Дискретная математика

том 30 выпуск 4 * 2018

УДК 512.541.5 DOI https://doi.org/10.4213/dm1539

Ортоморфизмы абелевых групп с минимально возможными попарными расстояниями

© 2018 г. А. В. Менячихин*

Изучаются ортоморфизмы абелевых 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. Предлагаются алгоритмы, позволяющие для данного ортоморфизма получать все ортоморфизмы, находящиеся на минимально возможном от него расстоянии, и оценивается трудоемкость этих алгоритмов. Приведены примеры таких абелевых групп, что множество их ортоморфизмов содержит элементы, расстояния от которых до остальных ортоморфизмов больше минимально возможного.

Ключевые слова: ортоморфизм, абелева группа, латинский квадрат, ортогональные латинские квадраты, метрика Кэли, квазигруппа, s-бокс, нелинейное преобразование, подстановка

1. Введение

Понятие ортоморфизма было впервые введено в [18, 19], детально изучено в [20, 21], получило развитие в [4, 5]. Ортоморфизмы находят широкое применение во многих криптографических конструкциях [14, 15]. Их изучение тесно связано с задачами построения кодов аутентификации [3, 9], систем ортогональных латинских квадратов [7, 8, 12] и квазигрупп [1, 2]. В основе проекта американского стандарта хеш-функции Edon-R [17], участника конкурса SHA-3, лежит использование квазигрупп и двух ортогональных латинских квадратов 8-го порядка. Некоторые атаки на блочные шифрсистемы существенно используют свойство неравномерности распределения суммы входных и выходных значений подстановки [11, 13, 16, 22].

Проблема существования ортоморфизмов конечных абелевых групп была решена в 1947 году [14]. Согласно [23] ортоморфизмы над конечной абелевой группой существуют тогда и только тогда, когда ее силовская 2-подгруппа либо тривиальна, либо не является циклической. Следовательно, ортоморфизмы существуют над любой абелевой группой нечетного порядка. Среди абелевых групп четного порядка,

*Место работы: Лаборатория ТВП, e-mail: and88@list.ru

над которыми существуют ортоморфизмы, можно выделить, например, аддитивную группу поля $\mathbb{F}_{2^t}, t > 1$.

Несмотря на то, что проблема существования ортоморфизмов абелевых групп решена, в группах достаточно большого порядка остается открытым вопрос об эффективном построении ортоморфизмов, обладающих заданными криптографическими качествами. Один из подходов к решению этого вопроса связан с поиском преобразований, оставляющих множество ортоморфизмов инвариантным. Далее рассматриваются ортоморфизмы абелевых групп, находящиеся на минимально возможном расстоянии друг от друга по метрике Кэли (далее расстояние Кэли). Метрика Кэли возникает в связи с задачей определения расстояния между подгруппами симметрической группы [10, 24]. В данной работе метрика возникла в связи с развитием методов синтеза нелинейных перемешивающих отображений [4, 5] и используется для построения с приемлемой трудоемкостью новых ортоморфизмов над абелевыми группами порядка n ($n \leqslant 2^{12}$).

Работа имеет следующую структуру. Второй раздел содержит основные определения и обозначения, необходимые для дальнейшего изложения результатов. Третий раздел содержит ряд утверждений, касающихся свойств ортоморфизмов, находящихся на минимально возможном расстоянии Кэли друг от друга. В нем приводятся также алгоритмы построения всех ортоморфизмов на минимально возможном расстоянии от заданного ортоморфизма и примеры ортоморфизмов, все расстояния от которых до остальных ортоморфизмов больше минимально возможного.

2. Основные определения и обозначения

Далее используются следующие обозначения:

$(G, *)$	–	конечная абелева группа с бинарной операцией $*$ и нейтральным элементом e, $\lvert G\rvert = n$,
$S(G)$	–	симметрическая группа на множестве G,
$\mathbb{F}_m^+$	–	аддитивная группа поля $\mathbb{F}_m$,
$\mathbb{Z}_m^+$	–	аддитивная группа кольца вычетов по модулю m,
$A \times B$	–	декартово произведение множеств A и B,
C_m^k	–	число различных сочетаний из m элементов по k,
A_m^k	–	число различных размещений из m элементов по k.

Определение 1. Подстановка $g \in S(G)$ называется ортоморфизмом группы G, если отображение $g' \colon G \to G$, определяемое условием $g'(x) = x^{-1} * g(x)$, $\forall x \in G$, 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:

$$G = \left\{ \underbrace{z_0}_{e}, z_1, ..., z_{n-1} \right\}, \ |G| = n, \ z_i < z_{i+1}, \ i = 0, ..., n-2.$$

Определение 2. Расстоянием Кэли для подстановок $g, h \in S(G)$ называется число

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

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 вид

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

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

Определение 3. Расстоянием Хемминга для подстановок $g, h \in S(G)$ называется число

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

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

Пусть G — конечная абелева группа, $|G| \geqslant 3$.

Утверждение 1. *Если* $g, h \in \operatorname{Orth}(G)$, $g \neq h$, *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:

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

Так как $g \in \operatorname{Orth}(G)$, то для построенной по определению 1 подстановки g' справедливо равенство

$$g'(x_1) = x_1^{-1} * g(x_1).$$

Так как $h \in \operatorname{Orth}(G)$, то справедливо одно из равенств

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

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

В первом случае имеем $g(x_1) = g(x_2)$ — противоречие, так как g — подстановка.

Во втором случае, $x_1 = x_2$ — противоречии условию $x_1 \neq x_2$, что элементы $x_1, x_2 \in G$ — различны.

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

Замечание 1. 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, т.е.

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

3.1. Ортоморфизмы на расстоянии Хемминга, равном 3. В этом подразделе излагается алгоритм построения множества $I_1\,(g)$ для произвольного ортоморфизма g, доказывается корректность работы алгоритма и приводятся оценки его трудоемкости. Получены также оценки мощности множества $I_1\,(g)$.

При изложении результатов параграфа полагаем, что G — конечная абелева группа порядка n, $n \geqslant 3$.

Алгоритм 1.

Вход. Ортоморфизм $g \in \mathrm{Orth}\,(G)$.

Шаг 0. Положить $i = 0$, $I_1\,(g) = \varnothing$.

Шаг 1. Если $i = A^2_{n-1}$, то алгоритм заканчивает свою работу, на выход подать элементы списка I_1.
Если $i < A^2_{n-1}$, то выбрать новую упорядоченную пару $(x_1, x_2) \in G^2$ со свойством $\max\{x_1, x_2\} \neq z_{n-1}$ и перейти на шаг 2.

Шаг 2. Вычислить элемент $x_3 = x_2 * g\,(x_2)^{-1} * g\,(x_1)$ и перейти на шаг 3.

Шаг 3. Увеличить значение i: $i = i + 1$.
Если $x_3 > \max\{x_1, x_2\}$ и $x_1 * g\,(x_2)^{-1} * g'\,(x_3) = e$, то
вычислить $h = (x_1, x_2)\,(x_2, x_3)\,g$,
добавить h в список $I_1\,(g)$.
Перейти на шаг 1.

Выход. Список $I_1\,(g)$.

Пример 1. Пусть $G = \mathbb{Z}^+_2 \times \mathbb{Z}^+_6$. Рассмотрим ортоморфизм g, заданный таблицей

x	00 01 02 03 04 05 10 11 12 13 14 15
$g\,(x)$	00 03 13 01 11 14 04 10 02 05 15 12
$g'\,(x)$	00 02 11 04 13 15 14 05 10 12 01 03

Результатом применения алгоритма 1 к ортоморфизму $g \in \mathrm{Orth}\,(G)$ является множество $I_1\,(g)$, состоящее из трех ортоморфизмов:

$I_1\,(g)$	15 03 13 01 11 00 04 10 02 05 14 12
	00 04 13 01 11 14 12 10 02 05 15 03
	00 03 13 02 11 14 04 01 10 05 15 12

Следующая теорема описывает свойства ортоморфизмов множества $I_1(g)$ и обосновывает корректность работы алгоритма 1.

Теорема 1. *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* $h = (x_1, x_2)(x_2, x_3)g$. *Тогда следующие условия эквивалентны*:

(1) $h \in \mathrm{Orth}(G)$,

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

Доказательство. Пусть h — ортоморфизм. Покажем, что выполнены условия (2). Заметим, что для элементов $h'(x_1)$, $h'(x_2)$, $h'(x_3)$ справедливы следующие соотношения

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

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

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

Справедливы равенства

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

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

Обратно, пусть выполнены условия (2). Покажем, что $h \in \mathrm{Orth}(G)$. В силу условия $x_1 * g(x_2)^{-1} * g'(x_3) = e$ справедливы равенства

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

Заметим, что из условий $\begin{cases} x_3 * g(x_1)^{-1} * g'(x_2) = e \\ x_1 * g(x_2)^{-1} * g'(x_3) = e \end{cases}$ следует, что

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

Тогда справедливы равенства $h'(x_2) = x_2^{-1} * g(x_3) = g'(x_1)$. В силу условия $x_3 * g(x_1)^{-1} * g'(x_2) = e$ справедливы равенства

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

Следовательно, h — ортоморфизм.

Утверждение 2. *Список* $I_1(g)$ *на выходе алгоритма* 1 *содержит все ортоморфизмы* $h \in \mathrm{Orth}(G)$, *находящиеся на расстоянии* $\chi(g, h) = 3$ *от ортоморфизма* g.

Доказательство. Пусть $g, h \in \mathrm{Orth}(G)$, $\chi(g, h) = 3$. Тогда существуют такие попарно различные элементы $x_1, x_2, x_3 \in G$, что $h = (x_1, x_2)(x_2, x_3)g$. Следовательно, выполнены условия п. 1 теоремы 1.

Обозначим через t_1 трудоемкость алгоритма 1.

Утверждение 3. *При $n \to \infty$ для величины t_1 справедлива оценка*

$$t_1 = O\left(n^2\right).$$

Доказательство. Трудоемкость алгоритма оценивается произведением числа A_{n-1}^2 повторений шага 1 алгоритма и фиксированного числа элементарных операций на шагах 2 и 3 алгоритма.

Из доказанного утверждения следует оценка количества ортоморфизмов в списке $I_1(g)$ на выходе алгоритма 1.

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

$$0 \leqslant |I_1(g)| \leqslant A_{n-1}^2. \tag{1}$$

Таблица 1 содержит оценки чисел $|I_1(g)|$ для всех таких абелевых групп G, $3 \leqslant |G| \leqslant 15$, что $|\mathrm{Orth}(G)| > 0$. Из таблицы следует достижимость оценок (1) для групп малого порядка. Нижняя оценка достигается, например, для групп $\mathbb{F}_5^+$, $\mathbb{F}_7^+$, $\mathbb{Z}_2^+ \times \mathbb{Z}_4^+$. Верхняя оценка достигается для группы $\mathbb{F}_3^+$.

Таблица 1. Оценки числа $|I_1(g)|$ для абелевых групп малого порядка

Группа G	$\lvert G\rvert$	$\lvert\mathrm{Orth}(G)\rvert$	$\min\limits_{g\in\mathrm{Orth}(G)} \lvert I_1(g)\rvert$	$\max\limits_{g\in\mathrm{Orth}(G)} \lvert I_1(g)\rvert$	A_{n-1}^2
$\mathbb{F}_3^+$	3	3	2	2	2
$\mathbb{F}_4^+$	4	8	4	4	6
$\mathbb{F}_5^+$	5	15	0	0	12
$\mathbb{F}_7^+$	7	133	0	15	30
$\mathbb{Z}_2^+ \times \mathbb{Z}_4^+$	8	384	0	0	42
$\mathbb{F}_8^+$	8	384	0	0	42
$\mathbb{Z}_9^+$	9	2025	3	15	56
$\mathbb{F}_9^+$	9	2241	0	24	56
$\mathbb{F}_{11}^+$	11	37851	0	6	90
$\mathbb{Z}_2^+ \times \mathbb{Z}_6^+$	12	198144	0	44	110
$\mathbb{F}_{13}^+$	13	1030367	0	52	132
$\mathbb{Z}_{15}^+$	15	2424195	0	30	182

Замечание 2. Трудоемкость алгоритма 1 по крайней мере в n раз меньше трудоемкости алгоритма, основанного на опробовании всех A_n^3 размещений элементов $x_1, x_2, x_3 \in G$ с последующим вычислением подстановки h и проверкой свойства $h' \in S(G)$.

3.2. Ортоморфизмы на расстоянии Хемминга, равном 4. В этом разделе излагается алгоритм построения множества $I_2(g)$ для произвольного ортоморфизма g, доказывается корректность работы алгоритма и приводятся оценки его трудоемкости. Получены также оценки мощности множества $I_2(g)$.

При изложении результатов параграфа полагаем, что G — конечная абелева группа порядка n, $n \geqslant 4$.

Алгоритм 2.

Вход. Ортоморфизм $g \in \mathrm{Orth}\,(G)$.

Шаг 0. Положить $i = 0$, $I_2\,(g) = \varnothing$.

Шаг 1. Проверить выполнение условий:
если $i = C_n^3 - 1$, то алгоритм заканчивает свою работу, на выход подать элементы списка $I_2\,(g)$,
если $i < C_n^3 - 1$, то
выбрать новое сочетание $(x_1, x_3, x_4) \in G^3$, удовлетворяющее условиям $x_1 < x_3 < x_4$, $x_1 \neq z_{n-3}$,
увеличить значение i: $i = i + 1$,
перейти на шаг 2.

Шаг 2. Вычислить элемент $x_2 = (g')^{-1}\left(g'\,(x_1)^{-1} * g'\,(x_3) * g'\,(x_4)\right)$;
если $x_1 < x_2$, то перейти на шаг 3,
в противном случае перейти на шаг 1.

Шаг 3. Проверить выполнение совокупности условий:

$$\begin{cases} \left(x_1 * g\,(x_2)^{-1} * g'\,(x_3)\right) = e, \text{либо} \left(x_1 * g\,(x_2)^{-1} * g'\,(x_4)\right) = e \\ \left(x_4 * g\,(x_3)^{-1} * g'\,(x_1)\right) = e, \text{либо} \left(x_4 * g\,(x_3)^{-1} * g'\,(x_2)\right) = e \end{cases}$$

Если условия выполнены, то
положить $h = (x_1, x_2)\,(x_3, x_4)\,g$,
добавить h в список $I_2\,(g)$.
Перейти на шаг 2.

Выход. Список $I_2\,(g)$.

Пример 2. Пусть $G = \mathbb{Z}_2^+ \times \mathbb{Z}_4^+$. Рассмотрим ортоморфизм g, заданный таблицей

x	00 01 02 03 10 11 12 13
$g\,(x)$	00 02 10 12 01 13 11 03
$g'\,(x)$	00 01 12 13 11 02 03 10

Результатом применения алгоритма 2 к ортоморфизму g является множество $I_2\,(g)$, состоящее из восьми ортоморфизмов:

	02 00 10 12 01 11 13 03
	10 02 00 12 01 03 11 13
	00 12 10 02 11 13 01 03
$I_2\,(g)$	00 02 12 10 03 13 11 01
	00 02 10 12 13 01 03 11
	12 10 02 00 01 13 11 03
	11 02 01 12 10 13 00 03
	00 03 10 13 01 12 11 02

Следующая теорема описывает свойства ортоморфизмов из множества $I_2\,(g)$ и обосновывает корректность работы алгоритма 2.

Теорема 2. *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* $h = (x_1, x_2)\,(x_3, x_4)\,g$. *Тогда следующие условия эквивалентны*:

(1) $h \in \mathrm{Orth}\,(G)$,

(2) *имеют место соотношения*

$$\begin{gathered} g'(x_1) * g'(x_2) * g'(x_3)^{-1} * g'(x_4)^{-1} = e, \\ \left(x_1 * g(x_2)^{-1} * g'(x_3)\right) = e \text{ или } \left(x_1 * g(x_2)^{-1} * g'(x_4)\right) = e, \\ \left(x_4 * g(x_3)^{-1} * g'(x_1)\right) = e \text{ или } \left(x_4 * g(x_3)^{-1} * g'(x_2)\right) = e. \end{gathered}$$

Доказательство. Пусть h — ортоморфизм. Покажем, что выполнены условия (2). Заметим, что элементы $h'(x_1)$, $h'(x_2)$, $h'(x_3)$, $h'(x_4)$ удовлетворяют следующим условиям:

$$\left\{ \begin{array}{l} h'(x_1) \neq g'(x_1) \\ h'(x_1) \neq g'(x_2) \end{array} \right., \left\{ \begin{array}{l} h'(x_2) \neq g'(x_1) \\ h'(x_2) \neq g'(x_2) \end{array} \right.,$$

$$\left\{ \begin{array}{l} h'(x_3) \neq g'(x_3) \\ h'(x_3) \neq g'(x_4) \end{array} \right., \left\{ \begin{array}{l} h'(x_4) \neq g'(x_3) \\ h'(x_4) \neq g'(x_4) \end{array} \right..$$

Тогда

$$(h'(x_1), h'(x_2), h'(x_3), h'(x_4)) \in \left\{ \begin{array}{c} (g'(x_3), g'(x_4), g'(x_1), g'(x_2)), \\ (g'(x_3), g'(x_4), g'(x_2), g'(x_1)), \\ (g'(x_4), g'(x_3), g'(x_1), g'(x_2)), \\ (g'(x_4), g'(x_3), g'(x_2), g'(x_1)) \end{array} \right\}.$$

В первом случае

$$\left\{ \begin{array}{l} h'(x_1) = g(x_2) * x_1^{-1} \\ h'(x_1) = g(x_3) * x_3^{-1} \end{array} \right., \left\{ \begin{array}{l} h'(x_2) = g(x_1) * x_2^{-1} \\ h'(x_2) = g(x_4) * x_4^{-1} \end{array} \right.,$$

$$\left\{ \begin{array}{l} h'(x_3) = g(x_4) * x_3^{-1} \\ h'(x_3) = g(x_1) * x_1^{-1} \end{array} \right., \left\{ \begin{array}{l} h'(x_4) = g(x_3) * x_4^{-1} \\ h'(x_4) = g(x_2) * x_2^{-1} \end{array} \right..$$

Поэтому

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

Аналогично рассматриваются оставшиеся 3 случая.

Обратно, пусть выполнены следующие равенства из п. (2):

$$\begin{gathered} g'(x_1) * g'(x_2) * g'(x_3)^{-1} * g'(x_4)^{-1} = e, \\ \left(x_1 * g(x_2)^{-1} * g'(x_3)\right) = e, \\ \left(x_4 * g(x_3)^{-1} * g'(x_2)\right) = e. \end{gathered}$$

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

Так как $h = (x_1, x_2)\,(x_3, x_4)\,g$, то элементы $h'\,(x_i)$, $i = \overline{1,4}$, имеют вид

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

Покажем, что $h'\,(x_1) = g'\,(x_3)$. Из равенства $\left(x_1 * g\,(x_2)^{-1} * g'\,(x_3)\right) = e$ следует, что $g'\,(x_3) = g\,(x_2) * x_1^{-1}$. Тогда

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

Покажем, что $h'\,(x_2) = g'\,(x_4)$. Так как

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

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

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

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

Покажем, что $h'\,(x_3) = g'\,(x_1)$. Из равенств

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

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

следует равенство $g'\,(x_1) = g\,(x_4) * x_3^{-1}$.

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

Покажем, что $h'\,(x_4) = g'\,(x_2)$. Из равенства $\left(x_4 * g\,(x_3)^{-1} * g'\,(x_2)\right) = e$ следует, что $g'\,(x_2) = g\,(x_3) * x_4^{-1}$. Поэтому $h'\,(x_4) = g\,(x_3) * x_4^{-1} = g'\,(x_2)\,.$

Следовательно, h — ортоморфизм.

Случаи выполнения других наборов равенств п. (2) теоремы проверяются аналогично.

Обозначим через t_2 трудоемкость алгоритма 2.

Утверждение 4. *При $n \to \infty$ для величины t_2 справедлива оценка*

$$t_2 = O\left(n^3\right).$$

Доказательство. Трудоемкость алгоритма оценивается произведением числа $C_n^3 - 1$ повторений шага 1 алгоритма и фиксированного числа элементарных операций на шагах 2 и 3 алгоритма.

Из доказанного утверждения следует оценка количества ортоморфизмов в списке $I_2\,(g)$ на выходе алгоритма 2.

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

$$0 \leqslant |I_2\,(g)| \leqslant C_n^3 - 1. \tag{2}$$

Таблица 2. Оценки числа $|I_2(g)|$ для абелевых групп малого порядка

Группа G	$\lvert G\rvert$	$\lvert\mathrm{Orth}(G)\rvert$	$\min\limits_{g\in\mathrm{Orth}(G)} \lvert I_2(g)\rvert$	$\max\limits_{g\in\mathrm{Orth}(G)} \lvert I_2(g)\rvert$	C_n^3-1
$\mathbb{F}_4^+$	4	8	3	3	3
$\mathbb{F}_5^+$	5	15	0	5	9
$\mathbb{F}_7^+$	7	133	0	6	34
$\mathbb{Z}_2^+ \times \mathbb{Z}_4^+$	8	384	8	8	55
$\mathbb{F}_8^+$	8	384	14	14	55
$\mathbb{Z}_9^+$	9	2025	0	6	83
$\mathbb{F}_9^+$	9	2241	0	18	83
$\mathbb{F}_{11}^+$	11	37851	0	10	164
$\mathbb{Z}_2^+ \times \mathbb{Z}_6^+$	12	198144	1	17	219
$\mathbb{F}_{13}^+$	13	1030367	0	39	285
$\mathbb{Z}_{15}^+$	15	2424195	0	42	454

Таблица 2 содержит оценки числа $|I_2(g)|$ для всех абелевых групп G, $4 \leqslant |G| \leqslant 15$ с $|\mathrm{Orth}(G)| > 0$. Из таблицы следует достижимость оценок (2) над группами малого порядка. Нижняя оценка достигается, например, над группами $\mathbb{F}_5^+$, $\mathbb{F}_7^+$, $\mathbb{Z}_9^+$. Верхняя оценка достигается над группой $\mathbb{F}_4^+$.

Замечание 3. Трудоемкость алгоритма 2, по крайней мере, в n раз меньше трудоемкости алгоритма, основанного на опробовании всех A_n^4 размещений элементов $x_1, x_2, x_3, x_4 \in G$, с последующим вычислением подстановки h и проверкой свойства $h' \in S(G)$.

Множество $\mathrm{Orth}(G)$ может содержать ортоморфизмы g, на минимально возможном расстоянии от которых нет ни одного ортоморфизма, т.е. $I(g) = \varnothing$. Этот факт иллюстрируется следующим примером.

Пример 3. (1) Пусть $G = \mathbb{F}_{2^4}^+$. Рассмотрим ортоморфизм g, заданный таблицей

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

Применением алгоритмов 1 и 2 легко убедиться в том, что на минимально возможном расстоянии от g ортоморфизмов нет.

(2) Пусть $G = \mathbb{Z}_{15}^+$. Рассмотрим ортоморфизм g, заданный таблицей

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

Применением алгоритмов 1 и 2 легко убедиться в том, что $I(g) = \varnothing$.

Автор благодарен Б.А. Погорелову, И.А. Круглову и С.И. Чечёте за полезные обсуждения и ценные замечания.

Список литературы

1. Глухов М.М., “О методах построения систем ортогональных квазигрупп с использованием групп”, *Математические вопросы криптографии*, **2**:4 (2011), 5–24.
2. Глухов М.М., “О применениях квазигрупп в криптографии”, *Прикл. дискрет. матем.*, **2**:2 (2008), 28–32.
3. Зубов А.Ю, *Математика кодов аутентификации*, М.: Гелиос АРВ, 2007, 480 с.
4. Менячихин А.В., “Спектрально-линейный и спектрально-дифференциальный методы построения S-боксов с близкими к оптимальным значениями криптографических параметров”, *Математические вопросы криптографии*, **8**:2 (2017), 97–116.
5. Менячихин А.В., “Устройство для построения ортоморфизмов, использующее парные разности”, *Патент на изобретение* № 2632119 *РФ*, **33** (2017).
6. Тришин А.Е., “О показателе нелинейности кусочно-линейных подстановок аддитивной группы поля F_{2^n}”, *Прикл. дискретн. матем.*, **4**:30 (2015), 32–42.
7. Тришин А.Е., “Способ построения ортогональных латинских квадратов на основе подстановочных двучленов конечных полей”, *Обозр. прикл. и промышл. матем.*, **15**:4 (2008), 764–765.
8. Тужилин М.Э., “Латинские квадраты и их применение в криптографии”, *Прикл. дискретн. матем. Приложение*, **3**:17 (2012), 47–52.
9. Черемушкин А.В., *Криптографические протоколы. Основные свойства и уязвимости*, Изд. центр «Академия», Москва, 2009, 272 с.
10. Buchheim C., Cameron P.J., Wu T., “On the subgroup distance problem”, *Electr. Colloq. Comput. Compl.*, **146** (2006).
11. Daemen J., “Limitations of the Even–Mansour construction”, ASIACRYPT’91, Lect. Notes Comput. Sci., **739**, 1991, 495–498.
12. Denes J., Keedwell A. D., *Latin squares and their applications*, Academiai Kiado, Budapest, 2015, 545 pp.
13. Dinur I., Dunkelman O., Keller N., Shamir A., “Key recovery attacks on 3-round Even–Mansour, 8-step LED-128, and full AES”, *http://eprint.iacr.org*/2013/391, 2013.
14. Evans A., *Orthomorphisms graphs and groups*, Berlin: Springer-Verlag, 1992.
15. Evans A., “Applications of complete mappings and orthomorphisms of finite groups”, *Quasigroups and relat. syst.*, **23** (2015), 5–30.
16. Even E. Mansour Y., “A construction of a cipher from a single pseudorandom permutation”, ASIACRYPT’91, Lect. Notes Comput. Sci., **739**, 1991, 210–224.
17. Gligoroski D., Markovski S., Kocarev L., “Edon-R: An infinite family of cryptographic hash functions”, *Int. J. Network Secur.*, **8**:3 (2009), 293–300.
18. Johnson D.M., Dulmage A.L. and Mendelsohn N.S., “Orthomorphisms of groups and orthogonal Latin squares”, I. *Canad. J. Math.*, **13** (1961), 356–372.
19. Mann H.B., “On orthogonal Latin squares”, *Bull. Amer. Math. Soc.*, **50** (1944), 249–257.
20. Niederreiter H., Robinson K., “Bol loops of order pq”, *Math. Proc. Cambr. Phil. Soc.*, **89** (1981), 241–256.
21. Niederreiter H., Robinson K., “Complete mappings of finite fields”, *J. Austral. Math. Soc. Ser.*, **33** (1982), 197–212.
22. Nikolic I., Wang L., Wu S., “Cryptoanalysis of round-reduce LED”, FSE’2013, Lect. Notes Comput. Sci., **8424**, 2013, 112–130.
23. Paige L.J., “A note on finite Abelian groups”, *Bull. Amer. Math. Soc.*, **53** (1947), 590–593.
24. Pinch R.G.E., “The distance of permutation from a subgroup of S_n”, *Combinatorics and Probability*, Cambridge Univ. Press, 2006, 473–479.

Статья поступила 29.06.2018.
Переработанный вариант поступил 05.10.2018.