ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 24 МАТЕМАТИКИ Выпуск 5
2017

Д. М. Ермилов (Москва, ТВП). **Оценка числа МДЦ-полиномов над кольцом Галуа характеристики p^2.**

Рассмотрим кольцо Галуа $R = GR(q^2, p^2)$ мощности q^2 и характеристики p^2. Обозначим через $G_{f,R}$ — граф полиномиального преобразования, заданного на кольце R полиномом $f(x)$. В работе [1] показано, что для любого полинома $f(x) \in R[x]$ длина произвольного цикла графа $G_{f,R}$ не превосходит величины $q(q-1)\,p^{n-2}$.

Рассмотрим биективный полином f над R, у которого граф $G_{f,R}$ содержит цикл максимальной длины $q(q-1)\,p^{n-2}$.

Будем называть такие полиномы *полиномами с максимальной* длиной циклов (*МДЦ-полиномами*).

В настоящей работе приводится нижняя оценка для числа МДЦ-полиномов над кольцами Галуа вида $GR(q^2, p^2)$.

Обозначим $\overline{R}$ фактор-кольцо R/J, $J = pR$. Заметим, что $\overline{R}$ является полем мощности q.

Введем естественный эпиморфизм колец $\phi : R \to \overline{R}$, который естественным образом может быть продолжен до эпиморфизма кольца многочленов $\widehat{\phi} : R[x] \to \overline{R}[x]$.

Пусть f' — стандартным образом определенная *производная* полинома f и

$$\alpha_f(a) = \left(f^{[q]}(x)\right)'_{x=a}.$$

Из результатов работы [1] следует, что если f является МДЦ-полиномом, то элемент $\alpha_f(a) \in R$ обратим для любого $a \in R$. Обозначим $\overline{a}$ образ элемента a под действием естественного эпиморфизма ϕ. Положим:

$$\delta_f(a) = \begin{cases} p, & \text{если} \quad \overline{\alpha}_f(a) = \overline{e}, \\ \operatorname{ord} \overline{\alpha}_f(a) & \text{в противном случае,} \end{cases} \tag{1}$$

где $\operatorname{ord} a$ — мультипликативный порядок элемента a поля $\overline{R}$ и e — единица кольца R.

Из работы [1] следует, что $\delta_f(a) \equiv \delta_f(b) \pmod J$ для любых $a, b \in R$, если f является МДЦ-полиномом. Поэтому для МДЦ-полинома f корректно обозначение δ_f.

Нам понадобится следующий результат из работы [2].

Утверждение [2, утверждение 21]. *Многочлен $f(x) \in R[x]$ является* МДЦ-*полиномом тогда и только тогда, когда $\overline{f}$ — полноцикловый полином над $\overline{R}$, и $\delta_f = q-1$.*

Пусть $N(q^2, p^2)$ есть число всех МДЦ-полиномов над кольцом R. В следующей теореме получена нижняя оценка для величины $N(q^2, p^2)$.

Теорема. *Во введенных обозначениях выполняется следующая оценка:*

$$(q-1)!\,\varphi(q-1) \leqslant N(q^2, p^2),$$

где φ — функция Эйлера.

Доказательство. Согласно утверждению достаточно показать, что для каждой пары, состоящей из примитивного элемента α поля $\overline{R}$ и полноциклового полинома f_1 поля $\overline{R}$ существует МДЦ-полином f над кольцом R.

Выберем и зафиксируем такие ненулевые элементы $\alpha_0, \alpha_1, \ldots, \alpha_{q-1} \in \overline{R}$, что $\alpha_0\alpha_1 \cdots \alpha_{q-1} = \alpha$.

Положим $c_i = f_1'(f_1^{[i]}(0))$, $i = 0, 1, \ldots, q-1$. Определим полином $h(x) \in \overline{R}[x]$ посредством соотношений

$$h\big(f_1^{[i]}(0)\big) = c_i - \alpha_i, \qquad i = 0, 1, \ldots, q-1.$$

Покажем, что полином $f(x) = f_1(x) + (x^q - x)\, h(x)$ является искомым МДЦ-полиномом над R.

Действительно,

$$\begin{aligned} \alpha_f &= (f^{[q]}(0))' \equiv \prod_{i=0}^{q-1} f'\big(f^{[i]}(0)\big) \\ &\equiv \prod_{i=0}^{q-1} \Big(f'\big(f^{[i]}(0)\big) - (c_i - \alpha_i)\Big) \equiv \alpha_0\alpha_1 \cdots \alpha_{q-1} = \alpha \pmod{J}. \end{aligned}$$

Кроме того, полином $\overline{f}(x)$ является полноцикловым полиномом над $\overline{R}$, поскольку $\overline{f}(x) \equiv f_1(x) \pmod{J}$. □

СПИСОК ЛИТЕРАТУРЫ

1. *Ермилов Д. М.*, *Козлитин О. А.* Цикловая структура полиномиального генератора над кольцом Галуа. — Математические вопросы криптографии, 2013, т. 4, в. 1, с. 27–57.
2. *Ермилов Д. М.*, *Козлитин О. А.* О строении графа полиномиального преобразования кольца Галуа. — Математические вопросы криптографии, 2015, т. 6, в. 3, с. 47–73.