Math-Net.Ru

Общероссийский математический портал

Д. М. Ермилов, О. А. Козлитин, О строении графа полиномиального преобразования кольца Галуа, *Матем. вопр. криптогр.*, 2015, том 6, выпуск 3, 47–73

DOI: <https://doi.org/10.4213/mvk160>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.80.97.219

26 апреля 2023 г., 13:47:41

О строении графа полиномиального преобразования кольца Галуа

Д. М. Ермилов, О. А. Козлитин

ООО «Центр сертификационных исследований», Москва

Получено 02.VI.2015

Изучаются графы полиномиальных преобразований кольца Галуа R мощности q^n и характеристики p^n . Описаны цикловые структуры биективных полиномиальных преобразований кольца R , имеющих цикл максимальной возможной длины $q(q-1)p^{n-2}$, и предложен алгоритм построения таких преобразований. В небиективном случае изучаются числовые характеристики подходов к циклам.

Ключевые слова: цикловая структура графа, полином с максимальной длиной цикла, полиномиальное преобразование кольца Галуа

On the structure of graph of polynomial transformation of the Galois ring

D. M. Ermilov, O. A. Kozlitin

LLC «Sertification Research Center», Moscow

Abstract. Graphs of polynomial transformations of Galois ring R having cardinality q^n and characteristic p^n are studied. A cyclic structure of polynomial permutations having maximal possible cycle length $q(q-1)p^{n-2}$ is described and an algorithm for the construction of such permutations is proposed. For graphs of nonbijective transformations some numerical characteristics of sets of noncyclic vertices are computed.

Key words: cyclic structure of graph, polynomial with maximal length cycle, polynomial transformation of the Galois ring

Citation: *Mathematical Aspects of Cryptography*, 2015, vol. 6, no. 3, pp. 47–73 (Russian).

© 2015 Д. М. Ермилов, О. А. Козлитин

1. Введение

Синтез генераторов псевдослучайных последовательностей (ПСП), обладающих заданными криптографическими свойствами, является актуальной проблемой современной теоретической криптографии. Скорость работы генератора — одна из наиболее важных его характеристик, что обуславливает интерес к преобразованиям алгебр, строящимся на основе «быстрых» операций. К таким операциям относятся, в частности, арифметические операции в легко реализуемом кольце. Преобразование φ кольца R , использующее операции сложения и умножения в R и не использующее иные операции, называется *полиномиальным*. Оно задается некоторым полиномом (многочленом) $f(x) \in R[x]$:

$$\forall a \in R : \quad \varphi(a) = f(a)$$

и позволяет вырабатывать ПСП $u \in R^\infty$ по следующему правилу:

$$\forall i \geq 0 : \quad u(i+1) = f(u(i)).$$

Один из первых вопросов, возникающий в связи с описанным способом выработки ПСП, — это вопрос о периодических свойствах последовательности u и, шире, о строении графа $G_{f,R}$ преобразования, заданного на кольце R полиномом f . В случае когда R — конечное поле, этот вопрос тривиален: всякое преобразование поля R полиномиально (см., например, [1]), поэтому множество графов $G_{f,R}$, $f(x) \in R[x]$ совпадает с множеством всех графов преобразований поля R . Общие свойства полиномиальных преобразований примарных колец вычетов рассмотрены в [2]. Описание полноцикловых линейных и квадратичных полиномиальных преобразований колец вычетов имеется в монографии [3]. Некоторые другие классы полноцикловых полиномиальных преобразований колец вычетов указал В. С. Анашин в [4]. Описание всех полноцикловых полиномиальных преобразований колец вычетов осуществлено в [5] М. В. Лариным. А. А. Нечаев в [6] описал полиномиальные преобразования произвольного конечного локального коммутативного кольца главных идеалов (кольца Галуа – Эйзенштейна, GE-кольца). В. Е. Викторенков в работах [7] и [8] начал описание общих свойств графа полиномиального преобразования конечного локального коммутативного кольца (не обязательно кольца главных идеалов). В [7] проведена классификация вершин графа $G_{f,R}$ и найдены связи между мощностями различных классов. В [8] изучается распределение некоторых числовых характеристик случайной полиномиальной подстановки, выбранной из множества всех полиномиальных подстановок в соответствии с равномерным распределением. Работа [9] посвящена описанию длин циклов графа полиномиального преобразования кольца

Галуа. Кольца Галуа образуют класс GE-колец, содержащий в себе как все конечные поля, так и все примарные кольца вычетов (см. [10]).

Пусть R — кольцо Галуа мощности q^n и характеристики p^n , где p — число, и $q = p^r$ для некоторого $r \geq 2$: $R = GR(q^n, p^n)$. В [9] показано, что в графе полинома над кольцом R нет циклов, длина которых больше $q(q - 1)p^{n-2}$. Эксперименты на ЭВМ показывают ([9]), что биективные полиномы над R с циклом длины $q(q - 1)p^{n-2}$ существуют. Такие полиномы будем называть *полиномами с максимальной длиной цикла* над кольцом R (МДЦ-полиномами над кольцом Галуа R).

Настоящая работа посвящена решению двух задач:

1. Описание цикловой структуры произвольного МДЦ-полинома.
2. Изучение числовых характеристик подходов к циклам небиективного полиномиального преобразования.

Первой задаче посвящены разделы 2 и 3, второй — раздел 4.

Для решения задачи 1 понадобится ряд обозначений и результатов из [9]. Пусть $J = pR$ — радикал кольца R , $\Gamma(R)$ — координатное множество кольца R :

$$\Gamma(R) = \{x \in R : x^q = x\},$$

$a \in R$, $f(x) \in R[x]$ — биективный полином, $R_s = R/J^s$, $s = 1, 2, \dots, n$. Рассмотрим естественные эпиморфизмы колец

$$\varphi_s : R \rightarrow R_s, \quad s = 1, 2, \dots, n,$$

которые стандартным образом продолжаются до эпиморфизмов колец многочленов

$$\varphi_s : R[x] \rightarrow R_s[x].$$

Положим $f_s(x) = \varphi_s(f(x))$, $s = 1, 2, \dots, n$. Пусть $t_n(a)$ — длина цикла C графа $G_{f,R}$, которому принадлежит вершина a . Длину цикла $\varphi_s(C)$ графа G_{f_s,R_s} обозначим через $t_s(a)$, $s = 1, 2, \dots, n$. Когда вершина a определяется контекстом, вместо $t_s(a)$ будем писать t_s , $s = 1, 2, \dots, n$. При $t \geq 1$ положим

$$f^{[t]} = f \circ f \circ \dots \circ f \quad (t \text{ раз}),$$

где $\circ$ — композиция полиномов. Будем говорить, что $f^{[t]}(x)$ — t -я композиционная степень полинома f . Пусть $d_s = \frac{t_{s+1}}{t_s}$, $s = 1, 2, \dots, n - 1$, $F'_s(x) =$

стандартным образом определенная *производная* полинома $F_s(x) = f^{[t_s]}(x)$ (см., например, [1]), и

$$\alpha_s = F'_s(a), \quad s = 1, 2, \dots, n.$$

Образ элемента α_s при естественном эпиморфизме $\varphi_1 : R \rightarrow \bar{R} = R/J$ обозначим через $\bar{\alpha}_s$. Следуя [9], назовем вершину a графа $G_{f,R}$ *особой*, если

$$f'(a) \equiv 0 \pmod{J},$$

и *неособой* в противном случае. Из [9, следствие 2] вытекает, что в случае биективного полинома $f(x)$ граф $G_{f,R}$ не содержит особых вершин. Поэтому для любого $s \in \{1, 2, \dots, n\}$ элемент α_s обратим в кольце R , т. е. $\bar{\alpha}_s \neq 0$. Обозначим через $\text{ord } \bar{\alpha}_s$ порядок элемента $\bar{\alpha}_s$ мультипликативной группы $\bar{R}^*$. Для всякого $s \in \{1, 2, \dots, n\}$ положим

$$\delta_s = \begin{cases} p, & \text{если } \bar{\alpha}_s = \bar{e}, \\ \text{ord } \bar{\alpha}_s & \text{в противном случае,} \end{cases} \quad (1)$$

где $\bar{e} = \varphi_1(e)$ — образ единицы e кольца R .

Ранее были получены следующие результаты (см. [9, следствие 4]).

Теорема 1. Если $f(x) \in R[x]$ — биективный полином, $p > 2$ и $\delta_1 \neq p$, то последовательность $d_1, d_2, \dots, d_{n-1}$ имеет вид а), б), в) или г):

- а) $1, 1, \dots, 1$;
- б) $1, 1, \dots, 1, \delta_1$;
- в) $1, 1, \dots, 1, \delta_1, 1, 1, \dots, 1$;
- г) $1, 1, \dots, 1, \delta_1, 1, 1, \dots, 1, p, p, \dots, p$.

В каждом случае первая серия единиц может отсутствовать.

Согласно [9, утверждение 10] при условии $\delta_1 \neq p$ для всякого элемента $a \in R$ существует единственный элемент a^* со свойствами $\bar{a} = \bar{a}^*$ и $t_n(a^*) = t_1(a^*)$. Будем называть a^* *отмеченным элементом, соответствующим элементу a* . Приведем аналог теоремы 1 для $p = 2$ (см. [9, теорема б]).

Теорема 2. Если $f(x) \in R[x]$ — биективный полином, $p = 2$ и $\delta_1 \neq p$, то последовательность $d_1, d_2, \dots, d_{n-1}$ имеет вид а), б), в), г), е) или ф):

- а) $1, 1, \dots, 1$;

- b) $1, 1, \dots, \delta_1$;
- c) $1, 1, \dots, \delta_1, 1, \dots, 1$;
- d) $1, 1, \dots, \delta_1, 1, \dots, 1, 2, \dots, 2$;
- e) $1, 1, \dots, \delta_1, 1, \dots, 1, 2, 1, \dots, 1$;
- f) $1, 1, \dots, \delta_1, 1, \dots, 1, 2, 1, \dots, 1, 2, \dots, 2$.

В каждом случае первая серия единиц может отсутствовать. Ситуация а) имеет место тогда и только тогда, когда $a = a^*$. Ситуации e) и f) возможны лишь в случае, когда $(F_1^{[\delta_1]})'(a) \equiv 3e \pmod{J^2}$.

Уточним теорему 2.

Утверждение 1. В условиях теоремы 2 ситуации e) и f) имеют место тогда и только тогда, когда $(F_1^{[\delta_1]})'(a) \equiv 3e \pmod{J^2}$.

Доказательство. Пусть для некоторого значения $s > 1$ выполняются соотношения

$$F_1^{[\delta_1]}(a) \equiv a \pmod{J^s} \quad \text{и} \quad F_1^{[\delta_1]}(a) \not\equiv a \pmod{J^{s+1}}.$$

Тогда для некоторого обратимого элемента $r \in R$ получим:

$$F_1^{[\delta_1]}(a) \equiv a + p^s r \pmod{J^{s+2}}.$$

По формуле Тейлора [9, следствие 1]

$$F_1^{[2\delta_1]}(a) \equiv a + p^s r (e + (F_1^{[\delta_1]})'(a)) \pmod{J^{s+2}}.$$

Последовательность $d_1, d_2, \dots, d_{n-1}$ имеет вид e) или f) тогда и только тогда, когда

$$F_1^{[2\delta_1]}(a) \equiv a \pmod{J^{s+2}},$$

т. е. когда выполняется соотношение

$$(F_1^{[\delta_1]})'(a) \equiv 3e \pmod{J^2}. \quad \square$$

Рассмотрим эпиморфизмы

$$\psi_s : R_{s+1} \rightarrow R_s,$$

приводящие элементы кольца R_{s+1} по модулю J^s , $s \in \{1, 2, \dots, n-1\}$. Множество $\psi_s^{-1}(C)$ будем называть *прообразом* цикла C относительно эпиморфизма ψ_s . В [9, теорема 7] было доказано следующее утверждение.

Теорема 3. Пусть $f(x) \in R[x]$ — биективный полином, C — цикл длины t графа $G_{f,R}$. Тогда:

- 1) если в прообразе цикла C есть цикл длины dt , где $d \mid q - 1$ и $d > 1$, то этот прообраз состоит из одного цикла длины t и $\frac{q-1}{d}$ циклов длины dt ,
- 2) если в прообразе цикла C есть цикл длины pt , то этот прообраз состоит из $\frac{q}{p}$ циклов длины pt ,
- 3) если в прообразе цикла C есть не менее двух циклов длины t , то этот прообраз состоит из q циклов длины t .

В разделах 2 и 3 на основе теорем 1, 2 и 3 получены следующие результаты:

1. Описана цикловая структура произвольного МДЦ-полинома (теорема 4).
2. Показано, что в случае $p > 2$ свойство «быть МДЦ-полиномом» эквивалентно свойству «быть МДЦ-полиномом по модулю J^3 » (теорема 6). При некоторых ограничениях это утверждение справедливо и в случае $p = 2$ (теорема 7).
3. В случае $p > 2$ предложен алгоритм построения МДЦ-полиномов (алгоритм 1).

2. Цикловая структура МДЦ-полинома

Всюду в этом разделе $f(x) \in R[x]$ — МДЦ-полином. Вопрос о числе циклов максимальной длины в графе $G_{f,R}$ решается следующим утверждением.

Утверждение 2. Пусть $f(x) \in R[x]$ — МДЦ-полином. Тогда в графе $G_{f,R}$ имеется точно $\left(\frac{q}{p}\right)^{n-2}$ циклов длины $(q-1)qp^{n-2}$.

Доказательство. По условию $f(x)$ — МДЦ-полином. Из теоремы 1 следует, что в графе $G_{f,R}$ существует цикл, у которого последовательность

$$d_1, d_2, \dots, d_{n-1} \quad (2)$$

имеет вид

$$q-1, p, p, \dots, p.$$

Воспользовавшись пп. 1) и 2) теоремы 3, получим, что в графе $G_{f,R}$ содержится $\left(\frac{q}{p}\right)^{n-2}$ циклов длины $(q-1)qp^{n-2}$. $\square$

Замечание 1. Из утверждения 2 следует, что если $f(x)$ — МДЦ-полином, то ровно $(q-1)q^{n-1}$ элементов кольца R лежат на циклах максимальной длины графа $G_{f,R}$.

Под *цикловой структурой* регулярного графа G будем понимать таблицу

$$[l_1^{k_1}, l_2^{k_2}, \dots, l_s^{k_s}],$$

указывающую, что граф G состоит из k_1 циклов длины l_1 , k_2 циклов длины l_2 , $\dots$, k_s циклов длины l_s .

Утверждение 3. Пусть $n \geq 2$, $f(x) \in R[x]$ — МДЦ-полином. Тогда в графе $G_{f,R}$ содержится хотя бы один цикл длины $q(q-1)$ и единственный цикл длины q .

Доказательство. Сначала докажем единственность цикла длины q . Пусть в графе $G_{f,R}$ существуют два цикла C_1, C_2 длины q . Зафиксируем элемент $a \in R$, который заведомо не лежит на циклах C_1 и C_2 . Например, можно взять элемент a , лежащий на некотором цикле максимальной длины. Для выбранного элемента a существуют два различных элемента $a^*, a^{**} \in R$, которые лежат на циклах C_1 и C_2 соответственно, причем

$$\bar{a} = \bar{a}^* \quad \text{и} \quad t_n(a^*) = t_1(a^*),$$

$$\bar{a} = \bar{a}^{**} \quad \text{и} \quad t_n(a^{**}) = t_1(a^{**}).$$

Получили противоречие с теоремой 2. Следовательно, цикл длины q единствен.

Рассмотрим последовательность цикловых структур графов

$$G_{f_2, R_2}, G_{f_3, R_3}, \dots, G_{f_s, R_s}, \dots, G_{f_n, R_n}.$$

Покажем, что в цикловой структуре графа G_{f_s, R_s} есть хотя бы один цикл длины $q(q-1)$, $s = 2, 3, \dots, n$.

В силу п. 1) теоремы 3 цикловая структура графа G_{f_2, R_2} имеет вид

$$[(q(q-1))^1, q^1].$$

Пусть $s \in \{3, 4, \dots, n-1\}$, и C — цикл длины q графа G_{f_s, R_s} . По теореме 3 цикловая структура прообраза $\psi_s^{-1}(C)$ имеет один из трех видов:

- а) $[(q(q-1))^1, q^1]$,
- б) $[q^q]$,
- с) $[(pq)^{\frac{q}{p}}]$.

Случай б) невозможен, так как цикл длины q единствен. Случай с) невозможен, поскольку согласно теоремам 1 и 2 первый отличный от 1 член последовательности (2) любого цикла МДЦ-полинома равен $q-1$. Значит, цикловая структура прообраза $\psi_s^{-1}(C)$ имеет вид а) и содержит цикл длины $q(q-1)$. $\square$

Обозначим через V_i множество вершин a графа $G_{f, R}$ со свойствами

$$t_i(a) = q \quad \text{и} \quad t_{i+1}(a) = q(q-1),$$

$i = 1, 2, \dots, n-1$, а через V_n — множество вершин a со свойством $t_n(a) = q$. Цикловая структура графа $G_{f, R}(V_1)$, порожденного множеством V_1 (см., например, [11]), описана утверждением 2 и равна

$$\left[(q(q-1)p^{n-2}) \left(\frac{q}{p} \right)^{n-2} \right].$$

Из утверждения 3 следует, что цикловые структуры графов $G_{f, R}(V_{n-1})$ и $G_{f, R}(V_n)$ равны $[(q(q-1))^1]$ и $[q^1]$ соответственно. Для описания цикловой структуры графа $G_{f, R}$ осталось найти цикловые структуры графов $G_{f, R}(V_i)$, $i = 2, 3, \dots, n-3$.

Напомним, что *нормой* элемента $a \in R$ называется наибольшее $k \in \{0, 1, \dots, n\}$ со свойством $a \in J^k$. Норму элемента a обозначим через $\|a\|$. Следующая теорема описывает цикловую структуру графа $G_{f, R}$ МДЦ-полинома.

Теорема 4. Пусть $f(x) \in R[x]$ — МДЦ-полином, $F(x) = f^{[q]}(x)$ и

$$r_i = (F'(a_i))^q - F'(a_i),$$

где $a_i \in V_i$, $i = 2, 3, \dots, n-3$. Если выполняется одно из условий:

- 1) $p > 2$,
- 2) $p = 2$ и $(F^{[q-1]})'(a) \not\equiv 3e \pmod{J^2}$, где a — элемент кольца R со свойством $t_2(a) = q$,

то цикловая структура графа $G_{f,R}(V_i)$ имеет вид

$$\left[(q(q-1)p^{n-(i+1)-(\|r_i\|-1)})^{q^{\|r_i\|-1}} \left(\frac{q}{p}\right)^{n-(i+1)-(\|r_i\|-1)} \right], \text{ если } \|r_i\| < n - (i+1),$$

и $\left[(q(q-1))^{(\frac{q}{p})^{n-(i+1)}} \right]$ в противном случае.

Доказательство. Выберем и зафиксируем $i \in \{2, 3, \dots, n-3\}$. Пусть $a_i \in V_i$. Рассмотрим последовательность длин циклов

$$t_1(a_i), t_2(a_i), \dots, t_n(a_i). \quad (3)$$

По определению множества V_i

$$\forall j \in \{1, 2, \dots, i\} : t_j(a_i) = q, \quad t_{i+1}(a_i) = q(q-1).$$

Поскольку $F(x) = f^{[q]}(x)$, верно соотношение

$$F(a_i) \equiv a_i \pmod{J^i}. \quad (4)$$

Пусть $s \in \{i+2, i+3, \dots, n\}$. Так как $t_{i+1}(a_i) = q(q-1)$, то

$$F(a_i) \equiv a_i + p^i y_s \pmod{J^s} \quad (5)$$

для подходящего обратимого элемента $y_s \in R$.

Из сравнения (5) и формулы Тейлора [9, следствие 1] следует, что

$$F^{[q-1]}(a_i) \equiv a_i + p^i y_s (e + F'(a_i) + (F'(a_i))^2 + \dots + (F'(a_i))^{q-2}) \pmod{J^s}.$$

Равенство $t_s(a_i) = q(q-1)$ верно в том и только том случае, когда

$$e + F'(a_i) + (F'(a_i))^2 + \dots + (F'(a_i))^{q-2} \equiv 0 \pmod{J^{s-i}}. \quad (6)$$

Соотношение (6) равносильно следующим соотношениям:

$$(F'(a_i))^{q-1} \equiv e \pmod{J^{s-i}}, \quad (F'(a_i))^q \equiv F'(a_i) \pmod{J^{s-2}},$$

$$r_i = (F'(a_i))^q - F'(a_i) \equiv 0 \pmod{J^{s-i}}.$$

Последнее соотношение не выполняется тогда и только тогда, когда $\|r_i\| < s - i$.

Если $\|r_i\| \leq n - i - 1$, то при $s = \|r_i\| + i + 1$ верно равенство $t_s(a_i) = pq(q-1)$. Если же $\|r_i\| > n - i - 1$, то $t_j(a_i) = q(q-1)$ для любого $j \in \{i+1, i+2, \dots, n\}$. В итоге, используя теоремы 1 и 2, получаем, что при $\|r_i\| \leq n - i - 1$ последовательность (3) имеет вид

$$q, \dots, q, q(q-1), \dots, q(q-1), pq(q-1), \dots, p^{n-i-\|r_i\|}q(q-1),$$

и по теореме 3 цикловая структура графа $G_{f,R}(V_i)$ равна

$$\left[(q(q-1)p^{n-i-\|r_i\|})^{q^{\|r_i\|-1}} \left(\frac{q}{p}\right)^{n-i-\|r_i\|} \right].$$

Если $\|r_i\| > n - i - 1$, то последовательность (3) имеет вид

$$q, \dots, q, q(q-1), \dots, q(q-1),$$

и по теореме 3 цикловая структура графа $G_{f,R}(V_i)$ равна $\left[(q(q-1))^{\left(\frac{q}{p}\right)^{n-(i+1)}} \right]$. □

Уточним вид цикловой структуры графа $G_{f,R}$. Для этого изучим последовательность норм

$$\|r_2\|, \|r_3\|, \dots, \|r_{n-1}\|$$

элементов r_i из условия теоремы 4.

Утверждение 4. Пусть r_i , $i = 2, 3, \dots, n-1$, — элементы кольца R , определенные в условии теоремы 4, и при некотором $i \geq 2$ выполняется неравенство $\|r_i\| < i$. Тогда

$$\forall j \in \{i+1, i+2, \dots, n\} : \quad \|r_i\| = \|r_j\|. \quad (7)$$

Доказательство. По определению

$$r_i = (F'(a_i))^q - F'(a_i),$$

где $a_i \in V_i$, $i = 2, 3, \dots, n-1$. Выберем и зафиксируем $i \in \{2, 3, \dots, n-2\}$. Так как

$$a_i \equiv a_j \pmod{J^k}$$

для всех $j \geq i$ и $k \leq i$, то

$$r_i \equiv r_j \pmod{J^k} \quad (8)$$

для всех $j \geq i$ и $k \leq i$. Равенства (7) следуют из соотношений (8). $\square$

При $\|r_2\| = 1$ в цикловой структуре графа $G_{f,R}$ циклы не максимальной длины имеют наибольшую возможную длину. Из теоремы 4 и утверждения 4 вытекает следующее утверждение.

Следствие 1. В условиях теоремы 4 при $\|r_2\| = 1$ цикловая структура графа $G_{f,R}$ МДЦ-полинома $f(x)$ имеет вид

$$\left[(q(q-1)p^{n-2})\left(\frac{q}{p}\right)^{n-2}, (q(q-1)p^{n-3})\left(\frac{q}{p}\right)^{n-3}, \dots, \right. \\ \left. (q(q-1)p)^{\frac{q}{p}}, (q(q-1))^1, q^1 \right]. \quad (9)$$

Вычисления на ЭВМ показывают, что преобразования с цикловой структурой (9) существуют. Следующая теорема дает достаточное условие для выполнения равенства $\|r_2\| = 1$.

Теорема 5. Пусть $f(x) \in R[x]$ — МДЦ-полином, $F(x) = f^{[q]}(x)$. Если выполняется одно из условий:

- 1) $p > 2$,
- 2) $p = 2$ и $(F^{[q-1]})'(a) \not\equiv 3e \pmod{J^2}$, где a — элемент кольца R со свойством $t_2(a) = q$,

и для всех $x \in R$ выполняется соотношение

$$F''(x) \equiv 0 \pmod{J}, \quad (10)$$

то цикловая структура графа $G_{f,R}$ имеет вид (9).

Доказательство. Ввиду следствия 1 достаточно доказать равенство $\|r_2\| = 1$.

Пусть $a_2 \in V_2$ и $\bar{a}_2 = \bar{c}_0$, где $c_0 \in \Gamma(R)$. Рассмотрим такой элемент $a_1 \in V_1$, что $\bar{a}_1 = \bar{c}_0$. Существует элемент d_0 со свойствами $\bar{c}_0 = \bar{d}_0$ и $a_1 \equiv d_0 \pmod{J^2}$. Поэтому

$$a_2 \equiv d_0 + pd_1 \equiv a_1 + pd_1 \pmod{J^2}$$

для некоторого элемента $d_1 \in \Gamma(R)$. Равенство $\|r_2\| = 1$ выполняется тогда и только тогда, когда

$$(F'(a_1 + pd_1))^q \not\equiv F'(a_1 + pd_1) \pmod{J^2}.$$

Используя формулу Тейлора, получим, что следующие утверждения эквивалентны:

$$\begin{aligned} (F'(a_1) + pd_1 F''(a_1))^q &\not\equiv F'(a_1) + pd_1 F''(a_1) \pmod{J^2}, \\ (F'(a_1))^q &\not\equiv F'(a_1) + pd_1 F''(a_1) \pmod{J^2}, \\ (F'(a_1))^q - F'(a_1) &\not\equiv pd_1 F''(a_1) \pmod{J^2}. \end{aligned} \quad (11)$$

Так как $\|r_1\| = 1$, то для элемента a_1 выполняется соотношение

$$(F'(a_1))^q - F'(a_1) \not\equiv 0 \pmod{J^2},$$

равносильное соотношению

$$(F'(a_1))^q - F'(a_1) \equiv p\gamma \pmod{J^2},$$

выполняющемуся для подходящего $\gamma \in R^*$. Тогда соотношение (11) равносильно соотношению

$$\gamma \not\equiv d_1 F''(a_1) \pmod{J}. \quad (12)$$

По условию $F''(a_1) \equiv 0 \pmod{J}$. Поэтому (12) эквивалентно условию $\bar{\gamma} \neq \bar{0}$, которое, очевидно, выполняется. Следовательно, $\|r_2\| = 1$. $\square$

Следствие 2. Пусть $f(x) \in R[x]$ — МДЦ-полином, $p = 2$ и

$$(F^{[q-1]})'(a) \not\equiv 3e \pmod{J^2},$$

где $a \in R$ — элемент со свойством $t_2(a) = q$. Тогда цикловая структура графа $G_{f,R}$ имеет вид (9).

Доказательство. Так как $F(x) \equiv x \pmod{J}$, то согласно [6, теорема 1] существует такой многочлен $g(x) \in R[x]$, что $F(x) = x + (x^q - x)g(x)$. Найдем вторую производную многочлена $F(x)$:

$$\begin{aligned} F''(x) &= ((x + (x^q - x)g(x)))' = (1 + (qx^{q-1} - 1)g(x) + (x^q - x)g'(x))' = \\ &= q(q-1)x^{q-2}g(x) + (qx^{q-1} - 1)g'(x) + (qx^{q-1} - 1)g'(x) + (x^q - x)g''(x) = \\ &= q(q-1)x^{q-2}g(x) + 2(qx^{q-1} - 1)g'(x) + (x^q - x)g''(x). \end{aligned}$$

Отсюда

$$F''(x) \equiv (x^q - x)g''(x) \equiv 0 \pmod{J}.$$

Следовательно, выполняются условия теоремы 5. □

3. Построение МДЦ-полиномов

Ниже будет показано, что описание МДЦ-полиномов над кольцом R сводится к описанию МДЦ-полиномов над кольцом $R_3 = GR(q^3, p^3)$. Этот факт позволяет предложить алгоритм построения МДЦ-полиномов над кольцом R .

Теорема 6. Пусть $p > 2$, $f(x) \in R[x]$. Тогда $f(x)$ является МДЦ-полиномом над R в том и только том случае, когда полином $f_3(x)$ является МДЦ-полиномом над R_3 .

Доказательство. Необходимость. Пусть $f(x) \in R[x]$ — МДЦ-полином. В силу пункта d) теоремы 1 в графе $G_{f,R}$ существует такой цикл, что последовательность $d_1, d_2, \dots, d_{n-1}$ равна $q-1, p, \dots, p$. Это означает, что в графе G_{f_3,R_3} содержится цикл длины $q(q-1)p$, и $f_3(x)$ является МДЦ-полиномом над R_3 .

Достаточность. Пусть $f_3(x)$ — МДЦ-полином над R_3 . Тогда существует такой цикл графа G_{f_3,R_3} , что значения d_1 и d_2 равны $q-1$ и p соответственно. В силу пункта d) теоремы 1 значения d_s равны p для всех $s \in \{3, 4, \dots, n-1\}$. Это означает, что в графе $G_{f,R}$ содержится цикл длины $q(q-1)p^{n-2}$, и $f(x)$ является МДЦ-полиномом над R . □

Аналогично теореме 6 с использованием теоремы 2 доказывается следующее утверждение.

Теорема 7. Пусть $p = 2$, $f_2(x) \in R_2[x]$ — МДЦ-полином, $F(x) = f^{[q]}(x)$ и

$$(F^{[q-1]})'(a) \not\equiv 3e \pmod{J^2} \quad (13)$$

для некоторого элемента $a \in R$ со свойством $t_2(a) = q(q-1)$. Тогда $f(x)$ является МДЦ-полиномом над R в том и только том случае, когда $f_3(x)$ является МДЦ-полиномом над R_3 .

Следующее утверждение показывает, что от условия (13) отказаться нельзя.

Утверждение 5. Пусть $p = 2$, $f_2(x) \in R_2[x]$ — МДЦ-полином, $F(x) = f^{[q]}(x)$ и

$$(F^{[q-1]})'(a) \equiv 3e \pmod{J^2}$$

для некоторого элемента $a \in R$ со свойством $t_2(a) = q(q-1)$. Тогда в графе $G_{f,R}$ нет циклов длины $q(q-1)p^{n-2}$.

Доказательство. Согласно утверждению 1 для любой вершины a графа $G_{f,R}$ последовательность

$$d_1(a), d_2(a), \dots, d_{n-1}(a)$$

имеет вид

1) либо $1, 1, \dots, 1, \delta_1, 1, 1, \dots, 1, 2, 1, 1, \dots, 1$,

2) либо $1, 1, \dots, 1, \delta_1, 1, 1, \dots, 1, 2, 1, 1, \dots, 1, 2, \dots, 2$,

причем третьи серии единиц имеют длину, отличную от нуля. Тогда наибольшая длина цикла графа $G_{f,R}$ равна $q(q-1)p^{n-3}$, что и требовалось доказать. $\square$

Следующие примеры получены с помощью вычислительных экспериментов. Они показывают, что свойство «быть МДЦ-полиномом» не эквивалентно свойству «быть МДЦ-полиномом по модулю p^2R ».

Пример 1. Рассмотрим кольцо Галуа $R = GR(15625, 125)$. Кольцо R изоморфно кольцу $R' = \mathbb{Z}_{125}[y]_{/y^2+y+1}$. Элементы кольца R' суть классы вида

$$[a_1y + a_0]_{y^2+y+1},$$

которые будем обозначать векторами $(a_1, a_0) \in \mathbb{Z}_{125}^2$. Например, элемент

$$[2y + 1]_{y^2+y+1} \in R'$$

будем обозначать вектором $(2, 1)$. отождествим кольцо R с кольцом R' . Рассмотрим полином $f(x) \in R[x]$:

$$f(x) = (0, 3)x^{23} + (0, 2)x^{22} + (4, 0)x^{20} + (0, 3)x^{19} + (0, 2)x^{18} + (0, 2)x^{16} + \\ + (1, 0)x^{15} + (0, 2)x^{14} + (1, 1)x^{12} + (2, 1)x^{11} + (0, 4)x^{10} + (4, 0)x^8 + (4, 0)x^7 + \\ + (1, 2)x^6 + (2, 3)x^5 + (0, 2)x^4 + (4, 1)x^3 + (3, 0)x^2 + (4, 3)x + (0, 2).$$

Цикловая структура графа G_{f_2, R_2} равна $[600^1, 25^1]$, т. е. $f_2(x) \in R_2[x]$ — МДЦ-полином. Однако $f(x)$ не является МДЦ-полиномом, так как цикловая структура графа $G_{f, R}$ равна $[600^{26}, 25^1]$.

Пример 2. Рассмотрим кольцо Галуа $R = GR(64, 8)$. Кольцо R изоморфно кольцу $R' = \mathbb{Z}_8[y]_{/y^2+y+1}$. Рассмотрим полином $f(x) \in R[x]$:

$$f(x) = (0, 1)x^6 + (1, 0)x^5 + (0, 1)x^4 + (0, 1)x^3 + (0, 1)x^2 + (0, 1)x + (0, 1).$$

Цикловая структура графа G_{f_2, R_2} равна $[12^1, 4^1]$, т. е. граф содержит цикл длины $q(q-1)$, и полином f_2 является МДЦ-полиномом над R_2 . Но цикловая структура графа $G_{f, R}$ равна $[12^5, 4^1]$. Это означает, что $f(x)$ не является МДЦ-полиномом.

Следующий пример иллюстрирует утверждение 5.

Пример 3. Рассмотрим кольцо Галуа $R = GR(256, 16)$. Кольцо R изоморфно кольцу $R' = \mathbb{Z}_{16}[y]_{/y^2+y+1}$. Рассмотрим полином $f(x) \in R[x]$:

$$f(x) = (1, 1)x^7 + (1, 0)x^6 + (0, 1)x^5 + (1, 0)x^4 + (1, 0)x^3 + (1, 0)x^2 + (0, 1)x + (0, 1).$$

Граф G_{f_3, R_3} имеет цикловую структуру $[24^2, 12^1, 4^1]$. В нем содержится цикл длины $q(q-1)p$, и, следовательно, f_3 — МДЦ-полином над R_3 . Однако цикловая структура графа $G_{f, R}$ равна $[24^{10}, 12^1, 4^1]$, и, следовательно, $f(x)$ не является МДЦ-полиномом.

Из теоремы 6 вытекает следующее описание МДЦ-полиномов.

Следствие 3. Пусть $p > 2$. Полином $f(x) \in R[x]$ является МДЦ-полиномом над R тогда и только тогда, когда $f(x)$ представляется в виде

$$f(x) = t(x) + r(x),$$

где $t(x)$ и $r(x)$ таковы, что $\varphi_3(t(x))$ — МДЦ-полином над кольцом R_3 и $\varphi_3(r(x))$ задает тождественное преобразование кольца R_3 .

Таким образом, в случае $p > 2$ построение МДЦ-полиномов над R сводится к построению МДЦ-полиномов над R_3 . Следующие утверждения позволяют предложить алгоритм построения МДЦ-полиномов над R_3 .

Утверждение 6. Многочлен $f(x) \in R_3[x]$ является МДЦ-полиномом над кольцом R_3 тогда и только тогда, когда $f_2(x)$ — МДЦ-полином над R_2 и

$$\varphi_2(F'(a)) \in R_2 \setminus \Gamma(R_2),$$

где $F(x) = f^{[q]}(x)$ и $a \in R$ — некоторый элемент со свойством $t_2(a) = q(q - 1)$.

Доказательство. Пусть $t_2(a) = q(q - 1)$. Имеем:

$$F(a) \equiv a \pmod{J} \quad \text{и} \quad F(a) \not\equiv a \pmod{J^2}.$$

Тогда для некоторого элемента $r \in R^*$ верно соотношение

$$F(a) \equiv a + pr \pmod{J^3}. \quad (14)$$

Используя формулу Тейлора, получаем

$$F^{[q-1]}(a) \equiv a + pr(e + F'(a) + (F'(a))^2 + \dots + (F'(a))^{q-2}) \pmod{J^3}. \quad (15)$$

Условие « $f(x) \in R_3[x]$ является МДЦ-полиномом над R_3 » равносильно существованию элемента $a \in R$ со свойствами $t_2(a) = q(q - 1)$ и

$$F^{[q-1]}(a) \not\equiv a \pmod{J^3}. \quad (16)$$

Соотношение (16) выполняется в том и только том случае, когда

$$e + F'(a) + (F'(a))^2 + \dots + (F'(a))^{q-2} \not\equiv 0 \pmod{J^2}.$$

Последнему соотношению эквивалентны следующие утверждения:

$$(F'(a))^{q-1} - e \not\equiv 0 \pmod{J^2}, \quad (F'(a))^q - F'(a) \not\equiv 0 \pmod{J^2},$$

$$\varphi_2(F'(a)) \in R_2 \setminus \Gamma(R_2),$$

что и требовалось доказать. □

Следующее утверждение — необходимое и достаточное условие свойства «быть МДЦ-полиномом над R_2 ».

Утверждение 7. Многочлен $f_2(x) \in R_2[x]$ является МДЦ-полиномом тогда и только тогда, когда $f_1(x)$ — полноцикловый полином над R_1 и $\delta_1 = q - 1$.

Доказательство. В силу теоремы 1 *необходимость* очевидна. Докажем *достаточность*. Для того чтобы $f_2(x)$ являлся МДЦ-полиномом, достаточно, чтобы для некоторого элемента $a \in R$ выполнялось соотношение

$$F(a) \not\equiv a \pmod{J^2}, \quad (17)$$

где $F(x) = f^{[q]}(x)$. Пусть $a = a_0 + pa_1$ — разложение Тейхмюллера элемента a и $F(a_0) = a_0 + pr$, $r \in R$. Тогда

$$F(a_0 + pa_1) \equiv F(a_0) + pa_1 F'(a_0) \equiv a_0 + p(r + a_1 F'(a_0)) \pmod{J^2},$$

и соотношение (17) запишется в виде

$$a_1 \not\equiv r(e - F'(a_0))^{-1} \pmod{J}.$$

Поэтому элемент $a \in R$ со свойством (17) существует. $\square$

Объединяя результаты утверждений 6 и 7, получим необходимое и достаточное условие свойства «быть МДЦ-полиномом над R_3 ».

Следствие 4. Многочлен $f_3(x) \in R_3[x]$ является МДЦ-полиномом над кольцом R_3 тогда и только тогда, когда выполняются условия:

- 1) $f_1(x)$ — полноцикловый полином над полем R_1 ;
- 2) $\delta_1 = q - 1$;
- 3) $\varphi_2(F'(a)) \in R_2 \setminus \Gamma(R_2)$, где $F(x) = f^{[q]}(x)$ и $a \in R$ — некоторый элемент со свойством $t_2(a) = q(q - 1)$.

Опишем алгоритм построения МДЦ-полиномов над кольцом R_3 .

Алгоритм 1. (построение МДЦ-полинома над R_3).

Шаг 1. Пусть $\{\omega_0, \omega_1, \dots, \omega_{q-1}\}$ — полная система вычетов по модулю J . Построить такой унитарный полином $r(x) \in R[x]$, что

$$\deg r(x) \leq q - 1 \quad \text{и} \quad \forall i \in \{0, 1, \dots, q - 1\} : \quad \bar{r}(\bar{\omega}_i) = \bar{\omega}_{i+1} \pmod{q}.$$

Шаг 2. Найти такой набор $(c_0, c_1, \dots, c_{q-1}) \in \bar{R}^q$, что

$$c_0 \cdot c_1 \cdot \dots \cdot c_{q-1} = c$$

— примитивный элемент поля $\bar{R}$. Построить такой унитарный полином $t(x) \in xR[x]$, что

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

Шаг 3. Положить $f(x) = r(x) + (x^q - x)t(x)$ и для произвольного элемента $a \in R$, обладающего свойствами $\bar{a} = \bar{w}_0$ и $t_2(a) = q(q-1)$, проверить выполнение условия

$$\varphi_2(F'(a)) \in R_2 \setminus \Gamma(R_2). \quad (18)$$

Если условие (18) выполнено, то $f_3(x)$ — МДЦ-полином над R_3 , СТОП. Иначе перейти к шагу 4.

Шаг 4. По формуле производной сложной функции

$$F'(x) = (f^{[q]})'(x) = f'(f^{[q-1]}(x)) \dots f'(f(x)) \cdot f'(x). \quad (19)$$

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

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

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

$$\sum_{i=0}^{q-1} \beta_i \alpha_i^{-1} \equiv 0 \pmod{J}. \quad (20)$$

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

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

Положить

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

Тогда $g_3(x) = \varphi_3(g)(x)$ — МДЦ-полином над R_3 . СТОП.

Конец алгоритма.

Обоснование алгоритма. Покажем, что для построенного в результате работы алгоритма полинома выполнены условия 1), 2), 3) следствия 4.

На шаге 1 алгоритма строится полноцикловый полином $\bar{r}(x)$ над полем $\bar{R}$, а так как $f_1(x) = \bar{r}(x)$, то для полинома $f(x)$ выполнено условие 1) следствия 4.

На шаге 2 алгоритма полином $f_1(x)$ поднимается до полинома

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

Найдем значение $\bar{\alpha}_1 = \varphi_1(F'(a))$, где $a \in R$ — некоторый элемент со свойством $\bar{a} = \bar{w}_0$. Согласно (19)

$$F'(a) \equiv f'(f^{[q-1]}(a)) \dots f'(f(a)) \cdot f'(a) \pmod{J},$$

поэтому

$$\begin{aligned} \bar{\alpha}_1 &= \varphi_1(F'(a)) = \varphi_1(f')(\bar{w}_0)\varphi_1(f')(\bar{w}_1) \dots \varphi_1(f')(\bar{w}_{q-1}) = \\ &= (\bar{r}'(\bar{w}_0) - \bar{t}(\bar{w}_0))(\bar{r}'(\bar{w}_1) - \bar{t}(\bar{w}_1)) \dots (\bar{r}'(\bar{w}_{q-1}) - \bar{t}(\bar{w}_{q-1})) = c_0 \cdot c_1 \dots c_{q-1} = c. \end{aligned}$$

По построению c — примитивный элемент поля $\bar{R}$, а значит, $\delta_1 = \text{ord } \bar{\alpha}_1 = q - 1$, и выполняется условие 2) следствия 4.

Согласно утверждению 7 $f_2(x)$ — МДЦ-полином над R_2 . Ввиду утверждения 3 граф G_{f_2, R_2} состоит из одного цикла длины q (все элементы на нем — отмеченные) и одного цикла длины $q(q - 1)$. В частности, это означает, что существует элемент $a \in R$ со свойствами

$$\bar{a} = \bar{w}_0 \quad \text{и} \quad t_2(a) = q(q - 1). \quad (21)$$

Далее будем считать, что $a \in R$ — элемент со свойствами (21).

Если $\varphi_2(F'(a)) \in R_2 \setminus \Gamma(R_2)$, то $f_3(x)$ есть МДЦ-полином над R_3 . Пусть теперь $\varphi_2(F'(a)) \in \Gamma(R_2)$. Рассмотрим полином

$$g(x) = r(x) + (x^q - x)t(x) + p(x^q - x)h(x),$$

построенный на шаге 4 алгоритма. Пусть $G(x) = g^{[q]}(x)$. Имеем:

$$\begin{aligned} G'(a) &\equiv (\alpha_0 + p(\beta_0 - h(w_0))) \cdot (\alpha_1 + p(\beta_1 - h(w_1))) \dots (\alpha_{q-1} + p(\beta_{q-1} - h(w_{q-1}))) \equiv \\ &\equiv \alpha_0 \cdot \alpha_1 \dots \alpha_{q-1} + p \left(\alpha_0 \cdot \alpha_1 \dots \alpha_{q-1} \cdot \left(\sum_{i=0}^{q-1} \beta_i \alpha_i^{-1} + e \right) \right) \pmod{J^2}. \end{aligned}$$

Ввиду (20) получаем:

$$G'(a) \equiv \alpha_0 \cdot \alpha_1 \dots \alpha_{q-1} + p\alpha_0 \cdot \alpha_1 \dots \alpha_{q-1} \pmod{J^2}, \quad (22)$$

откуда $\varphi_2(G'(a)) \notin \Gamma(R_2)$. Таким образом, для полинома $g(x)$ выполнено условие 3) следствия 4, и $g_3(x)$ есть МДЦ-полином над R_3 .

4. Небиективный случай

Теперь обратимся к задаче 2 (см. раздел 1) — изучению числовых характеристик подходов к циклам небиективного полиномиального преобразования f кольца $R = GR(q^n, p^n)$. Напомним необходимые обозначения и результаты из работы [9].

Как и в разделе 1, введем понятие *особой* вершины a графа $G_{f,R}$, а именно вершины, для которой выполняется соотношение

$$f'(a) \equiv 0 \pmod{J}.$$

Вершины графа $G_{f,R}$, не являющиеся особыми, называются *неособыми*.

Вершины, лежащие на цикле, назовем *циклическими*. Множества циклических вершин графов $G_{f,R}$ и $G_{\bar{f},\bar{R}}$ обозначим через C_f и $C_{\bar{f}}$ соответственно. Семейство $C_f^\# = C_f + J$ назовем множеством *псевдоциклических вершин*. Очевидно, что всякая циклическая вершина является псевдоциклической. *Расстоянием* от вершины $a \in R$ до множества $C_f^\#$ (или до множества C_f) назовем минимальное $t \in \mathbb{N}_0$ со свойством $f^{[t]}(a) \in C_f^\#$ (соответственно, $f^{[t]}(a) \in C_f$). Аналогично определяется расстояние от вершины $\bar{a} \in \bar{R}$ до множества $C_{\bar{f}}$. Для этих расстояний используются обозначения $\rho(a, C_f^\#)$, $\rho(a, C_f)$, $\rho(\bar{a}, C_{\bar{f}})$ соответственно.

Утверждение 8. Для всякого $a \in R$ справедливо равенство

$$\rho(a, C_f^\#) = \rho(\bar{a}, C_{\bar{f}}).$$

Поскольку преобразование f сохраняет конгруэнции кольца R , множество $C_f^\#$ инвариантно относительно f . Поэтому можно рассматривать подграф

$$G_{f,R}(C_f^\#) \leq G_{f,R},$$

порожденный множеством вершин $C_f^\#$. Утверждение 8 сводит описание графа G_f к описанию его подграфа $G_{f,R}(C_f^\#)$.

Пусть $a \in C_f^\#$ и цикл графа $G_{\bar{f},\bar{R}}$, содержащий вершину $\bar{a}$, имеет длину l . Положим

$$C_f(a) = \{a, f(a), \dots, f^{[l-1]}(a)\}.$$

Множество $C_f^\#(a) = C_f(a) + J$ назовем *псевдоциклом*, содержащим элемент a . Связь множеств $C_f^\#$ и $C_f^\#(a)$ раскрывает следующее утверждение.

Утверждение 9. Если в графе $G_{\bar{f}, \bar{R}}(C_{\bar{f}})$ ровно k циклов и $\bar{a}_1, \bar{a}_2, \dots, \bar{a}_k$ — их представители, то

$$C_{\bar{f}}^{\#} = \bigcup_{i=1}^k C_{\bar{f}}^{\#}(a_i), \quad (23)$$

причем слагаемые в разложении (23) попарно не пересекаются.

Псевдоцикл будем называть *особым*, если среди его вершин есть особые. Псевдоциклы, не являющиеся особыми, будем называть *неособыми*. Множество всех особых псевдоциклических вершин графа $G_{\bar{f}, R}$ обозначим через $SC_{\bar{f}}^{\#}$.

Теорема 8. Справедливы утверждения:

1. Компонентами связности всякого неособого псевдоцикла являются циклы без подходов.
2. Для всякой вершины $a \in SC_{\bar{f}}^{\#}$ существует единственный элемент $b \in J$ со свойством $a + b \in C_{\bar{f}}$. В частности, если $a \in SC_{\bar{f}}^{\#}$ и $\bar{a}$ лежит на цикле длины l , то псевдоцикл $C_{\bar{f}}^{\#}(a)$ есть цикл длины l с подходами.

Утверждения 8, 9 и теорема 8 сводят задачу 2 к исследованию псевдоцикла $C_{\bar{f}}^{\#}(a)$ в ситуации, когда a — особая псевдоциклическая вершина. По п. 2 теоремы 8 при $t_1(a) = l$ (см. раздел 1) псевдоцикл $C_{\bar{f}}^{\#}(a)$ состоит из одного цикла длины l и подходов к нему. Выберем и зафиксируем некоторую вершину $b \in C_{\bar{f}}^{\#}(a)$, удовлетворяющую равенству

$$\rho(b, C_{\bar{f}}) = \max\{\rho(v, C_{\bar{f}}) \mid v \in C_{\bar{f}}^{\#}(a)\}. \quad (24)$$

Обозначим $\lambda(a, \bar{f}) = \rho(b, C_{\bar{f}})$. Очевидно, величина $\lambda(a, \bar{f})$ равна длине самого длинного подхода в псевдоцикле $C_{\bar{f}}^{\#}(a)$.

Всякой вершине $v \in R$ можно сопоставить ее проекцию $\pi(v) = f^{[\rho(\bar{v}, C_{\bar{f}})]}(v)$ на множество $C_{\bar{f}}^{\#}$ псевдоциклических вершин графа $G_{\bar{f}, R}$. Согласно утверждению 8 вершина $\pi(v)$ есть ближайшая к v псевдоциклическая вершина графа $G_{\bar{f}, R}$.

Следующая оценка вытекает из утверждения 8 и п. 2 теоремы 8.

Утверждение 10. Если $\pi(v)$ — особая вершина графа $G_{\bar{f}, R}$, $D(v)$, $T(v)$, $D(\bar{v})$ и $T(\bar{v})$ — периоды и длины подходов последовательностей

$$(v, f(v), f^{[2]}(v), \dots) \quad \text{и} \quad (\bar{v}, \bar{f}(\bar{v}), \bar{f}^{[2]}(\bar{v}), \dots)$$

соответственно, то

$$D(\bar{v}) + T(\bar{v}) \leq D(v) + T(v) \leq D(\bar{v}) + T(\bar{v}) + \lambda(\pi(v), f). \quad (25)$$

Из неравенств (25) следует, что величина $\lambda(\pi(v), f)$ показывает, насколько может увеличиться сумма $D(v) + T(v)$ при переходе от поля $R_1 = \bar{R}$ к кольцу $R_n = R$. Цель дальнейших усилий — оценить $\lambda(a, f)$ для произвольной особой вершины a .

Обозначим через $S(\bar{a}, \bar{f})$ количество особых вершин в ряду

$$a, f(a), f^{[2]}(a), \dots, f^{[l-1]}(a),$$

где $l = t_1(a)$. Очевидно, величина $S(\bar{a}, \bar{f})$ полностью определяется значением $\bar{a}$ и многочленом $\bar{f}$. Поскольку a — особая вершина, $1 \leq S(\bar{a}, \bar{f}) \leq l$.

Теорема 9. Если a — особая псевдоциклическая вершина со свойством $t_1(a) = l$, то

$$\lambda(a, f) \leq l \cdot \left\lceil \frac{n-1}{S(\bar{a}, \bar{f})} \right\rceil. \quad (26)$$

Доказательство. Пусть вершина $b \in C_f^\#(a)$ определена равенством (24). Псевдоцикл $C_f^\#(a)$ состоит из единственного цикла с подходами. Пусть

$$a_0, a_1, \dots, a_{l-1}$$

— вершины этого цикла, занумерованные так, чтобы выполнялись соотношения

$$b \equiv a_0 \pmod{J}, \quad \forall s \geq 0 : a_{s+1} = f(a_s) \quad (27)$$

(в последнем равенстве суммирование в нижнем индексе осуществляется по модулю l). Определим a_s для любого $s \in \mathbb{N}_0$: будем считать, что $a_s = a_{r_l(s)}$, где $r_l(s)$ — остаток от деления s на l . Обозначим

$$\nu_s = \|f'(a_s)\|, \quad f'(a_s) = p^{\nu_s} \cdot r_s, \quad r_s \in R^* \quad (s \in \{0, 1, \dots, l-1\}).$$

Положим

$$n_0 = 1, \quad \forall s \geq 0 : n_{s+1} = \min\{2n_s, n_s + \nu_s\}. \quad (28)$$

Индукцией по s докажем, что

$$\forall s \geq 0 : f^{[s]}(b) \equiv a_s \pmod{J^{n_s}}. \quad (29)$$

При $s = 0$ все следует из (27). Осуществим индуктивный переход от s к $s + 1$. По предположению индукции существует такой элемент $r \in R$, что

$$f^{[s]}(b) = a_s + p^{n_s} r.$$

Ввиду (27) по формуле Тейлора имеем цепочку равенств и сравнений по модулю J^{2n_s} :

$$f^{[s+1]}(b) = f(f^{[s]}(b)) = f(a_s + p^{n_s} r) \equiv a_{s+1} + p^{\nu_s} r_s p^{n_s} r.$$

Отсюда, учитывая (28), получаем: $f^{[s+1]}(b) \equiv a_{s+1} \pmod{n_{s+1}}$. Соотношение (29) доказано.

Очевидно, что

$$\begin{aligned} \lambda(a, f) &= \min\{s \geq 0 : f^{[s]}(b) \in \{a_0, a_1, \dots, a_{l-1}\}\} \leq \\ &\leq \min\{s \geq 0 : f^{[s]}(b) = a_s\} \leq \min\{s \geq 0 : n_s \geq n\}. \end{aligned}$$

Оценим последнюю величину. Согласно (28) имеем:

$$n_{s+1} = n_s, \text{ если } \nu_s = 0; \quad n_{s+1} \geq n_s + 1, \text{ если } \nu_s > 0.$$

Поэтому

$$\forall s \geq 0 : n_{s+l} \geq n_s + |\{i \in \{0, 1, \dots, l-1\} : \nu_i > 0\}| = n_s + S(\bar{a}, \bar{f}).$$

В частности, для любого $k \in \mathbb{N}$ получаем:

$$n_{kl} \geq n_0 + k \cdot S(\bar{a}, \bar{f}) = 1 + k \cdot S(\bar{a}, \bar{f}).$$

Тогда

$$\min\{s \geq 0 : n_s \geq n\} \leq l \cdot \min\{k : 1 + k \cdot S(\bar{a}, \bar{f}) \geq n\} = l \cdot \left\lceil \frac{n-1}{S(\bar{a}, \bar{f})} \right\rceil.$$

Неравенство (26) доказано. $\square$

Комбинируя утверждение 10 и теорему 9, получаем следующее утверждение.

Следствие 5. Если $\pi(v)$ — особая вершина графа $G_{f,R}$, то в обозначениях утверждения 10 верно неравенство

$$D(v) + T(v) \leq D(\bar{v}) + T(\bar{v}) \cdot \left(1 + \left\lceil \frac{n-1}{S(\pi(v), \bar{f})} \right\rceil\right).$$

В частности, $D(v) + T(v) \leq D(\bar{v}) + T(\bar{v}) \cdot n$.

Напомним [9], что если в последовательности вершин

$$(v, f(v), f^{[2]}(v), \dots) \quad (30)$$

нет особых точек, то

$$D(v) = D(\bar{v}), \quad T(v) \leq T(\bar{v}) \cdot (q-1)p^{n-2},$$

причем для МДЦ-полиномов последняя оценка достигается. Таким образом, для последовательностей (30), не содержащих особых вершин, величина $D(v) + T(v)$ растет «со скоростью» $O(p^n)$ при $n \rightarrow \infty$. В то же время для последовательностей (30), содержащих особые вершины, может выполняться условие следствия 5, и тогда величина $D(v) + T(v)$ будет расти «со скоростью» $O(n)$. Поэтому многочлен f и начальную вершину v надо выбирать так, чтобы в последовательности (30) не было особых вершин. Это гарантировано, например, если f — биективный, или если производная $\bar{f}'$ не имеет корней в поле $\bar{R}$.

Пусть, как и ранее, a — особая псевдоциклическая вершина графа $G_{f,R}$. Для всякого $s \in \{0, 1, \dots, n\}$ положим $a_s = \varphi_s(a)$, $X_s = C_{f_s}^\#(a_s)$, $G_s = G_{f_s, R_s}(X_s)$ — подграф графа G_{f_s, R_s} , порожденный множеством вершин X_s . Вершину b графа G_n будем называть *концевой*, если ее *полустепень захода* [11] в графе G_n равна 0.

Согласно п.2 теоремы 8 граф G_n есть цикл с подходами. Цель дальнейших усилий — оценить число концевых вершин в графе G_n .

Пусть $[\alpha]$ — целая часть числа $\alpha \in \mathbb{Q}$.

Лемма 1. Если $b \in X_n$ — особая вершина, $\nu = \|f'(b)\|$, $k = \min\{\lfloor \frac{n}{2} \rfloor, \nu\}$. Тогда полустепень захода вершины $f(b)$ в графе G_n не меньше q^k .

Доказательство. Пусть элемент $r^* \in R^*$ определен равенством $f'(b) = p^\nu r^*$. Согласно формуле Тейлора при условии $t \geq \lfloor \frac{n}{2} \rfloor$ для всякого $r \in R$ имеет место цепочка равенств

$$f(b + p^t r) = f(b) + f'(b)p^t r = f(b) + p^{t+\nu} r r^*.$$

Следовательно, при $t = \max\{\lfloor \frac{n}{2} \rfloor, n - \nu\}$ полустепень захода вершины $f(b)$ не меньше, чем q^{n-t} . Осталось убедиться, что $n - t = \min\{\lfloor \frac{n}{2} \rfloor, \nu\} = k$. $\square$

В [9] получен следующий результат.

Лемма 2. Если $b \in X_n$ — неособая вершина, то полустепень захода вершины $f(b)$ в графе G_n равна 1.

Обозначим через $K(G_n)$ количество концевых вершин в графе G_n . Леммы 1 и 2 позволяют получить нижнюю оценку для величины $K(G_n)$. Заметим, что для всякой концевой вершины $v \in V_2$ все вершины из множества $\varphi_2^{-1}(v) \in V_n$ также являются концевыми. Поэтому при $n \geq 2$ верно неравенство

$$K(G_n) \geq q^{n-2}K(G_2), \quad (31)$$

и осталось исследовать граф G_2 . Граф G_2 есть цикл с подходами, состоящий из ql вершин, где l — длина цикла. На цикле графа G_2 имеется по крайней мере одна особая вершина (например, та, которая сравнима с a_2 по модулю J). Рассмотрим участок цикла, заключенный между двумя особыми вершинами (начало и конец участка могут совпадать):

$$c_1, c_2, c_3, \dots, c_s, c_{s+1},$$

где c_1, c_{s+1} — особые вершины, $c_2, c_3, \dots, c_s$ — неособые вершины. Согласно лемме 2 полустепени захода вершин $c_3, c_4, \dots, c_s, c_{s+1}$ равны 1. Исследуем строение подхода к вершине $c_{s+2} = f(c_{s+1})$. Этот подход представляет собой граф $T = G_2(V)$, где

$$V = \{v \in X_2 \setminus \{c_{s+1}\} \mid \exists m \geq 0 : f^{[m]}(v) = c_{s+2}\}.$$

Известно, что граф T является деревом. Пусть в дереве T есть маршрут из вершины u в вершину v . Тогда наименьшее $m \geq 0$ со свойством $f^{[m]}(u) = v$ будем обозначать через $\rho(u, v)$. Следующее утверждение исчерпывающе описывает строение дерева T .

Утверждение 11. В дереве T ровно $s(q-1) + 1$ вершин. При этом:

- 1) вершина c_{s+2} имеет полустепень захода $q-1$, а остальные неконцевые вершины имеют полустепень захода 1,
- 2) число концевых вершин равно $q-1$, причем для любой концевой вершины u верно равенство $\rho(u, c_{s+2}) = s$.

Доказательство. Вершина c_{s+1} является особой. Поскольку индекс нильпотентности кольца R_2 равен 2, согласно лемме 1 полустепень захода вершины c_{s+2} в графе G_2 равна q (больше, чем q , она, очевидно, быть не может). Поскольку вершина c_{s+1} не является вершиной дерева T , полустепень захода вершины c_{s+2} в дереве T равна $q-1$.

Выберем и зафиксируем произвольную вершину v_1 дерева T , для которой $f(v_1) = c_{s+2}$. Очевидно, $\bar{v}_1 = \bar{c}_{s+1}$. Вершина c_s — неособая, поэтому существует такой $r \in R$, что $f(c_s + pr) = v_1$. Положим $v_2 = c_s + pr$. Так как вершина v_2 неособая, то по лемме 2 полустепень захода вершины v_1 в дереве T равна 1.

Аналогично, поскольку c_{s-1} — неособая вершина, существует вершина v_3 со свойством $f(v_3) = v_2$. При этом вершина v_3 — неособая, и полустепень захода вершины v_2 в дереве T равна 1. Продолжая описанный процесс далее, получаем, что в дереве T существует цепь

$$v_s \rightarrow v_{s-1} \rightarrow v_{s-2} \rightarrow \dots \rightarrow v_3 \rightarrow v_2 \rightarrow v_1. \quad (32)$$

При этом полустепени захода каждой из вершин $v_1, v_2, \dots, v_{s-1}$ в дереве T равны 1, и $\bar{v}_s = \bar{c}_2$.

Покажем, что вершина v_s — концевая. Действительно, если вершина x такова, что $f(x) = v_s$, то $x = c_1 + pr$ для некоторого $r \in R$. Вершина c_1 — особая. Поэтому, согласно лемме 1, полустепень захода вершины c_2 в графе G_2 равна q . Следовательно, для любого $r \in R$ верно равенство $f(c_1 + pr) = c_2$, а тогда $f(x) \neq v_s$.

Итак, дерево T состоит из $(q - 1)$ попарно не пересекающихся по вершинам цепей вида (32), вершины c_{s+2} и дуг, соединяющих конечные вершины цепей (32) с вершиной c_{s+2} . Поэтому в дереве T ровно $(q - 1)s + 1$ вершин, $q - 1$ концевых вершин и расстояние от любой концевой вершины до вершины c_{s+2} равно s . $\square$

Утверждение 11 позволяет вычислить величину $K(G_2)$. Действительно, согласно п. 2 утверждения 11 число концевых вершин в $q - 1$ раз больше количества особых вершин на цикле графа G_2 :

$$K(G_2) = (q - 1) \cdot S(\bar{f}, \bar{a}).$$

Комбинируя полученное равенство и неравенство (31), получаем следующее утверждение.

Теорема 10. *Если a — особая псевдоциклическая вершина и G — подграф графа $G_{\bar{f}, R}$, порожденный множеством $C_{\bar{f}}^{\#}(a)$, то количество концевых вершин в графе G не меньше $q^{n-2}(q - 1) \cdot S(\bar{f}, \bar{a})$.*

Обозначим через $S_{\bar{f}}$ множество всех особых вершин графа $G_{\bar{f}, R}$. Утверждение 9 и теорема 10 обосновывают следующий факт.

Следствие 6. Если $\bar{f}$ — биекция, то число $K(G_{\bar{f},R})$ концевых вершин графа $G_{\bar{f},R}$ удовлетворяет неравенству

$$K(G_{\bar{f},R}) \geq q^{n-2}(q-1) \cdot |S_{\bar{f}}|.$$

Авторы благодарны профессору Александру Александровичу Нечаеву за постановку задачи и внимание к этой работе и посвящают статью светлой памяти безвременно ушедшего учителя.

Список литературы

- [1] Глухов М. М., Елизаров В. П., Нечаев А. А., *Алгебра*, М.: Гелиос-АРВ, 2003, 749 с.
- [2] Carlitz L., “Functions and polynomials (mod p^n)”, *Acta Arithmetica*, 1964, № 9, 66–78.
- [3] Кнут Д. Э., *Искусство программирования*, 2, Москва–Санкт-Петербург–Киев: Изд. дом Вильямс, 2000, 828 с.
- [4] Анашин В. С., “О группах и кольцах, обладающих транзитивными полиномами”, XVI Всесоюзная алгебраическая конференция: тезисы, ч. II, 1981, 4–5.
- [5] Ларин М. В., “Транзитивные полиномиальные преобразования колец вычетов”, *Дискретн. матем.*, 14:2 (2002), 20–32.
- [6] Нечаев А. А., “Полиномиальные преобразования конечных коммутативных колец главных идеалов”, *Математические заметки*, 27:6 (1980), 885–899.
- [7] Викторенков В. Е., “Орграф полиномиального преобразования над коммутативным локальным кольцом”, *Обозр. прикл. и промыш. матем.*, 7:2 (2000), 327.
- [8] Викторенков В. Е., “О некоторых характеристиках цикловой структуры случайных равновероятных подстановок с помеченными циклами и их применение для исследования полиномиальных преобразований колец”, *Обозр. прикл. и промыш. матем.*, 10:3 (2003), 621.
- [9] Ермилов Д. М., Козлитин О. А., “Цикловая структура полиномиального генератора над кольцом Галуа”, *Математические вопросы криптографии*, 4:1 (2013), 27–57.
- [10] Елизаров В. П., *Конечные кольца*, М.: Гелиос-АРВ, 2006, 304 с.
- [11] Асанов М. О., Баранский В. А., Расин В. В., *Дискретная математика: графы, матроиды, алгоритмы*, Ижевск: НИЦ Регулярная и хаотическая динамика, 2001, 288 с.