# Псевдогеометрии с кластерами и пример рекурсивного $[4, 2, 3]_{42}$-кода*

**В. Т. МАРКОВ**
*Московский государственный университет им. М. В. Ломоносова*
e-mail: markov@mech.math.msu.su

**А. А. НЕЧАЕВ**
*Московский государственный университет им. М. В. Ломоносова*
e-mail: alexnechaev@bnt-net.ru

**С. С. СКАЖЕНИК**
*Московский государственный университет им. М. В. Ломоносова*
e-mail: sskazhenik@yandex.ru

**Е. О. ТВЕРИТИНОВ**
*Московский государственный университет им. М. В. Ломоносова*
e-mail: eugenetver@yandex.ru

УДК 512.548.7+519.143+514.146.5

**Ключевые слова:** рекурсивные коды, МДР-коды, рекурсивно дифференцируемые квазигруппы, псевдогеометрии.

**Аннотация**

В 1998 г. Е. Коусело, С. Гонсалес, В. Т. Марков и А. А. Нечаев определили рекурсивные коды и получили результаты, позволяющие выдвинуть гипотезу о существовании рекурсивных МДР-кодов размерности 2 и длины 4 над любым конечным алфавитом мощности $q \notin \{2, 6\}$, которая осталась недоказанной лишь для $q \in \{14, 18, 26, 42\}$. В данной работе доказано существование такого кода для $q = 42$. Использована новая конструкция — псевдогеометрия с кластерами.

**Abstract**

*V. T. Markov, A. A. Nechaev, S. S. Skazhenik, E. O. Tveritinov, Pseudogeometries with clusters and an example of a recursive* $[4, 2, 3]_{42}$*-code*, Fundamentalnaya i prikladnaya matematika, vol. 14 (2008), no. 4, pp. 181—192.

In 1998, E. Couselo, S. Gonzalez, V. Markov, and A. Nechaev defined the recursive codes and obtained some results that allowed one to conjecture the existence of recursive MDS-codes of dimension 2 and length 4 over any finite alphabet of cardinality $q \notin \{2, 6\}$. This conjecture remained open only for $q \in \{14, 18, 26, 42\}$. It is shown in this paper that there exist such codes for $q = 42$. We used a new construction, that of pseudogeometry with clusters.

*Работа поддержана грантом РФФИ 08-01-00693-а и грантами поддержки научных школ НШ-1983.2008.1, НШ-4.2008.10.

*Фундаментальная и прикладная математика*, 2008, том 14, № 4, с. 181—192.

# 1. Введение

Пусть $\Omega = \{a_1, \ldots, a_q\}$ — произвольное конечное множество, $q = |\Omega| \geqslant 2$. Любое подмножество $\mathcal{K} \subseteq \Omega^n$ называется *кодом длины* $n$ или $n$*-кодом в алфавите* $\Omega$, код $\mathcal{K}$ называется $[n, k]_\Omega$*-кодом*, если $|\mathcal{K}| = q^k$ (здесь, вообще говоря, $k \in \mathbb{R}$). Мы назовём $k$ *комбинаторной размерностью* кода $\mathcal{K}$. *Расстояние* (*Хемминга*) $d(\vec{u}, \vec{v})$ между двумя словами $\vec{u}, \vec{v} \in \Omega^n$ определяется как число различных координат с одинаковыми номерами в словах $\vec{u}$ и $\vec{v}$. *Расстояние* $d(\mathcal{K})$ кода $\mathcal{K}$ есть минимум расстояний между его различными словами. Будем говорить, что $[n, k]_\Omega$-код $\mathcal{K}$ есть $[n, k, d]_\Omega$-код, или $[n, k, d]_q$-код, если $d(\mathcal{K}) = d$. Известно, что длина $n$, размерность $k$ и расстояние $d$ произвольного кода удовлетворяют неравенству

$$d \leqslant n - k + 1$$

(*граница Синглтона* [3]). Если $d = n - k + 1$, код называется *МДР-кодом*.

В первом нетривиальном случае, когда $n = 4$, $k = 2$, задача построения $[4, 2]_q$-МДР-кода, т. е. $[4, 2, 3]_q$-кода, эквивалентна построению двух ортогональных латинских квадратов в алфавите мощности $q$. Очевидно, таких квадратов не существует, если $q = 2$. Отсутствие таких квадратов при $q = 6$ (гипотеза Эйлера) было доказано в [5]. К середине прошлого века было доказано, что для всех остальных значений $q > 2$ ортогональная пара латинских квадратов, т. е. $[4, 2, 3]_q$-код, существует [4].

В [1, 2] было начато исследование проблемы, часть которой в рамках введённых определений можно сформулировать как проблему построения ортогональных латинских квадратов с дополнительными условиями. В общем виде эта проблема формулируется следующим образом.

Назовём код $\mathcal{K}$ *полным* $k$*-рекурсивным кодом*, если существует функция $f\colon \Omega^k \to \Omega$ $(k \leqslant n)$, такая что $\mathcal{K}$ есть множество всех слов $u(\overline{0, n-1}) = \big(u(0), \ldots, u(n-1)\big) \in \Omega^n$, удовлетворяющих условию $u(i + k) = f\big(u(i), \ldots, u(i + k - 1)\big)$ для $i \in \overline{0, n-k}$, $u(0), \ldots, u(k-1)$ — произвольные элементы из $\Omega$. Далее такой код обозначается через $\mathcal{K}(n, f)$. Любой подкод полного $k$-рекурсивного кода $\mathcal{K}$ назовём $k$*-рекурсивным*.

В [1, 2] исследовался вопрос о существовании (автоматически полного) рекурсивного МДР-кода при заданных значениях $n$, $k$ и $q$. В первом нетривиальном случае ($n = 4$, $k = 2$) было доказано существование рекурсивного $[4, 2, 3]_q$-кода при всех $q \notin \{2, 6, 14, 18, 26, 42\}$, причём если $q \in \{2, 6\}$, то таких кодов, как известно, не существует, а при $q \in \{14, 18, 26, 42\}$ вопрос остался открытым. Частично мы отвечаем на него в данной работе: построен рекурсивный $[4, 2, 3]_{42}$-код.

Отметим, что вопрос о существовании рекурсивного $[4, 2, 3]_q$-кода эквивалентен вопросу о существовании рекурсивно дифференцируемой квазигруппы порядка $q$ [1]. Напомним, что квазигруппа — это множество $\Omega$ с бинарной операцией $\cdot$, в которой каждое из уравнений $a \cdot x = b$ и $y \cdot a = b$ имеет единственное

решение для любых $a, b \in \Omega$. Операция на $\Omega$ может рассматриваться как функция $f\colon \Omega \times \Omega \to \Omega$, эта функция также будет иногда называться квазигруппой. Квазигруппа $(\Omega, \cdot)$ называется *рекурсивно дифференцируемой*, если операция $x \odot y = y \cdot (x \cdot y)$ определяет на $\Omega$ структуру квазигруппы. Группоид $(\Omega, \odot)$ называется *рекурсивной производной* квазигруппы $(\Omega, \cdot)$. Доказано [1, теорема 2.17], что код $\{(x, y, x \cdot y, x \odot y)\colon x, y \in \Omega\}$ (рекурсивный по определению) является МДР-кодом тогда и только тогда, когда квазигруппа $(\Omega, \cdot)$ рекурсивно дифференцируема, и любой рекурсивный $[4,2,3]_q$-код имеет такой вид.

Очевидно, что операция на конечном множестве $\Omega$ определяет квазигруппу тогда и только тогда, когда её таблица Кэли — латинский квадрат, т. е. каждая строка и каждый столбец этой таблицы есть перестановка элементов множества $\Omega$. Таким образом, построение рекурсивно дифференцируемой квазигруппы заданной мощности $q$ равносильно построению пары латинских квадратов, определённых операциями $\cdot$ и $\odot$ соответственно, причём эти латинские квадраты оказываются ортогональными (см., например, [4, с. 244]). В терминах квазигрупповых операций ортогональность таблиц Кэли $(\Omega, \circ)$ и $(\Omega, *)$ означает, что система уравнений $x \circ y = a$, $x * y = b$ имеет единственное решение $x, y \in \Omega$ для любых $a, b \in \Omega$.

Квазигруппа $(\Omega, \circ)$ называется *идемпотентной*, если $a \circ a = a$ для любого $a \in \Omega$.

В [1] использовались две основных конструкции: расширение квазигруппы с помощью трансверсалей и построение идемпотентных рекурсивно дифференцируемых квазигрупп с помощью псевдогеометрий. В данной работе использовано обобщение второго из этих подходов.

## 2. Псевдогеометрии с нуклеусами и кластерами

**Определение 2.1.** Пусть $\mathcal{P}$ — некоторое непустое множество (элементы которого будем называть *точками*), $\mathcal{L}$ — некоторое множество непустых подмножеств множества $\mathcal{P}$ (называемых *прямыми*). Пара $(\mathcal{P}, \mathcal{L})$ называется *псевдогеометрией*, если каждые две различные точки множества $\mathcal{P}$ принадлежат ровно одной прямой.

Пусть $(\mathcal{P}, \mathcal{L})$ — псевдогеометрия. Произвольное подмножество $\mathcal{N} \subset \mathcal{L}$, состоящее из попарно не пересекающихся прямых, называется *нуклеусом* псевдогеометрии $(\mathcal{P}, \mathcal{L})$.

**Теорема 2.2 [2, теорема 8].** *Пусть $(\mathcal{P}, \mathcal{L})$ — псевдогеометрия с нуклеусом $\mathcal{N}$, такая что выполняются следующие условия*:

1) *для любой прямой $L \in \mathcal{L} \setminus \mathcal{N}$ существует идемпотентная рекурсивно дифференцируемая квазигруппа $g_L(x, y)$ на множестве $L$;*
2) *для любой прямой $N \in \mathcal{N}$ существует рекурсивно дифференцируемая квазигруппа $h_N(x, y)$ на множестве $N$.*

*Тогда существует рекурсивно дифференцируемая квазигруппа на множестве $\mathcal{P}$.*

Переход к псевдогеометрии с кластерами состоит в том, что точки псевдогеометрии заменяются некоторыми непересекающимися конечными множествами, называемыми кластерами.

**Определение 2.3.** Рассмотрим некоторое разбиение $\mathcal{C}$ множества $\mathcal{P}$ на непустые непересекающиеся подмножества $C \in \mathcal{C}$. Элементы множества $\mathcal{C}$ назовём кластерами. Пусть $(\mathcal{C}, \mathcal{L})$ — псевдогеометрия с множеством точек $\mathcal{C}$. Тогда тройку $(\mathcal{P}, \mathcal{C}, \mathcal{L})$ назовём псевдогеометрией на кластерах $\mathcal{C}$. *Нуклеусом* псевдогеометрии $(\mathcal{P}, \mathcal{C}, \mathcal{L})$ назовём произвольное множество попарно не пересекающихся прямых. Объединение кластеров, принадлежащих прямой $L \in \mathcal{L}$, обозначим через $\bar{L}$.

Ясно, что обычную псевдогеометрию можно рассматривать как псевдогеометрию на кластерах, каждый из которых состоит из одной точки.

Следующее утверждение — обобщение теоремы 2.2.

**Теорема 2.4.** *Пусть $(\mathcal{P}, \mathcal{C}, \mathcal{L})$ — псевдогеометрия на кластерах $\mathcal{C}$ с нуклеусом $\mathcal{N}$ и для любой прямой $L \in \mathcal{L}$ определена квазигрупповая операция $g_L(x, y)$ на множестве $\bar{L}$, причём выполняются следующие условия*:

1) *каждая квазигруппа $(\bar{L}, g_L)$, $L \in \mathcal{L}$, рекурсивно дифференцируема*;
2) *если $C \in L$ и $L \in \mathcal{L} \setminus \mathcal{N}$, то $C$ — подквазигруппа в $\bar{L}$*;
3) *если $L, M \in \mathcal{L} \setminus \mathcal{N}$ и $L \cap M = \{C\}$, $C \in \mathcal{C}$, то $g_L(x, y) = g_M(x, y)$ для любых $x, y \in C$.*

*Тогда существует рекурсивно дифференцируемая квазигруппа на множестве $\mathcal{P}$.*

**Доказательство.** Определим операцию на множестве $\mathcal{P}$ следующим образом.

1. Если точки $x, y \in \mathcal{P}$ принадлежат различным кластерам $C_x$ и $C_y$, то существует единственная прямая $L \in \mathcal{L}$, содержащая оба этих кластера. Положим $g(x, y) = g_L(x, y)$.
2. Если точки $x, y \in \mathcal{P}$ принадлежат одному кластеру $C$ и существует (единственная по определению нуклеуса) прямая $L \in \mathcal{N}$, такая что $C \in L$, то положим $g(x, y) = g_L(x, y)$.
3. Если точки $x, y \in \mathcal{P}$ принадлежат одному кластеру $C$ и не существует прямой, принадлежащей нуклеусу и содержащей кластер $C$, то положим $g(x, y) = g_L(x, y)$, где $L$ — произвольная прямая, содержащая кластер $C$ (в силу третьего условия результат не зависит от выбора прямой $L$).

Аналогично доказательству теоремы 2.2, приведённому в [2], покажем, что операция $g(x, y)$ определяет квазигруппу на $\mathcal{P}$ и при условии 1) эта квазигруппа оказывается рекурсивно дифференцируемой. Действительно, пусть $x, z \in \mathcal{P}$. Рассмотрим два случая и в каждом из них найдём элемент $y \in \mathcal{P}$, такой что $g(x, y) = z$.

1. Точки $x, z \in \mathcal{P}$ принадлежат различным кластерам $C_x$ и $C_z$. Тогда существует единственная прямая $L \in \mathcal{L}$, содержащая оба эти кластера. Поскольку $g_L$ определяет квазигруппу на $\bar{L}$, существует элемент $y \in \bar{L}$, такой что $g_L(x, y) = z$. Если $y \notin C_x$, то по определению операции на $\mathcal{P}$ имеем

$g(x,y) = g_L(x,y) = z$. Если же $y \in C_x$, то в силу условия 2) $L \in \mathcal{N}$, и снова получаем $g(x,y) = g_L(x,y) = z$.

2. Точки $x, z \in \mathcal{P}$ принадлежат одному кластеру $C$. Тогда опять имеется две возможности. Если существует прямая $L \in \mathcal{N}$, содержащая кластер $C$, то найдётся точка $y \in \bar{L}$, такая что $g(x,y) = g_L(x,y) = z$. В противном случае можно выбрать любую прямую $L \in \mathcal{L}$, такую что $C \in L$. В силу условия 2) существует элемент $y \in C$, такой что $g_L(x,y) = z$, причём в силу условия 3) элемент $y$ не зависит от выбора прямой $L$. Снова по определению операции на $\mathcal{P}$ имеем $g(x,y) = g_L(x,y) = z$.

Аналогично проверяется возможность правого деления в группоиде $(\mathcal{P}, g)$. Из конечности множества $\mathcal{P}$ следует, что $(\mathcal{P}, g)$ — квазигруппа.

Осталось показать, что эта квазигруппа является рекурсивно дифференцируемой. Для этого достаточно проверить, что при любых $x, z \in \mathcal{P}$ существует элемент $y \in \mathcal{P}$, такой что $g\big(y, g(x,y)\big) = z$. Снова рассмотрим два случая.

1. Точки $x, z \in \mathcal{P}$ принадлежат различным кластерам $C_x$ и $C_z$. Тогда существует единственная прямая $L \in \mathcal{L}$, содержащая оба этих кластера. В силу условия 1) существует элемент $y \in \bar{L}$, такой что $g_L\big(y, g_L(x,y)\big) = z$. При этом $g_L(x,y) \in L$, следовательно, $g(x,y) = g_L(x,y)$ и $g\big(y, g(x,y)\big) = g_L\big(y, g_L(x,y)\big)$.
2. Если точки $x, z \in \mathcal{P}$ принадлежат одному кластеру $C$, то опять существуют две возможности. Если имеется прямая $L \in \mathcal{N}$, содержащая кластер $C$, то можно повторить предыдущие рассуждения. В противном случае достаточно воспользоваться тем, что подквазигруппа $C$ рекурсивно дифференцируемой квазигруппы очевидно является рекурсивно дифференцируемой. □

## 3. Основная конструкция

Опишем общую конструкцию построения псевдогеометрии из системы попарно ортогональных латинских квадратов.

Пусть $q$ — натуральное число, причём существует система $f_1, \ldots, f_k$ из $k$ попарно ортогональных латинских квадратов порядка $q$, $f_i \colon (\overline{0, q-1})^2 \to \overline{0, q-1}$. Рассмотрим множество $P$ всех пар $(x,y)$, $x \in \overline{0, q-1}$, $y \in \overline{-1, k}$. Определим прямые двух типов:

1) *горизонтальные прямые*

$$\{(x,y) \colon x \in \overline{0, q-1}\}$$

для любого фиксированного $y \in \overline{-1, k}$;

2) *наклонные прямые*

$$\{(i,-1), (j,0)\} \cup \{(f_y(i,j), y) \colon y \in \overline{1, k}\}$$

для любой фиксированной пары $i, j \in \overline{0, q-1}$.

Полученная псевдогеометрия $APG(q,k)$ содержит $q(k+2)$ точек, $k+2$ горизонтальных и $q^2$ наклонных прямых, причём каждая горизонтальная (наклонная) прямая содержит $q$ (соответственно $k+2$) точек.

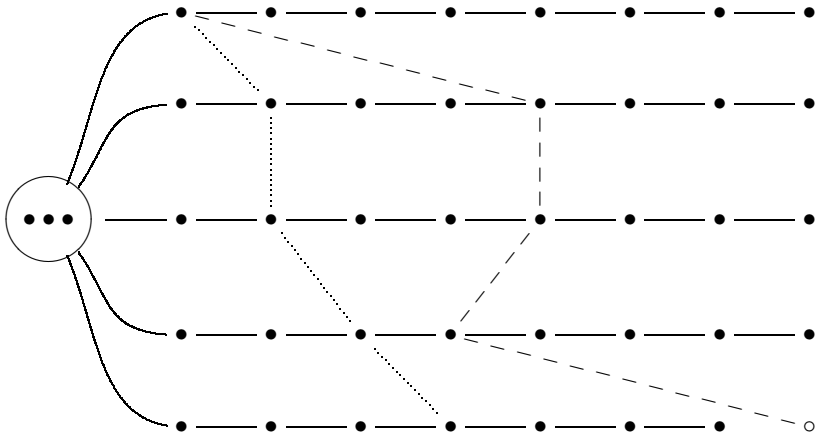

Рис. 1. Псевдогеометрия порядка 42

Рассмотрим псевдогеометрию $APG(8,5)$, использующую три ортогональных латинских квадрата, которые будут построены в разделе 4. Удалим из неё произвольную точку. Рассмотрим получившуюся псевдогеометрию как псевдогеометрию на кластерах $(\mathcal{P},\mathcal{C},\mathcal{L})$ (на данном этапе все кластеры порядка 1). Добавим один «бесконечно удалённый» кластер порядка 3 к множеству $\mathcal{C}$ и каждой горизонтальной прямой. Получим псевдогеометрию $(\mathcal{P}',\mathcal{C}',\mathcal{L}')$ порядка 42 с горизонтальными прямыми длины 10 и 11, наклонными прямыми длины 4 и 5. Прямые длины 4 и прямая длины 10 образуют нуклеус $N'$. Эти прямые действительно не пересекаются, так как их общий кластер был удалён, а через любые два кластера проходит только одна прямая. Построенная псевдогеометрия показана на рис. 1. Пустой кружок обозначает удалённую точку, а чёрные кружки — точки множества $\mathcal{P}$. Единственный нетривиальный кластер расположен в левой части рисунка. Сплошные линии показывают горизонтальные прямые, пунктирная линия — одну наклонную прямую, принадлежащую нуклеусу, а точечная — одну прямую, не принадлежащую нуклеусу.

Теперь, чтобы применить теорему 2.4 к указанной конструкции, осталось определить операции на прямых, удовлетворяющие условиям этой теоремы. Для этого нам потребуются некоторые дополнительные построения.

# 4. Вспомогательные построения

Для построения рекурсивно дифференцируемой квазигруппы порядка 42 нам понадобятся следующие объекты:

1) рекурсивно дифференцируемая квазигруппа порядка 4;
2) идемпотентная рекурсивно дифференцируемая квазигруппа порядка 5;
3) три попарно ортогональные квазигруппы порядка 8;
4) рекурсивно дифференцируемая квазигруппа порядка 10 с подквазигруппой порядка 3;
5) рекурсивно дифференцируемая квазигруппа порядка 11 с подквазигруппой порядка 3, такая что элементы, не входящие в эту подквазигруппу, — идемпотенты.

Квазигруппы из пунктов 1)—4) известны (см. [1,2]). Их также легко построить на компьютере и получить, например, следующие таблицы Кэли.

Квазигруппа порядка 4 и её рекурсивная производная:

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 2 & 3 & 0 & 1 \\ 3 & 2 & 1 & 0 \\ 1 & 0 & 3 & 2 \end{array}, \qquad \begin{array}{cccc} 0 & 3 & 1 & 2 \\ 2 & 1 & 3 & 0 \\ 3 & 0 & 2 & 1 \\ 1 & 2 & 0 & 3 \end{array}.$$

Квазигруппа порядка 5 и её рекурсивная производная:

$$\begin{array}{ccccc} 0 & 2 & 1 & 4 & 3 \\ 3 & 1 & 4 & 0 & 2 \\ 4 & 3 & 2 & 1 & 0 \\ 2 & 4 & 0 & 3 & 1 \\ 1 & 0 & 3 & 2 & 4 \end{array}, \qquad \begin{array}{ccccc} 0 & 4 & 3 & 1 & 2 \\ 4 & 1 & 0 & 2 & 3 \\ 3 & 0 & 2 & 4 & 1 \\ 1 & 2 & 4 & 3 & 0 \\ 2 & 3 & 1 & 0 & 4 \end{array}.$$

Ортогональные латинские квадраты порядка 8 получаются из следующей конструкции. Пусть $\mathbb{F}_8$ — поле из восьми элементов. Введём функции $f_i\colon \mathbb{F}_8^2 \to \mathbb{F}_8$,

$$f_i(x,y) = x + \alpha_i \cdot y,$$

где $\alpha_i$, $i \in \overline{1,3}$, — попарно различные элементы $\mathbb{F}_8^*$. Соответствующие квазигруппы попарно ортогональны. Мы использовали следующие три квадрата:

$$\begin{array}{cccccccc} 0&1&2&3&4&5&6&7 \\ 1&0&3&2&5&4&7&6 \\ 2&3&0&1&6&7&4&5 \\ 3&2&1&0&7&6&5&4 \\ 4&5&6&7&0&1&2&3 \\ 5&4&7&6&1&0&3&2 \\ 6&7&4&5&2&3&0&1 \\ 7&6&5&4&3&2&1&0 \end{array}, \qquad \begin{array}{cccccccc} 0&2&4&6&3&1&7&5 \\ 1&3&5&7&2&0&6&4 \\ 2&0&6&4&1&3&5&7 \\ 3&1&7&5&0&2&4&6 \\ 4&6&0&2&7&5&3&1 \\ 5&7&1&3&6&4&2&0 \\ 6&4&2&0&5&7&1&3 \\ 7&5&3&1&4&6&0&2 \end{array}, \qquad \begin{array}{cccccccc} 0&3&6&5&7&4&1&2 \\ 1&2&7&4&6&5&0&3 \\ 2&1&4&7&5&6&3&0 \\ 3&0&5&6&4&7&2&1 \\ 4&7&2&1&3&0&5&6 \\ 5&6&3&0&2&1&4&7 \\ 6&5&0&3&1&2&7&4 \\ 7&4&1&2&0&3&6&5 \end{array}.$$

Рекурсивно дифференцируемая квазигруппа порядка 10 с подквазигруппой порядка 3 получается расширением с помощью трансверсалей квазигруппы порядка 7 (см. [1, пример после следствия 4.6]):

$$\begin{array}{cccccccccc}
0 & 1 & 2 & 7 & 9 & 4 & 6 & 8 & 3 & 5 \\
1 & 2 & 0 & 8 & 3 & 5 & 7 & 9 & 4 & 6 \\
2 & 0 & 1 & 3 & 5 & 7 & 9 & 4 & 6 & 8 \\
4 & 3 & 8 & 9 & 1 & 0 & 5 & 6 & 7 & 2 \\
8 & 7 & 5 & 4 & 2 & 6 & 1 & 0 & 9 & 3 \\
5 & 4 & 9 & 6 & 7 & 8 & 2 & 3 & 1 & 0 \\
9 & 8 & 6 & 1 & 0 & 3 & 4 & 5 & 2 & 7 \\
6 & 5 & 3 & 2 & 4 & 1 & 0 & 7 & 8 & 9 \\
3 & 9 & 7 & 5 & 6 & 2 & 8 & 1 & 0 & 4 \\
7 & 6 & 4 & 0 & 8 & 9 & 3 & 2 & 5 & 1
\end{array}, \qquad
\begin{array}{cccccccccc}
0 & 2 & 1 & 6 & 3 & 7 & 4 & 8 & 5 & 9 \\
1 & 0 & 2 & 7 & 4 & 8 & 5 & 9 & 6 & 3 \\
2 & 1 & 0 & 9 & 6 & 3 & 7 & 4 & 8 & 5 \\
9 & 8 & 6 & 2 & 7 & 5 & 3 & 0 & 1 & 4 \\
3 & 9 & 7 & 1 & 5 & 2 & 8 & 6 & 4 & 0 \\
4 & 3 & 8 & 5 & 0 & 1 & 6 & 2 & 9 & 7 \\
5 & 4 & 9 & 3 & 8 & 6 & 0 & 1 & 7 & 2 \\
6 & 5 & 3 & 8 & 2 & 4 & 9 & 7 & 0 & 1 \\
7 & 6 & 4 & 0 & 1 & 9 & 2 & 5 & 3 & 8 \\
8 & 7 & 5 & 4 & 9 & 0 & 1 & 3 & 2 & 6
\end{array}.$$

Пример рекурсивно дифференцируемой квазигруппы порядка 11 с подквазигруппой порядка 3, дополнение к которой состоит из идемпотентов, не был известен ранее. В следующем разделе описан алгоритм её построения с помощью компьютера.

## 5. Алгоритм перебора для построения квазигруппы порядка 11

Обозначим $\Omega = \{0, \ldots, 10\}$, $G = (\Omega, \cdot)$, $G' = (\Omega, \odot)$, где $x \odot y = y \cdot (x \cdot y)$.

1. Берём $\mathbb{Z}_3$ в качестве рекурсивно дифференцируемой квазигруппы порядка 3 (так как она заполняет левый верхний угол в квазигруппе порядка 10) и заполняем левый верхний угол таблицы размера $11 \times 11$. Заполняем диагональ, учитывая идемпотентность остальных элементов $G$.
2. Запоминаем в массив «хорошие» перестановки порядка 8, т. е. не вступающие в конфликт с элементами на диагонали.
3. Пользуясь массивом из предыдущего пункта, заполняем первые три строки, на каждом шаге делая проверку по столбцам.
4. Запоминаем в массивы все перестановки порядка 7 и 4.
5. Далее заполняем таблицу построчно, пользуясь следующим соображением, которое существенно ускоряет перебор. Элементы 0, 1, 2 в $i$-й строке не могут находиться на позициях, которые определяются значениями первых трёх элементов $i$-го столбца. Это следует из того, что в $i$-й строке ($i \geqslant 4$) $G'^{\,\mathrm{op}}$ в первых трёх столбцах не могут встречаться 0, 1, 2. Конечно, 0, 1, 2 нельзя ставить и на первые три позиции $i$-й строки в $G$. Поэтому для распределения 0, 1, 2 остаются только четыре свободные позиции. Для этого нам понадобится массив перестановок порядка 4. Далее заполняем оставшиеся позиции с помощью массива перестановок порядка 7 и запускаем проверку по столбцам.

6. После заполнения очередной $i$-й строки производим следующую принципиальную проверку. Заметим, что, зная первые $i$ строк $G$, можно заполнить левый верхний квадрат размера $i \times i$ в $G'^{\mathrm{op}}$. Поэтому параллельно с $G$ заполняем $G'^{\mathrm{op}}$ и проводим проверку по столбцам, так как строки $G'^{\mathrm{op}}$ всегда являются перестановками.

Ниже приведены полученная квазигруппа и её рекурсивная производная:

$$
\begin{array}{ccccccccccc}
0 & 1 & 2 & 4 & 3 & 6 & 5 & 8 & 7 & 10 & 9 \\
1 & 2 & 0 & 5 & 6 & 3 & 4 & 9 & 10 & 7 & 8 \\
2 & 0 & 1 & 6 & 5 & 4 & 3 & 10 & 9 & 8 & 7 \\
5 & 6 & 7 & 3 & 9 & 8 & 10 & 4 & 0 & 2 & 1 \\
6 & 5 & 8 & 10 & 4 & 9 & 7 & 0 & 3 & 1 & 2 \\
4 & 10 & 3 & 9 & 7 & 5 & 8 & 1 & 2 & 0 & 6 \\
3 & 9 & 4 & 8 & 10 & 7 & 6 & 2 & 1 & 5 & 0 \\
10 & 4 & 9 & 0 & 8 & 1 & 2 & 7 & 5 & 6 & 3 \\
9 & 3 & 10 & 7 & 0 & 2 & 1 & 6 & 8 & 4 & 5 \\
7 & 8 & 5 & 2 & 1 & 10 & 0 & 3 & 6 & 9 & 4 \\
8 & 7 & 6 & 1 & 2 & 0 & 9 & 5 & 4 & 3 & 10
\end{array},
$$

$$
\begin{array}{ccccccccccc}
0 & 2 & 1 & 9 & 10 & 8 & 7 & 5 & 6 & 4 & 3 \\
1 & 0 & 2 & 8 & 7 & 9 & 10 & 6 & 5 & 3 & 4 \\
2 & 1 & 0 & 10 & 9 & 7 & 8 & 3 & 4 & 6 & 5 \\
6 & 4 & 10 & 3 & 1 & 2 & 0 & 8 & 9 & 5 & 7 \\
5 & 3 & 9 & 1 & 4 & 0 & 2 & 10 & 7 & 8 & 6 \\
3 & 8 & 6 & 2 & 0 & 5 & 1 & 4 & 10 & 7 & 9 \\
4 & 7 & 5 & 0 & 2 & 1 & 6 & 9 & 3 & 10 & 8 \\
9 & 6 & 8 & 5 & 3 & 10 & 4 & 7 & 2 & 0 & 1 \\
10 & 5 & 7 & 4 & 6 & 3 & 9 & 2 & 8 & 1 & 0 \\
8 & 10 & 4 & 7 & 5 & 6 & 3 & 0 & 1 & 9 & 2 \\
7 & 9 & 3 & 6 & 8 & 4 & 5 & 1 & 0 & 2 & 10
\end{array}.
$$

## 6. Рекурсивно дифференцируемая квазигруппа порядка 42

Пользуясь теоремой 2.4 и вспомогательными результатами разделов 4 и 5, получаем рекурсивно дифференцируемую квазигруппу порядка 42. Ниже приводятся таблицы Кэли построенной квазигруппы и её рекурсивной производной. Элементы алфавита $\Omega$ представлены цифрами 0—9 и буквами a—z, A—F.

Рекурсивно дифференцируемая квазигруппа порядка 42:

0 1 2 7 9 4 6 8 3 5 b a d c f e h g j i l k n m p o r q t s v u x w z y B A D C F E
1 2 0 8 3 5 7 9 4 6 c d a b g h e f k l i j o p m n s t q r w x u v A B y z E F C D
2 0 1 3 5 7 9 4 6 8 d c b a h g f e l k j i p o n m t s r q x w v u B A z y F E D C
4 3 8 9 1 0 5 6 7 2 i j k l m n o p a b c d e f g h y C B F E A D z q x v s r w u t
8 7 5 4 2 6 1 0 9 3 j i l k n m p o b a d c f e h g D z E A B F y C w r t u x q s v
5 4 9 6 7 8 2 3 1 0 k l i j o p m n c d a b g h e f z D A E F B C y x q s v w r t u
9 8 6 1 0 3 4 5 2 7 l k j i p o n m d c b a h g f e C y F B A E z D r w u t q x v s
6 5 3 2 4 1 0 7 8 9 m n o p i j k l e f g h a b c d A E z D C y F B v s q x u t r w
3 9 7 5 6 2 8 1 0 4 n m p o j i l k f e h g b a d c F B C y z D A E t u w r s v x q
7 6 4 0 8 9 3 2 5 1 o p m n k l i j g h e f c d a b B F y C D z E A s v x q t u w r
c d e q r s t u v w a g f h b 0 2 1 y z A B C D E p 3 4 5 6 7 8 9 x i j k l m n o F
d c f s t q r w x u h b g e 0 a 1 2 A B y z E F o D 5 6 3 4 9 v 7 8 k l i j C p m n
b h a u v w x q r s g e c f 1 2 0 d C D E F y n A B 7 8 9 t 3 4 5 6 m z o p i j k l
a g b w x u v s t q f h e d 2 1 c 0 E F C D m B y z 9 r 7 8 5 6 3 4 o p A n k l i j
h b g t s r q x w v 0 f 1 2 e c d a B A z l F E D C 6 5 4 3 u 9 8 7 y k j i p o n m
g a h r q t s v u x e 0 2 1 d f b c z y k A D C F E 4 3 6 5 8 7 w 9 j i l B n m p o
e f c x w v u t s r 2 1 h 0 a d g b F j D C B A z y q 9 8 7 6 5 4 3 p o n m l k E i
f e d v u x w r q t 1 2 0 g c b a h i C F E z y B A 8 7 s 9 4 3 6 5 n m p o j D l k
k l m y A C E B z F q t w v x u r s D o n p j 0 2 1 a g h b f d c e 3 8 4 7 5 i 6 9
l k n B z F D y A C r s x u w v q t p E o m 0 i 1 2 g a b h d f e c 7 4 8 3 9 6 j 5
j p i E C A y D F z s r u x v w t q o m B n 1 2 0 l h b a g c e f d 6 9 5 k 4 7 3 8
i o j D F z B E C A t q v w u x s r n p m y 2 1 k 0 b h g a e c d f l 5 9 6 8 3 7 4
p j o F D B z C E y u x s r t q v w 0 n 1 2 A k l i f d c e a g h b 9 6 m 5 7 4 8 3
o i p C E y A F D B v w t q s r u x m 0 2 1 l z j k d f e c g a b h 5 n 6 9 3 8 4 7
m n k z B D F A y E w v q t r s x u 2 1 p 0 i l C j c e f d h b a g 8 3 7 4 o 5 9 6
n m l A y E C z B D x u r s q t w v 1 2 0 o k j i F e c d f b h g a 4 7 3 8 6 9 5 p
s t u i m l p o k n y z A B C D E F 3 q 8 5 4 9 7 6 j w v x r 0 2 1 a b c d e f g h
t s v n j o k l p i z y B A D C F E 9 4 6 7 r 3 5 8 x m w u 0 q 1 2 b a d c f e h g
r x q j n k o p l m A B y z E F C D s 3 5 8 9 4 6 7 w u i v 1 2 0 t c d a b g h e f
q w r m i p l k o j B A z y F E D C 4 9 7 6 3 t 8 5 v x u n 2 1 s 0 d c b a h g f e
x r w k o j n m i p C D E F y z A B 8 5 3 u 7 6 4 9 0 v 1 2 l s t q e f g h a b c d
w q x p l m i j n k D C F E z y B A 6 7 9 4 5 8 v 3 u 0 2 1 t o r s f e h g b a d c
u v s l p i m n j o E F C D A B y z 5 8 w 3 6 7 9 4 2 1 x 0 q t k r g h e f c d a b
v u t o k n j i m l F E D C B A z y 7 6 4 9 8 5 3 x 1 2 0 w s r q p h g f e d c b a
A B C a g h b f d c 3 6 9 8 1 7 4 5 q v r e s x t w i k m o y j p n u E D F z 0 2 1
B A D g a b h d f e 4 5 n 7 9 8 3 6 u r v q w c x s l j p z i k m o F t E C 0 y 1 2
z F y h b a g c e f 5 4 7 m 8 9 6 3 t w s x d u q v o A k i n p j l E C r D 1 2 0 B
y E z b h g a e c d 6 3 8 9 7 k 5 4 x s f t v q u r n p j l o m B i D F C w 2 1 A 0
F z E f d c e a g h 7 o 5 4 6 3 8 9 w t x s u r b q p n l j m C i k 0 D 1 2 v A B y
E y F d f e c g a b 8 9 6 3 5 4 7 i h x t w q v r u m o D k p n l j C 0 2 1 B s z A
C D A c e f d h b a 9 8 3 6 4 5 j 7 v g u r x s w t E l n p k i o m 2 1 F 0 y B q z
D C B e c d f b h g p 7 4 5 3 6 9 8 r u q v t w s a k i o m j l n F 1 2 0 E A z y x.

Рекурсивная производная приведённой выше квазигруппы:

0 2 1 6 3 7 4 8 5 9 g h f e c d b a o p n m k l j i w x v u s t r q E F D C A B z y
1 0 2 7 4 8 5 9 6 3 f e g h d c a b n m o p l k i j v u w x t s q r D C E F B A y z
2 1 0 9 6 3 7 4 8 5 h g e f a b d c p o m n i j l k x w u v q r t s F E C D y z B A
9 8 6 2 7 5 3 0 1 4 y B E D F C z A q s u w t r x v a f b e c h d g i o p j n l k m
3 9 7 1 5 2 8 6 4 0 z A F C E D y B t r x v q s u w f a e b h c g d p j i o k m n l
4 3 8 5 0 1 6 2 9 7 A z C F D E B y w u s q v x r t b e a f d g c h n l k m i o p j
5 4 9 3 8 6 0 1 7 2 B y D E C F A z v x r t w u s q e b f a g d h c k m n l p j i o
6 5 3 8 2 4 9 7 0 1 C F A z B y D E x v t r u w q s c h d g a f b e j p o i m k l n
7 6 4 0 1 9 2 5 3 8 D E B y A z C F u w q s x v t r h c g d f a e b o i j p l n m k
8 7 5 4 9 0 1 3 2 6 E D y B z A F C r t v x s q w u d g c h b e a f m k l n j p o i
d b h y z A B C D E a 1 2 0 f g c e 3 4 5 6 7 8 9 F i j k l m n o p q r s t u v w x
c a g B A z y F E D 1 b 0 2 h e f d 4 3 6 5 8 7 C 9 l k j i p o n m r q t s v u x w
a f d E F C D A B y 2 0 c 1 b h e g 5 6 3 4 9 z 7 8 o p m n k l i j s t q r w x u v
b e c D C F E z y B 0 2 1 d g a h f 6 5 4 3 A 9 8 7 n m p o j i l k t s r q x w v u
g d f F E D C B A z c a h b e 2 0 1 7 8 9 y 3 4 5 6 p o n m l k j i u v w x q r s t
h c e C D E F y z A b d a g 2 f 1 0 8 7 B 9 4 3 6 5 m n o p i j k l v u x w r q t s
f h b z y B A D C F e c d a 0 1 g 2 9 E 7 8 5 6 3 4 j i l k n m p o w x u v s t q r
e g a A B y z E F C d f b c 1 0 2 h D 9 8 7 6 5 4 3 k l i j o p m n x w v u t s r q
l j p q t w v x u r 3 4 5 6 7 8 9 s i 1 2 0 n o k m y F D A z E C B a f b e c h d g
k i o s r u x v w t 4 3 6 5 8 7 q 9 1 j 0 2 p m n l E z B C F y A D f a e b h c g d
i n l u x s r t q v 5 6 3 4 9 w 7 8 2 0 k 1 j p m o F y A D E z B C b e a f d g c h
j m k w v q t r s x 6 5 4 3 u 9 8 7 0 2 1 l o i p n z E C B y F D A e b f a g d h c
o l n t q v w u x s 7 8 9 r 3 4 5 6 k i p j m 2 0 1 D A y F C B z E c h d g a f b e
p k m r s x u w v q 8 7 t 9 4 3 6 5 j l i o 2 n 1 0 B C E z A D F y h c g d f a e b
n p j x u r s q t w 9 v 7 8 5 6 3 4 m k l i 0 1 o 2 A D F y B C E z d g c h b e a f
m o i v w t q s r u x 9 8 7 6 5 4 3 l n j k 1 0 2 p C B z E D A y F g d h c e b f a
t r x a f b e c h d i l o n p m E k y g F z D B A C q 1 2 0 v w s u 3 5 7 9 6 4 j 8
s q w f a e b h c g j k p A o n i l F z y E d C D B 1 r 0 2 x u v t 6 4 m 8 3 5 7 9
q v t b e a f d g c k j m p n o l D h B A C y E F z 2 0 s 1 r x u w 9 7 5 3 8 i 4 6
r u s e b f a g d h l i z o m p k j A C D B F c y E 0 2 1 t w q x v 8 n 4 6 9 7 5 3
w t v c h d g a f b m p k j y i n o z F E e C A B D s q x r u 2 0 1 l 8 6 4 7 9 3 5
x s u h c g d f a e n C l i k j m p E y z F B D b A r t q w 2 v 1 0 7 9 3 5 o 8 6 4
v x r d g c h b e a o n i l j B p m C A f D z F E y u s t q 0 1 w 2 4 6 8 k 5 3 9 7
u w q g d h c e b f F m j k i l o n B D C A E y z a t v r s 1 0 2 x 5 3 9 7 4 6 8 p
B z F i p n k j o m q r s t l v w x a f b u c h d g 3 6 9 8 e 7 4 5 y 1 2 0 D E A C
A y E o j l m p i k r q n s v u x w f a e b h t g d 5 4 7 c 8 9 6 3 1 z 0 2 F C D B
y D B p i k n o j l s t q m w x u v b e a f r g c h 7 d 5 4 6 3 8 9 2 0 A 1 z F C E
z C A j o m l i p n t s r q x k v u e b w a g d h c 9 8 3 6 4 5 f 7 0 2 1 B E y F D
E B D n k i p m l j u o w x q r s t c h d g a f v e 6 3 8 9 7 b 5 4 A y F z C 2 0 1
F A C l m o j k n p v u x w r q t i s c g d f a e b 4 5 h 7 9 8 3 6 z B y E 2 D 1 0
D F z k n p i l m o w x u v s t j r d q c h b e a f g 7 4 5 3 6 9 8 C A B y 0 1 E 2
C E y m l j o n k i p w v u t s r q g d h c e b f x 8 9 6 3 5 4 7 a B D z A 1 0 2 F.

## Литература

[1] Гонсалес С., Коусело Е., Марков В., Нечаев А. Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы // Дискрет. мат. — 1998. — Т. 10, № 2. — С. 3—29.

[2] Гонсалес С., Коусело Е., Марков В., Нечаев А. Параметры рекурсивных МДР-кодов // Дискрет. мат. — 2000. — Т. 12, № 4. — С. 3—24.

[3] МакВильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. — М.: Связь, 1979.

[4] Холл М. Комбинаторика. — М.: Мир, 1970.

[5] Tarry G. Le problème de 36 officiers. 1, 2 // C. R. Assoc. Fr. Av. Sci. — 1900. — P. 122—123; 1901. — P. 170—203.