Сибирский математический журнал
Июль—август, 2006. Том 47, № 4

УДК 519.143

АСИМПТОТИКА ЧИСЛА n–КВАЗИГРУПП ПОРЯДКА 4

В. Н. Потапов, Д. С. Кротов

Аннотация: Асимптотика числа n-квазигрупп порядка 4 имеет вид $3^{n+1}2^{2^n+1}(1+o(1))$.

Ключевые слова: n-квазигруппа, МДР-коды, разложимость.

Алгебраическая система, состоящая из множества Σ мощности $|\Sigma| = k$ и n-арной операции $f : \Sigma^n \to \Sigma$, однозначно обратимой по каждой своей переменной, называется *n-квазигруппой порядка k*. Принято (см. [1]) называть *n-квазигруппой порядка k* также и соответствующую функцию f. Таблица значений n-квазигруппы порядка k называется *латинским n-кубом измерения k* (если $n = 2$, то — *латинским квадратом*). Кроме того, имеется взаимно однозначное соответствие между n-квазигруппами и МДР-кодами длины $n + 1$ с расстоянием 2.

Нетрудно показать, что для каждого n существуют только две n-квазигруппы порядка 2 и $3 \cdot 2^n$ различных n-квазигрупп порядка 3, составляющие один класс эквивалентности. В настоящей работе предпринято исследование свойств n-квазигрупп порядка 4 и получено асимптотическое представление $3^{n+1}2^{2^n+1}(1+o(1))$ их числа. Результаты исследования анонсированы в [2]. При $k > 4$ асимптотика числа и даже асимптотика логарифма числа n-квазигрупп остается неизвестной.

В § 1–4 даются необходимые определения и утверждения о четырехзначных МДР-кодах с расстоянием 2 и 2-кодах (§ 1), линейных 2-кодах (§ 2), n-квазигруппах порядка 4 (§ 3), полулинейных n-квазигруппах порядка 4 (§ 4). В § 5 доказано, что почти все (при $n \to \infty$) n-квазигруппы порядка 4 являются полулинейными, и установлены асимптотически точные границы их числа.

Помимо основного результата, самостоятельный интерес представляют лемма 1 о линейном антислое в 2-МДР-коде, лемма 4 о полулинейном слое в n-квазигруппе, а также леммы 2 и 3 о разложимости 2-МДР-кодов и n-квазигрупп, доказанные в [3, 4], и их следствие 3.

§ 1. МДР-коды и 2-коды

Пусть $\Sigma = \{0, 1, 2, 3\}$ и n — натуральное число. В настоящей статье изучаются подмножества Σ^n и определенные на Σ^n функции, обладающие некоторыми определенными ниже свойствами. Элементы множества Σ^n будем называть

Работа первого автора выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 05–01–00364).

© **2006 Потапов В. Н., Кротов Д. С.**

вершинами. Множество натуральных чисел от 1 до n обозначим через $[n]$. Для $\bar{y} = (y_1, \ldots, y_n)$ введем обозначение $\bar{y}^{(i)}\#x = (y_1, \ldots, y_{i-1}, x, y_{i+1}, \ldots, y_n)$.

Пусть $\bar{x} \in \Sigma^n$ и $k \in [n]$. Множество $\mathscr{E}_k(\bar{x}) \triangleq \{\bar{x}^{(k)}\#a : a \in \Sigma\}$ назовем *k-ребром.* Две различные вершины из Σ^n назовем *соседними*, если они принадлежат некоторому k-ребру, т. е. различаются только в одной координате.

Определение. Множество $C \subset \Sigma^n$ называется МДР-*кодом* (*длины* n) *с расстоянием* 2 (в дальнейшем просто МДР-*кодом*), если $|\mathscr{E}_k(\bar{x}) \cap C| = 1$ для всех $\bar{x} \in \Sigma^n$ и $k \in [n]$. Заметим, что $|C| = |\Sigma^n|/4 = 2^{2n-2}$.

Определение. Множество $S \subset \Sigma^n$ будем называть 2-*кодом*, если $|\mathscr{E}_k(\bar{x}) \cap S| = 2$ для всех $\bar{x} \in S$ и $k \in [n]$.

Определение. 2-Код $S \subset \Sigma^n$ будем называть 2-МДР-*кодом*, если $|S| = |\Sigma^n|/2 = 2^{2n-1}$. Другими словами, множество $S \subset \Sigma^n$ есть 2-МДР-код, если $|\mathscr{E}_k(\bar{x}) \cap S| = 2$ для всех $\bar{x} \in \Sigma^n$ и $k \in [n]$. Очевидно, что в этом случае множество $\Sigma^n \backslash S$ также является 2-МДР-кодом.

Обозначим через $\Gamma(S)$ *граф смежности* 2-кода $S \subset \Sigma^n$ с множеством вершин S и множеством ребер $\{(\bar{x}, \bar{y}) : \bar{x}, \bar{y}$ — соседние вершины $\Sigma^n\}$.

Определение. Непустой 2-код $S \subset \Sigma^n$ будем называть *простым*, если он является подмножеством некоторого 2-МДР-кода $S' \subset \Sigma^n$ и граф $\Gamma(S)$ связный. В качестве иллюстрации приведем все с точностью до эквивалентности непустые 2-коды в Σ^2 (рис. 1).

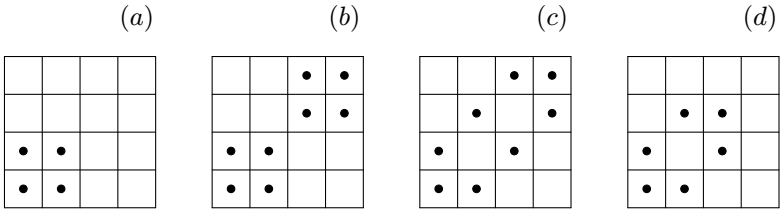

Рис. 1.

Из них 2-коды (a) и (c) являются простыми, (b) и (c) — 2-МДР-кодами.

Определение. 2-МДР-код S *расщепляемый*, если $S = C_1 \cup C_2$, где C_1 и C_2 — непересекающиеся МДР-коды. Нерасщепляемые 2-МДР-коды существуют в Σ^n начиная с $n = 3$. 2-МДР-код S является расщепляемым, если и только если $\Gamma(S)$ — двудольный граф.

Определение. *Изотопией*, или *n-изотопией*, назовем упорядоченный набор из n перестановок $\theta_i : \Sigma \to \Sigma$, $i \in [n]$. Пусть $\bar{\theta} = (\theta_1, \ldots, \theta_n)$ является изотопией и $S \subseteq \Sigma^n$. Введем обозначение $\bar{\theta}S \triangleq \{(\theta_1 x_1, \ldots, \theta_n x_n) : (x_1, \ldots, x_n) \in S\}$.

Определение. Множества $S_1 \subseteq \Sigma^n$ и $S_2 \subseteq \Sigma^n$ будем называть *эквивалентными*, если найдутся перестановка координат $\tau : [n] \to [n]$ и n-изотопия $\bar{\theta}$ такие, что

$$\chi_{S_1}(x_1, \ldots, x_n) \equiv \chi_{\bar{\theta}S_2}(x_{\tau(1)}, \ldots, x_{\tau(n)}),$$

здесь и далее через χ_B обозначается характеристическая функция множества B.

Очевидно, что эквивалентные 2-коды имеют эквивалентные графы смежности, являются или не являются 2-МДР-кодами одновременно, являются расщепляемыми или нерасщепляемыми одновременно, являются простыми или непростыми одновременно.

Предложение 1. *Пусть S — расщепляемый* 2-МДР-*код и γ — число простых* 2-*кодов, включенных в S. Тогда* 2-*код S включает ровно 2^γ различных* МДР-*кодов.*

Доказательство. Число МДР-кодов, включенных в S, равно числу способов выбрать долю двудольного графа $\Gamma(S)$. Поскольку в каждой из γ компонент связности графа $\Gamma(S)$ долю можно выбирать независимо, число способов выбора равняется 2^γ. $\square$

Определение. Пусть $S \subseteq \Sigma^n$, $k \in [n]$ и $y \in \Sigma$. Множество

$$\mathscr{L}_{k;y}S \triangleq \{(x_1, \ldots, x_{k-1}, x_k, \ldots, x_{n-1}) : (x_1, \ldots, x_{k-1}, y, x_k, \ldots, x_{n-1}) \in S\}$$

назовем y-м *слоем* множества S по k-му направлению.

Предложение 2. *Пусть $S, S' \subseteq \Sigma^n$ — некоторые множества, $k \in [n]$ и $\{a, b, c, d\} = \Sigma$.*

(a) *Если S —* 2-*код (расщепляемый* 2-*код,* 2-МДР-*код), то $\mathscr{L}_{k;a}S$ также является* 2-*кодом (расщепляемым* 2-*кодом,* 2-МДР-*кодом) в Σ^{n-1}.*

(b) *Если $k < k' \in [n]$, то $\mathscr{L}_{k;b}(\mathscr{L}_{k';a}S) = \mathscr{L}_{k'-1;a}(\mathscr{L}_{k;b}S)$.*

(c) $\mathscr{L}_{k;a}(S \cap S') = \mathscr{L}_{k;a}S \cap \mathscr{L}_{k;a}S'$.

(d) *Если S и S' —* 2-*коды и $\mathscr{L}_{k;a}S = \mathscr{L}_{k;a}S'$, $\mathscr{L}_{k;b}S = \mathscr{L}_{k;b}S'$, $\mathscr{L}_{k;c}S = \mathscr{L}_{k;c}S'$, то $\mathscr{L}_{k;d}S = \mathscr{L}_{k;d}S'$.*

(e) *Если S —* 2-МДР-*код и $\mathscr{L}_{k;a}S = \mathscr{L}_{k;b}S$, то $\mathscr{L}_{k;c}S = \mathscr{L}_{k;d}S = \Sigma^{n-1}\backslash\mathscr{L}_{k;a}S$.*

Покажем, что 2-МДР-код полностью определяется любым своим непустым подмножеством, которое само является 2-кодом.

Предложение 3 (о единственности продолжения 2-кода). *Пусть $S_1, S_2 \subset \Sigma^n$ —* 2-МДР-*коды. Тогда*

(a) *если $S_0 \subseteq S_1 \cap S_2$ — непустой* 2-*код, то $S_1 = S_2$;*

(b) *если $S_0 \subseteq S_1\backslash S_2$ — непустой* 2-*код, то $S_1 = \Sigma^n\backslash S_2$.*

Доказательство. Докажем (a) индукцией по n. При $n = 1$ утверждение тривиально. Пусть утверждение (a) верно при $n = m - 1$; покажем, что оно выполняется при $n = m$. По предложению 2(a) имеем: $\mathscr{L}_{1;a}S_0$ является 2-кодом, $\mathscr{L}_{1;a}S_1$ и $\mathscr{L}_{1;a}S_2$ суть 2-МДР-коды для всех $a \in \Sigma$. По предложению 2(c) $\mathscr{L}_{1;a}S_0 \subseteq \mathscr{L}_{1;a}S_1 \cap \mathscr{L}_{1;a}S_2$. Тогда по предположению индукции $\mathscr{L}_{1;a}S_1 = \mathscr{L}_{1;a}S_2$ для всех $a \in \Sigma$, для которых множество $\mathscr{L}_{1;a}S_0$ непустое. По определению 2-кода по крайней мере два из четырех множеств $\mathscr{L}_{1;a}S_0$, $a \in \Sigma$, непустые. Если непустыми являются три множества, то равенство $S_1 = S_2$ следует из предложения 2(d). Пусть два множества, например $\mathscr{L}_{1;2}S_0$ и $\mathscr{L}_{1;3}S_0$, пустые. Тогда $\mathscr{L}_{1;0}S_0 = \mathscr{L}_{1;1}S_0$, так как $|\mathscr{E}_1(\bar{x}) \cap S_0| = 2$ для всех $\bar{x} \in S_0$. Следовательно, $\mathscr{L}_{1;0}S_1 = \mathscr{L}_{1;1}S_1 = \mathscr{L}_{1;0}S_2 = \mathscr{L}_{1;1}S_2$ по предположению индукции. Тогда по предложению 2(e) получаем $S_1 = S_2$.

(b) Рассмотрим $S_2' \triangleq \Sigma^n\backslash S_2$. Поскольку S_2' является 2-МДР-кодом и $S_0 \subseteq S_1 \cap S_2'$, из (a) вытекает $S_2' = S_1$. $\square$

§ 2. Линейные 2-коды

Определение. Непустой 2-код $S \subset \Sigma^n$ называется *линейным*, если

$$\chi_S(x_1, \ldots, x_n) \equiv \chi_{S_1}(x_1) \oplus \chi_{S_2}(x_2) \oplus \cdots \oplus \chi_{S_n}(x_n), \tag{1}$$

где S_i $(1 \le i \le n)$ — множества в Σ и $\oplus$ — сложение по модулю 2. Очевидно, что S_i являются 2-МДР-кодами в Σ. Линейный 2-код в Σ^2 изображен на рис. 1(b).

В следующих двух предложениях доказаны элементарные свойства линейных 2-кодов.

Предложение 4 (свойства класса линейных 2-кодов). (a) *Линейные* 2-*коды образуют класс эквивалентности.*

(b) *Линейный* 2-*код является расщепляемым* 2-МДР-*кодом.*

(c) *Дополнение линейного* 2-*кода есть линейный* 2-*код.*

(d) 2-*Код* S *является линейным, если и только если найдется простой* 2-*код* $S_0 \subset S$, *эквивалентный* $\{0,1\}^n$.

(e) *Линейный* 2-*код однозначно определяется подмножеством всех своих вершин вида* $\bar{0}^{(i)}\#y$, $i \in [n]$, $y \in \Sigma$.

(f) *Число линейных* 2-*кодов в* Σ^n *равно* $2 \cdot 3^n$.

Доказательство. Свойства (a)–(c) следуют из определений.

(d) Необходимость. Согласно п. (a) без потери общности можно считать, что $\chi_S(x_1,\dots,x_n) \equiv \bigoplus\limits_{i=1}^{n} \chi_{\{2,3\}}(x_i)$. В этом случае $S_0 \triangleq \{2,3\} \times \{0,1\}^{n-1}$ есть подмножество S.

Достаточность. Пусть 2-код $S_0 \subset S$ эквивалентен множеству $\{0,1\}^n$. Не теряя общности, положим $S_0 = \{2,3\} \times \{0,1\}^{n-1}$. Тогда S_0 есть подмножество линейного 2-кода S', где $\chi_{S'}(x_1,\dots,x_n) \equiv \bigoplus\limits_{i=1}^{n} \chi_{\{2,3\}}(x_i)$. По предложению 3(a) имеем $S = S'$.

(e) Действительно, пусть 2-код S представим в виде (1). Обозначив $\chi^0 \triangleq \chi_S(\bar{0})$ и $\chi^i(y) \triangleq \chi_S(\bar{0}^{(i)}\#y)$, $i \in [n]$, имеем

$$\chi_S(x_1,\dots,x_n) \equiv \chi^0 \oplus \bigoplus_{i=1}^{n} (\chi^i(x_i) \oplus \chi^0), \tag{2}$$

что легко проверить, расписав χ_S по формуле (1).

(f) следует из представления (2). Действительно, χ^0 можно выбрать двумя способами, затем каждую из функций χ^i, $i \in [n]$, — тремя способами, учитывая, что она — характеристическая функция 2-МДР-кода в Σ и $\chi^i(\bar{0}) = \chi^0$. □

Множество $\{0,1\}^n$ (а также граф $\Gamma(\{0,1\}^n)$) называется *булевым* n-*кубом.* Следующее предложение вытекает из определений и предложения 2.

Предложение 5 (наследственные свойства линейных 2-кодов). (a) *Если* $S \subset \Sigma^n$ — *линейный* 2-*код, то* $\mathscr{L}_{k;y}S$ — *линейный* 2-*код.*

(b) *Пусть* $S \subset \Sigma^n$ *есть* 2-*код. Если по какому-либо направлению два слоя* S *линейны и совпадают, то* S — *линейный* 2-*код.*

Основным результатом данного раздела является следующая лемма, которая представляет собой частичное обращение п. (a) и частичное усиление п. (b) предложения 5. В лемме показано, что наличие линейного слоя в расщепляемом 2-МДР-коде влечет наличие по тому же направлению слоя, который является дополнением к первому, — «антислоя».

Лемма 1 (о линейном антислое). *Пусть* $S \subset \Sigma^n$ — *расщепляемый* 2-МДР-*код и* $L \triangleq \mathscr{L}_{k;a}S$ — *линейный* 2-*код для некоторых* $k \in [n]$ *и* $a \in \Sigma$. *Тогда*

(a) *найдется* $b \in \Sigma$ *такое, что* $\mathscr{L}_{k;b}S = \Sigma^{n-1}\backslash L$;

(b) $\Sigma^n\backslash S$ — *расщепляемый* 2-МДР-*код.*

Перед тем как приступить к доказательству леммы 1, введем обозначение $\neg(\alpha_1,\alpha_2,\dots,\alpha_n) \triangleq (\alpha_1 \oplus 1, \alpha_2 \oplus 1, \dots, \alpha_n \oplus 1)$, где $\alpha_i \in \{0,1\}$, и докажем два вспомогательных предложения.

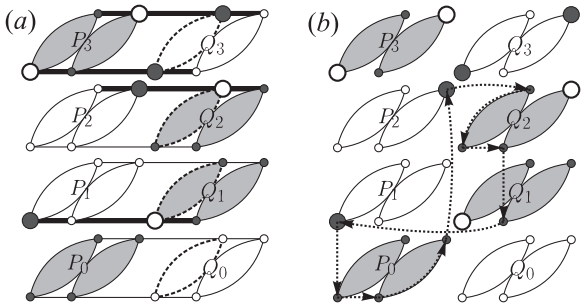

Рис. 2. Иллюстрация к предложению 7.

Предложение 6. *Пусть $\{P_1, P_2, P_3\}$ — разбиение булева n-куба, $n \geq 4$, на три непустых множества: $P_1 \cup P_2 \cup P_3 = \{0,1\}^n$. При этом выполнено условие:*

$(*)$ *для каждого $k \in [n]$ и каждого $b \in \{0,1\}$ хотя бы одно множество (слой) из $\mathscr{L}_{k;b}P_1$, $\mathscr{L}_{k;b}P_2$, $\mathscr{L}_{k;b}P_3$ пустое.*

Тогда $\{P_1, P_2, P_3\} = \{\{\bar\alpha\}, \{\neg\bar\alpha\}, \{0,1\}^n \backslash \{\bar\alpha, \neg\bar\alpha\}\}$, где $\bar\alpha \in \{0,1\}^n$.

Доказательство. Обозначим через $N_i \subseteq [n]$ множество координат k, значения которых не фиксированы в P_i, т. е. $\mathscr{L}_{k;0}P_i \neq \varnothing$ и $\mathscr{L}_{k;1}P_i \neq \varnothing$. Легко видеть, что множества N_1, N_2, N_3 попарно не пересекаются (если, к примеру, $k \in N_1 \cap N_2$, то из условия $(*)$ следует, что $\mathscr{L}_{k;0}P_3 = \varnothing$ и $\mathscr{L}_{k;1}P_3 = \varnothing$, а это противоречит непустоте P_3). Тогда из очевидного соотношения $2^n = |P_1| + |P_2| + |P_3| \leq 2^{|N_1|} + 2^{|N_2|} + 2^{|N_3|}$ вытекает, что $\{N_1, N_2, N_3\} = \{\varnothing, \varnothing, [n]\}$ и $\{P_1, P_2, P_3\} = \{\{\bar\alpha\}, \{\bar\beta\}, \{0,1\}^n \backslash \{\bar\alpha, \bar\beta\}\}$. Из $(*)$ прямо следует, что $\bar\beta = \neg\bar\alpha$. $\square$

Предложение 7. *Пусть S — 2-МДР-код в Σ^n, где $n \geq 3$, и $k \in [n]$. Пусть P_0, P_1, P_2, P_3 — пересечения четырех слоев множества S по k-му направлению с булевым $(n-1)$-кубом, т. е. $P_i \triangleq \mathscr{L}_{k;i}S \cap \{0,1\}^{n-1}$. Предположим, что верно одно из двух утверждений:*

(a) *$n = 3$, $P_i = \{0,1\}^2$ для некоторого i и $P_i \neq \varnothing$ для всех $i \in \{0,1,2,3\}$;*

(b) *$\{P_0, P_1, P_2, P_3\} = \{\{0,1\}^{n-1}, \{\bar\alpha\}, \{\bar\beta\}, \{0,1\}^{n-1} \backslash \{\bar\alpha, \bar\beta\}\}$, где $\bar\alpha \in \{0,1\}^{n-1}$ и $\bar\beta = \neg\bar\alpha$.*

Тогда 2-коды S и $\Sigma^n \backslash S$ нерасщепляемые.

Доказательство. (a) Имеется два неэквивалентных случая выбора множеств P_i. Нетрудно убедиться (оставим это читателю), что в каждом из случаев любая попытка восстановить 2-МДР-код S приводит к нерасщепляемому 2-МДР-коду с нерасщепляемым дополнением.

(b) Без потери общности можно считать, что $k = n$, $\bar\alpha = 0^{n-1}$, $\bar\beta = 1^{n-1}$,

$$P_0 = \{0,1\}^{n-1}, \quad P_1 = \{\bar\alpha\}, \quad P_2 = \{\bar\beta\}, \quad P_3 = \{0,1\}^{n-1} \backslash \{\bar\alpha, \bar\beta\}$$

(иначе, подобрав подходящие перестановку координат и изотопию, можно рассмотреть эквивалентный 2-код, удовлетворяющий этим условиям). Рассуждения будем проводить индукцией по n. База индукции — случай $n = 3$ — рассмотрен в п. (a). Предположим, что предложение верно при $n = m - 1$. Покажем, что оно выполняется и при $n = m$. Рассмотрим пересечения слоев $\mathscr{L}_{k;0}S$, $\mathscr{L}_{k;1}S$, $\mathscr{L}_{k;2}S$, $\mathscr{L}_{k;3}S$ с «соседним» булевому $(n-1)$-кубу $\{0,1\}^{n-1}$ эквивалентным ему множеством $E \triangleq \{2,3\} \times \{0,1\}^{n-2}$:

$$Q_i \triangleq \{2,3\} \times \{0,1\}^{n-2} \cap \mathscr{L}_{1;i}S.$$

Иллюстрации приведены на рис. 2.

(∗) Мы утверждаем, что множества Q_0, Q_1, Q_2, Q_3 определены с точностью до четырех элементов. Точнее,

$$Q_0 = \varnothing, \quad Q_1 = E\backslash\{\bar\alpha'\}, \quad Q_2 = E\backslash\{\bar\beta'\}, \quad Q_3 = \{\bar\alpha'', \bar\beta''\}, \tag{3}$$

где $\bar\alpha', \bar\alpha'' \in \{(2,0,\dots,0),(3,0,\dots,0)\}$ и $\bar\beta', \bar\beta'' \in \{(2,1,\dots,1),(3,1,\dots,1)\}$. Действительно, множество $\{0,1\}^{n-1} \cup E$ разбивается на 1-ребра вида $\mathscr{E}_1(\bar x)$, $\bar x \in \{0\} \times \{0,1\}^{n-2}$. Из того, что S есть 2-МДР-код, следует, что каждое такое 1-ребро содержит две вершины из $P_i \cup Q_i$ для любого $i \in \{0,1,2,3\}$. В частности,

• если такое 1-ребро содержит две вершины из P_i, то оно не содержит вершин из Q_i;

• если оно не содержит вершин из P_i, то содержит две вершины из Q_i.

Согласно (3) эти два правила определяют все вершины множеств Q_i, $i = 0,1,2,3$, за исключением четырех случаев (рис. 2(a), жирные горизонтальные линии):

• 1-ребро $\mathscr{E}_1(0,0,\dots,0)$ содержит ровно одну вершину $(0,0,\dots,0)$ из P_1,

• 1-ребро $\mathscr{E}_1(0,0,\dots,0)$ содержит ровно одну вершину $(1,0,\dots,0)$ из P_3,

• 1-ребро $\mathscr{E}_1(0,1,\dots,1)$ содержит ровно одну вершину $(1,1,\dots,1)$ из P_2,

• 1-ребро $\mathscr{E}_1(0,1,\dots,1)$ содержит ровно одну вершину $(0,1,\dots,1)$ из P_3.

В каждом из этих случаев есть возможность выбора вершины из Q_i для соответствующего i. Этому выбору соответствует выбор вершин $\alpha', \alpha'', \beta', \beta''$. Утверждение (∗) доказано.

Так как S есть 2-МДР-код, то каждая вершина из E принадлежит ровно двум множествам Q_i. Таким образом, из (3) сразу следует, что $\bar\alpha' = \bar\alpha''$ и $\bar\beta' = \bar\beta''$. Без потери общности можно считать, что $\bar\alpha' = \bar\alpha'' = (2,0,\dots,0)$. Таким образом, достаточно рассмотреть два случая: $\bar\beta' = \bar\beta'' = (2,1,\dots,1)$ (рис. 2(a)) и $\bar\beta' = \bar\beta'' = (3,1,\dots,1)$ (рис. 2(b)).

1. Случай $\bar\beta' = \bar\beta'' = (2,1,\dots,1)$ (рис. 2(a)). В этом случае мы можем использовать предположение индукции. Действительно, рассмотрим множество $\Sigma^{n-1}\backslash\mathscr{L}_{1;2}S$. Слои этого множества по последнему направлению в пересечении с булевым $(n-2)$-кубом совпадают с $\{0,1\}^{n-2}$, $\{(0,\dots,0)\}$, $\{(1,\dots,1)\}$ и $\{0,1\}^{n-1}\backslash\{(0,\dots,0),(1,\dots,1)\}$ (см. рис. 2(a), пунктир). По предположению индукции 2-коды $\Sigma^{n-1}\backslash\mathscr{L}_{1;2}S$ и $\mathscr{L}_{1;2}S$ нерасщепляемые. Следовательно, $\Sigma^n\backslash S$ и S также нерасщепляемые.

2. Случай $\bar\beta' = \bar\beta'' = (3,1,\dots,1)$ (рис. 2(b)). В этом случае в графе $\Gamma(S)$ можно указать цикл нечетной длины $2n+3$:

$$\begin{aligned}(0000\dots00,\ &\underbrace{1000\dots00,\ 1100\dots00,\ 1110\dots00,\ \cdots,1111\dots10}_{n-1},\ 1111\dots12,\\ &\underbrace{2111\dots12,\ 2011\dots12,\ 2001\dots12,\ \cdots,\ 2000\dots02}_{n-1},3000\dots02,\\ &3000\dots01,\ 0000\dots01)\end{aligned}$$

(рис. 2(b), пунктир), откуда следует, что этот граф не является двудольным и 2-код S нерасщепляемый по определению. Аналогично нечетный цикл

$$\begin{aligned}(2000\dots00,\ &\underbrace{3000\dots00,\ 3100\dots00,\ 3110\dots00,\ \cdots,3111\dots10}_{n-1},\ 3111\dots12,\\ &\underbrace{0111\dots12,\ 0011\dots12,\ 0001\dots12,\ \cdots,\ 0000\dots02}_{n-1},\ 1000\dots02,\\ &1000\dots01,\ 2000\dots01)\end{aligned}$$

в графе $\Gamma(\Sigma^n\backslash S)$ доказывает нерасщепляемость 2-кода $\Sigma^n\backslash S$. $\square$

Доказательство леммы 1. (a) Покажем утверждение по индукции. Базис индукции — случай $n = 2$ — тривиален. Пусть утверждение леммы верно для $n = m - 1$. Покажем, что оно выполняется при $n = m \geq 3$.

Учитывая сохранение свойств расщепляемости и линейности 2-кода при изотопии и перестановке переменных, а также предложение 4(d), без потери общности можно считать, что $k = n$, $a = 0$ и линейный 2-код L включает $\{0,1\}^{n-1}$. Пусть множества P_0, P_1, P_2 и P_3 определяются, как в предложении 7: $P_i \triangleq \{0,1\}^{n-1} \cap \mathscr{L}_{n;i}S$.

Нам достаточно показать, что хотя бы одно из множеств P_1, P_2, P_3 пустое. Тогда по предложению 3(b) соответствующий слой 2-кода S будет дополнением L.

$(*)$ Предположим противное: каждое из множеств P_1, P_2 и P_3 непустое.

$(**)$ Мы утверждаем, что тогда множества P_1, P_2 и P_3 удовлетворяют условиям предложения 6. Поскольку S есть 2-МДР-код, его слои по данному направлению составляют двукратное покрытие множества Σ^{n-1}, а множества P_0, P_1, P_2 и P_3 — двукратное покрытие множества $\{0,1\}^{n-1}$. Поскольку $P_0 = \{0,1\}^{n-1}$, получаем, что P_1, P_2 и P_3 попарно не пересекаются и $P_1 \cup P_2 \cup P_3 = \{0,1\}^{n-1}$. Осталось показать, что для любых $r \in [n-1]$ и $b \in \{0,1\}$ хотя бы одно множество из $\mathscr{L}_{r;b}P_1$, $\mathscr{L}_{r;b}P_2$, $\mathscr{L}_{r;b}P_3$ пустое. Это следует из индукционного предположения. Действительно, 2-код $\mathscr{L}_{r;b}S$ удовлетворяет всем условиям леммы, и по предположению индукции найдется его слой $\mathscr{L}_{n-1;i}\mathscr{L}_{r;b}S$, $i \in \{1,2,3\}$, являющийся дополнением «линейного» слоя $\mathscr{L}_{n-1;0}\mathscr{L}_{r;b}S$. Используя предложение 2(b),(d) и включение $\mathscr{L}_{n-1;0}\mathscr{L}_{r;b}S \supset \{0,1\}^{n-2}$, получаем

$$\mathscr{L}_{r;b}P_i = \mathscr{L}_{r;b}\big(\{0,1\}^{n-1} \cap \mathscr{L}_{n;i}S\big) = \{0,1\}^{n-2} \cap \mathscr{L}_{r;b}\mathscr{L}_{n;i}S$$
$$= \{0,1\}^{n-2} \cap \mathscr{L}_{n-1;i}\mathscr{L}_{r;b}S = \varnothing.$$

Утверждение $(**)$ доказано.

В силу предложения 6 множество S удовлетворяет условиям предложения 7. Из последнего следует, что 2-код S нерасщепляемый, что противоречит условиям леммы. Таким образом, предположение $(*)$ неверно, и одно из множеств P_1, P_2 и P_3 пустое.

Пусть $P_j = \varnothing$. Тогда $b = j$, $\{0,1\}^{n-1} \subset L\backslash\mathscr{L}_{n;b}S$, откуда $\mathscr{L}_{n;b}S = \Sigma^{n-1}\backslash L$ по предложению 3(b). Утверждение (a) леммы доказано.

(b) Как показано в п. (a), по направлению k два слоя 2-МДР-кода S являются дополнениями друг друга (до Σ^{n-1}). Из определения 2-кода следует, что оставшиеся два слоя также дополняют друг друга. Таким образом, соответствующая перестановка слоев переводит S в его дополнение $\Sigma^n\backslash S$, и из расщепляемости первого следует расщепляемость второго. $\square$

Примеры показывают, что условие линейности слоя в лемме 1 является существенным для наличия в расщепляемом 2-МДР-коде слоя, дополнительного к данному.

§ 3. МДР-коды и n-квазигруппы

Определение. Пусть $G \subseteq \Sigma^n = \{0,1,2,3\}^n$, функция $f : G \to \Sigma$ называется *частичной n-квазигруппой порядка* 4, если уравнение

$$f(\bar{a}^{(i)}\#x) = f(a_1, \ldots a_{i-1}, x, a_{i+1}, \ldots a_n) = b \tag{4}$$

имеет не более одного решения $x \in \Sigma$ при любых $\bar{a} \in \Sigma^n$ и $b \in \Sigma$. Если при этом $G = \Sigma^n$, то функция f называется *n-квазигруппой* порядка 4 (далее слова «порядка 4» будем опускать). В этом случае уравнение (4) будет иметь ровно одно решение при любых $\bar{a} \in \Sigma^n$ и $b \in \Sigma$. Через $f^{\langle i \rangle}$ будем обозначать *обращение* n-квазигруппы f по i-му аргументу, определяемое соотношением

$$f^{\langle i \rangle}(\bar{x}) = b \quad \Longleftrightarrow \quad f(\bar{x}^{(i)} \# b) = x_i.$$

Очевидно, что обращение n-квазигруппы f по произвольному аргументу также будет n-квазигруппой.

Определение. n-Квазигруппа $g : \Sigma^n \to \Sigma$ называется *продолжением* частичной n-квазигруппы $f : G \to \Sigma$, если $f = g|_G$. Частичная n-квазигруппа, которая имеет хотя бы одно продолжение, называется *продолжаемой*.

Определение. n-Квазигруппа f называется *приведенной*, если для всех $i \in [n]$ и $a \in \Sigma$ имеет место равенство $f(\bar{0}^{(i)} \# a) = a$. Перестановку $\tau : \Sigma \to \Sigma$ назовем *приведенной*, если $\tau(0) = 0$.

Определение. n-Квазигруппа f называется *разложимой*, если найдутся целое число m, $2 \leq m < n$, $(n - m + 1)$-квазигруппа h, m-квазигруппа g и перестановка $\sigma : [n] \to [n]$ такие, что

$$f(x_1, \ldots, x_n) \equiv h\left(g(x_{\sigma(1)}, \ldots, x_{\sigma(m)}), x_{\sigma(m+1)}, \ldots, x_{\sigma(n)}\right).$$

Пусть $f : \Sigma^n \to \Sigma$, определим множества

$$C(f) \triangleq \{(\bar{x}, f(\bar{x})) : \bar{x} \in \Sigma^n\},\ C_a(f) \triangleq \{\bar{x} \in \Sigma^n : f(\bar{x}) = a\},\ S_{a,b}(f) \triangleq C_a(f) \cup C_b(f).$$

Из определений вытекает

Предложение 8. (a) *Отображение $C(\cdot)$ — взаимно однозначное соответствие между множеством n-квазигруп и множеством* МДР*-кодов длины $n + 1$.*

(b) *Функция $f : \Sigma^n \to \Sigma$ является n-квазигруппой, если и только если для всех $a \in \Sigma$ множества $C_a(f)$ — попарно не пересекающиеся* МДР*-коды.*

(c) *Функция $f : \Sigma^n \to \Sigma$ является n-квазигруппой, если и только если для любых различных a и b из Σ множество $S_{a,b}(f)$ — расщепляемый* 2-МДР*-код.*

Определение. n-Квазигруппы f и g называются *эквивалентными*, если найдутся перестановка $\sigma : [n] \to [n]$ и $(n + 1)$-изотопия $\bar{\tau} = (\tau_0, \tau_1, \ldots, \tau_n)$ такие, что

$$f(x_1, \ldots, x_n) \equiv \tau_0 g(\tau_1 x_{\sigma(1)}, \ldots, \tau_n x_{\sigma(n)}).$$

Множество n-квазигрупп будем называть *замкнутым относительно эквивалентности*, если оно содержит n-квазигруппы вместе с их классами эквивалентности.

Из определений следует, что если n-квазигруппы f и g эквивалентны, то и МДР-коды $C(f)$ и $C(g)$ эквивалентны. Кроме того, n-квазигруппе f и ее обращению $f^{\langle i \rangle}$, $i \in [n]$, соответствуют эквивалентные МДР-коды $C(f)$ и $C(f^{\langle i \rangle})$. При $n \geq 3$ имеются примеры неэквивалентности n-квазигруппы и ее обращения. Поэтому из эквивалентности МДР-кодов не следует, что соответствующие им n-квазигруппы эквивалентны. Однако легко видеть, что

Предложение 9. (a) *Эквивалентные n-квазигруппы разложимы или неразложимы одновременно.*

(b) *Если n-квазигруппа f разложимая, то и ее обращения $f^{\langle i \rangle}$, $i \in [n]$, разложимые.*

Предложение 10. *Пусть $f : \Sigma^n \to \Sigma$ — n-квазигруппа. Тогда найдутся единственная изотопия $(\tau_0, \tau_1, \dots, \tau_n)$, где $\tau_0 = (0, a)$, $a \in \Sigma$, и приведенные перестановки $\tau_1, \dots, \tau_n : \Sigma \to \Sigma$ такие, что*

$$f(\bar{x}) \equiv \tau_0 g(\tau_1 x_1, \tau_2 x_2, \dots, \tau_n x_n), \tag{5}$$

где g — приведенная n-квазигруппа, $\bar{x} = (x_1, x_2, \dots, x_n)$.

Доказательство. Из (5) получаем, что

$$\begin{gathered} \tau_0(0) = f(0, \dots, 0), \quad \text{т. е. } \tau_0 = (0, f(0, \dots, 0)), \\ \tau_i(b) = \tau_0^{-1} f(\bar{0}^{(i)} \# b), \quad i = 1, \dots, n, \\ g(\bar{x}) = \tau_0^{-1} f\big(\tau_1^{-1} x_1, \tau_2^{-1} x_2, \dots, \tau_n^{-1} x_n\big), \end{gathered} \tag{6}$$

откуда следует единственность представления. С другой стороны, если определить $\tau_0, \tau_1, \dots, \tau_n$ и g равенствами (6), то условия предложения будут выполнены, что легко проверить непосредственно. □

Пусть V_n — множество всех n-квазигрупп порядка 4. Обозначим через $R_n \subseteq V_n$ множество разложимых n-квазигрупп и через $V_n^\star \subset V_n$ — множество приведенных n-квазигрупп. Для произвольного подмножества множества V_n, обозначенного прописной буквой с индексом, например W_n, введем следующие обозначения: $W_n^\star \triangleq W_n \cap V_n^\star$, $w_n \triangleq |W_n|$ и $w_n^\star \triangleq |W_n^\star|$.

Из предложения 10 непосредственно вытекает

Следствие 1. *Пусть $W_n \subseteq V_n$ — замкнутое относительно эквивалентности множество n-квазигрупп порядка 4. Тогда $w_n = 4 \cdot 6^n w_n^\star$.*

Частичную n-квазигруппу $g : G \to \Sigma$ назовем *совместимой* с n-квазигруппой f, если $f(\bar{x}) \neq g(\bar{x})$ для любого $\bar{x}$ из G. Обозначим через $F(g)$ множество всех n-квазигрупп, совместимых с n-квазигруппой g.

Предложение 11. *Пусть g — n-квазигруппа, $W_n \subseteq V_n$ — замкнутое относительно эквивалентности множество n-квазигрупп. Тогда $|F(g) \cap W_n| \leq 3^{n+1} w_n^*$.*

Доказательство. Рассмотрим множество $T \subset \Sigma^n$, состоящее из вершин, отличных от $(0, \dots, 0) \in \Sigma^n$ не более чем в одной позиции. Для каждой частичной n-квазигруппы $t : T \to \Sigma$ рассмотрим множество $W_n(t)$ ее продолжений из класса W_n: $W_n(t) \triangleq \{f \in W_n, f|_T = t\}$. Поскольку множество W_n замкнуто относительно эквивалентности, имеем $|W_n(t)| = w_n^\star$.

Нетрудно видеть, что найдется ровно 3^{n+1} различных частичных n-квазигрупп $t : T \to \Sigma$, совместимых с данной n-квазигруппой g. Поскольку n-квазигруппа $f \in W_n(t)$ совместима с g, только если $t = f|_T$ совместима с g, то количество n-квазигрупп из W_n, совместимых с g, не превосходит $3^{n+1} w_n^\star$. □

Пусть $q : \Sigma^{n-1} \times A \to \Sigma$ — частичная n-квазигруппа, $A \subseteq \Sigma$, α — элемент из A. *Слоем* частичной n-квазигруппы q будем называть подфункцию

$$q_\alpha(x_1, \dots, x_{n-1}) \triangleq q(x_1, \dots, x_{n-1}, \alpha).$$

Из предложения 11 и следствия 1 непосредственно вытекает

Следствие 2. *Пусть U_n — множество частичных n-квазигрупп $g : \Sigma^{n-1} \times \{a, b\} \to \Sigma$ таких, что их слои g_α, $\alpha \in \{a, b\}$, содержатся в замкнутом относительно эквивалентности множестве W_{n-1}. Тогда $|U_n| \leq (3w_{n-1}^2)/2^{n+1}$.*

Предложение 12 (представление разложимой n-квазигруппы суперпозицией ее подфункций). *Пусть h и g суть $(n-m+1)$- и m-квазигруппы и*

$$f(x,\bar y,\bar z)\triangleq h(g(x,\bar y),\bar z),$$
$$h_0(x,\bar z)\triangleq f(x,\bar 0,\bar z),\quad g_0(x,\bar y)\triangleq f(x,\bar y,\bar 0),\quad \delta(x)\triangleq f(x,\bar 0,\bar 0), \tag{7}$$

где $x\in\Sigma$, $\bar y\in\Sigma^{m-1}$, $\bar z\in\Sigma^{n-m}$. Тогда

$$f(x,\bar y,\bar z)\equiv h_0(\delta^{-1}(g_0(x,\bar y)),\bar z). \tag{8}$$

Доказательство. Из (7) следует, что

$$h_0(\cdot,\bar z)\equiv h(g(\cdot,\bar 0),\bar z),\quad g_0(x,\bar y)\equiv h(g(x,\bar y),\bar 0),\quad \delta^{-1}(\cdot)\equiv g^{\langle 1\rangle}(h^{\langle 1\rangle}(\cdot,\bar 0),\bar 0).$$

Подставив эти представления h_0, g_0 и δ^{-1} в тождество (8), легко убедиться в его истинности. □

Предложение 13 (о числе разложимых n-квазигрупп). *Для числа $r_n^\star$ приведенных разложимых n-квазигрупп верна оценка*

$$r_n^\star\le\sum_{m=2}^{n-1}\binom{n}{m}v_{n-m+1}^\star v_m^\star.$$

Доказательство. Из предложения 12 видно, что приведенная разложимая n-квазигруппа может быть представлена (возможно, не единственным образом) в виде суперпозиции приведенных $(n-m+1)$- и m-квазигрупп, где $m\in\{2,\dots,n-1\}$. Для каждого такого m число способов разбить набор переменных на две группы равно $\binom{n}{m}$ и число способов выбрать $(n-m+1)$- и m-квазигруппу равно $v_{n-m+1}^\star$ и $v_m^\star$ соответственно. Порядок переменных в каждой из двух групп несуществен, поскольку при перестановке переменных приведенная m-квазигруппа переходит в приведенную m-квазигруппу. □

§ 4. Полулинейные n-квазигруппы

Определение. n-Квазигруппа f называется *полулинейной*, если найдутся $a,b\in\Sigma$ такие, что $S_{a,b}(f)$ — линейный 2-код. n-Квазигруппа f называется *линейной*, если для всех $a,b\in\Sigma$, $a\ne b$ 2-код $S_{a,b}(f)$ линейный.

Предложение 14. *Приведенная линейная n-квазигруппа единственная.*

Доказательство. Утверждение следует из предложения 4(e) и того факта, что любая n-квазигруппа f однозначно определяется 2-МДР-кодами $S_{0,1}(f)$ и $S_{0,2}(f)$. □

Обозначим через $K_n\subseteq V_n$ множество полулинейных n-квазигрупп, а через $K_n(a,b)$ — множество полулинейных n-квазигрупп f, для которых 2-код $S_{a,b}(f)$ линейный. Легко видеть, что справедливо следующее утверждение.

Предложение 15. *Для любых различных a, b, c из Σ пересечение $K_n(a,b)\cap K_n(a,c)$ есть множество всех линейных n-квазигрупп.*

Из предложения 5(a) индукцией по m нетрудно доказать

Предложение 16. *Пусть f — полулинейная n-квазигруппа. Тогда для любых $(a_1,\dots,a_m)\in\Sigma^m$ функция*

$$g(x_1,\dots,x_{n-m})\triangleq f(x_1,\dots,x_{n-m},a_1,\dots,a_m)$$

является полулинейной m-квазигруппой.

Предложение 17. (a) *Эквивалентные n-квазигруппы являются или не являются полулинейными одновременно.*

(b) *Если f — полулинейная n-квазигруппа, то ее обращения $f^{\langle i\rangle}$, $i \in [n]$, также являются полулинейными n-квазигруппами.*

Доказательство. П. (a) следует из замкнутости относительно эквивалентности множества линейных 2-кодов (предложение 4(a)).

Докажем п. (b). Непосредственно проверяется, что полулинейность f эквивалентна тому, что найдутся $a_0 = a$, $b_0 = b$, $a_1, \ldots, a_n$, $b_1, \ldots, b_n$ такие, что $a_i \neq b_i$ и

$$\bigoplus_{i=0}^{n} \chi_{\{a_i,b_i\}}(x_i) = 0 \tag{9}$$

для любых $x_0, x_1, \ldots, x_n$, удовлетворяющих равенству $x_0 = f(x_1, x_2, \ldots, x_n)$. Поскольку выражение (9) симметрично относительно выбора зависимой переменной, получаем требуемое утверждение. □

Замечание. Приведенную линейную n-квазигруппу f можно представить в виде $f(x_1, \ldots, x_n) = x_1 * \cdots * x_n$, где $(\Sigma, *)$ — группа, изоморфная $Z_2 \times Z_2$, с таблицей сложения

$*$	0	1	2	3
0	0	1	2	3
1	1	0	3	2
2	2	3	0	1
3	3	2	1	0

Следующие две леммы доказаны в [3, 4]. Первая — о представлении непростого 2-МДР-кода через простые 2-коды меньших размерностей. Вторая лемма — необходимое нам следствие первой — связывает свойство разложимости n-квазигруппы q со свойством множества $S_{c,d}(q)$ быть непростым.

Лемма 2 (о разложении 2-МДР-кода) [3, 4]. *Пусть S — 2-МДР-код. Тогда найдется $k = k(S) \in [n]$ такое, что*

(a) *характеристическая функция χ_S представляется в виде*

$$\chi_S(\bar{x}) \equiv \bigoplus_{j=1}^{k} \chi_{S_j}(\tilde{x}_j), \tag{10}$$

где $\tilde{x}_j = (x_{i_{j,1}}, \ldots, x_{i_{j,n_j}})$ — непересекающиеся наборы переменных из $\bar{x}$, $S_j \subset \Sigma^{n_j}$ — простые 2-МДР-коды при $j \in [k]$; представление единственно с точностью до замены некоторых 2-МДР-кодов S_j на 2-МДР-коды $S_j \backslash \Sigma^{n_j}$;

(b) *S — объединение 2^{k-1} попарно не пересекающихся простых 2-кодов одинаковой мощности; $\Sigma^n \backslash S$ — объединение 2^{k-1} попарно не пересекающихся простых 2-кодов одинаковой мощности.*

Лемма 3 (о разложимости n-квазигрупп) [3, 4]. *Пусть $S \subset \Sigma^n$ — 2-МДР-код, удовлетворяющий равенству* (10)*, $c \neq d \in \Sigma$ и q — n-квазигруппа такая, что $S_{c,d}(q) = S$. Тогда*

$$q(\bar{x}) \equiv q_0(q_1(\tilde{x}_1), \ldots, q_k(\tilde{x}_k)), \tag{11}$$

где q_j — n_j-квазигруппы при $j \in [k]$, q_0 — полулинейная k-квазигруппа, а наборы переменных $\tilde{x}_j = (x_{i_{j,1}}, \ldots, x_{i_{j,n_j}})$, $j \in [k]$, и числа k, n_j определяются леммой 2.

Следствие 3. *Пусть* $\{a,b,c,d\}=\Sigma$, q *есть* n*-квазигруппа и частичная* n*-квазигруппа* $g\triangleq q|_{\Sigma^{n-1}\times\{a,b\}}$ *имеет более двух продолжений. Тогда* $q\in R_n\cup K_n$.

Доказательство. Из определений следует, что $C_a(f^{\langle n\rangle})=C(f_a)$ для произвольной n-квазигруппы f и ее обращения по n-му аргументу $f^{\langle n\rangle}$. Пусть

$$S\triangleq\Sigma^n\backslash(C(g_a)\cup C(g_b)).$$

Тогда для любого продолжения f частичной n-квазигруппы g верно

$$S=\Sigma^n\backslash(C(f_a)\cup C(f_b))=C(f_c)\cup C(f_d)=S_{c,d}(f^{\langle n\rangle}).$$

По условию частичная n-квазигруппа g имеет более двух продолжений f. Каждое из продолжений однозначно определяется слоем f_c. Значит, 2-МДР-код S включает более двух различных МДР-кодов $C(f_c)$. По предложению 1 2-МДР-код $S=S_{c,d}(q^{\langle n\rangle})$ состоит более чем из одного простого 2-кода. Согласно леммам 2 и 3 число k в представлении (11) не меньше 2. Если $k<n$, то из (11) следует разложимость $q^{\langle n\rangle}$, если $k=n$, то из (10) — полулинейность. Таким образом, $q^{\langle n\rangle}\in K_n\cup R_n$, и по предложениям 9(b) и 17(b) получаем $q\in K_n\cup R_n$. □

§ 5. О числе n-квазигрупп

В данном параграфе мы оценим число n-квазигрупп порядка 4, установив, что подкласс полулинейных n-квазигрупп является асимптотически самым мощным. Сначала вычислим количество полулинейных n-квазигрупп.

Теорема 1 (о числе полулинейных n-квазигрупп). *Имеют место равенства* $k_n^\star=3\cdot 2^{2^n-n-1}-2$, $k_n=3^{n+1}\cdot 2^{2^n+1}-2^3 6^n$.

Доказательство. Произвольную n-квазигруппу f из $K_n^\star(0,1)$ можно задать, сначала выбрав линейный 2-код $S_{0,1}(f)$, затем МДР-коды $C_0(f)\subset S_{0,1}(f)$ и $C_2(f)\subset\Sigma^n\backslash S_{0,1}(f)$. Линейный 2-код можно выбрать $2\cdot 3^n$ способами (предложение 4(f)), МДР-код в нем — $2^{2^{n-1}}$ способами (предложение 1). Таким образом,

$$|K_n(0,1)|=2\cdot 3^n\cdot 2^{2^{n-1}}\cdot 2^{2^{n-1}}=3^n\cdot 2^{2^n+1}.$$

По следствию 1 получаем $|K_n^\star(0,1)|=2^{2^n-n-1}$ и аналогично

$$|K_n^\star(0,2)|=|K_n^\star(0,3)|=2^{2^n-n-1}.$$

Из предложений 14, 15 следует, что попарные пересечения множеств $K_n^\star(0,1)$, $K_n^\star(0,2)$, $K_n^\star(0,3)$ содержат единственный элемент. Тогда по формуле включения-исключения

$$k_n^\star=|K_n^\star(0,1)\cup K_n^\star(0,2)\cup K_n^\star(0,3)|=3\cdot 2^{2^n-n-1}-3+1.$$

По следствию 1 имеем $k_n=4\cdot 6^n k_n^\star$. □

Замечание. Нижняя оценка $v_n\geq 3^{n+1}\cdot 2^{2^n+1}-2^3 6^n$ получена в [5].

В результате численного эксперимента получены значения

$$v_1^\star=1,\quad v_2^\star=4,\quad v_3^\star=64\quad[6],\quad v_4^\star=7132,\quad v_5^\star=201538000.\qquad(12)$$

Следующая лемма показывает, что наличие одного полулинейного слоя в n-квазигруппе влечет упорядочивание ее структуры.

Лемма 4 (о полулинейном слое). *Пусть q есть n-квазигруппа и найдется $\alpha \in \Sigma$ такое, что $q_\alpha \in K_{n-1}$. Тогда $q \in K_n \cup R_n$.*

Доказательство. Пусть для некоторого $\alpha \in \Sigma$ справедливо $q_\alpha \in K_{n-1}$ и, следовательно, 2-МДР-код $S_{a,b}(q_\alpha)$ линейный при некоторых $a, b \in \Sigma$. Рассмотрим $S_{a,b}(q)$, $S_{a,b}(q_\alpha) = \mathscr{L}_{n;\alpha}(S_{a,b}(q))$. Тогда по лемме 1 найдется $\beta \in \Sigma$, $\beta \neq \alpha$, такое, что

$$S_{a,b}(q_\beta) = \mathscr{L}_{n;\beta}(S_{a,b}(q)) = \Sigma^{n-1} \backslash S_{a,b}(q_\alpha),$$

т. е. $(n-1)$-квазигруппа q_β полулинейная.

$(*)$ Мы утверждаем, что у частичной n-квазигруппы $g \triangleq q|_{\Sigma^{n-1} \times \{\alpha,\beta\}}$ найдутся два полулинейных продолжения. Пусть $\{a, b, c, d\} = \{\alpha, \gamma, \beta, \delta\} = \Sigma$ и $\sigma \triangleq (ab)(cd)$ — перестановка символов Σ. Тогда функция f, определенная равенствами

$$f(x_1, \ldots, x_{n-1}, \alpha) \triangleq q(x_1, \ldots, x_{n-1}, \alpha),\ f(x_1, \ldots, x_{n-1}, \beta) \triangleq q(x_1, \ldots, x_{n-1}, \beta),$$

$$f(x_1, \ldots, x_{n-1}, \gamma) \triangleq \sigma q(x_1, \ldots, x_{n-1}, \alpha),\ f(x_1, \ldots, x_{n-1}, \delta) \triangleq \sigma q(x_1, \ldots, x_{n-1}, \beta),$$

является продолжением частичной n-квазигруппы g. Очевидно, что $S_{a,b}(f_\gamma) = S_{a,b}(f_\alpha) = S_{a,b}(q_\alpha)$, поэтому 2-коды $\mathscr{L}_{n;\alpha}(S_{a,b}(f)) = \mathscr{L}_{n;\gamma}(S_{a,b}(f))$ линейные, а значит, по предложению 5(b) и 2-код $S_{a,b}(f)$ линейный. Таким образом, n-квазигруппы f и $f'(\bar{x}) \triangleq f(x_1, \ldots, x_{n-1}, \tau(x_n))$, где $\tau \triangleq (\gamma, \delta)$, доказывают $(*)$.

В заключение заметим, что либо q совпадает с f или f' и тогда $q \in K_n$, либо g имеет более двух продолжений $(q,\ f,\ f')$ и тогда $q \in K_n \cup R_n$ по следствию 3. $\square$

Теорема 2 (о числе n-квазигрупп). *Если $n \geq 5$, то*

$$3^{n+1} 2^{2^n+1} \leq v_n \leq (3^{n+1} + 1) 2^{2^n+1}.$$

Доказательство. Пусть $q \in V_n$, рассмотрим частичную n-квазигруппу $g_{\alpha,\beta} = q|_{\Sigma^{n-1} \times \{\alpha,\beta\}}$ для произвольных $\alpha, \beta \in \Sigma$. Пусть частичная n-квазигруппа $g_{\alpha,\beta}$ имеет более двух продолжений, тогда из следствия 3 имеем $q \in K_n \cup R_n$. Пусть $q_\alpha \in K_{n-1}$ или $q_\beta \in K_{n-1}$, тогда по лемме 4 $q \in K_n \cup R_n$. Следовательно, если $q \notin K_n \cup R_n$, то для всех $\alpha, \beta \in \Sigma$ будет $q_\alpha, q_\beta \notin K_{n-1}$ и частичная n-квазигруппа $g_{\alpha,\beta}$ имеет два продолжения.

Введем обозначения $T_n \triangleq V_n \backslash K_n$ и $W_n \triangleq T_n \backslash R_n$. Из предложений 9(a) и 17(a) следует, что множества T_n и W_n замкнуты относительно эквивалентности. Тогда если $q \in W_n$, то $q_\alpha \in T_n$ для всех $\alpha \in \Sigma$ и по следствию 2

$$w_n \leq \frac{3 t_{n-1}^2}{2^n}. \tag{13}$$

$(*)$ Мы утверждаем, что верны три неравенства, доказательство которых проведем индукцией по n:

(a) $k_n^\star \leq v_n^\star \leq 2 k_n^\star$ при $n \geq 1$,

(b) $t_n \leq 2^{2^n+1}$ при $n \geq 5$,

(c) $v_n \leq (3^{n+1} + 1) 2^{2^n+1}$ при $n \geq 5$.

При $n \leq 5$ условия (a)–(c) проверяются исходя из точных значений для $k_n^\star$, $v_n^\star$, v_n, $t_n = v_n - k_n$ ((12), теорема 1). По предположению индукции (a) верно для $n \in [m]$, а (b), (c) — для $n = m \geq 5$. Покажем справедливость неравенств

(a)–(c) при $n = m+1$. Из неравенства (a) и теоремы 1 при $m \geq 5$, $m-1 > i > 2$ следует неравенство

$$v^\star_{m-i+1}v^\star_i \leq 4k^\star_{m-i+1}k^\star_i < 4 \cdot 9 \cdot 2^{2^{m-i+1}+2^i-m-3} < 4 \cdot 3 \cdot 2^{2^{m-1}-m-1} = v^\star_2 k^\star_{m-1} \leq v^\star_{m-1}v^\star_2.$$

Поскольку $v^\star_2 = 4$, из оценки для числа $r^\star_n$ (предложение 13) имеем

$$r^\star_{m+1} \leq \sum_{i=2}^{m} \binom{m+1}{i} v^\star_{(m+1)-i+1}v^\star_i \leq \sum_{i=2}^{m} \binom{m+1}{i} v^\star_m v^\star_2 < 2^{m+1} \cdot v^\star_m \cdot 4.$$

Подставляя (c) при $n = m$, получаем

$$r_{m+1} < 2^{m+3}(3^{m+1}+1)2^{2^m+1} < 2^{2^{m+1}}. \tag{14}$$

Кроме того, из неравенств (13) и (b) при $n = m$ приходим к неравенству

$$w_{m+1} \leq \frac{3t_m^2}{2^{m+1}} \leq \frac{3 \cdot 2^{2^{m+1}+2}}{2^{m+1}} < 2^{2^{m+1}}. \tag{15}$$

Из определений множеств T_m и W_m имеем $t_{m+1} \leq w_{m+1} + r_{m+1}$ и $v_{m+1} = t_{m+1} + k_{m+1}$. Тогда из неравенств (14) и (15) выводим неравенство (b) при $n = m+1$, а из теоремы 1 и неравенства (b) — неравенства (a) и (c) при $n = m+1$. Утверждение $(*)$ доказано.

Осталось доказать нижнюю оценку для числа v_n. Покажем сначала, что при $n \geq 4$ справедливо неравенство

$$t^\star_n \geq t^\star_3 v^\star_{n-2}. \tag{16}$$

Пусть $g \in T^\star_3$ и $h \in V^\star_{n-2}$. Тогда из предложения 16 следует, что n-квазигруппа

$$f(x_1, \ldots, x_n) \triangleq h(g(x_1, x_2, x_3), x_4, \ldots, x_n)$$

не является полулинейной. Нетрудно проверить, что различным парам из приведенных $(n-2)$-квазигруппы h и 3-квазигруппы g соответствуют различные приведенные n-квазигруппы f. Неравенство (16) доказано.

Из (12) и теоремы 1 вытекает, что $t^\star_3 = 18$. Тем самым из неравенства (16) и теоремы 1 имеем $v^\star_n = k^\star_n + t^\star_n \geq 3^n 2^{2^n-n-1}$ при $n \geq 4$. Тогда из следствия 1 получаем неравенство $v_n \geq 3^{n+1}2^{2^n+1}$ при $n \geq 4$. $\square$

Из теоремы 2 и предложения 8 непосредственно вытекает

Следствие 4 (асимптотики числа n-квазигрупп и числа МДР-кодов). *Пусть m_n — число* МДР-*кодов в Σ^n и v_n — число n-квазигрупп порядка* 4. *Тогда*

$$v_n = 3^{n+1}2^{2^n+1}(1+o(1)), \quad m_n = 3^n 2^{2^{n-1}+1}(1+o(1)).$$

ЛИТЕРАТУРА

1. *Белоусов В. Д.* n-Арные квазигруппы. Кишинев: Штиинца, 1972.
2. *Krotov D. S., Potapov V. N.* On the reconstruction of n-quasigroups of order 4 and the upper bounds on their number // Proc. conf. devoted to the 90th anniversary of Alexei A. Lyapunov. Novosibirsk, Russia, October 8–11, 2001. P. 323–327. [http://www.sbras.ru/ws/Lyap2001/2363]

3. *Krotov D. S.* On decomposition of $(n, 4^{n-1}, 2)_4$ MDS codes and double-codes // Proc. Eighth Intern. workshop on algebraic and combinatorial coding theory (ACCT-VIII), Sept. 8–14, 2002, Tsarskoe Selo, Russia. P. 168–171.

4. *Krotov D. S.* On decomposability of 4-ary distance 2 MDS codes, double-codes, and n-quasigroups of order 4 // arXiv.org eprint math.CO/0509358, 2005. Available from: http://arxiv.org/abs/math/0509358. (Submitted to Discrete Mathematics).

5. *Кротов Д. С.* Нижние оценки числа m-квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 2000. Т. 7, № 2. С. 47–53.

6. *Mullen G. L., Weber R. E.* Latin cubes of order ≤ 5 // Discrete Math. 1988. V. 32, N 3. P. 291–298.

Статья поступила 14 мая 2005 г., окончательный вариант — 31 января 2006 г.

Потапов Владимир Николаевич, Кротов Денис Станиславович
Институт математики им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4, Новосибирск 630090
vpotapov@math.nsc.ru, krotov@math.nsc.ru