Math-Net.Ru

Общероссийский математический портал

О. А. Козлитин, Периодические свойства многомерного полиномиального генератора над кольцом Галуа. I, *Матем. вопр. криптогр.*, 2018, том 9, выпуск 3, 61–98

DOI: <https://doi.org/10.4213/mvk263>

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: 54.162.127.20

26 апреля 2023 г., 18:11:24

**Периодические свойства
многомерного полиномиального генератора
над кольцом Галуа. I**

О. А. Козлитин

ООО «Центр сертификационных исследований», Москва

Получено 18.IV.2018

Аннотация. Изучаются периодические свойства многомерных полиномиальных подстановок над кольцом Галуа R . Вычислен максимум $L_m(R)$ длин циклов m -мерных полиномиальных подстановок. Предложен метод построения подстановок, обладающих циклом длины $L_m(R)$. В частном случае найден цикловой тип m -мерной полиномиальной подстановки. Работа обобщает полученные ранее результаты на случай произвольной размерности m и произвольного кольца Галуа R .

Ключевые слова: полиномиальный генератор, полиномиальная подстановка, цикловой тип

**Periodic properties of multidimensional polynomial generator
over the Galois ring. I**

O. A. Kozlitin

Certification Research Center, LLC, Moscow

Abstract. Periodic properties of multidimensional polynomial substitutions over the Galois ring are investigated. Maximum $L_m(R)$ of cycle lengths of m -dimensional polynomial substitutions is computed. A method permitting to construct substitutions with cycle of length $L_m(R)$ is suggested. For a particular case the cycle type of m -dimensional polynomial substitution is founded. The paper generalizes earlier results to the case of arbitrary dimension m and arbitrary Galois ring R .

Key words: polynomial generator, polynomial substitution, cycle type

1. Введение

Пусть R — конечное коммутативное кольцо с единицей e , $m \geq 2$, и $\mathbf{x} = (x_1, x_2, \dots, x_m)$ — строка переменных над кольцом R . Рассмотрим семейство многочленов

$$F_1(\mathbf{x}), \dots, F_m(\mathbf{x}) \in R[\mathbf{x}] \quad (1)$$

со свойством: преобразование $F: R^m \rightarrow R^m$, определенное равенством

$$F(\mathbf{x}) = (F_1(\mathbf{x}), \dots, F_m(\mathbf{x})), \quad (2)$$

биективно. В этой ситуации преобразование F будем называть *многомерной (m -мерной) полиномиальной подстановкой* с координатными полиномами (1).

Генератор, функция обратной связи которого задана равенством (2), называют *полиномиальным*. Такой генератор может быть использован для выработки псевдослучайных последовательностей с наперед заданными криптографическими свойствами (периодическими, сложностными и статистическими). Частным случаем полиномиального генератора является полиномиальный регистр сдвига. В этой работе рассматриваются *периодические* свойства полиномиального генератора.

Одномерный полиномиальный генератор над кольцом вычетов глубоко изучен М. В. Лариным [8]. В. С. Анашин [13] анонсировал описание всех конечных коммутативных колец с единицей, допускающих транзитивные полиномиальные преобразования.

В. Е. Викторенков [1] ввел терминологию и разработал основы математического аппарата, которые позволяют описывать периодические свойства полиномиальных преобразований произвольного конечного коммутативного кольца с единицей. В [4] и [5] получен ряд результатов о цикловой структуре биективного полиномиального преобразования кольца Галуа. В. Е. Викторенков [2] описал подходы к циклам небиективного полиномиального преобразования произвольного конечного коммутативного кольца с единицей, а также получил ряд результатов о длинах циклов. В [6] показано, что в классе колец Галуа–Эйзенштейна с заданными индексом нильпотентности и мощностью наибольшим периодом выходной последовательности обладают полиномиальные генераторы над кольцами Галуа.

Периодические свойства многомерного полиномиального генератора над кольцом вычетов изучал Н. Г. Парватов [16]. Одномерные полиномиальные преобразования произвольного конечного коммутативного цепного кольца (в частности, кольца Галуа) описаны и перечислены А. А. Нечаевым [12].

В [10] он построил так называемый *базис обобщенных тождеств* конечно-го коммутативного цепного кольца R , позволяющий перечислять его многомерные полиномиальные преобразования. В [14, § 5] содержится формула для числа m -местных полиномиальных функций над кольцом Галуа, из которой легко выводится формула для числа преобразований вида (2).

В настоящей работе изучается цикловая структура многомерных полиномиальных подстановок над кольцом Галуа, обладающих циклом максимальной возможной длины. Интерес к семейству колец Галуа обусловлен тем, что он включает в себя как все конечные поля, так и все примарные кольца вычетов. Согласно В. R. McDonald, “It is classically accepted that the researcher handles separately the finite field $GF(p^m)$ and the prime ring $\mathbb{Z}_{p^n}$. It is our belief that both cases should be treated simultaneously in the setting of a Galois ring” [15, с. 307].

Пусть $L_m(R)$ — максимум длин циклов m -мерных полиномиальных подстановок над кольцом Галуа R . Опишем основные результаты настоящей работы.

1. Показано, что для всякого *собственного* кольца Галуа R , т.е. кольца Галуа, отличного от конечного поля и от примарного кольца вычетов, верно равенство

$$L_m(R) = q^m (q^m - 1) p^{n-2}$$

(теорема 2).

2. Пусть $\tau(F, 2, \mathbf{x})$ — период последовательности

$$\mathbf{x}, F(\mathbf{x}), F(F(\mathbf{x})), \dots, \quad (3)$$

приведенной по модулю $p^2 R$. Описаны подстановки с *длинными циклами*, т.е. полиномиальные подстановки F , для которых существует $\mathbf{x} \in R^m$ со свойством $\tau(F, 2, \mathbf{x}) = q^m (q^m - 1)$ (следствие 2). Найдено количество вершин $\mathbf{x} \in R^m$, принадлежащих длинным циклам (следствие 3).

3. Предложен метод построения полиномиальных подстановок с циклом максимальной возможной длины $L_m(R)$ (МДЦ-подстановок, алгоритм А). В частном случае найден цикловой тип МДЦ-подстановки (теорема 8).

В статье обобщен ряд утверждений из [4], [5] и [16].

2. Максимальная длина цикла

Всюду далее $R = GR(q^n, p^n)$ — кольцо Галуа мощности q^n и характеристики p^n , $q = p^t$. Каждый полином $F_i(\mathbf{x}) \in R[\mathbf{x}]$ есть сумма мономов:

$$F_i(\mathbf{x}) = w_1(\mathbf{x}) + w_2(\mathbf{x}) + \dots + w_t(\mathbf{x}).$$

Стандартным образом определим *частную производную* монома

$$w(\mathbf{x}) = a x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}$$

по переменной x_j :

$$\frac{\partial w(\mathbf{x})}{\partial x_j} = \alpha_j a x_1^{\alpha_1} \dots x_{j-1}^{\alpha_{j-1}} x_j^{\alpha_j-1} x_{j+1}^{\alpha_{j+1}} \dots x_m^{\alpha_m}$$

(если $\alpha_j = 0$, то соответствующая частная производная считается равной 0). Распространив это определение по линейности, получим определение частной производной полинома $F_i(\mathbf{x})$ по переменной x_j :

$$\frac{\partial F_i(\mathbf{x})}{\partial x_j} = \sum_{s=1}^t \frac{\partial w_s(\mathbf{x})}{\partial x_j}.$$

Следуя [16], составим из частных производных *матрицу Якоби*:

$$J_F(\mathbf{x}) = \begin{pmatrix} \frac{\partial F_1(\mathbf{x})}{\partial x_1} & \frac{\partial F_2(\mathbf{x})}{\partial x_1} & \dots & \frac{\partial F_m(\mathbf{x})}{\partial x_1} \\ \frac{\partial F_1(\mathbf{x})}{\partial x_2} & \frac{\partial F_2(\mathbf{x})}{\partial x_2} & \dots & \frac{\partial F_m(\mathbf{x})}{\partial x_2} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial F_1(\mathbf{x})}{\partial x_m} & \frac{\partial F_2(\mathbf{x})}{\partial x_m} & \dots & \frac{\partial F_m(\mathbf{x})}{\partial x_m} \end{pmatrix}.$$

Выберем произвольное $s \in \{1, 2, \dots, n\}$. Для всякой полиномиальной подстановки F (вектора $\mathbf{x}$) обозначим через $\tilde{F}$ (соответственно, через $\tilde{\mathbf{x}}$) образ этой подстановки (вектора) при естественном эпиморфизме $R \rightarrow R/p^s R$. Обозначим через $\tau(F, s, \mathbf{x})$ длину того цикла подстановки $\tilde{F}$, которому принадлежит вектор $\tilde{\mathbf{x}}$.

Получим многомерный кольцевой аналог формулы Тейлора. Пусть

$$w(\mathbf{x}) = a x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}, \quad \mathbf{z} = (z_1, z_2, \dots, z_m), \quad l \geq 1.$$

Ввиду очевидного соотношения

$$(x_1 + p^s z_1)^{\alpha_1} \equiv x_1^{\alpha_1} + \alpha_1 x_1^{\alpha_1-1} p^s z_1 \pmod{p^{2s} R}$$

имеем:

$$\begin{aligned} w(\mathbf{x} + p^s \mathbf{z}) &\equiv \\ &\equiv a x_1^{\alpha_1} \prod_{i=2}^m (x_i + p^s z_i)^{\alpha_i} + a \alpha_1 x_1^{\alpha_1-1} x_2^{\alpha_2} \dots x_m^{\alpha_m} p^s z_1 \pmod{p^{2s} R}. \end{aligned}$$

Выполняя то же преобразование по 2-й, 3-й, ..., m -й переменным, получим цепочку сравнений по модулю $p^{2s} R$:

$$\begin{aligned} w(\mathbf{x} + p^s \mathbf{z}) &\equiv w(\mathbf{x}) + a \sum_{i=1}^m x_1^{\alpha_1} \dots x_{i-1}^{\alpha_{i-1}} \alpha_i x_i^{\alpha_i-1} x_{i+1}^{\alpha_{i+1}} \dots x_m^{\alpha_m} p^s z_i = \\ &= w(\mathbf{x}) + p^s \mathbf{z} \left(\frac{\partial w}{\partial x_1}(\mathbf{x}), \dots, \frac{\partial w}{\partial x_m}(\mathbf{x}) \right)^T, \end{aligned}$$

где « T » — операция транспонирования. Поэтому для всякого $i \in \{1, 2, \dots, m\}$ верно соотношение

$$F_i(\mathbf{x} + p^s \mathbf{z}) \equiv F_i(\mathbf{x}) + p^s \mathbf{z} J_i^\downarrow(\mathbf{x}) \pmod{p^{2s} R},$$

где $J_i^\downarrow(\mathbf{x})$ — i -й столбец матрицы Якоби $J_F(\mathbf{x})$. Отсюда

$$F(\mathbf{x} + p^s \mathbf{z}) \equiv F(\mathbf{x}) + p^s \mathbf{z} J_F(\mathbf{x}) \pmod{p^{2s} R}. \quad (4)$$

Поскольку преобразование F биективно, матрица $J_F(\mathbf{x})$ обратима для любого $\mathbf{x} \in R^m$.

Для всякого $s \in \{1, 2, \dots, n\}$ обозначим через τ_s величину $\tau(F, s, \mathbf{x})$. Положим

$$f_s = F^{[\tau_s]} = \underbrace{F \circ F \circ \dots \circ F}_{\tau_s \text{ раз}}.$$

Тогда, очевидно,

$$f_s(\mathbf{x}) \equiv \mathbf{x} \pmod{p^s R}.$$

Выразим матрицу $J_{f_1}(\mathbf{x})$ через матрицы $J_F(\bullet)$.

Исходя из определения производной нетрудно доказать стандартное правило дифференцирования произведения: для любых $u(\mathbf{x}), v(\mathbf{x}) \in R[\mathbf{x}]$, $i \in \{1, 2, \dots, m\}$ верно равенство

$$\frac{\partial u(\mathbf{x})v(\mathbf{x})}{\partial x_i} = v \frac{\partial u(\mathbf{x})}{\partial x_i} + u \frac{\partial v(\mathbf{x})}{\partial x_i}.$$

Поэтому если $G(\mathbf{x}) = (G_1(\mathbf{x}), G_2(\mathbf{x}), \dots, G_m(\mathbf{x}))$ — полиномиальная подстановка над R , то

$$\begin{aligned} \frac{\partial w(G(\mathbf{x}))}{\partial x_i} &= \frac{\partial}{\partial x_i} (a G_1(\mathbf{x})^{\alpha_1} G_2(\mathbf{x})^{\alpha_2} \dots G_m(\mathbf{x})^{\alpha_m}) = \\ &= \sum_{t=1}^m a G_1(\mathbf{x})^{\alpha_1} G_2(\mathbf{x})^{\alpha_2} \dots G_{t-1}(\mathbf{x})^{\alpha_{t-1}} (\alpha_t G_t(\mathbf{x})^{\alpha_t-1}) \times \\ &\quad \times G_{t+1}(\mathbf{x})^{\alpha_{t+1}} \dots G_m(\mathbf{x})^{\alpha_m} \frac{\partial G_t(\mathbf{x})}{\partial x_i} = \\ &= \sum_{t=1}^m \left(\frac{\partial w}{\partial x_t}(G) \cdot \frac{\partial G_t(\mathbf{x})}{\partial x_i} \right). \end{aligned}$$

Распространив полученное равенство по линейности, получим:

$$\frac{\partial F_j(G(\mathbf{x}))}{\partial x_i} = \sum_{t=1}^m \left(\frac{\partial F_j}{\partial x_t}(G) \cdot \frac{\partial G_t(\mathbf{x})}{\partial x_i} \right).$$

Отсюда получаем стандартную формулу «производной сложной функции»:

$$J_{F(G)}(\mathbf{x}) = J_G(\mathbf{x}) \cdot J_F(G(\mathbf{x})).$$

Из этой формулы следует равенство

$$J_{f_1}(\mathbf{x}) = \prod_{s=0}^{\tau_1-1} J_F(F^{[s]}(\mathbf{x})). \quad (5)$$

Пусть $J(\mathbf{x}) = J_{f_1}(\mathbf{x})$, $\overline{J(\mathbf{x})}$ есть образ матрицы $J(\mathbf{x})$ под действием естественного эпиморфизма $R \rightarrow \overline{R} = R/pR$. Ввиду (5) матрица $\overline{J(\mathbf{x})}$ является невырожденной при любом $\mathbf{x} \in R^m$. Следуя [16], обозначим через $\text{ord}_p J(\mathbf{x})$ порядок матрицы $\overline{J(\mathbf{x})}$ как элемента группы $\overline{R}_{m \times m}^*$ невырожденных $m \times m$ -матриц над полем $\overline{R}$.

Сформулируем центральный результат работы [16].

Теорема 1. Пусть $R = \mathbb{Z}_{p^n}$, $n \geq 2$, F — полиномиальная подстановка над R . Тогда

$$\tau(F, n, \mathbf{x}) \mid \tau_1 \cdot p^{n-1} \cdot \text{ord}_p J(\mathbf{x}) \quad (6)$$

при любом $\mathbf{x} \in R^m$. Если дополнительно известно, что $\bar{e}$ не является собственным значением матрицы $\overline{J(\mathbf{x})}$, то

$$\tau(F, n, \mathbf{x}) \mid \tau_1 \cdot p^{n-2} \cdot \text{ord}_p J(\mathbf{x}). \quad (7)$$

Рассмотрим величину

$$\xi(m, n, p) = \begin{cases} 2^{n+2}, & \text{если } m = p = 2, \\ p^{m+n-2}(p^m - 1) & \text{в противном случае.} \end{cases}$$

Следующий результат не нов. В целях полноты изложения получим его как следствие из теоремы 1.

Следствие 1. В условиях теоремы 1 для всякого $\mathbf{x} \in R^m$ верно неравенство $\tau(F, n, \mathbf{x}) \leq \xi(m, n, p)$.

Доказательство. Пусть $\chi(x)$ — характеристический многочлен матрицы $J(\mathbf{x})$. Возможны следующие случаи.

1. $m = p = 2$. В этой ситуации $R = \mathbb{Z}_{2^n}$. Поскольку $\overline{J(\mathbf{x})}$ — невырожденная матрица над $\overline{R} = \mathbb{Z}_2$, возможны два варианта: либо $\overline{\chi}(x) = x^2 \oplus \bar{e}$, либо $\overline{\chi}(x) = x^2 \oplus x \oplus \bar{e}$.

Если $\overline{\chi}(x) = x^2 \oplus \bar{e}$, то либо $\overline{J(\mathbf{x})} = E$ — единичная матрица, либо

$$\overline{J(\mathbf{x})} \approx \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

В обоих случаях $\text{ord } {}_p J(\mathbf{x}) \mid 2$. Тогда согласно (6) имеем:

$$\tau(F, n, \mathbf{x}) \leq 4 \cdot 2^{n-1} \cdot 2 = 2^{n+2} = \xi(m, n, p).$$

Если $\overline{\chi}(x) = x^2 \oplus x \oplus \bar{e}$, то в поле $GF(4)$ имеет место каноническое разложение $\overline{\chi}(x) = (x - \alpha)(x - \alpha^2)$, где $\text{ord } \alpha = 3$. Минимальный многочлен матрицы $\overline{J(\mathbf{x})}$ равен $\overline{\chi}(x)$, и, следовательно, $\text{ord } \overline{J(\mathbf{x})} = \text{ord } \alpha = 3$. Очевидно, $\bar{e}$ не является собственным значением матрицы $\overline{J(\mathbf{x})}$, и потому согласно (7) имеем:

$$\tau(F, n, \mathbf{x}) \leq 4 \cdot 2^{n-2} \cdot 3 < 2^{n+2} = \xi(m, n, p).$$

2. $m > 2$ или $p > 2$. Если $\bar{e}$ не является собственным значением матрицы $\overline{J(\mathbf{x})}$, то согласно (7) справедлива цепочка неравенств

$$\tau(F, n, \mathbf{x}) \leq p^m \cdot p^{n-2} \cdot (p^m - 1) = \xi(m, n, p).$$

Поэтому далее считаем, что $\bar{e}$ — собственное значение матрицы $\overline{J(\mathbf{x})}$. В этой ситуации существуют такие $k \in \{1, 2, \dots, m\}$ и унитарный многочлен $g(x) \in \overline{R}[x]$, что

$$\overline{\chi}(x) = (x - \bar{e})^k \cdot g(x) \quad \text{и} \quad g(\bar{e}) \neq 0.$$

Матрица $\overline{J(\mathbf{x})}$ подобна распавшейся матрице:

$$\overline{J(\mathbf{x})} \approx \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

где $\chi_A(x) = (x - \bar{e})^k$, $\chi_B(x) = g(x)$. Если $m_A(x) = (x - \bar{e})^s$ — минимальный многочлен матрицы A , то $\text{ord } A = p^c$, где

$$c = \lceil \log_p s \rceil \leq \lceil \log_p k \rceil.$$

Очевидно,

$$\text{ord } \overline{J(\mathbf{x})} \mid p^c \cdot \text{ord } B \leq p^c(p^{m-k} - 1) = p^{m-k+c} - p^c.$$

Возможны следующие случаи:

1. $k = 1$. Тогда $A = (\bar{e})$, и $\text{ord } \overline{J(\mathbf{x})} = \text{ord } B \leq p^{m-1} - 1$.
2. $k \geq 2$. В этой ситуации $c \leq \lceil \log_p k \rceil < k$, и $\text{ord } \overline{J(\mathbf{x})} \leq p^{m-1} - 1$.

В обоих случаях $\text{ord } \overline{J(\mathbf{x})} \leq p^{m-1} - 1$. Поэтому согласно (4)

$$\tau(F, n, \mathbf{x}) \leq p^m \cdot p^{n-1} \cdot (p^{m-1} - 1) = p^{m+n-2}(p^m - p) < \xi(m, n, p). \quad \square$$

Пусть $R = GR(q^n, p^n)$ — кольцо Галуа. Предложим верхнюю оценку для величины $\tau(F, n, \mathbf{x})$, зависящую только от размерности m подстановки F и параметров p, q, n кольца R . При доказательстве этой оценки нам понадобится кольцевой аналог понятия *двойственного базиса*, широко известного в случае, когда R — конечное поле (см., например, [9]).

Пусть $\text{Aut}(R)$ — группа автоморфизмов кольца R , функция «след» $\text{Tr}: R \rightarrow Q = \mathbb{Z}_{p^n}$ определена равенством

$$\text{Tr}(x) = \sum_{\sigma \in \text{Aut}(R)} \sigma(x).$$

Известно, что функция «след» является эпиморфизмом модулей ${}_Q R \rightarrow {}_Q Q$. Рассмотрим симметричную билинейную функцию $\varphi: R \times R \rightarrow Q$:

$$\forall \alpha, \beta \in R: \quad \varphi(\alpha, \beta) = \text{Tr}(\alpha \cdot \beta).$$

Заметим, что если для некоторого $\alpha \in R$ верно равенство $\varphi(\alpha, R) = 0$, то $\alpha = 0$. Действительно, если $\alpha \neq 0$, то $\alpha = p^k u$, где $u \in R^*$, $k < n$. Ввиду сюръективности функции «след» существует такой $\beta \in R$, что $\varphi(u, \beta) = e$. Но тогда $\varphi(\alpha, \beta) = p^k e \neq 0$. Противоречие.

Пусть $\mathbf{e} = (e_1, e_2, \dots, e_t)$ — базис модуля ${}_Q R$. Для всякого $j \in \{1, 2, \dots, t\}$ рассмотрим систему уравнений относительно $x \in R$:

$$\varphi(x, e_i) = \delta_{i,j}, \quad i = 1, 2, \dots, t, \quad (8)$$

где $\delta_{i,j}$ — символ Кронекера. Раскладывая x по базису $\mathbf{e}$, перейдем от системы (8) к системе линейных уравнений над кольцом Q :

$$\delta_{i,j} = \sum_{s=1}^t x_s \cdot \varphi(e_s, e_i), \quad i = 1, 2, \dots, t. \quad (9)$$

Матрица системы (9) обратима, поскольку система

$$\varphi(x, e_i) = 0, \quad i = 1, 2, \dots, t,$$

имеет единственное (нулевое) решение). Следовательно, система (9) (а значит, и система (8)) имеет единственное решение.

Обозначим единственное решение системы (8) через e'_j , $j = 1, 2, \dots, t$. Система $\mathbf{e}' = (e'_1, e'_2, \dots, e'_t)$ является базисом модуля ${}_Q R$. Действительно, пусть $\alpha \in R$ и

$$\varphi(\alpha, e_i) = a_i, \quad i = 1, 2, \dots, t. \quad (10)$$

Совокупность равенств (10) можно рассматривать как систему уравнений относительно α . Как и система (8), система (10) имеет единственное решение. Это решение равно

$$a_1 e'_1 + a_2 e'_2 + \dots + a_t e'_t.$$

Поэтому

$$\alpha = a_1 e'_1 + a_2 e'_2 + \dots + a_t e'_t,$$

и $\mathbf{e}'$ — базис модуля ${}_Q R$. Базис $\mathbf{e}'$ иногда называют *ортгоналим* к базису $\mathbf{e}$. В рамках этой работы будем называть базис $\mathbf{e}'$ *двойственным* к базису $\mathbf{e}$.

Сформулируем и докажем центральный результат этого раздела.

Теорема 2. Пусть $R = GR(q^n, p^n)$ — кольцо Галуа, отличное от примарного кольца вычетов и от конечного поля, $q = p^t$. Тогда

$$L_m(R) = q^m (q^m - 1) p^{n-2}. \quad (11)$$

Доказательство. Обозначим $Q = \mathbb{Z}_p^n$. Имеет место изоморфизм колец

$$R \cong Q[y]/G(y),$$

где $G(y) \in Q[y]$ — многочлен Галуа степени t . Согласно [11, теорема 5] верно равенство $R = Q[\alpha]$, где α — произвольный корень многочлена $G(y)$. Система

$$\mathbf{a} = (1, \alpha, \alpha^2, \dots, \alpha^{t-1})$$

есть базис модуля ${}_Q R$. Напомним, что $\mathbf{x} = (x_1, x_2, \dots, x_m)$ есть строка переменных над кольцом R . Положим $\mathbf{1}_i = (0, \dots, 0, e, 0, \dots, 0) \in R^m$, где e стоит на i -м месте, $i = 1, \dots, m$. Тогда

$$\mathbf{x} = \sum_{i=1}^m x_i \mathbf{1}_i = \sum_{i=1}^m \sum_{j=0}^{t-1} x_{i,j} \alpha^j \mathbf{1}_i,$$

где $x_{i,j}$ — переменная над кольцом Q . Аналогично, m -мерная полиномиальная подстановка F кольца R представляется в виде

$$F(\mathbf{x}) = \sum_{i=1}^m F_i(\mathbf{x}) \mathbf{1}_i = \sum_{i=1}^m \sum_{j=0}^{t-1} F_{i,j}(\mathbf{x}) \alpha^j \mathbf{1}_i,$$

где $F_i: R^m \rightarrow R$ — некоторые полиномы над кольцом R , а $F_{i,j}: R^m \rightarrow Q$ — некоторые функции. Если

$$\vec{\mathbf{x}} = (x_{1,0}, x_{2,0}, \dots, x_{m,0}, x_{1,1}, x_{2,1}, \dots, x_{m,1}, \dots, x_{1,t-1}, x_{2,t-1}, \dots, x_{m,t-1}),$$

то функции F_i и $F_{i,j}$ можно считать функциями от $\vec{\mathbf{x}}$. Докажем включения

$$\forall i \in \{1, \dots, m\}, j \in \{0, \dots, t-1\}: F_{i,j}(\vec{\mathbf{x}}) \in Q[\vec{\mathbf{x}}]. \quad (12)$$

Пусть $\mathbf{b} = (\beta_0, \beta_1, \dots, \beta_{t-1})$ — базис модуля ${}_Q R$, двойственный к $\mathbf{a}$:

$$\forall i, j \in \{0, \dots, t-1\}: \varphi(\beta_i, \alpha^j) = \delta_{i,j} e, \quad (13)$$

где $\delta_{i,j}$ — символ Кронекера. Рассмотрим следующее разложение $F_i(\vec{\mathbf{x}})$ по степеням α :

$$F_i(\vec{\mathbf{x}}) = \sum_{j=0}^{t-1} F_{i,j}(\vec{\mathbf{x}}) \alpha^j.$$

Тогда в силу (13)

$$F_{i,j}(\vec{\mathbf{x}}) = \varphi(\beta_j, F_i(\vec{\mathbf{x}})). \quad (14)$$

С другой стороны, поскольку $F_i(\mathbf{x}) \in R[\mathbf{x}]$, имеем:

$$F_i(\mathbf{x}) = \sum_{(k_1, k_2, \dots, k_m) \in \mathbb{N}_0^m} \varphi_{k_1, k_2, \dots, k_m}^{(i)} x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}, \quad (15)$$

где $\varphi_{k_1, k_2, \dots, k_m}^{(i)} \in R$. Введем обозначение:

$$\mathbf{k} = (k_{1,0}, k_{2,0}, \dots, k_{m,0}, k_{1,1}, k_{2,1}, \dots, k_{m,1}, \dots, k_{1,t-1}, k_{2,t-1}, \dots, k_{m,t-1}).$$

Из равенства (15) и соотношения

$$x_i = \sum_{j=0}^{t-1} x_{i,j} \alpha^j,$$

выполняющегося для всякого $i = 1, \dots, m$, вытекает возможность следующего представления:

$$F_i(\vec{\mathbf{x}}) = \sum_{\mathbf{k} \in \mathbb{N}_0^{mt}} c_{\mathbf{k}}^{(i)} \cdot (\vec{\mathbf{x}})^{\mathbf{k}}, \quad (16)$$

где $c_{\mathbf{k}}^{(i)} \in R$ и

$$(\vec{\mathbf{x}})^{\mathbf{k}} = x_{1,0}^{k_{1,0}} \cdots x_{m,0}^{k_{m,0}} x_{1,1}^{k_{1,1}} \cdots x_{m,1}^{k_{m,1}} \cdots x_{1,t-1}^{k_{1,t-1}} \cdots x_{m,t-1}^{k_{m,t-1}}.$$

Комбинируя (14) и (16), а также учитывая, что φ принимает значения в Q , получаем цепочку равенств

$$\begin{aligned} F_{i,j}(\vec{\mathbf{x}}) &= \varphi(\beta_j, F_i(\vec{\mathbf{x}})) = \\ &= \varphi\left(\beta_j, \sum_{\mathbf{k} \in \mathbb{N}_0^{mt}} c_{\mathbf{k}}^{(i)} \cdot (\vec{\mathbf{x}})^{\mathbf{k}}\right) = \\ &= \sum_{\mathbf{k} \in \mathbb{N}_0^{mt}} \varphi(\beta_j, c_{\mathbf{k}}^{(i)}) \cdot (\vec{\mathbf{x}})^{\mathbf{k}} \in Q[\vec{\mathbf{x}}]. \end{aligned}$$

Таким образом, включение (12) обосновано. Через $\Phi_a(F)$ обозначим mt -мерное полиномиальное преобразование G кольца Q , определенное равенством

$$G(\vec{\mathbf{x}}) = (F_{1,0}(\vec{\mathbf{x}}), \dots, F_{m,0}(\vec{\mathbf{x}}), \dots, F_{1,t-1}(\vec{\mathbf{x}}), \dots, F_{m,t-1}(\vec{\mathbf{x}})).$$

Поскольку разложение всякого элемента кольца R по базису $\mathbf{a}$ однозначно, графы преобразований F и $\Phi_{\mathbf{a}}(F)$ изоморфны. Поэтому максимум $L_m(R)$ длин циклов m -мерных биективных полиномиальных преобразований кольца R не превосходит максимума $L_{mt}(Q)$ длин циклов mt -мерных биективных полиномиальных преобразований кольца Q :

$$L_m(R) \leq L_{mt}(Q). \quad (17)$$

Поскольку кольцо R отлично от кольца вычетов, имеем: $t \geq 2$ и $mt \geq 4$. Согласно следствию 1

$$L_{mt}(Q) \leq \xi(mt, n, p) = q^m (q^m - 1) p^{n-2}.$$

Пользуясь неравенством (17), получаем оценку

$$L_m(R) \leq q^m (q^m - 1) p^{n-2}.$$

Заметим, что если S есть расширение Галуа степени m кольца Галуа R , то, повторив приведенное выше рассуждение для колец S и R (S будет «играть роль» кольца R , а R — кольца Q), получим неравенство

$$L_1(S) \leq L_m(R).$$

Кольцо S есть кольцо Галуа мощности r^n и характеристики p^n , где $r = q^m$. Согласно [3] имеет место цепочка равенств

$$L_1(S) = r(r-1)p^{n-2} = q^m(q^m-1)p^{n-2}.$$

Отсюда

$$q^m(q^m-1)p^{n-2} \leq L_m(R).$$

Равенство (11) доказано. $\square$

Всякую подстановку F вида (2), для которой существует вектор $\mathbf{x} \in R^m$ со свойством

$$\tau(F, n, \mathbf{x}) = q^m (q^m - 1) p^{n-2},$$

будем называть *подстановкой с циклом максимальной длины* (МДЦ-подстановкой). Дальнейшая цель — найти эффективный способ построения МДЦ-подстановок.

3. Подстановки с длинными циклами

В этом разделе построен класс подстановок, среди циклов которых есть циклы длины

$$q^m(q^m-1)p^w,$$

где $0 \leq w \leq n-2$. Все МДЦ-подстановки лежат в этом классе.

Пусть $R = GR(q^n, p^n)$, $n \geq 2$, $\mathbf{x} \in R^m$, F — подстановка вида (2),

$$f = f_1 = F^{[\tau_1]}, \quad J = J(\mathbf{x}) = J_f(\mathbf{x}),$$

σ — мультипликативный порядок матрицы $\bar{J}$, матрица $\Sigma(R, k, \mathbf{x})$ определена равенством

$$\Sigma(R, k, \mathbf{x}) = E + J + J^2 + \dots + J^{k-1},$$

где E — единичная $m \times m$ -матрица. Из (4) вытекает, что

$$f(\mathbf{x} + p^s \mathbf{y}) \equiv f(\mathbf{x}) + p^s \mathbf{y} J \pmod{p^{s+1} R} \quad (18)$$

для всякого $s \geq 0$ и для всякого $\mathbf{y} \in R^m$. Пусть вектор $\mathbf{z} \in R^m$ таков, что

$$f(\mathbf{x}) = \mathbf{x} + p\mathbf{z}. \quad (19)$$

Отсюда, пользуясь (18), индукцией по k получаем, что

$$\forall k \geq 0: \quad f^{[k]}(\mathbf{x}) \equiv \mathbf{x} + p\mathbf{z}\Sigma(R, k, \mathbf{x}) \pmod{p^2 R}.$$

Поскольку $\sigma = \text{ord } \bar{J}$, из последнего соотношения вытекает, что

$$\forall k \geq 0: \quad f^{[\sigma k]}(\mathbf{x}) \equiv \mathbf{x} + p\mathbf{z}k\Sigma(R, \sigma, \mathbf{x}) \pmod{p^2 R}. \quad (20)$$

Отсюда $f^{[\sigma p]}(\mathbf{x}) \equiv \mathbf{x} \pmod{p^2 R}$, и, следовательно,

$$\tau(F, 2, \mathbf{x}) \mid \tau_1 \cdot \sigma \cdot p. \quad (21)$$

Обозначим через $\|r\|$ норму элемента $r \in R$, т.е. такое максимальное $k \in \{0, 1, \dots, n\}$, что $r \in p^k R$. Для всякой матрицы $A = (a_{i,j})_{m \times m} \in R_{m,m}$ положим

$$\|A\| = \min_{i,j} \|a_{i,j}\|.$$

Если матрица $E - J$ обратима, т. е. $\bar{e}$ не является собственным значением матрицы $\bar{J}$, то верна цепочка равенств и неравенств:

$$\|p\mathbf{z}\Sigma(R, \sigma, \mathbf{x})\| = \|p\mathbf{z}\Sigma(R, \sigma, \mathbf{x})(E - J)\| = \|p\mathbf{z}(E - J^\sigma)\| \geq 2.$$

Отсюда и из (20) следует, что при условии $E - J \in R_{m,m}^*$ верно соотношение

$$\tau(F, 2, \mathbf{x}) \mid \tau_1 \cdot \sigma. \quad (22)$$

Следующий результат является простой адаптацией теоремы 1 к кольцам Галуа. В целях полноты изложения приведем его с доказательством.

Теорема 3. Пусть $R = GR(q^n, p^n)$, $n \geq 2$, F — полиномиальная подстановка над R . Тогда

$$\tau(F, n, \mathbf{x}) \mid \tau_1 \cdot p^{n-1} \cdot \text{ord}_p J(\mathbf{x}) \quad (23)$$

при любом $\mathbf{x} \in R^m$. Если дополнительно известно, что $\bar{e}$ не является собственным значением матрицы $\bar{J}(\mathbf{x})$, то

$$\tau(F, n, \mathbf{x}) \mid \tau_1 \cdot p^{n-2} \cdot \text{ord}_p J(\mathbf{x}). \quad (24)$$

Доказательство. Обозначим через φ преобразование $f^{[\sigma]}$. Тогда согласно формуле для производной сложной функции

$$\forall k \geq 0: \quad J_{f^{[\sigma k]}}(\mathbf{x}) = J_{\varphi^{[k]}}(\mathbf{x}) = \prod_{i=0}^{k-1} J_{\varphi}(\varphi^{[i]}(\mathbf{x})) \equiv J_{\varphi}(\mathbf{x})^k \pmod{pR}.$$

В то же время верна цепочка равенств и сравнений по модулю pR :

$$J_{\varphi}(\mathbf{x}) = \prod_{i=0}^{\sigma-1} J(f^{[i]}(\mathbf{x})) \equiv J^{\sigma} \equiv E.$$

Таким образом,

$$\forall k \geq 0: \quad J_{f^{[\sigma k]}}(\mathbf{x}) \equiv E \pmod{pR}. \quad (25)$$

Пусть $\bar{e}$ не является собственным значением матрицы $\bar{J}$. Индукцией по s докажем, что

$$\forall s \geq 0: \quad f^{[\sigma p^s]}(\mathbf{x}) \equiv \mathbf{x} \pmod{p^{s+2}R}. \quad (26)$$

Базу индукции ($s = 0$) обосновывает соотношение (22). Осуществим индуктивный переход от s к $s+1$. Положим $\varphi = f^{[\sigma p^s]}$. По предположению индукции

$$f^{[\sigma p^{s+1}]}(\mathbf{x}) = \varphi^{[p]}(\mathbf{x}) = \varphi^{[p-1]}(\mathbf{x} + p^{s+2}\mathbf{y}), \quad \text{где } \mathbf{y} \in R^m.$$

Тогда, согласно (4) и (25), получаем цепочку сравнений по модулю $p^{s+3}R$:

$$\begin{aligned} f^{[\sigma p^{s+1}]}(\mathbf{x}) &\equiv \varphi^{[p-1]}(\mathbf{x}) + p^{s+2}\mathbf{y} J_{\varphi^{[p-1]}}(\mathbf{x}) \equiv \varphi^{[p-1]}(\mathbf{x}) + p^{s+2}\mathbf{y} \equiv \\ &\equiv \varphi^{[p-2]}(\mathbf{x} + p^{s+2}\mathbf{y}) + p^{s+2}\mathbf{y} \equiv \varphi^{[p-2]}(\mathbf{x}) + 2p^{s+2}\mathbf{y} \equiv \dots \\ &\dots \equiv \mathbf{x} + p^{s+3}\mathbf{y} \equiv \mathbf{x}. \end{aligned}$$

Соотношение (26) доказано. Из (26) следует (24).

Пусть теперь $\bar{e}$ — собственное значение матрицы $\bar{J}$. Индукцией по s докажем, что

$$\forall s \geq 0: \quad f^{[\sigma p^s]}(\mathbf{x}) \equiv \mathbf{x} \pmod{p^{s+1}R}. \quad (27)$$

При $s = 0$ соотношение (27) очевидно. При $s = 1$ оно следует из (21). Пусть $s \geq 1$. Осуществим индуктивный переход от s к $s+1$. Положим $\varphi = f^{[\sigma p^s]}$. По предположению индукции

$$f^{[\sigma p^{s+1}]}(\mathbf{x}) = \varphi^{[p]}(\mathbf{x}) = \varphi^{[p-1]}(\mathbf{x} + p^{s+1}\mathbf{y}), \quad \text{где } \mathbf{y} \in R^m.$$

Тогда, согласно (4) и (25), получаем цепочку сравнений по модулю $p^{s+2}R$:

$$\begin{aligned} f^{[\sigma p^{s+1}]}(\mathbf{x}) &\equiv \varphi^{[p-1]}(\mathbf{x}) + p^{s+1}\mathbf{y} J_{\varphi^{[p-1]}}(\mathbf{x}) \equiv \varphi^{[p-1]}(\mathbf{x}) + p^{s+1}\mathbf{y} \equiv \\ &\equiv \varphi^{[p-2]}(\mathbf{x} + p^{s+1}\mathbf{y}) + p^{s+1}\mathbf{y} \equiv \varphi^{[p-2]}(\mathbf{x}) + 2p^{s+1}\mathbf{y} \equiv \dots \\ &\dots \equiv \mathbf{x} + p^{s+2}\mathbf{y} \equiv \mathbf{x}. \end{aligned}$$

Соотношение (27) доказано. Из (27) следует (23). $\square$

Обозначим через $\bar{\mathbf{x}}$ результат приведения вектора $\mathbf{x} = (x_1, x_2, \dots, x_m)$ по модулю pR :

$$\bar{\mathbf{x}} = (\bar{x}_1, \bar{x}_2, \dots, \bar{x}_m).$$

Покажем, что если m -мерная полиномиальная подстановка F и $\mathbf{x} \in R^m$ таковы, что $\bar{e}$ не является собственным значением матрицы $\bar{J}(\bar{\mathbf{x}})$, то для всякого значения $s \in \{1, 2, \dots, n\}$ существует единственный по модулю p^s вектор $\mathbf{x}^* \in R^m$ со свойствами

$$\bar{\mathbf{x}} = \overline{\mathbf{x}^*} \quad \text{и} \quad \tau(F, s, \mathbf{x}^*) = \tau(F, 1, \mathbf{x}^*). \quad (28)$$

Вектор $\mathbf{x}^*$ будем строить по вектору $\mathbf{x}$ и подстановке F индукцией по $s \geq 1$. При $s = 1$ положим $\mathbf{x}^* = \mathbf{x}$. Пусть $k \geq 1$, и для $s = k$ существует единственный по модулю p^s вектор $\mathbf{x}^*$ со свойствами (28). Положим $s = k + 1$.

Пусть $\Gamma(R) = \{x \in R: x^q = x\}$. Известно (см., например, [11]), что всякий элемент $r \in R$ единственным образом представляется в виде разложения Тейхмюллера:

$$r = r_0 + r_1 p + r_2 p^2 + \dots + r_{n-1} p^{n-1},$$

где

$$r_s = \gamma_s(r) \in \Gamma(R), \quad s = 0, 1, \dots, n-1.$$

Пусть $\mathbf{y} \in R^m$ — вектор вида

$$\mathbf{y}_0 + \mathbf{y}_1 p + \dots + \mathbf{y}_{k-1} p^{k-1}, \quad \mathbf{y}_i \in \Gamma(R)^m, \quad i = 0, 1, \dots, k-1,$$

который обладает свойствами

$$\bar{\mathbf{x}} = \bar{\mathbf{y}} \quad \text{и} \quad \tau(F, k, \mathbf{y}) = \tau(F, 1, \mathbf{y}).$$

Рассмотрим уравнение относительно $\mathbf{z} \in \Gamma(R)^m$:

$$\tau(F, k+1, \mathbf{y} + p^k \mathbf{z}) = \tau(F, 1, \mathbf{y}). \quad (29)$$

Чтобы осуществить индуктивный переход, достаточно показать, что уравнение (29) имеет единственное решение.

Поскольку $\bar{\mathbf{x}} = \bar{\mathbf{y}}$, уравнение (29) эквивалентно уравнению

$$f(\mathbf{y} + p^k \mathbf{z}) \equiv \mathbf{y} + p^k \mathbf{z} \pmod{p^{k+1} R},$$

которое переписывается в виде

$$f(\mathbf{y}) + p^k \mathbf{z} J(\mathbf{x}) \equiv \mathbf{y} + p^k \mathbf{z} \pmod{p^{k+1} R}.$$

Последнее уравнение, очевидно, эквивалентно уравнению

$$\mathbf{z}(J(\mathbf{x}) - E) \equiv \gamma_k(\mathbf{y} - f(\mathbf{y})) \pmod{pR}. \quad (30)$$

Так как $\bar{e}$ не является собственным значением матрицы $\overline{J(\mathbf{x})}$, матрица $J(\mathbf{x}) - E$ обратима. Поэтому уравнение (30) относительно $\mathbf{z} \in \Gamma(R)^m$ имеет единственное решение. Положив $s = n$ в (28), получаем следующее утверждение.

Утверждение 1. Если подстановка F и вектор $\mathbf{x} \in R^m$ таковы, что $\bar{e}$ не является собственным значением матрицы $\overline{J(\mathbf{x})}$, то существует единственный вектор $\mathbf{x}^* \in R^m$, удовлетворяющий условиям

$$\overline{\mathbf{x}} = \overline{\mathbf{x}^*} \quad \text{и} \quad \tau(F, n, \mathbf{x}^*) = \tau_1.$$

В частности, если $\overline{F}$ — полноцикловая подстановка, то среди циклов подстановки F имеется единственный цикл длины q^m .

Назовем подстановку F подстановкой с длинными циклами (ДЦ-подстановкой), если существует такой вектор $\mathbf{x} \in R^m$, что

$$\tau(F, 2, \mathbf{x}) = q^m(q^m - 1). \quad (31)$$

Цикл, которому принадлежит вектор $\mathbf{x}$ со свойством (31), будем называть длинным.

Из теоремы 3 следует, что для всякого вектора $\mathbf{x} \in R^m$, принадлежащего длинному циклу подстановки F , верно равенство

$$\tau(F, n, \mathbf{x}) = q^m(q^m - 1)p^w,$$

где $0 \leq w \leq n - 2$. Напомним (см. раздел 2), что $\chi(x)$ есть характеристический многочлен матрицы $J(\mathbf{x})$. Центральным результатом этого раздела является следующая теорема.

Теорема 4. Пусть $R = GR(q^n, p^n)$ — кольцо Галуа, отличное от примарного кольца вычетов и от конечного поля. Для данной подстановки F и данного вектора $\mathbf{x} \in R^m$ равенство (31) эквивалентно одновременному выполнению следующих условий:

1. преобразование $\overline{F}$ является полноцикловым,
2. $\text{ord}_p J(\mathbf{x}) = q^m - 1$,
3. $\gamma_1(\mathbf{x}) \neq \gamma_1(\mathbf{x}^*)$.

Доказательство. Пусть выполнено (31). Если $\bar{e}$ не является собственным значением матрицы $\overline{J(x)}$, то согласно (24) справедливо неравенство

$$q^m \cdot (q^m - 1) \leq \tau_1 \cdot \text{ord}_p J(\mathbf{x}).$$

Поскольку $\tau_1 \leq q^m$ и $\text{ord}_p J(\mathbf{x}) \leq q^m - 1$, имеем: $\tau_1 = q^m$, т. е. выполнен п. 1, и $\text{ord}_p J(\mathbf{x}) = q^m - 1$, т. е. выполнен п. 2. Если п. 3 при этом не выполнен, то $\mathbf{x} \equiv \mathbf{x}^* \pmod{p^2 R}$, и $\tau(F, 2, \mathbf{x}) = \tau_1 = q^m$. Противоречие с (31).

Пусть $\bar{e}$ — собственное значение матрицы $\overline{J(\mathbf{x})}$. Существуют такие $k \in \{1, 2, \dots, m\}$ и унитарный многочлен $g(x) \in \bar{R}[x]$, что

$$\bar{\chi}(x) = (x - \bar{e})^k \cdot g(x) \quad \text{и} \quad g(\bar{e}) \neq 0.$$

Матрица $\overline{J(\mathbf{x})}$ подобна распавшейся матрице:

$$\overline{J(\mathbf{x})} \approx \begin{pmatrix} A & 0 \\ 0 & B \end{pmatrix},$$

где $\chi_A(x) = (x - \bar{e})^k$, $\chi_B(x) = g(x)$. Если $m_A(x) = (x - \bar{e})^s$ — минимальный многочлен матрицы A , то $\text{ord } A = p^c$, где

$$c = \lceil \log_p s \rceil \leq \lceil \log_p k \rceil.$$

Очевидно,

$$\text{ord } \overline{J(\mathbf{x})} \mid p^c \cdot \text{ord } B \leq p^c (q^{m-k} - 1) = q^{m-k} p^c - p^c.$$

Возможны следующие случаи:

1. $k = 1$. Тогда $A = (\bar{e})$, и $\text{ord } \overline{J(\mathbf{x})} = \text{ord } B \leq q^{m-1} - 1$.
2. $k \geq 2$. В этой ситуации $c \leq \lceil \log_p k \rceil < k$, и $\text{ord } \overline{J(\mathbf{x})} \leq q^{m-1} - 1$.

В обоих случаях $\text{ord } \overline{J(\mathbf{x})} \leq q^{m-1} - 1$. Поэтому согласно (23)

$$q^m (q^m - 1) \leq \tau_1 \cdot p \cdot \text{ord } {}_p J(\mathbf{x}) \leq q^m \cdot p \cdot (q^{m-1} - 1) < q^m (q^m - 1).$$

Противоречие. Итак, $\bar{e}$ не является собственным значением матрицы $\overline{J(\mathbf{x})}$.

Обратно, пусть выполнены пп. 1, 2 и 3. Тогда $\tau_1 = q^m$, $\text{ord } {}_p J(\mathbf{x}) = q^m - 1$, и

$$f(\mathbf{x}) \equiv \mathbf{x} + p\mathbf{z} \pmod{p^2 R}, \quad (32)$$

где $\bar{\mathbf{z}} \neq 0$. Пусть число $k \in \mathbb{Z}$ таково, что

$$\tau(F, 2, \mathbf{x}) = \tau_1 \cdot k = q^m \cdot k.$$

Поскольку $\bar{e}$ не является собственным значением матрицы $\overline{J(\mathbf{x})}$, согласно (24) имеем: $k \mid q^m - 1$.

Ввиду (32)

$$f^{[k]}(\mathbf{x}) \equiv \mathbf{x} + p\mathbf{z}\Sigma(R, k, \mathbf{x}) \pmod{p^2R}.$$

Матрица $E - J^k$ обратима при $k < q^m - 1$ и равна 0 при $k = q^m - 1$. Поэтому величина

$$\|p\mathbf{z}\Sigma(R, k, \mathbf{x})\| = \|p\mathbf{z}(E + J + \dots + J^{k-1})\| = \|p\mathbf{z}(E - J^k)\|$$

больше или равна 2 тогда и только тогда, когда $k = q^m - 1$. Поскольку

$$f^{[k]}(\mathbf{x}) \equiv \mathbf{x} \pmod{p^2R},$$

получаем, что $k = q^m - 1$. Равенство (31) доказано. $\square$

Следующее утверждение описывает ДЦ-подстановки.

Следствие 2. Пусть в условиях теоремы 4 подстановка $\bar{F}$ является полноциклозой. Тогда следующие утверждения эквивалентны:

- 1) F есть ДЦ-подстановка,
- 2) $\text{ord}_p J(\mathbf{x}) = q^m - 1$ для всякого $\mathbf{x} \in R^m$,
- 3) $\text{ord}_p J(\mathbf{x}) = q^m - 1$ для некоторого $\mathbf{x} \in R^m$.

Доказательство. 1) $\Rightarrow$ 2). Пусть $\tilde{R} = R/p^2R$, $\tilde{F}$ есть образ F под действием естественного эпиморфизма $R \rightarrow \tilde{R}$. Согласно утверждению 1 граф $G_{\tilde{F}}$ преобразования $\tilde{F}$ кольца $\tilde{R}$ состоит из одного цикла длины q^m и одного длинного цикла длины $\tau = q^m(q^m - 1)$. Рассмотрим длинный цикл подстановки $\tilde{F}$:

$$w_0, w_1, \dots, w_{\tau-1}, \quad \tilde{F}(w_i) = w_{i+1} \pmod{\tau}, \quad i = 0, 1, \dots, \tau - 1.$$

Согласно п. 1 теоремы 4 в результате приведения по модулю радикала длинный цикл приобретает вид

$$\bar{w}_0, \bar{w}_1, \dots, \bar{w}_{q^m-1}, \bar{w}_0, \bar{w}_1, \dots, \bar{w}_{q^m-1}, \dots, \bar{w}_0, \bar{w}_1, \dots, \bar{w}_{q^m-1},$$

причем $\{\bar{w}_0, \bar{w}_1, \dots, \bar{w}_{q^m-1}\} = \bar{R}^m$. По п. 2 теоремы 4 найдется такой вектор $\mathbf{x} \in R^m$, что $\text{ord}_p J(\mathbf{x}) = q^m - 1$. Пусть значение $i \in \{0, 1, \dots, q^m - 1\}$ таково, что $\bar{\mathbf{x}} = \bar{w}_i$, а $\mathbf{y} \in R^m$ — произвольный вектор. Рассмотрим такое $j \in \{0, 1, \dots, q^m - 1\}$, что $\bar{\mathbf{y}} = \bar{w}_j$. Тогда

$$\bar{F}^{[j-i]}(\bar{\mathbf{x}}) = \bar{\mathbf{y}}.$$

Поскольку вектор $\mathbf{x}$ принадлежит длинному циклу подстановки F , то и вектор $\mathbf{a} = F^{[j-i]}(\mathbf{x})$ принадлежит длинному циклу подстановки F . По п. 2 теоремы 4 имеем:

$$\text{ord}_p J(\mathbf{a}) = q^m - 1. \quad (33)$$

В то же время

$$\text{ord}_p J(\mathbf{a}) = \text{ord}_p J(F^{[j-i]}(\mathbf{x})) = \text{ord}_p J(\mathbf{y}).$$

Отсюда и из (33) получаем п. 2).

Импликация «2) $\Rightarrow$ 3)» очевидна. Докажем импликацию «3) $\Rightarrow$ 1)». Выберем $\mathbf{x} \in R^m$ со свойством $\text{ord}_p J(\mathbf{x}) = q^m - 1$. Если $\gamma_1(\mathbf{x}) \neq \gamma_1(\mathbf{x}^*)$, то по теореме 4 выполняется равенство (31), и F — ДЦ-подстановка. Если же $\gamma_1(\mathbf{x}) = \gamma_1(\mathbf{x}^*)$, то рассмотрим вектор $\mathbf{a} \in \Gamma(R)^m \setminus \{0\}$ и вектор $\mathbf{y} = \mathbf{x} + p\mathbf{a}$. Поскольку $\bar{\mathbf{x}} = \bar{\mathbf{y}}$, имеем цепочку сравнений по модулю p^2R :

$$\mathbf{y}^* \equiv \mathbf{x}^* \equiv \mathbf{x}.$$

Поскольку $\mathbf{x} \not\equiv \mathbf{y} \pmod{p^2R}$, имеем: $\gamma_1(\mathbf{y}) \neq \gamma_1(\mathbf{y}^*)$. При этом

$$\text{ord}_p J(\mathbf{y}) = \text{ord}_p J(\mathbf{x}) = q^m - 1.$$

Тогда по теореме 4 выполняется равенство (31), и F — ДЦ-подстановка. $\square$

Следствие 2 является многомерным аналогом утверждения 7 из работы [5].

Покажем, как можно построить m -мерную подстановку F и вектор $\mathbf{x} \in R^m$ так, чтобы выполнялось равенство

$$\tau(F, 2, \mathbf{x}) = q^m(q^m - 1). \quad (34)$$

Пусть подстановка G такова, что $\bar{G}$ — полноцикловое преобразование. Произвольно выберем такие векторы $\mathbf{x} \in R^m$ и $w_0, w_1, \dots, w_{q^m-1} \in R^m$, что

$$\bar{w}_0 = \bar{\mathbf{x}} \quad \text{и} \quad \bar{G}(\bar{w}_i) = \bar{w}_{i+1} \pmod{q^m}, \quad i = 0, 1, \dots, q^m - 1.$$

Выберем и зафиксируем такой набор $m \times m$ -матриц $C_0, C_1, \dots, C_{q^m-1}$, обратимых над кольцом R , что

$$\text{ord}_p C = q^m - 1, \quad \text{где} \quad C = \prod_{i=0}^{q^m-1} C_i.$$

Пусть $\mathbf{z} = (z_1, z_2, \dots, z_m)$ — набор переменных над кольцом R . Существует такая матрица $\Phi(\mathbf{z}) \in R[\mathbf{z}]_{m,m}$, что

$$\forall i \in \{0, 1, \dots, q^m - 1\}: \quad \overline{\Phi}(\overline{w}_i) = \overline{C}_i \ominus \overline{J_G(w_i)}, \quad (35)$$

где « $\ominus$ » — вычитание в поле $\overline{R}$. Обозначим через $\mathbf{z}^q$ вектор $(z_1^q, z_2^q, \dots, z_m^q)$. Подстановку F будем строить так:

$$F(\mathbf{z}) = G(\mathbf{z}) + (\mathbf{z} - \mathbf{z}^q) \cdot \Phi(\mathbf{z}). \quad (36)$$

Поскольку для всякого вектора $\mathbf{x} \in R^m$ верно равенство $\overline{F}(\overline{\mathbf{x}}) = \overline{G}(\overline{\mathbf{x}})$, подстановка $\overline{F}$ является полноциклоной. Покажем, что F удовлетворяет п. 3) следствия 2.

Равенство (36) можно переписать в следующем виде:

$$\sum_{j=1}^m F_j(\mathbf{z}) \mathbf{1}_j = \sum_{j=1}^m G_j(\mathbf{z}) \mathbf{1}_j + \sum_{j=1}^m \sum_{i=1}^m (z_i - z_i^q) \cdot \varphi_{i,j}(\mathbf{z}) \cdot \mathbf{1}_j,$$

где $\varphi_{i,j}(\mathbf{z})$ — элемент, стоящий на пересечении i -й строки и j -го столбца матрицы $\Phi(\mathbf{z})$. Пусть $s \in \{1, 2, \dots, m\}$. Продифференцируем обе части по z_s :

$$\begin{aligned} \sum_{j=1}^m \frac{\partial F_j}{\partial z_s}(\mathbf{z}) \mathbf{1}_j &= \sum_{j=1}^m \frac{\partial G_j}{\partial z_s}(\mathbf{z}) \mathbf{1}_j + \sum_{j=1}^m \sum_{i=1}^m (e - qz_s^{q-1}) \cdot \delta_{i,s} \cdot \varphi_{i,j}(\mathbf{z}) \cdot \mathbf{1}_j + \\ &+ \sum_{j=1}^m \sum_{i=1}^m (z_i - z_i^q) \cdot \frac{\partial \varphi_{i,j}}{\partial z_s}(\mathbf{z}) \cdot \mathbf{1}_j, \end{aligned}$$

где $\delta_{i,s}$ — символ Кронекера. Отсюда

$$\begin{aligned} \sum_{j=1}^m \frac{\partial F_j}{\partial z_s}(\mathbf{z}) \mathbf{1}_j &= \sum_{j=1}^m \frac{\partial G_j}{\partial z_s}(\mathbf{z}) \mathbf{1}_j + \sum_{j=1}^m (e - qz_s^{q-1}) \cdot \varphi_{s,j}(\mathbf{z}) \cdot \mathbf{1}_j + \\ &+ \sum_{j=1}^m \sum_{i=1}^m (z_i - z_i^q) \cdot \frac{\partial \varphi_{i,j}}{\partial z_s}(\mathbf{z}) \cdot \mathbf{1}_j. \end{aligned}$$

Пусть $i \in \{0, 1, \dots, q^m - 1\}$. Из последнего равенства и из (35) получаем цепочку сравнений по модулю pR :

$$J_F(w_i) \equiv J_G(w_i) + \Phi(w_i) \equiv C_i.$$

Согласно (5) справедлива цепочка равенств и сравнений по модулю pR :

$$J_f(\mathbf{x}) \equiv \prod_{i=0}^{q^m-1} J_F(G^{[i]}(w_0)) \equiv \prod_{i=0}^{q^m-1} J_F(w_i) \equiv \prod_{i=0}^{q^m-1} C_i = C.$$

Отсюда $\text{ord}_p J_f(\mathbf{x}) = q^m - 1$, и по п. 3) следствия 2 подстановка F является ДЦ-подстановкой.

Если $\mathbf{x} \not\equiv \mathbf{x}^* \pmod{p^2 R}$, то по теореме 4 выполняется равенство (34). В противном случае равенство (34) выполняется для подстановки F и вектора $\mathbf{x} + p\mathbf{y}$, где $\mathbf{y} \in \Gamma(R)^m \setminus \{0\}$:

$$\tau(F, 2, \mathbf{x} + p\mathbf{y}) = q^m(q^m - 1).$$

Найдем число векторов, принадлежащих длинным циклам ДЦ-подстановки. Если F — ДЦ-подстановка, то по теореме 4 и следствию 2 для любого вектора $\mathbf{x} \in R^m$ реализуется одна из двух ситуаций:

1. $\mathbf{x} \equiv \mathbf{x}^* \pmod{p^2 R}$, и тогда $\tau(F, 2, \mathbf{x}) = q^m$;
2. $\mathbf{x} \not\equiv \mathbf{x}^* \pmod{p^2 R}$, и тогда $\tau(F, 2, \mathbf{x}) = q^m(q^m - 1)$.

Из этого факта вытекает следующее утверждение.

Следствие 3. Пусть в условиях теоремы 4 подстановка F является ДЦ-подстановкой. Тогда в графе G_F преобразования F ровно $q^m(q^m - 1)q^{m(n-2)}$ вершин принадлежат длинным циклам.

Доказательство. Вершину $\mathbf{x} \in R^m$, принадлежащую длинному циклу подстановки F , будем строить при помощи разложения Тейхмюллера:

$$\mathbf{x} = \mathbf{x}_0 + p\mathbf{x}_1 + \dots + p^{n-1}\mathbf{x}_{n-1},$$

где $\mathbf{x}_s \in \Gamma(R)^m$, $s = 0, 1, \dots, n-1$. Вектор $\mathbf{x}_0 \in \Gamma(R)^m$ выбираем произвольно, q^m способами. Для вектора $\mathbf{x}_0$ существует такой единственный вектор $\mathbf{y} \in \Gamma(R)^m$, что

$$\mathbf{x}^* \equiv \mathbf{x}_0 + p\mathbf{y} \pmod{p^2 R}.$$

Ситуация 2 реализуется тогда и только тогда, когда $\mathbf{x}_1 \neq \mathbf{y}$. Вектор

$$\mathbf{x}_1 \in \Gamma(R)^m \setminus \{\mathbf{y}\}$$

выбирается $q^m - 1$ способами. Набор векторов $\mathbf{x}_2, \dots, \mathbf{x}_{n-1} \in \Gamma(R)^m$ выбирается произвольно, $q^{m(n-2)}$ способами. $\square$

Далее будет показано, как следует видоизменить подстановку (36), чтобы она обладала циклом максимальной длины $q^m(q^m - 1)p^{n-2}$.

4. Профиль длинного цикла

Пусть F — ДЦ-подстановка, $f_s = F^{[\tau_s]}$, $s = 1, 2, \dots, n$, $\mathbf{x} \in R^m$. Очевидно, $J_{f_n}(\mathbf{x}) = E$. Поэтому существует такое минимальное $s \in \{1, 2, \dots, n\}$, что

$$J_{f_s}(\mathbf{x}) \equiv E \pmod{pR}.$$

Обозначим это минимальное s через s_0 . Понятно, что $s_0 = s_0(F, \mathbf{x})$. Если $\mathbf{x}$ принадлежит длинному циклу подстановки F , то $\tau_2 = \tau_1 \cdot \sigma$, и $s_0 = 2$ согласно (25). Всюду далее будем считать, что F — ДЦ-подстановка, а вектор $\mathbf{x}$ принадлежит ее длинному циклу.

Положим $d_s(\mathbf{x}) = \tau_{s+1}(\mathbf{x})/\tau_s(\mathbf{x})$, $s = 1, 2, \dots, n-1$. В этом разделе будет изучен *профиль* длинного цикла (3), т. е. последовательность

$$d_1(\mathbf{x}), d_2(\mathbf{x}), \dots, d_{n-1}(\mathbf{x}). \quad (37)$$

Для всякого $s \geq s_0 = 2$ положим $A_s(\mathbf{x}) = J_{f_s}(\mathbf{x})$. Справедливо следующее утверждение.

Утверждение 2. Если F — ДЦ-подстановка, вектор $\mathbf{x} \in R^m$ принадлежит ее длинному циклу, $s \geq s_0 = 2$, $j \geq 0$ и $f_s(\mathbf{x}) = \mathbf{x} + p^s \mathbf{y}$, то

$$f_s^{[j]}(\mathbf{x}) \equiv \mathbf{x} + p^s \mathbf{y} \sum_{k=0}^{j-1} A_s(\mathbf{x})^k \pmod{p^{2s}R}.$$

Доказательство. Индукция по $j \geq 0$. При $j = 0$ и $j = 1$ доказываемое равенство очевидно. Осуществим индуктивный переход от j к $j + 1$.

По формуле производной сложной функции имеем цепочку равенств и сравнений по модулю $p^s R$:

$$J_{f_s^{[j]}}(\mathbf{x}) = \prod_{i=0}^{j-1} J_{f_s}(f_s^{[i]}(\mathbf{x})) \equiv J_{f_s}(\mathbf{x})^j = A_s(\mathbf{x})^j. \quad (38)$$

Согласно (4) и (38) имеет место цепочка равенств и сравнений по модулю $p^{2s}R$:

$$\begin{aligned} f_s^{[j+1]}(\mathbf{x}) &= f_s^{[j]}(f_s(\mathbf{x})) = f_s^{[j]}(\mathbf{x} + p^s \mathbf{y}) \equiv f_s^{[j]}(\mathbf{x}) + p^s \mathbf{y} J_{f_s^{[j]}}(\mathbf{x}) \equiv \\ &\equiv \mathbf{x} + p^s \mathbf{y} \sum_{k=0}^{j-1} A_s(\mathbf{x})^k + p^s \mathbf{y} A_s(\mathbf{x})^j = \mathbf{x} + p^s \mathbf{y} \sum_{k=0}^j A_s(\mathbf{x})^k. \quad \square \end{aligned}$$

Всюду далее $p > 2$. Уточним в этой ситуации формулу (4).

Пусть $w(\mathbf{x}) \in R[\mathbf{x}]$ — моном:

$$w(\mathbf{x}) = a x_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}.$$

Обозначим через $w'(\mathbf{x})$ столбец

$$\left(\frac{\partial w}{\partial x_1}(\mathbf{x}), \dots, \frac{\partial w}{\partial x_m}(\mathbf{x}) \right)^T.$$

Согласно (4) имеем следующую цепочку сравнений по модулю $p^{3s}R$:

$$\begin{aligned} w(\mathbf{x} + p^s \mathbf{y}) &\equiv w(\mathbf{x}) + p^s \mathbf{y} w'(\mathbf{x}) + \\ &+ a \sum_{i=1}^m \binom{\alpha_i}{2} x_1^{\alpha_1} \dots x_{i-1}^{\alpha_{i-1}} (x_i^{\alpha_i-2} p^{2s} y_i^2) x_{i+1}^{\alpha_{i+1}} \dots x_m^{\alpha_m} + \\ &+ a \sum_{1 \leq i < j \leq m} \alpha_i \alpha_j \cdot x_1^{\alpha_1} \dots x_{i-1}^{\alpha_{i-1}} (x_i^{\alpha_i-1} p^s y_i) x_{i+1}^{\alpha_{i+1}} \dots \\ &\dots x_{j-1}^{\alpha_{j-1}} (x_j^{\alpha_j-1} p^s y_j) x_{j+1}^{\alpha_{j+1}} \dots x_m^{\alpha_m} = \\ &= w(\mathbf{x}) + p^s \mathbf{y} w'(\mathbf{x}) + \\ &+ \frac{1}{2} \sum_{i=1}^m \frac{\partial^2 w}{\partial x_i^2}(\mathbf{x}) \cdot p^{2s} y_i^2 + \frac{1}{2} \sum_{1 \leq i \neq j \leq m} \frac{\partial^2 w}{\partial x_i \partial x_j}(\mathbf{x}) \cdot p^{2s} y_i y_j = \\ &= w(\mathbf{x}) + p^s \mathbf{y} \cdot w'(\mathbf{x}) + \frac{p^{2s}}{2} \cdot \mathbf{y} w''(\mathbf{x}) \mathbf{y}^T, \end{aligned}$$

где « T » — символ операции транспонирования, а $w''(\mathbf{x})$ — матрица над R размерами $m \times m$, на пересечении i -й строки и j -го столбца которой стоит вторая производная

$$\frac{\partial^2 w}{\partial x_i \partial x_j}(\mathbf{x}).$$

Распространим полученную формулу по линейности:

$$\begin{aligned} \forall i \in \{1, 2, \dots, m\}: F_i(\mathbf{x} + p^s \mathbf{y}) &\equiv F_i(\mathbf{x}) + \\ &+ p^s \mathbf{y} F'_i(\mathbf{x}) + \frac{p^{2s}}{2} \mathbf{y} F''_i(\mathbf{x}) \mathbf{y}^T \pmod{p^{3s}R}. \end{aligned}$$

Отсюда находим, что для всякого $s \geq 1$ справедливо соотношение

$$F(\mathbf{x} + p^s \mathbf{y}) \equiv F(\mathbf{x}) + p^s \mathbf{y} J_F(\mathbf{x}) + \frac{p^{2s}}{2} \cdot d^2 F(\mathbf{x}, \mathbf{y}) \pmod{p^{3s} R}, \quad (39)$$

где

$$d^2 F(\mathbf{x}, \mathbf{y}) = (\mathbf{y} F_1''(\mathbf{x}) \mathbf{y}^T, \mathbf{y} F_2''(\mathbf{x}) \mathbf{y}^T, \dots, \mathbf{y} F_m''(\mathbf{x}) \mathbf{y}^T). \quad (40)$$

Формула (39) есть многомерная формула Тейлора для $p > 2$.

Следующее утверждение обобщает утверждение 2 в случае $p > 2$.

Утверждение 3. Если $p > 2$, F — ДЦ-подстановка, $\mathbf{x}$ принадлежит длинному циклу F , $j \geq 0$, $s \geq s_0 = 2$, $f_s(\mathbf{x}) = \mathbf{x} + p^s \mathbf{y}$, то

$$f_s^{[j]}(\mathbf{x}) \equiv \mathbf{x} + p^s \mathbf{y} \sum_{k=0}^{j-1} A_s(\mathbf{x})^k + \frac{p^{2s}}{2} \cdot \sum_{k=0}^{j-1} k^2 \cdot d^2 f_s(\mathbf{x}, \mathbf{y}) \pmod{p^{2s+1} R}. \quad (41)$$

Доказательство. Сначала покажем, что для любого $s \geq 2$ верно сравнение

$$J_{f_s}(\mathbf{x}) \equiv E \pmod{pR}. \quad (42)$$

При $s = s_0 = 2$ оно следует из определения величины s_0 . Осуществим индуктивный переход от s к $s+1$. Для краткости обозначим величину $d_s(\mathbf{x})$ через d_s . По формуле производной сложной функции имеем цепочку равенств и сравнений по модулю pR :

$$J_{f_{s+1}}(\mathbf{x}) = J_{f_s^{[d_s]}}(\mathbf{x}) = \prod_{j=0}^{d_s-1} J_{f_s}(f_s^{[j]}(\mathbf{x})) \equiv J_{f_s}(\mathbf{x})^{d_s} \equiv E.$$

Соотношение (42) доказано.

Докажем (41) индукцией по $j \geq 0$. При $j = 0$ и $j = 1$ доказываемое соотношение очевидно. Осуществим индуктивный переход от j к $j+1$. Положим

$$\mathbf{z} = \mathbf{y} \sum_{k=0}^{j-1} A_s(\mathbf{x})^k + \frac{p^s}{2} \sum_{k=0}^{j-1} k^2 \cdot d^2 f_s(\mathbf{x}, \mathbf{y}).$$

Тогда по предположению индукции $f_s^{[j]}(\mathbf{x}) = \mathbf{x} + p^s \mathbf{z}$.

В силу (39) и (42) имеем цепочку равенств и сравнений по модулю $p^{2s+1}R$:

$$\begin{aligned}
 f_s^{[j+1]}(\mathbf{x}) &= f_s(f_s^{[j]}(\mathbf{x})) \equiv f_s(\mathbf{x} + p^s \mathbf{z}) \equiv \\
 &\equiv f_s(\mathbf{x}) + p^s \mathbf{z} A_s(\mathbf{x}) + \frac{1}{2} p^{2s} d^2 f_s(\mathbf{x}, \mathbf{z}) \equiv \\
 &\equiv \mathbf{x} + p^s \mathbf{y} + p^s \mathbf{y} \sum_{k=1}^j A_s(\mathbf{x})^k + \\
 &\quad + \frac{p^{2s}}{2} \sum_{k=0}^{j-1} k^2 \cdot d^2 f_s(\mathbf{x}, \mathbf{y}) + \frac{p^{2s}}{2} d^2 f_s(\mathbf{x}, j\mathbf{y}) \equiv \\
 &\equiv \mathbf{x} + p^s \mathbf{y} \sum_{k=0}^j A_s(\mathbf{x})^k + \frac{p^{2s}}{2} \sum_{k=0}^j k^2 \cdot d^2 f_s(\mathbf{x}, \mathbf{y}). \quad \square
 \end{aligned}$$

Введем обозначение

$$\mu = \mu(F, \mathbf{x}) = \|f_2(\mathbf{x}) - \mathbf{x}\| - 2.$$

Очевидно, величина μ удовлетворяет следующему равенству:

$$\mu = \begin{cases} 0, & \text{если } d_2 > 1, \\ \max\{s \mid d_2 = d_3 = \dots = d_{s+1} = 1\}, & \text{если } d_2 = 1. \end{cases}$$

Центральным результатом этого раздела является следующая теорема.

Теорема 5. Если $p > 2$, F — ДЦ-подстановка, $\mathbf{x}$ принадлежит длинному циклу F , $2 \leq s \leq n-2$ и $d_s > 1$, то:

1. $d_s = p$,
2. $d_{s+1} > 1$.

В частности, если $p > 2$ и выполняется (31), то профиль (37) имеет вид

$$(q^m - 1), 1, 1, \dots, 1, p, p, \dots, p,$$

где количество «1» равно μ , и

$$\tau(F, n, \mathbf{x}) = q^m (q^m - 1) p^{n-\mu-2}.$$

Доказательство. Второе утверждение теоремы следует из пп. 1 и 2. Докажем пп. 1 и 2.

1. Так как $d_s > 1$, то существует $\mathbf{y} \in R^m$ со свойствами

$$\bar{\mathbf{y}} \neq 0 \quad \text{и} \quad f_s(\mathbf{x}) = \mathbf{x} + p^s \mathbf{y}.$$

Согласно (42) и утверждению 2

$$\forall j \geq 0: \quad f_s^{[j]}(\mathbf{x}) \equiv \mathbf{x} + p^s j \mathbf{y} \pmod{p^{s+1}R}.$$

Отсюда следует, что $d_s = p$.

2. Пусть $f_s(\mathbf{x}) = \mathbf{x} + p^s \mathbf{y}$, $\bar{\mathbf{y}} \neq 0$. Очевидно следующее сравнение по модулю p :

$$\sum_{k=0}^{p-1} k^2 = \frac{(p-1)p(2p-1)}{6} \equiv \begin{cases} 0, & \text{если } p > 3; \\ 2, & \text{если } p = 3. \end{cases}$$

Кроме того, согласно (42) для всякого $s \geq 2$ существует такая матрица $B_s(\mathbf{x})$, что $A_s(\mathbf{x}) = E + p B_s(\mathbf{x})$. Тогда верна следующая цепочка равенств и сравнений по модулю $p^2 R$:

$$\begin{aligned} \sum_{k=0}^{p-1} A_s(\mathbf{x})^k &= \sum_{k=0}^{p-1} (E + p B_s(\mathbf{x}))^k \equiv \sum_{k=0}^{p-1} (E + k p B_s(\mathbf{x})) \equiv \\ &\equiv p E + \binom{p}{2} p B_s(\mathbf{x}). \end{aligned}$$

Поскольку $p > 2$,

$$\sum_{k=0}^{p-1} A_s(\mathbf{x})^k \equiv p E \pmod{p^2 R}. \quad (43)$$

Далее рассмотрим два случая.

2.1. $p = 3$. Поскольку $s + 2 \leq 2s$, из утверждения 3 и (43) следует цепочка сравнений по модулю $p^{s+2} R$:

$$\begin{aligned} f_s^{[p]}(\mathbf{x}) &\equiv \mathbf{x} + p^s \mathbf{y} \sum_{k=0}^{p-1} A_s(\mathbf{x})^k + p^{2s} d^2 f_s(\mathbf{x}, \mathbf{y}) \equiv \\ &\equiv \mathbf{x} + p^s \mathbf{y} \sum_{k=0}^{p-1} A_s(\mathbf{x})^k \equiv \mathbf{x} + p^{s+1} \mathbf{y}. \end{aligned}$$

Так как $\bar{\mathbf{y}} \neq 0$, то $\tau_{s+2} > \tau_{s+1}$, т. е. $d_{s+1} > 1$.

2.2. $p > 3$. По утверждению 3 верно соотношение

$$f_s^{[p]}(\mathbf{x}) \equiv \mathbf{x} + p^s \mathbf{y} \sum_{k=0}^{p-1} A_s(\mathbf{x})^k \pmod{p^{2s+1}R}.$$

Поскольку $s+2 < 2s+1$, по формуле (43) имеем:

$$f_s^{[p]}(\mathbf{x}) \equiv \mathbf{x} + p^{s+1} \mathbf{y} \pmod{p^{s+2}R}.$$

Отсюда $d_{s+1} > 1$. □

В условиях теоремы 5 равенство

$$\tau(F, n, \mathbf{x}) = q^m (q^m - 1) p^{n-2} \quad (44)$$

выполняется тогда и только тогда, когда $\mu = 0$. В следующем разделе будет показано, как построить пару $(F, \mathbf{x})$, удовлетворяющую условиям теоремы 5 и равенству $\mu = 0$.

5. Построение МДЦ-подстановок

В этом разделе $R = GR(q^n, p^n)$ — собственное кольцо Галуа, $p > 2$. Пусть m -мерная полиномиальная подстановка F и вектор $\mathbf{x}$ обладают свойством (31):

$$\tau(F, 2, \mathbf{x}) = q^m (q^m - 1).$$

Ближайшая задача — получить необходимое и достаточное условие выполнения равенства

$$\tau(F, 3, \mathbf{x}) = q^m (q^m - 1) p,$$

которое, ввиду теоремы 5, эквивалентно равенству (44).

Пусть

$$f(\mathbf{x}) = f_1(\mathbf{x}), \quad J(\mathbf{x}) = J_f(\mathbf{x}),$$

F — ДЦ-подстановка и $\mathbf{x}$ принадлежит длинному циклу F . Тогда матрица $J(\mathbf{x}) - E$ обратима, и для всякого $k \geq 1$ корректно задана матрица

$$A^{[k]}(\mathbf{x}) = (J(\mathbf{x}) - E)^{-1} \cdot (J(\mathbf{x})^k - E) = E + J(\mathbf{x}) + \dots + J(\mathbf{x})^{k-1}.$$

Следующее утверждение является аналогом утверждения 3 для $s = 1$.

Утверждение 4. Если $p > 2$, F — ДЦ-подстановка, $\mathbf{x}$ принадлежит длинному циклу F , $j \geq 1$, $f(\mathbf{x}) = \mathbf{x} + p\mathbf{y}$, то

$$f^{[j]}(\mathbf{x}) \equiv \mathbf{x} + p\mathbf{y}A^{[j]}(\mathbf{x}) + \frac{p^2}{2}B^{[j]}(\mathbf{x}, \mathbf{y}) \pmod{p^3R}, \quad (45)$$

где $B^{[1]}(\mathbf{x}, \mathbf{y}) = 0$ и для всякого $j \geq 2$:

$$B^{[j]}(\mathbf{x}, \mathbf{y}) = \sum_{k=1}^{j-1} d^2 f(\mathbf{x}, \mathbf{y}A^{[k]}(\mathbf{x}))J(\mathbf{x})^{j-1-k}.$$

Доказательство. Индукция по $j \geq 1$. При $j = 1$ соотношение (45) очевидно. Осуществим индуктивный переход от j к $j + 1$. Положим

$$\mathbf{z} = \mathbf{y}A^{[j]}(\mathbf{x}) + \frac{p}{2}B^{[j]}(\mathbf{x}, \mathbf{y}).$$

Тогда по предположению индукции и формуле (39) имеем цепочку равенств и сравнений по модулю p^3R :

$$\begin{aligned} f^{[j+1]}(\mathbf{x}) &= f(f^{[j]}(\mathbf{x})) \equiv f(\mathbf{x} + p\mathbf{z}) \equiv f(\mathbf{x}) + p\mathbf{z}J(\mathbf{x}) + \frac{p^2}{2}d^2 f(\mathbf{x}, \mathbf{z}) \equiv \\ &\equiv \mathbf{x} + p\mathbf{y} + p\mathbf{y}A^{[j]}(\mathbf{x})J(\mathbf{x}) + \\ &\quad + \frac{p^2}{2}B^{[j]}(\mathbf{x}, \mathbf{y})J(\mathbf{x}) + \frac{p^2}{2}d^2 f(\mathbf{x}, \mathbf{y}A^{[j]}(\mathbf{x})) \equiv \\ &\equiv \mathbf{x} + p\mathbf{y}A^{[j+1]}(\mathbf{x}) + \frac{p^2}{2}\left[B^{[j]}(\mathbf{x}, \mathbf{y})J(\mathbf{x}) + d^2 f(\mathbf{x}, \mathbf{y}A^{[j]}(\mathbf{x}))\right] = \\ &= \mathbf{x} + p\mathbf{y}A^{[j+1]}(\mathbf{x}) + \\ &\quad + \frac{p^2}{2}\left[\sum_{k=1}^{j-1} d^2 f(\mathbf{x}, \mathbf{y}A^{[k]}(\mathbf{x}))J(\mathbf{x})^{j-k} + d^2 f(\mathbf{x}, \mathbf{y}A^{[j]}(\mathbf{x}))\right] = \\ &= \mathbf{x} + p\mathbf{y}A^{[j+1]}(\mathbf{x}) + \frac{p^2}{2}\left[\sum_{k=1}^j d^2 f(\mathbf{x}, \mathbf{y}A^{[k]}(\mathbf{x}))J(\mathbf{x})^{j-k}\right] = \\ &= \mathbf{x} + p\mathbf{y}A^{[j+1]}(\mathbf{x}) + \frac{p^2}{2}B^{[j+1]}(\mathbf{x}, \mathbf{y}). \quad \square \end{aligned}$$

Пусть $\sigma = q^m - 1$. Поэлементное разложение Тейхмюллера матрицы $A^{[\sigma]}(\mathbf{x})$ (см. раздел 3) имеет вид

$$A^{[\sigma]}(\mathbf{x}) = \sum_{s=1}^{n-1} p^s \gamma_s [A^{[\sigma]}(\mathbf{x})].$$

Тогда согласно (45)

$$f_2(\mathbf{x}) = f^{[\sigma]}(\mathbf{x}) = \mathbf{x} + p^2 \left(\mathbf{y} \gamma_1 [A^{[\sigma]}(\mathbf{x})] + \frac{1}{2} B^{[\sigma]}(\mathbf{x}, \mathbf{y}) \right) \pmod{p^3 R}.$$

Отсюда и из теоремы 5 вытекает следующий результат.

Теорема 6. Если $p > 2$, F — ДЦ-подстановка, $\mathbf{x}$ принадлежит длинному циклу F , $f(\mathbf{x}) = \mathbf{x} + p\mathbf{y}$, то равенство (44) эквивалентно условию

$$\mathbf{y} \gamma_1 [A^{[\sigma]}(\mathbf{x})] + \frac{1}{2} B^{[\sigma]}(\mathbf{x}, \mathbf{y}) \not\equiv 0 \pmod{pR}. \quad (46)$$

Следующий вопрос — как обеспечить выполнение условия (46)? Справедливо следующее утверждение.

Утверждение 5. Если $d^2 F(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod{pR}$ для любых $\mathbf{x}, \mathbf{y} \in R^m$, то

$$\forall j \geq 1, \mathbf{x}, \mathbf{y} \in R^m: \quad d^2 F^{[j]}(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod{pR}. \quad (47)$$

В частности,

$$\forall \mathbf{x}, \mathbf{y} \in R^m: \quad d^2 f(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod{pR}.$$

Доказательство. По условию

$$\forall s \in \{1, 2, \dots, m\}, \mathbf{x} \in R^m: \quad F_s''(\mathbf{x}) \equiv 0 \pmod{pR}.$$

Пусть $\mathbf{z} = (z_1, z_2, \dots, z_m)$ — строка переменных над кольцом R . Индукцией по $j \geq 1$ докажем, что

$$\forall s \in \{1, 2, \dots, m\}, \mathbf{x} \in R^m: \quad (F_s^{[j]})''(\mathbf{x}) \equiv 0 \pmod{pR}, \quad (48)$$

где $F_s^{[j]}(\mathbf{z})$ — s -й полином из представления (2) подстановки $F^{[j]}(\mathbf{z})$:

$$F^{[j]}(\mathbf{z}) = (F_1^{[j]}(\mathbf{z}), F_2^{[j]}(\mathbf{z}), \dots, F_m^{[j]}(\mathbf{z})).$$

Условие (48) эквивалентно условию (47).

При $j = 1$ сравнение (48) выполняется по условию. Осуществим индуктивный переход от j к $j + 1$. По формуле производной сложной функции

$$J_{F^{[j+1]}}(\mathbf{z}) = J_{F^{[j]}}(\mathbf{z}) \cdot J_F(F^{[j]}(\mathbf{z})).$$

Выберем и зафиксируем $s, l \in \{1, 2, \dots, m\}$. Тогда

$$\frac{\partial F_s^{[j+1]}}{\partial z_l}(\mathbf{z}) = \sum_{i=1}^m \frac{\partial F_s}{\partial z_i}(F^{[j]}(\mathbf{z})) \cdot \frac{\partial F_i^{[j]}}{\partial z_l}(\mathbf{z}). \quad (49)$$

Рассмотрим многочлены $\varphi(\mathbf{z}), \psi(\mathbf{z}) \in R[\mathbf{z}]$, определенные равенствами

$$\varphi(\mathbf{z}) = \frac{\partial F_s}{\partial z_i}(\mathbf{z}), \quad \psi(\mathbf{z}) = \frac{\partial F_i^{[j]}}{\partial z_l}(\mathbf{z}).$$

В этих обозначениях

$$\frac{\partial F_s}{\partial z_i}(F^{[j]}(\mathbf{z})) \cdot \frac{\partial F_i^{[j]}}{\partial z_l}(\mathbf{z}) = \varphi(F_1^{[j]}(\mathbf{z}), F_2^{[j]}(\mathbf{z}), \dots, F_m^{[j]}(\mathbf{z})) \cdot \psi(\mathbf{z}).$$

Выберем $k \in \{1, 2, \dots, m\}$. По формуле производной произведения

$$\begin{aligned} & \frac{\partial}{\partial z_k} \left[\frac{\partial F_s}{\partial z_i}(F^{[j]}(\mathbf{z})) \cdot \frac{\partial F_i^{[j]}}{\partial z_l}(\mathbf{z}) \right] = \\ & = \sum_{r=1}^m \frac{\partial \varphi}{\partial z_r}(F^{[j]}(\mathbf{z})) \cdot \frac{\partial F_r^{[j]}}{\partial z_k}(\mathbf{z}) \cdot \psi(\mathbf{z}) + \varphi(F^{[j]}(\mathbf{z})) \frac{\partial \psi}{\partial z_k}(\mathbf{z}). \end{aligned}$$

Пусть $\mathbf{x} \in R^m$. По предположению индукции

$$\frac{\partial \varphi}{\partial z_r}(F^{[j]}(\mathbf{x})) \equiv 0 \pmod{pR} \quad \text{и} \quad \frac{\partial \psi}{\partial z_k}(\mathbf{x}) \equiv 0 \pmod{pR}.$$

Отсюда и из (49) следует, что

$$\frac{\partial^2 F_s^{[j+1]}}{\partial z_k \partial z_l}(\mathbf{x}) \equiv 0 \pmod{pR}. \quad \square$$

Построим класс ДЦ-подстановок F со свойством

$$\forall \mathbf{x}, \mathbf{y} \in R^m: \quad d^2 F(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod{pR}. \quad (50)$$

Пусть $C \in R_{m,m}$ — обратимая матрица со свойством $\text{ord}_p(C) = q^m - 1$, $\gamma_0(x)$ — функция из разложения Тейхмюллера, $\Psi(\mathbf{z}) \in R[\mathbf{z}]_{m \times m}$. Подстановку $F(\mathbf{z})$ будем строить так:

$$F(\mathbf{z}) = \gamma_0[G(\mathbf{z})] + (\mathbf{z} - \mathbf{z}^q) C + p(\mathbf{z} - \mathbf{z}^q) \Psi(\mathbf{z}), \quad (51)$$

где $\overline{G}$ — полноцикловое полиномиальное преобразование векторного пространства $\overline{R}^m$. Функция $\gamma_0(x)$ задается многочленом $x^{q^{n-1}}$, поэтому преобразование (51) полиномиально.

Поскольку $F(\mathbf{x}) \equiv G(\mathbf{x}) \pmod{pR}$ для всякого $\mathbf{x} \in R^m$, преобразование $\overline{F}$ является полноцикловым. Пусть $s \in \{1, 2, \dots, m\}$. Тогда существует такой многочлен $\alpha(\mathbf{z}) \in R[\mathbf{z}]$, что

$$F_s(\mathbf{z}) = G_s(\mathbf{z})^{q^{n-1}} + \sum_{i=1}^m (z_i - z_i^q) c_{i,s} + p\alpha(\mathbf{z}).$$

Для любого $l \in \{1, 2, \dots, m\}$

$$\frac{\partial F_s}{\partial z_l}(\mathbf{z}) = q^{n-1} G_s(\mathbf{z})^{q^{n-1}-1} \cdot \frac{\partial G_s}{\partial z_l}(\mathbf{z}) + (e - qz_l^{q-1}) c_{l,s} + p \frac{\partial \alpha}{\partial z_l}(\mathbf{z}).$$

Поскольку R — собственное кольцо Галуа, $n \geq 2$. Следовательно, существует такой многочлен $\beta(\mathbf{z}) \in R[\mathbf{z}]$, что

$$\frac{\partial F_s}{\partial z_l}(\mathbf{z}) = c_{l,s} + p\beta(\mathbf{z}).$$

Поэтому

$$J_F(\mathbf{x}) \equiv C \pmod{pR} \quad \text{и} \quad F_s''(\mathbf{x}) \equiv 0 \pmod{pR}$$

для любых $\mathbf{x} \in R^m$ и $s \in \{1, 2, \dots, m\}$. Тогда верно (50) и, согласно (5),

$$\forall \mathbf{x} \in R^m: \quad J_f(\mathbf{x}) \equiv C^{q^m} \pmod{pR}.$$

Поэтому $\text{ord}_p J_f(\mathbf{x}) = q^m - 1$ для любого $\mathbf{x} \in R^m$, и по следствию 2 подстановка F является ДЦ-подстановкой. Согласно утверждению 5

$$\forall \mathbf{x}, \mathbf{y} \in R^m: \quad d^2 f(\mathbf{x}, \mathbf{y}) \equiv 0 \pmod{pR}. \quad (52)$$

Таким образом, для любого такого собственного кольца Галуа $R = GR(q^n, p^n)$, что $p > 2$, и для любого $m \geq 2$ над кольцом R существует m -мерная ДЦ-подстановка F со свойством (52).

Для ДЦ-подстановок F со свойством (52) условие (46) существенно упрощается и принимает вид

$$\mathbf{y} \gamma_1 [J_f(\mathbf{x})^{q^m} - J_f(\mathbf{x})] \not\equiv 0 \pmod{pR}. \quad (53)$$

Пусть $\chi(x)$ — характеристический многочлен матрицы $J_f(\mathbf{x})$, $\tilde{R} = R/p^2R$, $\tilde{\chi}(x)$ — образ многочлена $\chi(x)$ под действием естественного эпиморфизма $R \rightarrow \tilde{R}$. Хорошо известно (см., например, [7, теорема 4.4]), что при $p > 2$ унитарный реверсивный многочлен является многочленом максимального периода (ММП) тогда и только тогда, когда он — многочлен максимального периода (ММП) по модулю p^2 . Так как $\bar{\chi}(x)$ — ММП по модулю pR , то либо многочлен $\tilde{\chi}(x)$ — *отмеченный*, либо $\chi(x)$ — многочлен максимального периода.

Если $\tilde{\chi}(x)$ — отмеченный многочлен, то $J_f(\mathbf{x})^{q^m} \equiv J_f(\mathbf{x}) \pmod{p^2R}$, и условие (53) не выполняется. Пусть $\chi(x)$ — многочлен максимального периода, и α — его корень в кольце $S = GR(q^{mn}, p^n)$. В разложении Тейхмюллера

$$\alpha = \alpha_0 + p\alpha_1 + p^2\alpha_2 + \dots + p^{n-1}\alpha_{n-1}$$

элемент α_1 отличен от 0. Если $\langle \varphi \rangle = \text{Aut}(S/R)$, то существует такая матрица $T \in S_{m,m}^*$, что

$$T^{-1} J_f(\mathbf{x}) T = \text{diag}(\alpha, \varphi(\alpha), \dots, \varphi^{m-1}(\alpha)).$$

Нетрудно показать, что для любого $s \in \{0, 1, \dots, m-1\}$ выполняется сравнение

$$[\varphi^s(\alpha)]^{q^m} \equiv \varphi^s(\alpha_0) \pmod{p^2S}.$$

Тогда

$$T^{-1} [J_f(\mathbf{x})^{q^m} - J_f(\mathbf{x})] T \equiv -p \cdot \text{diag}(\alpha_1, \varphi(\alpha_1), \dots, \varphi^{m-1}(\alpha_1)) \pmod{p^2S}.$$

Следовательно, матрица $\gamma_1 [J_f(\mathbf{x})^{q^m} - J_f(\mathbf{x})]$ обратима по модулю pR . Если вектор $\mathbf{x}$ принадлежит длинному циклу ДЦ-подстановки F , то $\bar{\mathbf{y}} \neq 0$, и условие (53) выполняется. Таким образом, доказана следующая теорема.

Теорема 7. Если $p > 2$, $n \geq 3$, F — ДЦ-подстановка, $\mathbf{x}$ принадлежит длинному циклу F , $\chi(x)$ — характеристический многочлен матрицы $J_f(\mathbf{x})$ и выполняется условие (52), то следующие утверждения эквивалентны:

1. $\chi(x)$ — многочлен максимального периода,
2. $\tau(F, n, \mathbf{x}) = q^m (q^m - 1) p^{n-2}$.

В следующем алгоритме $\mathbf{z} = (z_1, z_2, \dots, z_m)$ — строка переменных над кольцом R . Алгоритм строит МДЦ-подстановку F вида (51), а также вектор $\mathbf{x} \in R^m$, принадлежащий циклу длины $L_m(R)$.

Алгоритм А. (Построение пары $(F, \mathbf{x})$ со свойством $\tau(F, n, \mathbf{x}) = L_m(R)$.)

1. Построить такое m -мерное полиномиальное преобразование G кольца R , что $\overline{G}$ — полноцикловое преобразование пространства $\overline{R}^m$. Выбрать $w_0 \in R^m$. Для всякого $i \in \{1, 2, \dots, q^m - 1\}$ вычислить $w_i = G(w_{i-1})$.
2. Построить $H(x) \in R[x]$ — многочлен, отмеченный по модулю p^2R . Выбрать $T \in R_{m,m}^*$. Положить $C = T^{-1}S(H)T$, где $S(H)$ — сопрягающая матрица для многочлена $H(x)$.
3. Положить

$$F(\mathbf{z}) := \gamma_0[G(\mathbf{z})] + (\mathbf{z} - \mathbf{z}^q)C + p(\mathbf{z} - \mathbf{z}^q)\Psi(\mathbf{z}),$$

где $\Psi(\mathbf{z}) \in R[\mathbf{z}]_{m,m}$ — произвольная матрица со свойствами

$$\begin{aligned} \forall i \in \{0, 1, \dots, q^m - 2\}: \quad & \Psi(w_i) \equiv 0 \pmod{pR} \text{ и} \\ & \Psi(w_{q^m-1}) \equiv -C \pmod{pR}. \end{aligned}$$

4. Выбрать $\mathbf{x} \in R^m$ со свойством $\overline{\mathbf{x}} = \overline{w}_0$. При помощи формулы (30) вычислить $\mathbf{x}^*$ по модулю p^2R . Если $\mathbf{x} \not\equiv \mathbf{x}^* \pmod{p^2R}$, то СТОП. Иначе положить $\mathbf{x} := \mathbf{x} + p\mathbf{a}$, где $\mathbf{a} \in \Gamma(R)^m \setminus \{0\}$.

Обоснование алгоритма. Очевидно, что алгоритм строит ДЦ-подстановку F вида (51) и вектор $\mathbf{x} \in R^m$, принадлежащий длинному циклу подстановки F . Как показано выше, подстановка F обладает свойством (52). По теореме 7 осталось доказать, что характеристический многочлен $\chi(x)$ матрицы $J_f(\mathbf{x})$ является многочленом максимального периода. Это условие эквивалентно обратимости матрицы

$$\gamma_1[J_f(\mathbf{x})^{q^m} - J_f(\mathbf{x})]. \quad (54)$$

По формуле производной сложной функции верно равенство

$$J_f(\mathbf{x}) = \prod_{s=0}^{q^m-1} J_F(F^{[s]}(\mathbf{x})).$$

Пусть векторы $\mathbf{y}_s \in R^m$ таковы, что $\overline{\mathbf{y}}_s = \overline{w}_s$, $s = 0, 1, 2, \dots$. Тогда

$$J_f(\mathbf{x}) = \prod_{s=0}^{q^m-1} J_F(\mathbf{y}_s). \quad (55)$$

Рассмотрим произвольные $i, j \in \{1, 2, \dots, m\}$. Имеем:

$$\begin{aligned} \frac{\partial F_j}{\partial z_i}(\mathbf{z}) &= q^{n-1} G_j(\mathbf{z})^{q^{n-1}-1} \frac{\partial G_j}{\partial z_j}(\mathbf{z}) + (e - q z_i^{q-1}) c_{i,j} + \\ &+ p \psi_{i,j}(\mathbf{z}) + p \sum_{k=1}^m (z_k - z_k^q) \frac{\partial \psi_{k,j}}{\partial z_i}(\mathbf{z}), \end{aligned}$$

где $\psi_{u,v}(\mathbf{z})$ — элемент, стоящий на пересечении u -й строки и v -го столбца матрицы $\Psi(\mathbf{z})$. Поскольку R — собственное кольцо Галуа, $p^2 \mid q \mid q^{n-1}$. Для всякого $s \in \{0, 1, \dots, m-1\}$

$$\frac{\partial F_j}{\partial z_i}(\mathbf{y}_s) \equiv c_{i,j} + p \psi_{i,j}(w_s) \pmod{p^2 R}.$$

Отсюда следует, что

$$J_F(\mathbf{y}_s) \equiv C + p \Psi(w_s) \pmod{p^2 R}.$$

По формуле (55) и согласно шагу 3 алгоритма А имеем цепочку сравнений по модулю $p^2 R$:

$$J_f(\mathbf{x}) \equiv C^{q^m-1} (C - p C) \equiv C - p C.$$

С другой стороны, поскольку $H(x)$ — отмеченный по модулю $p^2 R$, имеем еще одну серию сравнений по модулю $p^2 R$:

$$J_f(\mathbf{x})^{q^m} \equiv (C - p C)^{q^m} \equiv C^{q^m} \equiv C.$$

Тогда

$$J_f(\mathbf{x})^{q^m} - J_f(\mathbf{x}) \equiv p C \pmod{p^2 R},$$

и, следовательно,

$$\gamma_1 [J_f(\mathbf{x})^{q^m} - J_f(\mathbf{x})] \equiv C \pmod{p R}.$$

Поэтому матрица (54) обратима. $\square$

В заключение построим один класс МДЦ-подстановок, для которых удастся полностью описать их цикловую структуру.

Пусть Ω — непустое конечное множество. Цикловая структура произвольной подстановки $\varphi \in S(\Omega)$ характеризуется ее *цикловым типом*, т. е. многочленом

$$C_\varphi(y) = \sum_{i \geq 1} c_i^{(\varphi)} y^i \in \mathbb{Z}[y],$$

где $c_i^{(\varphi)}$ — количество циклов длины i в цикловой структуре φ , $i = 1, 2, \dots$. Если $G(x) \in R[x]$ — унитарный реверсивный многочлен, то под *цикловым типом* ЛРП-семейства $L_R(G)$ понимается цикловой тип $C_\psi(y)$, где $\psi: L_R(G) \rightarrow L_R(G)$ — преобразование, определенное равенством

$$\forall u \in L_R(G): \quad \psi(u) = xu.$$

Хорошо известно (см., например, [7]), что если $R = GR(q^n, p^n)$, а $G(x) \in R[x]$ — многочлен максимального периода степени m , то цикловой тип ЛРП-семейства $L_R(G)$ равен

$$C_{m,R}(y) = y + \sum_{s=0}^{n-1} \left(\frac{q^m}{p} \right)^{n-s-1} y^{(q^{m-1})p^{n-s-1}}.$$

Пусть $R = GR(q^n, p^n)$ — произвольное кольцо Галуа, отличное от конечного поля (случай, когда R — примарное кольцо вычетов, не исключен), $p > 2$, $m \geq 2$ и S — расширение Галуа степени m кольца R : $S = GR(q^{mn}, p^n)$. Рассмотрим одномерную полиномиальную подстановку F над кольцом S , заданную равенством

$$F(z) = a(z)^{q^{m(n-1)}} + (z^{q^m} - z)c + p(z^{q^m} - z)b(z), \quad (56)$$

где многочлен $\bar{a}$ задает полноцикловую подстановку над $\bar{S}$, $\langle c \rangle = \Gamma(S) \setminus \{0\}$, и для некоторой последовательности

$$w_0, w_1, \dots, w_{q^m-1} \in S,$$

обладающей свойством

$$w_{i+1} \equiv a(w_i) \pmod{pS}, \quad i = 0, 1, \dots,$$

выполняются равенства

$$\bar{b}(\bar{w}_0) = \bar{b}(\bar{w}_1) = \dots = \bar{b}(\bar{w}_{q^m-2}) = \bar{0} \quad \text{и} \quad \bar{b}(\bar{w}_{q^m-1}) = -\bar{c}.$$

Тогда $F''(\alpha) \equiv 0 \pmod{pS}$ для любого $\alpha \in S$. Заметим, что утверждение 5 справедливо и в случае $m = 1$. Поэтому для $f = F^{[q^m]}$ верно сравнение

$$\forall \alpha \in S: \quad f''(\alpha) \equiv 0 \pmod{pS}. \quad (57)$$

По построению (см. алгоритм 1 из работы [5]) и ввиду (57) подстановка F является МДЦ-подстановкой над кольцом S . Согласно [5, теорема 5] цикловой тип $C_F(y)$ подстановки F удовлетворяет равенству

$$C_F(y) = C_{m,R}(y^{q^m}).$$

Пусть $S = R[\alpha]$. Рассмотрим циклический базис $\mathbf{a} = (e, \alpha, \dots, \alpha^{m-1})$ модуля ${}_R S$. В обозначениях раздела 2 цикловые типы полиномиальных подстановок $F: S \rightarrow S$ и $\hat{F} = \Phi_{\mathbf{a}}(F): R^m \rightarrow R^m$ равны. Поэтому

$$C_{\hat{F}}(y) = C_F(y) = C_{m,R}(y^{q^m}).$$

Итак, доказана следующая теорема.

Теорема 8. Пусть $R = GR(q^n, p^n)$, $p > 2$, $m \geq 2$, $n \geq 2$, $S = GR(q^{mn}, p^n)$ — расширение Галуа степени m кольца R , F — подстановка над кольцом S вида (56). Тогда для любого $\alpha \in S$ со свойством $S = R[\alpha]$ цикловой тип $C_{\hat{F}}(y)$ полиномиальной подстановки $\hat{F} = \Phi_{\mathbf{a}}(F): R^m \rightarrow R^m$ удовлетворяет равенству

$$C_{\hat{F}}(y) = C_{m,R}(y^{q^m}).$$

В частности, на циклах длины $L_m(R)$ подстановки $\hat{F} = \Phi_{\mathbf{a}}(F)$ лежит ровно $q^{mn}(1 - q^{-m})$ векторов. Сравнивая с результатом следствия 3, получаем, что все длинные циклы подстановки $\hat{F}$ являются циклами максимальной возможной длины $L_m(R)$. «Почти все» векторы принадлежат циклам длины $L_m(R)$; доля векторов, не принадлежащих циклам длины $L_m(R)$, равна $q^{-m} = o(1)$, $m \rightarrow \infty$.

Автор признателен Д. М. Ермилову и В. Е. Викторенкову за полезное обсуждение результатов этой работы. Работа посвящается памяти А. А. Нечаева.

Список литературы

- [1] Викторенков В.Е., “Орграф полиномиального преобразования над коммутативным локальным кольцом”, *Обозрение прикл. и промышл. матем.*, **7:2** (2000), 327.
- [2] Викторенков В.Е., “О строении орграфов полиномиальных преобразований над конечными коммутативными кольцами с единицей”, *Дискретная математика*, **29:3** (2017), 3–23.
- [3] Ермилов Д.М., “Свойства полиномиальных генераторов с выходной последовательностью наибольшего периода над кольцом Галуа”, *Прикладная дискретная математика*, № 1 (27) (2015), 52–61.
- [4] Ермилов Д.М., Козлитин О.А., “Цикловая структура полиномиального генератора над кольцом Галуа”, *Математические вопросы криптографии*, **4:1** (2013), 27–57.
- [5] Ермилов Д.М., Козлитин О.А., “О строении графа полиномиального преобразования кольца Галуа”, *Математические вопросы криптографии*, **6:3** (2015), 47–73.
- [6] Козлитин О.А., “Оценка длины максимального цикла в графе полиномиального преобразования кольца Галуа–Эйзенштейна”, *Дискретная математика*, **29:4** (2017), 41–58.
- [7] Кузьмин А.С., Куракин В.Л., Нечаев А.А., “Псевдослучайные и полилинейные последовательности”, *Труды по дискретной математике*, **1** (1997), 139–202.
- [8] Ларин М.В., “Транзитивные полиномиальные преобразования колец вычетов”, *Дискретная математика*, **14:2** (2002), 20–32.
- [9] Лидл Р., Нидеррайтер Г., *Конечные поля*. В 2 т., М.: Мир, 1988, 824 с.
- [10] Нечаев А.А., “Базис обобщенных тождеств конечного коммутативного локального кольца главных идеалов”, *Алгебра и логика*, **18:2** (1979), 186–193.
- [11] Нечаев А.А., “Код Кердока в циклической форме”, *Дискретная математика*, **1:4** (1989), 123–139.
- [12] Нечаев А.А., “Полиномиальные преобразования конечных коммутативных колец главных идеалов”, *Математические заметки*, **27:6** (1980), 885–899.
- [13] Anashin V.S., “Uniformly distributed sequences in computer algebra or how to construct program generators of random numbers”, *J. of Math. Sciences*, **89:4** (1998), 1355–1390.
- [14] Brawley J. V., Mullen G. L., “Functions and polynomials over Galois ring”, *J. Number Theory*, **41** (1992), 156–166.
- [15] McDonald B. R., *Finite Rings with Identity*, New York: Dekker, 1974, ix+429 p.
- [16] Parvatov N.G., “On the period length of vector sequences generated by polynomials modulo prime powers”, *Прикладная дискретная математика*, № 1(31) (2016), 57–61.