Math-Net.Ru

Общероссийский математический портал

С. Гонсалес, Е. Коусело, В. Т. Марков, А. А. Нечаев,
Рекурсивные МДР-коды и рекурсивно дифференцируе-
мые квазигруппы, *Дискрет. матем.*, 1998, том 10, вы-
пуск 2, 3–29

DOI: <https://doi.org/10.4213/dm424>

Использование Общероссийского математического портала Math-Net.Ru под-
разумевает, что вы прочитали и согласны с пользовательским соглашением
<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.172.240.79

26 апреля 2023 г., 11:39:29

УДК 519.7

Рекурсивные МДР-коды и рекурсивно дифференцируемые квазигруппы

© 1998 г. С.Гонсалес, Е.Косусело, В.Т.Марков, А.А.Нечаев

Код длины n в алфавите из $q \geq 2$ элементов называется полным k -рекурсивным, если он состоит из всех отрезков длины n рекуррентных последовательностей, удовлетворяющих некоторому фиксированному (не обязательно линейному) закону рекурсии $f(x_1, \dots, x_k)$ порядка $k \leq n$. Пусть $n^r(k, q)$ — максимальное n , для которого существует такой код с расстоянием $n - k + 1$ (МДР-код). Условие $n^r(k, q) \geq n$ означает, что функция f вместе со своими $n - k - 1$ последовательными рекурсивными производными составляет ортогональную систему k -квазигрупп.

Доказано, что если $q \notin \{2, 6, 14, 18, 26, 42\}$, то $n^r(2, q) \geq 4$. Доказательство сводится к построению специальных пар ортогональных латинских квадратов.

1. Введение

Пусть $\Omega = \{a_1, \dots, a_q\}$ — произвольное конечное множество. Любое подмножество $\mathcal{X} \subseteq \Omega^n$ называется кодом длины n , или n -кодом в алфавите Ω , код называется $[n, k]_\Omega$ -кодом, если $|\mathcal{X}| = q^k$ (здесь, вообще говоря, $k \in \mathbf{R}$). Мы назовем k комбинаторной размерностью кода $\mathcal{X}$. Расстояние (Хемминга) $d(\mathbf{u}, \mathbf{v})$ между двумя словами $\mathbf{u}, \mathbf{v} \in \Omega^n$ определяется стандартно как число неравных координат в $\mathbf{u}$ и $\mathbf{v}$ с одинаковыми номерами. Расстояние $d(\mathcal{X})$ кода $\mathcal{X}$ есть минимум расстояний между его различными словами. Будем говорить, что $[n, k]_\Omega$ -код $\mathcal{X}$ есть $[n, k, d]_\Omega$ -код, если $d(\mathcal{X}) = d$.

Напомним, что всегда $d \leq n - k + 1$ (граница Синглтона [5]), и если $d = n - k + 1$, то код $\mathcal{X}$ называется МДР-кодом (при этом, естественно, k — целое число). Среди проблем теории кодов, исправляющих ошибки, мы выделим следующие две: найти (или, по крайней мере, оценить) максимум $n(k, q)$ длин k -мерных МДР-кодов в алфавите Ω мощности q и максимум $A_q(n, d)$ мощностей n -кодов над Ω с расстоянием не меньшим, чем d (см. [5]). Заметим, что условие $n(k, q) \geq n$ эквивалентно условию $A_q(n, n - k + 1) = q^k$.

Мы изучаем эти параметры только для следующего специального класса кодов. Назовем код $\mathcal{X}$ полным k -рекурсивным кодом, если существует функция $f: \Omega^k \rightarrow \Omega$, $k \leq n$, такая, что $\mathcal{X}$ есть множество всех слов $u(0, \dots, n-1) = (u(0), \dots, u(n-1))$, удовлетворяющих условию

$$u(i+k) = f(u(i), \dots, u(i+k-1)), \quad i = 0, \dots, n-k,$$

где $u(0), \dots, u(k-1)$ — произвольные элементы из Ω . Далее такой код обозначается через $\mathcal{K}(n, f)$.

Заметим, что любой систематический $[n, k]_\Omega$ -код с определяющими позициями $0, \dots, k-1$ (см. параграф 1) можно описать с помощью подходящей системы функций

$$f_i: \Omega^k \rightarrow \Omega, \quad i = 0, \dots, n-k-1,$$

как множество всех слов

$$(u_0, \dots, u_{k-1}, f_0(u_0, \dots, u_{k-1}), \dots, f_{n-k-1}(u_0, \dots, u_{k-1})).$$

Для кода $\mathcal{K}(n, f)$ эта система функций имеет вид

$$f_0 = f_0(x_0, \dots, x_{k-1}) = f(x_0, \dots, x_{k-1}),$$

$$f_1 = f_1(x_0, \dots, x_{k-1}) = f(x_1, \dots, x_{k-1}, f_0(x_0, \dots, x_{k-1})),$$

...

$$f_{k-1} = f_{k-1}(x_0, \dots, x_{k-1}) = f(x_{k-1}, f_0, \dots, f_{k-2}),$$

$$f_{i+k} = f_{i+k}(x_0, \dots, x_{k-1}) = f(f_i, \dots, f_{i+k-1}), \quad i \geq 0.$$

Любой подкод полного k -рекурсивного кода $\mathcal{K}$ назовем k -рекурсивным.

Введем следующие параметры: пусть $n^r(k, q)$ — максимальное n такое, что существует полный k -рекурсивный МДР-код длины n ; $A_q^{k\text{-rec}}(n, d)$ — максимум мощностей k -рекурсивных кодов над Ω длины n с расстоянием, не меньшим, чем d .

Интересно оценить эти параметры для различных значений q, k, n, d и сравнить их соответственно с параметрами $n(k, q)$ и $A_q(n, d)$. Очевидно,

$$n^r(k, q) \leq n(k, q),$$

$$A_q^{k\text{-rec}}(n, d) \leq A_q(n, d).$$

Главный вопрос: когда эти неравенства являются строгими, и когда они обращаются в равенства?

Наши основные результаты в этом направлении связаны со случаем $k = 2$. Общий случай будет рассмотрен в другой статье, которую предполагается опубликовать позднее. Доказано, что если $q \geq 3$ есть примарное число, то

$$n^r(2, q) = n(2, q) = q + 1; \quad (1.1)$$

если $q \geq 3$ и $q \notin \{14, 18, 26, 42\}$, то

$$A_q^{2\text{-rec}}(4, 3) = A_q(4, 3). \quad (1.2)$$

Последнее равенство означает, что при сделанных выше предположениях

$$A_6^{2\text{-rec}}(4, 3) = A_6(4, 3) = 34 \quad (1.3)$$

(см. [13]), и если $q \neq 6$, то

$$A_q^{2\text{-rec}}(4, 3) = A_q(4, 3) = q^2. \quad (1.4)$$

Вопрос о том, выполняется ли (1.2) для $q = 14, 18, 26, 42$, остается открытым.

Некоторые доказательства в параграфах 4 и 5 основаны на вычислениях с помощью компьютера. В основном эти результаты допускают непосредственную прямую проверку за разумное время, однако, один из них (следствие 8) такой проверке, видимо, не поддается.

2. Предварительные сведения. Квазигруппы и латинские квадраты

Напомним некоторые понятия и результаты теории кодов. Для данных натуральных n и $k \in \{1, \dots, n\}$ код $\mathcal{K} \subset \Omega^n$ называется систематическим с определяющими позициями $i_1 < \dots < i_k$, если для любых $c_1, \dots, c_k \in \Omega$ существует единственное слово $\mathbf{u} = (u(1), \dots, u(n)) \in \mathcal{K}$ такое, что $u(i_1, \dots, i_k) = (c_1, \dots, c_k)$, то есть $u(i_1) = c_1, \dots, u(i_k) = c_k$.

Предложение 1 ([5]). *Произвольный $[n, k]$ -код $\mathcal{K}$ есть МДР-код, если и только если это — систематический код и любые k его позиций являются определяющими.*

Пусть $\mathcal{K} \subseteq \Omega^n$ есть систематический $[n, k]$ -код с определяющими позициями $1, \dots, k$. Тогда, как было отмечено выше, существует система функций $f_s: \Omega^k \rightarrow \Omega$, $s = 1, \dots, n - k$, такая, что

$$\mathcal{K} = \{\mathbf{u} = (u(1, \dots, k), f_1(u(1, \dots, k)), \dots, f_{n-k}(u(1, \dots, k))) : u(1, \dots, k) \in \Omega^k\}. \quad (2.1)$$

Будем обозначать такой код через $\mathcal{K}(n \mid f_1, \dots, f_{n-k})$, при этом функции $f_1, \dots, f_{n-k}$ будем называть проверочными функциями кода $\mathcal{K}$.

Пусть $\mathcal{K} \subset \Omega^n$ и $\mathcal{L} \subset \Delta^n$ — два кода одинаковой длины (в разных алфавитах). Определим декартово произведение $\mathcal{K} \times \mathcal{L}$ этих кодов, полагая

$$\mathcal{K} \times \mathcal{L} = \{((u(1), v(1)), \dots, (u(n), v(n))) : u(1, \dots, n) \in \mathcal{K}, v(1, \dots, n) \in \mathcal{L}\}. \quad (2.2)$$

Заметим, что любому кодовому слову из $\mathcal{K} \times \mathcal{L}$ естественным образом сопоставляется единственная пара кодовых слов $\mathbf{u}$ и $\mathbf{v}$ из $\mathcal{K}$ и $\mathcal{L}$ соответственно.

Непосредственно из определений вытекает следующее утверждение.

Предложение 2. *Пусть*

$$\mathcal{K} = \mathcal{K}(n \mid f_1, \dots, f_{n-k}) \subset \Omega^n, \quad \mathcal{L} = \mathcal{L}(n \mid g_1, \dots, g_{n-k}) \subset \Delta^n$$

суть два систематических кода одинаковой длины с одним и тем же множеством определяющих позиций $1, \dots, k$, тогда

$$\mathcal{K} \times \mathcal{L} = \mathcal{K}(n \mid h_1, \dots, h_{n-k}),$$

где

$$h_s((u(1), v(1)), \dots, (u(k), v(k))) = (f_s(u(1, \dots, k)), g_s(v(1, \dots, k))), \quad s = 1, \dots, n - k.$$

Более того, справедлива следующая теорема.

Теорема 1. *Пусть $\mathcal{K} \subset \Omega^n$ и $\mathcal{L} \subset \Delta^n$. Тогда $\mathcal{K} \times \mathcal{L}$ есть систематический код с определяющими позициями $1, \dots, k$ тогда и только тогда, когда таков каждый из кодов $\mathcal{K}$ и $\mathcal{L}$.*

Доказательство. Достаточность сформулированных условий есть предложение 2. Допустим теперь, что код $\mathcal{K} \times \mathcal{L}$ обладает нужными свойствами. Тогда для любых $c_1, \dots, c_k \in \Omega$ и любых $d_1, \dots, d_k \in \Delta$ существует единственное слово $\mathbf{w} \in \mathcal{K} \times \mathcal{L}$ такое, что

$$w(1, \dots, k) = ((c_1, d_1), \dots, (c_k, d_k)).$$

Существует единственная пара слов $\mathbf{u} \in \mathcal{K}$ и $\mathbf{v} \in \mathcal{L}$, удовлетворяющая равенству

$$\mathbf{w} = ((u(1), v(1)), \dots, (u(n), v(n))),$$

это и есть искомая единственная пара слов со свойствами

$$u(1, \dots, k) = (c_1, \dots, c_k), \quad v(1, \dots, k) = (d_1, \dots, d_k).$$

Предложение 2 и теорема 1 дают следующее утверждение.

Следствие 1. *Декартово произведение $\mathcal{K} \times \mathcal{L}$ кодов $\mathcal{K}$ и $\mathcal{L}$ есть МДР-код, если и только если коды $\mathcal{K}$ и $\mathcal{L}$ суть МДР-коды одинаковой комбинаторной размерности.*

Будем называть пару (Ω, f) , состоящую из множества Ω и функции $f: \Omega^k \rightarrow \Omega$, а иногда и саму функцию f (когда Ω известно или несущественно) k -квазигруппой, если для любых $i \in \{1, \dots, k\}$ и $b_1, \dots, b_k \in \Omega$ уравнение

$$f(b_1, \dots, b_{i-1}, x, b_{i+1}, \dots, b_k) = b_i$$

имеет единственное решение в Ω [18, 2]. В частности, если $k = 2$, пара $(\Omega, f(x, y))$, $\Omega = \{a_1, \dots, a_q\}$, есть 2-квазигруппа, или просто квазигруппа, тогда и только тогда, когда ее таблица Кэли, то есть $q \times q$ матрица $\|f(a_i, a_j)\|$, есть латинский квадрат, то есть каждая строка и каждый столбец этой таблицы есть перестановка элементов множества Ω [1, 10].

Справедлив следующий очевидный критерий.

Предложение 3. *Функция $f: \Omega^k \rightarrow \Omega$ есть k -квазигруппа тогда и только тогда, когда $[k+1, k]$ -код $\mathcal{K}(k+1, f)$ есть МДР-код.*

Из предложений 1, 3 легко выводится следующее утверждение.

Предложение 4. *Если (2.1) есть МДР-код, то каждая из функций $f_i, i = 1, \dots, n-k$, есть k -квазигруппа.*

Обращение последнего утверждения в общем случае неверно (см. ниже пример 1).

Будем говорить, что система функций

$$f_t: \Omega^k \rightarrow \Omega, \quad t = 1, \dots, r, \quad (2.3)$$

есть ортогональная система k -квазигрупп, если значения любых k функций из множества

$$x_1, \dots, x_k, f_1(x_1, \dots, x_k), \dots, f_r(x_1, \dots, x_k) \quad (2.4)$$

однозначно определяют значения всех остальных функций этого множества. Более формально это означает, что для любых $b_1, \dots, b_k \in \Omega$, $s = 0, \dots, k$ и любых чисел

$$1 \leq i_1 < \dots < i_s \leq k, \quad 1 \leq j_1 < \dots < j_{k-s} \leq r,$$

система уравнений

$$\begin{aligned}
 x_{i_1} &= b_1, \\
 &\dots \\
 x_{i_s} &= b_s, \\
 f_{j_1}(\mathbf{x}) &= b_{s+1}, \\
 &\dots \\
 f_{j_{k-s}}(\mathbf{x}) &= b_k
 \end{aligned} \tag{2.5}$$

имеет единственное решение в Ω^k . В частности, при $s = k - 1$ разрешимость системы (2.5) означает, что (Ω, f_{j_1}) есть k -квазигруппа. Здесь уместно заметить, что это определение, по сути дела, эквивалентно определению ортогонального массива индекса 1 (см. [9, 10]). Теперь предложение 1 можно сформулировать в виде следующего утверждения.

Предложение 5. Код (2.1) есть МДР-код тогда и только тогда, когда $f_1, \dots, f_{n-k}$ есть ортогональная система k -квазигрупп.

Непосредственно из определений получаем следующее утверждение.

Предложение 6. Система из $r \geq k$ функций (2.3) есть ортогональная система квазигрупп тогда и только тогда, когда любая ее подсистема из k функций обладает этим свойством.

Для случая $k = 2$ рассматриваемое определение превращается в хорошо известное определение системы попарно ортогональных латинских квадратов (сокращенно СОЛК): $f_1(x_1, x_2), \dots, f_r(x_1, x_2)$ суть квазигруппы и для любых $b_1, b_2 \in \Omega$, $1 \leq j_1 < j_2 \leq r$ система из двух уравнений

$$\begin{aligned}
 f_{j_1}(x_1, x_2) &= b_1, \\
 f_{j_2}(x_1, x_2) &= b_2
 \end{aligned}$$

имеет единственное решение в Ω^2 [10]. Таким образом, мы имеем следующий хорошо известный результат, который можно рассматривать как следствие формально более общего предложения 5.

Предложение 7. Для заданной системы функций

$$f_1(x_1, x_2), \dots, f_{n-2}(x_1, x_2): \Omega^2 \rightarrow \Omega \tag{2.6}$$

$[n, 2]$ -код $\mathcal{K}(n \mid f_1, \dots, f_{n-2})$ есть МДР-код тогда и только тогда, когда (2.6) есть СОЛК (система ортогональных квазигрупп).

Пусть $N(k, q)$ — максимально возможная мощность ортогональной системы k -квазигрупп на множестве Ω из q элементов. Тогда параметр $n(k, q)$ из введения можно записать как $n(k, q) = N(k, q) + k$. Известны следующие значения и оценки этого параметра.

Теорема 2 ([9, 5, 12]). Если $q \leq k$, то $n(k, q) = k + 1$.

Если $k \leq q$ и q четно, то $n(k, q) \leq q + k - 1$.

Если $3 \leq k \leq q$ и q нечетно, то $n(k, q) \leq q + k - 2$.

Если $k < q$ и q — примарное число (то есть степень простого), то $n(k, q) \geq q + 1$.

Если q — примарное нечетное число, то $n(3, q) = q + 1$.

Если $m \geq 2$, то $n(3, 2^m) = n(2^m - 1, 2^m) = 2^m + 2$.

Следующее замечание позволяет использовать эти результаты для получения нижних оценок в случае не примарного алфавита (см. следствие 1).

Предложение 8. Справедливо неравенство

$$n(k, q_1 q_2) \geq \min\{n(k, q_1), n(k, q_2)\}.$$

Для случая $k = 2$

$$n(2, q) = 2 + N(q),$$

где $N(q)$ есть максимальное число попарно ортогональных латинских $q \times q$ квадратов. Подробный обзор результатов о $N(q)$ приведен в [10, 11, 12]. Мы приведем здесь только следующую общую сводку результатов.

Теорема 3. Пусть $q \in \mathbb{N}$, $q > 1$. Тогда

$N(q) \geq 2$, если и только если $q \notin \{2, 6\}$,

$N(q) \leq q - 1$,

если q примарно, то $N(q) = q - 1$,

$N(q_1 q_2) \geq \min\{N(q_1), N(q_2)\}$, в частности, если $q = q_1 \dots q_t$ есть каноническое разложение q , то $N(q) \geq \min\{q_1 - 1, \dots, q_t - 1\}$,

$N(q) \geq q^{10/143} - 2$,

$N(q) \geq 3$, если $q \notin \{2, 3, 6, 10\}$.

Вернемся к рекурсивным кодам. Для заданной функции $f: \Omega^k \rightarrow \Omega$ полный рекурсивный код $\mathcal{K}(n, f)$ был определен как код $\mathcal{K}(n \mid f^{(0)}, f^{(1)}, \dots, f^{(n-k-1)})$ вида (2.1) со следующими проверочными функциями:

$$f^{(0)}(\mathbf{x}) = f(\mathbf{x}),$$

$$f^{(1)}(\mathbf{x}) = f(x_2, \dots, x_k, f(\mathbf{x})),$$

...

$$f^{(t)}(\mathbf{x}) = f(x_{t+1}, \dots, x_k, f(\mathbf{x}), f^{(1)}(\mathbf{x}), \dots, f^{(t-1)}(\mathbf{x})), \quad t < k, \quad (2.7)$$

...

$$f^{(t)}(\mathbf{x}) = f(f^{(t-k)}(\mathbf{x}), \dots, f^{(t-1)}(\mathbf{x})), \quad t \geq k.$$

Будем называть функцию $f^{(t)}(\mathbf{x})$ из (2.7) t -й рекурсивной производной функции $f(\mathbf{x})$. Таким образом, ввиду предложения 4 справедливо следующее утверждение.

Следствие 2. Произвольный k -рекурсивный код $\mathcal{K}(n, f)$ в алфавите Ω есть МДР-код тогда и только тогда, когда система

$$f(\mathbf{x}), f^{(1)}(\mathbf{x}), \dots, f^{(n-k-1)}(\mathbf{x}),$$

состоящая из последовательных производных функции f , есть ортогональная система k -квазигрупп.

Допустим теперь, что, наряду с $f: \Omega^k \rightarrow \Omega$, задана также функция $g: \Delta^k \rightarrow \Delta$, где Δ есть некоторое другое конечное множество. Тогда мы можем определить декартово произведение k -квазигрупп (Ω, f) и (Δ, g) обычным способом: k -арная операция h на $\Omega \times \Delta$ задаётся равенством

$$h(w_1, \dots, w_k) = (f(u_1, \dots, u_k), g(v_1, \dots, v_k)),$$

где $w_i = (u_i, v_i)$, $u_i \in \Omega$, $v_i \in \Delta$, $i = 1, \dots, k$. Мы будем писать также $h = f \times g$. Непосредственно из определения следует, что

$$\begin{aligned} h^{(1)}(w_1, \dots, w_k) &= h(w_2, \dots, w_k, h(w_1, \dots, w_k)) \\ &= (f(u_2, \dots, u_k, f(u_1, \dots, u_k)), g(v_2, \dots, v_k, g(v_1, \dots, v_k))), \end{aligned}$$

то есть $h^{(1)} = f^{(1)} \times g^{(1)}$, и вообще,

$$h^{(t)} = f^{(t)} \times g^{(t)}, \quad t \in \mathbb{N}. \quad (2.8)$$

Теперь из определения декартова произведения кодов вытекает следующее утверждение.

Предложение 9. При введенных обозначениях

$$\mathcal{K}(n, f \times g) = \mathcal{K}(nf) \times \mathcal{K}(n, g)$$

для всех $n \in \mathbb{N}$.

Вместе со следствием 1 это приводит к следующему утверждению.

Следствие 3. Для любых $k, q_1, q_2 \in \mathbb{N}$ справедливо неравенство

$$n^r(k, q_1 q_2) \geq \min\{n^r(k, q_1), n^r(k, q_2)\}.$$

Лемма 1. Пусть задана функция $f: \Omega^k \rightarrow \Omega$. Тогда для любого $n \in \mathbb{N}$ и любого $\mathbf{u} = (u_1, \dots, u_n) \in \mathcal{K}(n, f)$ слова $(u_1, \dots, u_{n-1})$ и $(u_2, \dots, u_n)$ принадлежат коду $\mathcal{K}(n-1, f)$.

Для доказательства достаточно заметить, что включение $\mathbf{u} \in \mathcal{K}(n, f)$ эквивалентно системе соотношений

$$u_{i+k} = f(u_i, \dots, u_{i+k-1}), \quad i = 1, \dots, n-k.$$

Ввиду следствия 2 целесообразно ввести некоторые дополнительные определения. Для $t \in \mathbb{N}_0$ назовем k -квазигруппу $f: \Omega^k \rightarrow \Omega$ рекурсивно t -дифференцируемой (t -стабильной), если ее рекурсивные производные $f = f^{(0)}, \dots, f^{(t)}$ суть k -квазигруппы (если система рекурсивных производных (2.7) ортогональна, т.е. $\mathcal{K}(k+t+1, f)$ есть МДР-код).

Очевидно, любая k -квазигруппа 0-стабильна и 0-дифференцируема (предложение 3). Согласно следствию 2, любая t -стабильная квазигруппа рекурсивно t -дифференцируема. Если $k = 2$, то справедливо также и обратное утверждение.

Теорема 4. Квазигруппа $f: \Omega^2 \rightarrow \Omega$ рекурсивно t -дифференцируема, $t \in \mathbb{N}_0$, если и только если код $\mathcal{K}(t+3, f)$ есть МДР-код, то есть f есть t -стабильная квазигруппа.

Доказательство. Достаточно доказать, что если f рекурсивно t -дифференцируема, то она t -стабильна. Для $t = 0$ это следует из предложения 3. Проведем доказательство индукцией по t . Пусть утверждение справедливо для любого $t < m$, $m > 0$. Допустим, что $t = m$ и рассмотрим два разных кодовых слова:

$$\mathbf{u} = (u_1, \dots, u_{m+3}), \quad \mathbf{v} = (v_1, \dots, v_{m+3}).$$

По определению двумерного МДР-кода расстояние между ними должно удовлетворять неравенству

$$d(\mathbf{u}, \mathbf{v}) \geq (m+3) - 2 + 1 = m+2.$$

Допустим, что

$$d(\mathbf{u}, \mathbf{v}) \leq m+1. \quad (2.9)$$

Заметим, что $(u(1), u(2)) \neq (v(1), v(2))$, так как рассматриваемые слова различны. Тогда $u(1, \dots, m+2)$ и $v(1, \dots, m+2)$ суть различные слова кода $\mathcal{K}(m+2, f)$, который по предположению индукции есть МДР-код. Следовательно,

$$d(u(1, \dots, m+2), v(1, \dots, m+2)) \geq m+1 > 1, \quad (2.10)$$

и если элементы $u(m+3)$ и $v(m+3)$ различны, мы имеем противоречие с (2.9). Таким образом, $u(m+3) = v(m+3)$. Рассмотрим слова $u(2, \dots, m+2)$, $v(2, \dots, m+2)$. Они различны ввиду (2.10). Тогда по лемме 1 слова $u(2, \dots, m+3)$, $v(2, \dots, m+3)$ принадлежат одному и тому же МДР-коду $\mathcal{K}(m+2, f)$, поэтому

$$d(u(2, \dots, m+3), v(2, \dots, m+3)) \geq m+1.$$

Теперь повторное использование (2.9) приводит к равенству $u(1) = v(1)$, и мы получаем два равенства

$$\begin{aligned} u(1) &= v(1), \\ f^{(m)}((u(1), u(2))) &= f^{(m)}(v(1), v(2)). \end{aligned}$$

Так как $f^{(m)}(x, y)$ есть квазигруппа, отсюда следует, что $u(2) = v(2)$, $\mathbf{u} = \mathbf{v}$. Полученное противоречие доказывает теорему.

В случае $k > 2$ из рекурсивной t -дифференцируемости k -квазигруппы не следует, что система (2.7) ее рекурсивных производных ортогональна. Прежде, чем построить соответствующий пример (пример 1), приведем следующее обобщение хорошо известного результата относительно линейных МДР-кодов над полями. Здесь мы используем некоторые алгебраические понятия, которые могут быть найдены, например, в [3].

Левый модуль M над кольцом R с единицей (вообще говоря, некоммутативным) называется точным, если из условий $r \in R$ и $rM = 0$ следует, что $r = 0$.

Теорема 5. Пусть ${}_R M$ есть конечный точный модуль над кольцом R с единицей e и $f_s: M^k \rightarrow M$, $s = 1, \dots, n-k$, суть линейные функции вида

$$f_s(x_1, \dots, x_k) = f_{s1}x_1 + \dots + f_{sk}x_k, \quad s = 1, \dots, n-k.$$

Тогда $\mathcal{K}(n \mid f_1, \dots, f_{n-k})$ есть МДР-код, если и только если в матрице

$$F = \begin{pmatrix} f_{11} & \dots & f_{1k} \\ & \dots & \\ f_{n-k,1} & \dots & f_{n-k,k} \end{pmatrix}$$

все квадратные подматрицы обратимы.

Для доказательства достаточно заметить, что любая система уравнений вида (2.5) должна иметь единственное решение.

Матрицу, описанную в условии теоремы 5, назовем критической матрицей кода $\mathcal{K}(n \mid f_1, \dots, f_{n-k})$.

Пример 1. Приведем пример 1-дифференцируемой, но не 1-стабильной 3-квазигруппы. Пусть $\Omega = Z_5$ и $f: Z_5^3 \rightarrow Z_5$ есть линейная функция

$$f(x_1, x_2, x_3) = x_1 + 3x_2 + 4x_3.$$

Тогда

$$f^{(1)}(x_1, x_2, x_3) = 4x_1 + 2x_2 + 4x_3$$

и $f, f^{(1)}$ суть 3-квазигруппы, но $\mathcal{K}(5, f)$ — не МДР-код: его транспонированная критическая матрица

$$\begin{pmatrix} 1 & 3 & 4 \\ 4 & 2 & 4 \end{pmatrix}$$

имеет нулевой минор

$$\begin{vmatrix} 1 & 3 \\ 4 & 2 \end{vmatrix} = 0.$$

3. Оценки для примарного алфавита и их следствия

Введем дополнительно следующие понятия и параметры. Назовем код $\mathcal{K} \subset \Omega^n$ линейным (в широком смысле), если существует бинарная операция $+$ на Ω такая, что $(\Omega, +)$ — абелева группа и $\mathcal{K}$ — подгруппа в $(\Omega^n, +)$: $\mathcal{K} < (\Omega^n, +)$. Заметим, что если P — конечное поле, то в соответствии с классическим определением код $\mathcal{K}$ над P называется линейным, если он есть P -подпространство в P^n . Мы будем называть такой код линейным в классическом (или в узком) смысле. Эти понятия совпадают, если $q = |\Omega|$ есть простое число, и только в этом случае.

Пусть $l(k, q)$ есть максимум длин линейных k -мерных МДР-кодов в алфавите из q элементов (для произвольного $q \in \mathbb{N}$), и пусть $m(k, q)$ есть аналогичный параметр для линейных кодов в классическом смысле (только для примарных q). По аналогии с $n^r(k, q)$ мы вводим также параметры $l^r(k, q)$ для произвольного q , и $m^r(k, q)$ только для примарного q .

Будем называть функцию $f: \Omega^n \rightarrow \Omega$ и соответствующий код $\mathcal{K}(n, f)$ идемпотентными, если выполняется тождество $f(x, \dots, x) = x$. Последнее эквивалентно тому, что код $\mathcal{K}(n, f)$ содержит все константы: $(a, \dots, a) \in \mathcal{K}(n, f)$ для всех $a \in \Omega$. В дополнение к предыдущим шести параметрам определим $n^{ir}(k, q)$ как максимум длин идемпотентных рекурсивных k -мерных МДР-кодов, и аналогичные параметры

$l^{ir}(k, q)$ и $m^{ir}(k, q)$, соответственно, в классах всех линейных кодов и кодов линейных в узком смысле.

Таким образом, мы имеем матрицу параметров

$$M(k, q) = \begin{pmatrix} [m^{ir}(k, q) & m^r(k, q) & m(k, q)] \\ l^{ir}(k, q) & l^r(k, q) & l(k, q) \\ n^{ir}(k, q) & n^r(k, q) & n(k, q) \end{pmatrix},$$

в которой числа не убывают по строкам слева направо, и по столбцам сверху вниз. Естественно, первая строка этой матрицы, заключенная в квадратные скобки, появляется лишь в случае примарного q . Интересно оценить и сравнить элементы $M(k, q)$ для различных значений k и q . В дальнейшем равенство типа $x^{yz}(k, q) = k$ означает, что соответствующей k -квазигруппы не существует.

Для почти тривиального случая $q = 2$

$$M(k, 2) = \begin{pmatrix} k+1 & k+1 & k+1 \\ k+1 & k+1 & k+1 \\ k+1 & k+1 & k+1 \end{pmatrix}, \quad \text{если } k \text{ нечетно};$$

$$M(k, 2) = \begin{pmatrix} k & k+1 & k+1 \\ k & k+1 & k+1 \\ k+1 & k+1 & k+1 \end{pmatrix}, \quad \text{если } k \text{ четно}.$$

Эти факты легко следуют, в частности, из равенства $n(2, 2) = 2$ и неравенства

$$x(k+1, q) \leq x(k, q) + 1, \quad (3.1)$$

где $x = n, l, m$, которое легко получается из предложения 5.

Ниже часто используется следующая базисная конструкция. Пусть $P = \text{GF}(q)$ и

$$g(x) = x^k - g_{k-1}x^{k-1} - \dots - q_1x - g_0$$

есть некоторый унитарный многочлен над P . Обозначим через $L_P(g)$ множество всех линейных рекуррентных последовательностей $u: \mathbb{N}_0 \rightarrow P$ с характеристическим многочленом $g(X)$, то есть последовательностей, удовлетворяющих условию

$$u(i+k) = g_0u(i) + \dots + g_{k-1}u(i+k-1), \quad i \geq 0.$$

Тогда для любого фиксированного $n \geq k$ множество

$$\mathcal{K} = L_P^{\{0, \dots, n-1\}}(g) \quad (3.2)$$

всех начальных отрезков $u(0, \dots, n-1) = (u(0), \dots, u(n-1))$ таких последовательностей есть линейный в классическом смысле k -рекурсивный код

$$\mathcal{K} = \mathcal{K}(n, f), \quad f(x_0, \dots, x_{k-1}) = g_0x_0 + \dots + g_{n-1}x_{n-1}. \quad (3.3)$$

Очевидно этот код является идемпотентным тогда и только тогда, когда единица e поля P есть корень $g(x)$.

Теорема 6. Если число q примарно, то $m^r(2, q) = n^r(2, q) = q + 1$.

Доказательство. Для четного q этот результат следует из [14]. Мы приведем здесь собственное краткое доказательство для произвольного q . Выберем неприводимый над полем P многочлен $g(x)$ степени $k = 2$ такой, что его корень в поле $\text{GF}(q^2)$ есть примитивный элемент последнего. Тогда для $n = q + 1$ код (3.2) есть МДР-код. Согласно [20], отрезок $u(0, \dots, q^2 - 2)$ любой последовательности $u \in L_P(g) \setminus 0$ содержит ровно $q - 1$ нулей (следствие теоремы 8) и имеет вид

$$u(0, \dots, q^2 - 2) = (u(0, \dots, q), au(0, \dots, q), \dots, a^{q-2}u(0, \dots, q)),$$

где a — примитивный элемент поля P (теорема 10). Следовательно, для $n = q + 1$ каждое ненулевое слово $u(0, \dots, n - 1)$ кода (3.2) содержит ровно одну нулевую координату, то есть расстояние кода равно $n - 1$.

Теперь, используя следствие 3, мы получаем следующее утверждение.

Следствие 4. Пусть $q = p_1^{r_1} \dots p_t^{r_t}$ есть каноническое разложение числа q , тогда

$$n^r(2, q) \geq \min\{p_1^{r_1} + 1, \dots, p_t^{r_t} + 1\}.$$

В частности, $n^r(2, q) \geq 4$ для всех $q \geq 3$, $q \not\equiv 2 \pmod{4}$. Как и для произвольных латинских квадратов, случай $q \equiv 2 \pmod{4}$ является наиболее трудным.

Для $q = 6$ (гипотеза Эйлера) известно, что $n(2, 6) = 3$ и $A_6(4, 3) = 34 < 36$ (см., например, [13]). С использованием компьютера доказана следующая теорема.

Теорема 7. Справедливы равенства

$$A_6^{2\text{-rec}}(4, 3) = A_6(4, 3) = 34.$$

Доказательство. Рассмотрим квазигруппу $(0, \dots, 5, f)$ порядка 6 со следующей таблицей Кэли:

1	0	4	5	3	2
0	1	2	3	4	5
5	4	3	1	2	0
4	5	1	2	0	3
2	3	0	4	5	1
3	2	5	0	1	4

Тогда таблица Кэли производной операции есть

0	0	2	3	4	5
1	1	3	2	5	4
2	4	1	5	0	3
3	5	4	1	2	0
4	3	5	0	1	2
5	2	0	4	3	1

Легко проверить, что последний квадрат не является латинским, однако он ортогонален исходному. Таким образом, мы имеем рекурсивный почти МДР-код $\mathcal{H}(4, f)$. Действительно, рекурсивный код $\mathcal{H}(4, f) \setminus \{(0, 0, 1, 0), (1, 1, 1, 1)\}$ есть код максимально возможной мощности 34 с расстоянием 3.

Остальные случаи, когда q не примарно, будут рассмотрены в разделах 4 и 5.

Здесь мы укажем две нижние границы параметра $m^{ir}(2, q)$ для примарных и простых q . Будем использовать коды вида (3.2).

Предложение 10. Если число q примарно и $q \geq 3$, то $m^{ir}(2, q) \geq q - 1$.

Доказательство. Выберем $n = q - 1$ и $g(x) = (x - e)(x - \alpha)$, где α — примитивный элемент поля P . Тогда $\mathcal{H}$ есть $[q - 1, 2, q - 2]_q$ -рекурсивный МДР-код Рида–Соломона [5]. Параметры этого кода можно вычислить непосредственно без цитирования [5], с использованием теоремы 5. Действительно, транспонированная критическая матрица рассматриваемого кода имеет вид

$$\begin{pmatrix} -\alpha & -(\alpha^2 + \alpha) & \dots & -(\alpha^{(q-3)} + \dots + \alpha) \\ \alpha + e & \alpha^2 + \alpha + e & \dots & \alpha^{(q-3)} + \dots + \alpha + e \end{pmatrix}$$

и все ее миноры отличны от нуля.

Предложение 11. Если p — простое число и $p \geq 3$, то $m^{ir}(2, p) \geq p$.

Доказательство. Рассмотрим код (3.2) при $n = p$, $P = Z_p$ и $f(x) = (x - 1)^2$. Это рекурсивный код с порождающей матрицей

$$\begin{pmatrix} 1 & 1 & \dots & 1 \\ 0 & 1 & \dots & p - 1 \end{pmatrix}$$

Таким образом, это $[p, 2, p - 1]$ -код Рида–Соломона. Заметим также, что его транспонированная критическая матрица есть

$$F = \begin{pmatrix} -1 & -2 & \dots & -(p - 2) \\ 2 & 3 & \dots & (p - 1) \end{pmatrix}$$

и все ее миноры отличны от нуля.

4. Расширения рекурсивно дифференцируемых квазигрупп посредством трансверселей

Как известно, трансверсаль латинского квадрата (или квазигруппы) порядка q — это множество из q клеток, по одной из каждой строки и каждого столбца, в которых находятся попарно различные элементы (см. [10, 11]). Отождествляя, как и выше, квазигруппу (латинский квадрат) $(M, \circ)$ с МДР-кодом $\mathcal{H}(3, \circ)$, заметим, что ее трансверсали отождествляются в точности с $[3, 1, 3]$ -подкодами $T \subset \mathcal{H}(3, \circ)$. Действительно, если T — такой подкод, то для каждого $a \in M$ в T существует единственное слово вида (a, b, c) (причем $c = a \circ b$), и соответствующая T трансверсаль квадрата $(M, \circ)$ состоит из всех клеток с координатами (a, b) такими, что $(a, b, c) \in T$. Для любого целого $m > 2$ назовем $[m, 1, m]$ -подкод кода $\mathcal{H}(m, \circ)$ m -трансверсалью квазигруппы $(M, \circ)$, а произвольный $[m, 1, m]$ -подкод кода M^m обобщенной m -трансверсалью над множеством M . Допуская некоторую вольность речи, 3-трансверсали будем называть просто трансверсальями. Нетрудно увидеть, что при $q > 2$ любая обобщенная 3-трансверсаль является трансверсалью некоторого латинского квадрата.

Очевидно, что если $T \subset M^m$ — обобщенная m -трансверсаль, то для любых $a \in M$, $i \in \{1, \dots, m\}$, найдется единственное слово $\mathbf{w} = (w_1, \dots, w_m) \in T$ такое,

что $w_i = a$. Обозначим его через $\mathbf{w}T_i(a)$. Заметим также, что $T \subset M^m$ является обобщенной m -трансверсалью тогда и только тогда, когда T содержит q слов, скажем,

$$T = \{(a_{s1}, \dots, a_{sm}) : s = 1, \dots, q\},$$

и каждый столбец полной матрицы кода T

$$\begin{pmatrix} a_{11} & \dots & a_{1m} \\ \dots & \dots & \dots \\ a_{q1} & \dots & a_{qm} \end{pmatrix}$$

является перестановкой множества M .

Этот факт позволяет сопоставить обобщенной m -трансверсали T семейство из m^2 биекций

$$T_{ij} : M \rightarrow M, \quad i, j = 1, \dots, m,$$

определенных следующим правилом: $T_{ij}(a) = w_j$, где $(w_1, \dots, w_m) = \mathbf{w}T_i(a)$. Другими словами, $T_{ij}(a)$ — это j -я координата (единственного) слова из T , i -я координата которого равна a . Нетрудно видеть, что T_{ii} — тождественное отображение для любого $i = 1, \dots, m$, и что $T_{ij}T_{jk} = T_{ik}$ для любых $i, j, k = 1, \dots, m$ (здесь $T_{ij}T_{jk}$ означает произведение перестановок, то есть

$$(T_{ij}T_{jk})(a) = T_{jk}(T_{ij}(a)), \quad a \in M.$$

Следовательно, указанные биекции выражаются через $m - 1$ биекций $T_{12}, \dots, T_{1m}$, так как $T_{ij} = T_{1i}^{-1}T_{1j}$, $i = 1, \dots, m$. Назовем две обобщенные m -трансверсали $T_1, T_2 \in M^m$ параллельными, если $T_1 \cap T_2 = \emptyset$.

Пусть теперь $T \subset \mathcal{X}(3, \circ)$ — трансверсаль квазигруппы $(M, \circ)$ и отображения $T_{10}, T_{14} : M \rightarrow M$ определены формулами

$$T_{10}(a) \circ a = T_{12}(a), \quad T_{14}(a) = T_{12}(a) \circ T_{13}(a).$$

Назовем множество

$$\tilde{T} = \{(T_{10}(a), a, T_{12}(a), T_{13}(a), T_{14}(a)) : a \in M\} \subset \mathcal{X}(5, \circ)$$

двусторонним расширением трансверсали T . Понятия левого и правого расширения T определяются очевидным образом. Заметим, что левое (правое) расширение T является 4-трансверсалью тогда и только тогда, когда T_{10} (соответственно, T_{14}) — биекция. В этом случае обратное отображение T_{01} (соответственно, T_{41}) определено корректно. Двустороннее расширение $\tilde{T}$ трансверсали T есть 5-трансверсаль (квазигруппы $(M, \circ)$) в точности, если T_{14} и T_{01} суть биекции.

Конструкция, описанная ниже, представляет собой обобщение одной из конструкций, использованных Чжу Ле [19] для построения ортогональных пар латинских квадратов.

Пусть $(M, \circ)$ — квазигруппа порядка q и $T^{(1)}, \dots, T^{(m)}$ — система попарно параллельных трансверсалей M . Пусть, далее, $(H, \times)$ — некоторая квазигруппа порядка m : $H = \{\xi_1, \dots, \xi_m\}$, причем $M \cap H = \emptyset$. Определим новую операцию $*$ на множестве $\Omega = M \cup H$ следующим образом. Сначала для любого $s = 1, \dots, m$ определим множества

$$A_s = \{(a, b) \in M^2 : \exists c \in M : (a, b, c) \in T^{(s)}\} = \{(a, T_{12}^{(s)}(a)) : a \in M\},$$

$$B_s = \{(b, c) \in M^2 : \exists a \in M : (a, b, c) \in T^{(s)}\} = \{(b, T_{23}^{(s)}(b)) : b \in M\}.$$

Положим

$$A = \bigcup_{s=1}^m A_s, \quad B = \bigcup_{s=1}^m B_s$$

и заметим, что попарная параллельность наших трансверселей равносильна тому, что

$$A_s \cap A_t = \emptyset, \quad B_s \cap B_t = \emptyset, \quad s, t = 1, \dots, m, \quad s \neq t. \quad (4.1)$$

Теперь для любых $a, b \in M$ и $s, t = 1, \dots, k$ положим

$$a * b = a \circ b, \quad (a, b) \notin A, \quad (4.2)$$

$$a * b = \xi_s, \quad (a, b) \in A_s, \quad (4.3)$$

$$a * \xi_t = T_{13}^{(t)}(a), \quad (4.4)$$

$$\xi_s * b = T_{23}^{(s)}(b), \quad (4.5)$$

$$\xi_s * \xi_t = \xi_s \times \xi_t. \quad (4.6)$$

Предложение 12. Группоид $(\Omega, *)$ — квазигруппа.

Доказательство. Согласно предложению 3, достаточно доказать, что расстояние кода $\mathcal{K}(3, *)$ равно 2. Указанный код состоит из всех слов

- (1) $(a, b, a \circ b), \quad (a, b) \in M^2 \setminus A,$
- (2) $(a, b, \xi_s), \quad (a, b) \in A_s, \quad s = 1, \dots, m,$
- (3) $(a, \xi_s, c), \quad c = T_{13}^{(s)}(a), \quad a \in M, \quad s = 1, \dots, m,$
- (4) $(\xi_s, b, c), \quad (b, c) \in B_s, \quad s = 1, \dots, m,$
- (5) $(\xi_s, \xi_t, \xi_s \times \xi_t), \quad s, t = 1, \dots, m.$

Нетрудно проверить, что расстояние между любыми двумя различными словами перечисленных выше типов не менее 2. Например, пусть $(a, b) \in M^2 \setminus A$ и $\mathbf{w}_1 = (a, b, a \circ b)$ — слово типа (1). Если $\mathbf{w}_2 = (a', b', a' \circ b')$ — другое слово типа (1), то есть $(a', b') \in M^2 \setminus A$ и $(a, b) \neq (a', b')$, то $\mathbf{w}_1$ и $\mathbf{w}_2$ — два различных слова МДР-кода $\mathcal{K}(3, \circ)$, следовательно, $d(\mathbf{w}_1, \mathbf{w}_2) \geq 2$. Если $\mathbf{w}_2 = (a', b', \xi_s)$, где $(a', b') \in A_s$, то $(a', b') \neq (a, b)$ и $\xi_s \neq a \circ b$, следовательно, и в этом случае $d(\mathbf{w}_1, \mathbf{w}_2) \geq 2$. Случаи, когда $\mathbf{w}_2$ — слово типа (3) или (4), рассматриваются аналогично. Наконец, в последнем случае $\mathbf{w}_2 = (\xi_s, \xi_t, \xi_s \times \xi_t)$, и $d(\mathbf{w}_1, \mathbf{w}_2) = 3$.

Теперь пусть $\mathbf{w}_1 = (a, b, \xi_s), (a, b) \in A_s$. Тогда, если $\mathbf{w}_2 = (a', b', \xi_t)$ — слово того же типа, то либо $a \neq a'$ и $b \neq b'$, либо $s \neq t$ и $a \circ b \neq a' \circ b'$. В обоих случаях $d(\mathbf{w}_1, \mathbf{w}_2) \geq 2$. Если $\mathbf{w}_2$ — слово типа (3) или (4), то, очевидно, $c \neq \xi_s$, и из того, что $a \neq \xi_s$ и $b \neq \xi_s$, следует, что $d(\mathbf{w}_1, \mathbf{w}_2) \geq 3$. Оставшиеся случаи разбираются аналогично.

В описанной выше ситуации, мы говорим, что $(\Omega, *)$ — расширение квазигруппы $(M, \circ)$ квазигруппой $(H, \times)$ посредством системы параллельных трансверселей $T^{(1)}, \dots, T^{(m)}$, и используем обозначение $\Omega = M \uplus H$.

В дальнейшем мы для краткости будем называть рекурсивно 1-дифференцируемую квазигруппу дифференцируемой. Предположим, что M — дифференцируемая

квазигруппа, и найдем критерий того, что квазигруппа $M \uplus H$ также является дифференцируемой. Легко проверить, что производная операция $x \tilde{*} y = y * (x * y)$ удовлетворяет следующим условиям: для любых $a, b \in M$ и $s, t = 1, \dots, m$

$$\xi_s \tilde{*} b = b * T_{23}^{(s)}(b) = \xi_t, \text{ если } (b, T_{23}^{(s)}(b)) \in A_t, \quad (4.7)$$

$$\xi_s \tilde{*} b = b * T_{23}^{(s)}(b) = b \circ (T_{21}^{(s)}(b) \circ b), \text{ если } (b, T_{23}^{(s)}(b)) \notin A, \quad (4.8)$$

$$\xi_s \tilde{*} \xi_t = \xi_t \times (\xi_s \times \xi_t), \quad (4.9)$$

$$a \tilde{*} \xi_t = T_{23}^{(t)}(T_{13}^{(t)}(a)), \quad (4.10)$$

$$a \tilde{*} b = b \circ (a \circ b), \text{ если } (a, b) \notin A, (b, a \circ b) \notin A, \quad (4.11)$$

$$a \tilde{*} b = T_{13}^{(s)}(b) = T_{13}^{(s)}(T_{12}^{(s)}(a)), \text{ если } (a, b) \in A_s, \quad (4.12)$$

$$a \tilde{*} b = \xi_s, \text{ если } (a, b) \notin A, (b, a \circ b) \in A_s. \quad (4.13)$$

Теорема 4 показывает, что $(\Omega, *)$ является дифференцируемой квазигруппой тогда и только тогда, когда $(\Omega, \tilde{*})$ — квазигруппа. Более того, поскольку $(\Omega, *)$ является квазигруппой, то для любых $u, v \in \Omega$ уравнение $x \tilde{*} u = v$ имеет единственное решение. Таким образом, дифференцируемость квазигруппы равносильна разрешимости уравнения

$$u \tilde{*} x = v \quad (4.14)$$

относительно x при любых $u, v \in \Omega$.

Пусть $V(u) = \{u \tilde{*} \omega : \omega \in \Omega\}$ для любого $u \in \Omega$. Тогда каждое уравнение (4.14) имеет решение в том и только в том случае, когда для любого $u \in \Omega$ выполняется равенство

$$V(u) = \Omega. \quad (4.15)$$

Рассмотрим теперь два случая.

Пусть в первом случае $u = \xi_s \in H$. Тогда из (4.7)–(4.9) следует, что

$$V(\xi_s) = V_1^{(1)}(\xi_s) \cup V_2^{(1)}(\xi_s) \cup V_3^{(1)}(\xi_s), \quad (4.16)$$

где

$$V_1^{(1)}(\xi_s) = \{\xi_t : t = 1, \dots, m, \exists b \in M : (b, T_{23}^{(s)}(b)) \in A_t\}, \quad s = 1, \dots, m,$$

$$V_2^{(1)}(\xi_s) = \{b \circ (a \circ b) : (a, b) \in A_s, (b, T_{23}^{(s)}(b)) \notin A\}, \quad s = 1, \dots, m,$$

$$V_3^{(1)}(\xi_s) = \{\xi_t \times (\xi_s \times \xi_t), t = 1, \dots, m\}, \quad s = 1, \dots, m.$$

Так как $V_1^{(1)}(\xi_s) \cup V_3^{(1)}(\xi_s) \subseteq H$ и $V_2^{(1)}(\xi_s) \subseteq M$, (4.15) равносильно паре равенств

$$V_2^{(1)}(\xi_s) = M, \quad (4.17)$$

$$V_1^{(1)}(\xi_s) \cup V_3^{(1)}(\xi_s) = H. \quad (4.18)$$

Из определения множеств $V_1^{(1)}(\xi_s)$ и $V_2^{(1)}(\xi_s)$ видно, что они не пересекаются и общее число их элементов не превосходит числа различных элементов $b \in M$, откуда следует, что

$$|V_1^{(1)}(\xi_s)| + |V_2^{(1)}(\xi_s)| \leq |M|.$$

Поэтому из (4.17) и (4.18) следует, что

$$V_3^{(1)}(\xi_s) = H, \quad (4.19)$$

$$V_1^{(1)}(\xi_s) = \emptyset. \quad (4.20)$$

Обратно, из (4.17), (4.19) и (4.20) вытекает (4.18), таким образом, в рассматриваемом случае (4.15) равносильно (4.17), (4.19) и (4.20).

Выполнение условия (4.19) для всех $s = 1, \dots, m$ означает просто, что $(H, \times)$ — дифференцируемая квазигруппа, так как $(H, \times)$ — подквазигруппа квазигруппы $(\Omega, *)$.

Выполнение условия (4.20) для всех $s = 1, \dots, m$ равносильно тому, что $(b, a \circ b) \notin A$, если $(a, b) \in A$, или, поскольку $\{(b, a \circ b) : (a, b) \in A\} = B$, тому, что

$$A \cap B = \emptyset. \quad (4.21)$$

Из последнего условия следует, что

$$V_2^{(1)}(\xi_s) = \{b \circ (a \circ b) : (a, b) \in A_s\}, \quad s = 1, \dots, m.$$

Поэтому совокупность условий (4.17) и (4.20) равносильна (4.21) и тому, что правое расширение

$$\{a, b, c, b \circ c\} : (a, b, c) \in T^{(s)}\}$$

каждой трансверсали $T^{(s)}$ является трансверсалью кода $\mathcal{X}(4, *)$.

Таким образом, в рассматриваемой ситуации (4.15) равносильно тому, что $(H, \times)$ — дифференцируемая квазигруппа, $A \cap B = \emptyset$ и правое расширение каждой трансверсали есть трансверсаль. Мы будем предполагать выполнение последних трех условий при рассмотрении следующего случая. Заметим также, что в этой ситуации операция $\bar{*}$ определяется на самом деле только равенствами (4.8)–(4.13).

Рассмотрим теперь второй случай, когда $u = a \in M$. Используя (4.10)–(4.13), получаем, что

$$V(a) = \bigcup_{i=1}^4 V_i^{(2)}(a),$$

где

$$V_1^{(2)}(a) = \{T_{23}^{(t)}(T_{13}^{(t)}(a)) : t = 1, \dots, m\}, \quad (4.22)$$

$$V_2^{(2)}(a) = \{T_{13}^{(t)}(T_{12}^{(t)}(a)) : t = 1, \dots, m\}, \quad (4.23)$$

$$V_3^{(2)}(a) = \{b \circ (a \circ b) : b \in M, (a, b) \notin A, (b, a \circ b) \notin A\}, \quad (4.24)$$

$$V_4^{(2)}(a) = \{\xi_s : s = 1, \dots, m, \exists b \in M : (a, b) \notin A, (b, a \circ b) \in A_s\}, \quad (4.25)$$

причем, ввиду (4.21),

$$V_4^{(2)}(a) = \{\xi_s : s = 1, \dots, m, \exists b \in M : (b, a \circ b) \in A_s\}. \quad (4.26)$$

Так как $V_4^{(2)}(a) \subseteq H$ и

$$\bigcup_{i=1}^3 V_i^{(2)}(a) \subseteq M,$$

(4.15) эквивалентно паре равенств

$$V_4^{(2)}(a) = H, \quad (4.27)$$

$$\bigcup_{i=1}^3 V_i^{(2)}(a) = M. \quad (4.28)$$

Выполнение всех равенств вида (4.27) эквивалентно условию

$$\forall a \in M, s = 1, \dots, m: V_4^{(2)}(a) \ni \xi_s.$$

Используя понятие левого расширения трансверсали, перепишем это условие в виде

$$\forall a \in M, s = 1, \dots, m, \exists b \in M: a = T_{10}^{(s)}(b). \quad (4.29)$$

Поскольку M — конечное множество, (4.29) равносильно тому, что $T_{10}^{(s)}$ — биекция для каждого $s = 1, \dots, m$. Другими словами, это означает, что левое расширение каждой трансверсали $T^{(s)}$ является трансверсалью. Таким образом, вместе с условием на правые расширения, полученным при рассмотрении первого случая, (4.27) эквивалентно следующему условию: двустороннее расширение

$$\tilde{T}^{(s)} = \{(T_{10}^{(s)}(a), a, T_{12}^{(s)}(a), T_{13}^{(s)}(a), T_{14}^{(s)}(a)): a \in M\} \quad (4.30)$$

является трансверсалью кода $\mathcal{K}(5, \circ)$.

Рассмотрим теперь (4.28). Заметим, что $|V_1^{(2)}(a)| \leq m$ и $|V_2^{(2)}(a)| \leq m$. Пусть $T_{ij}^H(a) = \{T_{ij}^{(s)}(a), s1, \dots, m\}$. Тогда

$$\begin{aligned} (a, b) \in A &\iff b \in T_{12}^H(a), \\ (b, a \circ b) \in A &\iff a \in T_{10}^H(b). \end{aligned}$$

Поскольку левое расширение каждой трансверсали $T^{(s)}$ является трансверсалью, получаем, что

$$(b, a \circ b) \in A \iff b \in T_{01}^H(a).$$

В результате (4.24) можно переписать как

$$V_3^{(2)}(a) = \{b \circ (a \circ b): b \in M \setminus (T_{01}^H(a) \cup T_{12}^H(a))\}.$$

Здесь $T_{01}^H(a) \cap T_{12}^H(a) = \emptyset$ в силу (4.21). Более того, трансверсали параллельны и квазигруппа $(M, \circ)$ дифференцируема, поэтому

$$|T_{01}^H(a)| = |T_{12}^H(a)| = m, \quad |V_3^{(2)}(a)| = n - 2m.$$

Вместе с (4.28) это влечет равенства

$$\begin{aligned} |V_1^{(2)}(a)| &= m, \\ |V_2^{(2)}(a)| &= m, \\ V_1^{(2)}(a) \cap V_2^{(2)}(a) &= \emptyset, \\ V_1^{(2)}(a) \cup V_2^{(2)}(a) &= M \setminus V_3^{(2)}(a). \end{aligned} \quad (4.31)$$

Правая часть последнего равенства имеет вид

$$M \setminus V_3^{(2)}(a) = \{b \circ (a \circ b) : b \in (T_{01}^H(a) \cup T_{12}^H(a))\} = T_{03}^H(a) \cup T_{14}^H(a).$$

Таким образом, последнее условие из (4.31) означает, что

$$V_1^{(2)}(a) \cup V_2^{(2)}(a) = T_{03}^H(a) \cup T_{14}^H(a). \quad (4.32)$$

Обратно, (4.28) следует из равенств (4.31), (4.32) при условиях, полученных ранее.

В итоге получаем следующее утверждение.

Теорема 8. Пусть M — дифференцируемая квазигруппа, H — произвольная квазигруппа порядка m и $\{T^{(1)}, \dots, T^{(m)}\}$ — система параллельных трансверсалий M .

Тогда квазигруппа $M \uplus H$ дифференцируема в том и только в том случае, если выполнены следующие условия (мы используем обозначения, введенные выше):

- (1) квазигруппа H дифференцируема,
- (2) $A \cap B = \emptyset$ (см. (4.21)),
- (3) двустороннее расширение каждой трансверсали из $\{T^{(1)}, \dots, T^{(m)}\}$ является трансверсалью (см. (4.30)),
- (4) для любого $a \in M$, если

$$S_a = \{T_{23}^{(t)}(T_{13}^{(t)}(a)) : t = 1, \dots, m\},$$

$$U_a = \{T_{13}^{(t)}(T_{12}^{(t)}(a)) : t = 1, \dots, m\},$$

то $|S_a| = |U_a| = m$, $S_a \cap U_a = \emptyset$ (см. (4.31)),

- (5) для любого $a \in M$

$$S_a \cup U_a = T_{03}^H(a) \cup T_{14}^H(a)$$

(см. (4.32)).

Заметим, что описанная конструкция $M \uplus H$ является обобщением ранее предложенной в [17] конструкции, соответствующей случаю $m = 1$ (см. также [1, стр. 118]). Так как при $m = 1$ квазигруппа H бесконечно дифференцируема, представляется заманчивым использовать именно ее для расширения M до дифференцируемой квазигруппы. Однако, как показывает следующий результат, сама квазигруппа M в этом случае не может быть дифференцируемой.

Следствие 5. В условиях теоремы 8, квазигруппа $M \uplus H$ недифференцируема при $m = 1$.

Доказательство. В этом случае условия (2) и (5) несовместны. Действительно, пусть T — трансверсаль, с помощью которой расширяется дифференцируемая квазигруппа $(M, \circ)$. Тогда условие (5) означает, в частности, что для любого $a \in M$,

$$T_{23}(T_{13}(a)) \in \{T_{03}(a), T_{14}(a)\}.$$

Пусть $T_{23}(T_{13}(a)) = T_{03}(a)$. Тогда $T_{13}(a) = T_{02}(a)$. Отсюда, ввиду равенств $T_{13}(a) = a \circ T_{12}(a)$ и $T_{02}(a) = a \circ T_{01}(a)$, следует равенство $T_{12}(a) = T_{01}(a)$. Пусть $b = T_{12}(a) = T_{01}(a)$. Тогда

$$(b, a \circ b) = (T_{12}(a), T_{13}(a)) \in B,$$

$$(b, a \circ b) = (T_{01}(a), T_{02}(a)) \in A,$$

откуда $A \cap B \neq \emptyset$.

Теперь пусть $T_{23}(T_{13}(a)) = T_{14}(a)$. Тогда для $c = T_{13}(a)$ справедливо равенство $T_{21}(c) = T_{34}(c)$. Отсюда, ввиду соотношений $T_{23}(c) = T_{21}(c) \circ c$ и $T_{34}(c) = T_{32}(c) \circ c$, следует, что $T_{32}(c) = T_{21}(c)$. Пусть $d = T_{32}(c) = T(c)$. Тогда

$$(d, c) = (T_{21}(c), c) \in A,$$

$$(d, c) = (T_{32}(c), c) \in B,$$

поэтому опять $A \cap B \neq \emptyset$.

Ниже приводится пример, показывающий, что дифференцируемое расширение посредством одной трансверсали действительно возможно.

Пример 2. Рассмотрим пример расширения посредством одной трансверсали. Пусть M — квазигруппа порядка 3 с элементами 0, 1, 2 и таблицей Кэли

1	0	2
0	2	1,
2	1	0

где главная диагональ $T = \{(0, 0, 1), (1, 1, 2), (2, 2, 0)\}$. Тогда расширение тривиальной квазигруппой $H = \{\xi\}$ дает дифференцируемую квазигруппу с таблицей Кэли

ξ	0	2	1
0	ξ	1	2
2	1	ξ	0
1	2	0	ξ

Таким образом, в общем случае мы не знаем необходимых и достаточных условий того, что расширение — дифференцируемая квазигруппа.

Рассмотрим теперь частный случай описанной выше конструкции, когда M — левый модуль над кольцом R с единицей (вообще говоря, некоммутативным). Можно считать, что модуль ${}_R M$ точный.

Будем рассматривать квазигруппы вида $x \circ y = ax + by$ на M , где $a, b \in R^*$, R^* обозначает группу обратимых элементов кольца R . Эта квазигруппа дифференцируема тогда и только тогда, когда $a + b^2 \in R^*$ (теорема 4). Нетрудно заметить, что для любого подмножества $C = \{\sigma_1, \dots, \sigma_m\} \subseteq M$ и любого $\alpha \in R^*$ множества

$$\{(x, y, ax + by) : \alpha x + y = \sigma\}, \quad \sigma \in C,$$

образуют систему параллельных трансверсали квазигруппы M . Предположим, что существует дифференцируемая квазигруппа H порядка $|H| = |C|$. Применим условия теоремы 8, чтобы найти соотношения между параметрами a, b, α и C , гарантирующие дифференцируемость квазигруппы $M \uplus H$.

Сначала запишем для данного случая отображения и множества, использованные в этой теореме. Условие (1) выполнено.

Для любых $s, t = 1, \dots, m$

$$\begin{aligned} A_s &= \{(x, \sigma_s - \alpha x) : x \in M\}, \\ B_t &= \{(\sigma_t - \alpha x, (a - b\alpha)x + b\sigma_t) : x \in M\}. \end{aligned}$$

Очевидные преобразования показывают, что условие (2) равносильно условию

$$(b\alpha - a + \alpha^2)M \cap \{(b + \alpha)\sigma_t - \sigma_s : s, t = 1, \dots, m\} = \emptyset. \quad (4.33)$$

Однако, для нахождения достаточных условий дифференцируемости вместо последнего условия можно использовать более простое и более сильное условие

$$b = a\alpha^{-1} - \alpha, \quad a\alpha^{-1}C \cap C = \emptyset. \quad (4.34)$$

Двустороннее расширение трансверсали $T^{(s)}$ можно записать как

$$\begin{aligned} \tilde{T}^{(s)} &= \{(a^{-1}(\sigma_s - (\alpha + b)x), x, \sigma_s - \alpha x, ax + b(\sigma_s - \alpha x), \\ &\quad (a + b^2)\sigma_s + (ba - a\alpha - b^2\alpha)x) : x \in M\}. \end{aligned}$$

С учетом указанного выше условия $\alpha + b = a\alpha^{-1}$, это равносильно представлению

$$\tilde{T}^{(s)} = \{(a^{-1}\sigma_s - \alpha^{-1}x, x, \sigma_s - \alpha x, b\sigma_s + \alpha^2x, (a + b^2)\sigma_s - \alpha^3x) : x \in M\}. \quad (4.35)$$

Таким образом, $\tilde{T}^{(s)}$ оказывается трансверсалью, так как $\alpha \in R^*$, и условие (3) выполнено.

Далее, для любого $x \in M$

$$\begin{aligned} S_x &= \{(a\alpha^{-1} - \alpha b)\sigma_s - \alpha^3x : s = 1, \dots, m\}, \\ U_x &= \{(b + \alpha^2)\sigma_t - \alpha^3x : t = 1, \dots, m\}. \end{aligned}$$

Теперь очевидно, что равенства (4) истинны, если

$$a\alpha^{-1} - \alpha b, b + \alpha^2 \in R^*, \quad (a\alpha^{-1} - \alpha b)C \cap (b + \alpha^2)C = \emptyset.$$

Для того чтобы учесть условие (5) теоремы 8, заметим, что ввиду (4.35),

$$\tilde{T}_{03}^{(s)}(x) = (b + \alpha^3a^{-1})\sigma_s - \alpha^3x,$$

и ввиду (4.34)

$$b + \alpha^3a^{-1} = (ba\alpha^{-1} + \alpha^2)\alpha a^{-1} = (a + b^2)\alpha a^{-1}.$$

Поэтому

$$\begin{aligned} T_{03}^H(x) &= \{(a + b^2)\alpha a^{-1}\sigma_s - \alpha^3x : s = 1, \dots, m\}, \\ T_{14}^H(x) &= \{(a + b^2)\sigma_t - \alpha^3x : t = 1, \dots, m\}. \end{aligned}$$

Следовательно, условие (5) вытекает из соотношения

$$(a\alpha^{-1} - \alpha b)C \cup (b + \alpha^2)C = (a + b^2)(a\alpha^{-1}C \cup C).$$

В итоге получаем следующее утверждение.

Теорема 9. Пусть M — конечный точный модуль над кольцом R (вообще говоря, некоммутативным), $a, b, \alpha \in R$ и $C = \{\sigma_1, \dots, \sigma_m\} \subset M$, и пусть H — дифференцируемая квазигруппа порядка t . Допустим, что выполнены следующие условия:

- (1) $a, b, a + b^2, \alpha, a\alpha^{-1} - \alpha b, (b + \alpha^2) \in R^*$,
- (2) $b\alpha = a - \alpha^2$,
- (3) $a\alpha^{-1}C \cap C = (b + \alpha^2)C \cap (a\alpha^{-1} - \alpha b)C = \emptyset$,
- (4) $(a\alpha^{-1} - \alpha b)C \cup (b + \alpha^2)C = (a + b^2)(C \cup \alpha\alpha^{-1}C)$.

Тогда $(M, ax + by)$ — дифференцируемая квазигруппа, семейство множеств

$$T^{(s)} = \{(x, y, ax + by) : x, y \in M, \alpha x + y = \sigma_s\}, \quad s = 1, \dots, t,$$

является системой параллельных трансверсалей и соответствующее расширение $M \uplus H$ — дифференцируемая квазигруппа.

Следствие 6. Если $(l, 6) = 1$, то существует дифференцируемая квазигруппа порядка $7l + 3$.

Доказательство. Достаточно в теореме 9 взять $R = M = Z_7 \oplus Z_l$, $a = (2, 2)$, $b = (1, 1)$, $\alpha = (-2, 1)$, $t = 3$, $C = \{(1, 0), (2, 0), (4, 0)\}$.

Как важную иллюстрацию мы приведем дифференцируемую квазигруппу порядка 10 и ее производную:

0	1	2	9	4	8	7	6	5	3	0	7	8	1	9	4	2	6	5	3
8	7	4	5	6	9	1	3	2	0	5	3	1	7	8	2	9	0	6	4
9	5	8	7	1	2	3	0	6	4	3	9	6	4	2	7	8	1	0	5
6	0	9	2	8	7	5	4	3	1	7	8	4	9	0	5	3	2	1	6
7	2	3	4	9	6	8	1	0	5	6	4	7	8	5	9	1	3	2	0
3	8	7	6	0	1	9	5	4	2	9	2	0	5	7	8	6	4	3	1
5	9	0	8	7	3	4	2	1	6	8	0	9	3	1	6	7	5	4	2
1	3	5	0	2	4	6	7	8	9	1	5	2	6	3	0	4	7	9	8
2	4	6	1	3	5	0	8	9	7	2	6	3	0	4	1	5	8	7	9
4	6	1	3	5	0	2	9	7	8	4	1	5	2	6	3	0	9	8	7

Тем самым, для параметра $n^r(2, 10)$ справедлива та же самая оценка снизу, что и для $n(2, 10)$, так что согласно [10, 11] $n^r(2, 10) \geq 4$.

В таблице 1 перечислены значения $q \leq 126$, для которых применение теоремы 9 позволяет построить дифференцируемую квазигруппу порядка q .

В эту таблицу можно было бы включить и некоторые значения $q > 126$, но в следующем разделе мы предложим метод построения дифференцируемых квазигрупп, который годится для всех $q > 126$ (за исключением числа 164). Сейчас мы только заметим, что с учетом следствия 4 оценка $n^r(2, q) \geq 4$ справедлива для всех $q = \{3, \dots, 126\} \setminus \{6, 14, 18, 26, 42, 74\}$.

Таблица 1.

q	R	M	H	a	b	α	C
10	Z_7	Z_7	Z_3	2	1	5	1, 2, 4
22	Z_{19}	Z_{19}	Z_3	2	1	1	1, 7, 11
34	Z_{31}	Z_{31}	Z_3	5	4	26	1, 5, 25
38	Z_{35}	Z_{35}	Z_3	2	1	26	5, 10, 20
46	Z_{43}	Z_{43}	Z_3	4	14	8	1, 6, 36
58	Z_7^2	Z_7^2	Z_3^2	(2, 2)	(1, 1)	(5, 5)	$\{(u, v) : u, v \in \{1, 2, 4\}\}$
78	Z_{71}	Z_{71}	Z_7	4	8	30	1, 20, 30, 32, 37, 45, 48
82	Z_{79}	Z_{79}	Z_3	3	2	1	1, 23, 55
94	Z_{91}	Z_{91}	Z_3	2	1	89	13, 26, 52
98	Z_{95}	Z_{95}	Z_3	7	26	91	5, 35, 55
106	Z_{103}	Z_{103}	Z_3	19	18	1	1, 46, 56
118	Z_{109}	Z_{109}	Z_9	1	24	91	1, 16, 27, 38, 45, 63, 66, 75, 105
122	Z_{119}	Z_{119}	Z_3	1	61	117	17, 34, 68
126	Z_{121}	Z_{121}	Z_5	1	43	118	1, 3, 9, 27, 81

5. Построение идемпотентных рекурсивно дифференцируемых квазигрупп с помощью псевдогеометрий

Следуя [8], назовем пару $(P, \mathcal{L})$ псевдогеометрией, если P — некоторое непустое множество (элементы которого будут называться точками), $\mathcal{L}$ — некоторое множество непустых подмножеств P (называемых прямыми), и любые две различные точки принадлежат единственной прямой.

Приведем три стандартных примера псевдогеометрий.

Пример 3 (Аффинная плоскость $A^2(F)$). Пусть F — конечное поле, $P = F^2$. Определим прямые как множества решений $\{(x, y) \in P : ax + by + c = 0\}$ всех линейных уравнений с $a \neq 0$ или $b \neq 0$. Эта псевдогеометрия называется аффинной плоскостью над F и обозначается через $A^2(F)$. Легко видеть, что в этом случае $|P| = |F|^2$, $|\mathcal{L}| = |F|(|F| + 1)$, и каждая прямая содержит $|F|$ точек.

Пример 4 (Проективная плоскость $P^2(F)$). Заметим, что аффинная плоскость $A^2(F)$ содержит $|F| + 1$ пучков параллельных (то есть попарно непересекающихся) прямых. Добавим общую (бесконечно удаленную) точку ко всем прямым каждого пучка и назовем множество добавленных точек (бесконечно удаленной) прямой. Полученная псевдогеометрия называется проективной плоскостью над F и обозначается через $P^2(F)$. В этом случае $|P| = |\mathcal{L}| = |F|^2 + |F| + 1$, и каждая прямая содержит $|F| + 1$ точек.

Пример 5. (Сопровождающая псевдогеометрия для системы попарно ортогональных латинских квадратов.) Пусть q — натуральное число, причем существует система $\{f_1, \dots, f_k\}$ из k попарно ортогональных латинских квадратов порядка q ,

$$f_i : \{0, \dots, q-1\}^2 \rightarrow \{0, \dots, q-1\}, \quad i = 1, \dots, k.$$

Рассмотрим множество P всех пар (x, y) , $x = 0, \dots, q-1$, $y = -1, \dots, k$. Определим прямые двух типов:

горизонтальные прямые $\{(x, y): x = 0, \dots, q-1\}$ для любого фиксированного $y = -1, 0, 1, \dots, k$,

наклонные прямые $\{(i, -1), (j, 0)\} \cup \{(f_y(i, j), y): y = 1, \dots, k\}$ для любой фиксированной пары i, j , $i, j = 0, \dots, q-1$.

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

Пример 6 (Редуцированная псевдогеометрия). Пусть $(P, \mathcal{L})$ — произвольная псевдогеометрия и P' — произвольное непустое подмножество множества P . Положим

$$\mathcal{L}' = \{L \cap P': L \in \mathcal{L}, L \cap P' \neq \emptyset\}.$$

Легко видеть, что $(P', \mathcal{L}')$ также является псевдогеометрией.

В частности, если число q примарно, то сопровождающая псевдогеометрия с параметрами q, k , где $k \leq q-1$, может быть получена как редуцированная псевдогеометрия из проективной плоскости $P^2(GF(q))$ удалением всех точек, лежащих на $q-1-k$ прямых, проходящих через одну фиксированную точку.

Следующее утверждение очень близко к одной из основных конструкций из [8].

Теорема 10. Пусть $(P, \mathcal{L})$ — псевдогеометрия, причем для любой прямой $L \in \mathcal{L}$ существует идемпотентная рекурсивно дифференцируемая квазигруппа порядка $|L|$. Тогда существует идемпотентная рекурсивно дифференцируемая квазигруппа порядка $|P|$.

Доказательство. Сначала определим операцию $f_L: L^2 \rightarrow L$ на каждой прямой $L \in \mathcal{L}$ таким образом, чтобы превратить L в идемпотентную дифференцируемую квазигруппу. Тогда для любых различных точек $x, y \in P$ положим $f(x, y) = f_L(x, y)$, где L — (единственная) прямая, содержащая x и y , и положим $f(x, x) = x$ для любой точки $x \in P$. Очевидно, что операция f определена корректно. Более того, любое уравнение $f(y, f(u, y)) = v$ разрешимо в P . Действительно, если $u \neq v$ и L — прямая, содержащая точки u и v , то решение соответствующего уравнения для операции f_L одновременно является решением и для операции f , а если $u = v$, то $x = u = v$ — решение исходного уравнения в силу идемпотентности. Поскольку множество P конечно, существование решения при любом фиксированном u (или v) влечет его единственность. По теореме 4 (P, f) — дифференцируемая квазигруппа.

Теперь обозначим через I множество всех чисел $q \in \mathbb{N}$ таких, что существует идемпотентная дифференцируемая квазигруппа порядка q . Разумеется, $1 \in I$. Из предложений 10 и 11 вытекает, что если q — примарное число и $q \geq 5$, то $q \in I$, как и любое произведение таких чисел. С другой стороны, прямой перебор показывает, что $2, 3, 4 \notin I$. Вопрос о том, принадлежит ли 10 множеству I , остается, насколько известно авторам, открытым.

Укажем способ, позволяющий получать неизвестные элементы множества I из уже известных.

Таблица 2.

Теорема 11. Пусть числа $n, t, l, d_1, \dots, d_l$ таковы, что существует $t+l-2$ попарно ортогональных латинских квадратов n -го порядка, $n, t, t+1, \dots, t+l, d_1, \dots, d_l \in I$, и $d_i \leq n$ для всех $i = 1, \dots, l$.

Тогда

$$q = nt + d_1 + \dots + d_l \in I.$$

Доказательство. Рассмотрим сопровождающую псевдогеометрию $(P, \mathcal{L})$ (см. пример 5) для заданного множества попарно ортогональных латинских квадратов. Она содержит $t+l$ горизонтальных прямых, которые мы перенумеруем числами от 1 до $t+l$. Удалим $n-d_l$ точек $(t+l)$ -й горизонтальной прямой, $n-d_{l-1}$ точек $(t+l-1)$ -й горизонтальной прямой, и т.д. Пусть P' — множество оставшихся точек, $(P', \mathcal{L}')$ — редуцированная псевдогеометрия (см. пример 6). Ситуация иллюстрируется таблицей 2 (здесь $n = 8, t = 7, l = 2, d_1 = d_2 = 5$, пустые кружки представляют удаленные точки, а заполненные представляют точки множества P').

Если L — горизонтальная прямая из $\mathcal{L}$, то $|L \cap P'|$ — либо n , либо одно из чисел $d_i, i = 1, \dots, l$, поэтому на $L \cap P'$ можно определить структуру идемпотентной дифференцируемой квазигруппы. Если L — наклонная прямая из $\mathcal{L}$, то $t \leq |L \cap P'| \leq t+l$, так как L не может содержать более одной удаленной точки с каждой из l горизонтальных прямых, и снова на $L \cap P'$ можно определить структуру идемпотентной дифференцируемой квазигруппы. Теперь наше утверждение вытекает из теоремы 10.

Пусть $[a, b] = \{n \in \mathbb{N} : a \leq n \leq b\}$ для любых $a, b \in \mathbb{N}$.

Следствие 7. Если существует число k такое, что $[2^k - 1, 2^{2k+1}] \subset I$, то $n \in I$ для любого $n \geq 2^k - 1$.

Доказательство. Достаточно показать, что $[2^k - 1, 2^n] \subset I$ для любого $n \geq k$. Воспользуемся индукцией по n . В самом деле, для $n = k, k+1, \dots, 2k+1$ утверждение истинно по условию. Пусть $n \geq 2k+1$, причем $[2^{k+1} - 1, 2^n] \subset I$. Покажем, что $[2^k - 1, 2^{n+1}] \subset I$. Для этого возьмем любое число $x \in [2^n + 1, 2^{n+1} - 1]$ и запишем его в виде $x = 2^n + \alpha$, где $1 \leq \alpha < 2^n$. Положим $\alpha = 2^{n-k}q + r$, где $0 \leq r < 2^{n-k}$. Тогда $0 \leq q2^{n-k} < 2^n$, так что $0 \leq q < 2^k$, и

$$x = (2^k - 1)2^{n-k} + 2^{n-k} + q2^{n-k} + r = (2^k - 1 + q)2^{n-k} + 2^{n-k} + r$$

Положим $t = 2^k - 1 + q$, тогда $t \geq 2^k - 1$. Более того,

$$t + 2 = 2^k + 1 + q \leq 2^k + 2^k = 2^{k+1} \leq 2^{n-k} < 2^n,$$

поскольку $n \geq 2k + 1$. Следовательно, $t, t + 1, t + 2 \in I$ и существует t попарно ортогональных латинских квадратов примарного порядка 2^{n-k} (см. теорему 6 или [10]). Рассмотрим теперь представление

$$2^{n-k} + r = 2^{n-k-1} + r_1 + 2^{n-k-1} + r_2,$$

где $r_1 = [r/2]$, $r_2 = r - r_1$, и положим $d_i = 2^{n-k-1} + r_i$, $i = 1, 2$. Тогда $r_i \leq 2^{n-k-1}$ и

$$2^k \leq d_i \leq 2^{n-k} < 2^n, \quad i = 1, 2.$$

Согласно предположению индукции $d_1, d_2 \in I$, так что из теоремы 11 следует, что

$$x = 2^{n-k}t + 2^{n-k} + r = 2^{n-k}t + d_1 + d_2 \in I.$$

Поскольку примарное число $2^{n+1} > 4$ принадлежит множеству I , индуктивный переход завершен.

Следствие 8. Для любого числа $q \geq 127$, кроме, возможно, числа 164, существует идемпотентная рекурсивно дифференцируемая квазигруппа порядка q .

Доказательство. Компьютерный поиск, основанный на нескольких применениях теоремы 11 и предложения 8, показал, что

$$[127, 2^{17}] \setminus \{164, 674\} \subset I.$$

Мы не смогли определить, принадлежит ли число 164 множеству I , но, разумеется, $n^r(2, 164) \geq 5 > 4$, так как $164 = 4 \cdot 41$. Для второго исключения, числа 674, мы использовали псевдогеометрию, построенную при доказательстве теоремы 11, с параметрами

$$n = 89, \quad t = 7, \quad l = 51, \quad d_1 = \dots = d_{51} = 1.$$

Хотя эти параметры и не удовлетворяют условию (2) указанной теоремы, тем не менее, если удалить точки так, что все неудаленные точки укороченных прямых лежат на одной наклонной прямой из исходной сопровождающей псевдогеометрии, то любая прямая полученной псевдогеометрии содержит 7, 8, 58 или 89 точек. Остается показать, что $58 \in I$, но это следует из теоремы 11 с параметрами $n = 8$, $t = 7$, $l = 2$, $d_1 = d_2 = 1$. Тем самым проверено, что условия теоремы 7 выполнены при $k = 8$.

Как мы уже отметили в конце раздела 4, только для пяти чисел q существование дифференцируемой квазигруппы порядка q не вытекает из следствий 4, 8, теоремы 11 и таблицы 1. Это числа 14, 18, 26, 42 и 74. Но в случае $q = 74$ вопрос может быть решен с помощью конструкции из теоремы 11.

Предложение 13. Существует рекурсивно дифференцируемая квазигруппа порядка 74.

9. Bush K. A. Orthogonal arrays of index unity, *Ann. Math. Stat.* (1952) **23**, 426–434.
10. Dénes J., Keedwell A. D. *Latin Squares and Their Applications*. Academic Press, New York, 1974.
11. Dénes J., Keedwell A. D. *Latin Squares. New Developments in the Theory and Applications*. North-Holland, Amsterdam, 1991.
12. Heise W., Quattrocci P. *Informations- und Codierungstheorie*. Springer, Berlin, 1995.
13. Hill R. *A First Course in Coding Theory*. Clarendon Press, Oxford, 1994.
14. Koscielny C. Constructing a better cyclic code than cyclic Reed-Solomon code. *IEEE Trans. Inf. Theory* (1995) **41**, №4, 1191–1194.
15. Kurakin V. L., Kuzmin A. S., Mikhalev A. V., Nechaev A. A. Linear recurrences over rings and modules, *J. Math. Sci.* (1995) **76**, №6, 2793–2915.
16. van Lint J. H. *Introduction to Coding Theory*. Springer, Berlin, 1982.
17. Osborn J. M. New loops from old geometries. *Amer. Math. Monthly* (1961) **68**, 103–107.
18. Chein O., Pflugfelder H. O., Smith J. D. H. *Quasigroups and Loops: Theory and Applications*. Sigma Series in Pure Mathematics, v. 8, Heldermann, Berlin, 1990.
19. Zhu Lie. A short disproof of Euler's conjecture concerning orthogonal Latin squares. *Ars Combinatoria* (1982) **14**, 47–55.
20. Zierler N. Linear recurring sequences. *J. Soc. Ind. Appl. Math.* (1969) **7**, №1, 31–48.

Статья поступила 10.03.1998.