ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ПРИКЛАДНОЙ ДИСКРЕТНОЙ МАТЕМАТИКИ

УДК 512.624

КУСОЧНО-АФФИННЫЕ ПОДСТАНОВКИ КОНЕЧНЫХ ПОЛЕЙ

А. Д. Бугров

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

Определяется множество d-разбиений конечного поля $\mathrm{GF}(q)$. При $d = 2$ и $d = (q-1)/2$ оно полностью описано; при $d < \sqrt{q-1}$ выводится гипотеза о его строении. Приводится критерий на d-разбиение. Определяются кусочно-аффинные подстановки конечных полей. Получены оценка линейной характеристики кусочно-аффинных подстановок конечных полей и точные её значения при $d = 2$. Описаны многочлены, представляющие кусочно-аффинные подстановки. Доказано, что при $d \geqslant \sqrt{q-1}$ класс кусочно-аффинных подстановок образует всю симметрическую группу подстановок конечного поля.

Ключевые слова: *конечные поля, кусочно-линейные подстановки, кусочно-аффинные подстановки, линейная характеристика.*

DOI 10.17223/20710410/30/1

PIECEWISE-AFFINE PERMUTATIONS OF FINITE FIELDS

A. D. Bugrov

Certification Research Center, Moscow, Russia

E-mail: Bugrovalexey1@yandex.ru

Piecewise-affine permutations (p.-a. p.) are defined on any field $\mathrm{GF}(q)$. They are a generalization of piecewise-linear permutations firstly introduced by A. B. Evans. Here some estimates for linear characteristics of p.-a. p. on $\mathrm{GF}(q)$ are given. In some cases, their exact values are pointed. Polynomials representing p.-a. p. are described. Under some conditions on $\sqrt{q-1}$, it is proved that piecewise-affine permutations form the full symmetric group of $\mathrm{GF}(q)$.

Keywords: *finite field, piecewise-linear permutations, piecewise-affine permutations, linear characteristic of permutations.*

Введение

В данной работе рассматривается класс кусочно-аффинных подстановок конечных полей. Он является обобщением класса кусочно-линейных подстановок, впервые предложенного А. Б. Эвансом в работе [1]. А. Е. Тришиным в [2] получены оценки и в некоторых случаях найдены точные значения линейной характеристики кусочно-линейных подстановок поля, имеющего характеристику два.

Основным результатом настоящей работы являются оценки линейной характеристики для кусочно-аффинных подстановок произвольного поля (не обязательно характеристики два). В некоторых случаях для линейной характеристики приводятся точные значения. Кроме того, указываются некоторые свойства семейства всех кусочно-аффинных подстановок, свидетельствующие о том, что этот класс существенно более широкий, чем класс кусочно-линейных подстановок.

Для того чтобы определить кусочно-аффинные подстановки, будем использовать следующие обозначения: $P = \mathrm{GF}(q)$ — конечное поле из q элементов; e — единица поля P; ξ — примитивный элемент поля P; P^* — мультипликативная группа поля P. Пусть d, l — натуральные такие, что $q - 1 = dl$. Тогда $\langle \xi^d \rangle = H < P^*$ — подгруппа порядка l мультипликативной группы. Обозначим через $AGL(1, P)$ группу аффинных преобразований поля P:

$$AGL(1, P) = \{f_{a,b} : P \to P \mid f_{a,b}(x) = ax + b, a \in P^*, b \in P\}.$$

Введём следующее обозначение:

$$H_{a,b} = Ha + b, \quad a, b \in P.$$

Пусть векторы $\mathbf{a} = (a_0, \ldots, a_{d-1}) \in (P^*)^d$ и $\mathbf{b} = (b_0, \ldots, b_d) \in P^{d+1}$ такие, что множества H_{a_i,b_i}, $i \in \{0, \ldots, d-1\}$, попарно не пересекаются. Рассмотрим объединение

$$W = \bigsqcup_{i=0}^{d-1} H_{a_i,b_i} \sqcup \{b_d\},$$

где символ $\sqcup$ обозначает операцию объединения непересекающихся множеств. Если $W = P$, то будем говорить, что упорядоченная пара векторов $(\mathbf{a}, \mathbf{b})$ задает d-разбиение (H-разбиение) поля P. Пусть $R_d(P)$ — множество всех упорядоченных пар, задающих d-разбиения (H-разбиения) поля P:

$$R_d(P) = \left\{ (\mathbf{a}, \mathbf{b}) = ((a_0, a_1, \ldots, a_{d-1}), (b_0, b_1, \ldots, b_d)) \in (P^*)^d \times P^{d+1} : P = \bigsqcup_{i=0}^{d-1} H_{a_i,b_i} \sqcup \{b_d\} \right\}.$$

Заметим, что множество $R_d(P)$ не пусто для всех возможных d и q, так как мультипликативная группа поля P^* либо сама является подгруппой H (в случае $d = 1$) и $(e, (0, 0)) \in R_1(P)$, либо разбивается на смежные классы по подгруппе H:

$$P = P^* \sqcup \{0\} = \bigsqcup_{i=0}^{d-1} H_{\xi^i,0} \sqcup \{0\}, \quad ((e, \xi, \xi^2, \ldots, \xi^{d-1}), (0, 0, \ldots, 0)) \in R_d(P).$$

Разбиение, соответствующее паре $(\mathbf{a}, \mathbf{b}) \in R_d(P)$, будем называть тривиальным, если $b_0 = b_1 = \ldots = b_d$. Пусть $Rl_d(P)$ — множество всех упорядоченных пар векторов, задающих тривиальные d-разбиения:

$$Rl_d(P) = \{(\mathbf{a}, \mathbf{b}) \in R_d(P) : b_0 = b_1 = \ldots = b_d\}.$$

Заметим, что для любой пары $(\mathbf{a}, \mathbf{b}) \in Rl_d(P)$ выполняется следующее свойство: множества $\{H, H\xi, \ldots, H\xi^{d-1}\}$ и $\{Ha_0, Ha_1, \ldots, Ha_{d-1}\}$ совпадают. Таким образом, $Rl_d(P) = \{(\mathbf{a}, \mathbf{b}) \in (P^*)^d \times (P^{d+1}) : b_0 = b_1 = \ldots = b_d \in P, a_{s(i)} = \xi^i, s \in S_d\}$, где S_d — симметрическая группа подстановок множества $\{0, 1, \ldots, d-1\}$.

Кусочно-аффинной подстановкой поля P, соответствующей парам $(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}) \in$ $\in R_d(P)$, будем называть отображение

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(x) = \begin{cases} hc_i + e_i, & \text{если } x = ha_i + b_i \in H_{a_i,b_i},\ i \in \{0,\dots,d-1\}, \\ e_d, & \text{если } x = b_d. \end{cases}$$

В случае, когда $\mathbf{b} = \mathbf{e} = (0,0,\dots,0)$, кусочно-аффинные подстановки будем называть кусочно-линейными.

Введённое определение кусочно-аффинной подстановки корректно (заданное отображение действительно является подстановкой), так как

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(P) = \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(\bigsqcup_{i=0}^{d-1} H_{a_i,b_i} \sqcup \{b_d\}) =$$
$$= \bigcup_{i=0}^{d-1} \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(H_{a_i,b_i}) \cup \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}(b_d) = \bigcup_{i=0}^{d-1} H_{c_i,e_i} \cup \{e_d\} = \bigsqcup_{i=0}^{d-1} H_{c_i,e_i} \sqcup \{e_d\} = P.$$

Для обозначения подстановки $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}$ будем также использовать запись

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} = \begin{pmatrix} b_d & H_{a_0,b_0} & H_{a_1,b_1} & \dots & H_{a_{d-1},b_{d-1}} \\ e_d & H_{c_0,e_0} & H_{c_1,e_1} & \dots & H_{c_{d-1},e_{d-1}} \end{pmatrix},$$

где ограничение $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}$ на $H_{a_i,b_i}, i \in \{0,\dots,d-1\}$ выглядит следующим образом:

$$\begin{pmatrix} H_{a_i,b_i} \\ H_{c_i,e_i} \end{pmatrix} = \begin{pmatrix} a_i\xi^0 + b_i & a_i\xi^d + b_i & \dots & a_i\xi^{d(l-1)} + b_i \\ c_i\xi^0 + e_i & c_i\xi^d + e_i & \dots & c_i\xi^{d(l-1)} + e_i \end{pmatrix}.$$

Заметим, что отображение $\omega : ((\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e})) \mapsto \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}$ неинъективно. Например, тождественная подстановка представляется как $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{a},\mathbf{b}} = \Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{c},\mathbf{e}}$ для любых $(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}) \in$ $\in R_d(P)$.

Множество кусочно-аффинных подстановок, образованных d-разбиениями поля P, будем обозначать $A_d(P)$. Справедливо равенство

$$A_d(P) = \{\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} : (\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}) \in R_d(P)\}.$$

Множество кусочно-линейных подстановок, образованных d-разбиениями поля P, будем обозначать $L_d(P)$. Таким образом,

$$L_d(P) = \{\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} : (\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}) \in Rl_d(P), \mathbf{b} = \mathbf{e} = (0,0,\dots,0)\}.$$

1. Некоторые свойства класса кусочно-аффинных подстановок

Утверждение 1.

1) Для любых пар $(\mathbf{a},\mathbf{b}),(\mathbf{c},\mathbf{e}),(\mathbf{f},\mathbf{g})$ из $R_d(P)$ верно равенство

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}\Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{f},\mathbf{g}} = \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{f},\mathbf{g}}.$$

2) Группа $AGL(1,P)$ аффинных подстановок поля P вложена в множество $A_d(P)$ так, что для любой подстановки $g \in AGL(1,P)$ и любой пары $(\mathbf{a},\mathbf{b}) \in R_d(P)$ найдутся пары $(\mathbf{c},\mathbf{e}),(\mathbf{k},\mathbf{t}) \in R_d(P)$, такие, что $g = \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} = \Delta^{\mathbf{k},\mathbf{t}}_{\mathbf{a},\mathbf{b}}$.

3) Для любой кусочно-аффинной подстановки $\Delta^{\mathbf{a,b}}_{\mathbf{c,e}} \in A_d(P)$ и для любых аффинных преобразований $k, g \in AGL(1,P)$, где $k(x) = \alpha x + \beta$, $g(x) = \gamma x + \lambda$, верно равенство $k\Delta^{\mathbf{a,b}}_{\mathbf{c,e}} g = \Delta^{\mathbf{u,v}}_{\mathbf{f,g}}$, где

$$(\mathbf{u},\mathbf{v})=((\alpha^{-1}a_0,\alpha^{-1}a_1,\dots,\alpha^{-1}a_{d-1}),(\alpha^{-1}b_0-\alpha^{-1}\beta,\alpha^{-1}b_1-\alpha^{-1}\beta,\dots,\alpha^{-1}b_d-\alpha^{-1}\beta)),$$
$$(\mathbf{f},\mathbf{g}) = ((\gamma c_0,\gamma c_1,\dots,\gamma c_{d-1}),(\gamma e_0+\lambda,\gamma e_1+\lambda,\dots,\gamma e_d+\lambda)).$$

4) Если $d_1|d_2$ и $d_2|(q-1)$, то $A_{d_1}(P) \subset A_{d_2}(P)$.

5) Если $\dfrac{q-1}{d} = l \leqslant 2$, то для любого произвольного разбиения $P = \bigsqcup\limits_{i=0}^{d-1} R_i \sqcup \{r\}$, где $|R_i| = l$, $i \in \{0,\dots,d-1\}$, существует пара $(\mathbf{a},\mathbf{b}) \in R_d(P)$, такая, что $H_{a_i,b_i} = R_i$, $b_d = r$ для любого $i \in \{0,\dots,d-1\}$.

6) Если $\dfrac{q-1}{d} = l \leqslant 2$, то $A_d(P) = S(P)$, где $S(P)$ — симметрическая группа подстановок поля P.

7) Если $R_d(P) = Rl_d(P)$, то $A_d(P) = V^+(P)L_d(P)V^+(P)$, где $V^+(P)$ — группа сдвигов поля P.

Доказательство.

1) Пусть $x \in H_{a_i,b_i}$, тогда существует $h \in H$, что $x = ha_i + b_i$. По определению $\Delta^{\mathbf{a,b}}_{\mathbf{c,e}}(x) = hc_i + e_i \in H_{c_i,e_i}$, следовательно, $\Delta^{\mathbf{c,e}}_{\mathbf{f,g}}(hc_i+e_i) = hf_i + g_i$. Если $x = b_d$, то

$$\Delta^{\mathbf{a,b}}_{\mathbf{c,e}}\Delta^{\mathbf{c,e}}_{\mathbf{f,g}}(x) = \Delta^{\mathbf{c,e}}_{\mathbf{f,g}}(e_d) = g_d.$$

2) Если $g(x) = \alpha x + \beta$, где $\alpha \in P^*$, $\beta \in P$, то при $(\mathbf{c},\mathbf{e}) = ((\alpha a_0,\dots,\alpha a_{d-1}),(\alpha b_0 + {}+\beta,\dots,\alpha b_{d-1}+\beta,\alpha b_d+\beta))$ для любых $i \in \{0,\dots,d-1\}$, $h \in H$ имеем

$$\Delta^{\mathbf{a,b}}_{\mathbf{c,e}}(ha_i+b_i) = ha_i\alpha + \alpha b_i + \beta = \alpha(ha_i+b_i)+\beta, \quad \Delta^{\mathbf{a,b}}_{\mathbf{c,e}}(b_d) = \alpha b_d + \beta,$$

то есть $\Delta^{\mathbf{a,b}}_{\mathbf{c,e}}$ действует на P, как и g.

Аналогично при

$$(\mathbf{c},\mathbf{e}) = ((\alpha^{-1}a_0,\dots,\alpha^{-1}a_{d-1}),(\alpha^{-1}b_0-\alpha^{-1}\beta,\dots,\alpha^{-1}b_{d-1}-\alpha^{-1}\beta,\alpha^{-1}b_d-\alpha^{-1}\beta))$$

для любых $i \in \{0,\dots,d-1\}$, $h \in H$ имеем

$$\Delta^{\mathbf{c,e}}_{\mathbf{a,b}}(hc_i+e_i) = ha_i + b_i = \alpha(hc_i+e_i)+\beta, \quad \Delta^{\mathbf{c,e}}_{\mathbf{a,b}}(e_d) = b_d = \alpha e_d + \beta.$$

3) Пусть $F = \Delta^{\mathbf{a,b}}_{\mathbf{c,e}}$, тогда по п. 2 существуют пары $(\mathbf{f},\mathbf{g}),(\mathbf{u},\mathbf{v}) \in R_d(P)$, такие, что $k = \Delta^{\mathbf{u,v}}_{\mathbf{a,b}}, g = \Delta^{\mathbf{c,e}}_{\mathbf{f,g}}$. Из п. 1 следует, что $kFg = \Delta^{\mathbf{u,v}}_{\mathbf{f,g}}$. Заметим, что для любых $i \in \{0,\dots,d-1\}$, $h \in H$

$$kFg(k^{-1}(a_ih+b_i)) = g(c_ih+e_i), \quad kFg(k^{-1}(b_d)) = g(e_d),$$

следовательно,

$$\Delta^{\mathbf{u,v}}_{\mathbf{f,g}}(\alpha^{-1}a_ih+\alpha^{-1}b_0-\alpha^{-1}\beta) = \gamma c_ih+\gamma e_i+\lambda, \quad \Delta^{\mathbf{u,v}}_{\mathbf{f,g}}(\alpha^{-1}b_d-\alpha^{-1}\beta) = \gamma e_d+\lambda.$$

4) Пусть H, G — подгруппы P^*, такие, что $|H| = l_1 = (q-1)/d_1$, $|G| = l_2 = (q-1)/d_2$. Тогда $l_2|l_1$ и $G < H$. Группу H разобьём на смежные классы по подгруппе G:

$$H = \bigsqcup_{j=0}^{d_2/d_1-1} G\xi^{d_1 j}.$$

Зададим отображение $\tau : R_{d_1}(P) \to (P^*)^{d_2} \times P^{d_2+1}$ таким образом, что $\tau(\mathbf{a}, \mathbf{b}) = (\mathbf{c}, \mathbf{e})$, где

$$(\mathbf{a}, \mathbf{b}) = ((a_0, \ldots, a_{d_1-1}), (b_0, \ldots, d_{d_1})),$$
$$(\mathbf{c}, \mathbf{e}) = ((\underbrace{a_0, \xi^{d_1} a_0, \ldots, \xi^{d_2-d_1} a_0}_{d_2/d_1}, \ldots, \underbrace{a_{d_1-1}, \xi^{d_1} a_{d_1-1}, \ldots, \xi^{d_2-d_1} a_{d_1-1}}_{d_2/d_1}),$$
$$(\underbrace{b_0, b_0, \ldots, b_0}_{d_2/d_1}, \ldots, \underbrace{b_{d_1-1}, b_{d_1-1}, \ldots, b_{d_1-1}}_{d_2/d_1}, b_{d_1})).$$

В силу равенств

$$P = \bigsqcup_{i=0}^{d_1-1} H_{a_i,b_i} \sqcup \{b_{d_1}\} = \bigsqcup_{i=0}^{d_1-1} \left(\left(\bigsqcup_{j=0}^{d_2/d_1-1} G\xi^{d_1 j} \right) a_i + b_i \right) \sqcup \{b_{d_1}\} =$$
$$= \bigsqcup_{i=0}^{d_1-1} \left(\bigsqcup_{j=0}^{d_2/d_1-1} G\xi^{jd_1} a_i + b_i \right) \sqcup \{b_{d_1}\} = \bigsqcup_{i=0}^{d_1-1} \left(G_{a_i,b_i} \sqcup G_{\xi^{d_1} a_i,b_i} \sqcup \ldots \sqcup G_{\xi^{d_2-d_1} a_i,b_i} \right) \sqcup \{b_{d_1}\}$$

имеем $(\mathbf{c}, \mathbf{e}) \in R_{d_2}(P)$.

Теперь покажем, что $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{u},\mathbf{v}} = \Delta^{\tau(\mathbf{a},\mathbf{b})}_{\tau(\mathbf{u},\mathbf{v})} \in A_{d_2}(P)$ для любой кусочно-аффинной подстановки $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{u},\mathbf{v}} \in A_{d_1}(P)$. Выберем любой элемент x поля P. Если он равен b_{d_1}, то

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{u},\mathbf{v}}(x) = \Delta^{\tau(\mathbf{a},\mathbf{b})}_{\tau(\mathbf{u},\mathbf{v})}(x).$$

Если $x = ha_i + b_i \in H_{a_i,b_i}$, где $h \in H$, $i \in \{0, \ldots, d_1 - 1\}$, то найдутся $g \in G$, $j \in \{0, \ldots, d_2/d_1 - 1\}$, такие, что $h = g\xi^{jd_1}$. Следовательно, $ha_i + b_i = g\xi^{jd_1} a_i + b_i$. Пусть $\tau(\mathbf{a}, \mathbf{b}) = (\mathbf{c}, \mathbf{e})$, $\tau(\mathbf{u}, \mathbf{v}) = (\mathbf{f}, \mathbf{t})$. Заметим, что

$$c_{id_2/d_1+j} = \xi^{jd_1} a_i, f_{id_2/d_1+j} = \xi^{jd_1} u_i,$$

$$e_{id_2/d_1+j} = b_i, t_{id_2/d_1+j} = v_i$$

при всех $i \in \{0, \ldots, d_1 - 1\}$, $j \in \{0, \ldots, d_2/d_1 - 1\}$. Тогда

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{u},\mathbf{v}}(ha_i + b_i) = hu_i + v_i = g\xi^{jd_1} u_i + v_i =$$
$$= gf_{id_2/d_1+j} + t_{id_2/d_1+j} = \Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{f},\mathbf{t}}(gc_{id_2/d_1+j} + e_{id_2/d_1+j}) = \Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{f},\mathbf{t}}(g\xi^{jd_1} a_i + b_i) = \Delta^{\mathbf{c},\mathbf{e}}_{\mathbf{f},\mathbf{t}}(ha_i + b_i).$$

5) Группа $AGL(1, P)$ 2-транзитивна, значит, для любого множества $R \subset P$ из не более чем двух элементов существуют $a \in P^*$, $b \in P$, такие, что $H_{a,b} = R$.

6) При $l = 1$ доказательство очевидно. Пусть $l = 2$. Выберем любую подстановку $s \in S(P)$, такую, что

$$s = \begin{pmatrix} u_0 & u_1 & \ldots & u_{q-1} \\ v_0 & v_1 & \ldots & v_{q-1} \end{pmatrix}.$$

Тогда из п. 5 следует, что существуют пары $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{e}) \in R_2(P)$, такие, что $H_{a_i,b_i} = \{u_{2i}, u_{2i+1}\}$, $H_{c_i,e_i} = \{v_{2i}, v_{2i+1}\}$, $b_d = u_{q-1}$, $e_d = v_{q-1}$, то есть $s = \Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}}$.

7) Включение $V^+(P)L_d(P)V^+(P) \subset A_d(P)$ следует из п. 3. Для любых $\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} \in A_d(P)$, $(\mathbf{a}, \mathbf{b}), (\mathbf{c}, \mathbf{e}) \in Rl_d(P)$, $\mathbf{b} = (b, b, \ldots, b), \mathbf{e} = (e, e, \ldots, e)$ из п. 3 и $R_d(P) = Rl_d(P)$ следует равенство

$$\Delta^{\mathbf{a},\mathbf{b}}_{\mathbf{c},\mathbf{e}} = k\Delta^{\mathbf{a},\theta}_{\mathbf{c},\theta} g,$$

где $\theta = (0, 0, \ldots, 0)$; $\Delta^{\mathbf{a},\theta}_{\mathbf{c},\theta} \in L_d(P)$; $k(x) = x - b$; $g(x) = x + e$. ■

Замечание 1. Из условия $d = 2$ следует, что $\mathrm{char}\ P \neq 2$, так как $d|(q-1)$.

Лемма 1. Пусть $d = 2$, $H = \langle \xi^2 \rangle$, $q > 5$. Тогда для любого $b \in P^*$ существуют $a_1, a_2 \in H$ и $a_3, a_4 \in H\xi$, такие, что $a_1 - a_2 = a_3 - a_4 = b$.

Доказательство. Пусть $f : P^n \to P$ — произвольное отображение и

$$N^*(f(x_1, \ldots, x_n) = b) = |\{(a_1, \ldots, a_n) : a_1, \ldots, a_n \in P^*, f(a_1, \ldots, a_n) = b\}|.$$

Если η — квадратичный характер поля P, то получим равенства

$$N^*(x_1^2 - x_2^2 = b) = \sum_{c_1+c_2=b; c_1,c_2 \in P^*} N^*(x_1^2 = c_1) N^*(-x_2^2 = c_2) =$$

$$= \sum_{c_1+c_2=b; c_1,c_2 \in P^*} (1 + \eta(c_1))(1 + \eta(-c_2)) = \sum_{c_1+c_2=b; c_1,c_2 \in P^*} [1 + \eta(-c_2) + \eta(c_1) + \eta(-c_1c_2)] =$$

$$= q - 2 + \sum_{c \notin \{0,b\}} \eta(-c) + \sum_{c \notin \{0,b\}} \eta(c) + \eta(-1) \sum_{c_1+c_2=b; c_1,c_2 \in P^*} \eta(c_1c_2) =$$

$$= q - 2 + \sum_{c \notin \{0,b\}} \eta(-c) + \sum_{c \notin \{0,b\}} \eta(c) + \eta(-1) \sum_{c \notin \{0,b\}} \eta(cb - c^2).$$

Используя равенства $\eta(0) = 0$, $\sum\limits_{c \in P^*} \eta(c) = 0$ (свойство мультипликативных характеров) и $\sum\limits_{c \in P} \eta(cb - c^2) = -\eta(-1)$ [3, теорема 5.48], имеем

$$N^*(x_1^2 - x_2^2 = b) = q - 2 - \eta(-b) - \eta(b) - \eta(-1)\eta(-1) = q - 3 - \eta(-b) - \eta(b).$$

Легко заметить, что при $q > 5$ выполнено $N^*(x_1^2 - x_2^2 = b) > 0$, следовательно, существуют $a_1, a_2 \in H$, такие, что $a_1 - a_2 = b$, для любого $b \in P^*$. Из существования решения уравнения

$$x_1 - x_2 = b, \quad \text{где} \quad x_1, x_2 \in H, \ b \in P^*,$$

следует существование решения уравнения

$$x_1 - x_2 = b, \quad \text{где} \quad x_1, x_2 \in H\xi, \ b \in P^*,$$

и существование $a_1, a_2 \in H\xi$, таких, что $a_1 - a_2 = b$, $b \in P^*$. ■

Лемма 2. Пусть $d = 2$, $q > 5$. Тогда для любого $b \in P^*$ существуют $a_1 \in H$, $a_2 \in H\xi$, такие, что $a_1 - a_2 = b$.

Доказательство. Заметим, что H состоит из всех элементов, являющихся квадратами элементов из P^*, а $H\xi$ состоит из всех ненулевых элементов, не являющихся квадратами. Справедливы следующие соотношения:

$$N^*(x_1^2 - \xi x_2^2 = b) = \sum_{c_1+c_2=b; c_1,c_2 \in P^*} N^*(x_1^2 = c_1) N^*(x_2^2 = -\xi^{-1}c_2) =$$

$$= \sum_{c_1+c_2=b; c_1,c_2 \in P^*} (1 + \eta(c_1))(1 + \eta(-\xi^{-1}c_2)) =$$

$$= \sum_{c_1+c_2=b; c_1,c_2 \in P^*} [1 + \eta(-\xi^{-1}c_2) + \eta(c_1) + \eta(-\xi^{-1}c_1c_2)] =$$

$$= q - 2 + \eta(-\xi^{-1}) \sum_{c \notin \{0,b\}} \eta(c) + \sum_{c \notin \{0,b\}} \eta(c) + \eta(-\xi^{-1}) \sum_{c_1+c_2=b; c_1,c_2 \in P^*} \eta(c_1c_2) =$$

$$= q - 2 + \eta(-\xi^{-1}) \sum_{c \notin \{0,b\}} \eta(c) + \sum_{c \notin \{0,b\}} \eta(c) + \eta(-\xi^{-1}) \sum_{c \notin \{0,b\}} \eta(cb - c^2).$$

Используя равенства $\eta(0) = 0$, $\sum\limits_{c \in P^*} \eta(c) = 0$ (свойство мультипликативных характеров) и $\sum\limits_{c \in P} \eta(cb - c^2) = -\eta(-1)$ [3, теорема 5.48], имеем

$$N^*(x_1^2 - \xi x_2^2 = b) = q - 2 - \eta(-\xi^{-1})\eta(b) - \eta(b) - \eta(-\xi^{-1})\eta(-1) = \\ = q - 2 - \eta(b)(1 + \eta(-\xi^{-1})) - \eta(\xi^{-1}).$$

Легко заметить, что при $q > 5$ выполнено $N^*(x_1^2 - \xi x_2^2 = b) > 0$. ■

Замечание 2. При $q = 3, 5$ леммы 1 и 2 неверны.

Теорема 1. Если $q > 5$, то $R_2(P) = Rl_2(P)$.

Доказательство. Пусть $(\mathbf{a}, \mathbf{b}) = ((a_0, a_1), (b_0, b_1, b_2)) \in R_2(P)$.

1) Если $Ha_0 = Ha_1$, то $b_0 \neq b_1$ (в силу определения $(\mathbf{a}, \mathbf{b})$), и для любых $x \in H_{a_0,b_0}$, $y \in H_{a_1,b_1}$ выполнено

$$x = a_0 h_x + b_0 \neq a_1 h_y + b_1 = y,$$

где $h_x, h_y \in H$. Следовательно, $a_0 h_x - a_1 h_y \neq b_1 - b_0$. Заметим, что $a_0 h_x - a_1 h_y$ пробегает P^* по лемме 1. Значит, $b_1 - b_0 = 0$, и получено противоречие с соотношением $b_0 \neq b_1$.

2) Если $Ha_0 \neq Ha_1$ и $b_0 \neq b_1$, то аналогично случаю 1 получаем противоречие с помощью леммы 2.

Таким образом, если $Ha_0 = Ha_1$, то $(\mathbf{a}, \mathbf{b}) \notin R_2(P)$; если $Ha_0 \neq Ha_1$, то $(\mathbf{a}, \mathbf{b})$ может быть разбиением только в случае $b_0 = b_1 = b_2$. ■

Следствие 1. Если $q > 5$, то выполняется равенство

$$A_2(P) = V^+(P) L_2(P) V^+(P).$$

Если $q = 3, 5$, то выполняется равенство

$$A_2(P) = S(P).$$

Доказательство. Следует из п. 7 утверждения 1. ■

Утверждение 2. Пусть $(\mathbf{a}, \mathbf{b}) \in R_d(P)$ и $x_1^d - x_2^d$ пробегает всю группу P^* при $(x_1, x_2) \in (P^*)^2$, то есть для любого $c \in P^*$ существуют $f, e \in P^*$, такие, что $f^d - e^d = c$. Тогда среди смежных классов $Ha_0, Ha_1, \ldots, Ha_{d-1}$ нет двух одинаковых.

Доказательство. От противного: пусть в наборе $(Ha_0, Ha_1, \ldots, Ha_{d-1})$ есть два одинаковых класса $Ha_i = Ha_k$, $i, k \in \{0, \ldots, d-1\}$, $i \neq k$. Тогда $b_i \neq b_k$ ввиду $(Ha_i + b_i) \cap (Ha_k + b_k) = \varnothing$, из чего получаем противоречие по аналогии с доказательством теоремы 1. ■

Гипотеза 1. Если $d < \sqrt{q-1}$, то есть количество классов в разбиении меньше, чем элементов в одном классе, то $R_d(P)$ состоит только из тривиальных разбиений и выполняется равенство

$$A_d(P) = V^+(P) L_d(P) V^+(P).$$

Замечание 3. Теоретически обоснован случай $q > 5$, $d = 2$. Экспериментально гипотеза подтверждена на малых значениях d и q (см. п. 9).

Следующая теорема даёт способ построения нетривиального d-разбиения.

Теорема 2. Пусть $(l+1)|q$, $h_1, h_2 \in H$, $(\mathbf{a}, \mathbf{b}) \in R_d(P)$, $b_i = b_d$, $i \in \{0, \ldots, d-1\}$. Тогда $((a_0, \ldots, a_{i-1}, a_i h_1, a_{i+1}, \ldots, a_{d-1}), (b_0, \ldots, b_{i-1}, a_i h_2 + b_d, b_{i+1}, \ldots, b_{d-1}, a_i h_2 + b_d))$ — нетривиальное d-разбиение.

Доказательство. Достаточно показать, что

$$H_{a_i,b_d} \sqcup \{b_d\} = H_{a_i h_1, a_i h_2 + b_d} \sqcup \{a_i h_2 + b_d\}.$$

Если $(l+1)|q = p^n$, то $l = p^k - 1$ для некоторого $1 \leqslant k \leqslant n$, а так как $p^k - 1 = l|(q-1) = p^n - 1$, то $k|n$ и $H \cup \{0\}$ — подполе поля P. В частности, $H \cup \{0\}$ замкнуто относительно умножения на h_1 и прибавления h_2. Значит,

$$\begin{gathered} H_{a_i,b_d} \sqcup \{b_d\} = \{H \sqcup \{0\}\}a_i + b_d = \{Hh_1 \sqcup \{0\}\}a_i + b_d = \{Hh_1 + h_2 \sqcup \{h_2\}\}a_i + b_d = \\ = \{H_{h_1,h_2} \sqcup \{h_2\}\}a_i + b_d = H_{a_i h_1, a_i h_2 + b_d} \sqcup \{a_i h_2 + b_d\}. \end{gathered}$$

Теорема доказана. ■

Замечание 4. Данная теорема применима в случае, когда $P = \mathrm{GF}(q)$, где $q = p^n$, имеет собственное подполе, то есть n имеет собственный делитель.

2. Критерий на d-разбиение

Теорема 3. Пусть $2 < q$, $1 < d < q - 1$. Пара векторов

$$(\mathbf{a}, \mathbf{b}) \in (P^*)^d \times P^{d+1}$$

образует d-разбиение тогда и только тогда, когда для любых $i, j \in \{0, \ldots, d-1\}$, $i \neq j$, выполняются следующие условия:

1) $(b_j = b_i) \Rightarrow (\dfrac{a_j}{a_i} \notin H)$;
2) $(b_j \neq b_i) \Rightarrow \left(\dfrac{a_i h - a_j}{b_j - b_i} \notin H \text{ для всех } h \in H\right)$;
3) $b_d = -l \sum\limits_{j=0}^{d-1} b_j$.

Доказательство. Пара векторов $(\mathbf{a}, \mathbf{b})$ задает d-разбиение тогда и только тогда, когда

$$P = \bigsqcup_{i=0}^{d-1} H_{a_i,b_i} \sqcup \{b_d\},$$

то есть для любых $i, j \in \{0, \ldots, d-1\}$, $i \neq j$,

а) $H_{a_i,b_i} \cap H_{a_j,b_j} = \varnothing$;
б) $b_d \notin H_{a_i,b_i}$.

Условие «а» равносильно тому, что для любых $h_1, h_2 \in H$, $i, j \in \{0, \ldots, d-1\}$, $i \neq j$, выполняется неравенство $a_i h_1 + b_i \neq a_j h_2 + b_j$. Пусть $h_1 = h_2 h$, $h \in H$, тогда

$$h_2(a_i h - a_j) \neq b_j - b_i.$$

В итоге «а» равносильно следующим условиям:

$$\left(h_2^{-1} \neq \frac{a_i h - a_j}{b_j - b_i}\right) \Leftrightarrow \left(\frac{a_i h - a_j}{b_j - b_i} \notin H\right) \text{ при } b_i \neq b_j;$$

$$(a_i h - a_j \neq 0) \Leftrightarrow \left(\frac{a_j}{a_i} \in H\right) \text{ при } b_i = b_j.$$

Пункт «б», при условии «а», равносилен тому, что

$$b_d + \sum_{j=0}^{d-1} \sum_{c \in H_{a_j, b_j}} c = 0,$$

так как сумма элементов конечного поля, имеющего мощность, не равную двум, равна нулю. Тогда, пользуясь тем, что сумма элементов любой неединичной подгруппы группы P^* равна нулю, получаем

$$b_d = -\sum_{j=0}^{d-1} \sum_{c \in H_{a_j, b_j}} c = -\sum_{j=0}^{d-1} \sum_{c \in H} (a_j c + b_j) = -\sum_{j=0}^{d-1} a_j \sum_{c \in H} c - \sum_{j=0}^{d-1} |H| b_j = -l \sum_{j=0}^{d-1} b_j,$$

из чего следует утверждение теоремы. ■

3. Близость между дискретными функциями

Определим удобное для наших вычислений понятие близости в случае произвольного поля и сравним его с другими понятиями близости [4, 5].

Пусть $P_0 = \mathrm{GF}(p)$ — простое подполе поля $P = \mathrm{GF}(q)$, $f, g : P_0^n \to P_0$, χ — канонический аддитивный характер поля P_0, задаваемый равенством $\chi(x) = e^{2\pi i \frac{x}{p}}$, $x \in P_0$. Множество всех характеров группы $(P_0, +)$ имеет вид $\{\chi_a : a \in P_0\}$, где $\chi_a(x) = \chi(ax)$, $x \in P_0$, для всех $a \in P_0$. Определим коэффициент кросс-корреляции между функциями f и g равенством

$$C_a(f, g) = \sum_{\mathbf{x} \in P_0^n} \chi_a(f(\mathbf{x}) - g(\mathbf{x})), \quad a \in P_0 \backslash \{0\}.$$

Обозначим

$$C(f, g) = \max_{a \in P_0 \backslash \{0\}} |C_a(f, g)|.$$

Покажем, что $C(f, g) = 0$ тогда и только тогда, когда в множестве $\{f(\mathbf{x}) - g(\mathbf{x}) : \mathbf{x} \in P_0^n\}$ любой элемент из P_0 появляется ровно $\dfrac{|P_0|^n}{|P_0|} = |P_0|^{n-1}$ раз. В обратную сторону утверждение верно в силу равенства $\sum\limits_{c \in P_0} \chi_a(c) = 0$, $a \neq 0$.

Докажем утверждение в прямую сторону. Пусть N — число решений уравнения $f(\mathbf{x}) - g(\mathbf{x}) = b$. Тогда из равенства для любых элементов $c, d \in P_0$

$$\sum_{\chi} \chi(c)\overline{\chi(d)} = \begin{cases} 0, & \text{если } c \neq d, \\ p, & \text{если } c = d, \end{cases}$$

где суммирование осуществляется по всем характерам χ группы $(P_0, +)$, следуют равенства

$$N = \frac{1}{p} \sum_{\mathbf{c} \in P_0^n} \sum_{\chi} \chi(f(\mathbf{c}) - g(\mathbf{c}))\overline{\chi(b)} = p^{n-1} + \frac{1}{p} \sum_{\chi \neq \chi_0} \overline{\chi(b)} \sum_{\mathbf{c} \in P_0^n} \chi(f(\mathbf{c}) - g(\mathbf{c})) = p^{n-1}.$$

В двоичном случае ($P_0 = \{0, 1\}$) имеем

$$C(f, g) = |C_e(f, g)| = \left| \sum_{\mathbf{x} \in \{0,1\}^n} \chi_1(f(\mathbf{x}) - g(\mathbf{x})) \right| = \left| \sum_{\mathbf{x} \in \{0,1\}^n} (-1)^{f(\mathbf{x}) \oplus g(\mathbf{x})} \right|,$$

так как $\chi_1(x) = (-1)^x$ — единственный нетривиальный характер поля GF(2). Чем меньше $C(f,g)$, тем более «различны» функции $f(\mathbf{x})$ и $g(\mathbf{x})$.

Пусть теперь g пробегает всё множество аффинных функций от n переменных над полем P_0, то есть $g(\mathbf{x}) = g(x_1,\ldots,x_n) = a_1x_1 + a_2x_2 + \ldots + a_nx_n + b$, где $a_1,\ldots,a_n,b$ — элементы из P_0. Рассмотрим величину

$$C(f) = \max_g C(f,g) = \max_g \max_{a\in P_0^*} |C_a(f,g)|, \tag{1}$$

которую назовём близостью f к классу всех аффинных функций от n переменных над полем P_0. Вместо функции $g(x) = a_1x_1 + a_2x_2 + \ldots + a_nx_n + b$ достаточно рассмотреть только функции вида $h(x) = a_1x_1 + a_2x_2 + \ldots + a_nx_n$, так как

$$C_a(f,g) = \overline{\chi}_a(b)C_a(f,h), \quad |C_a(f,g)| = |C_a(f,h)|.$$

В работе [4] близость между функциями $f,g : P_0^n \to P_0$ определяется как

$$\delta(f,g) = \frac{p}{p-1}\sum_{y\in P_0}(\mathbf{P}(f-g=y) - 1/p)^2,$$

где вероятность $\mathbf{P}$ определяется при условии, что аргументы функций f и g выбираются случайно и равновероятно. Выразим $\delta(f,g)$ через коэффициенты кросс-корреляции $C_a(f,g)$. Рассмотрим величину

$$N_y(f-g) = |\{\mathbf{x}\in P_0^n : f(\mathbf{x}) - g(\mathbf{x}) = y\}|.$$

Пусть χ_a — аддитивный характер поля P_0. Из равенства

$$\sum_{a\in P_0}\chi_a(x) = \begin{cases} 0, & \text{если } x\neq 0,\\ p, & \text{если } x = 0,\end{cases}$$

следует, что

$$N_y(f-g) = \frac{1}{p}\sum_{\mathbf{x}\in P_0^n}\sum_{a\in P_0}\chi_a(f(\mathbf{x}) - g(\mathbf{x}) - y) = \frac{1}{p}\sum_{a\in P_0}\overline{\chi}_a(y)\sum_{\mathbf{x}\in P_0^n}\chi_a(f(\mathbf{x}) - g(\mathbf{x})) =$$
$$= \frac{1}{p}\sum_{a\in P_0\setminus\{0\}}\overline{\chi}_a(y)C_a(f,g) + p^{n-1}.$$

Тогда

$$P(f-g=y) - 1/p = \frac{N_y(f-g)}{p^n} - \frac{1}{p} =$$
$$= \frac{\dfrac{1}{p}\displaystyle\sum_{a\in P_0^*}\overline{\chi}_a(y)C_a(f,g) + p^{n-1}}{p^n} - \frac{1}{p} = \frac{1}{p^{n+1}}\sum_{a\in P_0^*}\overline{\chi}_a(y)C_a(f,g).$$

С использованием предыдущих равенств получаем

$$\delta(f,g) = \frac{p}{(p-1)p^{2(n+1)}}\sum_{y\in P_0}\left(\sum_{a\in P_0^*}\overline{\chi}_a(y)C_a(f,g)\right)^2 =$$
$$= \frac{p}{(p-1)p^{2(n+1)}}\sum_{y\in P_0}\left(\sum_{a\in P_0^*}\overline{\chi}_a(y)C_a(f,g)\right)\left(\sum_{b\in P_0^*}\overline{\chi}_b(y)C_b(f,g)\right) =$$
$$= \frac{p}{(p-1)p^{2(n+1)}}\sum_{a,b\in P_0^*}C_a(f,g)C_b(f,g)\sum_{y\in P_0}\overline{\chi}_a(y)\overline{\chi}_b(y).$$

Из свойств аддитивных характеров следует, что

$$\sum_{y\in P_0}\overline{\chi}_a(y)\overline{\chi}_b(y)=\begin{cases}0, & \text{если } a+b=0,\\ p & \text{иначе.}\end{cases}$$

Значит,

$$\delta(f,g)=\frac{p^2}{(p-1)p^{2(n+1)}}\sum_{a\in P_0^*}C_a(f,g)C_{-a}(f,g)=\frac{1}{(p-1)p^{2n}}\sum_{a\in P_0^*}|C_a(f,g)|^2.$$

Таким образом, нахождение точных значений коэффициентов кросс-корреляции $C_a(f,g)$ или получение оценок сверху их модулей позволяет соответственно найти величину $\delta(f,g)$ или получить её оценку сверху.

4. Линейная характеристика преобразований конечного поля

Определим линейную характеристику подстановки. Рассмотрим $P=\mathrm{GF}(q)$ — расширение степени n поля $P_0=\mathrm{GF}(p)$, $q=p^n$. Пусть $F: P\to P$, $\alpha_1,\ldots,\alpha_n$ — базис линейного пространства P_{P_0}, $F_1,\ldots,F_n$ — координатные функции отображения F, то есть

$$F(x)=\alpha_1F_1(x)+\ldots+\alpha_nF_n(x)=\alpha_1f_1(x_1,\ldots,x_n)+\ldots+\alpha_nf_n(x_1,\ldots,x_n),$$

где $f_i: P_0^n\to P_0$; $x=\alpha_1x_1+\ldots+\alpha_nx_n$. Введём обозначение

$$C_a^F(\alpha,\beta)=\sum_{x\in P}\chi_a(\alpha x-\beta F(x)),$$

где $\alpha\in P$; $a\in P^*$; $\beta\in P^*$; $\mathrm{Tr}_p^q: P\to P_0$ — функция следа; $\chi_a(y)=e^{2\pi i\frac{\mathrm{Tr}_p^q(ay)}{p}}$ — аддитивный характер поля P. Величину

$$\delta(F)=\max_{\alpha\in P,\beta\in P^*,a\in P_0^*}\left|C_a^F(\alpha,\beta)\right|=\max_{\alpha\in P,\beta\in P^*,a\in P_0^*}\left|\sum_{x\in P}\chi_a(\alpha x-\beta F(x))\right|$$

будем называть линейной характеристикой преобразования F. Пусть $\beta_1,\ldots,\beta_n$ — базис, двойственный к базису $\alpha_1,\ldots,\alpha_n$, то есть такой, что выполнено условие

$$\mathrm{Tr}_p^q(\alpha_i\beta_j)=\begin{cases}0, & \text{если } i\neq j,\\ 1, & \text{если } i=j.\end{cases}$$

Такой базис существует [3]. Пусть элементы $a_1,\ldots,a_n,c_1,\ldots,c_n\in P_0$ такие, что

$$\alpha=\beta_1a_1+\ldots+\beta_na_n,\beta=\beta_1c_1+\ldots+\beta_nc_n,$$

тогда

$$\beta F(x)=\left(\sum_{i=1}^n\beta_ic_i\right)\left(\sum_{j=1}^n\alpha_jf_j(x_1,\ldots,x_n)\right)=\sum_{i,j\in\{1,\ldots,n\}}\alpha_j\beta_if_j(x_1,\ldots,x_n)c_i,$$

$$\alpha x=\left(\sum_{i=1}^n\beta_ia_i\right)\left(\sum_{j=1}^n\alpha_jx_j\right)=\sum_{i,j\in\{1,\ldots,n\}}\alpha_j\beta_ix_ja_i,$$

$$\chi_a(\alpha x-\beta F(x))=\exp\left\{2\pi i\frac{1}{p}\mathrm{Tr}_p^q\left(a(\sum_{i,j\in\{1,\dots,n\}}\alpha_j\beta_i x_j a_i-\sum_{i,j\in\{1,\dots,n\}}\alpha_j\beta_i f_j(x_1,\dots,x_n)c_i)\right)\right\}=$$

$$=\exp\left\{2\pi i\frac{a}{p}\left(\sum_{i,j\in\{1,\dots,n\}}\mathrm{Tr}_p^q(\alpha_j\beta_i x_j a_i)-\sum_{i,j\in\{1,\dots,n\}}\mathrm{Tr}_p^q(\alpha_j\beta_i f_j(x_1,\dots,x_n)c_i)\right)\right\}=$$

$$=\exp\left\{2\pi i\frac{a}{p}\left(\sum_{j\in\{1,\dots,n\}}x_j a_j-\sum_{j\in\{1,\dots,n\}}f_j(x_1,\dots,x_n)c_j\right)\right\}.$$

Отсюда, согласно обозначениям п. 3,

$$\left|C_a^F(\alpha,\beta)\right|=\left|\sum_{\mathbf{x}\in P_0^n}\chi_a\left(\sum_{j=1}^n a_jx_j-\sum_{j=1}^n f_j(x_1,\dots,x_n)c_j\right)\right|=\left|C_a\left(\sum_{j=1}^n a_jx_j,\sum_{j=1}^n f_j(x_1,\dots,x_n)c_j\right)\right|.$$

Значит,

$$\delta(F)=\max_{\alpha\in P,\beta\in P^*,a\in P_0^*}\left|C_a^F(\alpha,\beta)\right)|=$$

$$=\max_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}\max_{\mathbf{a}\in P_0^n}\max_{a\in P_0^*}\left|C_a\left(\sum_{j\in\{1,\dots,n\}}x_ja_j,\sum_{j\in\{1,\dots,n\}}f_j(x_1,\dots,x_n)c_j\right)\right|.$$

Согласно формуле (1), $\delta(F)=\max\limits_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}C\left(\sum\limits_j f_j(x_1,\dots,x_n)c_j\right)$. Таким образом, $\delta(F)$ — максимальная близость нетривиальных линейных комбинаций координатных функций преобразования F к классу всех аффинных функций от n переменных над полем P_0. Кроме того, заметим, что при фиксированном $a\in P_0^*$

$$\max_{\alpha\in P,\beta\in P^*}\left|C_a^F(\alpha,\beta)\right|=\max_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}\max_{\mathbf{a}\in P_0^n}\left|C_a\left(\sum_{j=1}^n x_ja_j-\sum_{j=1}^n f_j(x_1,\dots,x_n)c_j\right)\right|=$$

$$=\max_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}\max_{\mathbf{a}\in P_0^n}\left|C_e\left(\sum_j ax_ja_j-\sum_j af_j(x_1,\dots,x_n)c_j\right)\right|=$$

$$=\max_{\mathbf{c}\in P_0^n\setminus\{\mathbf{0}\}}\max_{\mathbf{a}\in P_0^n}\left|C_e\left(\sum_j x_ja_j-\sum_j f_j(x_1,\dots,x_n)c_j\right)\right|=\max_{\alpha\in P,\beta\in P^*}\left|C_e^F(\alpha,\beta)\right|.$$

В итоге

$$\delta(F)=\max_{\alpha\in P,\beta\in P^*}\left|C_e^F(\alpha,\beta)\right|.$$

Этой формулой будем пользоваться всюду в дальнейшем. В случае поля чётной характеристики такое определение линейной характеристики используется в работе [2]. В [5] определяется функция согласия, которая отличается от функции δ только нормирующим множителем.

Оценим снизу величину $\delta(F)$, где F — подстановка поля P. Для этого выведем аналог равенства Парсеваля для коэффициентов Уолша — Адамара булевой функции:

$$\sum_{\alpha\in P}\sum_{\beta\in P^*}\left|C_e^F(\alpha,\beta)\right|^2=\sum_{\alpha\in P}\sum_{\beta\in P^*}C_e^F(\alpha,\beta)\overline{C_e^F(\alpha,\beta)}=$$

$$=\sum_{\alpha\in P}\sum_{\beta\in P^*}\left(\sum_{x\in P}\chi(\alpha x+\beta F(x))\right)\left(\sum_{y\in P}\chi(-\alpha y-\beta F(y))\right)=$$

$$=\sum_{x\in P}\sum_{\beta\in P^*}\sum_{y\in P}\chi(\beta(F(x)-F(y)))\sum_{\alpha\in P}\chi(\alpha(x-y))=\sum_{x\in P}\sum_{\beta\in P^*}\sum_{y\in P}\chi(\beta(F(x)-F(y)))q\delta_{x,y},$$

где

$$\delta_{x,y} = \begin{cases} 0, & \text{если } x \neq y, \\ 1, & \text{если } x = y. \end{cases}$$

Значит,

$$\sum_{\alpha\in P}\sum_{\beta\in P^*}\left|C_e^F(\alpha,\beta)\right|^2 = \sum_{x\in P}\sum_{y\in P} q\delta_{x,y}\sum_{\beta\in P^*}\chi(\beta(F(x)-F(y))) =$$
$$= \sum_{x\in P}\sum_{y\in P} q\delta_{x,y}\left(q\delta_{x,y}-1\right) = q^2(q-1).$$

Следовательно,

$$\delta(F) = \max_{\alpha\in P,\beta\in P^*}\left|C_e^F(\alpha,\beta)\right| \geqslant \sqrt{q}.$$

5. Линейная характеристика кусочно-аффинных подстановок

Исследуем некоторые свойства линейной характеристики кусочно-аффинных подстановок. Пусть $P = \mathrm{GF}(q)$, χ — канонический аддитивный характер поля P, определяемый равенством

$$\chi(y) = e^{2\pi i\frac{\mathrm{Tr}(y)}{p}}, y \in P,$$

где $\mathrm{Tr}(y)$ — функция абсолютного следа поля P.

Теорема 4. Пусть $\Delta_{(\mathbf{c},\mathbf{e})}^{(\mathbf{a},\mathbf{b})} = F \in A_d(P)$ и элементы $a_0^{-1}c_0, \ldots, a_{d-1}^{-1}c_{d-1}$ попарно различные. Если для любых $\alpha \in P$, $\beta \in P^*$:

1) среди элементов $\alpha a_j - \beta c_j$, $j \in \{0,\ldots,d-1\}$, нет нулевого, то

$$\left|C_e^F(\alpha,\beta) - \delta_1\right| \leqslant (d-1)\sqrt{q},$$

где

$$\delta_1 = \chi(\alpha b_d - \beta e_d) - \frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j - \beta e_j);$$

2) среди элементов $\alpha a_j - \beta c_j$, $\alpha \in P$, $\beta \in P^*$, $j \in \{0,\ldots,d-1\}$, есть нулевой $\alpha a_{j_0} + \beta c_{j_0} = 0$, то

$$\left|C_e^F(\alpha,\beta) - \delta_2\right| \leqslant \frac{(d-1)^2}{d}\sqrt{q},$$

где

$$\delta_2 = \chi(\alpha b_d - \beta e_d) - \frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j - \beta e_j) + \left(l + \frac{1}{d}\right)\chi(\alpha b_{j_0} - \beta e_{j_0}).$$

Доказательство. Для произвольных $\alpha \in P$, $\beta \in P^*$ имеем равенство

$$C_e^F(\alpha,\beta) = \sum_{x\in P}\chi(\alpha x - \beta F(x)).$$

Получим далее

$$C_e^F(\alpha,\beta) = \chi(\alpha b_d - \beta e_d) + \sum_{j=0}^{d-1}\sum_{x\in H_{a_j,b_j}}\chi(\alpha x - \beta((x-b_j){a_j}^{-1}c_j + e_j)) =$$

$$= \chi(\alpha b_d - \beta e_d) + \sum_{j=0}^{d-1}\sum_{x\in H_{a_j,b_j}}\chi(\alpha x - \beta x{a_j}^{-1}c_j - \beta(-b_j{a_j}^{-1}c_j + e_j)) =$$

$$= \chi(\alpha b_d - \beta e_d) + \sum_{j=0}^{d-1}\sum_{x\in H}\chi(\alpha x a_j + \alpha b_j - \beta x c_j - \beta{a_j}^{-1}c_j b_j - \beta(-b_j{a_j}^{-1}c_j + e_j)).$$

Тогда

$$C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)+\sum_{j=0}^{d-1}\sum_{x\in H}\chi((\alpha a_j-\beta c_j)x)\chi(\alpha b_j-\beta e_j). \tag{2}$$

Введём обозначение $\gamma_j=\alpha-\beta a_j^{-1}c_j$. Заметим, что по условию теоремы числа $a_0^{-1}c_0$, $\ldots$, $a_{d-1}^{-1}c_{d-1}$ попарно различны. Поэтому при фиксированных элементах $\alpha\in P$, $\beta\in P^*$ элементы $\gamma_0,\ldots,\gamma_{d-1}$ попарно различны и возможен один из двух случаев:

а) $\gamma_j\neq 0$ для всех $j\in\{0,\ldots,d-1\}$ (среди них нет нуля);

б) существует $j_0\in\{0,\ldots,d-1\}$, такой, что $\gamma_{j_0}=0$, и $\gamma_j\neq 0$ для всех $j\in\{0,\ldots,d-1\}\backslash\{j_0\}$ (среди них есть один нуль).

Пусть имеет место случай «а». Воспользуемся разложением аддитивного характера χ по мультипликативным характерам поля P [3]:

$$\chi(y)=\frac{1}{q-1}\sum_{\psi}G(\overline{\psi},\chi)\psi(y),\ y\in P^*,$$

где сумма берётся по всем мультипликативным характерам ψ поля P; $\overline{\psi}$ — характер, сопряжённый для характера ψ; $G(\psi,\chi)$ — сумма Гаусса, определяемая равенством

$$G(\psi,\chi)=\sum_{c\in P^*}\psi(c)\chi(c).$$

Из (2) получим

$$C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)+\frac{1}{dl}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)\sum_{\psi}G(\overline{\psi},\chi)\psi(\alpha a_j-\beta c_j)\sum_{x\in H}\psi(x).$$

Учитывая равенство

$$\sum_{x\in H}\psi(x)=\begin{cases}|H|, & \text{если } \psi\in\operatorname{Ann}(H),\\ 0, & \text{если } \psi\notin\operatorname{Ann}(H),\end{cases}$$

где $\operatorname{Ann}(H)$ — аннулятор группы $H=\langle\xi^d\rangle$, состоящий из всех мультипликативных характеров ψ поля P, для которых $\psi(\xi^d)=1$, получим

$$C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)+\frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)\sum_{\psi\in\operatorname{Ann}(H)}G(\overline{\psi},\chi)\psi(\alpha a_j-\beta c_j).$$

Пусть ψ_0 — тривиальный мультипликативный характер. Тогда, учитывая равенства $dl=q-1$ и $G(\overline{\psi_0},\chi)=-1$, получим

$$\begin{aligned}C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)-\frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)+\\ +\frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)\sum_{\psi\in\operatorname{Ann}(H)\backslash\{\psi_0\}}G(\overline{\psi},\chi)\psi(\alpha a_j-\beta c_j).\end{aligned} \tag{3}$$

Учитывая равенства $|\chi(x)|=1$, $|\psi(y)|=1$ для любых $y\in P^*$, $x\in P$; $|\operatorname{Ann}(H)|=d$; $|G(\psi,\chi)|=\sqrt{q}$ для всех $\psi\neq\psi_0$; $\delta_1=\chi(\alpha b_d-\beta e_d)-\frac{1}{d}\sum_{j=0}^{d-1}\chi(\alpha b_j-\beta e_j)$, получим оценку

$$|C_e^F(\alpha,\beta)-\delta_1|\leqslant\frac{1}{d}(d-1)\sqrt{q}d=(d-1)\sqrt{q}. \tag{4}$$

Пусть имеет место случай «б»: $\gamma_{j_0}=0$ для некоторого индекса $j_0\in\{0,\dots,d-1\}$ и $\gamma_j\neq 0$ для всех $j\neq j_0$. Учитывая, что $\chi(0)=1$, из равенства (2) получим

$$C_e^F(\alpha,\beta)=\chi(\alpha b_d-\beta e_d)+\sum_{x\in H}\chi(\alpha b_{j_0}-\beta e_{j_0})+\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\sum_{x\in H}\chi((\alpha a_j-\beta c_j)x)\chi(\alpha b_j-\beta e_j)=$$
$$=\chi(\alpha b_d-\beta e_d)+\sum_{x\in H}\chi(\alpha b_{j_0}-\beta e_{j_0})+$$
$$+\frac{1}{dl}\sum_{\psi}G(\overline{\psi},\chi)\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\psi(\alpha a_j-\beta c_j)\chi(\alpha b_j-\beta e_j)\sum_{x\in H}\psi(x)=\chi(\alpha b_d-\beta e_d)+$$
$$+l\chi(\alpha b_{j_0}-\beta e_{j_0})+\frac{1}{d}\sum_{\psi\in\mathrm{Ann}(H)}G(\overline{\psi},\chi)\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\psi(\alpha a_j-\beta c_j)\chi(\alpha b_j-\beta e_j)=$$
$$=\chi(\alpha b_d-\beta e_d)-\frac{1}{d}\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\chi(\alpha b_j-\beta e_j)+l\chi(\alpha b_{j_0}-\beta e_{j_0})+ \tag{5}$$
$$+\frac{1}{d}\sum_{\psi\in\mathrm{Ann}(H)\setminus\{\psi_0\}}G(\overline{\psi},\chi)\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\psi(\alpha a_j-\beta c_j)\chi(\alpha b_j-\beta e_j)=$$
$$=\chi(\alpha b_d-\beta e_d)-\frac{1}{d}\sum_{j\in\{0,\dots,d-1\}}\chi(\alpha b_j-\beta e_j)+\left(l+\frac{1}{d}\right)\chi(\alpha b_{j_0}-\beta e_{j_0})+$$
$$+\frac{1}{d}\sum_{\psi\in\mathrm{Ann}(H)\setminus\{\psi_0\}}G(\overline{\psi},\chi)\sum_{j\in\{0,\dots,d-1\}\setminus\{j_0\}}\psi(\alpha a_j-\beta c_j)\chi(\alpha b_j-\beta e_j).$$

Получаем оценку

$$|C_e^F(\alpha,\beta)-\delta_2|\leqslant\frac{1}{d}(d-1)\sqrt{q}(d-1)=\frac{(d-1)^2}{d}\sqrt{q}. \tag{6}$$

Объединяя (4) и (6), получаем требуемый результат. ■

6. Частные случаи и примеры

Лемма 3. Пусть $F:P\to P$ — произвольное преобразование поля P, $g,h\in$ $\in AGL(1,P)$. Тогда $|C_a^F(\alpha a^{-1},\beta c)|=|C_a^{gFh}(\alpha,\beta)|$.

Доказательство. Пусть $g(x)=ax+b$, $h(x)=cx+e$. Тогда справедливы следующие равенства:

$$C_a^{gFh}(\alpha,\beta)=\sum_{x\in P}\chi_a\left(\alpha x-\beta h(F(g(x)))\right)=$$
$$=\sum_{x\in P}\chi_a\left(\alpha g^{-1}(x)-\beta h(F(x))\right)=\sum_{x\in P}\chi_a\left(\alpha xa^{-1}-\alpha a^{-1}b-\beta cF(x)-\beta e\right)=$$
$$=\sum_{x\in P}\chi_a\left(\alpha a^{-1}x-\beta cF(x)\right)\chi_a\left(-\alpha a^{-1}b-\beta e\right)==\chi_a\left(-\alpha a^{-1}b-\beta e\right)C_a^F(\alpha a^{-1},\beta c).$$

Остаётся заметить, что $|\chi_a(-\alpha a^{-1}b-\beta e)|=1$. ■

Следствие 2. В условиях леммы 3 $\delta(F)=\delta(gFh)$.

Утверждение 3. Пусть $q>9$, $F\in A_2(P)$. Тогда $\delta(F)\in\left\{\dfrac{q\pm\sqrt{q}}{2},\dfrac{\sqrt{q^2+q}}{2},q\right\}$.

Доказательство. Из лемм 1 и 2 следует, что $R_2(P)=Rl_2(P)$ при $q>5$. Из п. 7 утверждения 1 следует $A_2(P)=V^+(P)L_2(P)V^+(P)$. Используя лемму 3, получаем, что для любой подстановки $F=\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\mathbf{b}}\in A_2(P)$ существует $W=\Delta_{\mathbf{c},\theta}^{\mathbf{a},\theta}$, такая, что

$\delta(F) = \delta(W)$. Пусть $\langle \xi^2 \rangle = H < P^*$ — подгруппа, образованная всеми ненулевыми элементами поля P, возведёнными в квадрат. Заметим, что векторы (Ha_0, Ha_1), (Hc_0, Hc_1), $(H, H\xi)$ совпадают при некоторой перестановке координат. Тогда если $c_0/a_0 = c_1/a_1$, то для любого $h \in Ha_0$ верно $W(h) = hc_0/a_0$, для $h \in Ha_1$ верно $W(h) = hc_1/a_1$ и $W(0) = 0$, то есть W действует так же, как $g(x) = x \cdot c_0/a_0$, следовательно, W — линейная подстановка и $\delta(W) = q$.

Пусть $c_0/a_0 \neq c_1/a_1$. Тогда дословно повторим рассуждения теоремы 4 о значении $\delta(W)$, а именно: если в теореме 4 имеет место случай «а», то воспользуемся равенством (3) и при подстановке известных значений получим

$$C_e^W(\alpha, \beta) = \frac{1}{2}\left(G(\eta, \chi)\eta(\alpha a_0 - \beta c_0) + G(\eta, \chi)\eta(\alpha a_1 - \beta c_1)\right) \in \{\pm G(\eta, \chi), 0\},$$

где η — квадратичный характер. Если имеет место случай «б», то, используя равенство (5), получим

$$C_e^W(\alpha, \beta) = \frac{q}{2} + \frac{1}{2}G(\eta, \chi)\eta(\alpha a_j - \beta c_j), \text{ где } j \in \{0, 1\}.$$

Известно [3], что

$$G(\eta, \chi) = \begin{cases} (-1)^{n-1}\sqrt{q}, & \text{если } p \equiv 1 \pmod 4, \\ (-1)^{n-1} i^n \sqrt{q}, & \text{если } p \equiv 3 \pmod 4. \end{cases}$$

Значит, если $p \equiv 1 \pmod 4$ или $p \equiv 3 \pmod 4$ и при этом $2|n$, то $|C_e^W(\alpha, \beta)| \in \in \left\{\frac{q - \sqrt{q}}{2}, \frac{q + \sqrt{q}}{2}\right\}$; если $p \equiv 3 \pmod 4$ и $2 \not| n$, то $|C_e^W(\alpha, \beta)| = \frac{\sqrt{q^2 + q}}{2}$. Таким образом,

$$|C_e^W(\alpha, \beta)| \in \left\{0, \frac{q - \sqrt{q}}{2}, \frac{q + \sqrt{q}}{2}, \frac{\sqrt{q^2 + q}}{2}, \sqrt{q}\right\}.$$

Заметим, что $\delta(F) \neq 0$, так как при вычислении $\delta(F)$ всегда существуют такие α, β, что имеет место только случай «б» теоремы 4. Если $q > 9$, то $\frac{q - \sqrt{q}}{2} > \sqrt{q}$, и тогда

$$\delta(F) = \begin{cases} \frac{q \pm \sqrt{q}}{2}, & \text{если } (p \equiv 1 \pmod 4) \vee (p \equiv 3 \pmod 4) \wedge 2 \mid n), \\ \frac{\sqrt{q^2 + q}}{2} & \text{иначе.} \end{cases}$$

Утверждение доказано. ■

Пример 1. Рассмотрим подстановку в поле GF(13):

$$(\mathbf{a}, \mathbf{0}) = ((1, 2, 4, 8), (0, 0, 0, 0, 0)) \in Rl_4(\mathrm{GF}(13)),$$

$$(\mathbf{c}, \mathbf{e}) = ((3, 4, 1, 9), (5, 0, 2, 6, 0)) \in R_4(\mathrm{GF}(13)),$$

$$\delta(\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\mathbf{0}})/q = 6{,}5/13 = 1/2.$$

7. О многочленах, соответствующих кусочно-аффинным подстановкам

Введём обозначение

$$\mathrm{pol}(x) = \sum_{i=0}^{d-1} x^{il} = x^{dl} + x^{(d-1)l} + \ldots + x^{l}.$$

Данный многочлен интересен для кусочных относительно H функций своими значениями:

$$\mathrm{pol}(h) = \begin{cases} d, & \text{если } h \in H, \\ 0 & \text{иначе.} \end{cases}$$

Используя $\mathrm{pol}(x)$, можно составить аналог интерполяционного многочлена Лагранжа для кусочно-аффинных подстановок.

Утверждение 4. Пусть $\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\mathbf{b}} \in A_d(P)$. Тогда

$$\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\mathbf{b}}(x) = (1-(x-b_d)^{q-1})e_d + \sum_{i=0}^{d-1} \left((x-b_i)a_i^{-1}c_i + e_i\right) \mathrm{pol}\left((x-b_i)a_i^{-1}\right) d^{-1}.$$

Доказательство. Заметим, что d^{-1} существует, так как d и p — взаимно простые числа. Нетрудно заметить, что $\mathrm{pol}\left((x-b_i)a_i^{-1}\right) d^{-1}$ принимает значение 1 на $Ha_i + b_i$ и 0 на остальных элементах поля P. Корректное отображение b_d в e_d обеспечивает слагаемое $(1-(x-b_d)^{q-1})e_d$. ■

Следствие 3. Для любой подстановки вида $\Delta_{\mathbf{c},\theta}^{\mathbf{a},\theta} \in L_d(P)$ существуют $f_0, \ldots, f_{d-1} \in P$, такие, что

$$\Delta_{\mathbf{c},\theta}^{\mathbf{a},\theta}(x) = x \sum_{i=0}^{d-1} f_i x^{il}.$$

Для любой подстановки вида $\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\theta} \in A_d(P)$ существуют $f_0, \ldots, f_{d-1}, h_0, \ldots, h_{d-1} \in P$, такие, что

$$\Delta_{\mathbf{c},\mathbf{e}}^{\mathbf{a},\theta}(x) = x \sum_{i=0}^{d-1} f_i x^{il} + \sum_{i=0}^{d-1} h_i x^{il} + (1-x^{q-1})e_d.$$

Утверждение 5. Подстановка, задаваемая многочленом x^s, является кусочно-линейной из $L_d(P)$ тогда и только тогда, когда $l|(s-1)$ и $(s, q-1) = 1$, где $dl = q-1$.

Доказательство. Сразу заметим, что условие $(s, q-1) = 1$ равносильно тому, что x^s задает подстановку в поле $\mathrm{GF}(q)$. Пусть x^s задает подстановку $\Delta_{\mathbf{c},\theta}^{\mathbf{a},\theta} \in L_d(P)$, тогда найдётся $i \in \{0, \ldots, d-1\}$, что $a_i \in H$. Так как $(H, \cdot)$ — группа, x^s отображает блок H в себя так, что $x^s(h) = ha_i^{-1}c_i \in H$ для любого $h \in H$. Значит, $a_i^{-1}c_i \in H$. Заметим, что $x^s(1) = 1$, тогда $a_i^{-1}c_i = 1$. Из равенств $x^s(\xi^d) = \xi^{ds} = \xi^d a_i^{-1}c_i = \xi^d$ следует, что $\xi^{d(s-1)} = 1$, $q-1|d(s-1)$, а значит, $l|(s-1)$.

Пусть $l|(s-1)$, следовательно, $\xi^{ds} = \xi^d$. Достаточно показать, что x^s является кусочно-линейной функцией, то есть $x^s(ha) = hc$ для любого $h \in H$ и некоторых $a, c \in P^*$. Действительно, $x^s(ha) = h^s a^s = ha^s = hc$. ■

8. Группа, образуемая кусочно-аффинными подстановками, и группа кусочно-линейных подстановок

Пусть $G_d(P)$ — группа, порождённая всеми кусочно-аффинными подстановками. Нетрудно заметить, что $L_d(P)$ — группа.

Утверждение 6.

1) $L_d(P)$ имеет две орбиты — P^* и $\{0\}$;
2) пусть $W = \{H, H\xi, \ldots, H\xi^{d-1}\}$, $R \in W$. Тогда $f(R) \in W$ для любой подстановки $f \in L_d(P)$, то есть сохраняется структура смежного класса по подгруппе H;
3) $G_d(P)$ 2-транзитивна;
4) $G_d(P)$ примитивна.

Доказательство. Пункты 1 и 2 очевидны; п. 3 следует из того, что $AGL(1, P)$ 2-транзитивна и лежит в $A_d(P)$; п. 4 непосредственно следует из п. 3. ■

Минимальной степенью группы $G < S(\Omega)$ будем называть число

$$\mu(G) = \min\{|\mathrm{supp}(g)| : g \in G\backslash\{e\}\},$$

где $\mathrm{supp}(g) = \{\alpha \in P : g(\alpha) \neq \alpha\}$.

Приведём формулировку теоремы из работы [6, с. 155].

Теорема 5. Пусть 2-транзитивная группа $G < S_n$ не содержит группу A_n — знакопеременную группу. Тогда имеют место следующие оценки:

1) $\mu(G) > \sqrt{n-1} + 1 \geqslant \sqrt{n}$ для всех n;
2) $\mu(G) \geqslant n/8$ для всех n;
3) $\mu(G) \geqslant n/4$ для всех $n > 216$.

Следствие 4. Пусть $1 < l \leqslant d$, где $l = |H|$. Тогда $G_d(P)$ содержит знакопеременную группу поля P.

Доказательство. Выберем произвольную пару $(\mathbf{a}, \mathbf{b}) \in R_d(P)$. Заметим, что

$$(\mathbf{c}, \mathbf{b}) = ((a_0\xi^d, a_1, \ldots, a_{d-1}), \mathbf{b}) \in R_d(P),$$

так как $H_{a_0,b_0} = H_{a_0\xi^d,b_0}$. Рассмотрим подстановку $g = \Delta^{(\mathbf{a},\mathbf{b})}_{(\mathbf{c},\mathbf{b})}$. Легко видеть, что при $l > 1$

$$\mathrm{supp}(g) = H_{a_0,b_0}.$$

Из того, что $l \leqslant d$, $ld = q - 1$, следует соотношение $l \leqslant \sqrt{q-1}$, то есть

$$\mu(G_d(P)) \leqslant |\mathrm{supp}(g)| = l \leqslant \sqrt{q-1}.$$

Остаётся воспользоваться теоремой 5 и утверждением 6. ■

Следствие 5. Если $1 < l \leqslant d$, то $G_d(P) = S(P)$.

Доказательство. Заметим, что подстановка $g = \Delta^{(\mathbf{a},\mathbf{b})}_{(\mathbf{c},\mathbf{b})}$, определённая в доказательстве следствия 4, является циклом длины l, а именно $g(\xi^{kd}a_0 + b_0) = \xi^{(k+1)d}a_0 + b_0$. Если l чётное, то $g \notin A(P)$, следовательно, $G_d(P) = S(P)$. Пусть l нечётное. Определим подстановку $f = \Delta^{(\mathbf{a},\mathbf{b})}_{(\mathbf{c},\mathbf{b})}$, где $(\mathbf{a}, \mathbf{b}) \in R_d(P)$, $(\mathbf{c}, \mathbf{b}) = ((a_1, a_0, a_2, \ldots, a_{d-1}), (b_1, b_0, b_2, \ldots, b_d)) \in R_d(P)$. Из определения $\Delta^{(\mathbf{a},\mathbf{b})}_{(\mathbf{c},\mathbf{b})}$ следует, что

$$f = (a_0 + b_0, a_1 + b_1)(\xi^d a_0 + b_0, \xi^d a_1 + b_1) \cdots (\xi^{d(l-1)}a_0 + b_0, \xi^{d(l-1)}a_1 + b_1),$$

то есть f — произведение нечётного числа транспозиций. Следовательно, $f \notin A(P)$ и $G_d(P) = S(P)$. ■

9. Результаты эксперимента

В ходе выполнения работы написана программа, выполняющая построение множества $R_d(P)$. При изучении этого множества для малых значений d и q получены следующие результаты:

1) Если $d < l$, то $R_d(P) = Rl_d(P)$. Это подтвердилось на следующих парах (d, q): (3,16), (3,64), (7,64), (3,256), (5,256), (7,512), (3,1024), (11,1024), (2,17), (4,81), (5,81), (8,81), (4,25), (6,37).
2) В случае $d = l$ справедливы два результата: $R_d(P) = Rl_d(P)$ или $R_d(P) = Rl_d(P) \sqcup C_d(P)$, где $C_d(P)$ состоит из пар вида $(\mathbf{a}, \mathbf{b}) = ((\alpha, \alpha, \ldots, \alpha), (b_0, b_1, \ldots, b_d))$. Первое равенство подтвердилось для следующих значений (d, q): (6, 37), (10, 101), (13,197). Второе равенство выполняется при $(d, q) = (4, 17)$.
3) Если $d > l$, то $R_d(P) \neq Rl_d(P)$. Это подтвердилось на следующих парах (d, q): (4,13), (5,16), (6,25), (8, 25), (9,64), (12, 37), (21, 64).

ЛИТЕРАТУРА

1. *Evans A. B.* Orthomorphism Graphs of Groups. Lecture Notes in Mathematics. Berlin: Springer Verlag, 1992. 114 p.
2. *Тришин А. Е.* О показателе нелинейности кусочно-линейных подстановок аддитивной группы поля F_{2^n} // Прикладная дискретная математика. 2015. № 4(30). С. 32–42
3. *Лидл Р., Нидеррайтер Г.* Конечные поля: в 2-х т.: пер. с. англ. М.: Мир, 1988. 822 с.
4. *Солодовников В. И.* О совпадении класса бент-функций с классом функций, минимально близких к линейным // Прикладная дискретная математика. 2012. № 3(17). С. 25–33.
5. *Кузьмин А. С., Марков В. Т., Нечаев А. А. и др.* Бент-функции и гипербент-функции над полем из 2^l элементов // Проблемы передачи информации. 2008. Т. 44. № 1. С. 15–37.
6. *Dixon J. and Mortimer B.* Permutation Groups. Berlin; N. Y.: Springer Verlag, 1996. 346 p.

REFERENCES

1. *Evans A. B.* Orthomorphism Graphs of Groups. Lecture Notes in Mathematics, Berlin, Springer Verlag, 1992. 114 p.
2. *Trishin A. E.* O pokazatele nelineynosti kusochno-lineynykh podstanovok additivnoy gruppy polya F_{2^n} [The nonlinearity index is a piecewise-linear substitution of the additive group of the field F_{2^n}]. Prikladnaya diskretnaya matematika, 2015, no. 4(30), pp. 32–42 (in Russian)
3. *Lidl R., Niderrayter G.* Konechnye polya [Finite Fields]. Moscow, Mir Publ., 1988, vol. 1, 2. 822 p. (in Russian)
4. *Solodovnikov V. I.* O sovpadenii klassa bent-funktsiy s klassom funktsiy, minimal'no blizkikh k lineynym [On the coincidence of the class of bent-functions with the class of functions which are minimally close to linear functions]. Prikladnaya diskretnaya matematika, 2012, no. 3(17), pp. 25–33. (in Russian)
5. *Kuz'min A. S., Markov V. T., Nechaev A. A., et al.* Bent and hyper-bent functions over a field of 2^l elements. Problems of Information Transmission, 2008, vol. 44, no. 1, pp. 12–33.
6. *Dixon J. and Mortimer B.* Permutation Groups. Berlin, N. Y., Springer Verlag, 1996. 346 p.