УДК 621.391:519.7+621.391.1:004.7

ПОКАЗАТЕЛЬ 2-ТРАНЗИТИВНОСТИ ОДНОГО КЛАССА ПОДСТАНОВОК КОНЕЧНОГО ПОЛЯ

Д. У. Эрнандес Пилото

ООО «Центр сертификационных исследований», г. Москва, Россия

А. В. Аборневым предложен класс подстановок простого поля, построенный с помощью разрядных функций над кольцом вычетов по модулю p^2. В данной работе рассматривается более широкий класс подстановок произвольного конечного поля, полученный заменой разрядных функций на произвольные отображения. Приводится оценка снизу показателя 2-транзитивности множества Σh, где Σ — регулярная группа подстановок, а h — подстановка из нового класса. Получены достаточные условия достижимости указанной оценки.

Ключевые слова: *подстановки конечных полей, транзитивные группы подстановок, показатель 2-транзитивности.*

DOI 10.17223/20710410/46/2

2-TRANSITIVITY DEGREE FOR ONE CLASS OF SUBSTITUTIONS OVER FINITE FIELDS

D. H. Hernández Piloto

Certification Research Center, Moscow, Russia

E-mail: dhhernandez2410@gmail.com

The paper deals with the class of substitutions proposed by A. V. Abornev, constructed using digit functions γ_1 over the ring $\mathbb{Z}_{p^2}$ of the form $h(\mathbf{x}) = \mathbf{z}$, where $\mathbf{z} = \mathbf{z}_1 + p\mathbf{z}_2$, $(\mathbf{z}_1|\mathbf{z}_2) = \gamma_1(\mathbf{x}K)$ and K is a matrix of dimensions $m \times 2m$. We consider a generalization of this class of substitutions using arbitrary functions $F : P^m \to P^m$ over finite field P in the place of the digit functions γ_1. A set Σ is called 2-transitive if for any pairs $\alpha = (a_1, a_2)$, $\beta = (b_1, b_2)$ in Σ there exists a substitution g, such that $g(a_i) = b_i$, $i \in \{1, 2\}$. We are interested in the degree of 2-transitivity of a group Σ, denoted by $d_2(\Sigma)$, which is equal to the smallest natural value k, such that $(\Sigma)^k$ is a 2-transitive group. The main goal is to find groups of substitutions with the minimum of this parameter. Using our construction, it is demonstrated that the degree of 2-transitivity is lower bounded by 4. When $F(x + a) - F(x)$ is a substitution for any $a \in P^m \backslash \{\mathbf{0}\}$, the degree of 2-transitivity of the composition Σh is equal to 4. In other papers these functions were called planar. Notice that in a field with characteristic 2 planar functions do not exist. If the characteristic is not 2, then these functions exist. Indeed, if Q is an extension of degree m of P, $\hat{F}(x) = x^2$ for all $x \in Q$, and $\alpha_1, \ldots, \alpha_m$ is the base of the vector space Q_P, then the function $F(x_1, \ldots, x_m) = \hat{F}(\alpha_1 x_1 + \ldots + \alpha_m x_m)$, $x_1, \ldots, x_m \in P$, is planar.

Keywords: *transitivity, degree of 2-transitivity, digit function, regular group, substitution.*

Введение

Пусть p — произвольное простое число и $R = \mathbb{Z}_{p^2}$ — кольцо вычетов по модулю p^2.

Определение 1. Подмножество $\Gamma(R) = \{a \in R : a^p = a\}$ называют p-адическим разрядным множеством кольца R.

Каждый элемент $a \in R$ однозначно представляется в виде $a = a_0 + pa_1$, $a_i \in \Gamma(R)$, $i \in \{0, 1\}$, называемом p-адическим разложением элемента a.

Определение 2. Отображения $\gamma_i : R \to \Gamma(R)$, $\gamma_i(a) = a_i$, $i \in \{0, 1\}$, будем называть p-адическими разрядными функциями, а элементы $a_i = \gamma_i(a)$ — p-адическими разрядами элемента a.

Для каждого вектора $\mathbf{a} = (a_1, \ldots, a_t) \in R^t$ определим вектор $\gamma_1(\mathbf{a}) = (\gamma_1(a_1), \ldots, \gamma_1(a_t))$. Обозначим через $R^*_{m,m}$ множество всех обратимых матриц порядка m над кольцом R.

Определение 3. Назовём матрицу K размера $m \times n$ над R разрядно-инъективной, если любая ненулевая строка $\mathbf{a} \in R^m$ однозначно восстанавливается по строке $\gamma_1(\mathbf{a}K) \in R^n$.

Теорема 1 [1]. Пусть $G \in R^*_{m,m}, U \in R^*_{m,m}$. Тогда матрица

$$K = U(E|E + pG)_{m \times 2m}$$

является разрядно-инъективной и отображение $h : R^m \to R^m$, действующее на произвольной строке $\mathbf{x} \in R^m$ по правилу

$$h(\mathbf{x}) = \mathbf{z}, \text{ где } \mathbf{z} = \mathbf{z}_1 + p\mathbf{z}_2 \in R^m, (\mathbf{z}_1|\mathbf{z}_2) = \gamma_1(\mathbf{x}K) \in R^{2m},$$

является подстановкой.

Используя p-адическое разложение, запишем матрицу U в виде $U = U_0 + pU_1$. Тогда

$$\begin{gathered}\gamma_1(\mathbf{x}K) = (\gamma_1((\mathbf{x_0} + p\mathbf{x_1})(U_0 + pU_1)), \gamma_1((\mathbf{x_0} + p\mathbf{x_1})(U_0 + p(U_1 + U_0G)))) = \\ = (\gamma_1(\mathbf{x_0}U_0) + \mathbf{x_0}U_1 + \mathbf{x_1}U_0, \gamma_1(\mathbf{x_0}U_0) + \mathbf{x_0}U_1 + \mathbf{x_1}U_0 + \mathbf{x_0}U_0G),\end{gathered}$$

где в правой части равенства сложение векторов осуществляется покоординатно в поле $\mathbb{Z}_p$. Следовательно, отображение h действует по правилу

$$(\mathbf{x_0}, \mathbf{x_1}) \mapsto (\gamma_1(\mathbf{x_0}U_0) + \mathbf{x_0}U_1 + \mathbf{x_1}U_0, \gamma_1(\mathbf{x_0}U_0) + \mathbf{x_0}U_1 + \mathbf{x_1}U_0 + \mathbf{x_0}U_0G). \tag{1}$$

Схематично отображение h представлено на рис. 1.

Таким образом, имеем следующую систему:

$$\begin{cases}\gamma_1(\mathbf{x_0}U_0) + \mathbf{x_0}U_1 + \mathbf{x_1}U_0 = \mathbf{a_0}, \\ \mathbf{a_0} + \mathbf{x_0}U_0G = \mathbf{a_1}.\end{cases}$$

Ввиду указанного строения стало очевидным, что вычисление прообраза подстановки сводится к решению системы линейных уравнений и имеет сложность $O(m^3)$ при $m \to \infty$.

В настоящей работе предлагается более общая конструкция, полученная заменой на рис. 1 блока, отмеченного пунктирными линиями, на произвольное отображение F. Построенные подстановки рассматриваются над произвольным конечным полем P.

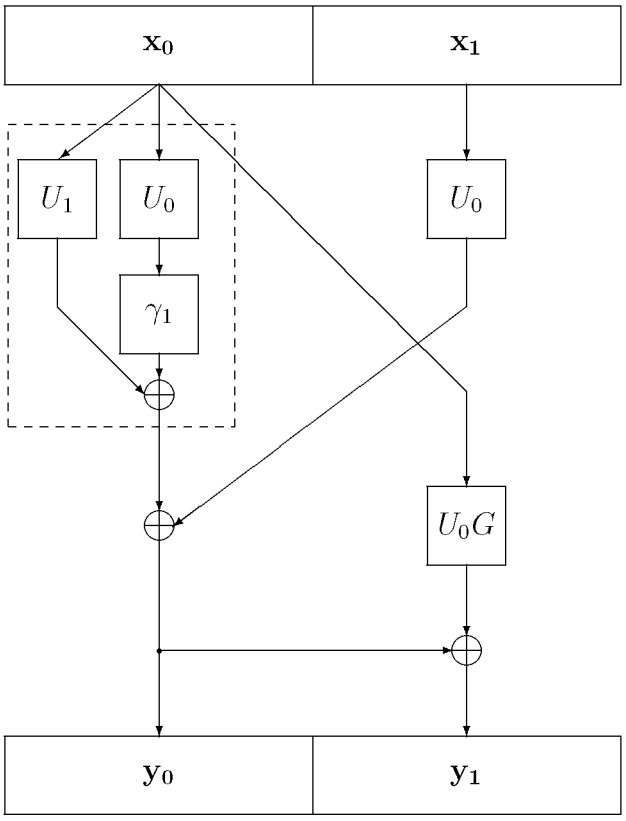

Рис. 1

1. Новая конструкция и ее свойства

Пусть P — произвольное конечное поле. Рассмотрим отображение $h : P^{2m} \to P^{2m}$, действующее по правилу

$$h(\mathbf{x_0}, \mathbf{x_1}) = (F(\mathbf{x_0}) + \mathbf{x_1}U, F(\mathbf{x_0}) + \mathbf{x_1}U + \mathbf{x_0}G), \tag{2}$$

где $\mathbf{x_0}, \mathbf{x_1} \in P^m$; $U, G \in P^*_{m,m}$; $F : P^m \to P^m$ — произвольное отображение. Схематично отображение h представлено на рис. 2.

Теорема 2. Отображение $h : P^{2m} \to P^{2m}$, определённое равенством (2), является подстановкой.

Доказательство. Достаточно показать, что отображение h инъективно. Пусть $\mathbf{a}, \mathbf{b} \in P^{2m}$ такие, что $h(\mathbf{a_0}, \mathbf{a_1}) = h(\mathbf{b_0}, \mathbf{b_1})$. Тогда $h(\mathbf{a_0}, \mathbf{a_1}) = (F(\mathbf{a_0}) + \mathbf{a_1}U, F(\mathbf{a_0}) + \mathbf{a_1}U + \mathbf{a_0}G)$, $h(\mathbf{b_0}, \mathbf{b_1}) = (F(\mathbf{b_0}) + \mathbf{b_1}U, F(\mathbf{b_0}) + \mathbf{b_1}U + \mathbf{b_0}G)$ и справедливы равенства

$$\begin{cases} F(\mathbf{a_0}) + \mathbf{a_1}U = \mathbf{c_0}, \\ \mathbf{c_0} + \mathbf{a_0}G = \mathbf{c_1}, \\ F(\mathbf{b_0}) + \mathbf{b_1}U = \mathbf{c_0}, \\ \mathbf{c_0} + \mathbf{b_0}G = \mathbf{c_1}. \end{cases}$$

Отсюда $\mathbf{c_0} + \mathbf{a_0}G = \mathbf{c_0} + \mathbf{b_0}G$, т. е. $\mathbf{a_0}G = \mathbf{b_0}G$, а значит, $\mathbf{a_0} = \mathbf{b_0}$. Теперь $F(\mathbf{a_0}) + \mathbf{a_1}U = F(\mathbf{b_0}) + \mathbf{b_1}U$, а так как $\mathbf{a_0} = \mathbf{b_0}$, то $\mathbf{a_1}U = \mathbf{b_1}U$ и, следовательно, $\mathbf{a_1} = \mathbf{b_1}$. ■

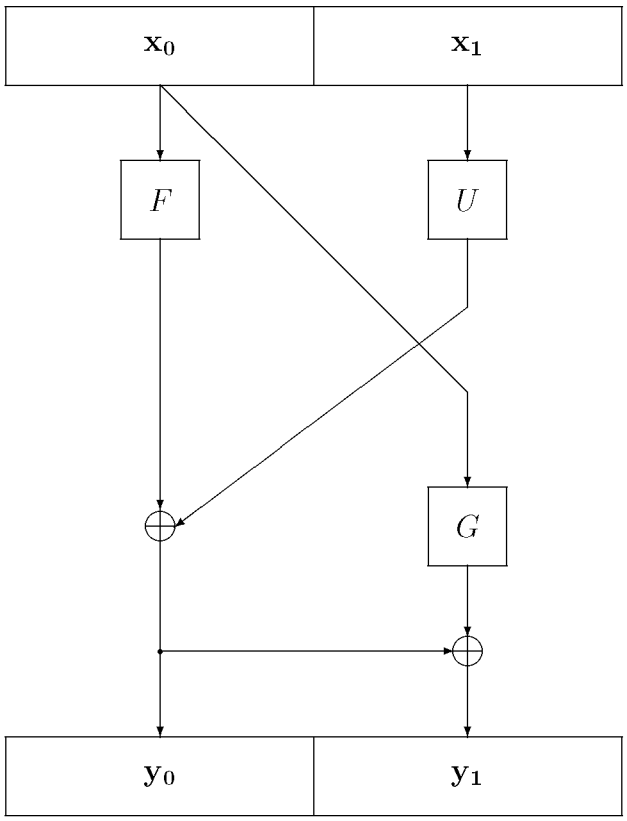

Рис. 2

Обозначим через $S(\Omega)$ симметрическую группу подстановок на множестве Ω.

Определение 4. Группа подстановок $\Sigma < S(\Omega)$ называется регулярной, если для любых $a, b \in \Omega$ в Σ существует единственная подстановка σ, удовлетворяющая условию $\sigma(a) = b$.

Рассмотрим произведение регулярной группы Σ на подстановку h.

Определение 5. Множество Σh называется 2-транзитивным, если для любых двух наборов $\alpha = (a_1, a_2), \beta = (b_1, b_2)$ из P^{2m} в Σh существует подстановка g, переводящая α в β, т. е. удовлетворяющая условию $g(a_i) = b_i$, $i \in \{1, 2\}$.

Определение 6. Показателем 2-транзитивности множества подстановок Σh называется число $d_2(\Sigma h)$, равное минимальному натуральному значению k, такому, что множество $(\Sigma h)^k$ является 2-транзитивным.

Интерес представляют подстановки с минимальным значением данного параметра. Согласно [2], достаточно рассмотреть матрицу Q_h переходов ненулевых разностей биграмм вида

$$(Q_h)_{(N-1)\times(N-1)} = \frac{1}{N}(\nu_{\mathbf{ab}})_{\mathbf{a},\mathbf{b}\in P^{2m}\setminus\theta},$$

где $\nu_{\mathbf{ab}} = |\{\mathbf{x} \in P^{2m} : h(\mathbf{x} + \mathbf{a}) - h(\mathbf{x}) = \mathbf{b}\}|$ и $N = |P^{2m}|$. Заметим, что для нахождения показателя 2-транзитивности достаточно описать степени матрицы Q_h, поскольку $d_2(\Sigma h) = k$ тогда и только тогда, когда $Q_h^{k-1} > 0$, а матрицы $Q_h^1, \ldots, Q_h^{k-2}$ содержат нулевые элементы.

Приведём некоторые факты из работы [1].

Утверждение 1. Элемент $\nu_{\mathbf{ab}}$ для матрицы Q_h равен числу решений системы уравнений

$$\begin{cases} \mathbf{b_0} = \gamma_1(\mathbf{a}U) + \gamma_1(\mathbf{x_0} + \gamma_0(\mathbf{a_0}U)), \\ \mathbf{b_1} = \mathbf{b_0} + \gamma_0(\mathbf{a}U)G - \gamma_1(\mathbf{x_1} + \mathbf{b_0}) \end{cases}$$

относительно $\mathbf{x_0}, \mathbf{x_1} \in \mathbb{Z}_p^m$.

Теорема 3. Пусть h — подстановка на $\mathbb{Z}_p^{2m}$, определённая равенством (1). Тогда $d_2(\Sigma h) \geqslant 4$.

Теорема 4. Пусть $p = 2$, $m \in \mathbb{N}$, подстановка h вида (1) выбрана так, что все миноры матрицы U_0 отличны от нуля. Тогда $d_2(\Sigma h) = 4$.

Получим аналоги этих утверждений применительно к новому классу подстановок. Пусть h — подстановка вида (2). Для оценки элементов $\nu_{\mathbf{ab}}$ матрицы Q_h используем

Утверждение 2. Элемент $\nu_{\mathbf{ab}}$ матрицы Q_h равен числу решений системы уравнений

$$\begin{cases} \mathbf{b_0} = F(\mathbf{x_0} + \mathbf{a_0}) - F(\mathbf{x_0}) + \mathbf{a_1}U, \\ \mathbf{b_1} = \mathbf{b_0} + \mathbf{a_0}G \end{cases}$$

относительно $\mathbf{x_0} \in P^m$.

Доказательство. Для произвольных обратимых матриц U, G, по определению, элемент $\nu_{\mathbf{ab}}$ есть число решений уравнения

$$\mathbf{b} = h(\mathbf{x} + \mathbf{a}) - h(\mathbf{x}) \tag{3}$$

относительно $\mathbf{x} \in P^{2m}$. Пользуясь (2), из (3) для строки $\mathbf{b} = (\mathbf{b_0}, \mathbf{b_1})$ получим равенство

$$\begin{gathered} h(\mathbf{x} + \mathbf{a}) - h(\mathbf{x}) = (F(\mathbf{x_0} + \mathbf{a_0}) + (\mathbf{x_1} + \mathbf{a_1})U, F(\mathbf{x_0} + \mathbf{a_0}) + (\mathbf{x_1} + \mathbf{a_1})U + (\mathbf{x_0} + \mathbf{a_0})G) - \\ -(F(\mathbf{x_0}) + \mathbf{x_1}U, F(\mathbf{x_0}) + \mathbf{x_1}U + \mathbf{x_0}G) = (F(\mathbf{x_0} + \mathbf{a_0}) + \mathbf{x_1}U + \mathbf{a_1}U, F(\mathbf{x_0} + \mathbf{a_0}) + \mathbf{x_1}U + \\ + \mathbf{a_1}U + \mathbf{x_0}G + \mathbf{a_0}G) - (F(\mathbf{x_0}) + \mathbf{x_1}U, F(\mathbf{x_0}) + \mathbf{x_1}U + \mathbf{x_0}G) = \\ = (F(\mathbf{x_0} + \mathbf{a_0}) - F(\mathbf{x_0}) + \mathbf{a_1}U, F(\mathbf{x_0} + \mathbf{a_0}) - F(\mathbf{x_0}) + \mathbf{a_1}U + \mathbf{a_0}G). \end{gathered}$$

Значит,

$$\begin{cases} \mathbf{b_0} = F(\mathbf{x_0} + \mathbf{a_0}) - F(\mathbf{x_0}) + \mathbf{a_1}U, \\ \mathbf{b_1} = \mathbf{b_0} + \mathbf{a_0}G. \end{cases}$$

Утверждение доказано. ■

Теорема 5. Пусть h—подстановка на P^{2m}, определённая равенством (2). Тогда $d_2(\Sigma h) \geqslant 4$.

Доказательство. Достаточно показать, что матрица Q_h^2 содержит нулевые элементы. Элементы $\nu_{\mathbf{ac}}^{(2)}$ матрицы Q_h^2 опишем, используя утверждение 2. Заметим, что

$$\nu_{\mathbf{ac}}^{(2)} = \frac{1}{N^2} \sum_{\mathbf{b} \in P^m} \nu_{\mathbf{ab}} \nu_{\mathbf{bc}}$$

и, согласно утверждению 2, произведение $\nu_{\mathbf{ab}}\nu_{\mathbf{bc}}$ равно числу решений $(\mathbf{x_0}, \mathbf{y_0}) \in (P^m)^2$ системы

$$\begin{cases} \mathbf{b_0} = F(\mathbf{x_0} + \mathbf{a_0}) - F(\mathbf{x_0}) + \mathbf{a_1}U, \\ \mathbf{b_1} = \mathbf{b_0} + \mathbf{a_0}G, \\ \mathbf{c_0} = F(\mathbf{y_0} + \mathbf{b_0}) - F(\mathbf{y_0}) + \mathbf{b_1}U, \\ \mathbf{c_1} = \mathbf{c_0} + \mathbf{b_0}G. \end{cases} \tag{4}$$

Элемент $\nu^{(2)}_{\mathbf{ac}}$ пропорционален числу решений системы (4) относительно системы независимых переменных $(\mathbf{x_0}, \mathbf{y_0}, \mathbf{b_0}, \mathbf{b_1}) \in (P^m)^4$. При этом условие $\nu^{(2)}_{\mathbf{ac}} > 0$ равносильно совместности системы (4) относительно последнего набора неизвестных. Покажем, что в матрице Q^2_h всегда есть нулевые элементы. Пусть $\mathbf{a_0} = \mathbf{c_0} = \mathbf{0}$. Первое и последнее уравнения системы (4) принимают следующий вид:

$$\begin{cases} \mathbf{b_0} = \mathbf{a_1}U, \\ \mathbf{c_1} = \mathbf{b_0}G. \end{cases}$$

Следствием данной системы является уравнение $\mathbf{c_1} = \mathbf{a_1}UG$. Пусть $\mathbf{a_1}, \mathbf{c_1} \in P^m$ выбраны так, что последнее равенство не выполняется. Тогда для $\mathbf{a_0} = \mathbf{c_0} = \mathbf{0}$ элемент $\nu^{(2)}_{\mathbf{ac}}$ равен нулю. ■

2. Условия для транзитивности и 2-транзитивности множества Σh

Пусть $\Sigma < S(\Omega)$ — регулярная группа подстановок и h — произвольная подстановка из $S(\Omega)$. Тогда несложно заметить, что произведение Σh является регулярным множеством подстановок, и, как следствие, оно транзитивно.

Теорема 6. Пусть $F(\mathbf{x}+\mathbf{f}) - F(\mathbf{x})$ для любого $\mathbf{f} \in P^m \backslash \{\mathbf{0}\}$ является подстановкой на P^m. Тогда для любой подстановки h вида (2) выполнено равенство $d_2(\Sigma h) = 4$.

Доказательство. Достаточно доказать, что $Q^3_h > 0$. Опишем элементы $\nu^{(3)}_{\mathbf{ad}}$ матрицы Q^3_h, используя утверждение 2. Заметим, что

$$\nu^{(3)}_{\mathbf{ad}} = \frac{1}{N^3} \sum_{\mathbf{b},\mathbf{c} \in P^m} \nu_{\mathbf{ab}} \nu_{\mathbf{bc}} \nu_{\mathbf{cd}}$$

и, согласно утверждению 2, произведение $\nu_{\mathbf{ab}}\nu_{\mathbf{bc}}\nu_{\mathbf{cd}}$ равно числу решений $(\mathbf{x_0}, \mathbf{y_0}, \mathbf{z_0}) \in \in (P^m)^3$ системы

$$\begin{cases} \mathbf{b_0} = F(\mathbf{x_0} + \mathbf{a_0}) - F(\mathbf{x_0}) + \mathbf{a_1}U, \\ \mathbf{b_1} = \mathbf{b_0} + \mathbf{a_0}G, \\ \mathbf{c_0} = F(\mathbf{y_0} + \mathbf{b_0}) - F(\mathbf{y_0}) + \mathbf{b_1}U, \\ \mathbf{c_1} = \mathbf{c_0} + \mathbf{b_0}G, \\ \mathbf{d_0} = F(\mathbf{z_0} + \mathbf{c_0}) - F(\mathbf{z_0}) + \mathbf{c_1}U, \\ \mathbf{d_1} = \mathbf{d_0} + \mathbf{c_0}G, \end{cases} \tag{5}$$

а $\nu^{(3)}_{\mathbf{ad}}$ пропорционально числу решений системы (5) относительно системы независимых переменных $(\mathbf{x_0}, \mathbf{y_0}, \mathbf{z_0}, \mathbf{b_0}, \mathbf{b_1}, \mathbf{c_0}, \mathbf{c_1}) \in (P^m)^7$. При этом условие $\nu^{(3)}_{\mathbf{ad}} > 0$ равносильно совместности системы (5) относительно последнего набора неизвестных. Покажем, что в условиях теоремы неравенство $\nu^{(3)}_{\mathbf{ad}} > 0$ выполняется при всех $\mathbf{a}, \mathbf{d} \in P^m \backslash \mathbf{0}$. Из пятого и шестого уравнений системы (5) можно выразить переменные $\mathbf{c_0}, \mathbf{c_1}$ соответственно через остальные переменные следующим образом:

$$\mathbf{c_0} = (\mathbf{d_1} - \mathbf{d_0})G^{-1},$$
$$\mathbf{c_1} = (\mathbf{d_0} - (F(\mathbf{z_0} + \mathbf{c_0}) - F(\mathbf{z_0})))U^{-1}.$$

Подставив в третье и пятое уравнения выражения для $\mathbf{b_1}, \mathbf{c_1}$ из второго и четвертого уравнений соответственно, получим

$$F(\mathbf{y_0} + \mathbf{b_0}) - F(\mathbf{y_0}) = \mathbf{c_0} - \mathbf{b_0}U - \mathbf{a_0}GU,$$
$$F(\mathbf{z_0} + \mathbf{c_0}) - F(\mathbf{z_0}) = \mathbf{d_0} - \mathbf{c_0}U - \mathbf{b_0}GU.$$

Из приведённых рассуждений следует, что система (5) равносильна системе уравнений

$$\begin{cases} F(\mathbf{y}_0 + \mathbf{b}_0) - F(\mathbf{y}_0) = \mathbf{c}_0 - \mathbf{b}_0 U - \mathbf{a}_0 GU, \\ F(\mathbf{z}_0 + \mathbf{c}_0) - F(\mathbf{z}_0) = \mathbf{d}_0 - \mathbf{c}_0 U - \mathbf{b}_0 GU, \\ \mathbf{b}_0 = F(\mathbf{x}_0 + \mathbf{a}_0) - F(\mathbf{x}_0) + \mathbf{a_1} U, \\ \mathbf{c}_0 = (\mathbf{d_1} - \mathbf{d}_0) G^{-1}, \\ \mathbf{b_1} = \mathbf{b}_0 + \mathbf{a}_0 G, \\ \mathbf{c_1} = (\mathbf{d}_0 - (F(\mathbf{z}_0 + \mathbf{c}_0) - F(\mathbf{z}_0))) U^{-1} \end{cases} \tag{6}$$

и совместна тогда и только тогда, когда совместна система из первых четырёх уравнений системы (6). Пусть $\mathbf{a} \in P^m \backslash \mathbf{0}$ — произвольный вектор. Покажем, что в уравнении

$$\mathbf{b}_0 = F(\mathbf{x}_0 + \mathbf{a}_0) - F(\mathbf{x}_0) + \mathbf{a_1} U$$

найдётся $\mathbf{x}_0 \in P^m$, при котором $\mathbf{b}_0 \neq \mathbf{0}$. Для доказательства рассмотрим два случая:

1) Пусть $\mathbf{a}_0 = \mathbf{0}$, тогда $\mathbf{b}_0 = \mathbf{a_1} U \neq \mathbf{0}$.

2) Если $\mathbf{a}_0 \neq \mathbf{0}$, то существование искомого $\mathbf{x}_0$ следует из того, что $F(\mathbf{x}_0 + \mathbf{a}_0) - F(\mathbf{x}_0)$ не является константой. Зафиксируем произвольные $\mathbf{a}, \mathbf{d} \in P^m \backslash \mathbf{0}$. Элемент $\mathbf{x}_0 \in P^m$ выберем так, чтобы выполнялось условие $\mathbf{b}_0 \neq \mathbf{0}$. Если $\mathbf{c}_0 \neq \mathbf{0}$, то получим систему

$$\begin{cases} F(\mathbf{y}_0 + \mathbf{b}_0) - F(\mathbf{y}_0) = \mathbf{c}_0 - \mathbf{b}_0 U - \mathbf{a}_0 GU, \\ F(\mathbf{z}_0 + \mathbf{c}_0) - F(\mathbf{z}_0) = \mathbf{d}_0 - \mathbf{c}_0 U - \mathbf{b}_0 GU, \end{cases} \tag{7}$$

совместную по выбору F. Если $\mathbf{c}_0 = \mathbf{0}$, то

$$\begin{cases} F(\mathbf{y}_0 + \mathbf{b}_0) - F(\mathbf{y}_0) = -\mathbf{b}_0 U - \mathbf{a}_0 GU, \\ \mathbf{d}_0 = \mathbf{b}_0 GU. \end{cases} \tag{8}$$

Преобразовав второе уравнение с использованием уравнений из системы (5)

$$\mathbf{d}_0 = (\mathbf{b_1} - \mathbf{a}_0 G) GU = \mathbf{b_1} GU - \mathbf{a}_0 G^2 U = (-(F(\mathbf{y}_0 + \mathbf{b}_0) - F(\mathbf{y}_0)) U^{-1}) GU - \mathbf{a}_0 G^2 U,$$

получим

$$\mathbf{d}_0 = -(F(\mathbf{y}_0 + \mathbf{b}_0) - F(\mathbf{y}_0)) U^{-1} GU - \mathbf{a}_0 G^2 U.$$

Тогда

$$F(\mathbf{y}_0 + \mathbf{b}_0) - F(\mathbf{y}_0) = -d_0 U^{-1} G^{-1} U - \mathbf{a}_0 GU = -(\mathbf{b}_0 GU) U^{-1} G^{-1} U - \mathbf{a}_0 GU = -\mathbf{b}_0 U - \mathbf{a}_0 GU.$$

Получили первое уравнение из (8), и, аналогично (7), система совместна. Таким образом, доказано, что все элементы матрицы Q_h^3 положительны. ■

Отметим, что в случае поля характеристики 2 не существует отображений F, удовлетворяющих условию теоремы 6. Если характеристика поля отлична от 2, то такие отображения существуют. Действительно, пусть Q — расширение поля P степени m, $\hat{F}(x) = x^2$ для всех $x \in Q$. Тогда если $\alpha_1, \ldots, \alpha_m$ — базис векторного пространства Q_P, то условиям теоремы 6 удовлетворяет отображение $F(x_1, \ldots, x_m) = \hat{F}(\alpha_1 x_1 + \ldots + \alpha_m x_m)$, $x_1, \ldots, x_m \in P$. Функции, удовлетворяющие условию теоремы 6, названы в работе [3] планарными. В этой работе приводится обзор известных результатов о планарных функциях и указаны широкие классы рассматриваемых функций.

Заключение

Построен новый класс подстановок, обобщающий подстановки, предложенные в [1]. Удалось оценить снизу показатель 2-транзитивности для произведения регулярной группы подстановок на произвольную подстановку нового класса. Приведены достаточные условия обращения доказанной оценки в равенство.

Автор выражает благодарность И. В. Чередникy за постановку задачи и внимание к работе.

ЛИТЕРАТУРА

1. *Аборнев А. В.* Подстановки, индуцированные разрядно-инъективными преобразованиями модуля над кольцом Галуа // Прикладная дискретная математика. 2013. № 4. С. 5–15.
2. *Глухов М. М.* О 2-транзитивности произведения регулярных групп подстановок // Труды по дискретной математике. М.: Физматлит, 2000. С. 37–52.
3. *Глухов М. М.* О приближении дискретных функций линейными функциями // Математические вопросы криптографии. 2016. Т. 7. № 4. С. 29–50.

REFERENCES

1. *Abornev A. V.* Podstanovki, indutsirovannye razryadno-inektivnymi preobrazovaniyami modulya nad koltsom Galua [Substitutions induced by digit-injective transformations of a module over a Galois ring]. Prikladnaya Diskretnaya Matematika, 2013, no. 4, pp. 5–15. (in Russian)
2. *Glukhov M. M.* O 2-tranzitivnosti proizvedeniya regulyarnykh grupp podstanovok [On 2-transitivity of the composition of regular substitution groups]. Trudy po Diskretnoy Matematike. Moscow, Fizmatlit Publ., 2000, pp. 37–52. (in Russian)
3. *Glukhov M. M.* O priblizhenii diskretnykh funktsiy lineynymi funktsiyami [On the approximation of discrete functions by linear functions]. Matematicheskie Voprosy Kriptografii, 2016, vol. 7, no. 4, pp. 29–50. (in Russian)