аннулируемая идеалом I . Множество всех k -ЛРП над кольцом R , аннулируемых идеалом I , обозначим через $L_R(I)$ и назовем ЛРП-семейством. Пусть $T(I)$ – период идеала I , а $T(u)$ – период рекурренты u . Тогда $T(u) \leq T(I)$. В отдельных случаях (при $k = 2$ и $R = \mathbb{Z}_2$) полностью описана цикловая структура ЛРП-семейства $L_R(I)$. Построено большое семейство последовательностей $u \in L_R(I)$, обладающих свойством $T(u) = T(I)$.

Пусть $k = 2$ и 2-ЛРП u индуцирует начальное заполнение самоуправляемого 2-ЛРС. Обозначим через β функцию самоуправления, а через ψ – функцию выхода этого автомата. Понятно, что период $T(\gamma)$ выходной последовательности γ определяется не только начальным заполнением 2-ЛРС, но также функциями β и ψ . Легко показать, что $T(\gamma) \leq T(u)$. Автором построены большие классы функций β и ψ , для которых $T(\gamma) = T(u)$. Для функций β и ψ из этих классов описаны частотные свойства и ранг последовательности γ .

Изложим результаты, относящиеся к использованию k -ЛРС в качестве генератора ПСП, более подробно. Сначала рассмотрим случай $k = 2$. Неформально 2-ЛРС можно описать следующим образом. Пусть R – конечное коммутативное кольцо с единицей, $F_0(x)$ и $F_1(x)$ – унитарные полиномы степеней m_0 и m_1 соответственно. Пусть R_{m_0, m_1} – матрица над R размера $m_0 \times m_1$ и $w(0) \in R_{m_0, m_1}$. Рассмотрим отображение

$$u : \mathbb{N}_0^2 \rightarrow R$$

такое, что

$$u[\overline{0, m_0 - 1} \times \overline{0, m_1 - 1}] = w(0),$$

т.е. на пересечении $(i + 1)$ -й строки и $(j + 1)$ -го столбца матрицы $w(0)$ находится элемент $u(i, j)$, $i = 0, 1, \dots, m_0 - 1$, $j = 0, 1, \dots, m_1 - 1$, и в следующей таблице каждый столбец есть линейная рекуррентная последовательность (ЛРП) с характеристическим многочленом $F_0(x)$, а каждая строка – ЛРП с характеристическим многочленом $F_1(x)$:

$u(0, 0)$	$u(0, 1)$	$u(0, 2)$	$\dots$	$u(0, j)$	$\dots$
$u(1, 0)$	$u(1, 1)$	$u(1, 2)$	$\dots$	$u(1, j)$	$\dots$
$u(2, 0)$	$u(2, 1)$	$u(2, 2)$	$\dots$	$u(2, j)$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$
$u(i, 0)$	$u(i, 1)$	$u(i, 2)$	$\dots$	$u(i, j)$	$\dots$
$\dots$	$\dots$	$\dots$	$\dots$	$\dots$	$\dots$

По таблице движется прямоугольное «окно» размерами $m_0 \times m_1$ ячеек. Заполнение $w(i)$ окна есть заполнение 2-ЛРС в i -й такт работы. Далее будем придерживаться следующих соглашений:

- (1) Закон движения окна задан двоичной *управляющей последовательностью* δ . Если $\delta(i) = 0$, окно сдвигается на один шаг вниз. Если $\delta(i) = 1$, окно сдвигается на один шаг вправо.
- (2) Последовательность δ либо подается на автомат извне, либо всякий ее знак $\delta(i)$ получается из текущего заполнения окна при помощи *функции самоуправления* β :

$$\delta(i) = \beta(w(i)), \quad i = 0, 1, 2, \dots$$

В первом случае автомат называется неавтономным и обозначается через $\mathfrak{A}$. Во втором случае автомат называется самоуправляемым и обозначается через $\mathfrak{A}^\beta$.

- (3) Знак $\gamma(i)$ выходной последовательности γ получается из текущего заполнения $w(i)$ с помощью линейной функции выхода ψ :

$$\gamma(i) = \psi(w(i)), \quad i = 0, 1, 2, \dots$$

Далее рассматриваем случай «квадратного» 2-ЛРС, т.е. ситуацию $m_0 = m_1 = m$. Пусть φ_0 и φ_1 суть частичные функции перехода автомата $\mathfrak{A}$:

$$w(i+1) = \varphi_{\beta(w(i))}(w(i)),$$

$r, n \in \mathbb{N}$, $R = GR(q^n, 2^n)$, $q = 2^r$, $m \geq 2$, $F_0(x) = F_1(x) = F(x)$ есть многочлен максимального периода $(q^m - 1)2^{n-1}$, $\deg F(x) = m$. Предположим, что функция выхода ψ возвращает содержимое некоторой фиксированной ячейки матрицы-аргумента:

$$\psi(z) = z_{k,l},$$

где $z = (z_{i,j}) \in R_{m,m}$.

Положим $\tau = q^m - 1$ и рассмотрим автоморфизм σ R -бимодуля $R_{m,m}$, определенный равенством

$$\sigma = \varphi_0^{2^{n-2}(\tau-1)} \circ \varphi_1^{2^{n-2}(\tau+1)}.$$

Пусть θ – корень многочлена F в кольце $S = GR(q^{mn}, 2^n)$, $\alpha = \theta^{2^{n-2}(\tau-1)}$, $\mu_j(x)$ – минимальный многочлен элемента $\bar{\alpha}^{q^j-1}$ над полем $\bar{R}$, $j = 1, 2, \dots, m-1$. Тогда характеристический многочлен автоморфизма σ имеет следующее каноническое разложение:

$$\chi_\sigma(x) = G_0(x)G_1(x) \dots G_{m-1}(x),$$

где $\bar{G}_0(x) = (x-1)^m$, $\bar{G}_j(x) = \mu_j(x)$, $j = 1, 2, \dots, m-1$. Это разложение индуцирует однозначное представление каждого состояния w автомата $\mathfrak{A}^\beta$

$$w = a_0 + a_1 + a_2 + \dots + a_{m-1},$$

где $a_j \in \text{Ker } G_j(\sigma)$, $j = 0, 1, \dots, m-1$. Назовем *типом состояния* w следующий вектор:

$$\text{typ } w = (n - \|a_0\|, n - \|a_1\|, \dots, n - \|a_{m-1}\|) \in \{0, 1, \dots, n\}^m.$$

Если $e_{i,j}$ есть матричная единица (матрица, в которой на пересечении $(i+1)$ -й строки и $(j+1)$ -го столбца стоит единица, а на остальных позициях – нули), то имеет место равенство

$$a_0 = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} v(i+j) e_{i,j},$$

где $v \in L_R(F)$. В этой ситуации будем говорить, что последовательность v *ассоциирована* с матрицей w .

Построим функцию самоуправления β . Каждой функции $f: \bar{R}^m \rightarrow \mathbb{Z}_2$ со свойством $f(0, 0, \dots, 0) = 0$ поставим в соответствие ее *вес*:

$$|f| = |\{\alpha \in \bar{R}^m : f(\alpha) = 1\}|.$$

Рассмотрим отображение ξ , сопоставляющее каждому вектору $\mathbf{t} \in \{0, 1, \dots, n\}^m$ некоторую функцию $\xi(\mathbf{t}) = f_{\mathbf{t}}$, обладающую свойством $(|f_{\mathbf{t}}|, \tau) = 1$. Если $w \in R_{m,m}$ и $\mathbf{t} = \text{typ } w$, то положим

$$\beta(w) = f_{\mathbf{t}}(\bar{v}(0), \bar{v}(1), \dots, \bar{v}(m-1)),$$

где $v \in L_R(F)$ есть ЛРП, ассоциированная с w . Далее рассматриваем лишь такие начальные заполнения $w = w(0)$, для которых $\bar{a}_0 \neq 0$.

Выражение «свойство выполняется почти для всех состояний» означает, что доля состояний, для которых свойство не выполняется, есть $o(1)$, $m \rightarrow \infty$. Пусть ε_j есть индикатор неравенства $a_j \neq 0$, $j = 1, 2, \dots, m-1$. В [10] сформулированы и доказаны следующие утверждения:

(1) Если $\tau_j = \tau / (q^{(m,j)} - 1)$, $j = 1, 2, \dots, m-1$, то

$$T(\gamma) = 2^{n-1} \tau \cdot [\tau_1^{\varepsilon_1}, \tau_2^{\varepsilon_2}, \dots, \tau_{m-1}^{\varepsilon_{m-1}}] \leq 2^{n-1} \cdot \frac{\tau^2}{q-1}. \quad (3)$$

(2) Неравенство (3) обращается в равенство тогда и только тогда, когда

$$\text{НОД}(\varepsilon_1, 2\varepsilon_2, 3\varepsilon_3, \dots, (m-1)\varepsilon_{m-1}, m) = 1.$$

Почти для всех начальных состояний $w(0)$ имеет место соотношение

$$T(\gamma) = O(q^{2m}), \quad m \rightarrow \infty.$$

(3) Количество $N(\mathfrak{A}^\beta)$ начальных состояний, для которых

$$T(\gamma) = 2^{n-1} \cdot \frac{\tau^2}{q-1},$$

выражается формулой

$$N(\mathfrak{A}^\beta) = (q^m - 1) \sum_{d|m} \mu(m/d) q^{m(nd-1)},$$

где μ есть функция Мёбиуса. Почти все начальные состояния принадлежат циклам максимальной длины.

Пусть $t = \min\{\|a_1\|, \|a_2\|, \dots, \|a_{m-1}\|\}$. Рассмотрим разложение Тейхмюллера выходной последовательности γ :

$$\gamma = \gamma_0 + 2\gamma_1 + \dots + 2^{n-1}\gamma_{n-1}.$$

Обсудим линейную сложность (ранг) и частотные характеристики последовательности γ_t . Обозначим через $p_z(\gamma_t)$ относительную частоту встречаемости элемента z на цикле последовательности γ_t . В [10] сформулированы и доказаны следующие утверждения:

- (1) Если $J = \{j \in \overline{1, m-1} : \|a_j\| = t\}$, то существует такая ЛРП $v \in L_R(F)$, что $\bar{v} \neq 0$ и выполняется следующее двойное неравенство:

$$m \cdot \sum_{j \in J} \tau_j \leq \text{rang } \gamma_t - \text{rang } v_t \leq m \cdot |J| \cdot \tau,$$

где v_t есть t -й разряд в разложении Тейхмюллера последовательности v . Таким образом,

$$\text{rang } \gamma_t = O(m^2 q^m), \quad m \rightarrow \infty.$$

- (2) Если $n = 1$, то

$$m + m \sum_{j=1}^{m-1} \tau_j \varepsilon_j \leq \text{rang } \gamma \leq m + m\tau \sum_{j=1}^{m-1} \varepsilon_j.$$

Если $\varepsilon_j = 1$ для всех $j \in \mathbb{Z}_m^*$, то

$$\text{rang } \gamma \geq m + m\varphi(m) \cdot \frac{q^m - 1}{q - 1},$$

где φ есть функция Эйлера.

- (3) Пусть $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{m-1} = 1$, $t = \|a_j\|$, $q > 2$,

$$C = \left(\frac{q-1}{q-2} \sqrt{q} + \frac{q-1}{q^{(m,j)}-1} \right) \cdot \left(1 + \frac{\sqrt{q}}{q-2} \right)^{-1}$$

и начальное состояние $w(0)$ принадлежит циклу максимальной длины. Тогда для всякого $z \in \bar{R} = GF(q)$ справедливы следующие утверждения:

а) если $(q-1, \tau_j) < C$, то

$$\left| p_z(\gamma_t) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q \cdot \tau^2} \right| < \frac{1}{2(q^m - 1)} + \frac{(\sqrt{q} + 1)(q-1)}{q^m - 1} q^{m/2-1},$$

б) если $(q-1, \tau_j) \geq C$, то

$$\left| p_z(\gamma_t) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q \cdot \tau^2} \right| < \frac{1}{2(q^m - 1)} + \frac{(q-1)^2}{q^m - 1} q^{m/2-1}.$$

(4) Пусть $\varepsilon_1 + \varepsilon_2 + \dots + \varepsilon_{m-1} = 1$, $t = \|a_j\|$ и $(q-1) \mid \tau_j$. Тогда для всех $z \in \bar{R}$

$$\left| p_z(\gamma_t) - \frac{\tau^2 - (1-q)^{\delta_{z,0}}}{q\tau^2} \right| \leq \frac{1}{2\tau} + \frac{q-1}{q} \cdot \left(\frac{1}{\tau_j} - \frac{1}{\tau} \right) \cdot q^{m/2}.$$

Пусть теперь $R = \mathbb{Z}_2$, $\vec{w} = (w(0), w(1), \dots, w(i), \dots)$. Очевидно, что $T(\vec{w}) \leq \tau^2$. Функцию

$$\beta : R_{m,m} \rightarrow \mathbb{Z}_2$$

назовем *оптимальной*, если при условии $a_0 \neq 0$ равенство $T(\vec{w}) = \tau^2$ эквивалентно равенству

$$\text{НОД}(\varepsilon_1, 2\varepsilon_2, 3\varepsilon_3, \dots, (m-1)\varepsilon_{m-1}, m) = 1.$$

Дальнейшая цель – описать оптимальные функции β .

Напомним, что $I = (F, F)$ – унитарный идеал кольца $R[x_0, x_1]$. Циклом, которому принадлежит рекуррента $u \in L_R(I) = L_R(F, F)$, называется множество

$$C = C(u) = \{x_0^{t_0} x_1^{t_1} u \mid (t_0, t_1) \in \mathbb{N}_0^2\}.$$

ЛРП-семейство $L_R(F, F)$ состоит из циклов. Положим

$$\mathfrak{F} = \{0, 1, \dots, m-1\} \times \{0, 1, \dots, m-1\}.$$

Если рекурренты u_1 и u_2 принадлежат одному и тому же циклу, то

$$\text{typ } u_1[\mathfrak{F}] = \text{typ } u_2[\mathfrak{F}].$$

Типом цикла C называется вектор $\text{typ } C = \text{typ } u[\mathfrak{F}]$. Положим

$$C[\mathfrak{F}] = \{u[\mathfrak{F}] \mid u \in C\},$$

$$V = \{(1, c_1, \dots, c_{m-1}) \in \{0, 1\}^m \mid \text{НОД}(c_1, 2c_2, 3c_3, \dots, (m-1)c_{m-1}, m) = 1\}.$$

Теорема 7 ([6]). Функция самоуправления β оптимальна тогда и только тогда, когда для каждого цикла $C \subset L_R(F, F)$ со свойством $\text{typ } C \in V$ существует такая булева функция $f(x_1, x_2, \dots, x_m)$, что $f(0, 0, \dots, 0) = 0$, $(|f|, \tau) = 1$ и

$$\forall w \in C[\mathfrak{F}] : \quad \beta(w) = f(v(0), v(1), \dots, v(m-1)),$$

где $v \in L_R(F)$ – ЛРП, ассоциированная с w .

Пусть функция $\psi_{i,j} : R_{m,m} \rightarrow R$ определена равенством

$$z = \sum_{i=0}^{m-1} \sum_{j=0}^{m-1} \psi_{i,j}(z) e_{i,j}, \quad z \in R_{m,m}.$$

Существуют такие число $t \in \{1, 2, \dots, m^2\}$ и множество пар

$$(i_1, j_1), (i_2, j_2), \dots, (i_t, j_t) \in \mathfrak{F},$$

что

$$\psi = \sum_{k=1}^t \psi_{i_k, j_k}.$$

Пусть $s \in \{0, 1, \dots, m-1\}$. Рассмотрим полином

$$\chi_s(x) = \sum_{k=1}^t x^{2^s i_k + j_k} \in R[x].$$

Типом линейной функции ψ назовем вектор

$$\text{typ } \psi = (\varepsilon'_0, \varepsilon'_1, \dots, \varepsilon'_{m-1}),$$

где

$$\varepsilon_s = \begin{cases} 0, & \text{если } F(x) \mid \chi_s(x), \\ 1 & \text{в противном случае,} \end{cases} \quad s \in \{0, 1, \dots, m-1\}.$$

Теорема 8 ([6]). Пусть β – оптимальная функция самоуправления,

$$\text{typ } w(0) = (\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{m-1}) \in V,$$

ψ – линейная функция, $\text{typ } \psi = (\varepsilon'_0, \varepsilon'_1, \dots, \varepsilon'_{m-1})$,

$$\lambda_s = \varepsilon'_s \varepsilon_s, \quad s = 0, 1, \dots, m-1.$$

Тогда

$$T(\gamma) = [\tau^{\lambda_0}, (\tau\tau_1)^{\lambda_1}, (\tau\tau_2)^{\lambda_2}, \dots, (\tau\tau_{m-1})^{\lambda_{m-1}}],$$

где $\tau_s = \tau/(2^{(m,s)} - 1)$, $s = 1, 2, \dots, m-1$. Равенство $T(\gamma) = \tau^2$ выполняется тогда и только тогда, когда

$$\text{НОД}(\lambda_1, 2\lambda_2, \dots, (m-1)\lambda_{m-1}, m) = 1.$$

Если $\nu \in L_R(F, F)$, назовем *длиной цикла* $C(\nu)$ величину $T(\nu) = |C(\nu)|$, т. е. *период* последовательности ν . *Цикловым типом* семейства $L_R(F, F)$ называется полином

$$C_F(y) = \sum_{t \geq 1} C_{F,t} \cdot y^t,$$

где $C_{F,t}$ есть число циклов длины t в семействе $L_R(F, F)$.

Теорема 9 ([6]). Пусть $R = \mathbb{Z}_2$, $F(x)$ есть многочлен максимального периода $\tau = 2^m - 1 \geq 3$ и $\tau_d = \tau / (2^d - 1)$ для каждого $d \mid m$. Тогда:

1. Если $m = d_1 > d_2 > d_3 > \dots > d_l = 1$ суть все натуральные делители числа m , то длины циклов семейства $L_R(F, F)$ образуют серию

$$1 < \tau = \tau\tau_{d_1} < \tau\tau_{d_2} < \dots < \tau\tau_{d_l} = \tau^2.$$

2. Пусть $\nu \in L_R(F, F)$ и $\text{typ } \nu[\mathfrak{F}] = (\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{m-1})$. Равенство $T(\nu) = 1$ имеет место тогда и только тогда, когда $\nu = 0$. Равенство $T(\nu) = \tau\tau_d$ выполняется тогда и только тогда, когда

$$\nu \neq 0 \text{ и } \text{НОД}(\varepsilon_1, 2\varepsilon_2, 3\varepsilon_3, \dots, (m-1)\varepsilon_{m-1}, m) = d.$$

3. Цикловой тип $C_F(y)$ семейства $L_R(F, F)$ выражается формулой

$$C_F(y) = y + y^\tau + \sum_{d \mid m, d < m} (\tau\tau_d)^{-1} \sum_{t \mid \frac{m}{d}} \mu\left(\frac{m}{dt}\right) 2^{mt} y^{\tau\tau_d},$$

где μ есть функция Мёбиуса.

Рассмотрим теперь k -мерный случай в ситуации $k \geq 3$. Пусть

$$F_0(x), F_1(x), \dots, F_{k-1}(x) \quad (4)$$

– многочлены максимального периода и верна цепочка равенств

$$\deg F_0(x) = \deg F_1(x) = \dots = \deg F_{k-1}(x) = m \geq 2.$$

Рассмотрим идеал $I \triangleleft R_k = R[x_0, x_1, \dots, x_{k-1}]$, порожденный многочленами (4):

$$I = (F_0(x_0), F_1(x_1), \dots, F_{k-1}(x_{k-1}))_{R_k}. \quad (5)$$

Для всякой k -ЛРП $u \in L_R(I)$ вводятся понятия *цикла*

$$C(u) = \{x_0^{t_0} x_1^{t_1} \dots x_{k-1}^{t_{k-1}} u \mid (t_0, t_1, \dots, t_{k-1}) \in \mathbb{N}_0^k\}$$

и периода $T(u) = |C(u)|$. Введем понятие *периода идеала* I .

Группой вектор-периодов идеала I называется подгруппа $\mathfrak{P}(I)$ группы $(\mathbb{Z}^k, +)$, порожденная векторами $\mathbf{t} = (t_0, t_1, \dots, t_{k-1}) \in \mathbb{N}_0^k$ со свойством $\mathbf{x}^{\mathbf{t}} - 1 \in I$, где $\mathbf{x}^{\mathbf{t}} = x_0^{t_0} x_1^{t_1} \dots x_{k-1}^{t_{k-1}}$. Периодом $T(I)$ идеала I называется индекс $|\mathbb{Z}^k : \mathfrak{P}(I)|$ подгруппы $\mathfrak{P}(I)$ в группе $\mathbb{Z}^k$. Период идеала I является верхней оценкой для периода любой рекурренты $u \in L_R(I)$:

$$\forall u \in L_R(I) : T(u) \mid T(I).$$

Назовем k -ЛРП u квазимаксимальной, если

$$u \in L_R(I) \quad \text{и} \quad T(u) = T(I),$$

где идеал $I \triangleleft R_k$ определен равенством (5). Рассмотрим квазимаксимальные рекурренты над полем $R = GF(q)$.

Пусть $\tau = q^m - 1$. Имеют место следующие утверждения.

Теорема 10 ([7]). Пусть $R = GF(q)$, $k \geq 3$, $m \geq 1$, многочлены (4) суть многочлены максимального периода степени m , идеал I кольца R_k порожден многочленами (4). В семействе $L_R(I)$ существуют квазимаксимальные k -ЛРП тогда и только тогда, когда выполнено равенство

$$(\tau, (q-1)^2) = q-1. \quad (6)$$

Если (6) выполнено, то доля квазимаксимальных k -ЛРП среди всех рекуррент из семейства $L_R(I)$ не меньше $(1 - q^{-m})^k$.

Теорема 11 ([7]). В условиях предыдущей теоремы и при выполнении равенства (6) в семействе $L_R(I)$ имеется не менее

$$(q-1)^{k-1} q^{m^k - mk}$$

циклов максимальной возможной длины $T(I)$.

Список литературы

- [1] Викторенков В.Е., “Орграф полиномиального преобразования над коммутативным локальным кольцом”, *Обозр. прикл. пром. матем.*, **7:2** (2000), 327.
- [2] Викторенков В.Е., “О строении орграфов полиномиальных преобразований над конечными коммутативными кольцами с единицей”, *Дискретная математика*, **29:3** (2017), 3–23.
- [3] Глухов М.М., Елизаров В.П., Нечаев А.А., *Алгебра : Учебник*, 2-е изд., испр. и доп., СПб. : Лань, 2015, 608 с.

- [4] Ермилов Д.М., Козлитин О.А., “Цикловая структура полиномиального генератора над кольцом Галуа”, *Математические вопросы криптографии*, **4**:1 (2013), 27–57.
- [5] Ермилов Д.М., Козлитин О.А., “О строении графа полиномиального преобразования кольца Галуа”, *Математические вопросы криптографии*, **6**:3 (2015), 47–73.
- [6] Козлитин О.А., “Использование 2-линейного регистра сдвига для выработки псевдослучайных последовательностей”, *Математические вопросы криптографии*, **5**:1 (2014), 39–72.
- [7] Козлитин О.А., “О периодических свойствах полилинейных регистров сдвига”, *Дискретная математика*, **29**:1 (2017), 27–50.
- [8] Козлитин О.А., “Оценка длины максимального цикла в графе полиномиального преобразования кольца Галуа–Эйзенштейна”, *Дискретная математика*, **29**:4 (2017), 41–58.
- [9] Козлитин О.А., “Периодические свойства многомерного полиномиального генератора над кольцом Галуа, Γ ”, *Математические вопросы криптографии*, **9**:3 (2018), 61–98.
- [10] Козлитин О.А., “2-линейный регистр сдвига над кольцом Галуа четной характеристики”, *Математические вопросы криптографии*, **3**:2 (2012), 27–61.
- [11] Кузьмин А.С., Куракин В.Л., Нечаев А.А., “Псевдослучайные и полилинейные последовательности”, *Труды по дискретной математике*, **1** (1997), 139–202.
- [12] Ларин М.В., “Транзитивные полиномиальные преобразования колец вычетов”, *Дискретная математика*, **14**:2 (2002), 20–32.
- [13] Нечаев А.А., “Многомерные регистры сдвига и сложность мультипоследовательностей”, *Труды по дискретной математике*, **6** (2003), 150–165.
- [14] Anashin V.S., “Uniformly distributed sequences in computer algebra or how to construct program generators of random numbers”, *J. Math. Sci.*, **89**:4 (1998), 1355–1390.
- [15] Nomura T., Fukuda A., “Linear recurring planes and two-dimensional cyclic codes”, *Electr. Commun. Japan*, **54**:3 (1971), 23–30.