

ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

DOI 10.17223/20710410/23/2

УДК 512.6

ПОСТРОЕНИЕ ПОДСТАНОВОК С ИСПОЛЬЗОВАНИЕМ РАЗРЯДНО-ПОДСТАНОВОЧНЫХ ПРЕОБРАЗОВАНИЙ МОДУЛЯ НАД КОЛЬЦОМ ГАЛУА ХАРАКТЕРИСТИКИ 4

А. В. Аборнев

*ООО «Центр сертификационных исследований», г. Москва, Россия***E-mail:** abconf.c@gmail.com

Решается задача построения нелинейных подстановок на пространстве большой размерности с использованием только матрицы над кольцом Галуа характеристики 4 и разрядной функции этого кольца. Каждая такая подстановка может быть представлена как вектор-функция, у которой координатными функциями являются многочлены над полем. Ранее был анонсирован результат о построении подстановок из рассматриваемого класса, у которых ровно две координатные функции являются нелинейными. Здесь приводится полное доказательство этого результата.

Ключевые слова: *разрядно-подстановочная матрица, подстановка, кольцо Галуа.*

Введение

Пусть $R = \text{GR}(q^2, p^2)$ — кольцо Галуа мощности q^2 , характеристики p^2 с полем вычетов $\bar{R} = R/pR = \text{GF}(q)$, $q = p^r$. В частности, при $r = 1$ имеем $R = \mathbb{Z}_{p^2}$. Подмножество $P = \Gamma(R) = \{a \in R : a^q = a\}$ называют *p-адическим координатным множеством*, или *координатным множеством Тейхмюллера* кольца R . Будем называть его также *разрядным* множеством.

Каждый элемент $a \in R$ однозначно представляется в виде

$$a = a_0 + pa_1, \quad a_s \in P, \quad s \in \{0, 1\},$$

называемом *p-адическим разложением элемента a*. Отображения

$$\gamma_s : R \rightarrow P, \quad \gamma_s(a) = a_s, \quad s \in \{0, 1\},$$

будем называть *разрядными функциями в разрядном множестве P*, а элементы $a_s = \gamma_s(a)$ — *p-адическими разрядами элемента a*.

Алгебра $(P, \oplus, \cdot)$ с операцией сложения $a \oplus b = \gamma_0(a + b)$, $a, b \in P$, является полем.

Понятия *p-адического разложения* и значения функции γ_s естественным образом (поэлементно) распространяются на матрицы $A \in R_{m \times m}$. При этом мы используем обозначение $A_s = \gamma_s(A) = (a_s(ij))$. Таким же естественным образом операции $\oplus, \cdot$ распространяются на матрицы над полем P , при этом операцию умножения матриц над полем обозначим через $\odot$.

Каждая матрица $A \in R_{m,m}$ определяет отображение $\pi_A : P^m \rightarrow P^m$

$$\pi_A(\mathbf{y}) = \gamma_1(\mathbf{y}A^T) = \gamma_1(\mathbf{y}A_0^T) \oplus (\mathbf{y} \odot A_1^T) = (\psi_1(\mathbf{y}), \dots, \psi_m(\mathbf{y})), \quad \mathbf{y} \in P^m, \quad (1)$$

где $\psi_1, \dots, \psi_m$ — координатные функции и T — оператор транспонирования. Будем говорить, что π_A — *нелинейное* отображение, если оно не является гомоморфизмом группы $(P^m, \oplus)$.

В работе [1] было впервые показано, что для любого $m > 1$ существует обратимая матрица A , такая, что π_A является нелинейной подстановкой на пространстве P^m .

Если π_A — подстановка, то система функций $\psi_1, \dots, \psi_m$ в (1) называется *ортогональной* [2], матрица A при этом называется *разрядно-подстановочной* (или *РП-матрицей*).

Координатные функции $\psi_1, \dots, \psi_m$ в (1) суть многочлены над полем P от переменных $\mathbf{y} = (y_1, \dots, y_m) \in P^m$ вида

$$\psi_i(\mathbf{y}) = \gamma_1(a_0(i1)y_1 + \dots + a_0(im)y_m) \oplus l_i(\mathbf{y}), \quad i = 1, \dots, m, \quad (2)$$

где $l_i(\mathbf{y}) = a_1(i1)y_1 \oplus \dots \oplus a_1(im)y_m$ — линейные функции; γ_1 — однородный многочлен степени q над P . Для $p = 2$ имеем

$$\gamma_1(a_0(i1)y_1 + \dots + a_0(im)y_m) = \sigma_2(a_0(i1)y_1, \dots, a_0(im)y_m)^h, \quad (3)$$

где $h = 2^{r-1}$, $\sigma_2(x_1, \dots, x_m) = \sum_{1 \leq j < k \leq m} \oplus x_j x_k$ — элементарная симметрическая функция порядка 2 [3].

Вообще говоря, координатная функция $\psi_i(\mathbf{y})$ не является линейной тогда и только тогда, когда i -я строка матрицы A содержит более чем один обратимый элемент.

Всюду далее $R = \text{GR}(q^2, 4)$. Пусть $q = 2^r$, $A = A_0 + 2A_1$, $A_s = (a_s(ij)) \in P_{m,m}$, $s = 0, 1$. Сделаем невырожденную замену переменных $x_j^2 = y_j$, $j = 1, \dots, m$, в (2). Пользуясь (3), получаем, что ортогональность исходной системы (1) эквивалентна ортогональности следующей системы квадратичных функций от переменных $\mathbf{x} = (x_1, \dots, x_m)$:

$$g_i(\mathbf{x}) = \sigma_2(a_0^h(i1)x_1, \dots, a_0^h(im)x_m) \oplus d_i(\mathbf{x}), \quad i = 1, \dots, m, \quad (4)$$

где $d_i(\mathbf{x}) = \sum_{j=1}^m \oplus a_1(ij)x_j^2$, $i = 1, \dots, m$, — *диагональные* квадратичные функции. Очевидно, любая ортогональная система (4) соответствует некоторой РП-матрице. Таким образом, задача построения РП-матриц в рассматриваемом случае эквивалентна задаче построения ортогональных систем (4).

В общем случае задача построения ортогональных систем многочленов не решена. Однако известны системы многочленов Диксона [2] и регулярные системы вида $g(\mathbf{x})$, $g(\mathbf{x}S)$, $\dots$, $g(\mathbf{x}S^{m-1})$, где g — квадратичная функция, существенно зависящая от переменных x_1, x_2, x_3 ; S — сопровождающая матрица некоторого многочлена степени m над P [4].

Основные результаты

Сначала опишем линейные преобразования, которые сохраняют свойство матрицы быть разрядно-подстановочной.

Рассмотрим множество Π_m всех разрядно-подстановочных матриц над кольцом R размера $m \times m$. Преобразование $\varphi : R_{m,m} \rightarrow R_{m,m}$ будем называть *Π-стабильным*, если выполнено условие

$$(A \in \Pi_m) \iff (\varphi(A) \in \Pi_m).$$

Утверждение 1. Множество линейных Π -стабильных преобразований содержит следующие элементарные преобразования:

- 1) перестановка строк (столбцов) матрицы;
- 2) умножение строки (столбца) матрицы на элемент из $\Gamma(R)^*$.

Доказательство. Для доказательства достаточно заметить, что матрица является разрядно-подстановочной тогда и только тогда, когда система координатных функций соответствующей подстановки ортогональна. Действительно, указанные преобразования строк матрицы A равносильны соответствующим преобразованиям многочленов в системе (2). Перестановка столбцов эквивалентна перестановке переменных $x_1, \dots, x_m$.

Пусть теперь φ — умножение k -го столбца матрицы A на $c \in \Gamma(R)^*$. Положим $A' = \varphi(A)$. В этом случае отображение $\pi_{A'}$ задается системой многочленов

$$\psi'_i(x_1, \dots, x_m) = a_1(i1)x_1 \oplus \dots \oplus ca_1(ik)x_k \oplus \dots \oplus a_1(im)x_m \oplus \bigoplus_{(j_1 \dots j_m) \in I(m,p)} \frac{1}{j_1! \dots j_m!} (a_0(i1)x_1)^{h_{j_1}} \dots (ca_0(ik)x_k)^{h_{j_k}} \dots (a_0(im)x_m)^{h_{j_m}},$$

где $i = 1, \dots, m$. Очевидно, невырожденная замена переменных $y_k = cx_k$, $y_j = x_j$, $j \neq k$ сохраняет свойство ортогональности системы многочленов. При этом полученная система многочленов $\psi_i(y_1, \dots, y_m)$, $i = 1, \dots, m$, является системой координатных функций преобразования π_A . ■

Будем называть преобразования матриц из теоремы 1 *мономиальными*. Назовём *мономиальной* матрицу вида

$$\begin{pmatrix} a_1 \vec{E}_{i_1} \\ \vdots \\ a_m \vec{E}_{i_m} \end{pmatrix},$$

где $(i_1, \dots, i_m)$ — перестановка чисел от 1 до m ; $\vec{E}_k$ — k -я строка единичной матрицы; $a_k \in \Gamma(R)^*$, $k = 1, \dots, m$.

Очевидно, мономиальное преобразование системы строк (столбцов) матрицы равносильно умножению её на соответствующую мономиальную матрицу слева (справа).

Следствие 1. Умножение матрицы A слева (справа) на мономиальную матрицу является Π -стабильным преобразованием.

Будем говорить, что матрицы $A, B \in R_{m,m}$ *мономиально-эквивалентны*, если B получается из A применением конечного набора мономиальных преобразований. Так как произведение мономиальных матриц и матрица, обратная к мономиальной, также есть мономиальная матрица, то отношение мономиальной эквивалентности рефлексивно, симметрично и транзитивно, и мономиальная эквивалентность матриц A, B равносильна условию $B = M_1 A M_2$, где M_1, M_2 — мономиальные матрицы.

В связи со сказанным для описания множества Π_m достаточно в каждом классе мономиально-эквивалентных матриц из $R_{m,m}$ найти удобный для анализа элемент и проверить его принадлежность множеству Π_m .

Приведём необходимые результаты из теории квадратичных функций [5, 6]. Для любой квадратичной функции $g : P^m \rightarrow P$ билинейная функция $f : P^m \times P^m \rightarrow P$ вида

$$f(\mathbf{x}, \mathbf{y}) = g(\mathbf{x} \oplus \mathbf{y}) \oplus g(\mathbf{x}) \oplus g(\mathbf{y}) \quad (5)$$

называется *билинейной функцией, ассоциированной с g* .

Множество всех квадратичных функций, ассоциированных с одной и той же билинейной функцией f , есть множество всех функций вида $g(\mathbf{x}) \oplus d(\mathbf{x})$, где $d : P^m \rightarrow P$ — диагональная квадратичная функция. Подпространство $V_f^\perp = \{\mathbf{a} \in P^m : f(P^m, \mathbf{a}) = 0\}$ называется *ядром* f . Из (5) получаем свойство полулинейности ограничения g на $V_f^\perp$:

$$\forall a, b \in P \quad \forall \mathbf{u} \in V_f^\perp \quad (g(a\mathbf{x} \oplus b\mathbf{u}) = a^2 g(\mathbf{x}) \oplus b^2 g(\mathbf{u})). \quad (6)$$

Пусть $g_1, \dots, g_k$ — некоторая система квадратичных функций с ассоциированными билинейными функциями $f_1, \dots, f_k$ соответственно. Обозначим через $\mathcal{L}(g_1, \dots, g_k)$ множество, состоящее из $\mathbf{0}$ и всех векторов $\mathbf{b} \in P^m$, удовлетворяющих условию

$$\exists (c_1, \dots, c_k) \in P^k \setminus \{0\} \quad (\mathbf{b} \in V_{c_1 f_1 \oplus \dots \oplus c_k f_k}^\perp, (c_1 g_1 \oplus \dots \oplus c_k g_k)(\mathbf{b}) \neq 0).$$

В работе [1] предлагается следующий способ построения ортогональных систем квадратичных функций.

Рассмотрим систему

$$g_1(x_1, \dots, x_m), \dots, g_k(x_1, \dots, x_m) \quad (7)$$

квадратичных функций и систему диагональных квадратичных функций

$$d_{k+1}, \dots, d_m. \quad (8)$$

Заметим, что подпространство

$$K = \{\mathbf{x} : d_i(\mathbf{x}) = 0, i = k+1, \dots, m\} \quad (9)$$

удовлетворяет условию $\dim K \geq k$, и $\dim K = k$, если и только если система (8) линейно независима.

Теорема 1 [1]. Для системы (7) следующие утверждения эквивалентны:

- 1) Существует система диагональных квадратичных функций (8), такая, что система $g_1, \dots, g_k, d_{k+1}, \dots, d_m$ ортогональна.
- 2) Существует система диагональных квадратичных функций (8) такая, что подпространство (9) удовлетворяет условиям

$$\dim K = k, K \subseteq \mathcal{L}(g_1, \dots, g_k). \quad (10)$$

- 3) Существует подпространство $K \leqslant_P P^m$, удовлетворяющее (10).

Многочлен $g \in P[x_1, \dots, x_m]$ называется *сбалансированным*, если для каждого $a \in P$ уравнение $g(\mathbf{x}) = a$ имеет $|P|^{m-1}$ решений.

Дополнение уже двух квадратичных функций до ортогональной системы является более сложной задачей. Зафиксируем числа $1 < s \leqslant k < t \leqslant m$. Ниже для любого $m > 2$ описаны системы из двух квадратичных функций

$$\begin{cases} g_1(x_1, \dots, x_m) = \sigma_2(x_1, \dots, x_k) \oplus d_{11}x_1^2 \oplus \dots \oplus d_{1m}x_m^2, \\ g_2(x_1, \dots, x_m) = \sigma_2(x_s, \dots, x_t) \oplus d_{21}x_1^2 \oplus \dots \oplus d_{2m}x_m^2, \end{cases} \quad (11)$$

которые дополняются некоторыми диагональными квадратичными функциями $d_3, \dots, d_m$ до ортогональной системы

$$\begin{aligned} g_1 &= \sigma_2(x_1, \dots, x_k) \oplus d_{11}x_1^2 \oplus \dots \oplus d_{1m}x_m^2, \\ g_2 &= \sigma_2(x_s, \dots, x_t) \oplus d_{21}x_1^2 \oplus \dots \oplus d_{2m}x_m^2, \\ d_3 &= d_{31}x_1^2 \oplus \dots \oplus d_{3m}x_m^2, \\ &\vdots \\ d_m &= d_{m1}x_1^2 \oplus \dots \oplus d_{mm}x_m^2. \end{aligned} \quad (12)$$

Такая система определяет РП-матрицу $A = A_0 + 2A_1 \in R_{m,m}$, где $A_1 = (d_{ij})$, A_0 — обратимая матрица вида

$$A_0 = \begin{pmatrix} \underbrace{e \dots e}_k 0 \dots 0 \\ 0 \dots 0 \underbrace{e \dots e}_{t-s+1} 0 \dots 0 \\ \dots \end{pmatrix}$$

и каждая из строк A_0 с номерами $i \in \{3, \dots, m\}$ содержит ровно по одному ненулевому элементу.

Обозначим через $f_{n,l}(\mathbf{x}, \mathbf{y})$, $1 \leq n < l \leq m$, билинейную функцию, ассоциированную с $\sigma_2(x_n, \dots, x_l)$ в P^m . Для чисел s, k, t из (11) определим ядро: $V_0^\perp = V_{f_{1,k}}^\perp \cap V_{f_{s,t}}^\perp$.

Теорема 2. Для системы (11) тогда и только тогда существует система функций (12), такая, что

$$\Pi = (g_1, g_2, d_3, \dots, d_m) : P^m \rightarrow P^m \quad (13)$$

является биекцией, когда существует пара векторов $\mathbf{u}, \mathbf{v} \in P^m$, удовлетворяющая одному из следующих условий 1–6:

1. а) $\mathbf{u}, \mathbf{v} \in V_0^\perp$,
б) система векторов $\{(g_1(\mathbf{u}), g_2(\mathbf{u})), (g_1(\mathbf{v}), g_2(\mathbf{v}))\}$ линейно независима над P ;
2. а) $\mathbf{u} \in V_0^\perp$, $\mathbf{v} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp \setminus V_0^\perp$ для некоторых $c_1, c_2 \in P$,
б) $(g_1(\mathbf{u}), g_2(\mathbf{u})) \neq (0, 0)$, $(c_1 g_1 \oplus c_2 g_2)(\mathbf{u}) = 0$, $(c_1 g_1 \oplus c_2 g_2)(\mathbf{v}) \neq 0$;
3. а) $s-1 \equiv t-k \equiv k-s+1 \equiv 1 \pmod{2}$ и

$$\begin{aligned} \mathbf{u} &= (0, \dots, 0, 0, \dots, 0, e, \dots, e, *, \dots, *), \\ \mathbf{v} &= (\underbrace{e, \dots, e}_{s-1}, \underbrace{0, \dots, 0}_{k-s+1}, \underbrace{0, \dots, 0}_{t-k+1}, *, \dots, *), \end{aligned}$$

- б) многочлен $D_1(x) = g_1(\mathbf{u}) \oplus x g_2(\mathbf{u}) \oplus x^2 g_1(\mathbf{v}) \oplus x^3 g_2(\mathbf{v})$ не имеет корней в P , $g_2(\mathbf{v}) \neq 0$;
4. а) $s-1 \equiv t-k \equiv 1 \pmod{2}$, $k-s+1 \equiv 0 \pmod{2}$ и

$$\begin{aligned} \mathbf{u} &= (e, \dots, e, e, \dots, e, \delta_1, \dots, \delta_1, *, \dots, *), \\ \mathbf{v} &= (\underbrace{\delta_2, \dots, \delta_2}_{s-1}, \underbrace{e, \dots, e}_{k-s+1}, \underbrace{e, \dots, e}_{t-k+1}, *, \dots, *), \end{aligned}$$

где $\delta_1 \neq e$, $\delta_2 \neq e$,

- б) многочлен $D_2(x) = g_1(\mathbf{u}) \oplus x \frac{\delta_2 \oplus e}{\delta_1 \oplus e} g_2(\mathbf{u}) \oplus x^2 g_1(\mathbf{v}) \oplus x^3 \frac{\delta_2 \oplus e}{\delta_1 \oplus e} g_2(\mathbf{v})$ не имеет корней в P , $g_2(\mathbf{v}) \neq 0$;
5. а) $s-1 \equiv 1 \pmod{2}$, $t-k \equiv k-s+1 \equiv 0 \pmod{2}$ и

$$\begin{aligned} \mathbf{u} &= (e, \dots, e, e, \dots, e, 0, \dots, 0, *, \dots, *), \\ \mathbf{v} &= (\underbrace{e, \dots, e}_{s-1}, \underbrace{0, \dots, 0}_{k-s+1}, \underbrace{0, \dots, 0}_{t-k+1}, *, \dots, *), \end{aligned}$$

- б) многочлен $D_3(x) = g_1(\mathbf{u}) \oplus x g_2(\mathbf{u}) \oplus x^2 g_1(\mathbf{v}) \oplus x^3 g_2(\mathbf{v})$ не имеет корней в P , $g_2(\mathbf{v}) \neq 0$;

6. а) $s - 1 \equiv 0 \pmod{2}$, $t - k \equiv 1 \pmod{2}$, $k - s + 1 \equiv 0 \pmod{2}$ и

$$\mathbf{u} = (\underbrace{0, \dots, 0}_{s-1}, \underbrace{0, \dots, 0}_{k-s+1}, \underbrace{e, \dots, e}_{t-k+1}, *, \dots, *),$$

$$\mathbf{v} = (0, \dots, 0, e, \dots, e, e, \dots, e, *, \dots, *),$$

- б) многочлен $D_4(x) = g_1(\mathbf{u}) \oplus x g_2(\mathbf{u}) \oplus x^2 g_1(\mathbf{v}) \oplus x^3 g_2(\mathbf{v})$ не имеет корней в P , $g_2(\mathbf{v}) \neq 0$.

Доказательство. По теореме 1, пара квадратичных функций g_1, g_2 дополняется некоторыми диагональными квадратичными функциями $d_3, \dots, d_m$ до биекции (13) тогда и только тогда, когда существует подпространство $K < P^m$, такое, что

$$K \subset \mathcal{L}(g_1, g_2), \quad \dim K = 2. \quad (14)$$

Заметим, что $\mathcal{L}(g_1, g_2)$ состоит из $\mathbf{0}$ и всех векторов $\mathbf{b} \in P^m$, удовлетворяющих условию

$$\exists (c_1, c_2) \in P^2 \setminus \{\mathbf{0}\} \quad \left(\mathbf{b} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp, \quad (c_1 g_1 \oplus c_2 g_2)(\mathbf{b}) \neq 0 \right). \quad (15)$$

Достаточность. Для каждого пункта 1–6 теоремы покажем, что если выполнено условие подпункта а и $K = \langle \mathbf{u}, \mathbf{v} \rangle$, то (14) равносильно условию подпункта б. Тогда достаточность условий теоремы будет доказана.

1. Пусть $\mathbf{u}, \mathbf{v} \in V_0^\perp$ и $\varphi : P \rightarrow P$ — автоморфизм Фробениуса: $\varphi(x) = x^2$. Заметим, что $V_0^\perp = \bigcap_{(c_1, c_2) \neq (0,0)} V_{c_1 f_1 \oplus c_2 f_2}^\perp$. Следовательно, ввиду (15)

$$\forall \mathbf{b} \in V_0^\perp \quad (\mathbf{b} \in \mathcal{L}(g_1, g_2) \Leftrightarrow (g_1(\mathbf{b}), g_2(\mathbf{b})) \neq (0, 0)),$$

и из (6) получаем, что линейная независимость векторов $(g_1(\mathbf{u}), g_2(\mathbf{u})), (g_1(\mathbf{v}), g_2(\mathbf{v}))$ эквивалентна условию

$$\forall (c_1, c_2) \in P^2 \setminus \{\mathbf{0}\} \quad ((g_1(c_1^h \mathbf{u} \oplus c_2^h \mathbf{v}), g_2(c_1^h \mathbf{u} \oplus c_2^h \mathbf{v})) \neq (0, 0)),$$

где $h = q/2 = 2^{r-1}$, то есть $K = \langle \mathbf{u}, \mathbf{v} \rangle \subset \mathcal{L}(g_1, g_2)$ и $\dim K = 2$.

2. Пусть $\mathbf{u} \in V_0^\perp$, $\mathbf{v} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp$ для $(c_1, c_2) \in P^2 \setminus \{\mathbf{0}\}$. Из (15) и условий $(g_1(\mathbf{u}), g_2(\mathbf{u})) \neq (0, 0)$, $(c_1 g_1 \oplus c_2 g_2)(\mathbf{v}) \neq 0$ следует, что $\mathbf{u} \in \mathcal{L}(g_1, g_2)$ и $\mathbf{v} \in \mathcal{L}(g_1, g_2)$. Пусть $K = \langle \mathbf{u}, \mathbf{v} \rangle$. Чтобы доказать (14), достаточно показать, что $\mathbf{u} \oplus c\mathbf{v} \in \mathcal{L}(g_1, g_2)$ для всех $c \in P^*$. Ввиду $\mathbf{u} \oplus c\mathbf{v} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp$ требуется доказать соотношение

$$(c_1 g_1 \oplus c_2 g_2)(\mathbf{u} \oplus c\mathbf{v}) \neq 0.$$

По условию п. 2б теоремы и (6) получаем

$$(c_1 g_1 \oplus c_2 g_2)(\mathbf{u} \oplus c\mathbf{v}) = (c_1 g_1 \oplus c_2 g_2)(\mathbf{u}) \oplus c^2 (c_1 g_1 \oplus c_2 g_2)(\mathbf{v}) = c^2 (c_1 g_1 \oplus c_2 g_2)(\mathbf{v}) \neq 0.$$

Если же условие п. 2б не выполнено, то получаем $K \not\subset \mathcal{L}(g_1, g_2)$. Случай доказан.

Для доказательства остальных случаев понадобятся дополнительные обозначения и результаты. По определению (15) множество $\mathcal{M} = \bigcup_{(c_1, c_2) \in P^2 \setminus \{\mathbf{0}\}} V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp$ содержит

множество $\mathcal{L}(g_1, g_2)$. Поэтому для доказательства того, что некоторый вектор $\mathbf{b}$ принадлежит $\mathcal{L}(g_1, g_2)$, будем сначала доказывать, что $\mathbf{b} \in \mathcal{M}$. Нам понадобятся свойства векторов $\mathbf{b} \in \mathcal{M}$. Очевидно, что

$$\mathcal{M} = V_{f_{1,k}}^\perp \cup V_{f_{s,t}}^\perp \cup \left(\bigcup_{c \in P^*} V_{f_{1,k} \oplus c f_{s,t}}^\perp \right). \quad (16)$$

Нетрудно доказать, что для любой билинейной функции $f_{\overline{l,n}}$, ассоциированной с квадратичной функцией $\sigma_2(x_l, \dots, x_n)$, $1 \leq l < n \leq m$, выполняется

$$f_{\overline{l,n}}(\mathbf{x}, \mathbf{y}) = \sum_{i=l}^n \sum_{\substack{j=l \\ j \neq i}}^n x_i y_j = (x_l, \dots, x_n)(E \oplus I)(y_l, \dots, y_n)^T. \quad (17)$$

Для $\mathbf{b} \in P^m$ имеем

$$f_{\overline{l,n}}(\mathbf{b}, \mathbf{x}) = 0 \Leftrightarrow (b_l, \dots, b_n)(E \oplus I)(x_l, \dots, x_n)^T = 0 \Leftrightarrow (b_l, \dots, b_n)(E \oplus I) = \mathbf{0}.$$

Поэтому, пользуясь линейной алгеброй, можно доказать, что

$$\left((b_1, \dots, b_m) \in V_{f_{\overline{l,n}}}^\perp \right) \Leftrightarrow (b_l = \dots = b_n = (n - l + 1)\delta, \quad \delta \in P). \quad (18)$$

Для описания множества $\mathcal{M} \setminus \left(V_{f_{\overline{1,k}}}^\perp \cup V_{f_{\overline{s,t}}}^\perp \right)$ понадобятся две леммы.

Лемма 1. Если $\delta \in P$, $1 \leq l < n \leq m$, то

$$f_{\overline{l,n}}(\mathbf{x}, \mathbf{b}) = \delta \sum_{i=l}^n x_i \Leftrightarrow \exists a \in P (b_l = \dots = b_n = a, \delta = (n - l)a).$$

Доказательство. Не ограничивая общности, можно рассмотреть билинейную функцию $f_{\overline{1,m}}$. Тогда $f_{\overline{1,m}}(\mathbf{x}, \mathbf{b}) = \mathbf{x}(E \oplus I)\mathbf{b}$, где $I = (1)_{m \times m}$. Поэтому равенство $f_{\overline{1,m}}(\mathbf{x}, \mathbf{b}) = \delta \sum_{i=1}^m x_i$ эквивалентно уравнению

$$(E \oplus I)\mathbf{b} = (\delta, \dots, \delta)^T. \quad (19)$$

Заметим, что дефект матрицы $E \oplus I$ равен остатку от деления m на 2. Если m чётно, то $(E \oplus I)$ — обратимая матрица и $\mathbf{b} = (\delta, \dots, \delta)^T$ — единственное решение (19).

Пусть m нечётно. Если $\delta \neq 0$, то уравнение (19) не имеет решений, потому что $\mathbf{1}(E \oplus I) = \mathbf{0}$, но $\mathbf{1}(\delta, \dots, \delta)^T = \delta \neq 0$. Если $\delta = 0$, то $\mathbf{b} \in V_{f_{\overline{1,m}}}^\perp$. Таким образом, равенство (19) выполнено тогда и только тогда, когда $\delta = 0$ и существует $a \in P$, такое, что $b_1 = \dots = b_m = a$. ■

Лемма 2. При введённых выше обозначениях вектор $\mathbf{b} \in P^m$ принадлежит $V_{f_{\overline{1,k}} \oplus c f_{\overline{s,t}}}^\perp$, для данного $c \in P^*$, тогда и только тогда, когда существуют $a_1, a_2, a_3 \in P$, такие, что выполнены соотношения

$$\begin{aligned} 1) \quad & b_1 = \dots = b_{s-1} = a_1, \quad \sum_{j=s}^k b_j = s a_1; \\ 2) \quad & b_{k+1} = \dots = b_t = a_2, \quad \sum_{j=s}^k b_j = (t - k + 1) a_2; \\ 3) \quad & \begin{cases} (s-1)a_1 \oplus (t-k)a_2 = 0, & \text{если } c = e, \\ b_s = \dots = b_k = a_3, \quad \frac{(s-1)a_1 \oplus c(t-k)a_2}{(c \oplus e)} = (k-s)a_3, & \text{если } c \neq e. \end{cases} \end{aligned}$$

Доказательство. Пусть $\mathbf{b} \in V_{f_{\overline{1,k}} \oplus c f_{\overline{s,t}}}^\perp$ для некоторого $c \in P^*$, то есть

$$f_{\overline{1,k}}(\mathbf{x}, \mathbf{b}) \oplus c f_{\overline{s,t}}(\mathbf{x}, \mathbf{b}) = 0. \quad (20)$$

Из (17) имеем

$$\begin{aligned} f_{1,k}(\mathbf{x}, \mathbf{b}) \oplus c f_{s,t}(\mathbf{x}, \mathbf{b}) &= f_{1,s-1}(\mathbf{x}, \mathbf{b}) \oplus \sum_{j=s}^k b_j \sum_{i=1}^{s-1} x_i \oplus \sum_{j=1}^{s-1} b_j \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) \oplus \\ &\oplus c \left(f_{s,k}(\mathbf{x}, \mathbf{b}) \oplus \sum_{j=k+1}^t b_j \sum_{i=s}^k x_i \oplus \sum_{j=s}^k b_j \sum_{i=k+1}^t x_i \oplus f_{k+1,t}(\mathbf{x}, \mathbf{b}) \right). \end{aligned}$$

Разбивая переменные на три группы, получаем, что равенство (20) эквивалентно следующим трём соотношениям:

$$f_{1,s-1}(\mathbf{x}, \mathbf{b}) = \sum_{j=s}^k b_j \sum_{i=1}^{s-1} x_i; \quad (21)$$

$$f_{k+1,t}(\mathbf{x}, \mathbf{b}) = \sum_{j=s}^k b_j \sum_{i=k+1}^t x_i; \quad (22)$$

$$\sum_{j=1}^{s-1} b_j \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) = c \left(\sum_{j=k+1}^t b_j \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) \right). \quad (23)$$

По лемме 1 равенство (21) равносильно условию 1 леммы 2. Аналогично, (22) эквивалентно условию 2 леммы 2.

Следовательно, (23) выполнено тогда и только тогда, когда

$$(s-1)a_1 \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) = c \left((t-k)a_2 \sum_{i=s}^k x_i \oplus f_{s,k}(\mathbf{x}, \mathbf{b}) \right).$$

Если $c = e$, то имеем $((s-1)a_1 \oplus (t-k)a_2) \sum_{i=s}^k x_i = 0$, то есть $(s-1)a_1 \oplus (t-k)a_2 = 0$.

Если $c \in P \setminus \{0, e\}$, то

$$f_{s,k}(\mathbf{x}, \mathbf{b}) = \frac{(s-1)a_1 \oplus c(t-k)a_2}{e \oplus c} \sum_{i=s}^k x_i.$$

Применяя лемму 1, получаем условие 3 леммы 2. ■

Продолжение доказательства достаточности условий теоремы 2

3. Пусть условия п. 3 теоремы выполнены. Так как многочлен $D_1(x)$ не имеет корней в P , то $g_1(\mathbf{u}) \neq 0$. Из (18) имеем $\mathbf{u} \in V_{f_{1,k}}^\perp$, $\mathbf{v} \in V_{f_{s,t}}^\perp$, и так как $g_1(\mathbf{u}) \neq 0$, $g_2(\mathbf{v}) \neq 0$, получаем $\mathbf{u}, \mathbf{v} \in \mathcal{L}(g_1, g_2)$. Пусть $K = \langle \mathbf{u}, \mathbf{v} \rangle$. Теперь для доказательства условия (14) достаточно доказать, что $\mathbf{u} \oplus d\mathbf{v} \in \mathcal{L}(g_1, g_2)$ для любых $d \in P^*$. Действительно, для

$$\mathbf{b} = \mathbf{u} \oplus d\mathbf{v} = (\underbrace{d, \dots, d}_{s-1}, \underbrace{0, \dots, 0}_{k-s+1}, \underbrace{e, \dots, e}_{t-k+1}, *, \dots, *)$$

по лемме 2 получаем $\mathbf{b} \in V_{f_{1,k} \oplus d f_{s,t}}^\perp$. Из свойства (6) полулинейности имеем $(g_1 \oplus dg_2)(\mathbf{b}) = D_1(d)$. Следовательно, из условия п. 3б теоремы получаем $\mathbf{b} \in \mathcal{L}(g_1, g_2)$.

Очевидно, что если при условии п. 3а условие п. 3б не выполнено, то (14) неверно.

4. Пусть условия п. 4 теоремы выполнены. Из (18) имеем $\mathbf{u} \in V_{f_{1,k}}^\perp$, $\mathbf{v} \in V_{f_{s,t}}^\perp$. Как и в п. 3, пользуясь соотношениями $g_1(\mathbf{u}) \neq 0$, $g_2(\mathbf{v}) \neq 0$, получаем $\mathbf{u}, \mathbf{v} \in \mathcal{L}(g_1, g_2)$.

Пусть $K = \langle \mathbf{u}, \mathbf{v} \rangle$. Теперь для доказательства условия (14) достаточно доказать, что $\mathbf{u} \oplus d\mathbf{v} \in \mathcal{L}(g_1, g_2)$ для любого $d \in P^*$. Действительно,

$$\mathbf{b} = (\underbrace{e \oplus d\delta_2, \dots, e \oplus d\delta_2}_{s-1}, \underbrace{e \oplus d, \dots, e \oplus d}_{k-s+1}, \underbrace{\delta_1 \oplus d, \dots, \delta_1 \oplus d}_{t-k+1}, *, \dots, *).$$

Нетрудно убедиться, что $\mathbf{b}$ удовлетворяет условиям леммы 2 для $c = \frac{\delta_2 \oplus e}{\delta_1 \oplus e}d$, то есть $\mathbf{b} \in V_{f_{1,k} \oplus cf_{s,t}}^\perp$. Из (6) получаем $(g_1 \oplus cg_2)(\mathbf{b}) = D_2(d)$. Теперь из условия 4 теоремы следует, что $\mathbf{b} \in \mathcal{L}(g_1, g_2)$.

Если при условии п. 4а условие п. 4б не выполнено, то (14) неверно.

5. Пусть условия п. 5 теоремы выполнены. Из (18) имеем $\mathbf{u} \in V_{f_{1,k}}^\perp$, $\mathbf{v} \in V_{f_{s,t}}^\perp$. Пользуясь $g_1(\mathbf{u}) \neq 0$, $g_2(\mathbf{v}) \neq 0$, получаем, что $\mathbf{u}, \mathbf{v} \in \mathcal{L}(g_1, g_2)$. Пусть $K = \langle \mathbf{u}, \mathbf{v} \rangle$. Теперь для доказательства условия (14) достаточно доказать, что $\mathbf{u} \oplus d\mathbf{v} \in \mathcal{L}(g_1, g_2)$ для любого $d \in P^*$. Действительно,

$$\mathbf{b} = (\underbrace{e \oplus d, \dots, e \oplus d}_{s-1}, \underbrace{e, \dots, e}_{k-s+1}, \underbrace{0, \dots, 0}_{t-k+1}, *, \dots, *).$$

По лемме 2 получаем $\mathbf{b} \in V_{f_{1,k} \oplus df_{s,t}}^\perp$. Как в п. 3, пользуясь $(g_1 \oplus dg_2)(\mathbf{b}) = D_3(d)$ и условием п. 5 теоремы, получаем $\mathbf{b} \in \mathcal{L}(g_1, g_2)$.

Пункт 6 симметричен п. 5 относительно чётности чисел $s-1$, $t-k$.

Необходимость. Предположим, что существует подпространство $K = \langle \mathbf{u}, \mathbf{v} \rangle$, удовлетворяющее условию (14). Если один из векторов $\mathbf{u}, \mathbf{v}$ принадлежит множеству $V_0^\perp$, то выполнено условие п. 1 или 2 теоремы. В этом случае теорема доказана.

Если $\mathbf{u}, \mathbf{v} \in V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp \setminus V_0^\perp$ для некоторых $c_1, c_2 \in P$, то включение $K \subset \mathcal{L}(g_1, g_2)$ не выполнено в силу свойства (6) полулинейности и условия (15). Отсюда также следует, что если $\mathbf{u}, \mathbf{v} \in P^m \setminus V_0^\perp$, $K = \langle \mathbf{u}, \mathbf{v} \rangle$ и $K \subset \mathcal{L}(g_1, g_2)$, то для $c_1, c_2 \in P$

$$\dim \left(K \cap V_{c_1 f_{1,k} \oplus c_2 f_{s,t}}^\perp \right) = 1, \quad (24)$$

и векторы $\mathbf{u}, \mathbf{v}$ могут быть выбраны так, что

$$\mathbf{u} \in V_{f_{1,k}}^\perp \setminus V_0^\perp, \quad \mathbf{v} \in V_{f_{s,t}}^\perp \setminus V_0^\perp. \quad (25)$$

Таким образом, для доказательства необходимости условия теоремы остаётся показать, что если $K = \langle \mathbf{u}, \mathbf{v} \rangle$, где $\mathbf{u}, \mathbf{v}$ выбраны в соответствии с (25), и верно (14), то выполнено одно из условий п. 3а–6а теоремы.

Сначала рассмотрим случаи, когда для чисел s, k, t не выполнены соотношения из условия теоремы. Они исчерпываются следующим списком:

- 1) $s-1 \equiv t-k \equiv 0 \pmod{2}$, $\mathbf{u}, \mathbf{v} \notin V_0^\perp$;
- 2) $s-1 \not\equiv t-k \pmod{2}$, $k-s+1 \equiv 1 \pmod{2}$, $\mathbf{u}, \mathbf{v} \notin V_0^\perp$.

Действительно, если, например, $\mathbf{u} \in V_0^\perp$, то имеет место случай 1 или 2 теоремы. Если не выполняются соотношения для чисел k, s, t , то имеет место один из случаев 3–6.

Покажем, что в этих двух случаях не выполняется условие (14). Для этого воспользуемся тем, что множество $\mathcal{M}$ из (16) содержит $\mathcal{L}(g_1, g_2)$, и применим лемму 2.

1. Пусть $s-1 \equiv t-k \equiv 0 \pmod{2}$, $\mathbf{u}, \mathbf{v} \notin V_0^\perp$.

По лемме 2 вектор $\mathbf{b}$ принадлежит ядру $V_{f_{1,k} \oplus cf_{s,t}}^\perp$ тогда и только тогда, когда выполнено соотношение

$$b_1 = \dots = b_{s-1} = \sum_{j=s}^k b_j = b_{k+1} = \dots = b_t = a_1, \quad (26)$$

и при $c \notin \{0, e\}$

$$\begin{cases} b_s = \dots = b_k = 0, & \text{если } k - s \equiv 1 \pmod{2}, \\ b_s = \dots = b_k, & \text{если } k - s \equiv 0 \pmod{2}. \end{cases}$$

Отсюда, если $c \notin \{0, e\}$, то

$$\begin{cases} b_1 = \dots = b_t = 0, & \text{если } k - s \equiv 1 \pmod{2}, \\ b_1 = \dots = b_t, & \text{если } k - s \equiv 0 \pmod{2}. \end{cases}$$

Последнее условие означает, что $\mathbf{b} \in V_0^\perp$. Поэтому если $P \neq \text{GF}(2)$, то получаем противоречие с равенством (24).

Рассмотрим случай, когда $P = \text{GF}(2)$. Имеем $K = \{\mathbf{0}, \mathbf{u}, \mathbf{v}, \mathbf{b}\}$, при этом для некоторых $a_1, a_2 \in P$

$$\begin{aligned} \mathbf{u} &= (a_1, \dots, a_1, a_1, \dots, a_1, *, \dots, *, * \dots) \in V_{f_{1,k}}^\perp, \\ \mathbf{v} &= (*, \dots, *, a_2, \dots, a_2, a_2, \dots, a_2, * \dots) \in V_{f_{s,t}}^\perp, \\ \mathbf{b} &= \mathbf{u} \oplus \mathbf{v} \in V_{f_{1,k} \oplus f_{s,t}}^\perp. \end{aligned}$$

Отсюда и равенств (26) получаем, что $b_s = \dots = b_k$ и для $c_1, c_2 \in P$

$$\begin{aligned} \mathbf{u} &= (a_1, \dots, a_1, a_1, \dots, a_1, c_1, \dots, c_1, * \dots) \in V_{f_{1,k}}^\perp, \\ \mathbf{v} &= (c_2, \dots, c_2, a_2, \dots, a_2, a_2, \dots, a_2, * \dots) \in V_{f_{s,t}}^\perp. \end{aligned}$$

Если $k - s + 1 \equiv 0 \pmod{2}$, то числа $k, t - s + 1$ также чётны, и из (18) следуют соотношения $a_1 = 0, a_2 = 0$. Отсюда $\mathbf{b} = (0, \dots, 0, 0, \dots, 0, 0, \dots, 0, *, \dots)$.

Если же $k - s + 1 \equiv 0 \pmod{2}$, то $\mathbf{b} = (b, \dots, b, b, \dots, b, b, \dots, b, *, \dots)$, $b \in P$.

В обоих случаях $\mathbf{b} \in V_0^\perp$ — противоречие.

2. Пусть теперь $s - 1 \not\equiv t - k \pmod{2}$, $k - s + 1 \equiv 1 \pmod{2}$, $\mathbf{u}, \mathbf{v} \notin V_0^\perp$. Не ограничивая общности, будем считать, что $s - 1$ чётно.

При данных s, k, t по лемме 2 вектор $\mathbf{b}$ принадлежит ядру $V_{f_{1,k} \oplus cf_{s,t}}^\perp$ тогда и только тогда, когда выполнено соотношение

$$b_1 = \dots = b_{s-1} = \sum_{j=s}^k b_j = b_{k+1} = \dots = b_t = 0, \quad (27)$$

и при $c \notin \{0, e\}$ получаем $b_s = \dots = b_k = a_3 \in P$. Отсюда, если $c \notin \{0, e\}$, то в силу нечётности $k - s + 1$ имеем $b_1 = \dots = b_t = 0$, то есть $\mathbf{b} \in V_0^\perp$.

Рассмотрим случай $P = \text{GF}(2)$. Аналогично получаем, что $b_s = \dots = b_k$, и так как $k - s + 1$ нечётно, то в силу равенств $b_s = \dots = b_k = 0$ и (27) имеем $\mathbf{b} \in V_0^\perp$. Это означает, что при условии (25) включение (14) не выполняется.

Пусть теперь $K = \langle \mathbf{u}, \mathbf{v} \rangle$, где $\mathbf{u}, \mathbf{v}$ выбраны в соответствии с (25), верно (14) и для чисел s, k, t выполнено одно из условий п. 3а–6а теоремы. Для завершения доказательства теоремы остаётся показать, что тогда векторы $\mathbf{u}, \mathbf{v}$ можно выбрать такими, как в условиях п. 3а–6а.

Проведём такое доказательство для случая 3. Остальные случаи разбираются аналогично. Пусть $s - 1 \equiv t - k \equiv k - s + 1 \equiv 1 \pmod{2}$. Порождающие векторы $\mathbf{u}, \mathbf{v}$ пространства K , как было показано выше, можно выбрать так, чтобы выполнялись условия (25).

Кроме того, из (24) следует, что для каждого $d \in P^*$ существует $c \in P^*$, такое, что $\mathbf{b} = \mathbf{u} \oplus d\mathbf{v} \in V_{f_{1,k} \oplus cf_{s,t}}^\perp$. При данных s, k, t по лемме 2 последнее включение равносильно системе соотношений

$$b_1 = \dots = b_{s-1} = a_1, \sum_{j=s}^k b_j = 0, b_{k+1} = \dots = b_t = a_2,$$

где, кроме того,

$$\begin{cases} a_1 = a_2, & \text{если } c = e, \\ b_s = \dots = b_k = a_3 \in P, \quad a_1 \oplus ca_2 = 0, & \text{если } c \notin \{0, e\}. \end{cases}$$

Отсюда, пользуясь свойством (18) и учитывая, что числа $k, t-s+1$ чётны, получаем, что для некоторых $u_1, v_1 \in P$

$$\begin{aligned} \mathbf{u} &= (0, \dots, 0, 0, \dots, 0, u_1, \dots, u_1, * \dots) \in V_{f_{1,k}}^\perp, \\ \mathbf{v} &= (v_1, \dots, v_1, 0, \dots, 0, 0, \dots, 0, * \dots) \in V_{f_{s,t}}^\perp. \end{aligned}$$

В качестве u_1, v_1 можно выбрать $e \in P$. Случай доказан.

Поступая аналогично в оставшихся случаях, получаем требуемые условия. ■

Заключение

Полученные в работе результаты показывают, что, используя только линейные преобразования модуля и разрядные функции кольца Галуа, можно строить эффективно реализуемые подстановки большой степени, у которых две координатные функции нелинейны. В дальнейшем интерес представляет изучение криптографических свойств описанных подстановок и расширение классов РП-матриц.

Автор выражает глубокую благодарность профессору А. А. Нечаеву за постановку задачи и внимание к проводимым исследованиям.

ЛИТЕРАТУРА

1. *Nechaev A. A. and Abornev A. V.* Nonlinear permutations on a space over a finite field induced by linear transformations of a module over a Galois ring // Математические вопросы криптографии. 2013. Т. 4. Вып. 2. С. 81–100.
2. *Лидл Р., Нидеррайтер Г.* Конечные поля. Т. 1. М.: Мир, 1988.
3. *Кузьмин А. С., Нечаев А. А.* Линейные рекуррентные последовательности над кольцами Галуа // Алгебра и Логика. 1995. Т. 34. № 2. С. 169–189.
4. *Никонов В. Г., Саранцев А. В.* О сложности реализации в базисе ДНФ регулярных систем булевых функций // Математические вопросы криптографии. 2010. Т. 1. Вып. 3. С. 45–65.
5. *Diedonné J. -A.* La Géométrie des Groupes Classiques. Ergebnisse der Mathematik und ihrer Grenzgebiete. B. 5. Springer, 1971.
6. *Kuzmin A. S. and Nechaev A. A.* Trace-function on a Galois ring in coding theory // LNCS. 1997. V. 1255. P. 277–290.