О. В. Камловский (Москва, ТВП). **Оценки для числа элементов на отрезках линейных рекуррентных последовательностей над кольцами вычетов.**

Рассмотрим последовательность $u = (u(i))_{i=0}^{\infty}$ элементов кольца $\mathbf{Z}_{p^n}$ вычетов по модулю p^n, где p — простое число. Будем считать, что последовательность u является линейной рекуррентной последовательностью (ЛРП) над кольцом $\mathbf{Z}_{p^n}$, т. е. знаки этой последовательности удовлетворяют условию:

$$u(i+m) = a_0u(i) + a_1u(i+1) + \cdots + a_{m-1}u(i+m-1), \qquad i \geqslant 0,$$

где $a_0, a_1, \ldots, a_{m-1}$ — фиксированные элементы из кольца $\mathbf{Z}_{p^n}$. Назовем характеристический многочлен $F(x) = x^m - a_{m-1}x^{m-1} - \cdots - a_1x - a_0$ ЛРП u реверсивным многочленом Галуа над кольцом $\mathbf{Z}_{p^n}$, если многочлен $\overline{F}(x)$, полученный из многочлена $F(x)$ приведением всех его коэффициентов по модулю p, неприводим над полем $\mathbf{Z}_p$ и отличен от x. Обозначим $L(F)^*$ множество всех ЛРП u над кольцом $\mathbf{Z}_{p^n}$ с характеристическим многочленом $F(x)$, у которых среди элементов $u(0), u(1), \ldots, u(m-1)$ есть хотя бы один обратимый элемент кольца $\mathbf{Z}_{p^n}$. Каждая ЛРП u из множества $L(F)^*$ будет чисто периодической последовательностью периода $T(u)$, который совпадает с периодом $T(F)$ многочлена $F(x)$, причем справедливы равенства $T(u) = T(F) = p^\nu T(\overline{F}) = p^\nu(p^m-1)/d$, где $0 \leqslant \nu \leqslant n-1$, а d — делитель числа $p^m - 1$ (см., например, [2]).

Представляет интерес нахождение числа $N_l(z,u)$ появлений элемента z кольца $\mathbf{Z}_{p^n}$ среди элементов $u(0), u(1), \ldots, u(l-1)$. Рассматриваемые частоты хорошо изучены в случае, когда u является ЛРП над полем $\mathbf{Z}_p$ или над произвольным конечным полем (см., например, обзор в работе [3]). В другом частном случае, когда u ЛРП над кольцом $\mathbf{Z}_{p^n}$, а $l = T(u)$, также получено большое количество результатов (см. [1], [5], [6]). Менее изученным является вопрос о частотах $N_l(z,u)$ при значениях l, отличных от величины $T(u)$ (см. [4] и цитированную там литературу). В работе, представленной данным сообщением, приводятся оценки рассматриваемых частот, полученные с использованием метода тригонометрических сумм.

Теорема 1. *Пусть $F(x)$ — реверсивный многочлен Галуа над кольцом $\mathbf{Z}_{p^n}$ степени m, $u \in L(F)^*$, $T(u) = T(F) = p^\nu(p^m-1)/d$. Тогда при всех $l \leqslant T(u)$ и всех z из кольца $\mathbf{Z}_{p^n}$ справедливо неравенство*:

$$\left| N_l(z,u) - \frac{l}{p^n} \right| \leqslant \frac{p^{2n}-1}{p+1}\left(\frac{2}{\pi}\ln T(u) + \frac{7}{5}\right)p^{m/2+\nu-n}. \tag{1}$$

Следует заметить, что участвующая в оценке (1) величина l/p^n является естественной средней частотой появления элемента на отрезке длины l последовательности u. Неравенство (1) можно рассматривать как оценку отклонения частоты $N_l(z,u)$ от среднего значения.

Теорема 2. *Пусть $F(x)$ — реверсивный многочлен Галуа над кольцом $\mathbf{Z}_{p^n}$ степени m. Тогда при каждом $l \leqslant T(\overline{F})$ найдутся такие ЛРП u из множества $L(F)^*$ и элемент z кольца $\mathbf{Z}_{p^n}$, что*

$$\left| N_l(z,u) - \frac{l}{p^n} \right| \geqslant l^{1/2}\left(\frac{(1-p^{-n})(p^m-l)}{p^n(p^m-1)}\right)^{1/2}.$$

Рассмотрим многочлен $F(x)$ над кольцом $\mathbf{Z}_{p^n}$, имеющий период $T(F) = p^\nu(p^m - 1)$. Тогда если p — нечетное число и $l = (p^m+1)/2$, то по теореме 2 найдутся такие ЛРП u из множества $L(F)^*$ и элемент z из кольца $\mathbf{Z}_{p^n}$, что

$$\left| N_l(z,u) - \frac{l}{p^n} \right| > \frac{(p^n-1)^{1/2}}{2}p^{m/2-n}.$$

Этот пример показывает, что в оценке (1) величина $p^{m/2}$ не может быть заменена на показательную функцию (от переменной m) с меньшим основанием степени.

Работа поддержана грантом Президента РФ НШ–8564.2006.10.

СПИСОК ЛИТЕРАТУРЫ

1. *Камловский О. В.*, *Кузьмин А. С.* Оценки частот появления элементов в линейных рекуррентных последовательностях над кольцами Галуа. — Фунд. и прикл. матем., 2000, т. 6, в. 4, с. 1083–1094.
2. *Нечаев А. А.* Цикловые типы линейных подстановок над конечными коммутативными кольцами. — Матем. сб., 1993, т. 184, № 3, с. 21–56.
3. *Лидл Р.*, *Нидеррайтер Г.* Конечные поля. Т. 1, 2. М.: Мир, 1988, 824 с.
4. *Hu H.*, *Feng D.*, *Wu W.* Incomplete exponential sums over Galois rings with applications to some binary sequences derived from $\mathbf{Z}_{2^l}$. — IEEE Trans. Inform. Theory, 2006, v. 52, № 5, p. 2260–2265.
5. *Kumar P. V.*, *Helleseth T.*, *Calderbank A. R.* An upper bound for Weil exponential sums over Galois rings and applications. — IEEE Trans. Inform. Theory, 1995, v. 41, № 2, p. 456–468.
6. *Kuzmin A. S.*, *Nechaev A. A.* Complete weight enumerators of generalized Kerdock code and related linear codes over Galois ring. — Discrete Appl. Math., 2001, v. 111, p. 117–137.