ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 27 МАТЕМАТИКИ Выпуск 1
2020

А. Р. Васин (Москва, ООО «Центр сертификационных исследований»). **О статистических свойствах одного класса линейных рекуррент над кольцами Галуа и их усложнений.**

УДК

Резюме: Рассматривается класс линейных рекуррентных последовательностей (ЛРП) над кольцами Галуа, получающихся суммой счётчиковых последовательностей и ЛРП меньшего порядка. Для последовательностей из этого класса приводятся оценки частот появления наборов элементов, коэффициента кросс-корреляции последовательности старших разрядов, а также отклонения.

Ключевые слова: линейные рекуррентные последовательности, кольцо Галуа, распределение элементов в последовательности, отклонение, тригонометрические суммы.

Введение. В настоящее время при построении генераторов псевдослучайных последовательностей важную роль играют линейные рекуррентные последовательности над кольцами Галуа (см. [1]). Важно уметь строить, так называемые, равномерные ЛРП, у которых на отрезках, длина которых кратна периоду последовательности, каждый элемент кольца появляется одинаково часто (см. [2],[3]). Кроме того, для практических приложений необходимо усложнить исходную последовательность для построения последовательности с большим рангом (линейной сложностью). Один из таких способов построения равномерных ЛРП основан на сложении исходной (основной) ЛРП со счетчиковой последовательностью и последующим выделением старшего p-адического разряда.

Псевдослучайные последовательности, используемые в различных приложениях, должны удовлетворять ряду статистических требований. Они должны обладать хорошими частотными характеристиками, низкими коэффициентами кросс-корреляции и малым отклонением.

В данной работе исследуется класс ЛРП над кольцами Галуа, получающихся суммой счетчиковых последовательностей и ЛРП меньшего порядка. Над примарными кольцами вычетов последовательности из рассматриваемого класса являются равномерными ЛРП. Для таких последовательностей приводятся оценки частот появлений наборов, коэффициента кросс-корреляции и отклония, которые уточняют известные оценки соответствующих величин для произвольных ЛРП над кольцами Галуа из работ [4]–[6].

1. Основные определения и обозначения. Рассмотрим кольцо Галуа $R = GR(p^{tn}, p^n)$ характеристики p^n с $p^{tn} = q^n$ элементами (см. [7], [8]). Напомним, что последовательность $w = (w(i))_{i=0}^{\infty}$ элементов кольца R называется ЛРП порядка m, если выполнено равенство

$$w(i+m) = a_0 w(i) + a_1 w(i+1) + \cdots + a_{m-1} w(i+m-1), \qquad i \geqslant 0,$$

где $a_0, \ldots, a_{m-1}$ — фиксированные элементы кольца R. При этом многочлен

$$H(x) = x^m - a_{m-1} x^{m-1} - \cdots - a_1 x - a_0$$

называется характеристическим многочленом последовательности w. Обозначим через $L_R(H)$ множество всех ЛРП над кольцом R с характеристическим многочленом $H(x)$.

Многочлен $F(x) \in R[x]$ будем называть реверсивным многочленом, если элемент $F(0)$ является обратимым элементом кольца R. Через $\overline{F}(x)$ обозначим образ многочлена $F(x)$ при действии естественного эпиморфизма колец многочленов $R[x] \to \overline{R}[x]$, где $\overline{R} = R/pR$ — факторкольцо кольца R по идеалу pR. Многочлен $F(x)$ будем называть многочленом Галуа, если $\overline{F}(x)$ является неприводимым многочленом над полем $\overline{R} = GF(p^t)$.

Пусть $F(x)$ — унитарный реверсивный многочлен Галуа степени $m-2$ над R, $H(x) = (x-1)^2F(x)$. Рассмотрим семейство $L_R(H)$ всех ЛРП над кольцом R с характеристическим многочленом $H(x)$. Всюду далее будет изучаться случай, когда $\overline{F}(x) \neq x-1$. Тогда (см. [1], [9]) каждая ЛРП $w \in L_R(H)$ однозначно представима в виде

$$w = v + u,$$

где $v \in L_R((x-1)^2)$, $u \in L_R(F)$, причем v однозначно представима в виде

$$v(i) = ai + b,\ i \geqslant 0,\ a, b \in R.$$

В случае кольца вычетов $\mathbb{Z}_{p^n}$ из p^n элементов последовательность w будет равномерной (см. [1], [9]) тогда и только тогда, когда a является обратимым элементом кольца $\mathbb{Z}_{p^n}$.

Период последовательности w из класса $L_R(H)$ равен

$$T(w) = p^n T(\overline{F}) = \frac{p^n(q^{m-2}-1)}{d},$$

где d — делитель числа $q^{m-2}-1$.

Через $\Gamma(R)$ обозначим множество Тейхмюллера

$$\Gamma(R) = \{0, e, \xi, \xi^2, \ldots, \xi^{q-2}\} = \{x \in R \,|\, x^q = x\}.$$

Для произвольного элемента x кольца R справедливо p-адическое разложение

$$x = x_0 + px_1 + \cdots + p^{n-1}x_{n-1},$$

где элементы $x_0, x_1, \ldots, x_{n-1}$ из множества $\Gamma(R)$. Рассмотрим отображение $f : R \to GF(p^t)$, ставящее в соответствие каждому элементу x кольца R старший разряд x_{n-1} его p-адического разложения. Через $w' = f(w)$ обозначим последовательность с элементами $f(w(i))$, $i \geqslant 0$. В случае, когда w — равномерная последовательность, разрядная последовательность w' также будет равномерной над $GF(p^t)$.

2. Оценка числа появлений наборов в ЛРП векторов. Рассмотрим последовательности $w_1, \ldots, w_r$ над кольцом $R = GR(p^{tn}, p^n)$, $r \geqslant 1$. Назовем эти последовательности линейно независимыми над кольцом R, если для всех ненулевых векторов $(c_1, \ldots, c_r) \in R^r$ последовательность $c_1w_1 + \cdots + c_rw_r$ будет отлична от нулевой последовательности. Далее будем предполагать, что последовательности $w_1, \ldots, w_r$ из множества $L_R(H)$, где $H(x)$ — некоторый унитарный многочлен над кольцом R. Тогда последовательность $(w_1(i), \ldots, w_r(i))_{i=0}^{\infty}$ будем называть ЛРП векторов с характеристическим многочленом $H(x)$.

Пусть $l \in \mathbb{N}$, $\vec{z} = (z_1, \ldots, z_r)$ — некоторый вектор из R^r. Число целых чисел $i \in \overline{0, l-1}$, удовлетворяющих системе

$$\begin{cases} w_1(i) = z_1, \\ w_2(i) = z_2, \\ \quad \cdots \\ w_r(i) = z_r, \end{cases}$$

обозначим через $N_l(\vec{z}, w_1, \ldots, w_r)$. Величина $N_l(\vec{z}, w_1, \ldots, w_r)$ равна числу появлений r-граммы $\vec{z}$ на начальном отрезке длины l ЛРП векторов. Отметим, что результаты о частотах появления элементов в ЛРП векторов являются обобщениями результатов о частотных характеристиках одной ЛРП.

Приведем новую оценку величины $\left|N_l(\vec{z}, w_1, \ldots, w_r) - \frac{l}{q^{nr}}\right|$. В этой оценке величина $\frac{l}{q^{nr}}$ является «естественным» средним значением числа появлений вектора $\vec{z}$ на отрезке длины l в ЛРП векторов.

Теорема 1. *Пусть $F(x)$ — реверсивный многочлен Галуа степени $m-2$ над кольцом $R = GR(p^{tn}, p^n)$, такой что $\overline{F}(x) \neq x-1$, $T(F) = p^\nu T(\overline{F}) = p^\nu(q^{m-2}-1)/d$, $w_1, \ldots, w_r$ — линейно независимая система ЛРП над кольцом R с характеристическим многочленом $H(x)$. Пусть также $\nu \leqslant \frac{t(m-2)}{2}$, $d < p^\nu q^{m/2-1}$. Тогда для всех $\vec{z} \in R^r$ и всех натуральных l, таких что $q^{m/2-1} \leqslant l \leqslant T(F)$, справедлива оценка*

$$\left|N_l(\vec{z}, w_1, \ldots, w_r) - \frac{l}{q^{nr}}\right| < 2\frac{q^{nr}-1}{q^{nr}} p^{\frac{n+\nu-1}{2}} l^{\frac{1}{2}} q^{\frac{m-2}{4}}.$$

Результаты теоремы можно применить для оценки минимальной длины l отрезка, на котором появятся все векторы из R^r в ЛРП векторов $(w_1(i), \ldots, w_r(i))$.

Следствие 1. *Пусть в условиях теоремы дополнительно выполнено соотношение*

$$l > 4(q^{nr}-1)^2 p^{n+\nu-1} q^{\frac{m-2}{2}}.$$

Тогда среди векторов $(w_1(i), \ldots, w_r(i))$, где $0 \leqslant i \leqslant l-1$, появятся все векторы из множества R^r.

3. Оценка коэффициента кросс-корреляции разрядных последовательностей. В качестве одной из мер близости двух последовательностей можно использовать коэффициенты кросс-корреляции. Пусть $w_1(i) = a_1 i + b_1 + u_1(i)$, $w_2(i) = a_2 i + b_2 + u_2(i)$, $i \geqslant 0$, где $a_1, a_2, b_1, b_2 \in R$, $u_1, u_2 \in L_R(F)$. Напомним, что функция $f : R \to GF(p^t)$ ставит в соответствие каждому элементу x кольца R старший разряд x_{n-1} его p-адического разложения. Коэффициентом кросс-корреляции последовательностей

$$w_1' = f(w_1),\ w_2' = f(w_2)$$

называется величина

$$C_{w_1', w_2'}(\psi, l, t) = \sum_{i=0}^{l-1} \psi(w_1'(i) - w_2'(i+t)),$$

где $l, t \in \mathbb{N}$, ψ — нетривиальный аддитивный характер поля $GF(p^t)$. Поскольку дальнейшие результаты не будут зависеть от выбора характера ψ, для рассматриваемого коэффициента будем использовать обозначение $C_{w_1', w_2'}(l, t)$. Коэффициент кросс-корреляции позволяет численно выразить близость двух векторов

$$(w_1'(0), \ldots, w_1'(l-1)) \text{ и } (w_2'(t), \ldots, w_2'(l+t-1))$$

следующим образом: чем меньше величина $|C_{w_1', w_2'}(l, t)|$, тем более отличаются друг от друга рассматриваемые векторы. Для совпадающих векторов коэффициент равен l, а для различающихся в каждом элементе — нулю.

Будем говорить, что два вектора $\vec{\alpha}$ и $\vec{\beta}$ из элементов кольца R находятся в отношении "$\sim$", и обозначать $\vec{\alpha} \sim \vec{\beta}$, если существует элемент $c \in R^*$, такой что $\vec{\alpha} = c\vec{\beta}$.

Теорема 2. Пусть $F(x)$ — реверсивный многочлен Галуа степени $m-2$ над кольцом R, $\overline{F}(x) \neq x-1$, $(u_1(0), \ldots, u_1(m-3), a_1) \not\sim (u_2(t), \ldots, u_2(t+m-3), a_2)$,

$n \geqslant 2$, $\nu \leqslant \frac{t(m-2)}{2}$, $d < p^{\nu} q^{m/2-1}$. Тогда при всех $q^{\frac{m-2}{2}} \leqslant l \leqslant T(F)$ справедлива оценка

$$|C_{w_1', w_2'}(l,t)| < 2p^{\frac{n+\nu-1}{2}} l^{\frac{1}{2}} q^{\frac{m-2}{4}+n}.$$

Одним из приложений оценки из теоремы является следующее утверждение.

Утверждение 1. Пусть $F(x)$ — реверсивный многочлен Галуа степени $m-2$ над кольцом R, $\overline{F}(x) \neq x-1$, $(u_1(0), \ldots, u_1(m-3), a_1) \not\sim (u_2(t), \ldots, u_2(t+m-3), a_2)$, $n \geqslant 2$, $\nu \leqslant \frac{t(m-2)}{2}$, $d < p^{\nu} q^{m/2-1}$. Рассмотрим величину

$$l_0 = \left[4p^{\nu+n-1} q^{\frac{m-2}{2}+2n}\right] + 1.$$

Тогда если $l_0 \leqslant T(F)$, то

$$(w_1'(0), \ldots, w_1'(l_0-1)) \neq (w_2'(t), \ldots, w_2'(t+l_0-1)).$$

4. Оценка отклонения ЛРП из рассматриваемого класса. Один способ определения того, насколько распределение некоторой последовательности близко к равномерному, заключается в вычислении величины, которая называется отклонением (статистикой Колмогорова).

Введем обозначение $I = [0,1)$ и зафиксируем некоторое натуральное число l.

Отклонением D_l^* (см. [10, определение 1.2]) последовательности $x_0, \ldots, x_{l-1}$ чисел из I называется величина

$$D_l^* = D_l^*(x_0, \ldots, x_{l-1}) = \sup_{0<\alpha\leqslant 1} \left| \frac{A([0,\alpha), l)}{l} - \alpha \right|,$$

где $A([0,\alpha), l)$ — число элементов последовательности $x_0, \ldots, x_{l-1}$, попадающих в полуинтервал $[0,\alpha)$.

Величина D_l^* определяет отклонение реального распределения элементов последовательности от «идеального» равномерного распределения. Более подробное изложение теории отклонения можно найти в книгах [10] и [11].

Рассматривая кольцо R как модуль над кольцом $\mathbb{Z}_{p^n}$ вычетов по модулю p^n, произвольный элемент x кольца R можно записать как

$$x = a_0 + a_1\xi + \cdots + a_{t-1}\xi^{t-1}, \tag{1}$$

где $a_0, \ldots, a_{t-1} \in \mathbb{Z}_{p^n}$. Для произвольного элемента x кольца R вида (1) определим нормализующее отображение $\eta\colon R \to [0,1)$:

$$\eta(x) = \frac{(a_0 + a_1 p^n + \cdots + a_{t-1} p^{n(t-1)})}{p^{tn}},$$

где $a_i \in \mathbb{Z}_{p^n}$.

Положим

$$C(R) = t\left(\frac{4}{\pi^2} n \ln p + \frac{9}{5} - \frac{1}{p^n}\right) - \frac{p^n - 1}{p^n}.$$

Теорема 3. *Пусть P — последовательность чисел*

$$y_i = \eta(w(i)),\ 0 \leqslant i \leqslant l-1,$$

в интервале $[0,1)$, порожденная ненулевой линейной рекуррентой w над кольцом Галуа (см. [6]) с характеристическим многочленом $H(x) = (x-1)^2 F(x)$, $T(F) = p^{\nu} T(\overline{F}) = p^{\nu}(q^{m-2}-1)/d$, $\nu \leqslant \frac{t(m-2)}{2}$, $d < p^{\nu} q^{m/2-1}$. Тогда для чисел l, удовлетворяющих неравенствам $q^{\frac{m-2}{2}} \leqslant l \leqslant T(F)$, справедлива оценка

$$D_l^*(P) < \frac{1}{q^n} + 2C(R) p^{\frac{n+\nu-1}{2}} l^{-1/2} q^{\frac{m-2}{4}}.$$

Результат теоремы несколько уточняет оценки отклонения произвольных ЛРП над кольцами Галуа из работы [6]. Однако асимптотический характер полученной оценки остается равным $O(l^{-1/2}q^{m/4})$ при $m \to \infty$, $l = O(q^m)$.

СПИСОК ЛИТЕРАТУРЫ

1. *Kurakin V. L.*, *Kuzmin A. S.*, *Mikhalev A. V.*, *Nechaev A. A.* Linear recurring sequences over rings and modules, J. Math. Sci., 1995, 76:6, p. 2793–2915.
2. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов. — Дискретн. матем., 2002, т. 14, в. 2, с. 20–32.
3. *Анашин В. С.* Равномерно распределенные последовательности целых p-адических чисел. — Дискретн. матем., 2002, т. 14, в. 4, с. 3–64.
4. *Васин А. П.* Оценки частот наборов элементов на отрезках линейных рекуррентных последовательностей над кольцами Галуа. — Дискретн. матем., 2019, т. 31, в. 2.
5. *Камловский О. В.* Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа. — Изв. РАН. Сер. матем., 2013, т. 77, в. 6, с. 71–96.
6. *Васин А. П.* Оценки отклонения линейных рекуррентных последовательностей над кольцами Галуа. — Дискретн. матем., 2019, т. 31, в. 3.
7. *Нечаев А. А.* Код Кердока в циклической форме. — Дискретн. матем., 1989, т. 1, в. 4, с. 123–139.
8. *McDonald B. R.* Finite rings with identity, Pure and Applied Mathematics, 28, Dekker, New York, 1974.
9. *Камловский О. В.* Распределение r-грамм в одном классе равномерных последовательностей над кольцами вычетов. — Проблемы передачи информации, 2014, Т. 50, в. 1, с. 98–115.
10. *Кейперс Л.*, *Нидеррейтер Г.* Равномерное распределение последовательностей. Наука. Гл. ред. физ.-матем. лит., 1985.
11. *Niederreiter H.*, *Winterhof A.* Applied number theory, Springer International Publishing, 2015.

УДК

Vasin A. R. (Moscow, LLC «center for certification research»). **On the statistical properties of one class of linear recurring sequences over Galois rings and their complications.**

Abstract: We consider a class of linear recurring sequences (LRS) over Galois rings that result from the summation of counter sequences and LRS of lesser order. For sequences from this class bounds on the frequencies of tuples, the cross-correlation coefficient of the highest order digit sequence, and the discrepancy are derived.

Keywords: linear recurring sequences, Galois ring, distribution of elements in a sequence, discrepancy, exponential sums.