ОБОЗРЕНИЕ
ПРИКЛАДНОЙ И ПРОМЫШЛЕННОЙ
Том 19 МАТЕМАТИКИ Выпуск 5
2012

Д. М. Ермилов (Москва, ТВП). **О поиске цикловой структуры полиномиальных преобразований колец Галуа.**

Рассмотрим биективное полиномиальное преобразование задающиеся полиномом $F(x)$ над кольцом Галуа $R = \mathrm{GR}\,(q^n, p^n)$. *Цикловой структурой полиномиального преобразования* $F(x)$ называют таблицу $[l_1^{k_1}, l_2^{k_2}, \ldots, l_t^{k_t}]$, указывающую, что подстановка, которая задается полиномиальным преобразованием $F(x)$, состоит из k_1 циклов длины l_1, ... , k_t циклов длины l_t.

Предлагаемый алгоритм позволяет находить цикловую структуру $F(x)$ над кольцом Галуа R не более, чем за $O\,(q^3 n^2)$ вычислений значения $F(x)$ в точке.

Нахождение цикловой структуры с низкой трудоемкостью открывает путь к разработке методов построения подстановок над кольцами Галуа с заданной цикловой структурой.

Пусть J — радикал кольца R. Каждому полиному $F(x)$ поставим в соответствие граф этого полиномиального преобразования G_F и рассмотрим произвольный цикл C графа G_F. Обозначим t_n длину цикла C. Если привести этот цикл по модулю J^s, то получим цикл длины t_s, $s \in \{1, 2, \ldots, n-1\}$. Следующие теоремы устанавливают взаимосвязь между величинами $t_1, t_2, \ldots, t_n$ при различных p. Пусть $d_i = t_{i+1}/t_i$, $i = 1, 2, \ldots, n-1$.

Теорема 1. *Пусть* $F(x) \in R[x]$. *Последовательность* $d_1, d_2, \ldots, d_{n-1}$ *для произвольного цикла* C *графа* G_F *при* $p \neq 2$ *может иметь вид*: a) $1, 1, \ldots, 1$; b) $1, 1, \ldots, 1, p, \ldots, p$; c) $1, 1, \ldots, \delta, 1, \ldots, 1$; d) $1, 1, \ldots, \delta, 1, \ldots, 1, p, \ldots, p$, *где* δ *— некоторый параметр полинома* $F(x)$.

В случае, когда характеристика кольца R четна, описание последовательности $d_1, \ldots, d_{n-1}$ дает следующее утверждение.

Теорема 2. *Пусть* $F(x) \in R[x]$. *Последовательность* $d_1, d_2, \ldots, d_{n-1}$ *для произвольного цикла* C *графа* G_F *при* $p = 2$ *может иметь вид*: a) $1, 1, \ldots, 1$; b) $1, 1, \ldots, 1, 2, \ldots, 2$; c) $1, 1, \ldots, \delta$; d) $1, 1, \ldots, \delta, 1, \ldots, 1$; f) $1, 1, \ldots, \delta, 1, \ldots, 1, 2$; g) $1, 1, \ldots, 1, \delta, 1, \ldots, 1, 2, e_1, e_2, \ldots, e_l$, *где* $e_i \in \{1, 2\}$, $i = 0, 1, \ldots, l$ *и* δ *— некоторый параметр полинома* $F(x)$.

С помощью результатов приведенных теорем можно дать ответ на вопрос: циклы какой длины могут быть сравнимы с заданным циклом C графа G_F? Ответим на вопрос о количестве циклов, сравнимых с заданным циклом C графа G_F по произвольному модулю J^k, $k \in \{1, 2, \ldots, n\}$.

Выберем и зафиксируем $s \in \{1, 2, \ldots, n\}$. Рассмотрим эпиморфизм $\phi_s : R/J^{s+1} \to R/J^s$. Пусть цикл C имеет длину t по модулю J^s. Назовем множество $\phi_s^{-1}(C)$ *полным прообразом* цикла C относительно ϕ_s.

Теорема 3. *Пусть цикл* C *имеет длину* t *по модулю* J^s. *Тогда*:

1) *если в полном прообразе* $\phi_s^{-1}(C)$ *содержится цикл длины* dt, *где* $d|q-1$, *то полный прообраз цикла* C *относительно* ϕ_s *состоит из одного цикла длины* t *и* $(q-1)/d$ *циклов длины* dt;

© Редакция журнала «ОПиПМ», 2012 г.

2) *если в полном прообразе* $\phi_s^{-1}(C)$ *содержится цикл длины* pt, *то полный прообраз цикла* C *относительно* ϕ_s *состоит из* q/p *циклов длины* pt;

3) *если в полном прообразе* $\phi_s^{-1}(C)$ *содержится более двух циклов длины* t, *то полный прообраз цикла* C *относительно* ϕ_s *состоит из* q *циклов длины* t.

Полученные теоретические результаты позволили предложить алгоритм поиска цикловой структуры. На первом шаге алгоритма находится цикловая структура полиномиального преобразования $F(x)$ над полем R/J. Далее для каждого цикла C из найденной цикловой структуры выполняется поиск циклов графа G_F, которые сравнимы с циклом C по модулю J. Это делается с помощью построения цепочки множеств циклов, сравнимых с циклом C по модулям $J, J^2, \ldots, J^n$ соответственно. Последнее множество из полученной цепочки содержит циклы искомой цикловой структуры.

Используя результаты изложенных теорем, удалось показать возможность построения упомянутой выше цепочки множеств циклов с низкой трудоемкостью и оценить общую сложность алгоритма величиной $O\left(q^3 n^2\right)$.

Алгоритм допускает эффективное распараллеливание. При использовании m процессоров сложность алгоритма оценивается величиной $O\left(q^3 n^2/m\right)$.

Работа выполнена при поддержке гранта Президента РФ НШ-8.2010.10

СПИСОК ЛИТЕРАТУРЫ

1. *Анашин В. С.* О группах и кольцах, обладающих транзитивными полиномами. — В сб.: Тезисы XVI-й Всесоюзной алгебраической конференции. Часть II. Ленинград: 1981, с. 4–5.
2. *Елизаров В. П.* Конечные кольца. М.: Гелиос–АРВ, 2006.
3. *Ларин М. В.* Транзитивные полиномиальные преобразования колец вычетов. — Дискретн. матем., 2002, т. 14, в. 2, с. 20–32.