УДК 519.719.2 DOI 10.17223/20710410/66/5

ОРТОМОРФИЗМЫ ГРУПП С МИНИМАЛЬНО ВОЗМОЖНЫМИ ПОПАРНЫМИ РАССТОЯНИЯМИ

С. В. Спиридонов

Лаборатория ТВП, г. Москва, Россия

E-mail: SpiridonovSV00@yandex.ru

Изучаются ортоморфизмы групп, находящиеся на минимально возможном расстоянии друг от друга по метрике Кэли. Описан класс преобразований, переводящих произвольный заданный ортоморфизм в множество всех ортоморфизмов, находящихся от исходного на минимально возможном расстоянии Кэли, равном двум. С помощью спектрально-разностного метода построения подстановок над обобщённой группой кватернионов Q_{4n}, $4n = 2^t$ $(t = 4, \ldots, 8)$, найдены ортоморфизмы с близкими к оптимальным значениями разностных характеристик.

Ключевые слова: *ортоморфизм, латинский квадрат, ортогональные латинские квадраты, метрика Кэли, s-бокс, нелинейное преобразование, подстановка, обобщённая группа кватернионов.*

ORTHOMORPHISMS OF GROUPS WITH MINIMAL POSSIBLE PAIRWISE DISTANCES

S. V. Spiridonov

TVP Laboratory, Moscow, Russia

Orthomorphisms of groups, which are at the minimum possible distance from each other according to the Cayley metric are studied. A class of transformations is described that map an arbitrary given orthomorphism into the set of all orthomorphisms that are at the minimum possible Cayley distance of two from the original. Using the spectral-difference method for constructing substitutions over the generalized quaternion group Q_{4n}, where $4n = 2^t$ $(t = 4, \ldots, 8)$, orthomorphisms with values of difference characteristics close to optimal have been found.

Keywords: *orthomorphism, Latin square, orthogonal Latin squares, Cayley metric, s-box, nonlinear transformation, substitution, generalized quaternion group.*

Введение

Понятие ортоморфизма впервые введено в работах [1, 2]. В терминах вполне перестановочных многочленов поля $\mathbb{F}_q$ ортоморфизмы детально изучались в [3, 4], некоторые подходы к построению ортоморфизмов приведены в [5, 6]. Ортоморфизмы активно изучались в 50–60-е годы XX в. в связи с некоторыми техническими приложениями как частный случай «проблемы параллельных перепаек» [7]. Ортоморфизмы находят широкое применение во многих криптографических конструкциях [8, 9]. Их изучение тесно связано с задачами построения кодов аутентификации [10, 11], систем ортогональных латинских квадратов [12–14] и квазигрупп [15, 16]. Необходимость развития методов построения ортоморфизмов над произвольными группами возникает в связи

с появлением ряда работ о неабелевых группах наложения ключа и их использовании при синтезе шифрсистем [17–19].

В данной работе результаты [6] обобщаются на произвольную группу G. Предложены алгоритмы, позволяющие для заданного ортоморфизма получить все ортоморфизмы, находящиеся на минимально возможном расстоянии от него. Описан класс преобразований, переводящих произвольный заданный ортоморфизм в множество всех ортоморфизмов, находящихся от исходного на минимально возможном расстоянии Кэли, равном двум. Полученные результаты иллюстрируются примерами над обобщённой группой кватернионов Q_{4n}.

Работа имеет следующую структуру. Пункт 1 содержит основные определения и обозначения, необходимые для дальнейшего изложения результатов. В п. 2 приведены утверждения, касающиеся свойств ортоморфизмов, находящихся на минимально возможном расстоянии Кэли друг от друга, и алгоритмы построения всех таких ортоморфизмов. Пункт 3 содержит результаты по построению ортоморфизмов с близкими к оптимальным значениями разностных характеристик.

1. Основные определения и обозначения

В работе используются следующие обозначения:

$(G, *)$	—	конечная группа с бинарной операцией $*$ и нейтральным элементом e;
$G^\times$	—	множество элементов группы G без нейтрального элемента e;
$S(G)$	—	симметрическая группа на множестве G;
A_m^k	—	число различных размещений из m элементов по k;
C_m^k	—	число различных сочетаний из m элементов по k;
Q_{4n}	—	обобщённая группа кватернионов порядка $4n$.

Определение 1. Подстановка $g \in S(G)$ называется *ортоморфизмом* группы G, если отображение $g' : G \to G$, определяемое условием $g'(x) = x^{-1} * g(x)$, где x^{-1} — элемент, обратный для $x \in G$ относительно операции $*$, является подстановкой из $S(G)$.

Множество всех ортоморфизмов группы G обозначим через $\mathrm{Orth}(G)$. На элементах группы G вводится произвольное отношение порядка:

$$G = \{e = z_0, z_1, \ldots, z_{n-1}\}, \quad |G| = n, \quad z_i < z_{i+1}, \quad i = 0, 1, \ldots, n-2.$$

Определение 2. *Расстоянием Кэли* между подстановками $g, h \in S(G)$ называется число

$$\tau(g, h) = \sum_{i=1}^{m} k_i(l_i - 1) = n - \sum_{i=1}^{m} k_i,$$

где k_i — число циклов длины l_i в разложении подстановки $h^{-1}g$ в произведение независимых циклов, т. е. цикловая структура подстановки $h^{-1}g$ имеет следующий вид:

$$[h^{-1}g] = \left[l_1^{k_1}, l_2^{k_2}, \ldots, l_m^{k_m}\right].$$

Нетрудно видеть, что $\tau(g, h)$ — это минимальное число транспозиций, переводящих подстановку g в h.

Определение 3. *Расстоянием Хемминга* между подстановками $g, h \in S(G)$ называется число

$$\chi(g, h) = |\{x \in G : g(x) \neq h(x)\}|.$$

Без существенных изменений для случая произвольной группы G справедливо утверждение из работы [6].

Утверждение 1. Если $g, h \in \mathrm{Orth}(G)$, $g \neq h$, то $\tau(g,h) \geqslant 2$.

Доказательство. Заметим, что для любых подстановок $g, h \in S(G)$, $g \neq h$, справедливо $\tau(g,h) \geqslant 1$. Пусть $\tau(g,h) = 1$. Тогда существуют такие $x_1, x_2 \in G$, что $x_1 \neq x_2$ и $h = (x_1, x_2)g$. Ортоморфизм h может быть записан в виде таблицы:

$$h = \begin{pmatrix} \dots & x_1 & \dots & x_2 & \dots \\ \dots & g(x_2) & \dots & g(x_1) & \dots \end{pmatrix}.$$

Так как $g \in \mathrm{Orth}(G)$, для построенной по определению 1 подстановки g' справедливо равенство $g'(x_1) = x_1^{-1} * g(x_1)$. Так как $h \in \mathrm{Orth}(G)$, то имеет место $g'(x_1) = x_1^{-1} * g(x_2)$ либо $g'(x_1) = x_2^{-1} * g(x_1)$. Следовательно,

$$\begin{cases} g'(x_1) = x_1^{-1} * g(x_1), \\ g'(x_1) = x_1^{-1} * g(x_2) \end{cases} \quad \text{либо} \quad \begin{cases} g'(x_1) = x_1^{-1} * g(x_1), \\ g'(x_1) = x_2^{-1} * g(x_1). \end{cases}$$

В первом случае имеем $g(x_1) = g(x_2)$ — противоречие, так как g — подстановка. Во втором случае $x_1 = x_2$ — противоречие условию $x_1 \neq x_2$. ■

Будем говорить, что ортоморфизмы $g, h \in \mathrm{Orth}(G)$, $g \neq h$, находятся на минимально возможном расстоянии друг от друга, если $\tau(g,h) = 2$.

Нетрудно видеть, что ортоморфизмы $g, h \in \mathrm{Orth}(G)$, находящиеся на расстоянии Кэли $\tau(g,h) = 2$, имеют расстояние Хемминга $\chi(g,h) = 3$ или $\chi(g,h) = 4$.

Пусть $I_i(g) = \{h \in \mathrm{Orth}(G) : \tau(g,h) = 2,\ \chi(g,h) = i+2\}$, $i = 1, 2$. Через $I(g)$ будем обозначать множество ортоморфизмов, находящихся на минимально возможном расстоянии Кэли от g, то есть

$$I(g) = \{h \in \mathrm{Orth}(G) : \tau(g,h) = 2\} = I_1(g) \cup I_2(g).$$

Изучение стойкости блочных шифрсистем с неабелевой группой наложения ключа относительно разностного метода криптоанализа может потребовать рассмотрения двух различных разностных характеристик перемешивающих отображений.

Определение 4. *Разностными характеристиками* $p_g^{(1)}$ и $p_g^{(2)}$ подстановки $g \in S(G)$ называются величины:

$$p_g^{(i)} = \max_{\alpha,\beta \in G^\times} {p_{\alpha,\beta}^g}^{(i)},\ i = 1, 2,$$

где

$${p_{\alpha,\beta}^g}^{(1)} = |G|^{-1} \cdot |\{x \in G : g(x)^{-1} * g(x * \alpha) = \beta\}|,$$
$${p_{\alpha,\beta}^g}^{(2)} = |G|^{-1} \cdot |\{x \in G : g(\alpha * x) * g(x)^{-1} = \beta\}|.$$

Замечание 1. Нетрудно видеть, что справедливы неравенства

$$p_g^{(1)} \leqslant 1,\ p_g^{(2)} \leqslant 1.$$

Верхняя оценка достижима, например, для тождественной подстановки.

Определение 5. *Обобщённой группой кватернионов* Q_{4n} с бинарной операцией $*$ и нейтральным элементом e называется неабелева конечная группа порядка $4n$, порождённая двумя элементами x и y:

$$\langle x, y \mid x^{2n} = y^4 = 1,\ x^n = y^2,\ y^{-1} * x * y = x^{-1} \rangle.$$

Из определения следует, что элементы Q_{4n} можно записать в виде

$$x^k y^j,\ 0 \leqslant k \leqslant 2n-1,\ j \in \{0,1\}.$$

Элементам Q_{4n} сопоставим элементы из $\mathbb{Z}_{4n}$ с помощью функции $\varphi : Q_{4n} \to \mathbb{Z}_{4n}$:

$$\varphi(x^k y^j) = 2n\, j + k.$$

Всюду далее элементы $z \in Q_{4n}$ обобщённой группы кватернионов будем записывать в виде их образа $\varphi(z) \in \mathbb{Z}_{4n}$.

2. Построение ортоморфизмов, находящихся на минимально возможном расстоянии от данного ортоморфизма

Приведём алгоритмы построения множеств $I_1(g)$ и $I_2(g)$ для произвольного ортоморфизма g, имеющие меньшую трудоёмкость по сравнению с наивным алгоритмом, основанным на переборе всех A_n^4 размещений.

2.1. Ортоморфизмы на расстоянии Хемминга, равном 3

Алгоритм 1 строит множества $I_1(g)$ для произвольного ортоморфизма g. Полагаем, что G — конечная группа порядка n, $n \geqslant 4$.

Алгоритм 1.

Вход: Ортоморфизм $g \in \mathrm{Orth}(G)$.
Выход: Список $I_1(g)$.

1: $i := 0$, $I_1(g) := \varnothing$.
2: **Если** $i = \mathrm{A}_{n-1}^2$, **то**
   закончить работу, на выход подать элементы списка I_1.
3: **Если** $i < \mathrm{A}_{n-1}^2$, **то**
4: выбрать новую упорядоченную пару $(x_1, x_2) \in G^2$ со свойством $\max\{x_1, x_2\} \neq z_{n-1}$;
5: $i := i + 1$;
6: перейти на шаг 7.
7: $x_3 := g(x_2) * g(x_1)^{-1} * x_1$.
8: **Если** $x_3 > \max\{x_1, x_2\}$, **то**
   перейти на шаг 9, **иначе** перейти на шаг 2.
9: $i := i + 1$.
10: **Если** $g(x_1)^{-1} * x_2 * x_1^{-1} * g(x_3) = e$ и $g(x_3)^{-1} * x_1 * x_2^{-1} * g(x_2) = e$, **то**
11: $h := (x_3, x_2)(x_2, x_1)g$; добавить h в список $I_1(g)$.
12: Перейти на шаг 2.

Пример 1. Рассмотрим ортоморфизм $g \in Q_{16}$, заданный табл. 1.

Таблица 1

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$g(x)$	0	2	1	5	8	a	9	d	3	c	6	f	e	7	b	4
$g'(x)$	0	1	7	2	c	d	b	e	9	5	8	4	6	a	3	f

Результатом применения алгоритма 1 к ортоморфизму $g \in \mathrm{Orth}(Q_{16})$ является множество $I_1(g)$, состоящее из четырёх ортоморфизмов (табл. 2).

Таблица 2

Ортоморфизм																Транспозиции
1	0	2	5	8	a	9	d	3	c	6	f	e	7	b	4	(0,1)(1,2)
4	2	1	5	8	a	9	d	3	c	6	0	e	7	b	f	(0,b)(b,f)
0	2	1	5	9	8	a	d	3	c	6	f	e	7	b	4	(4,5)(5,6)
0	2	1	5	8	e	9	d	a	c	6	f	3	7	b	4	(5,8)(8,c)

Следующее утверждение описывает свойства ортоморфизмов множества $I_1(g)$ и показывает корректность работы алгоритма 1.

Утверждение 2. Пусть $g \in \mathrm{Orth}(G)$, $h \in S(G)$ и существуют такие попарно различные элементы $x_1, x_2, x_3 \in G$, что $h = (x_3, x_2)(x_2, x_1)g$. Тогда следующие условия эквивалентны:

1) $h \in \mathrm{Orth}(G)$;
2) имеют место равенства

$$\begin{cases} g(x_1)^{-1} * x_2 * g'(x_3) = e, \\ g(x_2)^{-1} * x_3 * g'(x_1) = e, \\ g(x_3)^{-1} * x_1 * g'(x_2) = e. \end{cases} \tag{1}$$

Доказательство. Пусть h — ортоморфизм. Покажем, что выполнены равенства (1). Заметим, что для элементов $h'(x_1)$, $h'(x_2)$, $h'(x_3)$ справедливы следующие соотношения:

$$\begin{array}{lll} h'(x_1) \neq g'(x_1), & h'(x_2) \neq g'(x_2), & h'(x_3) \neq g'(x_3), \\ h'(x_1) \neq g'(x_3), & h'(x_2) \neq g'(x_1), & h'(x_3) \neq g'(x_2). \end{array}$$

Следовательно, $h'(x_1) = g'(x_2)$, $h'(x_2) = g'(x_3)$, $h'(x_3) = g'(x_1)$ и

$$\begin{array}{lll} h'(x_1) = x_1^{-1} * g(x_3), & h'(x_2) = x_2^{-1} * g(x_1), & h'(x_3) = x_3^{-1} * g(x_2), \\ h'(x_1) = x_2^{-1} * g(x_2), & h'(x_2) = x_3^{-1} * g(x_3), & h'(x_3) = x_1^{-1} * g(x_1). \end{array}$$

Справедливы равенства

$$\begin{aligned} e = h'(x_1)^{-1} * h'(x_1) = g(x_3)^{-1} * x_1 * g'(x_2), \\ e = h'(x_2)^{-1} * h'(x_2) = g(x_1)^{-1} * x_2 * g'(x_3), \\ e = h'(x_3)^{-1} * h'(x_3) = g(x_2)^{-1} * x_3 * g'(x_1). \end{aligned}$$

Обратно, пусть выполнены равенства (1). Тогда

$$\begin{aligned} h'(x_1) = x_1^{-1} * g(x_3) = g'(x_2), \\ h'(x_2) = x_2^{-1} * g(x_1) = g'(x_3), \\ h'(x_3) = x_3^{-1} * g(x_2) = g'(x_1). \end{aligned}$$

Следовательно, h — ортоморфизм. ■

Обозначим через t_1 трудоёмкость алгоритма 1.

Утверждение 3. При $n \to \infty$ для величины t_1 справедлива оценка $t_1 = O(n^2)$.

Доказательство. Трудоёмкость алгоритма 1 оценивается произведением числа A^2_{n-1} повторений шага 2 и фиксированного числа элементарных операций на шагах 7 и 9 алгоритма. ■

Замечание 2. Трудоёмкость алгоритма 1, по крайней мере, в n раз меньше трудоёмкости алгоритма, основанного на переборе всех A^3_n размещений элементов $x_1, x_2, x_3 \in G$, вычислении подстановки h и проверке свойства $h \in \mathrm{Orth}(G)$.

Из утверждения 3 следуют оценки числа ортоморфизмов в списке $I_1(g)$ на выходе алгоритма 1.

Следствие 1. Для любого $g \in \mathrm{Orth}(G)$ справедливы неравенства

$$0 \leqslant |I_1(g)| \leqslant \mathrm{A}^2_{n-1}.$$

Табл. 3 иллюстрирует достижимость нижних и верхних оценок числа $|I_1(g)|$ для обобщённой группы кватернионов Q_{4n}, $n = 2, 4, 8, 16, 32, 64$.

Таблица 3

Группа G	Нижняя оценка $\lvert I_1(g)\rvert$	Наименьшее найденное значение $\lvert I_1(g)\rvert$	Наибольшее найденное значение $\lvert I_1(g)\rvert$	Верхняя оценка $\lvert I_1(g)\rvert$
Q_8	0	0	0	42
Q_{16}	0	0	9	210
Q_{32}	0	0	7	930
Q_{64}	0	0	15	3906
Q_{128}	0	0	29	16002
Q_{256}	0	0	43	64770

2.2. Ортоморфизмы на расстоянии Хемминга, равном 4

Алгоритм 2 строит множество $I_2(g)$ для произвольного ортоморфизма g. Как и ранее, полагаем, что G — конечная группа порядка n, $n \geqslant 4$.

Пример 2. Рассмотрим ортоморфизм $g \in Q_8$, заданный табл. 4.

Таблица 4

x	0	1	2	3	4	5	6	7
$g(x)$	0	2	4	6	1	3	7	5
$g'(x)$	0	1	6	7	5	4	3	2

Результатом применения алгоритма 2 к ортоморфизму $g \in \mathrm{Orth}(Q_8)$ является множество $I_2(g)$, состоящее из восьми ортоморфизмов (табл. 5).

Таблица 5

Ортоморфизм								Транспозиции
2	0	4	6	1	3	5	7	$(0,1)(6,7)$
4	2	0	6	1	5	7	3	$(0,2)(5,7)$
6	4	2	0	1	3	7	5	$(0,3)(1,2)$
3	2	4	7	1	0	6	5	$(0,5)(3,6)$
7	2	4	3	1	6	0	5	$(0,6)(3,5)$
0	6	4	2	7	3	1	5	$(1,3)(4,6)$
0	2	6	4	3	1	7	5	$(2,3)(4,5)$
0	2	4	6	5	7	3	1	$(4,7)(5,6)$

Нетрудно видеть, что полученные ортоморфизмы задают латинские квадраты, ортогональные к таблице Кэли группы Q_8, например:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 3 & 0 & 5 & 6 & 7 & 4 \\ 2 & 3 & 0 & 1 & 6 & 7 & 4 & 5 \\ 3 & 0 & 1 & 2 & 7 & 4 & 5 & 6 \\ 4 & 7 & 6 & 5 & 2 & 1 & 0 & 3 \\ 5 & 4 & 7 & 6 & 3 & 2 & 1 & 0 \\ 6 & 5 & 4 & 7 & 0 & 3 & 2 & 1 \\ 7 & 6 & 5 & 4 & 1 & 0 & 3 & 2 \end{pmatrix}, \quad \begin{pmatrix} 4 & 2 & 0 & 6 & 1 & 5 & 7 & 3 \\ 7 & 3 & 1 & 5 & 2 & 4 & 6 & 0 \\ 6 & 0 & 2 & 4 & 3 & 7 & 5 & 1 \\ 5 & 1 & 3 & 7 & 0 & 6 & 4 & 2 \\ 2 & 6 & 4 & 0 & 5 & 3 & 1 & 7 \\ 1 & 7 & 5 & 3 & 6 & 2 & 0 & 4 \\ 0 & 4 & 6 & 2 & 7 & 1 & 3 & 5 \\ 3 & 5 & 7 & 1 & 4 & 0 & 2 & 6 \end{pmatrix}.$$

Алгоритм 2.

Вход: Ортоморфизм $g \in \mathrm{Orth}(G)$.
Выход: Список $I_2(g)$.

1: $i := 0$, $I_2(g) := \varnothing$.
2: **Если** $i = \mathrm{C}_n^3 - 1$, **то**
закончить работу, на выход подать элементы списка I_2.
3: **Если** $i < \mathrm{C}_n^3 - 1$, **то**
4: выбрать новое сочетание $(x_1, x_3, x_4) \in G^3$, удовлетворяющее условиям $x_1 < x_3 < x_4$, $x_1 \neq z_{n-3}$;
5: $i := i + 1$;
6: перейти на шаг 7.
7: $x_2 := g(x_1) * g(x_4)^{-1} * x_4$; $\widetilde{x}_2 := g(x_1) * g(x_3)^{-1} * x_3$.
8: **Если** $x_1 < x_2$ или $x_1 < \widetilde{x}_2$, **то**
перейти на шаг 9, **иначе** перейти на шаг 2.
9: Проверить справедливость систем равенств (2) и (3):

$$\begin{cases} \left[\begin{cases} g(x_4)^{-1} * x_3 * x_1^{-1} * g(x_1) = e, \\ g(x_3)^{-1} * x_4 * x_2^{-1} * g(x_2) = e, \end{cases} \right. \\ \left. \left[\begin{cases} g(x_4)^{-1} * x_3 * x_2^{-1} * g(x_2) = e, \\ g(x_3)^{-1} * x_4 * x_1^{-1} * g(x_1) = e, \end{cases} \right. \\ g(x_2)^{-1} * x_1 * x_3^{-1} * g(x_3) = e; \end{cases} \tag{2}$$

$$\begin{cases} \left[\begin{cases} g(x_4)^{-1} * x_3 * x_1^{-1} * g(x_1) = e, \\ g(x_3)^{-1} * x_4 * \widetilde{x}_2^{-1} * g(\widetilde{x}_2) = e, \end{cases} \right. \\ \left. \left[\begin{cases} g(x_4)^{-1} * x_3 * \widetilde{x}_2^{-1} * g(\widetilde{x}_2) = e, \\ g(x_3)^{-1} * x_4 * x_1^{-1} * g(x_1) = e, \end{cases} \right. \\ g(x_1)^{-1} * \widetilde{x}_2 * x_3^{-1} * g(x_3) = e. \end{cases} \tag{3}$$

10: **Если** выполнена система (2), **то**
11: для элемента x_2 вычислить $h = (x_4, x_3)(x_2, x_1)g$, добавить h в список $I_2(g)$.
12: **Если** выполнена система (3), **то**
13: для элемента $\widetilde{x}_2$ вычислить $\widetilde{h} = (x_4, x_3)(\widetilde{x}_2, x_1)g$, добавить $\widetilde{h}$ в список $I_2(g)$.
14: Перейти на шаг 2.

Следующее утверждение описывает свойства ортоморфизмов множества $I_2(g)$ и показывает корректность работы алгоритма 2.

Утверждение 4. Пусть $g \in \mathrm{Orth}(G), h \in S(G)$, существуют такие попарно различные элементы $x_1, x_2, x_3, x_4 \in G$, что $h = (x_4, x_3)(x_2, x_1)g$. Тогда следующие условия эквивалентны:

1) $h \in \mathrm{Orth}(G)$;
2) справедлива одна из систем равенств (4) или (5):

$$\begin{cases} \left[\begin{cases} g(x_4)^{-1} * x_3 * g'(x_1) = e, \\ g(x_3)^{-1} * x_4 * g'(x_2) = e, \end{cases} \\ \left[\begin{cases} g(x_4)^{-1} * x_3 * g'(x_2) = e, \\ g(x_3)^{-1} * x_4 * g'(x_1) = e, \end{cases} \\ g(x_1)^{-1} * x_2 * g'(x_4) = e, \\ g(x_2)^{-1} * x_1 * g'(x_3) = e; \end{cases} \tag{4}$$

$$\begin{cases} \left[\begin{cases} g(x_4)^{-1} * x_3 * g'(x_1) = e, \\ g(x_3)^{-1} * x_4 * g'(x_2) = e, \end{cases} \\ \left[\begin{cases} g(x_4)^{-1} * x_3 * g'(x_2) = e, \\ g(x_3)^{-1} * x_4 * g'(x_1) = e, \end{cases} \\ g(x_1)^{-1} * x_2 * g'(x_3) = e, \\ g(x_1)^{-1} * x_2 * g'(x_3) = e. \end{cases} \tag{5}$$

Доказательство. Пусть h — ортоморфизм. Покажем, что выполнено условие 2. Элементы $h'(x_1)$, $h'(x_2)$, $h'(x_3)$, $h'(x_4)$ удовлетворяют следующим условиям:

$$\begin{array}{llll} h'(x_1) \neq g'(x_1), & h'(x_2) \neq g'(x_2), & h'(x_3) \neq g'(x_3), & h'(x_4) \neq g'(x_3), \\ h'(x_1) \neq g'(x_2), & h'(x_2) \neq g'(x_3), & h'(x_3) \neq g'(x_4), & h'(x_4) \neq g'(x_4). \end{array}$$

Следовательно,

$$\big(h'(x_1), h'(x_2), h'(x_3), h'(x_4)\big) \in \{\big(g'(x_3), g'(x_4), g'(x_1), g'(x_2)\big), \big(g'(x_3), g'(x_4), g'(x_2), g'(x_1)\big), \\ \big(g'(x_4), g'(x_3), g'(x_1), g'(x_2)\big), \big(g'(x_4), g'(x_3), g'(x_2), g'(x_1)\big)\}.$$

Если $\big(h'(x_1), h'(x_2), h'(x_3), h'(x_4)\big) = \big(g'(x_3), g'(x_4), g'(x_1), g'(x_2)\big)$, то

$$\begin{array}{ll} \begin{cases} h'(x_1) = x_1^{-1} * g(x_2), \\ h'(x_1) = x_3^{-1} * g(x_3); \end{cases} & \begin{cases} h'(x_2) = x_2^{-1} * g(x_1), \\ h'(x_2) = x_4^{-1} * g(x_4); \end{cases} \\ \begin{cases} h'(x_3) = x_3^{-1} * g(x_4), \\ h'(x_3) = x_1^{-1} * g(x_1); \end{cases} & \begin{cases} h'(x_4) = x_4^{-1} * g(x_3), \\ h'(x_3) = x_2^{-1} * g(x_2), \end{cases} \end{array}$$

поэтому

$$\begin{aligned} e &= h'(x_1)^{-1} * h'(x_1) = g(x_2)^{-1} * x_1 * x_3^{-1} * g(x_3) = g(x_2)^{-1} * x_1 * g'(x_3), \\ e &= h'(x_2)^{-1} * h'(x_2) = g(x_1)^{-1} * x_2 * x_4^{-1} * g(x_4) = g(x_1)^{-1} * x_2 * g'(x_4), \\ e &= h'(x_3)^{-1} * h'(x_3) = g(x_4)^{-1} * x_3 * x_1^{-1} * g(x_1) = g(x_4)^{-1} * x_3 * g'(x_1), \\ e &= h'(x_4)^{-1} * h'(x_4) = g(x_3)^{-1} * x_4 * x_2^{-1} * g(x_2) = g(x_3)^{-1} * x_4 * g'(x_2). \end{aligned}$$

Аналогично рассматриваются оставшиеся три случая.

Обратно, пусть выполнены следующие равенства из п. 2:

$$g(x_2)^{-1} * x_1 * g'(x_3) = e,$$
$$g(x_1)^{-1} * x_2 * g'(x_4) = e,$$
$$g(x_4)^{-1} * x_3 * g'(x_1) = e,$$
$$g(x_3)^{-1} * x_4 * g'(x_2) = e.$$

Покажем, что $h \in \mathrm{Orth}(G)$.

Так как $h = (x_4, x_3)(x_2, x_1)g$, то элементы $h'(x_i)$, $i = 1, 2, 3, 4$, имеют вид

$$h'(x_1) = x_1^{-1} * g(x_2), \qquad h'(x_2) = x_2^{-1} * g(x_1),$$
$$h'(x_3) = x_3^{-1} * g(x_4), \qquad h'(x_4) = x_4^{-1} * g(x_3).$$

Из равенства $g(x_2)^{-1} * x_1 * g'(x_3) = e$ следует, что $g'(x_3) = x_1^{-1} * g(x_2) = h'(x_1)$.
Из равенства $g(x_1)^{-1} * x_2 * g'(x_4) = e$ следует, что $g'(x_4) = x_2^{-1} * g(x_1) = h'(x_2)$.
Из равенства $g(x_4)^{-1} * x_3 * g'(x_1) = e$ следует, что $g'(x_1) = x_3^{-1} * g(x_4) = h'(x_1)$.
Из равенства $g(x_3)^{-1} * x_4 * g'(x_2) = e$ следует, что $g'(x_2) = x_4^{-1} * g(x_3) = h'(x_4)$.
Следовательно, h — ортоморфизм.

Случаи выполнения других наборов равенств п. 2 утверждения 4 проверяются аналогично. ■

Обозначим через t_2 трудоёмкость алгоритма 2.

Утверждение 5. При $n \to \infty$ для величины t_2 справедлива оценка $t_2 = O(n^3)$.

Доказательство. Трудоёмкость алгоритма 2 оценивается произведением числа $(\mathrm{C}_n^3 - 1)$ повторений шага 2 и фиксированного числа элементарных операций на шагах 7 и 9 алгоритма. ■

Замечание 3. Трудоёмкость алгоритма 2, по крайней мере, в n раз меньше трудоёмкости алгоритма, основанного на переборе всех A_n^4 размещений элементов $x_1, x_2, x_3, x_4 \in G$, вычислении подстановки h и проверке свойства $h \in \mathrm{Orth}(G)$.

Из утверждения 5 следуют оценки числа ортоморфизмов в списке $I_2(g)$ на выходе алгоритма 2.

Следствие 2. Для любого $g \in \mathrm{Orth}(G)$ справедливы неравенства

$$0 \leqslant |I_2(g)| \leqslant \mathrm{C}_n^3 - 1.$$

В табл. 6 приведены данные о достижимости нижних и верхних оценок числа $|I_2(g)|$ для обобщённой группы кватернионов Q_{4n}, $n = 2, 4, 8, 16, 32, 64$.

Таблица 6

Группа G	Нижняя оценка $\lvert I_2(g)\rvert$	Наименьшее найденное значение $\lvert I_2(g)\rvert$	Наибольшее найденное значение $\lvert I_2(g)\rvert$	Верхняя оценка $\lvert I_2(g)\rvert$
Q_8	0	8	8	55
Q_{16}	0	2	31	559
Q_{32}	0	10	46	4959
Q_{64}	0	32	83	41663
Q_{128}	0	42	103	341375
Q_{256}	0	78	170	2763519

3. Экспериментальные результаты

Ортоморфизмы, описанные в [9, 18], обладают близкими к 1 значениями разностных характеристик. Примеры таких ортоморфизмов содержатся в табл. 7–11.

Алгоритмы 1 и 2 настоящей работы были использованы в составе спектрально-разностного метода [20, 21] для построения ортоморфизмов $g \in Q_{2^n}$ обобщённой группы кватернионов с близкими к оптимальным значениями разностных характеристик $p_g^{(1)}$ и $p_g^{(2)}$. В табл. 12–16 приведены примеры ортоморфизмов обобщённой группы кватернионов $g \in \mathrm{Orth}(Q_{4n})$, где $4n = 2^t$ $(t = 4, 5, 6, 7, 8)$, с близкими к оптимальным значениями разностных характеристик. Такие подстановки являются перспективными для использования в качестве нелинейных перемешивающих преобразований в блочных шифрсистемах с операцией наложения ключа из группы Q_{4n}, где $4n = 2^t$, $t \geqslant 3$.

Таблица 7

$g \in \mathrm{Orth}(Q_{16})$																$p_g^{(1)}$	$p_g^{(2)}$
0	2	4	6	8	a	c	e	1	3	5	7	d	f	9	b	12/16	12/16
0	2	4	6	c	e	8	a	9	b	d	f	1	3	5	7	12/16	12/16

Таблица 8

$g \in \mathrm{Orth}(Q_{32})$																$p_g^{(1)}$	$p_g^{(2)}$
0	2	4	6	8	a	c	e	10	12	14	16	18	1a	1c	1e	28/32	24/32
1	3	5	7	9	b	d	f	19	1b	1d	1f	11	13	15	17		
0	2	4	6	8	a	c	e	18	1a	1c	1e	10	12	14	16	28/32	24/32
11	13	15	17	19	1b	1d	1f	1	3	5	7	9	b	d	f		

Таблица 9

$g \in \mathrm{Orth}(Q_{64})$																$p_g^{(1)}$	$p_g^{(2)}$
0	2	4	6	8	a	c	e	10	12	14	16	18	1a	1c	1e	60/64	48/64
20	22	24	26	28	2a	2c	2e	30	32	34	36	38	3a	3c	3e		
1	3	5	7	9	b	d	f	11	13	15	17	19	1b	1d	1f		
31	33	35	37	39	3b	3d	3f	21	23	25	27	29	2b	2d	2f		
0	2	4	6	8	a	c	e	10	12	14	16	18	1a	1c	1e	60/64	48/64
30	32	34	36	38	3a	3c	3e	20	22	24	26	28	2a	2c	2e		
21	23	25	27	29	2b	2d	2f	31	33	35	37	39	3b	3d	3f		
1	3	5	7	9	b	d	f	11	13	15	17	19	1b	1d	1f		

Таблица 10

$g \in \mathrm{Orth}(Q_{128})$																$p_g^{(1)}$	$p_g^{(2)}$
0	2	4	6	8	a	c	e	10	12	14	16	18	1a	1c	1e		
20	22	24	26	28	2a	2c	2e	30	32	34	36	38	3a	3c	3e		
40	42	44	46	48	4a	4c	4e	50	52	54	56	58	5a	5c	5e		
60	62	64	66	68	6a	6c	6e	70	72	74	76	78	7a	7c	7e	$\frac{124}{128}$	$\frac{96}{128}$
1	3	5	7	9	b	d	f	11	13	15	17	19	1b	1d	1f		
21	23	25	27	29	2b	2d	2f	31	33	35	37	39	3b	3d	3f		
61	63	65	67	69	6b	6d	6f	71	73	75	77	79	7b	7d	7f		
41	43	45	47	49	4b	4d	4f	51	53	55	57	59	5b	5d	5f		
0	2	4	6	8	a	c	e	10	12	14	16	18	1a	1c	1e		
20	22	24	26	28	2a	2c	2e	30	32	34	36	38	3a	3c	3e		
60	62	64	66	68	6a	6c	6e	70	72	74	76	78	7a	7c	7e		
40	42	44	46	48	4a	4c	4e	50	52	54	56	58	5a	5c	5e	$\frac{124}{128}$	$\frac{96}{128}$
41	43	45	47	49	4b	4d	4f	51	53	55	57	59	5b	5d	5f		
61	63	65	67	69	6b	6d	6f	71	73	75	77	79	7b	7d	7f		
1	3	5	7	9	b	d	f	11	13	15	17	19	1b	1d	1f		
21	23	25	27	29	2b	2d	2f	31	33	35	37	39	3b	3d	3f		

Таблица 11

$g \in \mathrm{Orth}(Q_{256})$																$p_g^{(1)}$	$p_g^{(2)}$
0	2	4	6	8	a	c	e	10	12	14	16	18	1a	1c	1e		
20	22	24	26	28	2a	2c	2e	30	32	34	36	38	3a	3c	3e		
40	42	44	46	48	4a	4c	4e	50	52	54	56	58	5a	5c	5e		
60	62	64	66	68	6a	6c	6e	70	72	74	76	78	7a	7c	7e		
80	82	84	86	88	8a	8c	8e	90	92	94	96	98	9a	9c	9e		
a0	a2	a4	a6	a8	aa	ac	ae	b0	b2	b4	b6	b8	ba	bc	be		
c0	c2	c4	c6	c8	ca	cc	ce	d0	d2	d4	d6	d8	da	dc	de		
e0	e2	e4	e6	e8	ea	ec	ee	f0	f2	f4	f6	f8	fa	fc	fe	$\frac{252}{256}$	$\frac{192}{256}$
1	3	5	7	9	b	d	f	11	13	15	17	19	1b	1d	1f		
21	23	25	27	29	2b	2d	2f	31	33	35	37	39	3b	3d	3f		
41	43	45	47	49	4b	4d	4f	51	53	55	57	59	5b	5d	5f		
61	63	65	67	69	6b	6d	6f	71	73	75	77	79	7b	7d	7f		
c1	c3	c5	c7	c9	cb	cd	cf	d1	d3	d5	d7	d9	db	dd	df		
e1	e3	e5	e7	e9	eb	ed	ef	f1	f3	f5	f7	f9	fb	fd	ff		
81	83	85	87	89	8b	8d	8f	91	93	95	97	99	9b	9d	9f		
a1	a3	a5	a7	a9	ab	ad	af	b1	b3	b5	b7	b9	bb	bd	bf		
0	2	4	6	8	a	c	e	10	12	14	16	18	1a	1c	1e		
20	22	24	26	28	2a	2c	2e	30	32	34	36	38	3a	3c	3e		
40	42	44	46	48	4a	4c	4e	50	52	54	56	58	5a	5c	5e		
60	62	64	66	68	6a	6c	6e	70	72	74	76	78	7a	7c	7e		
c0	c2	c4	c6	c8	ca	cc	ce	d0	d2	d4	d6	d8	da	dc	de		
e0	e2	e4	e6	e8	ea	ec	ee	f0	f2	f4	f6	f8	fa	fc	fe		
80	82	84	86	88	8a	8c	8e	90	92	94	96	98	9a	9c	9e		
a0	a2	a4	a6	a8	aa	ac	ae	b0	b2	b4	b6	b8	ba	bc	be	$\frac{252}{256}$	$\frac{192}{256}$
81	83	85	87	89	8b	8d	8f	91	93	95	97	99	9b	9d	9f		
a1	a3	a5	a7	a9	ab	ad	af	b1	b3	b5	b7	b9	bb	bd	bf		
c1	c3	c5	c7	c9	cb	cd	cf	d1	d3	d5	d7	d9	db	dd	df		
e1	e3	e5	e7	e9	eb	ed	ef	f1	f3	f5	f7	f9	fb	fd	ff		
1	3	5	7	9	b	d	f	11	13	15	17	19	1b	1d	1f		
21	23	25	27	29	2b	2d	2f	31	33	35	37	39	3b	3d	3f		
41	43	45	47	49	4b	4d	4f	51	53	55	57	59	5b	5d	5f		
61	63	65	67	69	6b	6d	6f	71	73	75	77	79	7b	7d	7f		

Таблица 12

$g \in \mathrm{Orth}(Q_{16})$																$p_g^{(1)}$	$p_g^{(2)}$
c	f	3	6	e	a	0	4	1	9	5	7	d	2	8	b	3/16	3/16
c	0	8	6	4	e	b	5	1	3	7	a	f	9	2	d	3/16	3/16

Таблица 13

$g \in \mathrm{Orth}(Q_{32})$																$p_g^{(1)}$	$p_g^{(2)}$
10	b	a	5	1c	c	8	16	18	14	1a	4	15	13	d	1	4/32	4/32
3	2	0	e	9	12	1e	1f	17	f	1d	1b	11	7	19	6		
f	2	18	1c	1f	13	4	17	10	1	0	6	c	a	1b	16	4/32	4/32
1e	15	5	7	1d	b	d	3	14	e	11	9	12	1a	19	8		

Таблица 14

$g \in \mathrm{Orth}(Q_{64})$																$p_g^{(1)}$	$p_g^{(2)}$
20	2c	28	24	e	2	3a	5	35	38	21	16	17	31	a	14	4/64	5/64
11	23	2e	26	1c	32	6	2a	18	4	1	c	0	29	7	30		
34	3	1d	2f	2b	37	d	1f	22	12	15	3c	19	1b	3e	f		
39	8	33	3d	1a	3b	b	3f	9	13	25	27	36	1e	10	2d		
32	3f	28	24	e	2	23	5	2c	38	21	27	17	12	1c	1a	4/64	5/64
11	31	35	26	a	20	6	2a	18	4	1	c	0	29	7	30		
34	3	2e	2f	2b	3d	d	1f	22	3a	15	14	8	1b	3e	f		
39	b	33	37	3c	3b	19	1d	9	10	25	16	36	1e	13	2d		

Таблица 15

$g \in \mathrm{Orth}(Q_{128})$																$p_g^{(1)}$	$p_g^{(2)}$
7a	46	33	5e	56	42	c	20	10	71	44	52	15	79	1c	55		
4c	a	24	36	63	6a	41	6	30	39	7d	48	5f	73	3c	3e		
7c	2d	32	21	f	4a	54	2e	12	65	75	1f	18	40	5c	3		
60	49	25	5d	68	2f	6e	34	6b	47	2c	22	37	35	14	1a	$\frac{5}{128}$	$\frac{6}{128}$
31	7	4	4e	0	7b	d	8	11	74	66	4b	23	29	77	7e		
62	4d	6c	16	27	b	57	26	3f	13	19	72	61	3b	3d	1		
2a	2	5b	67	59	6f	3a	70	28	64	6d	51	5	2b	17	7f		
9	45	1d	43	1e	58	1b	4f	53	76	78	5a	69	50	e	38		
a	46	32	5e	56	72	9	20	6d	7a	6e	73	15	79	1c	5a		
68	39	4f	36	35	6a	3d	6	30	31	3c	2d	45	5d	4c	3e		
71	7d	65	62	f	48	6c	2e	12	54	74	7e	18	41	c	76		
60	49	25	66	44	2f	34	e	6b	22	2c	16	37	2	14	7	$\frac{5}{128}$	$\frac{6}{128}$
52	1f	2a	4e	0	7b	8	26	47	33	75	4b	23	29	51	11		
21	4d	43	d	27	b	70	1a	3f	13	19	4a	40	3b	1e	1		
4	5b	2b	67	59	6f	3a	5f	28	7c	42	77	5	61	17	57		
5c	64	1d	24	50	58	1b	7f	53	3	78	55	69	63	10	38		

Таблица 16

$g \in \mathrm{Orth}(Q_{256})$																$p_g^{(1)}$	$p_g^{(2)}$
3c	7a	49	fe	6d	45	e6	d9	b5	12	14	96	82	a2	d4	80		
41	2	8	e1	38	ca	c0	f8	67	d2	94	36	c	60	0	ef		
e8	8d	8c	25	b8	4a	cc	70	78	39	46	dc	d1	6a	5a	be		
64	f4	f1	90	f0	1	bd	43	1f	a9	13	a8	50	d8	4c	6e		
de	e4	c4	bf	24	2a	d0	93	cd	b1	e3	6	f3	52	61	e0		
6f	d5	99	1d	28	1a	10	a1	30	35	ab	8b	a5	9e	4d	ba		
54	22	68	44	c8	da	af	1e	9	56	47	d6	86	f6	16	2e		
5e	a	7	76	c9	c2	48	4e	84	32	b4	f2	2f	ac	fc	31	$\frac{5}{256}$	$\frac{7}{256}$
9c	eb	3a	26	23	21	5b	6b	a0	72	9f	4b	f5	e2	e	8e		
53	cb	15	c6	f	d7	2d	a4	91	fb	75	58	f9	7b	33	3f		
f7	7e	3	2b	d3	b	bc	b0	51	db	ad	cf	74	34	a6	8f		
8a	63	b3	85	e9	88	c1	9d	3d	73	b6	37	79	3b	7d	a7		
d	fd	fa	c7	65	1c	ec	19	55	b7	5	df	ce	a3	c3	7c		
9a	aa	66	71	b2	5f	b9	3e	42	e7	5c	27	89	dd	6c	77		
81	83	87	97	17	2c	ae	4f	29	ee	95	57	5d	11	98	40		
18	1b	4	7f	69	62	e5	ea	92	ff	c5	20	ed	bb	9b	59		
3c	7a	49	fe	6d	aa	e6	d9	b5	5b	14	96	82	a2	5f	80		
41	2	8	e1	38	ca	c0	f8	67	d2	94	36	c	60	0	ef		
e8	a1	8c	25	b8	4a	cc	70	78	39	6b	dc	92	6a	5a	be		
64	f4	f1	f	f0	1	bd	43	1f	a9	13	a8	50	d8	4c	6e		
de	e4	c4	59	24	2a	2c	93	cd	b1	e3	6	f3	52	61	e0		
6f	d5	99	1d	28	1a	10	8d	30	b6	ab	8b	a5	9e	4d	ba		
54	7d	68	44	c8	da	af	d3	9	56	47	d6	86	f6	16	2e		
5e	a	eb	76	c9	c2	7f	4e	84	32	b4	f2	2f	ac	fc	31	$\frac{5}{256}$	$\frac{7}{256}$
9c	77	3a	26	23	21	45	4b	a0	72	9f	d4	f5	e2	e	8e		
53	cb	15	c6	90	d7	2d	a4	91	fb	75	58	f9	7b	33	3f		
f7	7e	3	2b	65	b	bc	b0	51	db	ad	cf	74	34	a6	8f		
8a	63	57	85	e9	88	c1	9d	46	73	35	37	79	3b	22	a7		
d	fd	fa	c7	b3	1c	ec	19	55	b7	5	df	ce	a3	c3	7c		
9a	7	66	71	b2	3d	b9	3e	42	e7	5c	27	89	dd	4f	1e		
81	83	87	97	e5	d0	ae	6c	29	ee	95	12	5d	11	98	40		
18	1b	4	48	69	62	17	ea	d1	ff	c5	20	ed	bb	9b	bf		

Заключение

В работе изложены алгоритмы построения для произвольного ортоморфизма произвольной группы множеств $I_1(g)$ и $I_2(g)$, содержащих ортоморфизмы, находящиеся на минимально возможном расстоянии от исходного, приведены обоснование и трудоёмкость данных алгоритмов. Кроме этого, с помощью спектрально-разностного метода построены ортоморфизмы обобщённой группы кватернионов порядка 16, 32, 64, 128, 256 с близкими к оптимальным значениями разностных характеристик $p_g^{(1)}$ и $p_g^{(2)}$.

Автор выражает благодарность научному руководителю А. В. Менячихину за постановку задачи и Д. А. Бурову за ценные замечания.

ЛИТЕРАТУРА

1. *Johnson D. M., Dulmage A. L., and Mendelsohn N. S.* Orthomorphisms of groups and orthogonal Latin squares. I // Canad. J. Math. 1961. V. 13. P. 356–372.
2. *Mann H. B.* On orthogonal Latin squares // Bull. Amer. Math. Soc. 1944. V. 50. P. 249–257.
3. *Niederreiter H. and Robinson K.* Bol loops of order pq // Math. Proc. Cambr. Phil. Soc. 1981. V. 89. P. 241–256.
4. *Niederreiter H. and Robinson K.* Complete mappings of finite fields // J. Austral. Math. Soc. Ser. A. 1982. V. 33. No. 2. P. 197–212.

5. *Менячихин А. В.* Метод ограниченного дефицита и задача построения ортоморфизмов и почти ортоморфизмов абелевых групп // Дискретная математика. 2019. Т. 31. № 3. С. 58–77.
6. *Менячихин А. В.* Ортоморфизмы абелевых групп с минимально возможными попарными расстояниями // Дискретная математика. 2018. Т. 30. № 4. С. 55–65.
7. *Сачков В. Н.* Цепи Маркова итерационных систем преобразований // Тр. по дискр. матем. 2002. Т. 6. С. 165–183.
8. *Evans A. B.* Applications of complete mappings and orthomorphisms of finite groups // Quasigroups Relat. Syst. 2015. V. 23. P. 5–30.
9. *Evans A. B.* Orthomorphism Graphs of Groups. Lecture Notes in Math. Berlin: Springer, 1992. V. 1535.
10. *Зубов А. Ю.* Математика кодов аутентификации. М.: Гелиос АРВ, 2007. 480 с.
11. *Черемушкин А. В.* Криптографические протоколы. Основные свойства и уязвимости. М.: Изд. центр «Академия», 2009. 272 с.
12. *Тришин А. Е.* Способ построения ортогональных латинских квадратов на основе подстановочных двучленов конечных полей // Обозр. прикл. и промышл. матем. 2008. Т. 15. № 4. С. 764–765.
13. *Тужилин М. Э.* Латинские квадраты и их применение в криптографии // Прикладная дискретная математика. 2012. № 3(17). С. 47–52.
14. *Denes J. and Keedwell A. D.* Latin Squares and their Applications. Budapest: Academiai Kiado, 2015. 545 p.
15. *Глухов М. М.* О методах построения систем ортогональных квазигрупп с использованием групп // Математические вопросы криптографии. 2011. Т. 2. № 4. С. 5–24.
16. *Глухов М. М.* О применениях квазигрупп в криптографии // Прикладная дискретная математика. 2008. № 2(2). С. 28–32.
17. *Погорелов Б. А., Пудовкина М. А.* Вариации ортоморфизмов и псевдоадамаровых преобразований на неабелевой группе // Прикладная дискретная математика. Приложение. 2019. № 12. С. 24–27.
18. *Погорелов Б. А., Пудовкина М. А.* Классы кусочно-квазиаффинных преобразований на обобщенной 2-группе кватернионов // Дискретная математика. 2022. Т. 34. № 1. С. 103–125.
19. *Погорелов Б. А., Пудовкина М. А.* Классы кусочно-квазиаффинных подстановок на диэдральной, полудиэдральной и модулярной максимально-циклической 2-группах // Дискретная математика. 2022. Т. 34. № 2. С. 50–66.
20. *Menyachikhin A. V.* Spectral-linear and sectral-differntial methods for generating S-boxes having almost optimal cryptographic parameters // Матем. вопр. криптогр. 2017. Т. 8. № 2. С. 97–116.
21. *Menyachikhin A. V.* The change in linear and differential characteristics of substitution after the multiplication by transposition // Матем. вопр. криптогр. 2020. Т. 11. № 2. С. 111–123.

REFERENCES

1. *Johnson D. M., Dulmage A. L., and Mendelsohn N. S.* Orthomorphisms of groups and orthogonal Latin squares. I. Canad. J. Math., 1961, vol. 13, pp. 356–372.
2. *Mann H. B.* On orthogonal Latin squares. Bull. Amer. Math. Soc., 1944, vol. 50, pp. 249–257.
3. *Niederreiter H. and Robinson K.* Bol loops of order *pq*. Math. Proc. Cambr. Phil. Soc., 1981, vol. 89, pp. 241–256.
4. *Niederreiter H. and Robinson K.* Complete mappings of finite fields // J. Austral. Math. Soc., Ser. A, 1982, vol. 33, no. 2, pp. 197–212.

5. *Menyachikhin A. V.* The limited deficit method and the problem of constructing orthomorphisms and almost orthomorphisms of Abelian groups. Discrete Math. Appl., 2021, vol. 31, no. 5, pp. 327–343.
6. *Menyachikhin A. V.* Orthomorphisms of Abelian groups with minimum possible pairwise distances. Discrete Math. Appl., 2020, vol. 30, no. 3, pp. 177–186.
7. *Sachkov V. N.* Tsepi Markova iteratsionnykh sistem preobrazovaniy [Markov chains of iterative transformation systems]. Tr. po Diskr. Matem., 2002, vol. 6, pp. 165–183. (in Russian)
8. *Evans A. B.* Applications of complete mappings and orthomorphisms of finite groups. Quasigroups and Relat. Syst., 2015, vol. 23, pp. 5–30.
9. *Evans A. B.* Orthomorphism Graphs of Groups. Lecture Notes in Math., Berlin, Springer, 1992, vol. 1535.
10. *Zubov A. Yu.* Matematika kodov autentifikatsii [Mathematics of Authentication Codes]. Moscow, Gelios ARV Publ., 2007. 480 p.
11. *Cheremushkin A. V.* Kriptograficheskiye protokoly. Osnovnyye svoystva i uyazvimosti [Cryptographic Protocols. Basic Properties and Vulnerabilities]. Moscow, Akademiya Publ., 2009. 272 p.
12. *Trishin A. E.* Sposob postroyeniya ortogonal'nykh latinskikh kvadratov na osnove podstanovochnykh dvuchlenov konechnykh poley [A method for constructing orthogonal Latin squares based on wildcard binomials of finite fields]. Obozr. Prikl. i Promyshl. Matem., 2008, vol. 15, no. 4, pp. 764–765. (in Russian)
13. *Tuzhilin M. E.* Latinskiye kvadraty i ikh primeneniye v kriptografii [Latin squares and their applications in cryptography]. Prikladnaya Diskretnaya Matematika, 2012, no. 3(17), pp. 47–52. (in Russian)
14. *Denes J. and Keedwell A. D.* Latin Squares and their Applications. Budapest, Academiai Kiado, 2015. 545 p.
15. *Glukhov M. M.* O metodakh postroyeniya sistem ortogonal'nykh kvazigrupp s ispol'zovaniyem grupp [On a method of construction of orthogonal quasigroup systems by means of groups.] Mat. Vopr. Kriptogr., 2011, vol. 2, no. 4, pp. 5–24. (in Russian)
16. *Glukhov M. M.* O primeneniyakh kvazigrupp v kriptografii [Some applications of quasigroups in cryptography]. Prikladnaya Diskretnaya Matematika, 2008, no. 2(2), pp. 28–32. (in Russian)
17. *Pogorelov B. A. and Pudovkina M. A.* Variatsii ortomorfizmov i psevdoadamarovykh preobrazovaniy na neabelevoy gruppe [Variations of orthomorphisms and pseudo-Hadamard transformations on nonabelian groups]. Prikladnaya Diskretnaya Matematika. Prilozhenie, 2019, no. 12, pp. 24–27. (in Russian)
18. *Pogorelov B. A. and Pudovkina M. A.* Classes of piecewise-quasiaffine transformations on the generalized 2-group of quaternions. Discrete Math. Appl., 2023, vol. 33, no. 5, pp. 299–316.
19. *Pogorelov B. A. and Pudovkina M. A.* Classes of piecewise quasiaffine transformations on dihedral, quasidihedral and modular maximal-cyclic 2-groups. Discrete Math. Appl., 2024, vol. 34, no. 1, pp. 15–27.
20. *Menyachikhin A. V.* Spectral-linear and spectral-differntial methods for generating S-boxes having almost optimal cryptographic parameters. Mat. Vopr. Kriptogr., 2017, vol. 8, no. 2, pp. 97–116.
21. *Menyachikhin A. V.* The change in linear and differential characteristics of substitution after the multiplication by transposition. Mat. Vopr. Kriptogr., 2020, vol. 11, no. 2, pp. 111–123.