

Д. М. Е р м и л о в, О. А. К о з л и т и н (Москва, ТВП). О циклах полиномиального преобразования кольца Галуа

Пусть R — кольцо. Один из способов выработки псевдослучайных последовательностей над R состоит в использовании рекурренты с глубиной зависимости 1:

$$\forall i \geq 0: \quad u(i+1) = F(u(i)), \quad (1)$$

где $u(0) = a \in R$ — начальное заполнение, а F — некоторое полиномиальное преобразование кольца R . Вычисление периода последовательности u — первый естественный вопрос, возникающий в связи с генератором (1). В случае, когда R — примарное кольцо вычетов, этот вопрос рассматривался в работах ряда авторов, среди которых следует выделить В. С. Анашина [1] и М. В. Ларина [2]. Имеются отдельные результаты о периодических свойствах генератора (1) в ситуации, когда R — простейшее некоммутативное локальное кольцо главных идеалов [3]. Вместе с тем, существует важный класс коммутативных колец, занимающий промежуточное положение между примарными кольцами вычетов и конечными локальными кольцами главных идеалов, — кольца Галуа. Это — минимальный класс колец, содержащий как все примарные кольца вычетов, так и все конечные поля [2]. В работе, представленной данным докладом, изучаются периодические свойства полиномиального преобразования F кольца Галуа $R = GR(2^{mn}, 2^n)$.

Для всякого $i \in \{1, 2, \dots, n\}$ обозначим φ_i отображение, приводящее многочлены над кольцом R по модулю $2^i R$. Пусть элемент $a \in R$ лежит на цикле преобразования F . Длину цикла преобразования $\varphi_i(F)$, содержащего элемент $\varphi_i(a)$, обозначим $t_i(a)$. Имеем последовательность натуральных чисел

$$t_1(a), t_2(a), \dots, t_i(a), \dots, t_n(a), \quad (2)$$

где $t_i(a) \mid t_{i+1}(a)$ для всякого $i \in \{1, 2, \dots, n-1\}$. Задача о вычислении периода последовательности u сводится к изучению поведения последовательности (2).

Для всякого $t \geq 1$ обозначим $F^{[t]}(x)$ t -ю композиционную степень преобразования F :

$$F^{[t]} = F \circ F \circ \dots \circ F \text{ (} t \text{ раз)}.$$

Пусть $f = F^{[t_1(a)]}$ ($\alpha = f'(a)$) — значение производной от f в точке a , $d_i = t_{i+1}(a)/t_i(a)$, $i = 1, 2, \dots, n-1$, $J = 2R$, 0 и e — соответственно ноль и единица кольца R . Обозначим $\bar{\alpha}$ образ элемента α под действием естественного эпиморфизма $R \rightarrow \bar{R} = R/J$.

Теорема. Если $\bar{\alpha} \notin \{\bar{0}, \bar{e}\}$ и $\delta = \text{ord } \bar{\alpha}$ — порядок $\bar{\alpha}$ в мультипликативной группе поля $\text{GF}(2^m)$, то последовательность $d_1, d_2, \dots, d_{n-1}$ имеет вид а), б), в), г), е) или ф):

- а) $1, 1, \dots, 1$;
- б) $1, 1, \dots, 1, \delta$;

- c) $1, 1, \dots, 1, \delta, 1, 1, \dots, 1$;
- d) $1, 1, \dots, 1, \delta, 1, 1, \dots, 1, 2, 2, \dots, 2$;
- e) $1, 1, \dots, 1, \delta, 1, 1, \dots, 1, 2, 1, 1, \dots, 1$;
- f) $1, 1, \dots, 1, \delta, 1, 1, \dots, 1, 2, 1, 1, \dots, 1, 2, 2, \dots, 2$.

В каждом пункте любая серия единиц может отсутствовать. Ситуации e) и f) возможны лишь при условии $(f^{[\delta]})'(a) \equiv 3e \pmod{J^2}$.

Следствие. В условиях теоремы справедливо неравенство

$$t_n(a) \leq 2^{n-2}(2^m - 1)t_1(a). \quad (3)$$

Вычисления на ЭВМ показывают, что оценка (3) достижима. Так, над кольцом $R = \text{GR}(2^{3 \cdot 3}, 2^3)$ существует пара (F, a) , для которой неравенство (3) обращается в равенство.

Работа выполнена при поддержке гранта Президента РФ НШ-6260.2012.10.

СПИСОК ЛИТЕРАТУРЫ

1. Анашин В. С. О группах и кольцах, обладающих транзитивными полиномами. — Тезисы XVI Всесоюзной алгебраической конференции. Часть II. Л.: 1981, с. 4–5.
2. Елизаров В. П. Конечные кольца. М.: Гелиос-АРВ, 2006, 304 с.
3. Козмитин О. А. Полиномиальные преобразования GEO-кольца простой характеристики. — Дискретная математика, 2004, т. 16, в. 3, с. 105–117.
4. Ларин М. В. Транзитивные полиномиальные преобразования колец вычетов. — Дискретная математика, 2002, т. 14, в. 2, с. 20–32.
5. Нечаев А. А. Полиномиальные преобразования конечных коммутативных колец главных идеалов. — Матем. заметки, 1980, т. 27, в. 6, с. 885–899.