О Б О З Р Е Н И Е
П Р И К Л А Д Н О Й И П Р О М Ы Ш Л Е Н Н О Й
Том 21 М А Т Е М А Т И К И Выпуск 4
2014

Д. М. Е р м и л о в (Москва, ТВП). **Алгоритм построения МДЦ-полиномов над кольцом Галуа.**

Рассмотрим кольцо Галуа $R = \mathbf{GR}(q^n, p^n)$ мощности q^n и характеристики p^n. Обозначим через $G_{f,R}$ — граф полиномального 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 биективные полиномы над R, у которых 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).

Из результатов работы [2] следует, что описание общего вида МДЦ-полиномов над кольцами Галуа сводится к описанию МДЦ-полиномов над кольцами Галуа вида $\mathbf{GR}(q^3, p^3)$.

Обозначим через J множество pR делителей нуля кольца Галуа R, $J^k = p^k R$ и $R_k = R/J^k$ — факторкольцо кольца R по идеалу J^k. Рассмотрим эпиморфизмы колец

$$\phi_i : R \to R_i$$

для $i \in \{1, 2, \ldots, n\}$, которые естественным образом продолжаются до эпиморфизмов колец многочленов

$$\widehat{\phi}_i : R[x] \to R_i[x].$$

Зафиксируем МДЦ-полином $f(x) \in R[x]$ и положим $f_i(x) = \widehat{\phi}_i(f(x))$, $i \in \{1, 2, \ldots, n\}$.

Обозначим через $f^{[0]}(x)$ тождественное преобразование, а через $f^{[m]}(x)$, $m \in \mathbf{N}$, — преобразование

$$f \circ f \circ \cdots \circ f \ (m \text{ раз}),$$

где $\circ$ — операция *композиции*. Производную многочлена $f(x)$ кольца $R[x]$ будем обозначать через $f'(x)$ (см. например, [3]). Порядок элемента $a \in R$ будем обозначать через $\operatorname{ord}(a)$.

Пусть далее $R = \mathbf{GR}(q^3, p^3)$, $p > 2$. Следующая теорема уточняет результаты работы [2]:

Теорема. *Пусть* $f(x) \in R[x]$, $F(x) = f^{[q]}(x)$. *Полином* $f(x)$ *является МДЦ-полиномом над кольцом* R *тогда и только тогда, когда выполняются условия*:

1) $f_1(x)$ — *полноцикловый полином над полем* R_1;

2) $\delta = q - 1$, *где* $\delta = \operatorname{ord}(F'(a)), a \in R_1$;

3) $F'(a) \in R_2 \setminus \Gamma(R_2)$, *где элемент* $a \in R_2$ *лежит на цикле длины* $q(q-1)$ *графа* G_{f_2,R_2}.

Будем обозначать образ элемента $a \in R$ под действием естественного эпиморфизма $\phi_1 : R \to R_1$ через $\overline{a}$. Сформулируем алгоритм построения МДЦ-полиномов над кольцом R_3.

А л г о р и т м (построение МДЦ-полиномов над R_3).

Ш а г 1. Пусть $(\overline{w}_0, \overline{w}_1, \ldots, \overline{w}_{q-1})$ — полноцикловая подстановка поля R_1. Построить унитарный полином $r(x) \in R[x]$ такой, что

$$\deg r(x) \leqslant q-1 \quad \text{и} \quad \forall\, i \in \{0,1,\ldots,q-1\}: \quad \overline{r}(\overline{w}_i) = \overline{w}_{i+1 (\mathrm{mod}\, q)}.$$

Ш а г 2. Найти такой набор $(c_0, c_1, \ldots, c_{q-1}) \in R_1^q$, что $c_0 \cdot c_1 \cdot \ldots \cdot c_{q-1} = c$ есть примитивный элемент поля R_1. Построить такой унитарный полином $t(x) \in R[x]$, что

$$\deg t(x) \leqslant q-1 \quad \text{и} \quad \forall\, i \in \{0,1,\ldots,q-1\}: \quad \overline{t}(\overline{w}_i) = \overline{r}'(\overline{w}_i) - c_i.$$

Ш а г 3. Положить $f(x) = r(x) + (x^q - x)t(x)$ и проверить условие

$$\varphi_2(F'(a)) \in R_2 \setminus \Gamma(R_2), \tag{1}$$

где элемент $a \in R$ таков, что $\overline{a} = \overline{w}_0$. Если условие (1) выполнено, то $f_3(x)$ — МДЦ-полином над R_3, СТОП. Иначе перейти к шагу 4.

Ш а г 4. По формуле производной сложной функции имеем:

$$F'(x) = (f^{[q]}(x))' = f'(f^{[q-1]}(x)) \cdots f'(f(x)) \cdot f'(x). \tag{2}$$

Пусть $\alpha_i + p\beta_i$ — разложение Тейхмюллера (см. [4]) элемента $\varphi_2(f'(f^{[i]}(a)))$, $i = 0, 1, \ldots, q-1$. Нетрудно проверить, что верно следующее сравнение по модулю J^2:

$$(\alpha_0 + p\beta_0) \cdot (\alpha_1 + p\beta_1) \cdots (\alpha_{q-1} + p\beta_{q-1}) \equiv \alpha_0 \cdots \alpha_{q-1} + p \cdot \alpha_0 \cdots \alpha_{q-1} \sum_{i=0}^{q-1} \beta_i \alpha_i^{-1}.$$

Тогда из условия $\varphi_2(F'(a)) \in \Gamma(R_2)$ следует, что

$$\sum_{i=0}^{q-1} \beta_i \alpha_i^{-1} \equiv 0 \,(\mathrm{mod}\, J).$$

Построить унитарный многочлен $h(x) \in R[x]$ такой, что

$$\deg h(x) \leqslant q-1, \quad \forall\, i \in \{0,1,\ldots,q-2\}: \quad \overline{h}(\overline{w}_i) = 0, \quad \overline{h}(\overline{w}_{q-1}) = -\overline{\alpha}_{q-1}.$$

Положить

$$f(x) = r(x) + (x^q - x)t(x) + p(x^q - x)h(x).$$

Тогда $f_3(x)$ — МДЦ-полином над R_3. СТОП.

Конец работы алгоритма.

СПИСОК ЛИТЕРАТУРЫ

1. *Ермилов Д. М.*, *Козлитин О. А.* Цикловая структура полиномиального генератора над кольцом Галуа. — Матем. вопросы криптографии, 2013, т. 4, в. 1, с. 27–57.
2. *Ермилов Д. М.* Полиномиальные подстановки над кольцом Галуа, содержащие цикл максимальной длины. — Обозрение прикл. и промышл. матем., 2014, т. 1, в. 1, с. 56.
3. *Глухов М. М.*, *Елизаров В. П.*, *Нечаев А. А.* Алгебра. М.: Гелиос-АРВ, 2003, 749 с.
4. *Нечаев А. А.* Конечные кольца главных идеалов. — Матем. сб., 1973, т. 91(133), в. 3(7), с. 350–366.