Math-Net.Ru

Общероссийский математический портал

О. А. Козлитин, Периодические свойства многомерного полиномиального генератора над кольцом Галуа. II, *Матем. вopr. криптогр.*, 2020, том 11, выпуск 1, 63–100

DOI: <https://doi.org/10.4213/mvk315>

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: 35.173.137.237

26 апреля 2023 г., 07:32:46

Периодические свойства многомерного полиномиального генератора над кольцом Галуа. II

О. А. Козлитин

ООО «Центр сертификационных исследований», Москва

Получено 29.IV.2019

Аннотация. Изучаются периодические свойства m -мерных полиномиальных подстановок над кольцом Галуа R четной характеристики. Предложен метод построения подстановок, обладающих циклом, длина которого является максимальной возможной для данных R и m . Описан цикловой тип m -мерной полиномиальной подстановки специального вида.

Ключевые слова: полиномиальная подстановка, цикловой тип

Periodical properties of multidimensional polynomial generator over Galois ring. II

O. A. Kozlitin

Certification Research Center, LLC, Moscow

Abstract. Periodic properties of m -dimensional polynomial substitutions over the Galois ring R of even characteristic are investigated. A method permitting for the given R and m to construct substitutions with maximal possible cycle length is proposed. The cycle type of m -dimensional polynomial substitutions of the special form is described.

Keywords: polynomial substitution, cyclic type

1. Введение

Пусть $R = GR(q^n, p^n)$ – кольцо Галуа мощности q^n и характеристики p^n (см., например, [8]), $q = p^t$, $t \geq 1$, $m \geq 1$, $\mathbf{x} = (x_1, x_2, \dots, x_m)$ – строка переменных над кольцом R . Рассмотрим семейство многочленов

$$F_1(\mathbf{x}), F_2(\mathbf{x}), \dots, F_m(\mathbf{x}) \in R[\mathbf{x}]$$

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

$$\forall \mathbf{a} \in R^m : F(\mathbf{a}) = (F_1(\mathbf{a}), \dots, F_m(\mathbf{a})), \quad (1)$$

биективно. Всякое преобразование вида (1) будем называть *m -мерной полиномиальной подстановкой*. В случае когда размерность m известна или не имеет значения, m -мерную полиномиальную подстановку будем называть *многомерной полиномиальной подстановкой*.

Функция F вида (1) может использоваться в качестве функции перехода состояний так называемого *полиномиального генератора*. Полиномиальный генератор применяется для выработки псевдослучайных последовательностей (ПСП) с гарантированными криптографическими (в частности, периодическими) свойствами. Важнейшие понятия, а также основы математического аппарата, необходимые для исследования периодических свойств полиномиального генератора, сформулированы В.С. Анашиным [1], М.В. Лариным [9], В.Е. Викторенковым [3] и в дальнейшем развиты в [4–7, 10]. Обзор литературы на эту тему можно найти в [4, 7].

Настоящая работа является продолжением [7]. Перечислим основные результаты работы [7]. Пусть $L_m(R)$ – максимум длин циклов m -мерных полиномиальных подстановок над кольцом Галуа R .

- 1) Показано, что для всякого *собственного* кольца Галуа R , т. е. кольца Галуа, отличного от конечного поля и от примарного кольца вычетов, верно равенство $L_m(R) = q^m(q^m - 1)p^{n-2}$.
- 2) При $p > 2$ предложен метод построения полиномиальных подстановок, обладающих циклом максимальной возможной длины $L_m(R)$ (так называемых МДЦ-подстановок).

Результаты настоящей работы относятся к случаю $p = 2$. Перечислим их.

- 1) Описаны длины циклов m -мерной полиномиальной подстановки (теорема 7).

- 2) Предложен алгоритм, позволяющий строить широкий класс МДЦ-подстановок (алгоритм 13).
- 3) Описан цикловой тип МДЦ-подстановок специального вида (теорема 18).

Всюду по тексту используются обозначения из [7].

2. Случай $p = 2$: длины циклов

В этом и следующем разделах $p = 2$, т.е. R – кольцо Галуа четной характеристики 2^n . Случай $p > 2$ был ранее рассмотрен в [7].

Пусть $\mathbf{a} \in R^m$, $s \geq 1$, $\tau_s = \tau_s(\mathbf{a}) = \tau(F, s, \mathbf{a})$ – период реверсивной последовательности

$$\mathbf{a} \bmod 2^s R, \quad F(\mathbf{a}) \bmod 2^s R, \quad F(F(\mathbf{a})) \bmod 2^s R, \dots,$$

где приведение по модулю идеала осуществляется по координатно. Для всякого $i \geq 1$ обозначим i -ю композиционную степень преобразования F через $F^{[i]}$:

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

и положим $f_s = F^{[\tau_s]}$, $s = 1, 2, \dots$. Всякому преобразованию F вида (1) сопоставим матрицу Якоби $J_F(\mathbf{x})$:

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

где частные производные от многочленов вводятся стандартным образом (см., например, [10]). Согласно формуле производной сложной функции имеем:

$$J_{f_s}(\mathbf{x}) = \prod_{i=0}^{\tau_s-1} J_F(F^{[i]}(\mathbf{x})). \quad (2)$$

Поскольку F биективно, матрица $J_F(\mathbf{a})$ обратима при любом $\mathbf{a} \in R^m$. Следовательно, матрица $J_{f_s}(\mathbf{a})$ обратима.

Преобразование f_n является тождественным, поэтому $J_{f_n}(\mathbf{a}) = E$. Существует такое $s \in \{1, 2, \dots, n\}$, что

$$J_{f_s}(\mathbf{a}) \equiv E \pmod{2R}. \quad (3)$$

Обозначим минимальное s со свойством (3) через s_0 . Понятно, что $s_0 = s_0(F, \mathbf{a})$. Введем обозначение: $A_s(\mathbf{a}) = J_{f_s}(\mathbf{a})$. Следующая лемма отражает одно полезное свойство величины s_0 .

Лемма 1. Для всякого $s \geq s_0$ верно соотношение

$$A_s(\mathbf{a}) \equiv E \pmod{2R}.$$

Доказательство. Очевидно, что $\tau_{s_0} \mid \tau_s$, т. е. существует такое $\Delta \in \mathbb{N}$, что $\tau_s = \Delta \cdot \tau_{s_0}$. Поскольку

$$\forall i \geq 0 : F^{[i+\tau_{s_0}]}(\mathbf{a}) = F^{[\tau_{s_0}]}(F^{[i]}(\mathbf{a})) \equiv F^{[i]}(\mathbf{a}) \pmod{2R},$$

по формулам (2) и (3) получаем цепочку равенств и сравнений по модулю $2R$:

$$\begin{aligned} J_{f_s}(\mathbf{a}) &= \prod_{i=0}^{\tau_s-1} J_F(F^{[i]}(\mathbf{a})) = \prod_{k=0}^{\Delta-1} \prod_{i=k\tau_{s_0}}^{(k+1)\tau_{s_0}-1} J_F(F^{[i]}(\mathbf{a})) \\ &\equiv \prod_{k=0}^{\Delta-1} \prod_{i=0}^{\tau_{s_0}-1} J_F(F^{[i]}(\mathbf{a})) = [A_{s_0}(\mathbf{a})]^\Delta \equiv E. \end{aligned}$$

□

Для всякого $i \in \{1, 2, \dots, m\}$ обозначим через $F_i''(\mathbf{x})$ матрицу, состоящую из вторых производных:

$$F_i''(\mathbf{x}) = \begin{pmatrix} \frac{\partial^2 F_i(\mathbf{x})}{\partial x_1^2} & \frac{\partial^2 F_i(\mathbf{x})}{\partial x_1 \partial x_2} & \dots & \frac{\partial^2 F_i(\mathbf{x})}{\partial x_1 \partial x_m} \\ \frac{\partial^2 F_i(\mathbf{x})}{\partial x_2 \partial x_1} & \frac{\partial^2 F_i(\mathbf{x})}{\partial x_2^2} & \dots & \frac{\partial^2 F_i(\mathbf{x})}{\partial x_2 \partial x_m} \\ \vdots & \vdots & \ddots & \vdots \\ \frac{\partial^2 F_i(\mathbf{x})}{\partial x_m \partial x_1} & \frac{\partial^2 F_i(\mathbf{x})}{\partial x_m \partial x_2} & \dots & \frac{\partial^2 F_i(\mathbf{x})}{\partial x_m^2} \end{pmatrix}.$$

Согласно [7, утверждение 5] условие

$$\forall i \in \{1, 2, \dots, m\}, \mathbf{a} \in R^m : F_i''(\mathbf{a}) \equiv 0 \pmod{2R} \quad (4)$$

влечет соотношение

$$\forall i \in \{1, 2, \dots, m\}, j \geq 1, \mathbf{a} \in R^m : G_i''(\mathbf{a}) \equiv 0 \pmod{2R}, \quad (5)$$

где

$$(G_1(\mathbf{x}), G_2(\mathbf{x}), \dots, G_m(\mathbf{x})) = F^{[j]}(\mathbf{x}).$$

Условие (4) выполняется, например, если каждый моном w всякого многочлена $F_i(\mathbf{x})$, $i = 1, 2, \dots, m$, удовлетворяет одному из условий:

- 1) либо степень $\deg_{x_j}(w)$ четна для всякого $j \in \{1, 2, \dots, m\}$,
- 2) либо существует единственное такое $j \in \{1, 2, \dots, m\}$, что степень $\deg_{x_j}(w)$ нечетна.

В частности, при $m = 1$ условие (4) всегда выполняется.

Пусть $k \geq 0$. Для краткости обозначим матрицу $J_{f_s^{[2^k]}(\mathbf{x})}$ через $A_{s,k}(\mathbf{x})$. При условии (4) лемму 1 можно обобщить.

Лемма 2. Пусть $\mathbf{a} \in R^m$ и выполнено (4). Тогда для любых $k \geq 0$ и $s \geq s_0$ верно соотношение

$$A_{s,k}(\mathbf{a}) \equiv E \pmod{2^{\min\{s,k\}+1}R}.$$

Доказательство. Индукцией по $k \geq 0$ покажем, что

$$A_{s,k}(\mathbf{a}) \equiv A_s(\mathbf{a})^{2^k} \pmod{2^{s+1}R}. \quad (6)$$

При $k = 0$ соотношение (6) очевидно. Осуществим индуктивный переход от k к $k + 1$. Рассмотрим последовательность $u \in (R^m)^\infty$, определенную равенствами

$$u(0) = \mathbf{a}, \quad \forall i \geq 1: \quad u(i) = F^{[i]}(u(0)).$$

Имеем цепочку соотношений:

$$\begin{aligned} A_{s,k+1}(\mathbf{a}) &= J_{F^{[2^{k+1}\tau_s]}(\mathbf{a})} = \prod_{i=0}^{2^{k+1}\tau_s-1} J_F(u(i)) \\ &= \prod_{i=0}^{2^k\tau_s-1} J_F(u(i)) \times \prod_{j=2^k\tau_s}^{2^{k+1}\tau_s-1} J_F(u(j)) = A_{s,k}(\mathbf{a}) \cdot A_{s,k}(u(2^k\tau_s)). \end{aligned} \quad (7)$$

Пусть

$$f_s^{[2^k]}(\mathbf{x}) = (G_1(\mathbf{x}), G_2(\mathbf{x}), \dots, G_m(\mathbf{x})).$$

Поскольку $f_s^{[2^k]} = F^{[2^k\tau_s]}$, в силу (5) имеем: $G_i''(\mathbf{a}) \equiv 0 \pmod{2R}$. Это означает, что если $J_{f_s^{[2^k]}(\mathbf{x})} = (\varphi_{\mu,\nu}(\mathbf{x}))_{m \times m}$, то для любого $i \in \{1, 2, \dots, m\}$ верно соотношение

$$\frac{\partial \varphi_{\mu,\nu}}{\partial x_i}(\mathbf{a}) \equiv 0 \pmod{2R}. \quad (8)$$

Из формулы Тейлора [7, формула (18)] и определения величины s_0 следует, что для всякого $s \geq s_0$ справедливо соотношение

$$f_s^{[2]}(\mathbf{a}) \equiv \mathbf{a} \pmod{2^{s+1}R}. \quad (9)$$

Поэтому для всякого $k \geq 0$ имеем: $\tau_{s+k} \mid \tau_s \cdot 2^k$. Следовательно, существует такой вектор $\mathbf{b} \in R^m$, что $u(\tau_s \cdot 2^k) = \mathbf{a} + 2^{s+k}\mathbf{b}$. Ввиду (8) для любых $\mu, \nu \in \{1, 2, \dots, m\}$ получаем цепочку равенств и сравнений по модулю $2^{s+k+1}R$:

$$\varphi_{\mu,\nu}(u(\tau_s \cdot 2^k)) = \varphi_{\mu,\nu}(\mathbf{a} + 2^{s+k}\mathbf{b}) \equiv \varphi_{\mu,\nu}(\mathbf{a}) + 2^{s+k} \left[\sum_{i=1}^m b_i \frac{\partial \varphi_{\mu,\nu}}{\partial x_i}(\mathbf{a}) \right] \equiv \varphi_{\mu,\nu}(\mathbf{a}).$$

Поэтому

$$A_{s,k}(u(2^k \tau_s)) \equiv A_{s,k}(\mathbf{a}) \pmod{2^{s+k+1}R}.$$

Отсюда и из (7) следует, что

$$A_{s,k+1}(\mathbf{a}) \equiv A_{s,k}(\mathbf{a})^2 \pmod{2^{s+k+1}R}.$$

По предположению индукции имеем цепочку сравнений по модулю $2^{s+1}R$:

$$A_{s,k+1}(\mathbf{a}) \equiv A_{s,k}(\mathbf{a})^2 \equiv A_s(\mathbf{a})^{2^{k+1}}.$$

Соотношение (6) доказано.

По лемме 1 существует такая матрица $U_s(\mathbf{a})$, что $A_s(\mathbf{a}) = E + 2U_s(\mathbf{a})$. Тогда

$$A_s(\mathbf{a})^2 = E + 4U_s(\mathbf{a}) + 4U_s(\mathbf{a})^2 \equiv E \pmod{2^2R}.$$

Аналогично,

$$A_s(\mathbf{a})^{2^2} \equiv E \pmod{2^3R}, \quad \dots, \quad A_s(\mathbf{a})^{2^k} \equiv E \pmod{2^{k+1}R}.$$

Отсюда и из (6) получаем требуемое утверждение. $\square$

Пусть $C = C(F, \mathbf{a})$ – цикл полиномиальной подстановки F , которому принадлежит вектор $\mathbf{a} \in R^m$. Следуя [7], для всякого $s \in \{1, 2, \dots, n-1\}$ положим

$$d_s = d_s(C) = \tau_{s+1}(\mathbf{a}) / \tau_s(\mathbf{a}).$$

Изучим *профиль* цикла C , т. е. последовательность

$$d_1(C), d_2(C), \dots, d_{n-1}(C). \quad (10)$$

В тех случаях, когда вектор $\mathbf{a}$ (а значит, и цикл C) фиксирован, вместо $d_s(C)$ будем писать d_s , $s = 1, 2, \dots, n-1$. Из соотношения (9) вытекает, что

$$\forall s \geq s_0 : (d_s > 1) \Rightarrow (d_s = 2). \quad (11)$$

Рассмотрим величину $\nu = \nu(\mathbf{a})$, определенную равенством

$$\nu = \begin{cases} 0, & \text{если } d_{s_0} > 1, \\ \max\{\lambda \in \{1, \dots, n - s_0\} : d_{s_0} = d_{s_0+1} = \dots = d_{s_0+\lambda-1} = 1\}, & \text{если } d_{s_0} = 1. \end{cases}$$

Профиль (10) цикла C разобьем на 2 части:

$$(d_1, d_2, \dots, d_{s_0-1}) \quad (12)$$

и

$$(d_{s_0}, d_{s_0+1}, \dots, d_{n-1}). \quad (13)$$

Сначала опишем строение отрезка (13). Согласно (11) он состоит из «1» и «2».

Утверждение 3. При условии (4) имеет место одна из следующих ситуаций:

1) $\nu = n - s_0$ и отрезок (13) состоит из единиц,

2) $\nu \leq n - s_0 - 1$ и отрезок (13) имеет вид

$$(1, 1, \dots, 1, 2, 2, \dots, 2),$$

где число единиц равно ν ,

3) $\nu \leq n - s_0 - 2$, и отрезок (13) имеет вид

$$(1, 1, \dots, 1, 2, 1, 1, \dots, 1),$$

где длина первой серии единиц равна ν ,

4) существует такое значение $\rho \geq 1$, что $\nu \leq n - \rho - s_0 - 2$ и отрезок (13) имеет вид

$$(1, 1, \dots, 1, 2, 1, 1, \dots, 1, 2, 2, \dots, 2),$$

где длина первой серии единиц равна ν , а второй – ρ .

Доказательство. Если $\nu = n - s_0$, то отрезок (13) состоит из единиц, т. е. имеет место ситуация 1). Пусть $\nu < n - s_0$. Тогда $d_{s_0+\nu} = 2$. Рассмотрим максимальное значение $\rho \in \{0, 1, \dots, n - \nu - s_0 - 1\}$, для которого $d_{s_0+\nu+1} = d_{s_0+\nu+2} = \dots = d_{s_0+\nu+\rho} = 1$. Возможны следующие случаи:

А. $\rho = 0$. Покажем, что имеет место ситуация 2). Если $\nu = n - s_0 - 1$, то все доказано. Если $\nu < n - s_0 - 1$, то $d_{s_0+\nu+1} = 2$. Индукцией по s докажем, что

$$d_s = 2 \quad \forall s \in \{s_0 + \nu + 1, s_0 + \nu + 2, \dots, n - 1\}. \quad (14)$$

База индукции ($s = s_0 + \nu + 1$) очевидна. Если $\nu = n - s_0 - 2$, то все доказано. Пусть $\nu < n - s_0 - 2$ и для некоторого $s \in \{s_0 + \nu + 1, s_0 + \nu + 2, \dots, n - 2\}$ верна цепочка равенств

$$d_{s_0+\nu+1} = d_{s_0+\nu+2} = \dots = d_s = 2. \quad (15)$$

Докажем, что $d_{s+1} = 2$. В силу (11) достаточно доказать, что $d_{s+1} > 1$, или, что равносильно, $\tau_{s+2} > \tau_{s+1}$.

Ввиду (9) имеем: $\tau_s \mid \tau_{s_0} \cdot 2^{s-s_0}$. Следовательно, $\tau_s = 2^k \cdot \tau_{s_0}$, где $k \leq s - s_0$. Если $k = 0$, то имеет место цепочка соотношений

$$2 = d_{s_0+\nu} = \frac{\tau_{s_0+\nu+1}}{\tau_{s_0+\nu}} \mid \frac{\tau_s}{\tau_{s_0}} = 1.$$

Противоречие. Поэтому $k \geq 1$. Поскольку $s \geq 2$ и выполнено условие (4), верна цепочка равенств и сравнений по модулю $4R$:

$$J_{f_s}(\mathbf{a}) = J_{f_{s_0}^{[2^k]}(\mathbf{a})} = A_{s_0,k}(\mathbf{a}) \equiv E. \quad (16)$$

Пусть вектор $\mathbf{b} \in R^m$ таков, что

$$f_s(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{b}.$$

Если $\mathbf{b} \equiv 0 \pmod{2R}$, то $\tau_{s+1} = \tau_s$, что противоречит вытекающему из (15) равенству $d_s = 2$. Следовательно, $\mathbf{b} \not\equiv 0 \pmod{2R}$. Так как $s \geq 2$, имеем: $s + 2 \leq 2s$. Согласно (16) и [7, формула (4)] получаем цепочку равенств и сравнений по модулю $2^{s+2}R$:

$$f_{s+1}(\mathbf{a}) = f_s^{[2]}(\mathbf{a}) = f_s(\mathbf{a} + 2^s \mathbf{b}) \equiv f_s(\mathbf{a}) + 2^s \mathbf{b} J_{f_s}(\mathbf{a}) \equiv \mathbf{a} + 2^{s+1} \mathbf{b}.$$

Поэтому $\tau_{s+2} > \tau_{s+1}$. Равенство (14) доказано.

В. Если $\rho = n - \nu - s_0 - 1 \geq 1$, то имеет место ситуация 3).

С. Пусть $1 \leq \rho \leq n - \nu - s_0 - 2$. Покажем, что имеет место ситуация 4). По определению величины ρ имеем: $d_{s_0 + \nu + \rho + 1} = 2$. Индукцией по s докажем, что

$$d_s = 2 \quad \forall s \in \{s_0 + \nu + \rho + 1, s_0 + \nu + \rho + 2, \dots, n - 1\}.$$

База индукции ($s = s_0 + \nu + \rho + 1$) очевидна. Пусть

$$s \in \{s_0 + \nu + \rho + 1, s_0 + \nu + \rho + 2, \dots, n - 2\}$$

и верна цепочка равенств $d_{s_0 + \nu + \rho + 1} = d_{s_0 + \nu + \rho + 2} = \dots = d_s = 2$. Докажем, что $d_{s+1} = 2$. Для этого достаточно показать, что $\tau_{s+2} > \tau_{s+1}$. Дальнейшее рассуждение состоит в дословном повторении выкладок из п. А. $\square$

Укажем необходимое и достаточное условие для реализации ситуации 2). При $\nu = n - s_0 - 1$ она, очевидно, реализуется. Далее будем рассматривать случай $\nu \leq n - s_0 - 2$. Введем обозначения, аналогичные тем, которые использовались в [7]:

$$d^2 f_{s_0}(\mathbf{x}, \mathbf{y}) = (\mathbf{y} G_1''(\mathbf{x}) \mathbf{y}^T, \mathbf{y} G_2''(\mathbf{x}) \mathbf{y}^T, \dots, \mathbf{y} G_m''(\mathbf{x}) \mathbf{y}^T),$$

где $\mathbf{y} = (y_1, y_2, \dots, y_m)$ – строка переменных над R , « T » – символ операции транспонирования и

$$f_{s_0}(\mathbf{x}) = (G_1(\mathbf{x}), G_2(\mathbf{x}), \dots, G_m(\mathbf{x})). \quad (17)$$

Как уже отмечалось, условие (4) влечет соотношение

$$d^2 f_{s_0}(\mathbf{a}, \mathbf{b}) \equiv 0 \pmod{2R},$$

выполняющееся для всякого $\mathbf{b} \in R^m$. Поэтому существует $\Delta(\mathbf{a}, \mathbf{b}) \in R^m$ со свойством $d^2 f_{s_0}(\mathbf{a}, \mathbf{b}) = 2\Delta(\mathbf{a}, \mathbf{b})$.

Лемма 4. Во введенных обозначениях для любых векторов $\mathbf{a}, \mathbf{b} \in R^m$ имеет место сравнение

$$f_{s_0}(\mathbf{a} + 2\mathbf{b}) \equiv f_{s_0}(\mathbf{a}) + 2\mathbf{b} A_{s_0}(\mathbf{a}) + 4\Delta(\mathbf{a}, \mathbf{b}) \pmod{8R}.$$

Доказательство. Всякий многочлен $G_i(\mathbf{x})$ из представления (17) есть сумма мономов вида

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

Обозначим через $w'(\mathbf{a})$ столбец $\left(\frac{\partial w}{\partial x_1}(\mathbf{a}), \dots, \frac{\partial w}{\partial x_m}(\mathbf{a})\right)^T$. Согласно [7, формула (4)] верна цепочка сравнений по модулю $8R$:

$$\begin{aligned} w(\mathbf{a} + 2\mathbf{b}) &\equiv w(\mathbf{a}) + 2\mathbf{b}w'(\mathbf{a}) + a \sum_{i=1}^m \binom{\alpha_i}{2} a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}} (a_i^{\alpha_i-2} \cdot 4b_i^2) a_{i+1}^{\alpha_{i+1}} \dots a_m^{\alpha_m} \\ &+ a \sum_{1 \leq i < j \leq m} \alpha_i \alpha_j \cdot a_1^{\alpha_1} \dots a_{i-1}^{\alpha_{i-1}} (a_i^{\alpha_i-1} \cdot 2b_i) a_{i+1}^{\alpha_{i+1}} \dots a_{j-1}^{\alpha_{j-1}} (a_j^{\alpha_j-1} \cdot 2b_j) a_{j+1}^{\alpha_{j+1}} \dots a_m^{\alpha_m} \\ &= w(\mathbf{a}) + 2\mathbf{b}w'(\mathbf{a}) + \sum_{i=1}^m \frac{\partial^2 w}{\partial x_i^2}(\mathbf{a}) \cdot 2b_i^2 + \sum_{1 \leq i \neq j \leq m} \frac{\partial^2 w}{\partial x_i \partial x_j}(\mathbf{a}) \cdot 2b_i b_j \\ &= w(\mathbf{a}) + 2\mathbf{b}w'(\mathbf{a}) + 2\mathbf{b}w''(\mathbf{a})\mathbf{b}^T. \end{aligned}$$

Распространив полученную формулу по линейности, имеем:

$$G_i(\mathbf{a} + 2\mathbf{b}) \equiv G_i(\mathbf{a}) + 2\mathbf{b}G'_i(\mathbf{a}) + 2\mathbf{b}G''_i(\mathbf{a})\mathbf{b}^T \pmod{8R} \quad \forall i \in \{1, 2, \dots, m\}.$$

Учитывая, что $d^2 f_{s_0}(\mathbf{a}, \mathbf{b}) = 2\Delta(\mathbf{a}, \mathbf{b})$, получаем требуемое соотношение. $\square$

Верно следующее утверждение.

Утверждение 5. Пусть выполнено (4), $\nu \leq n - s_0 - 2$, матрица $C(\mathbf{a}) \in R_{m,m}$ удовлетворяет равенству $A_{s_0}(\mathbf{a}) = E + 2C(\mathbf{a})$ и вектор $\mathbf{b} \in R^m$ удовлетворяет равенству $f_{s_0}(\mathbf{a}) = \mathbf{a} + 2^{s_0+\nu}\mathbf{b}$. Тогда:

- 1) если $s_0 + \nu = 1$, то ситуация 2) из утверждения 3 реализуется тогда и только тогда, когда $\mathbf{b}(E + C(\mathbf{a})) \not\equiv \Delta(\mathbf{a}, \mathbf{b}) \pmod{2R}$,
- 2) если $s_0 + \nu \geq 2$, то ситуация 2) из утверждения 3 реализуется тогда и только тогда, когда $\mathbf{b}(E + C(\mathbf{a})) \not\equiv 0 \pmod{2R}$.

Доказательство. 1) Пусть $s_0 + \nu = 1$, т. е. $s_0 = 1$ и $\nu = 0$. Тогда $d_1 = 2$. По определению величины s_0 и в силу (16) имеем:

$$A_1(\mathbf{a}) \equiv E \pmod{2R} \quad \text{и} \quad A_s(\mathbf{a}) \equiv E \pmod{4R} \quad \forall s \geq 2. \quad (18)$$

Согласно введенным обозначениям

$$A_1(\mathbf{a}) = E + 2C(\mathbf{a}) \quad \text{и} \quad f_1(\mathbf{a}) = \mathbf{a} + 2\mathbf{b}.$$

Поскольку $d_1 > 1$, имеем: $\mathbf{b} \notin 2R^m$. Достаточно доказать следующую эквивалентность:

$$(d_1 = d_2 = \dots = d_{n-1} = 2) \Leftrightarrow (\mathbf{b}(E + C(\mathbf{a})) \not\equiv \Delta(\mathbf{a}, \mathbf{b}) \pmod{2R}).$$

Импликацию « $\Rightarrow$ » докажем методом «от противного». Пусть

$$\mathbf{b}(E + C(\mathbf{a})) \equiv \Delta(\mathbf{a}, \mathbf{b}) \pmod{2R}.$$

В силу леммы 4 имеем цепочку равенств и сравнений по модулю $8R$:

$$\begin{aligned} f_2(\mathbf{a}) &= f_1^{[2]}(\mathbf{a}) = f_1(\mathbf{a} + 2\mathbf{b}) \equiv f_1(\mathbf{a}) + 2\mathbf{b}A_1(\mathbf{a}) + 4\Delta(\mathbf{a}, \mathbf{b}) \\ &= \mathbf{a} + 4[\mathbf{b}(E + C(\mathbf{a})) + \Delta(\mathbf{a}, \mathbf{b})]. \end{aligned} \quad (19)$$

Значит, $f_2(\mathbf{a}) \equiv \mathbf{a} \pmod{8R}$, и $d_2 = 1$. Противоречие.

Докажем импликацию « $\Leftarrow$ ». Пусть

$$\mathbf{b}(E + C(\mathbf{a})) \not\equiv \Delta(\mathbf{a}, \mathbf{b}) \pmod{2R}.$$

Согласно (19) отсюда следует, что $f_2(\mathbf{a}) \not\equiv \mathbf{a} \pmod{8R}$, т. е. $d_2 = 2$. Докажем теперь, что

$$\forall s \in \{2, 3, \dots, n-2\}: \quad (d_s = 2) \Rightarrow (d_{s+1} = 2). \quad (20)$$

Пусть $d_s = 2$. Тогда существует такой вектор $\mathbf{c} \in R^m \setminus 2R^m$, что $f_s(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{c}$. В силу неравенства $s+2 \leq 2s$ и согласно [7, формула (4)] имеем цепочку равенств и сравнений по модулю $2^{s+2}R$:

$$f_{s+1}(\mathbf{a}) = f_s^{[2]}(\mathbf{a}) = f_s(\mathbf{a} + 2^s \mathbf{c}) \equiv f_s(\mathbf{a}) + 2^s \mathbf{c}A_s(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{c}(E + A_s(\mathbf{a})).$$

Но тогда ввиду (18) верно соотношение

$$f_{s+1}(\mathbf{a}) \equiv \mathbf{a} + 2^{s+1} \mathbf{c} \pmod{2^{s+2}R},$$

откуда $d_{s+1} = 2$. Импликация (20) доказана, и п. 1 утверждения доказан.

2) Пусть $s_0 + \nu \in \{2, 3, \dots, n-2\}$. Тогда $d_{s_0+\nu} = 2$. Достаточно доказать, что имеет место эквивалентность

$$(d_{s_0+\nu} = d_{s_0+\nu+1} = \dots = d_{n-1} = 2) \Leftrightarrow (\mathbf{b}(E + C(\mathbf{a})) \not\equiv 0 \pmod{2R}).$$

Импликацию « $\Rightarrow$ » докажем методом «от противного». Пусть

$$\mathbf{b}(E + C(\mathbf{a})) \equiv 0 \pmod{2R}. \quad (21)$$

Поскольку $\tau_{s_0} = \tau_{s_0+\nu}$, верны равенства

$$\forall i \geq 0: \quad f_{s_0}(F^{[i]}(\mathbf{a})) = f_{s_0+\nu}(F^{[i]}(\mathbf{a})).$$

Так как $s_0 + \nu + 2 \leq 2(s_0 + \nu)$, согласно [7, формула (4)] верна следующая цепочка равенств и сравнений по модулю $2^{s_0 + \nu + 2}R$:

$$\begin{aligned} f_{s_0 + \nu + 1}(\mathbf{a}) &= f_{s_0 + \nu}^{[2]}(\mathbf{a}) = f_{s_0}(f_{s_0}(\mathbf{a})) = f_{s_0}(\mathbf{a} + 2^{s_0 + \nu}\mathbf{b}) \equiv f_{s_0}(\mathbf{a}) + 2^{s_0 + \nu}\mathbf{b}A_{s_0}(\mathbf{a}) \\ &= \mathbf{a} + 2^{s_0 + \nu}\mathbf{b}(E + A_{s_0}(\mathbf{a})) = \mathbf{a} + 2^{s_0 + \nu + 1}\mathbf{b}(E + C(\mathbf{a})). \end{aligned} \quad (22)$$

Отсюда и из (21) следует, что

$$f_{s_0 + \nu + 1}(\mathbf{a}) \equiv \mathbf{a} \pmod{2^{s_0 + \nu + 2}R}.$$

Поэтому $d_{s_0 + \nu + 1} = 1$. Противоречие.

Докажем импликацию « $\Leftarrow$ ». Пусть условие (21) не выполнено. Согласно (22) имеем: $d_{s_0 + \nu + 1} = 2$. Докажем, что

$$\forall s \in \{s_0 + \nu + 1, s_0 + \nu + 2, \dots, n - 2\}: \quad (d_s = 2) \Rightarrow (d_{s+1} = 2). \quad (23)$$

Пусть $d_s = 2$. Ввиду (9) верно соотношение $\tau_s \mid \tau_{s_0} \cdot 2^{s - s_0}$. В то же время

$$2\tau_{s_0} = d_{s_0 + \nu}\tau_{s_0 + \nu} = \tau_{s_0 + \nu + 1} \mid \tau_s.$$

Поэтому $\tau_s = 2^k \cdot \tau_{s_0}$, где $k \geq 1$. Тогда справедлива цепочка соотношений (16), и $A_s(\mathbf{a}) \equiv E \pmod{4R}$. Существует такой вектор $\mathbf{c} \in R^m \setminus 2R^m$, что $f_s(\mathbf{a}) = \mathbf{a} + 2^s\mathbf{c}$. В силу неравенства $s + 2 \leq 2s$ и согласно [7, формула (4)] имеем цепочку равенств и сравнений по модулю $2^{s+2}R$:

$$\begin{aligned} f_{s+1}(\mathbf{a}) &= f_s^{[2]}(\mathbf{a}) = f_s(\mathbf{a} + 2^s\mathbf{c}) \\ &\equiv f_s(\mathbf{a}) + 2^s\mathbf{c}A_s(\mathbf{a}) = \mathbf{a} + 2^s\mathbf{c}(E + A_s(\mathbf{a})) \equiv \mathbf{a} + 2^{s+1}\mathbf{c}. \end{aligned}$$

Следовательно, $d_{s+1} = 2$. Импликация (23) доказана. $\square$

Утверждение 5 является многомерным обобщением теоремы 5 из [5].

Если $s_0 = 1$, то отрезок (10) совпадает с отрезком (13), и профиль цикла C описан. Далее в этом разделе $s_0 \geq 2$.

Рассмотрим отрезок (12). Следуя [7], введем обозначения: $f = f_1$, $J = J_f(\mathbf{a})$, $\chi(x)$ – характеристический многочлен J , σ – мультипликативный порядок $\bar{J}$. Будем рассматривать такие преобразования F вида (1) и такие векторы $\mathbf{a} \in R^m$, для которых имеет место (4) и многочлен $\bar{\chi}(x)$ неприводим над $\bar{R}$. Вопрос о существовании пар $(F, \mathbf{a})$, обладающих указанными свойствами, будет решаться в разделе 3.

Утверждение 6. Пусть $s_0 \geq 2$, многочлен $\bar{\chi}(x)$ неприводим над $\bar{R}$, и для некоторого $i \in \{2, 3, \dots, n\}$ выполнена цепочка равенств и неравенств

$$\tau_1 = \tau_2 = \dots = \tau_{i-1} < \tau_i.$$

Тогда $d_{i-1} = \sigma$ и $i = s_0$. В частности, для отрезка (12) имеет место одна из следующих ситуаций:

- а) $d_1 = d_2 = \dots = d_{s_0-1} = 1$,
- б) $d_1 = d_2 = \dots = d_{s_0-2} = 1, d_{s_0-1} = \sigma$.

Доказательство. Индукцией по $j \geq 1$ покажем, что при условии

$$f(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{b}, \quad \bar{\mathbf{b}} \neq \bar{\mathbf{0}}, \quad s \geq 1, \quad (24)$$

для всякого j верно соотношение

$$f^{[j]}(\mathbf{a}) \equiv \mathbf{a} + 2^s \mathbf{b} \sum_{k=0}^{j-1} J^k \pmod{2^{s+1}R}. \quad (25)$$

Осуществим индуктивный переход от j к $j+1$. Поскольку $2s \geq s+1$, в силу [7, формула (4)] и по предположению индукции имеем цепочку равенств и сравнений по модулю $2^{s+1}R$:

$$f^{[j+1]}(\mathbf{a}) = f(f^{[j]}(\mathbf{a})) \equiv f(\mathbf{a} + 2^s \mathbf{b} \sum_{k=0}^{j-1} J^k) \equiv f(\mathbf{a}) + 2^s \mathbf{b} \sum_{k=1}^j J^k = \mathbf{a} + 2^s \mathbf{b} \sum_{k=0}^j J^k.$$

Так как $\tau_1 = \tau_2 = \dots = \tau_{i-1}$, то $f = f_2 = \dots = f_{i-1}$. Тогда

$$\begin{aligned} d_{i-1} &= \min\{k \geq 1 \mid f_{i-1}^{[k]}(\mathbf{a}) \equiv \mathbf{a} \pmod{2^i R}\} \\ &= \min\{k \geq 1 \mid f^{[k]}(\mathbf{a}) \equiv \mathbf{a} \pmod{2^i R}\}. \end{aligned}$$

В формуле (24) значение s равно $i-1$. Сравнение (25) переписывается в виде

$$f^{[j]}(\mathbf{a}) \equiv \mathbf{a} + 2^{i-1} \mathbf{b} \sum_{k=0}^{j-1} J^k \pmod{2^i R}. \quad (26)$$

Многочлен $\bar{\chi}(x)$ неприводим над $\bar{R}$. Поэтому при $k \in \{1, 2, \dots, \sigma-1\}$ матрица $\bar{J}^k$ не имеет собственного значения $\bar{e}$, и матрица $J^k - E$ обратима. Так как $s_0 \geq 2$, верно неравенство $\sigma \geq 3$. Следовательно, (26) можно записать так:

$$f^{[j]}(\mathbf{a}) \equiv \mathbf{a} + 2^{i-1} \mathbf{b} (J - E)^{-1} (J^j - E) \pmod{2^i R}.$$

Отсюда $d_{i-1} = \sigma$. Тогда $\tau_i = \sigma \cdot \tau_{i-1} = \sigma \cdot \tau_1$. По формуле (2) имеем цепочку равенств и сравнений по модулю $2R$:

$$J_{f_i}(\mathbf{a}) = \prod_{j=0}^{\tau_i-1} J_F(F^{[j]}(\mathbf{a})) = \prod_{k=0}^{\sigma-1} \prod_{j=k\tau_1}^{(k+1)\tau_1-1} J_F(F^{[j]}(\mathbf{a}))$$

$$\equiv \prod_{k=0}^{\sigma-1} \prod_{j=0}^{\tau_1-1} J_F(F^{[j]}(\mathbf{a})) = J^\sigma \equiv E.$$

Следовательно, $i \geq s_0$. Если $s_0 \leq i - 1$, то $J = J_{f_{i-1}}(\mathbf{a}) \equiv E \pmod{2R}$. Это невозможно, поскольку $\sigma \geq 3$. Итак, $i = s_0$. Второе доказываемое утверждение с очевидностью вытекает из первого утверждения. $\square$

Утверждение 6 является многомерным обобщением леммы 8 из [5].

Согласно [7, утверждение 1] для любой пары $(F, \mathbf{a})$ со свойством $\chi(\bar{e}) \neq \bar{0}$ существует единственный такой вектор $\mathbf{a}^* \in R^m$, что

$$\bar{\mathbf{a}} = \bar{\mathbf{a}}^* \quad \text{и} \quad \tau(F, n, \mathbf{a}^*) = \tau(F, 1, \mathbf{a}^*).$$

Напомним, что $A_s(\mathbf{a}) = J_{f_s}(\mathbf{a})$, $s = 1, 2, \dots, n$. Следующая теорема объединяет утверждения 3, 5 и 6.

Теорема 7. Пусть $p = 2$, $\mathbf{a} \in R^m$, $\bar{\chi}(\bar{e}) \neq \bar{0}$ и выполняется условие (4). Тогда верны следующие утверждения.

I. Если $s_0 = 1$, то последовательность (10) имеет один из следующих видов:

- a) $(1, 1, \dots, 1)$,
- b) $(1, 1, \dots, 1, 2, 2, \dots, 2)$,
- c) $(1, 1, \dots, 1, 2, 1, 1, \dots, 1)$,
- d) $(1, 1, \dots, 1, 2, 1, 1, \dots, 1, 2, 2, \dots, 2)$.

Ситуация I.a) реализуется тогда и только тогда, когда $\mathbf{a} = \mathbf{a}^*$.

II. Пусть $s_0 = 1$, ν – длина первой серии из единиц в последовательности (10), $\nu \leq n - 3$, $A_1(\mathbf{a}) = E + 2C(\mathbf{a})$, $f(\mathbf{a}) = \mathbf{a} + 2^{\nu+1}\mathbf{b}$, вектор $\Delta(\mathbf{a}, \mathbf{b})$ определен равенством

$$d^2 f(\mathbf{a}, \mathbf{b}) = 2\Delta(\mathbf{a}, \mathbf{b}).$$

Справедливы следующие утверждения.

a) Если $\nu = 0$, то ситуация I.b) реализуется тогда и только тогда, когда

$$\mathbf{b}(E + C(\mathbf{a})) \not\equiv \Delta(\mathbf{a}, \mathbf{b}) \pmod{2R}.$$

b) Если $\nu > 0$, то ситуация I.b) реализуется тогда и только тогда, когда

$$\mathbf{b}(E + C(\mathbf{a})) \not\equiv 0 \pmod{2R}.$$

III. Если $s_0 > 1$, многочлен $\bar{\chi}(x)$ неприводим над полем $\bar{R}$ и σ – мультипликативный порядок любого корня многочлена $\bar{\chi}(x)$ в его поле разложения, то последовательность (10) имеет один из следующих видов:

- a) $(1, 1, \dots, 1)$,
- b) $(1, 1, \dots, 1, \sigma)$,
- c) $(1, 1, \dots, 1, \sigma, 1, 1, \dots, 1)$,
- d) $(1, 1, \dots, 1, \sigma, 1, 1, \dots, 1, 2, 2, \dots, 2)$,
- e) $(1, 1, \dots, 1, \sigma, 1, 1, \dots, 1, 2, 1, 1, \dots, 1)$,
- f) $(1, 1, \dots, 1, \sigma, 1, 1, \dots, 1, 2, 1, 1, \dots, 1, 2, 2, \dots, 2)$.

Ситуация III.a) реализуется тогда и только тогда, когда $\mathbf{a} = \mathbf{a}^*$.

IV. Пусть $s_0 > 1$, многочлен $\bar{\chi}(x)$ неприводим над $\bar{R}$, ν – длина второй серии из единиц в последовательности (10), $\nu \leq n - s_0 - 2$, $A_{s_0}(\mathbf{a}) = E + 2C(\mathbf{a})$, $f_{s_0}(\mathbf{a}) = \mathbf{a} + 2^{s_0+\nu}\mathbf{b}$. Ситуация III.d) реализуется тогда и только тогда, когда $\mathbf{b}(E + C(\mathbf{a})) \not\equiv 0 \pmod{2R}$.

Теорема 7 обобщает на многомерный случай теоремы 4, 5 и 6 из [5], а также утверждение 1 из [6]. В следующем разделе будет построено семейство таких нелинейных подстановок F , что для всякого $\mathbf{a} \in R^m$ имеет место (4) и многочлен $\bar{\chi}(x)$ неприводим над $\bar{R}$.

3. Алгоритм построения МДЦ-подстановок в случае $p = 2$

Всюду в этом разделе $q > p = 2$ и $n \geq 4$, т. е. кольцо Галуа $R = GR(2^{tn}, 2^n)$ отлично от кольца вычетов и имеет характеристику $2^n \geq 16$. Пусть $L_m(F)$ – максимум длин циклов m -мерной полиномиальной подстановки F , и

$$L_m(R) = \max_F L_m(F),$$

где максимум берется по всем m -мерным полиномиальным подстановкам F кольца R . Согласно [7, теорема 2] верно равенство

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

где $q = |\bar{R}| = 2^t$. Подстановки F , обладающие циклом длины $L_m(R)$, названы в [7] подстановками с максимальной длиной цикла

(МДЦ-подстановками). В этом разделе предложен алгоритм построения одного класса МДЦ-подстановок.

Для построения МДЦ-подстановок используется следующая лемма.

Лемма 8. Пусть $R = GR(2^{tn}, 2^n)$, $t \geq 2$, $m \geq 1$, F – m -мерная полиномиальная подстановка кольца R со свойством (4). Если $\mathbf{a}, \mathbf{b} \in R^m$ и вектор $\Delta_F(\mathbf{a}, \mathbf{b})$ определен равенством $d^2 F(\mathbf{a}, \mathbf{b}) = 2\Delta_F(\mathbf{a}, \mathbf{b})$, то

$$F(\mathbf{a} + 2^s \mathbf{b}) \equiv F(\mathbf{a}) + 2^s \mathbf{b} J_F(\mathbf{a}) + 2^{2s} \Delta_F(\mathbf{a}, \mathbf{b}) \pmod{2^{3s} R} \quad \forall s \geq 1.$$

Доказательство. Аналогично доказательству леммы 4 проверяется, что для любого монома

$$w(\mathbf{x}) = ax_1^{\alpha_1} x_2^{\alpha_2} \dots x_m^{\alpha_m}$$

выполняется сравнение

$$w(\mathbf{a} + 2^s \mathbf{b}) \equiv w(\mathbf{a}) + 2^s \mathbf{b} w'(\mathbf{a}) + 2^{2s-1} \mathbf{b} w''(\mathbf{a}) \mathbf{b}^T \pmod{2^{3s} R}.$$

Распространив эту формулу по линейности, получим:

$$F(\mathbf{a} + 2^s \mathbf{b}) \equiv F(\mathbf{a}) + 2^s \mathbf{b} J_F(\mathbf{a}) + 2^{2s-1} d^2 F(\mathbf{a}, \mathbf{b}) \pmod{2^{3s} R}.$$

Отсюда и из равенства $d^2 F(\mathbf{a}, \mathbf{b}) = 2\Delta_F(\mathbf{a}, \mathbf{b})$ вытекает требуемый результат. $\square$

Следуя [7], назовем полиномиальную подстановку F *подстановкой с длинными циклами* (ДЦ-подстановкой), если существует такой вектор $\mathbf{a} \in R^m$, что

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

Согласно [7, теорема 4] подстановка F является ДЦ-подстановкой тогда и только тогда, когда подстановка $\bar{F}$ – полноцикловая и для любого вектора $\mathbf{c} \in R^m$ характеристический многочлен $\bar{\chi}(x)$ матрицы $\bar{J}(\mathbf{c})$ есть многочлен максимального периода. Всякая МДЦ-подстановка, очевидно, является ДЦ-подстановкой.

ДЦ- и МДЦ-подстановки строятся в классе полиномиальных подстановок F следующего вида:

$$F(\mathbf{x}) = G(\mathbf{x}^q) + (\mathbf{x} - \mathbf{x}^q)(\Phi(\mathbf{x}^4) + 2\Psi(\mathbf{x}^2)), \quad (27)$$

где полиномиальная подстановка G такова, что $\bar{G}$ – полноцикловая подстановка, $\mathbf{x}^k = (x_1^k, x_2^k, \dots, x_m^k)$, $k \in \mathbb{N}$, $\Phi(\mathbf{x})$ и $\Psi(\mathbf{x})$ – матрицы размеров $m \times m$ над кольцом $R[\mathbf{x}]$. Подстановку F вида (27) обозначим через $F[G, \Phi, \Psi]$.

Лемма 9. Для любого вектора $\mathbf{a} \in R^m$, всякого $s \geq 1$ и любых матриц

$$\Phi(\mathbf{x}), \Phi_1(\mathbf{x}), \Phi_2(\mathbf{x}), \Psi_1(\mathbf{x}), \Psi_2(\mathbf{x}) \in (R[\mathbf{x}])_{m,m}$$

справедливы следующие утверждения:

1. Если $\mathcal{F}_1 = \mathcal{F}_1[G, \Phi_1, \Psi_1]$ и $\mathcal{F}_2 = \mathcal{F}_2[G, \Phi_2, \Psi_2]$, то

$$\mathcal{F}_1^{[s]}(\mathbf{a}) \equiv \mathcal{F}_2^{[s]}(\mathbf{a}) \pmod{2R},$$

2. Если $\mathcal{F}_1 = \mathcal{F}_1[G, \Phi, \Psi_1]$ и $\mathcal{F}_2 = \mathcal{F}_2[G, \Phi, \Psi_2]$, то

$$\mathcal{F}_1^{[s]}(\mathbf{a}) \equiv \mathcal{F}_2^{[s]}(\mathbf{a}) \pmod{4R}.$$

Доказательство. При $s = 1$ утверждения леммы вытекают из очевидных соотношений, выполняющихся для всякой подстановки $\mathcal{F} = \mathcal{F}[G, \Phi, \Psi]$:

$$\mathcal{F}(\mathbf{a}) \equiv G(\mathbf{a}) \pmod{2R}, \quad \mathcal{F}(\mathbf{a}) \equiv G(\mathbf{a}^q) + (\mathbf{a} - \mathbf{a}^q)\Phi(\mathbf{a}^4) \pmod{4R}.$$

Осуществим индуктивный переход от s к $s + 1$. Полиномиальное преобразование *консервативно*, т. е. сохраняет все конгруэнции кольца R . Отсюда, из базы и предположения индукции следуют цепочки равенств и сравнений (в случае 1 – по модулю $2R$, в случае 2 – по модулю $4R$):

$$\mathcal{F}_1^{[s+1]}(\mathbf{a}) = \mathcal{F}_1(\mathcal{F}_1^{[s]}(\mathbf{a})) \equiv \mathcal{F}_1(\mathcal{F}_2^{[s]}(\mathbf{a})) \equiv \mathcal{F}_2(\mathcal{F}_2^{[s]}(\mathbf{a})) = \mathcal{F}_2^{[s+1]}(\mathbf{a}).$$

□

Напомним (см., например, [8]), что *нормой* $\|a\|$ элемента $a \in R$ называется максимальное такое значение $k \in \{0, 1, \dots, n\}$, что $a \in 2^k R$, а *нормой вектора* $\mathbf{a} \in R^m$ называется минимум норм его компонент. Следующий результат – центральный в этом разделе.

Утверждение 10. Пусть $q > p = 2$, $n \geq 4$.

- 1) Если подстановка F имеет вид (27), $\mathbf{a} \in R^m$, $f = f_1$, то для любых $\mathbf{b} \in R^m$ и $j \geq 1$ верно неравенство $\|d^2 F^{[j]}(\mathbf{a}, \mathbf{b})\| \geq 2$. В частности, подстановка F обладает свойством (4) и выполняется сравнение

$$f(\mathbf{a} + 2\mathbf{b}) \equiv f(\mathbf{a}) + 2\mathbf{b}J_f(\mathbf{a}) \pmod{8R}. \quad (28)$$

- 2) Для любого полноциклового полиномиального преобразования G и всякого набора матриц $M_0, M_1, \dots, M_{q^m-1} \in R_{m,m}$ существуют такие матрицы

$$\Phi(\mathbf{x}), \Psi(\mathbf{x}) \in R[\mathbf{x}]_{m,m},$$

что для полиномиальной подстановки $F = F[G, \Phi, \Psi]$ выполнены соотношения

$$J_F(F^{[s]}(\mathbf{a})) \equiv M_s \pmod{4R} \quad \forall s \geq 0. \quad (29)$$

Доказательство. 1) Индукцией по $j \geq 1$ докажем, что

$$\left(F_i^{[j]}\right)''(\mathbf{x}) \in (4R[\mathbf{x}])_{m,m} \quad \forall i \in \{1, 2, \dots, m\}. \quad (30)$$

База индукции: $j = 1$. Если $\varphi_{s,i}(\mathbf{x})$ – элемент, стоящий на пересечении s -й строки и i -го столбца матрицы $\Phi(\mathbf{x})$, а $\psi_{s,i}(\mathbf{x})$ – элемент, стоящий на пересечении s -й строки и i -го столбца матрицы $\Psi(\mathbf{x})$, то согласно (27) для всякого $i \in \{1, 2, \dots, m\}$

$$F_i(\mathbf{x}) = G_i(\mathbf{x}^q) + \sum_{s=1}^m (x_s - x_s^q)(\varphi_{s,i}(\mathbf{x}^4) + 2\psi_{s,i}(\mathbf{x}^2)).$$

Пусть $k \in \{1, 2, \dots, m\}$. Справедлива следующая цепочка равенств:

$$\begin{aligned} \frac{\partial F_i}{\partial x_k}(\mathbf{x}) &= \sum_{s=1}^m \frac{\partial G_i}{\partial x_s}(\mathbf{x}^q) \frac{\partial x_s^q}{\partial x_k} + \sum_{s=1}^m \frac{\partial (x_s - x_s^q)}{\partial x_k} (\varphi_{s,i}(\mathbf{x}^4) + 2\psi_{s,i}(\mathbf{x}^2)) \\ &\quad + \sum_{s=1}^m (x_s - x_s^q) \frac{\partial (\varphi_{s,i}(\mathbf{x}^4) + 2\psi_{s,i}(\mathbf{x}^2))}{\partial x_k} \\ &= q \cdot \frac{\partial G_i}{\partial x_s}(\mathbf{x}^q) x_k^{q-1} + (1 - qx_k^{q-1})(\varphi_{k,i}(\mathbf{x}^4) + 2\psi_{k,i}(\mathbf{x}^2)) \\ &\quad + \sum_{s=1}^m (x_s - x_s^q) \left[\sum_{u=1}^m \frac{\partial \varphi_{s,i}}{\partial x_u}(\mathbf{x}^4) \frac{\partial x_u^4}{\partial x_k} + 2 \sum_{v=1}^m \frac{\partial \psi_{s,i}}{\partial x_v}(\mathbf{x}^2) \frac{\partial x_v^2}{\partial x_k} \right]. \end{aligned}$$

Напомним, что $4 \mid q$. Сгруппировав мономы, у которых коэффициенты принадлежат идеалу $4R$, получим, что существует многочлен $H_{k,i}(\mathbf{x}) \in R[\mathbf{x}]$ со свойством

$$\frac{\partial F_i}{\partial x_k}(\mathbf{x}) = \varphi_{k,i}(\mathbf{x}^4) + 2\psi_{k,i}(\mathbf{x}^2) + 4H_{k,i}(\mathbf{x}). \quad (31)$$

Пусть $l \in \{1, 2, \dots, m\}$. Дифференцируя (31) по x_l , получаем:

$$\begin{aligned} \frac{\partial^2 F_i}{\partial x_l \partial x_k}(\mathbf{z}) &= 4 \frac{\partial H_{k,i}}{\partial x_l}(\mathbf{x}) + \sum_{u=1}^m \frac{\partial \varphi_{k,i}}{\partial x_u}(\mathbf{x}^4) \frac{\partial x_u^4}{\partial x_l} + 2 \sum_{v=1}^m \frac{\partial \psi_{k,i}}{\partial x_v}(\mathbf{x}^2) \frac{\partial x_v^2}{\partial x_l} \\ &= 4 \frac{\partial H_{k,i}}{\partial x_l}(\mathbf{x}) + 4 \frac{\partial \varphi_{k,i}}{\partial x_l}(\mathbf{x}^4) x_l^3 + 4 \frac{\partial \psi_{k,i}}{\partial x_l}(\mathbf{x}^2) x_l. \end{aligned}$$

Отсюда $F_i''(\mathbf{x}) \in (4R[\mathbf{x}])_{m,m}$ для всякого $i \in \{1, 2, \dots, m\}$.

Осуществим индуктивный переход от j к $j+1$. Пусть $k \in \{1, 2, \dots, m\}$. Имеем:

$$\frac{\partial F_i^{[j+1]}}{\partial x_k}(\mathbf{x}) = \frac{\partial F_i(F^{[j]})}{\partial x_k}(\mathbf{x}) = \sum_{s=1}^m \frac{\partial F_i}{\partial x_s}(F^{[j]}(\mathbf{x})) \cdot \frac{\partial F_s^{[j]}}{\partial x_k}(\mathbf{x}).$$

Всякой паре $(i, s) \in \{1, 2, \dots, m\}^2$ сопоставим многочлены

$$\alpha_{s,i}(\mathbf{x}) = \frac{\partial F_i}{\partial x_s}(\mathbf{x}) \quad \text{и} \quad \beta_{k,s}^{[j]}(\mathbf{x}) = \frac{\partial F_s^{[j]}}{\partial x_k}(\mathbf{x}).$$

Тогда

$$\frac{\partial F_i^{[j+1]}}{\partial x_k}(\mathbf{x}) = \sum_{s=1}^m \alpha_{s,i}(F^{[j]}(\mathbf{x})) \cdot \beta_{k,s}^{[j]}(\mathbf{x}). \quad (32)$$

Пусть $r \in \{1, 2, \dots, m\}$. Согласно базе индукции и предположению индукции верны включения

$$\frac{\partial \alpha_{s,i}}{\partial x_r}(\mathbf{x}) \in 4R[\mathbf{x}] \quad \text{и} \quad \frac{\partial \beta_{k,s}^{[j]}}{\partial x_r}(\mathbf{x}) \in 4R[\mathbf{x}]. \quad (33)$$

Для всякого $l \in \{1, 2, \dots, m\}$ имеет место цепочка равенств

$$\begin{aligned} &\frac{\partial}{\partial x_l} \left(\alpha_{s,i}(F^{[j]}(\mathbf{x})) \cdot \beta_{k,s}^{[j]}(\mathbf{x}) \right) \\ &= \left(\sum_{r=1}^m \frac{\partial \alpha_{s,i}}{\partial x_r}(F^{[j]}(\mathbf{x})) \frac{\partial F_r^{[j]}}{\partial x_l}(\mathbf{x}) \right) \cdot \beta_{k,s}^{[j]}(\mathbf{x}) + \alpha_{s,i}(F^{[j]}(\mathbf{x})) \cdot \sum_{r=1}^m \frac{\partial \beta_{k,s}^{[j]}}{\partial x_r}(\mathbf{x}) \frac{\partial F_r^{[j]}}{\partial x_l}(\mathbf{x}). \end{aligned}$$

Отсюда, а также из (32) и (33) следует, что

$$\frac{\partial^2 F_i^{[j+1]}}{\partial x_l \partial x_k}(\mathbf{x}) \in 4R[\mathbf{x}].$$

Таким образом,

$$\left(F_i^{[j+1]}\right)''(\mathbf{x}) \in (4R[\mathbf{x}])_{m,m}.$$

Индуктивный переход завершен, и включение (30) доказано.

Из (30) следует, что для любого $j \geq 1$ и любых $\mathbf{a}, \mathbf{b} \in R^m$ выполняется неравенство

$$\|d^2 F^{[j]}(\mathbf{a}, \mathbf{b})\| \geq 2. \quad (34)$$

По лемме 8

$$f(\mathbf{a} + 2\mathbf{b}) \equiv f(\mathbf{a}) + 2\mathbf{b}J_f(\mathbf{a}) + 2d^2 f(\mathbf{a}, \mathbf{b}) \pmod{8R}.$$

Поскольку $f = F^{[\tau_1]}$, согласно (34) имеем: $\|d^2 f(\mathbf{a}, \mathbf{b})\| \geq 2$. Отсюда следует (28).

2) Пусть последовательность векторов

$$u_0, u_1, \dots, u_s, \dots$$

определена равенствами

$$u_0 = \mathbf{a}, \quad \forall s \geq 1: \quad u_s = G^{[s]}(u_0).$$

Отображения $x \mapsto x^2$ и $x \mapsto x^4$ суть автоморфизмы поля $\bar{R} = GF(2^t)$ (первое из них – автоморфизм Фробениуса, второе – квадрат автоморфизма Фробениуса). Так как преобразование $\bar{G}$ – полноцикловое, то

$$\{\bar{u}_0^2, \bar{u}_1^2, \dots, \bar{u}_{q^m-1}^2\} = \{\bar{u}_0^4, \bar{u}_1^4, \dots, \bar{u}_{q^m-1}^4\} = \bar{R}^m. \quad (35)$$

Для всякого $s \in \{0, 1, \dots, q^m - 1\}$ представим матрицу M_s в виде разложения Тейхмюллера по модулю $4R$:

$$M_s \equiv M_s^{(0)} + 2M_s^{(1)} \pmod{4R}, \quad M_s^{(0)}, M_s^{(1)} \in \Gamma(R)_{m,m}.$$

Пусть $i, j \in \{1, 2, \dots, m\}$. В силу (35) существует такой многочлен $\varphi_{i,j}(\mathbf{x}) \in R[\mathbf{x}]$, что

$$\varphi_{i,j}(u_s^4) \equiv m_{s,i,j}^{(0)} \pmod{2R} \quad \forall s \geq 0, \quad (36)$$

где $m_{s,i,j}^{(0)}$ – элемент, стоящий в i -й строке и j -м столбце матрицы $M_s^{(0)}$. Тогда

$$\varphi_{i,j}(u_s^4) \equiv m_{s,i,j}^{(0)} \pmod{2R} \quad \forall s \geq 0,$$

т. е.

$$\Phi(u_s^4) \equiv M_s^{(0)} \pmod{2R} \quad \forall s \geq 0. \quad (37)$$

Рассмотрим подстановку $H = H[G, \Phi, 0]$, а также последовательность векторов $w_0, w_1, \dots$, определенную равенствами

$$w_0 = u_0 = \mathbf{a}, \quad w_s = H^{[s]}(w_0) \quad \forall s \geq 1.$$

Согласно п. 1) леммы 9 имеем: $\bar{u}_s = \bar{w}_s$ при всех $s \geq 0$. Поэтому (37) эквивалентно соотношению

$$\Phi(w_s^4) \equiv M_s^{(0)} \pmod{2R} \quad \forall s \geq 0. \quad (38)$$

Пусть $i, j \in \{1, 2, \dots, m\}$, $s \geq 0$. Согласно (38) элемент $\varphi_{i,j}(w_s^4)$ следующим образом представляется разложением Тейхмюллера по модулю $4R$:

$$\varphi_{i,j}(w_s^4) \equiv m_{s,i,j}^{(0)} + 2\gamma_1[\varphi_{i,j}(w_s^4)] \pmod{4R}.$$

В матричной форме это соотношение имеет вид

$$\Phi(w_s^4) \equiv M_s^{(0)} + 2\gamma_1[\Phi(w_s^4)] \pmod{4R} \quad \forall s \geq 0. \quad (39)$$

В силу (35) существует такой многочлен $\psi_{i,j}(\mathbf{x}) \in R[\mathbf{x}]$, что

$$2\psi_{i,j}(w_s^2) \equiv 2m_{s,i,j}^{(1)} - 2\gamma_1[\varphi_{i,j}(w_s^4)] \pmod{4R} \quad \forall s \geq 0,$$

где $m_{s,i,j}^{(1)}$ – элемент, стоящий в i -й строке и j -м столбце матрицы $M_s^{(1)}$. Иными словами,

$$\forall s \geq 0: \quad 2\Psi(w_s^2) \equiv 2M_s^{(1)} - 2\gamma_1[\Phi(w_s^4)] \pmod{4R}. \quad (40)$$

Из (39) и (40) следует, что

$$\Phi(w_s^4) + 2\Psi(w_s^2) \equiv M_s \pmod{4R}. \quad (41)$$

Теперь рассмотрим $F = F[G, \Phi, \Psi]$. Согласно п. 2 леммы 9

$$F^{[s]}(\mathbf{a}) \equiv w_s \pmod{4R} \quad \forall s \geq 0.$$

Отсюда и согласно (31) для всякого $s \in \{0, 1, \dots, q^m - 1\}$ имеет место сравнение

$$\frac{\partial F_j}{\partial x_i}(F^{[s]}(\mathbf{a})) \equiv \varphi_{i,j}(w_s^4) + 2\psi_{i,j}(w_s^2) \pmod{4R} \quad \forall i, j \in \{1, 2, \dots, m\}.$$

Поэтому с учетом (41)

$$J_F(F^{[s]}(\mathbf{a})) \equiv \Phi(w_s^4) + 2\Psi(w_s^2) \equiv M_s \pmod{4R}.$$

□

Пусть $\mathbf{a} \in R^m$, G – m -мерное полиномиальное преобразование, полноцикловое по модулю радикала, $M_0, M_1, \dots, M_{q^m-1}$ – матрицы над R размера $m \times m$, $M_s^{(0)}$ и $M_s^{(1)}$ – первый и второй разряды в разложении Тейхмюллера матрицы M_s соответственно, $s = 0, 1, \dots, q^m - 1$. Обозначим через

$$\mathfrak{F}(\mathbf{a}, G, M_0, M_1, \dots, M_{q^m-1}) \quad (42)$$

множество таких подстановок $F = F[G, \Phi, \Psi]$, что матрицы $\Phi(\mathbf{x})$ и $\Psi(\mathbf{x})$ удовлетворяют следующим сравнениям по модулю $2R$:

$$\Phi(G^{[s]}(\mathbf{a})^4) \equiv M_s^{(0)}, \quad \Psi(G^{[s]}(\mathbf{a})^2) \equiv M_s^{(1)} - \gamma_1[\Phi(H^{[s]}(\mathbf{a})^4)] \quad \forall s \geq 0,$$

где $H = H[G, \Phi, 0]$.

Заметим, что всякая подстановка вида (27) принадлежит семейству (42) при подходящих матрицах $M_0, M_1, \dots, M_{q^m-1}$. Действительно, при фиксированных векторе $\mathbf{a} \in R^m$, полноцикловом преобразовании G и матрицах $\Phi(\mathbf{x}), \Psi(\mathbf{x}) \in R[\mathbf{x}]_{m,m}$ матрицы $M_0, M_1, \dots, M_{q^m-1}$ можно выбрать в соответствии со следующей процедурой.

- 1) Пусть $u_0 = \mathbf{a}$, $u_{i+1} = G(u_i^q)$, $i = 0, 1, 2, \dots$. Положить

$$M_s^{(0)} = \gamma_0(\Phi(u_s^4)), \quad s = 0, 1, \dots, q^m - 1,$$

где γ_0 – нулевая координатная функция из разложения Тейхмюллера.

- 2) Пусть $v_0 = \mathbf{a}$, $v_{i+1} = G(v_i^q) + (v_i - v_i^q)\Phi(v_i^4)$, $i = 0, 1, 2, \dots$. Положить

$$M_s^{(1)} = \gamma_0[\Psi(v_s^2) + \gamma_1[\Phi(v_s^4)]], \quad s = 0, 1, \dots, q^m - 1.$$

- 3) Положить $M_s = M_s^{(0)} + 2M_s^{(1)} + 4N_s$, где $N_s \in R_{m,m}$ – произвольная матрица, $s = 0, 1, \dots, q^m - 1$.

Поэтому далее считаем, что рассматриваемая подстановка F вида (27) принадлежит семейству (42).

Пусть $f = f_1 = F^{[\tau_1(\mathbf{a})]}$. Согласно утверждению 10 и формуле (2) имеют место соотношения

$$f(\mathbf{a} + 2\mathbf{b}) \equiv f(\mathbf{a}) + 2\mathbf{b}J_f(\mathbf{a}) \pmod{8R} \quad \forall \mathbf{b} \in R^m, \quad (43)$$

$$J_f(\mathbf{a}) \equiv M_0 \cdot M_1 \cdot \dots \cdot M_{q^m-1} \pmod{4R}. \quad (44)$$

В частности, из того, что F – подстановка, следует, что все матрицы M_s обратимы, $s = 0, 1, \dots, q^m - 1$. Ближайшая цель – найти необходимое и достаточное условие того, что подстановка F является МДЦ-подстановкой.

Пусть $\mathbf{b} \in R^m$, $\hat{R} = R/4R$, $R \rightarrow \hat{R}$ – естественный эпиморфизм, $\hat{J}_f(\mathbf{b})$ – образ матрицы $J_f(\mathbf{b})$ под действием этого эпиморфизма, $\chi_{F,\mathbf{b}}(x)$ – характеристический многочлен матрицы $\hat{J}_f(\mathbf{b})$. Покажем, что многочлен $\chi_{F,\mathbf{b}}(x)$ не зависит от выбора вектора $\mathbf{b} \in R^m$. Сначала – лемма.

Лемма 11. Если F – подстановка вида (27), то для любых векторов $\mathbf{a}, \mathbf{b} \in R^m$ имеет место сравнение

$$J_F(\mathbf{a} + 2\mathbf{b}) \equiv J_F(\mathbf{a}) \pmod{4R}. \quad (45)$$

Доказательство. Выберем и зафиксируем $i, j, k \in \{1, 2, \dots, m\}$, $\mathbf{a}, \mathbf{b} \in R^m$. Положим

$$\mathcal{F}(\mathbf{x}) = \frac{\partial F_j}{\partial x_i}(\mathbf{x}).$$

Согласно (30)

$$\frac{\partial \mathcal{F}}{\partial x_k}(\mathbf{x}) = \frac{\partial^2 F_j}{\partial x_k \partial x_i}(\mathbf{x}) \in 4R[\mathbf{x}],$$

поэтому

$$\frac{\partial \mathcal{F}}{\partial x_k}(\mathbf{a}) \equiv 0 \pmod{2R}.$$

Согласно [7, формула (4)]

$$\mathcal{F}(\mathbf{a} + 2\mathbf{b}) \equiv \mathcal{F}(\mathbf{a}) + 2\mathbf{b}J^\downarrow(\mathbf{a}) \pmod{4R},$$

где

$$J^\downarrow(\mathbf{a}) = \left(\frac{\partial \mathcal{F}}{\partial z_1}(\mathbf{a}), \frac{\partial \mathcal{F}}{\partial z_2}(\mathbf{a}), \dots, \frac{\partial \mathcal{F}}{\partial z_m}(\mathbf{a}), \right)^T,$$

а « T » – символ операции транспонирования. Поэтому

$$\forall i, j \in \{1, 2, \dots, m\}: \quad \frac{\partial F_j}{\partial z_i}(\mathbf{a} + 2\mathbf{b}) \equiv \frac{\partial F_j}{\partial z_i}(\mathbf{a}) \pmod{4R},$$

и, следовательно, верно сравнение (45). $\square$

Так как $\bar{F}$ – полноцикловое преобразование, для $\mathbf{b}$ существует единственное такое $i \in \{0, 1, \dots, q^m - 1\}$, что

$$\mathbf{b} \equiv F^{[i]}(\mathbf{a}) \pmod{2R}.$$

Тогда $\chi_{F,\mathbf{b}}(x)$ есть характеристический многочлен матрицы $\widehat{J}_f(F^{[i]}(\mathbf{a}))$. Согласно лемме 11, (2) и (29) выполняется цепочка равенств и сравнений по модулю $4R$:

$$J_f(\mathbf{b}) \equiv J_f(F^{[i]}(\mathbf{a})) = \prod_{j=0}^{\tau_1(\mathbf{a})-1} J_F(F^{[i+j]}(\mathbf{a})) \equiv \prod_{j=0}^{\tau_1(\mathbf{a})-1} J_F(F^{[i \oplus j]}(\mathbf{a})),$$

где $\oplus$ есть сложение по модулю $\tau_1(\mathbf{a}) = q^m$. По п. 2) утверждения 10 справедливо сравнение по модулю $4R$:

$$J_f(\mathbf{b}) \equiv M_i \cdot M_{i+1} \cdots M_{q^m-1} \cdot M_0 \cdot M_1 \cdots M_{i-1}.$$

Поскольку все матрицы M_s , $s = 0, 1, \dots, q^m - 1$, обратимы, в силу (44) имеем:

$$J_f(\mathbf{b}) \equiv M_i \cdot M_{i+1} \cdots M_{q^m-1} \cdot M_0 \cdot M_1 \cdots M_{i-1} \approx \prod_{s=0}^{q^m-1} M_s \equiv J_f(\mathbf{a}),$$

где все сравнения – по модулю $4R$, а $\approx$ есть отношение подобия матриц. Поэтому $\chi_{F,\mathbf{b}}(x)$ совпадает с характеристическим многочленом матрицы $\widehat{J}_f(\mathbf{a})$. Таким образом, многочлен $\chi_{F,\mathbf{b}}(x)$ не зависит от выбора вектора $\mathbf{b} \in R^m$. В связи с этим многочлен $\chi_{F,\mathbf{b}}(x)$ будем далее обозначать через $\chi_F(x)$.

Следующая теорема показывает, что МДЦ-подстановки играют в теории полиномиальных преобразований такую же роль, какую многочлены максимального периода играют в теории ЛРП.

Теорема 12. Пусть $q > p = 2$ и $n \geq 4$. Для любой подстановки F из семейства (42) следующие утверждения эквивалентны:

- а) F есть МДЦ-подстановка,
- б) χ_F есть многочлен максимального периода.

Доказательство. Согласно [7, теорема 4] и п. III теоремы 7 равенство

$$\tau(F, n, \mathbf{a}) = q^m(q^m - 1) \cdot 2^{n-2} \quad (46)$$

эквивалентно одновременному выполнению четырех условий:

- 1) $\bar{F}$ – полноцикловое преобразование пространства $\bar{R}^m$,
- 2) $\bar{\chi}_F$ – многочлен максимального периода,

3) $\mathbf{a} \not\equiv \mathbf{a}^* \pmod{4R}$,

4) если $f_2(\mathbf{a}) = \mathbf{a} + 4\mathbf{b}$ и $J_{f_2}(\mathbf{a}) = E + 2C(\mathbf{a})$, то $\mathbf{b}(E + C(\mathbf{a})) \not\equiv 0 \pmod{2R}$.

Пусть $\sigma = q^m - 1$. Согласно [8, теорема 4.4] многочлен $\chi_F(x) \in \widehat{R}[x]$ является многочленом максимального периода тогда и только тогда, когда одновременно выполняются два условия:

а) $\bar{\chi}_F$ – многочлен максимального периода,

б) если $x^\sigma \equiv e + 2U(x) \pmod{\chi_F}$, где $\deg U(x) < m$, то $\bar{U} \notin \{\bar{0}, \bar{e}\}$.

Если $\bar{\chi}_F$ – многочлен максимального периода, то для вектора $\mathbf{a}$ выполняется условие 3). Поскольку F – подстановка из семейства (42), условие 1) выполнено. Покажем, что в ситуации, когда $\bar{\chi}_F$ – многочлен максимального периода и вектор $\mathbf{a}$ удовлетворяет условию 3), условия 4) и б) эквивалентны.

Рассмотрим разложение Тейхмюллера корня a многочлена $\chi_F(x)$ в расширении Галуа $\widehat{S} = GR(q^{2m}, 4)$ кольца $\widehat{R} = GR(q^2, 4)$:

$$a = a_0 + 2a_1, \quad a_0, a_1 \in \Gamma(\widehat{S}).$$

Тогда условие б) эквивалентно совокупности условий

$$a^{q^m} = a + 2U(a)a \quad \text{и} \quad \bar{U}(\bar{a}) \notin \{\bar{0}, \bar{e}\},$$

т. е.

$$a_1 \notin \{0, a_0\}. \quad (47)$$

Пусть $f_2(\mathbf{a}) = \mathbf{a} + 4\mathbf{b}$. Покажем, что условия $a_1 \neq 0$ и $\bar{\mathbf{b}} \neq \bar{0}$ равносильны.

Поскольку $\mathbf{a}$ удовлетворяет условию 3), имеем: $f(\mathbf{a}) = \mathbf{a} + 2\mathbf{t}_1$, где $\bar{\mathbf{t}}_1 \neq \bar{0}$. Обозначим $J = J_f(\mathbf{a})$. Используя формулу (28), индукцией по $k \geq 1$ нетрудно показать, что

$$f^{[k]}(\mathbf{a}) \equiv \mathbf{a} + 2\mathbf{t}_1(E + J + \dots + J^{k-1}) \pmod{8R}.$$

Согласно [7, теорема 4] совокупность условий 1)–3) эквивалентна равенству $\tau(F, 2, \mathbf{a}) = q^m \cdot \sigma$. Следовательно, $f_2 = f^{[\sigma]}$ и имеет место сравнение

$$f_2(\mathbf{a}) \equiv \mathbf{a} + 2\mathbf{t}_1(J - E)^{-1}(J^\sigma - E) \pmod{8R}.$$

Пусть $\mathbf{t}_2 = \mathbf{t}_1(J - E)^{-1}$. Условие $\bar{\mathbf{b}} = \bar{0}$ равносильно условию

$$\mathbf{t}_2(J^{q^m} - J) \equiv 0 \pmod{4R}. \quad (48)$$

Над кольцом $\widehat{S}$ матрица $\widehat{J}^{q^m} - \widehat{J}$ подобна матрице $2 \cdot \text{diag}(a_1, a_1^q, \dots, a_1^{q^{m-1}})$. Поскольку $\bar{t}_2 \neq \bar{0}$, условие (48) равносильно условию $a_1 = 0$.

Согласно утверждению 6 и равенству $\tau(F, 2, \mathbf{a}) = q^m \cdot \sigma$ имеем: $s_0 = 2$. Следовательно, существует такая матрица $C(\mathbf{a})$, что

$$J_{f_2}(\mathbf{a}) = E + 2C(\mathbf{a}).$$

Покажем, что обратимость матрицы $E + C(\mathbf{a})$ равносильна условию $a_1 \neq a_0$.

Пусть

$$M = \prod_{s=0}^{q^m-1} M_s.$$

Согласно (44) верно сравнение

$$J_f(\mathbf{a}) \equiv M \pmod{4R}.$$

Из леммы 11 и формулы (2) производной сложной функции следует цепочка сравнений по модулю $4R$:

$$J_{f_2}(\mathbf{a}) \equiv M^\sigma \equiv J_f(\mathbf{a})^\sigma.$$

Поскольку в кольце $\widehat{S}$

$$(a_0 + 2a_1)^{q^m-1} = e + 2a_0^{-1}a_1,$$

имеем подобие матриц над $\bar{S} = \text{GF}(q^m)$

$$\bar{C}(\mathbf{a}) \approx \text{diag}((\bar{a}_0)^{-1} \cdot \bar{a}_1, (\bar{a}_0)^{-q} \cdot \bar{a}_1^q, \dots, (\bar{a}_0)^{-q^{m-1}} \cdot \bar{a}_1^{q^{m-1}}). \quad (49)$$

Тогда обратимость матрицы $\bar{E} + \bar{C}(\mathbf{a})$ (и, следовательно, обратимость матрицы $E + C(\mathbf{a})$) равносильна условию $a_1 \neq a_0$.

Итак, условие (47) равносильно совокупности условий

$$\bar{\mathbf{b}} \neq \bar{\mathbf{0}} \quad \text{и} \quad E + C(\mathbf{a}) \in R_{m,m}^*. \quad (50)$$

Из (50) следует, что

$$\mathbf{b}(E + C(\mathbf{a})) \not\equiv 0 \pmod{2R}. \quad (51)$$

Осталось доказать, что из (51) следует (50).

Пусть выполнено (51). Очевидно, $\bar{\mathbf{b}} \neq \bar{0}$. Пусть $\oplus$ – сложение в поле $\bar{S}$. Согласно (49) матрица $\bar{E} \oplus \bar{C}(\mathbf{a})$ подобна матрице

$$\text{diag}(\bar{e} \oplus (\bar{a}_0)^{-1} \cdot \bar{a}_1, \bar{e} \oplus (\bar{a}_0)^{-q} \cdot \bar{a}_1^q, \dots, \bar{e} \oplus (\bar{a}_0)^{-q^{m-1}} \cdot \bar{a}_1^{q^{m-1}}).$$

Соотношение (51) означает, что $a_0^{q^i} \neq a_1^{q^i}$ для некоторого $i \in \{0, 1, \dots, m-1\}$, и $a_0 \neq a_1$. Поэтому матрица $E + C(\mathbf{a})$ обратима. $\square$

Теорема 12 – двоичный аналог теоремы 7 из [7]. Она позволяет сформулировать алгоритм построения МДЦ-подстановок.

Алгоритм 13. (Построение МДЦ-подстановки).

Вход: вектор $\mathbf{a} \in R^m$.

Выход: полиномиальная подстановка F , для которой $\tau(F, n, \mathbf{a}) = L_m(R)$.

1. Построить такое m -мерное полиномиальное преобразование G кольца R , что $\bar{G}$ – полноцикловое преобразование пространства $\bar{R}^m$. Положить

$$F(\mathbf{x}) = G(\mathbf{x}^q).$$

2. Построить $\chi(x) \in R[x]$ – многочлен максимального периода степени m . Пусть $S(\chi)$ – его сопровождающая матрица. Выбрать и зафиксировать такие матрицы

$$M_0, M_1, \dots, M_{q^m-1} \in R_{m,m},$$

что

$$\prod_{s=0}^{q^m-1} M_s \approx S(\chi).$$

Для каждого $s \in \{0, 1, \dots, q^m-1\}$ найти разложение

$$M_s \equiv M_s^{(0)} + 2M_s^{(1)} \pmod{4R},$$

где $M_s^{(0)}, M_s^{(1)} \in \Gamma(R)_{m,m}$.

3. Выбрать матрицу $\Phi(\mathbf{x}) \in R[\mathbf{x}]_{m,m}$ так, что

$$\Phi(F^{[s]}(\mathbf{a})^4) \equiv M_s^{(0)} \pmod{2R} \quad \forall s \in \{0, 1, \dots, q^m-1\}.$$

Положить $F(\mathbf{x}) = F(\mathbf{x}) + (\mathbf{x} - \mathbf{x}^q)\Phi(\mathbf{x}^4)$.

4. Выбрать матрицу $\Psi(\mathbf{x}) \in R[\mathbf{x}]_{m,m}$ так, что

$$\Psi(F^{[s]}(\mathbf{a})^2) \equiv M_s^{(1)} - \gamma_1[\Phi(F^{[s]}(\mathbf{a})^4)] \pmod{2R} \quad \forall s \in \{0, 1, \dots, q^m - 1\},$$

где γ_1 – первая координатная функция из разложения Теймюллера. Положить $F(\mathbf{x}) = F(\mathbf{x}) + 2(\mathbf{x} - \mathbf{x}^q)\Psi(\mathbf{x}^2)$.

Алгоритм 13 является двоичным аналогом алгоритма А из [7]. Он позволяет построить любую МДЦ-подстановку вида (27). Кроме того, можно сформулировать очевидное следствие из теоремы 12.

Следствие 14. Пусть $q > p = 2$ и $n \geq 4$. Для любой подстановки F вида (27) следующие утверждения эквивалентны:

- а) F есть МДЦ-подстановка,
- б) χ_F есть многочлен максимального периода.

В связи с этим многочлен $\chi_F(x)$ естественно назвать *характеристическим многочленом* подстановки F вида (27).

4. О цикловых типах МДЦ-подстановок

В этом разделе $p = 2$, $t \geq 2$, $q = p^t$, $n \geq 4$, $R = GR(q^n, p^n)$ – кольцо Галуа, $m \geq 2$, G – m -мерное полиномиальное преобразование, полноцикловое по модулю радикала, F – m -мерная подстановка над R вида (27). Рассмотрим *цикловой тип* подстановки F , отождествляемый с многочленом

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

где $c_i^{(F)}$ – количество циклов длины i в цикловой записи подстановки F .

Положим $R_n = R$. Для всякого $s \in \{1, 2, \dots, n - 1\}$ обозначим через R_s фактор-кольцо $R/2^s R$, а через φ_s – эпиморфизм $R_{s+1} \rightarrow R_s$, определенный равенством

$$\forall a \in R: \quad \varphi_s(a + 2^{s+1}R) = a + 2^s R.$$

Обозначим через $\psi_s(F)$ образ F при естественном эпиморфизме $\psi_s: R \rightarrow R_s$. Пусть C – некоторый цикл в графе преобразования $\psi_s(F)$; назовем *прообразом* цикла C множество

$$\varphi_s^{-1}(C) = \{\mathbf{a} \in R_{s+1}^m \mid \varphi_s(\mathbf{a}) \in C\}.$$

Пусть $s \in \{1, 2, \dots, n-1\}$, ψ_n – тождественное преобразование кольца R . Наделим $\varphi_s^{-1}(C)$ структурой орграфа: упорядоченная пара $(\mathbf{u}, \mathbf{v}) \in R_{s+1}^{2m}$ является дугой тогда и только тогда, когда

$$F(\mathbf{u}) \equiv \mathbf{v} \pmod{2^{s+1}R}.$$

Прообраз $\varphi_s^{-1}(C)$ инвариантен относительно преобразования $\psi_{s+1}(F)$. Поэтому орграф $\varphi_s^{-1}(C)$ представляет собой совокупность циклов.

Как и ранее, $f = f_1$. Следуя [5], назовем l -циклом цикл длины $l \geq 1$.

Лемма 15. Пусть F – подстановка вида (27), ее характеристический многочлен $\chi_F(x)$ есть многочлен Галуа над кольцом $R/4R$, C – l -цикл в графе преобразования $\psi_s(F)$. Тогда:

1. если в прообразе цикла C есть цикл длины dl , где $d \mid q^m - 1$ и $d > 1$, то этот прообраз состоит из одного цикла длины l и $\frac{q^m - 1}{d}$ циклов длины dl ,
2. если в прообразе цикла C есть цикл длины $2l$, то этот прообраз состоит из $\frac{q^m}{2}$ циклов длины $2l$,
3. если в прообразе цикла C есть не менее двух циклов длины l , то этот прообраз состоит из q^m циклов длины l .

Доказательство. Пусть $s \in \{1, 2, \dots, n-1\}$. Выберем и зафиксируем такой вектор $\mathbf{a} \in R^m$, что его образ $\tilde{\mathbf{a}}$ при эпиморфизме ψ_s принадлежит циклу C . При отображении φ_s у вершины $\tilde{\mathbf{a}}$ имеется $|\bar{R}|^m = q^m$ прообразов. Опишем распределение этих прообразов по циклам орграфа $\varphi_s^{-1}(C)$.

1. Пусть орграф $\varphi_s^{-1}(C)$ содержит цикл длины dl , $d \mid q^m - 1$, $d > 1$. Это означает, что существует такой вектор $\mathbf{b} \in R^m$, что

$$\tau_{s+1}(\mathbf{a} + 2^s \mathbf{b}) = dl. \quad (52)$$

По условию F – подстановка вида (27). При обосновании п. 1) утверждения 10 было показано, что всякая подстановка вида (27) обладает свойством (4). Поскольку многочлен $\bar{\chi}_F(x)$ неприводим над $\bar{R}$ и имеет степень $m \geq 2$, для подстановки F выполнены условия теоремы 7. Поскольку d нечетно и отлично от 1, по п. III теоремы 7 имеют место соотношения

$$\tau_1(\mathbf{a}) = \tau_2(\mathbf{a}) = \dots = \tau_s(\mathbf{a}) = l, \quad (53)$$

и число d совпадает с мультипликативным порядком любого корня многочлена $\bar{\chi}_F(x)$ в его поле разложения $GF(q^m)$.

Пусть вектор $\mathbf{r} \in R^m$ таков, что $f_s(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{r}$. Ввиду (53) $f_s = f$, и, следовательно,

$$f(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{r}. \quad (54)$$

При фиксированном $\mathbf{a}$ рассмотрим равенство (52) как уравнение относительно $\mathbf{b} \in R^m$. Очевидно, это уравнение эквивалентно соотношению

$$f_s(\mathbf{a} + 2^s \mathbf{b}) \not\equiv \mathbf{a} + 2^s \mathbf{b} \pmod{2^{s+1}R},$$

т. е.

$$f(\mathbf{a} + 2^s \mathbf{b}) \not\equiv \mathbf{a} + 2^s \mathbf{b} \pmod{2^{s+1}R}. \quad (55)$$

Пусть $J = J_f(\mathbf{a})$. Согласно [7, формула (18)]

$$f(\mathbf{a} + 2^s \mathbf{b}) \equiv f(\mathbf{a}) + 2^s \mathbf{b} J \pmod{2^{s+1}R}.$$

Ввиду (54) соотношение (55) приобретает вид

$$\mathbf{a} + 2^s \mathbf{r} + 2^s \mathbf{b} J \not\equiv \mathbf{a} + 2^s \mathbf{b} \pmod{2^{s+1}R},$$

т. е.

$$\bar{\mathbf{b}}(\bar{E} \oplus \bar{J}) \neq \bar{\mathbf{r}},$$

где $\oplus$ – сложение в поле $\bar{R}$. Поскольку характеристический многочлен $\bar{\chi}_F$ матрицы $\bar{J}$ неприводим над $\bar{R}$ и $m \geq 2$, элемент $\bar{e}$ не является собственным значением матрицы $\bar{J}$. Поэтому матрица $\bar{E} \oplus \bar{J}$ обратима. Таким образом, по модулю радикала существует единственный вектор $\mathbf{b} \in R^m$, не являющийся решением уравнения (52). Это означает, что у вершины $\tilde{\mathbf{a}}$ есть единственный прообраз, принадлежащий циклу длины l , и $q^m - 1$ прообразов, принадлежащих циклам длины dl . На одном dl -цикле лежат d прообразов вершины $\tilde{\mathbf{a}}$ (они расположены на цикле с шагом l). Поэтому орграф $\varphi_s^{-1}(C)$ состоит из одного цикла длины l и $\frac{q^m-1}{d}$ циклов длины dl .

2. Пусть орграф $\varphi_s^{-1}(C)$ содержит цикл длины $2l$. Поскольку число вершин в орграфе $\varphi_s^{-1}(C)$ равно $q^m l$, достаточно показать, что все вершины этого орграфа принадлежат циклам длины $2l$. Величина s_0 , определенная в разделе 2 как минимальное значение $s \geq 1$, удовлетворяющее соотношению (3), зависит от $\mathbf{a}$: $s_0 = s_0(\mathbf{a})$. Возможны две ситуации: **A)** $s_0(\mathbf{a}) = 1$ и **B)** $s_0(\mathbf{a}) > 1$.

A) $s_0(\mathbf{a}) = 1$. По лемме 1 верно равенство $\overline{J_{f_s}(\mathbf{a})} = \bar{E}$. Поскольку $2s \geq s + 1$, из [7, формула (4)] следует, что для всякого $\mathbf{b} \in R^m$ верно соотношение

$$f_s(\mathbf{a} + 2^s \mathbf{b}) \equiv f_s(\mathbf{a}) + 2^s \mathbf{b} \pmod{2^{s+1}R}. \quad (56)$$

Пусть вектор $\mathbf{r} \in R^m$ удовлетворяет равенству $f_s(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{r}$. Согласно (56) и п. I теоремы 7 для всякого $\mathbf{b} \in R^m$ справедлива цепочка эквивалентностей:

$$\begin{aligned} \tau_{s+1}(\mathbf{a} + 2^s \mathbf{b}) = 2l &\Leftrightarrow \tau_{s+1}(\mathbf{a} + 2^s \mathbf{b}) > \tau_s(\mathbf{a}) \Leftrightarrow \\ &\Leftrightarrow f_s(\mathbf{a} + 2^s \mathbf{b}) \not\equiv \mathbf{a} + 2^s \mathbf{b} \pmod{2^{s+1}R} \Leftrightarrow \bar{\mathbf{r}} \neq \bar{0}. \end{aligned} \quad (57)$$

Поскольку в прообразе $\varphi_s^{-1}(C)$ есть цикл длины $2l$, то $\bar{\mathbf{r}} \neq \bar{0}$. Следовательно, все циклы в орграфе $\varphi_s^{-1}(C)$ имеют длину $2l$.

В) $s_0(\mathbf{a}) > 1$. По определению величины s_0

$$s_0(\mathbf{a}) = s_0(\mathbf{a} + 2^s \mathbf{b}) \quad \forall \mathbf{b} \in R^m. \quad (58)$$

Так как в орграфе $\varphi_s^{-1}(C)$ есть цикл длины $2l$, то для некоторого $\mathbf{b} \in R^m$ верно равенство

$$\tau_{s+1}(\mathbf{a} + 2^s \mathbf{b}) = 2\tau_s(\mathbf{a}).$$

Согласно (58) имеем: $s_0(\mathbf{a} + 2^s \mathbf{b}) > 1$. Из утверждения 6, п. III теоремы 7 и (58) следует, что

$$s \geq s_0(\mathbf{a} + 2^s \mathbf{b}) = s_0(\mathbf{a}).$$

По лемме 1 верно равенство $\overline{J_{f_s}(\mathbf{a})} = \bar{E}$, и имеет место соотношение (56). Пусть вектор $\mathbf{r} \in R^m$ удовлетворяет равенству $f_s(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{r}$. Согласно (11) и (56) справедлива цепочка эквивалентностей (57). Доказательство завершается так же, как в п. **А)**.

3. Пусть существуют такие векторы $\mathbf{c}, \mathbf{d} \in R^m$, что

$$\bar{\mathbf{c}} \neq \bar{\mathbf{d}} \quad \text{и} \quad \tau_{s+1}(\mathbf{a} + 2^s \mathbf{c}) = l = \tau_{s+1}(\mathbf{a} + 2^s \mathbf{d}).$$

Покажем, что все циклы в орграфе $\varphi_s^{-1}(C)$ имеют длину l . Пусть вектор $\mathbf{r} \in R^m$ удовлетворяет равенству $f_s(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{r}$. Для всякого вектора $\mathbf{b} \in R^m$ имеет место цепочка эквивалентностей

$$\begin{aligned} \tau_{s+1}(\mathbf{a} + 2^s \mathbf{b}) = \tau_s(\mathbf{a}) &\Leftrightarrow f_s(\mathbf{a} + 2^s \mathbf{b}) \equiv \mathbf{a} + 2^s \mathbf{b} \pmod{2^{s+1}R} \Leftrightarrow \\ &\Leftrightarrow f_s(\mathbf{a} + 2^s \mathbf{b}) \equiv f_s(\mathbf{a}) + 2^s(\mathbf{b} - \mathbf{r}) \pmod{2^{s+1}R}. \end{aligned} \quad (59)$$

Обозначим: $A_s(\mathbf{a}) = J_{f_s}(\mathbf{a})$. Поскольку $2s \geq s + 1$, из [7, формула (4)] следует, что

$$f_s(\mathbf{a} + 2^s \mathbf{b}) \equiv f_s(\mathbf{a}) + 2^s \mathbf{b} A_s(\mathbf{a}) \pmod{2^{s+1}R}.$$

Отсюда и из цепочки (59) следует, что для всякого $\mathbf{b} \in R^m$

$$\tau_{s+1}(\mathbf{a} + 2^s \mathbf{b}) = l \Leftrightarrow \bar{\mathbf{b}}(\bar{E} \oplus \overline{A_s(\mathbf{a})}) = \bar{\mathbf{r}}. \quad (60)$$

В частности, для ненулевого вектора $\bar{\mathbf{c}} \oplus \bar{\mathbf{d}}$ выполняется равенство

$$(\bar{\mathbf{c}} \oplus \bar{\mathbf{d}})(\bar{E} \oplus \overline{A_s(\mathbf{a})}) = \bar{0}.$$

Пусть $\Delta = d_1 d_2 \dots d_{s-1}$, $J = J_f(\mathbf{a})$. Аналогично доказательству леммы 1 нетрудно показать, что

$$\overline{A_s(\mathbf{a})} = \bar{J}^\Delta.$$

Характеристический многочлен $\bar{\chi}_F(x)$ матрицы $\bar{J}$ неприводим над $\bar{R}$. Пусть σ – мультипликативный порядок любого его корня в поле разложения. Равенство

$$(\bar{\mathbf{c}} \oplus \bar{\mathbf{d}})(\bar{E} \oplus \bar{J}^\Delta) = \bar{0}$$

возможно лишь в ситуации, когда $\sigma \mid \Delta$. Но тогда матрица $\bar{E} \oplus \overline{A_s(\mathbf{a})}$ нулевая, и эквивалентность (60) переписывается в виде

$$\tau_{s+1}(\mathbf{a} + 2^s \mathbf{b}) = l \Leftrightarrow \bar{\mathbf{r}} = \bar{0}. \quad (61)$$

Эквивалентность (61) имеет место для всякого вектора $\mathbf{b} \in R^m$. Так как

$$\tau_{s+1}(\mathbf{a} + 2^s \mathbf{c}) = l,$$

то $\bar{\mathbf{r}} = \bar{0}$. Поэтому равенство

$$\tau_{s+1}(\mathbf{a} + 2^s \mathbf{b}) = l$$

выполняется для любого вектора $\mathbf{b} \in R^m$, и в орграфе $\varphi_s^{-1}(C)$ все циклы имеют длину l . $\square$

Лемма 15 является m -мерным двоичным аналогом теоремы 7 из [5].

Пусть F – МДЦ-подстановка вида (27). Цель дальнейших выкладок – описать цикловой тип $C_F(y)$ подстановки F . Сначала уточним теорему 7.

Утверждение 16. Пусть F – МДЦ-подстановка вида (27) и C – один из циклов подстановки F , вектор $\mathbf{a}$ принадлежит циклу C . Тогда профиль (10) цикла C имеет один из следующих видов:

- а) $(1, 1, \dots, 1)$,
- б) $(1, 1, \dots, 1, q^m - 1)$,

c) $(1, 1, \dots, 1, q^m - 1, 2, \dots, 2)$,

d) $(q^m - 1, 2, 2, \dots, 2)$.

Ситуация а) имеет место тогда и только тогда, когда $\mathbf{a} = \mathbf{a}^*$.

Доказательство. Рассмотрим разложение Тейхмюллера корня a многочлена $\chi_F(x)$ в расширении Галуа $\hat{S} = GR(q^{2m}, 4)$ кольца $\hat{R} = GR(q^2, 4)$:

$$a = a_0 + 2a_1, \quad a_0, a_1 \in \Gamma(\hat{S}).$$

Как показано при доказательстве теоремы 12, тот факт, что $\chi_F(x)$ – многочлен максимального периода, эквивалентен условию (47):

$$a_1 \notin \{0, a_0\}.$$

Обозначим мультипликативный порядок a_0 через σ . Очевидно, $\sigma = q^m - 1$.

По п. III теоремы 7 либо $\mathbf{a} = \mathbf{a}^*$ (тогда имеет место ситуация а)), либо существует единственное значение $s \in \{1, 2, \dots, n - 1\}$ со свойством $d_s = \sigma$. Пусть ситуация а) не реализуется. Рассмотрим соответствующее значение s .

Если $s = n - 1$, то по п. III теоремы 7 имеет место ситуация б). Далее рассматриваем случай $s \leq n - 2$. Докажем сначала, что $d_{s+1} = 2$. Согласно п. III теоремы 7 достаточно доказать, что $d_{s+1} > 1$.

Пусть $J = J_f(\mathbf{a})$. В силу теоремы 7 имеем: $d_1 = d_2 = \dots = d_{s-1} = 1$. Отсюда, пользуясь ранее введенными обозначениями, получаем:

$$A_s(\mathbf{a}) = J_{f_s}(\mathbf{a}) = J.$$

Поскольку $d_s = \sigma > 1$, существует такой вектор $\mathbf{b} \in R^m$, что $\bar{\mathbf{b}} \neq \bar{0}$ и $f_s(\mathbf{a}) = \mathbf{a} + 2^s \mathbf{b}$. Возможны две ситуации:

1) $s = 1$. Так как $f(\mathbf{a}) = \mathbf{a} + 2\mathbf{b}$, то из соотношения (28) индукцией по $j \geq 1$ получаем:

$$f^{[j]}(\mathbf{a}) \equiv \mathbf{a} + 2\mathbf{b}(E + J + \dots + J^{j-1}) \pmod{8R} \quad \forall j \geq 1.$$

Поэтому верна следующая цепочка равенств и сравнений по модулю $8R$:

$$f_2(\mathbf{a}) = f^{[\sigma]}(\mathbf{a}) \equiv \mathbf{a} + 2\mathbf{b}(E - J)^{-1}(E - J^\sigma).$$

Пусть $\hat{J}$ – образ J под действием естественного эпиморфизма $R \rightarrow \hat{R}$. Как показано при обосновании теоремы 12, над кольцом $\hat{S}$ матрица $\hat{J}^{q^m} - \hat{J}$ подобна матрице

$$2 \cdot \text{diag}(a_1, a_1^q, \dots, a_1^{q^{m-1}}).$$

Так как $a_1 \neq 0$, то $f_2(\mathbf{a}) \not\equiv \mathbf{a} \pmod{8R}$, т. е. $d_{s+1} = d_2 > 1$.

2) $s > 1$. Поскольку $2s \geq s+2$, используя [7, формула (4)], индукцией по $j \geq 1$ нетрудно получить соотношение

$$f_s^{[j]}(\mathbf{a}) \equiv \mathbf{a} + 2^s \mathbf{b}(E + J + \dots + J^{j-1}) \pmod{2^{s+2}R} \quad \forall j \geq 1.$$

Рассуждая аналогично п. 1), получаем:

$$f_{s+1}(\mathbf{a}) = f_s^{[\sigma]}(\mathbf{a}) \not\equiv \mathbf{a} \pmod{2^{s+2}R}.$$

Следовательно, $d_{s+1} > 1$.

По утверждению 6 и теореме 7 имеем: $s = s_0 - 1$, где $s_0 = s_0(\mathbf{a})$. Таким образом, верна следующая совокупность равенств:

$$d_1 = d_2 = \dots = d_{s_0-2} = 1, \quad d_{s_0-1} = \sigma, \quad d_{s_0} = 2,$$

т. е., в обозначениях теоремы 7, $\nu = 0$. Случаю $s_0 = n - 1$ соответствует ситуация с). Пусть $s_0 \leq n - 2$. Согласно теореме 7 отрезок профиля

$$(d_{s_0+1}, d_{s_0+2}, \dots, d_{n-1})$$

может иметь один из двух видов:

$$\mathbf{A}) (2, 2, \dots, 2),$$

$$\mathbf{B}) (1, 1, \dots, 1, 2, 2, \dots, 2), \text{ где серия единиц имеет ненулевую длину.}$$

Осталось показать, что ситуация **B)** невозможна.

Согласно п. IV теоремы 7 ситуация **B)** реализуется тогда и только тогда, когда

$$\mathbf{b}(E + C(\mathbf{a})) \equiv 0 \pmod{2R}, \quad (62)$$

где вектор $\mathbf{b}$ и матрица $C(\mathbf{a})$ определены равенствами

$$f_{s_0}(\mathbf{a}) = \mathbf{a} + 2^{s_0} \mathbf{b} \quad \text{и} \quad A_{s_0}(\mathbf{a}) = E + 2C(\mathbf{a})$$

соответственно. Поскольку $d_{s_0} > 1$, имеем: $\bar{\mathbf{b}} \neq \bar{0}$. Докажем обратимость матрицы $E + C(\mathbf{a})$ (и тогда соотношение (62), очевидно, не выполняется).

Поскольку $f_{s_0-1} = f$, имеем: $f_{s_0} = f^{[\sigma]}$. Согласно лемме 11 и формуле (2) справедлива цепочка равенств и сравнений по модулю $4R$:

$$A_{s_0}(\mathbf{a}) = \prod_{i=0}^{\tau_{s_0}-1} J_F(F^{[i]}(\mathbf{a})) = \prod_{j=0}^{\sigma-1} \prod_{i=0}^{\tau_1-1} J_F(F^{[i+j\tau_1]}(\mathbf{a}))$$

$$\equiv \prod_{j=0}^{\sigma-1} \prod_{i=0}^{\tau_1-1} J_F(F^{[i]}(\mathbf{a})) = J^\sigma.$$

Значит, $2C(\mathbf{a}) = J^\sigma - E$, и, поскольку в кольце $\widehat{S}$ верно равенство

$$(a_0 + 2a_1)^{q^m-1} = e + 2a_0^{-1}a_1,$$

имеем подобие матриц над $\bar{S}$:

$$\bar{C}(\mathbf{a}) \approx \text{diag}((\bar{a}_0)^{-1} \cdot \bar{a}_1, (\bar{a}_0)^{-q} \cdot \bar{a}_1^q, \dots, (\bar{a}_0)^{-q^{m-1}} \cdot \bar{a}_1^{q^{m-1}}).$$

Поскольку $a_1 \neq a_0$, матрица $E + C(\mathbf{a})$ обратима. $\square$

Проклассифицируем вершины графа G_F преобразования F . Согласно [7, утверждение 1] граф G_F имеет единственный цикл длины q^m . Будем называть этот цикл *отмеченным*; все элементы отмеченного цикла также будем называть *отмеченными*.

Для всякого $i \in \{0, 1, \dots, n-2\}$ обозначим через V_i множество неотмеченных вершин $\mathbf{a}$, удовлетворяющих условиям

$$\tau_1(\mathbf{a}) = \tau_2(\mathbf{a}) = \dots = \tau_{i+1}(\mathbf{a}) = q^m, \quad \tau_{i+2}(\mathbf{a}) = q^m(q^m - 1).$$

Из утверждения 16 следует, что множество $V_0 \cup V_1 \cup \dots \cup V_{n-2}$ есть множество всех неотмеченных вершин графа G_F . Заметим также, что каждое множество V_i инвариантно относительно F , и, согласно утверждению 16,

$$\tau(\mathbf{a}) = q^m(q^m - 1)2^{n-2-i} \quad \forall i \in \{0, 1, \dots, n-2\}, \mathbf{a} \in V_i.$$

Пусть $N_i(F)$ – количество циклов в графе $G_F(V_i)$, порожденном множеством V_i , $i = 0, 1, \dots, n-2$ (см., например, [2]). Тогда цикловой тип $C_F(y)$ подстановки F можно записать следующим образом:

$$C_F(y) = y^{q^m} + \sum_{i=0}^{n-2} N_i(F) \cdot y^{q^m(q^m-1)2^{n-2-i}}. \quad (63)$$

Используя лемму 15, вычислим величины $N_i(F)$, $i = 0, 1, \dots, n-2$.

Лемма 17. Если F – МДЦ-подстановка вида (27), $i \in \{0, 1, \dots, n-2\}$ и V_i не пусто, то верно равенство

$$N_i(F) = \left(\frac{q^m}{2}\right)^{n-2-i}.$$

Доказательство. Пусть V_i не пусто. Если $\mathbf{a} \in V_i$, то $\tau(F, i+1, \mathbf{a}) = \tau(F, 1, \mathbf{a})$, и согласно [7, утверждение 1] $\mathbf{a} \equiv \mathbf{a}^* \pmod{2^{i+1}R}$. Следовательно, множество $\psi_{i+1}(V_i)$ состоит из единственного цикла преобразования $\psi_{i+1}(F)$. Обозначим этот цикл через C . Длина цикла C равна q^m .

В множестве $\psi_{i+2}(V_i)$ имеется цикл длины $q^m(q^m - 1)$. По п. 1 леммы 15 прообраз $\varphi_{i+1}^{-1}(C)$ состоит из единственного цикла преобразования $\psi_{i+2}(F)$. Следовательно, множество $\psi_{i+2}(V_i)$ состоит из единственного цикла преобразования $\psi_{i+2}(F)$. Обозначим этот цикл через D . Длина цикла D равна $q^m(q^m - 1)$.

Пусть $j \in \{i+2, i+3, \dots, n-1\}$ и множество $\psi_j(V_i)$ состоит из $N \geq 1$ циклов, каждый из которых имеет длину $q^m(q^m - 1)2^{j-i-2}$. Рассмотрим любой из этих циклов; обозначим его через T . В множестве $\psi_{j+1}(V_i)$ имеется такой цикл U длины $q^m(q^m - 1)2^{j-i-1}$, что $\varphi_j(U) = T$. По п. 2 леммы 15 прообраз $\varphi_j^{-1}(T)$ состоит из $q^m/2$ циклов, каждый из которых имеет длину $q^m(q^m - 1)2^{j-i-1}$. Следовательно, множество $\psi_{j+1}(V_i)$ состоит из $N \cdot q^m/2$ циклов, каждый из которых имеет длину $q^m(q^m - 1)2^{j-i-1}$.

Таким образом, множество $V_i = \psi_n(V_i)$ состоит из $\left(\frac{q^m}{2}\right)^{n-2-i}$ циклов преобразования $F = \psi_n(F)$, каждый из которых имеет длину $q^m(q^m - 1)2^{n-2-i}$. $\square$

Остался непроясненным вопрос, для каких $i \in \{0, 1, \dots, n-2\}$ множество V_i не пусто. В силу леммы 17 верна цепочка равенств и неравенств:

$$q^{mn} = q^m + \sum_{i=0}^{n-2} N_i(F) \cdot q^m(q^m - 1)2^{n-2-i} \quad (64)$$

$$\leq q^m + q^m(q^m - 1) \sum_{j=0}^{n-2} q^{mj} = q^m + q^m(q^{m(n-1)} - 1) = q^{mn}.$$

Следовательно, неравенство в цепочке (64) представляет собой равенство, для каждого $i \in \{0, 1, \dots, n-2\}$ множество V_i не пусто, и верно равенство

$$\forall i \in \{0, 1, \dots, n-2\} : \quad N_i(F) = \left(\frac{q^m}{2}\right)^{n-2-i}. \quad (65)$$

Из (63) и (65) вытекает следующая теорема, являющаяся центральным результатом этого раздела.

Теорема 18. Если $p = 2, t \geq 2, q = p^t, n \geq 4, R = GR(q^n, p^n)$ – кольцо Галуа, $m \geq 2, F$ – m -мерная МДЦ-подстановка над R вида (27), то цикловой тип $C_F(y)$ подстановки F выражается формулой

$$C_F(y) = y^{q^m} + \sum_{s=0}^{n-2} \left(\frac{q^m}{2} \right)^s \cdot y^{q^m(q^m-1)2^s}. \quad (66)$$

Теорема 18 является двоичным аналогом теоремы 8 из [7]. Из нее, в частности, следует, что «почти все» вершины принадлежат циклам длины $L_m(R)$. Доля вершин, не принадлежащих циклам максимальной длины, равна $q^{-m} = o(1), m \rightarrow \infty$.

Сделаем еще одно замечание. Пусть $\mathbf{a} \in R^m$. Согласно [8, теорема 4.4(с)] характеристический многочлен $\chi(x)$ матрицы $J_f(\mathbf{a})$ является многочленом максимального периода (ММП) тогда и только тогда, когда он является ММП по модулю $4R$, т. е. когда многочлен $\chi_F(x)$ является ММП. По условию $\chi_F(x)$ есть ММП, поэтому $\chi(x)$ есть ММП независимо от выбора $\mathbf{a} \in R^m$.

Пусть $\tilde{R} = \psi_{n-1}(R) = R/2^{n-1}R$, $\tilde{\chi}$ есть образ χ под действием естественного эпиморфизма ψ_{n-1} . Хорошо известно (см., например, [8, теорема 4.6]), что цикловой тип $Z_{\tilde{\chi}}(y)$ ЛРП-семейства $L_{\tilde{R}}(\tilde{\chi})$ выражается формулой

$$Z_{\tilde{\chi}}(y) = y + \sum_{s=0}^{n-2} \left(\frac{q^m}{2} \right)^s \cdot y^{(q^m-1)2^s}.$$

Отсюда и из теоремы 18 вытекает равенство

$$C_F(y) = Z_{\tilde{\chi}}(y^{q^m}).$$

Таким образом, цикловой тип $C_F(y)$ отличается от циклового типа ЛРП-семейства $L_{\tilde{R}}(\tilde{\chi})$ лишь тем, что длины всех циклов в q^m раз больше.

Автор выражает глубокую признательность В.Е. Викторенкову за обсуждение полученных результатов и А.М. Зубкову за существенную помощь при подготовке статьи.

Работа посвящается памяти Михаила Михайловича Глухова.

Список литературы

- [1] Анашин В.С., “О группах и кольцах, обладающих транзитивными полиномами”, XVI Всесоюз. алгебр. конф.: тезисы, ч. II, 1981, 4–5.

- [2] Асанов М.О., Баранский В.А., Расин В.В., *Дискретная математика: графы, матроиды, алгоритмы. Учебное пособие. 2-е изд., испр. и доп.*, Санкт-Петербург–Москва–Краснодар: Лань, 2010, 368 с.
- [3] Викторенков В.Е., “Орграф полиномиального преобразования над коммутативным локальным кольцом”, *Обозр. прикл. и промышл. матем.*, **7:2** (2000), 327.
- [4] Викторенков В.Е., “О строении орграфов полиномиальных преобразований над конечными коммутативными кольцами с единицей”, *Дискретная математика*, **29:3** (2017), 3–23.
- [5] Ермилов Д.М., Козлитин О.А., “Цикловая структура полиномиального генератора над кольцом Галуа”, *Математические вопросы криптографии*, **4:1** (2013), 27–57.
- [6] Ермилов Д.М., Козлитин О.А., “О строении графа полиномиального преобразования кольца Галуа”, *Математические вопросы криптографии*, **6:3** (2015), 47–73.
- [7] Козлитин О.А., “Периодические свойства многомерного полиномиального генератора над кольцом Галуа, Γ ”, *Математические вопросы криптографии*, **9:3** (2018), 61–98.
- [8] Кузьмин А.С., Куракин В.Л., Нечаев А.А., “Псевдослучайные и полилинейные последовательности”, *Труды по дискретной математике*, **1** (1997), 139–202.
- [9] Ларин М.В., “Транзитивные полиномиальные преобразования колец вычетов”, *Дискретная математика*, **14:2** (2002), 20–32.
- [10] Parvatov N.G., “On the period length of vector sequences generated by polynomials modulo prime powers”, *Прикладная дискретная математика*, 2016, № 1(31), 57–61.