ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 27 МАТЕМАТИКИ Выпуск 2
2020

Секция **«Стохастические аспекты задач передачи, обработки и защиты информации»**

ВАСИН А. Р.

О СТАТИСТИЧЕСКИХ СВОЙСТВАХ ОДНОГО КЛАССА ЛИНЕЙНЫХ РЕКУРРЕНТ НАД КОЛЬЦАМИ ГАЛУА И ИХ УСЛОЖНЕНИЙ [1)]

Рассматривается класс линейных рекуррентных последовательностей (ЛРП) над кольцами Галуа, получающихся суммой счетчиковых 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 и фразы: кольцо Галуа, линейные рекуррентные последовательности, распределение элементов в последовательности, отклонение ЛРП, тригонометрические суммы

Содержание

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.

DOI https://doi.org/10.52513/08698325_2020_27_2_114

[1)] От Редакции. Публикуется по решению Программного комитета ВШКСМ в качестве пленарного доклада — лекции им. академика АК РФ В. Ф. Колчина на XXIV Всероссийской Школе-коллоквиуме по стохастическим методам (Сочи–Дагомыс, 14–19 сентября 2020 г.)

Теорема 3. *Пусть P — последовательность чисел*

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

в интервале $[0,1)$, порожденная ненулевой линейной рекуррентой w над кольцом Галуа (см. [7]) *с характеристическим многочленом $H(x) = (x-1)^2 F(x)$,*

$$T(F) = p^\nu T(\overline{F}) = \frac{p^\nu(q^{m-2}-1)}{d}, \quad \nu \leqslant \frac{t(m-2)}{2}, \quad d < p^\nu q^{m/2-1}.$$

Тогда для чисел l, удовлетворяющих неравенствам $q^{(m-2)2} \leqslant l \leqslant T(F)$, справедлива оценка

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

Результат теоремы 3 несколько уточняет оценки отклонения произвольных ЛРП над кольцами Галуа из работы [7]. Однако асимптотический характер полученной оценки остается равным

$$O\Big(\frac{q^{m/4}}{\sqrt{l}}\Big) \quad \text{при} \quad m \to \infty, \quad l = O(q^m).$$

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, v. 76, № 6, p. 2793–2915.
2. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов. — Дискретн. матем., 2002, т. 14, в. 2, с. 20–32. // *Larin M. V.* Transitive polynomial transformations of residue class rings. — Discrete Math. Appl., 2002, v. 12, is. 2, p. 127–140.
3. *Анашин В. С.* Равномерно распределенные последовательности целых p-адических чисел. — Дискретн. матем., 2002, т. 14, в. 4, с. 3–64. // *Anashin V. S.* Uniformly distributed sequences of p-adic integers. — Discrete Math. Appl., 2002, v. 12, is. 6, p. 527–590.
4. *Горески М.*, *Клаппер А.* Регистры сдвига и порождаемые ими алгебраические последовательности. — Обозрение прикл. и промышл. матем., 2014, вв. 4–6, 2015, вв. 1–3. // *Goresky M.*, *Klapper A.* Algebraic Shift Register Sequences. Cambridge: Cambridge Univ. Press, 2012, 514 p.
5. *Васин А. Р.* Оценки частот наборов элементов на отрезках линейных рекуррентных последовательностей над кольцами Галуа. — Дискретн. матем., 2019, т. 31, в. 2, с. 57–68. // *Vasin A. R.* Bounds on the frequencies of tuples on parts of the period of linear recurring sequences over Galois rings. — Discrete Math. Appl., 2019, v. 29, is. 5, p. 335–343.
6. *Камловский О. В.* Частотные характеристики разрядных последовательностей линейных рекуррент над кольцами Галуа. — Изв. РАН. Сер. матем., 2013, т. 77, в. 6, с. 71–96. // *Kamlovskii O. V.* Frequency characteristics of coordinate sequences of linear recurrences over Galois rings. — Izvestiya: Mathematics, 2013, v. 77, is. 6, p. 1130–1154.

7. *Васин А. Р.* Оценки отклонения линейных рекуррентных последовательностей над кольцами Галуа. — Дискретн. матем., 2019, т. 31, в. 3, с. 57–68. // *Vasin A. R.* Bounds on the discrepancy of linear recurring sequences over Galois rings. — Discrete Math. Appl., 2020, v. 30, is. 2, p. 129–135.
8. *Нечаев А. А.* Код Кердока в циклической форме. — Дискретн. матем., 1989, т. 1, в. 4, с. 123–139. // *Nechaev A. A.* Kerdock code in a cyclic form. — Discrete Math. Appl., 1991, v. 1, is. 4, p. 365–384.
9. *McDonald B. R.* Finite Rings with Identity. N.Y.: Dekker, 1974, 448 p. (Ser. Pure and Applied Mathematics. V. 28.)
10. *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. // *Kamlovskii O. V.* Distribution of r-tuples in one class of uniformly distributed sequences over residue rings.— Probl. Inf. Transm., 2014, v. 50, is. 1, p. 90–105.
11. *Кейперс Л.*, *Нидеррейтер Г.* Равномерное распределение последовательностей. М.: Наука/Физматлит, 1985, 407 с. // *Kuipers L.*, Niederreiter H. Uniform Distribution of Sequences. N. Y. etc.: Wiley, 1974, xiv+390 p.
12. *Niederreiter H.*, *Winterhof A.* Applied Number Theory, Cham: Springer Internat. Publ., 2015, x+442 p.

Поступила в редакцию
31.VII.2020

UDC 512.6+519.2 DOI https://doi.org/10.52513/08698325_2020_27_2_114

A. R. Vasin (Moscow, Center for Certification Research, LLC)**. On the statistical properties of a 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 of a sequence, exponential sums.