ПРОБЛЕМЫ ПЕРЕДАЧИ ИНФОРМАЦИИ

Том 55 **2019** **Вып. 4**

УДК 621.391.1 : 519.1

© 2019 г. **Д.С. Кротов, В.Н. Потапов**

О СПЕКТРЕ МОЩНОСТЕЙ И ЧИСЛЕ ЛАТИНСКИХ БИТРЕЙДОВ ПОРЯДКА 3[1, 2]

Унитрейдом (латинским) порядка k называется подмножество вершин графа Хэмминга $H(n,k)$, которое либо пересекается по двум вершинам, либо совсем не пересекается с любой максимальной кликой. Битрейдом называется двудольный, т.е. разделяющийся на два независимых подмножества, унитрейд. Исследуется спектр мощностей битрейдов в графе Хэмминга $H(n,k)$ при $k=3$ (троичном гиперкубе) и рост числа таких битрейдов с ростом n. В частности, определены все возможные малые (до $2{,}5\cdot 2^n$) и большие (от $14\cdot 3^{n-3}$) мощности битрейдов размерности n и доказано, что мощность битрейда принимает значения, только сравнимые с 0 или 2^n по модулю 3 (этот результат имеет трактовку в терминах троичного кода типа Рида – Маллера). Часть результатов применима для произвольного k. Доказано, что при $k=3$ и растущем n число неэквивалентных битрейдов не меньше $2^{(2/3-o(1))n}$ и не больше 2^{α^n}, $\alpha<2$ (порядок роста двойного логарифма от этого числа остается неизвестным). Альтернативно исследуемое множество B_n битрейдов порядка 3 можно определить следующим образом: B_0 состоит из трех чисел $-1,0,1$; B_n состоит из всех упорядоченных троек (a,b,c) элементов из B_{n-1}, таких что $a+b+c=0$.

Ключевые слова: латинские битрейды, унитрейды, коды Рида – Маллера, комбинаторные конфигурации, булевы функции.

DOI: 10.1134/S0555292319040028

§ 1. Введение

Для комбинаторных объектов (конфигураций) различного типа оказывается полезно вводить понятие битрейда так, чтобы определение битрейда не опиралось непосредственно на определение исходных объектов, но включало всевозможные разности (например, симметрические) объектов этого типа (см. [1]). Битрейды отражают возможную разницу между двумя комбинаторными конфигурациями одного и того же типа, что важно при перечислении, описании и исследовании свойств комбинаторных конфигураций. Известны исследования битрейдов (или трейдов) комбинаторных блок-дизайнов [2–6], латинских квадратов [7], обобщенных дизайнов в частично упорядоченных множествах [8], совершенных кодов [9, 10], корреляционно-иммунных булевых функций и бент-функций [11]. В настоящей статье рассматриваются латинские битрейды, соответствующие МДР-кодам с расстоянием 2, или (что

[1] Работа выполнена за счет грантов Российского научного фонда № 14-11-00555 (результаты §§ 2, 3 и пп. 4.1, 4.5, 5.2) и № 18-11-00136 (результаты пп. 4.2–4.4, 4.6, 5.1).

[2] Результаты работы были частично представлены на конференциях International Conference and PhD–Master Summer School “Groups and Graphs, Metrics and Manifolds” G2M2, Yekaterinburg, July 22–30, 2017, International Workshop on Algebraic Combinatorics, Hefei, China, November 22–25, 2018, и 3rd Hungarian–Russian Combinatorics Workshop, Moscow, May 20–22, 2019.

эквивалентно) латинским гиперкубам, или полиадическим квазигруппам. Исследован спектр возможных мощностей битрейдов и получены оценки их числа.

Перейдем к формальным определениям. Пусть $Q_k = \{0, \dots, k-1\}$. Определим расстояние Хэмминга $d(u, v)$ как число несовпадающих компонент в наборах $u, v \in Q_k^n$. Метрическое пространство (Q_k^n, d), а также граф ΓQ_k^n расстояний 1 на множестве вершин Q_k^n, называется k-ичным n-мерным гиперкубом или графом Хэмминга. Весом вершины $u \in Q_k^n$ называется величина $\mathrm{wt}(u) = d(u, \bar{0})$, где $\bar{0}$ – набор из n нулей (далее также используются аналогичные обозначения $\bar{1}$, $\overline{-1}$). Гранью в Q_k^n называется множество вершин гиперкуба, полученное фиксацией значений одной или нескольких координат. Множество $U \subset Q_k^n$ называется *унитрейдом* (*размерности* n), если мощности его пересечений с одномерными гранями (максимальными кликами в ΓQ_k^n) принимают только два значения 0 и 2. Обычно битрейдом называется пара $\{U_0, U_1\}$, состоящая из двух независимых долей двудольного унитрейда $U = U_0 \cup U_1$. Но нам будет удобно называть *битрейдом* такой унитрейд $U \subset Q_k^n$, что подграф ΓU, порожденный множеством вершин U, является двудольным. В двумерном случае ($n = 2$) любой унитрейд является битрейдом. Действительно, из теоремы Кёнига следует, что любая квадратная $(0,1)$-матрица, содержащая одинаковое число единиц в каждом столбце и каждой строке, содержит диагональ. Значит, таблица характеристической функции двумерного унитрейда, которую можно рассматривать как $(0,1)$-матрицу, после удаления нулевых строк и столбцов содержит две непересекающиеся диагонали из единиц. При $n \geqslant 3$ и $k \geqslant 3$ имеются унитрейды, которые не являются битрейдами. Минимальный пример приведен ниже, в нем три двумерные таблицы соответствуют трем параллельным гиперграням трехмерного унитрейда:

$$\begin{array}{|c|c|c|}\hline \mathbf{1} & \mathbf{1} & 0 \\ \hline \mathbf{1} & 0 & \mathbf{1} \\ \hline 0 & \mathbf{1} & \mathbf{1} \\ \hline \end{array}, \quad \begin{array}{|c|c|c|}\hline 0 & \mathbf{1} & \mathbf{1} \\ \hline \mathbf{1} & 0 & \mathbf{1} \\ \hline \mathbf{1} & \mathbf{1} & 0 \\ \hline \end{array}, \quad \begin{array}{|c|c|c|}\hline \mathbf{1} & 0 & \mathbf{1} \\ \hline 0 & 0 & 0 \\ \hline \mathbf{1} & 0 & \mathbf{1} \\ \hline \end{array}. \tag{1}$$

Рассмотрим соответствие между данным выше определением и общим понятием битрейда. *МДР-кодом* называется подмножество гиперкуба Q_k^n, пересекающееся с каждой гранью фиксированной размерности r ровно по одному элементу. Нетрудно видеть, что МДР-коды – это коды с минимальным расстоянием между вершинами $r+1$ и максимальной для этого кодового расстояния мощностью k^{n-r}, т.е. коды, достигающие границы Синглтона. В данном контексте нас интересуют только МДР-коды с кодовым расстоянием 2, т.е. когда $r = 1$. (Функция, выражающая значение одной из координат вершин такого кода через значения $n-1$ оставшихся, называется латинским $(n-1)$-кубом, в случае $n = 3$ – латинским квадратом, а алгебраическая система с такой функцией в качестве операции – $(n-1)$-арной квазигруппой). Из определений видно, что симметрическая разность двух МДР-кодов является битрейдом.

Группа изометрий гиперкуба Q_k^n порождается группой перестановок координат и группой изотопий, т.е. перестановок элементов Q_k в каждой координате. В случае $k = 3$ группа изометрий Q_3^n состоит только из аффинных преобразований гиперкуба Q_3^n как n-мерного векторного пространства над полем $\mathrm{GF}(3)$. Подмножества гиперкуба, которые можно перевести друг в друга изометриями пространства, называются *эквивалентными*. *Ретрактом* множества $U \subset Q_k^n$ будем называть подмножество гиперкуба Q_k^{n-1}, полученное как пересечение множества U с некоторой гранью размерности $n-1$. Направлением ретракта или гиперграни будем называть номер зафиксированной в этой грани координаты. Из определений следуют

Предложение 1. *Любой ретракт унитрейда* (*битрейда*, *МДР-кода*) *является унитрейдом* (*битрейдом*, *МДР-кодом*) *в гиперкубе меньшей размерности.*

Предложение 2. *Образ унитрейда* (*битрейда*, *МДР-кода*) *при изометрии гиперкуба является унитрейдом* (*битрейдом*, *МДР-кодом*).

В статье мы почти полностью ограничиваемся рассмотрением битрейдов в Q_3^n. Этот случай представляется нам ключевым, поскольку любой троичный битрейд можно изометрично вложить в гиперкуб большего порядка Q_k^n, $k \geqslant 4$, таким образом, ответ на многие вопросы в общем случае представляется не проще, чем для случая $k = 3$. Одним из таких вопросов является проблема асимптотики двойного логарифма числа объектов при фиксированном k и растущем n, причем именно для случая $k = 3$ эта проблема наиболее ярко выражена: имеющаяся нижняя оценка числа битрейдов не доказывает, что это величина дважды экспоненциальна, в то время как верхняя оценка близка к тривиальной 2^{2^n} (от которой нам все же удалось несколько оторваться в настоящей статье, см. теорему 8 ниже). Для других порядков, $k > 3$, дважды экспоненциальная нижняя оценка достигается за счет свитчинговой конструкции, основанной на возможности разместить в рассматриваемом пространстве непересекающиеся битрейды (см. нижние оценки для числа латинских гиперкубов в [12, 13]). С одной стороны, ограниченное число "степеней свободы" латинских битрейдов порядка 3 позволяет надеяться на построение стройной комбинаторно-алгебраической теории этих объектов (попытка такого построения представлена в настоящей статье), с другой стороны, сложность некоторых вопросов полностью раскрывается уже для этого малого порядка.

Для исследования унитрейдов в статье используются методы линейной алгебры (§ 2 и п. 4.2), теории булевых функций (§ 3) и теории кодирования (§ 3 и п. 4.1). В частности, показана связь задачи описания троичных битрейдов с задачей нахождения полиномиальной сложности булевой функции [14, 15]. Известна также связь троичных битрейдов с почти уравновешенными булевыми функциями (предложение 7).

В § 4 исследуется спектр мощностей троичных битрейдов, а также унитрейдов и битрейдов бóльших порядков. Показано, что мощность любого троичного битрейда размерности n сравнима с 0 или 2^n по модулю три. Минимальная мощность непустого битрейда (не только троичного) размерности n равна 2^n. Все возможные мощности битрейдов, не превышающие $2 \cdot 2^n$, были известны ранее (см. [16]). В настоящей статье указана связь спектра мощностей битрейдов с весовым спектром двоичного кода Рида – Маллера (предложение 9). Кроме того, определены все возможные мощности унитрейдов и битрейдов размерности n от минимальной 2^n до $2{,}5 \cdot 2^n$ (теоремы 1, 5, следствие 7). Троичным битрейдом максимальной мощности $2 \cdot 3^{n-1}$ является пара непересекающихся МДР-кодов. Как известно (см., например, [17]) имеется единственный (с точностью до эквивалентности) троичный битрейд такой мощности. Отметим, что уже для порядка 4 имеется дважды экспоненциальное число неэквивалентных битрейдов максимальной мощности $2 \cdot 4^{n-1}$ (см. [13, 17]).

Одной из основных задач исследования битрейдов является определение их числа как функции от размерности n и порядка k. Благодаря тому, что битрейды соответствуют разностям комбинаторных объектов, исследование разнообразия битрейдов открывает перспективы исследования разнообразия исходных объектов и оценки их числа. Для латинских гиперкубов (порядка больше 4) размерности n, с которыми связаны исследуемые нами битрейды, до сих пор неизвестен даже порядок роста логарифма числа при $n \to \infty$ (см. [13]). В [16] была получена почти экспоненциальная ($e^{\Omega(\sqrt{n})}$) асимптотическая нижняя оценка числа неэквивалентных битрейдов в Q_3^n. В п. 5.1 доказана нижняя оценка $2^{(2/3-o(1))n}$ числа неэквивалентных битрейдов в Q_3^n при $n \to \infty$ (теорема 7) и показано, что подобным нашему методом нельзя получить нижнюю оценку выше экспоненциальной (теорема 6). В п. 5.2 получена верхняя оценка вида 2^{α^n}, $\alpha < 2$, для числа битрейдов в Q_3^n (теорема 8), которая существенно улучшает тривиальную верхнюю оценку 2^{2^n}. Однако вопрос о скоро-

сти роста числа троичных битрейдов размерности n остается открытым: неизвестно даже, является ли эта функция экспоненциальной или дважды экспоненциальной по n. Результаты численного эксперимента для малых n, представленные в таблице в п. 4.5, показывают рост быстрее экспоненциального, но вывод о линейном росте двойного логарифма числа представляется пока поспешным.

Метод доказательства верхней оценки связан с тем, что в гиперкубе Q_3^n при $n \geqslant 7$ удалось указать множество мощности строго больше $3^n - 2^n$, которое не включает в себя ни одного битрейда и даже симметрических разностей двух битрейдов. Для более известной задачи о максимальном подмножестве гиперкуба без арифметической прогрессии (что в троичном гиперкубе совпадает с подмножеством, не включающем одномерного аффинного подпространства) недавно была получена асимптотическая верхняя оценка вида $o(\alpha^n)$, где $\alpha < 3$ (см. [18]). Нахождение в троичном гиперкубе подмножества максимальной мощности, которое не включает битрейдов, остается актуальной задачей.

Завершая § 1, опишем рекурсивно класс B_n объектов, который определяется очень естественно и оказывается эквивалентен классу латинских битрейдов порядка 3 (данная формулировка приводится с иллюстративной целью и нигде в тексте больше не используется):

$$B_0 = \{-1, 0, 1\}, \quad B_n = \{(a, b, c) \in B_{n-1}^3 \mid a + b + c = 0\}.$$

Если представлять элементы класса B_n как n-мерные таблицы, заполненные числами $-1, 0, 1$, то множество ячеек с ненулевыми значениями в такой таблице как раз и образует битрейд.

§ 2. Линейные пространства

Пусть $\mathbb{F}$ – некоторое поле. Рассмотрим множество функций $\{g\colon Q_k^n \to \mathbb{F}\}$ как векторное пространство над полем $\mathbb{F}$. Обозначим через $\mathbb{V}_{n,k}(\mathbb{F})$ подпространство, состоящее из функций, сумма значений которых по любой одномерной грани (максимальной клике в графе ΓQ_k^n) равна 0. Рассмотрим битрейд $B \subset Q_k^n$. Ему соответствует функция $b[B]\colon Q_k^n \to \{0, \pm 1\}$, которая на одной доле битрейда принимает значение 1, на другой – значение -1, а в остальных вершинах равна 0. Рассмотрим $\{0, \pm 1\}$ как подмножество поля $\mathbb{F}$ (для поля характеристики 2 имеем $-1 = 1$). Очевидно, $b[B] \in \mathbb{V}_{n,k}(\mathbb{F})$. Характеристическая функция унитрейда содержится в $\mathbb{V}_{n,k}(\mathbb{F})$ в случае, когда поле $\mathbb{F}$ имеет характеристику 2.

Введем следующий частичный порядок $\preceq$ на Q_k: элемент $k-1$ будем считать максимальным, а все остальные элементы из Q_k несравнимыми друг с другом. Распространим частичный порядок на Q_k^n. Пусть $(x_1, \ldots, x_n), (y_1, \ldots, y_n) \in Q_k^n$. Введем обозначение $(x_1, \ldots, x_n) \preceq (y_1, \ldots, y_n)$, если для любого $i \in \{1, \ldots, n\}$ верно, что $x_i \preceq y_i$. Отметим, что множество $G_y = \{x \in Q_k^n \mid x \preceq y\}$ является гранью гиперкуба Q_k^n размерности, равной числу символов $k-1$ в наборе y.

Покажем, что $\dim \mathbb{V}_{n,k}(\mathbb{F}) = (k-1)^n$. Пусть $f \in \mathbb{V}_{n,k}(\mathbb{F})$. Сумма значений функции f по каждой грани любой ненулевой размерности равна нулю, поэтому

$$f(y) = -\sum_{x \in Q_{k-1}^n,\, x \preceq y} f(x) \quad \text{при } y \in Q_k^n \setminus Q_{k-1}^n. \tag{2}$$

Следовательно, для определения функции $f \in \mathbb{V}_{n,k}(\mathbb{F})$ необходимо и достаточно определить ее на всех минимальных элементах, т.е. на Q_{k-1}^n. Построим семейство линейно независимых функций той же мощности. Пусть $x \in Q_{k-1}^n$. Рассмотрим множество $B_x = \{y \in Q_k^n \mid x \preceq y\}$. Нетрудно видеть, что граф ΓB_x изоморфен булеву гиперкубу ΓQ_2^n, в частности, B_x является битрейдом. Здесь набору $z \in Q_2^n$ соответствует вершина $y \in B_x$, у которой координаты, соответствующие единицам

в наборе z, равны $k-1$, а координаты, соответствующие нулям в наборе z, такие же, как в наборе x. Определим $\widetilde{\mathrm{wt}}(y)$ как число координат в наборе y, равных $k-1$, т.е. $\widetilde{\mathrm{wt}}(y) = \mathrm{wt}(z)$. Соответствующую этому битрейду функцию можно задать явной формулой $b_x(y) = (-1)^{\widetilde{\mathrm{wt}}(y)}\chi_{B_x}(y)$. Поскольку $\mathrm{supp}(b_x) \cap Q^n_{k-1} = \{x\}$, набор функций $\{b_x \mid x \in Q^n_{k-1}\}$ является базисом в $\mathbb{V}_{n,k}(\mathbb{F})$, и значит, $\dim \mathbb{V}_{n,k}(\mathbb{F}) = (k-1)^n$.

Следующее утверждение нетрудно доказать по индукции (см. [16]).

Предложение 3. *Пусть* $f \in \mathbb{V}_{n,k}(\mathbb{F})$ *и* $\mathrm{supp}(f) \neq \varnothing$. *Тогда* (a) $|\mathrm{supp}(f)| \geqslant 2^n$; (b) *если* $|\mathrm{supp}(f)| = 2^n$, *то граф* $\Gamma(\mathrm{supp}(f))$ *изоморфен булеву гиперкубу* ΓQ^n_2.

Нетрудно видеть, что имеется всего $\binom{k}{2}^n$ вариантов выбрать унитрейд (битрейд) с носителем мощности 2^n. Как показано выше, базис пространства $\mathbb{V}_{n,k}(\mathrm{GF}(2))$ можно составить из характеристических функций булева гиперкуба (точнее множеств, индуцирующих подграф, изоморфный булевому гиперкубу размерности n). Поскольку при $k > 2$ число таких множеств больше размерности пространства, унитрейды не единственным образом представляются в виде линейной комбинации над $\mathrm{GF}(2)$ булевых гиперкубов. Минимальное число булевых гиперкубов в таком представлении унитрейда U будем называть *рангом* унитрейда и обозначать $\mathrm{rank}(U)$.

Рассмотрим более подробно троичный гиперкуб. Любой элемент пространства $\mathbb{V}_{n,3}(\mathrm{GF}(2))$ является унитрейдом, поскольку четное число единиц из трех возможных в одномерной грани равняется 0 или 2. Размерность пространства $\mathbb{V}_{n,3}(\mathrm{GF}(2))$ равна 2^n, поэтому в гиперкубе Q^n_3 имеется ровно 2^{2^n} различных унитрейдов. Методом индукции по размерности n нетрудно доказать

Предложение 4. (a) *Любая пара непустых унитрейдов в* Q^n_3 *имеет непустое пересечение.*

(b) *Если в* Q^n_3 *непустой унитрейд является подмножеством другого унитрейда, то эти унитрейды совпадают.*

(c) *Граф* ΓU *унитрейда* U *связен в* Q^n_3.

Из утверждения (c) следует, что если унитрейд $U \subset Q^n_3$ является битрейдом, то он разделяется на две доли однозначно.

§ 3. Булевы функции

Пусть $f\colon Q^n_2 \to Q_2$ – некоторая булева функция. Определим функцию $U[f]\colon Q^n_3 \to Q_2$ равенством $U[f](y) = \bigoplus\limits_{x \in Q^n_2,\, x \preceq y} f(x)$ (здесь и далее операция $\oplus$ обозначает сложение в двоичном поле $\mathrm{GF}(2)$). Из определения видно, что $U[f]|_{Q^n_2} = f$. Из совпадения определения функции $U[f]$ и формулы (2) над полем $\mathrm{GF}(2)$ следует, что $U[f]$ – характеристическая функция унитрейда в Q^n_3. Более того, из вышеизложенного следует, что между булевыми функциями и троичными унитрейдами имеется взаимно-однозначное соответствие.

Пусть $x \in Q^n_2$. Введем следующие обозначения: $x^1_i = x_i$, $x^{-1}_i = x_i \oplus 1$, $x^0_i = 1$, и если $x = (x_1, \ldots, x_n)$, то $x^v = x^{v_1}_1 \ldots x^{v_n}_n$, где $v \in Q^n_3 = \{0, \pm 1\}^n$.

Полиномиальным представлением булевой функции f называется формула вида $f(x) = f^A(x_1, \ldots, x_n) = \bigoplus\limits_{v \in A \subset Q^n_3} x^v$. Минимальное количество слагаемых в этом представлении $(\min |A|)$ называется *полиномиальной сложностью* функции f (см. [15]).

Обозначим $\{0, \pm 1\}_0 = \{0, 1\}$, $\{0, \pm 1\}_1 = \{1, -1\}$, $\{0, \pm 1\}_{-1} = \{0, -1\}$ и $\{0, \pm 1\}_v = \{0, \pm 1\}_{v_1} \times \ldots \times \{0, \pm 1\}_{v_n}$. Вложенные в Q^n_3 булевы гиперкубы исчерпываются кубами вида $\{0, \pm 1\}_v$. Нетрудно видеть, что сужение характеристической функции гиперкуба $\{0, \pm 1\}_v$ на булев подкуб $\{0, 1\}^n$ совпадает с мономом x^v, т.е. $\chi_{\{0,\pm 1\}_v}(x) = x^v$

при $x \in Q_2^n$. Поэтому $U[f^A] = \bigoplus\limits_{v \in A \subset Q_3^n} \chi_{\{0,\pm 1\}_v}$, и $\operatorname{rank}(U[f])$ равен полиномиальной сложности функции f. Проблема нахождения представления булевой функции минимальной полиномиальной сложности (minimization of exclusive-OR-sum-of-products) рассматривается, например, в [14]. Известно (см. [15]), что для размерности 5 максимальная сложность булевой функции равна 9, для размерности 6 она равна 15, и существуют булевы функции от семи аргументов с полиномиальной сложностью 24.

Из определения полиномиальной сложности следует, что полиномиальная сложность булевой функции не больше суммы сложностей двух ее подфункций, полученных фиксацией 0 и 1 некоторой переменной. Отсюда вытекает

Следствие 1. *Ранг унитрейда не превосходит суммы рангов двух его различных ретрактов по произвольной координате.*

Полиномиальное представление булевой функции неоднозначно. Но если не использовать один из операторов x^0, x^1 или x^{-1}, то представление приобретает однозначность. В § 2 рассматривался базис в пространстве $f \in \mathbb{V}_{n,3}(\mathrm{GF}(2))$, соответствующий операторам x^1 и x^{-1}. Если исключить оператор x^{-1} ("отрицание"), мы приходим к базису из сложения и умножения над GF(2). А именно, каждая булева функция $f\colon Q_2^n \to Q_2$ может быть единственным образом представлена в виде *многочлена Жегалкина* (в *алгебраической нормальной форме*)

$$f(x_1, \ldots, x_n) = \bigoplus_{y \in Q_2^n} G[f](y) x_1^{y_1} \ldots x_n^{y_n},$$

где $G[f]\colon Q_2^n \to Q_2$ – булева функция.

Алгебраической степенью булевой функции f называется максимальная степень слагаемого в ее многочлене Жегалкина, т.е. $\deg f = \max\limits_{G[f](y)=1} \mathrm{wt}(y)$.

Справедливо следующее

Предложение 5. *Для любой булевой функции f верно равенство* $G[f](y) = \bigoplus\limits_{x \in Q_2^n,\, x \preceq y} f(x)$.

Таким образом, $G[f]$ является преобразованием Мёбиуса функции f над полем GF(2). Поскольку $f(x) = \bigoplus\limits_{y \in Q_2^n,\, x \preceq y} G[f](y)$, имеем равенство $G[G[f]] = f$ для любой булевой функции f. Из определений преобразования Мёбиуса и оператора $U[\,\cdot\,]$ видно, что $U[f]|_{\{0,2\}^n}$ является преобразованием Мёбиуса булевой функции f.

Из предложения 5 непосредственно следует известное

Предложение 6. *Булева функция $f\colon Q_2^n \to Q_2$ имеет четное число единиц во всех гранях размерности не меньше m тогда и только тогда, когда* $\deg f \leqslant m-1$.

Наборы значений булевых функций $f\colon Q_2^n \to Q_2$ можно рассматривать как элементы булева куба размерности 2^n. Множество наборов значений булевых функций алгебраической степени не выше m называется кодом Рида – Маллера $\mathcal{R}(m,n)$ в $Q_2^{2^n}$. Известно, что минимальный вес ненулевого кодового набора $\mathcal{R}(m,n)$, совпадающий с мощностью носителя соответствующей булевой функции, равен 2^{n-m}.

Замечание 1. Отметим, что аналогичным образом множество элементов пространства $\mathbb{V}_{n,k}(\mathrm{GF}(q))$ можно рассматривать как линейный код длины k^n и мощности $q^{(k-1)^n}$ с кодовым расстоянием 2^n. В частности, унитрейды в Q_3^n образуют двоичный код длины 3^n и мощности 2^{2^n} с кодовым расстоянием 2^n.

В случае, когда $k = q$, пространство $\mathbb{V}_{n,k}(\mathrm{GF}(q))$ имеет достаточно естественное представление в терминах полиномов: оно состоит из всех функций, которые ортогональны любому моному, не зависящему существенно хотя бы от одной из n пере-

менных. Легко понять, что для простого q базисом $\mathbb{V}_{n,q}(\mathrm{GF}(q))$ является множество всех мономов, у которых степень каждой переменной не превосходит $q-2$. Таким образом, $\mathbb{V}_{n,q}(\mathrm{GF}(q))$ можно рассматривать как один из вариантов недвоичного обобщения кодов Рида – Маллера. В частности, один из результатов п. 4.2 (следствие 2) можно трактовать в терминах весового распределения этого кода при $q = 3$: каждая третья компонента этого распределения нулевая.

В [19] указана связь между троичными битрейдами и равномерностью распределения единиц булевой функции по граням. Булева функция называется *почти уравновешенной в гранях*, если число нулей и единиц функции отличается не более чем на 2 в любой грани любого размера.

Предложение 7. *Пусть булева функция f уравновешена в гранях, а $p(x) = x_1 \oplus \ldots \oplus x_n$ – счетчик четности. Тогда унитрейд $U[f \oplus p]$ является битрейдом.*

Из предложения 1 следует, что если булева функция f соответствует битрейду $U[f]$, то и ее подфункции, полученные фиксацией некоторых переменных, также соответствуют битрейдам в гиперкубах меньшей размерности.

§ 4. Мощностной спектр множества битрейдов

В этом параграфе будут доказаны свойства спектра мощностей троичных битрейдов, а также битрейдов и унитрейдов малой мощности в произвольных гиперкубах.

4.1. Мощности унитрейдов и весовой спектр кодов Рида – Маллера. Из предложения 3 следует, что минимальная мощность непустого унитрейда размерности n равна 2^n. В [16] было доказано

Предложение 8. *Любой унитрейд $U \subset Q_k^n$, мощность которого удовлетворяет неравенствам $2^{n+1} > |U| \geqslant 2^n$, является битрейдом, имеет* $\mathrm{rank}(U) = 2$ *и мощность $|U| = 2^{n+1} - 2^{s+1}$, где $s \in \{0, \ldots, n-1\}$.*

Используя результаты исследований весового спектра кодов Рида – Маллера, можно сильно сузить спектр гипотетических малых (от 2^n до $5 \cdot 2^{n-1}$) мощностей унитрейдов размерности n.

Предложение 9. *Пусть U – унитрейд в Q_k^n, $k = 2^\tau$. Тогда существует вектор $u \in \mathcal{R}((\tau-1)n, \tau n)$, такой что $|U| = \mathrm{wt}(u)$.*

Доказательство. Пусть $f = \chi_U \colon Q_k^n \to \{0,1\}$. Рассмотрим произвольное взаимно-однозначное отображение $\psi \colon Q_2^\tau \to Q_k$. Пусть булева функция F определена равенством

$$F = f(\psi(x_1, \ldots, x_\tau), \psi(x_{\tau+1}, \ldots, x_{2\tau}), \ldots, \psi(x_{\tau(n-1)+1}, \ldots, x_{\tau n})).$$

Проверим, что $\deg F \leqslant (\tau-1)n$. Рассмотрим любую грань Δ булева гиперкуба размерности $(\tau-1)n+1$. Поскольку Δ получена фиксацией значений $n-1$ переменных, найдется i от 0 до $n-1$ такое, что значения переменных $x_{\tau i+1}$, …, $x_{\tau i+\tau}$ не фиксированы в грани Δ. По определению унитрейда при фиксированных значениях всех остальных переменных, кроме $x_{\tau i+1}, \ldots, x_{\tau i+\tau}$, функция F принимает значение 1 четное число раз. Значит, она принимает значение 1 четное число раз в грани Δ. Из предложения 6 следует, что $\deg F \leqslant (\tau-1)n$. Поэтому набор значений функции F содержится в коде $\mathcal{R}((\tau-1)n, \tau n)$. Следовательно, унитрейду U соответствует некоторый вектор $u \in \mathcal{R}((\tau-1)n, \tau n)$. А поскольку функции F и f одинаковое число раз принимают значение 1, имеем $|U| = \mathrm{wt}(u)$. ▲

Замечание 2. $[t]$-трейд в Q_k^N определяется как пара непересекающихся множеств вершин из Q_k^N, разность характеристических функций которых имеет сумму 0 по любой $(N-t)$-мерной грани. По определению битрейд в Q_k^N является $[N-1]$-трейдом.

Аналогично предложению 9 доказывается следующий факт: битрейду в Q_k^n, $k = 2^\tau$, соответствует $[t]$-трейд в $Q_2^{\tau n}$, где $t = n-1$. $[t]$-трейды естественным образом соответствуют разностям ортогональных массивов и алгебраических t-дизайнов в графах Хэмминга. Аналогичное нашему исследование мощностей малых двоичных $[t]$-трейдов было проведено в работе [6]. В частности, построены трейды с мощностями из серий, рассмотренных нами в п. 4.6.

В [20,21] показано, что ненулевые вершины кода $\mathcal{R}(m,n)$ могут иметь вес только вида $\alpha_m 2^{n-m}$, где $\alpha_m = 2 - 2^{-k}$, $k = 0, \dots, n-m-1$, или $\alpha_m = 2 + 2^{-k}$, $k = 2, \dots, \left\lfloor \dfrac{n-m}{2} \right\rfloor$, или $\alpha_m = 2\dfrac{1}{2} - 2^{-k}$, $k = 1, \dots, n-m-1$, или $\alpha_m = 2\dfrac{1}{2} - 2^{-k} - 2^{-(k+1)}$, $k = 3, \dots, n-m-2$, или $\alpha_m \geqslant 2\dfrac{1}{2}$.

Теорема 1. *Мощность унитрейда в Q_k^n может принимать только значения вида $\alpha_n 2^n$, где*

$$\alpha_n = 2 - 2^{-k}, \quad k = 0, \dots, n-1, \quad \textit{или}$$
$$\alpha_n = 2 + 2^{-k}, \quad k = 2, \dots, \lfloor n/2 \rfloor, \quad \textit{или}$$
$$\alpha_n = 2\frac{1}{2} - 2^{-k}, \quad k = 1, \dots, n-1, \quad \textit{или}$$
$$\alpha_n = 2\frac{1}{2} - 2^{-k} - 2^{-(k+1)}, \quad k = 3, \dots, n-2, \quad \textit{или} \quad \alpha_n \geqslant 2\frac{1}{2}.$$

Доказательство. Любой унитрейд в Q_k^n имеет мощность не меньше 2^n (предложение 3). Сужение унитрейда на грань (ретракт) есть унитрейд по предложению 1. Поэтому унитрейд, пересекающийся с пятью параллельными гипергранями некоторого направления, имеет мощность не менее $5 \cdot 2^{n-1}$ (последний случай в утверждении теоремы). Если же унитрейд пересекается не более чем с четырьмя параллельными гипергранями любого направления и является подмножеством вершин подграфа, изоморфного Q_4^n, то в этом случае требуемое следует из предложения 9 ($\tau = 2$) и перечисленных выше результатов работ [20,21]. ▲

4.2. Троичные битрейды как линейные функции над полем GF(3). Вначале выберем подходящий базис в пространстве $\mathbb{V}_{n,3}(\mathrm{GF}(3))$. Здесь нам будет удобно считать, что $Q_3 = \{0, \pm 1\} = \mathrm{GF}(3)$ ($-1 \equiv 2 \bmod 3$). Пусть $s_0(a) = 1$ и $s_1(a) = a$. Определим функции $s_\alpha \colon Q_3^n \to Q_3$, $\alpha \in Q_2^n$, равенствами $s_\alpha(x) = s_{\alpha_1}(x_1) \dots s_{\alpha_n}(x_n)$.

Предложение 10. (a) $s_\alpha \in \mathbb{V}_{n,3}(\mathrm{GF}(3))$;
(b) $\{s_\alpha \mid \alpha \in Q_2^n\}$ – *базис в* $\mathbb{V}_{n,3}(\mathrm{GF}(3))$;
(c) $\langle s_\alpha, s_\beta \rangle_3 = \sum\limits_{x \in Q_3^n} s_\alpha(x) s_\beta(x) = 0$ *за исключением случая* $\alpha = \beta = \bar{1}$.

Доказательство. Утверждение (a) следует из того факта, что $\sum\limits_{a \in Q_3} s_0(a) = \sum\limits_{a \in Q_3} s_1(a) = 0$.

(b) Заметим, что $\alpha \in \mathrm{supp}(s_\alpha)$, а $\alpha \in \mathrm{supp}(s_\beta)$, только если $\beta \preceq \alpha$, $\alpha, \beta \in Q_2^n$. Упорядочим функции s_α в порядке (частичном) убывания от $\bar{1}$ до $\bar{0}$. Носитель каждой следующей функции содержит точку, которая не содержится в носителях предыдущих функций. Поэтому на каждом шаге мы будем получать линейно независимое семейство функций. Как показано выше, $\dim(\mathbb{V}_{n,3}(\mathrm{GF}(3))) = 2^n$, следовательно, семейство линейно независимых функций мощности 2^n является базисом.

(c) Пусть набор α имеет нулевую координату. Без ограничения общности будем считать, что $\alpha_n = 0$. Тогда справедливы равенства

$$\sum_{x \in Q_3^n} s_\alpha(x) s_\beta(x) =$$

$$= \sum s_{\alpha_1}(x_1)s_{\beta_1}(x_1)\dots s_{\alpha_{n-1}}(x_{n-1})s_{\beta_{n-1}}(x_{n-1}) \sum_{x_n\in Q_3} s_0(x_n)s_{\beta_n}(x_n) =$$

$$= \sum s_{\alpha_1}(x_1)s_{\beta_1}(x_1)\dots s_{\alpha_{n-1}}(x_{n-1})s_{\beta_{n-1}}(x_{n-1}) \sum_{x_n\in Q_3} s_{\beta_n}(x_n) = 0. \quad \blacktriangle$$

Следствие 2. *Для любого* $f \in \mathbb{V}_{n,3}(\mathrm{GF}(3))$ *верно* $\langle f, f\rangle_3 \in \{0, 2^n \bmod 3\}$.

Доказательство. Из предложения 10 следует, что $f = \sum\limits_{\alpha\in Q_2^n} a_\alpha s_\alpha$ и

$$\langle f, f\rangle_3 = \sum_{\alpha,\beta\in Q_2^n} a_\alpha a_\beta \sum_{x\in Q_3^n} s_\alpha(x)s_\beta(x) = a_{\bar 1}^2 \sum_{x\in Q_3^n} s_{\bar 1}^2 = a_{\bar 1}^2 |\mathrm{supp}(s_{\bar 1})| = a_{\bar 1}^2 2^n,$$

где все операции выполняются в поле GF(3). $\blacktriangle$

Как отмечено в замечании 1, пространство $\mathbb{V}_{n,3}(\mathrm{GF}(3))$ является троичным кодом типа Рида–Маллера, а следствие 2 означает, что весовой спектр этого кода имеет нули в каждой третьей компоненте.

Теорема 2. *Для любого битрейда* $B \subset Q_3^n$ *верно, что* $|B| \equiv 0, 2^n \bmod 3$.

Доказательство. Рассмотрим функцию $b\colon Q_3^n \to Q_3$, принимающую значения 1 и -1 на двух долях битрейда B и значение 0 в остальных точках. Тогда $b \in \mathbb{V}_{n,3}(\mathrm{GF}(3))$ и $|B| \bmod 3 = \langle b, b\rangle_3 \in \{0, 2^n \bmod 3\}$. $\blacktriangle$

Следствие 3. *Не существует битрейда* $U \subset Q_3^n$ *мощности* 2^{n+1}.

4.3. Некоторые свойства мощностного спектра троичных битрейдов. Рассмотрим несколько простых свойств битрейдов. Пусть f – булева функция от переменных $x_1, \dots, x_n$, а g – булева функция от переменных $y_1, \dots, y_m$, и наборы переменных не пересекаются. Обозначим через $f(x)g(y)$ булеву функцию от $n+m$ переменных. В [16] имеется

Предложение 11. *Если* $U[f] \subset Q_3^n$ *и* $U[g] \subset Q_3^m$ *– битрейды, то* $U[f(x)g(y)] \subset Q_3^{n+m}$ *– битрейд и* $|U[f(x)g(y)]| = |U[f]||U[g]|$.

В частности, в качестве g можно рассмотреть линейную функцию $g(y) = \bigoplus y_i$ и как следствие получить такое свойство: если в Q_3^n имеется битрейд мощности a, то в Q_3^{n+m} имеется битрейд мощности $a2^m$. Эту конструкцию можно рассматривать как частный случай декартова произведения двух битрейдов. Декартово произведение двух битрейдов является битрейдом не только в троичном гиперкубе, но и в гиперкубах над произвольным алфавитом. Унитрейды, которые можно представить в виде декартова произведения, будем называть *разложимыми*.

Теорема 3 (о построении разложимых битрейдов). *Пусть* $B \subset Q_k^n$ *и* $C \subset Q_k^n$ *– битрейды. Тогда в* Q_k^{n+m} *имеются битрейды мощности* $|B|\cdot|C|$, $2^m|B|$, $k^m|B|$.

Доказательство. Битрейды мощности $|B|\cdot|C|$ и $2^m|B|$ можно построить с помощью декартова произведения. Возможность построения битрейда мощности $k^m|B|$ можно доказать по индукции из случая $m = 1$, который разберем отдельно. Пусть функция $b\colon Q_k^n \to \{-1, 0, 1\}$ принимает значения 1 и -1 на двух долях некоторого битрейда и 0 в остальных точках. Тогда функция $b'\colon Q_k^{n+1} \to \{-1, 0, 1\}$, заданная равенством $b'(x_1, \dots, x_n, x_{n+1}) = b(x_1, \dots, x_{n-1}, (x_n + x_{n+1}) \bmod k)$, определяет битрейд размерности $n+1$ и мощности $k|B|$. $\blacktriangle$

Предложение 12. *Если унитрейд* $U \subset Q_3^n$ *имеет пустой ретракт по некоторому направлению, то он эквивалентен унитрейду* $U[f]$, *где* f *– булева функция, не зависящая от одной из переменных. При этом* U *является битрейдом тогда и только тогда, когда битрейдом является любой из его непустых ретрактов по тому же направлению.*

Доказательство. Без ограничения общности можно считать, что $U \cap \{x_n = -1\} = \varnothing$. Тогда из определения унитрейда имеем $U \cap \{x_n = 0\} = U \cap \{x_n = 1\} = U'$ и $U = U' \times \{0, 1\}$. Пусть $U' = U[f]$ и $g(x_1, \ldots, x_n) = f(x_1, \ldots, x_{n-1})$. Тогда $U = U[g]$. Из предложений 1 и 11 следует, что унитрейды U и U' являются битрейдами одновременно. ▲

Поскольку каждая одномерная грань гиперкуба пересекается с унитрейдом не более чем по двум вершинам, троичный унитрейд U размерности n содержит не более $2 \cdot 3^{n-1}$ вершин. При этом в случае равенства $|U| = 2 \cdot 3^{n-1}$ дополнение $Q_3^n \setminus U$ является МДР-кодом. Как известно (см., например, [17]), в Q_3^n имеется единственный с точностью до эквивалентности МДР-код, являющийся линейным (т.е. аффинным подпространством над полем GF(3)). Дополнение аффинного подпространства над GF(3) состоит из двух его смежных классов. Поэтому унитрейд максимальной мощности единственный и является битрейдом, что отражено в первой части следующей теоремы.

Теорема 4 (о битрейдах большой мощности). *Справедливы следующие утверждения*:

(a) *В Q_3^n имеется только один с точностью до эквивалентности унитрейд B максимальной мощности $2 \cdot 3^{n-1}$, который является битрейдом и может быть задан равенством $B = \{x \in Q_3^n \mid x_1 + \ldots + x_n \not\equiv 0 \bmod 3\} = U[\ell]$, где ℓ – некоторая симметричная булева функция.*

(b) *В Q_3^n имеются битрейды мощности $14 \cdot 3^{n-3}$.*

(c) *В Q_3^n не существует битрейдов мощности, промежуточной между $14 \cdot 3^{n-3}$ и $2 \cdot 3^{n-1}$.*

Доказательство. Осталось доказать утверждения (b) и (c). В Q_3^3 имеется битрейд $U[x_1x_2x_3 \oplus (x_1 \oplus 1)(x_2 \oplus 1)(x_3 \oplus 1)]$ мощности 14. Из теоремы 3 получаем (b).

Докажем (c) по индукции. Базой индукции является случай $n = 3$, который легко проверить непосредственно. Пусть теперь $U^{n+1} \subset Q_3^{n+1}$ – некоторый битрейд. Если три различных ретракта какого-то одного направления имеют мощности меньше $2 \cdot 3^{n-1}$, то $|U^{n+1}| \leqslant 14 \cdot 3^{n-2}$ по предположению индукции. Предположим, что в U^{n+1} найдется по одному ретракту каждого направления мощности $2 \cdot 3^{n-1}$. Без ограничения общности можно полагать, что каждый из этих ретрактов соответствует нулевому значению некоторой переменной ($x_i = 0$). По утверждению (a) они с точностью до эквивалентности заданы линейными над GF(3) функциями. Тогда $U^{n+1} = U[f]$, где $f = \ell$ или $f = \ell \oplus x_1 \ldots x_{n+1}$. Однако вторая функция имеет недвудольный трехмерный ретракт при $n \geqslant 4$. Действительно, рассмотрим трехмерный ретракт, полученный из $U[f]$, где $f = \ell \oplus x_1 \ldots x_{n+1}$, фиксацией координат $x_4 = \ldots = x_{n+1} = 1$. Если $n - 2 = 0, 1 \bmod 3$, то этот ретракт эквивалентен недвудольному унитрейду (1); если $n - 2 = 2 \bmod 3$, то недвудольному унитрейду (1) эквивалентен ретракт, полученный фиксацией координат $x_4 = 2$, $x_5 = \ldots = x_{n+1} = 1$. Поэтому в случае, когда $U[f] \subset Q_3^{n+1}$ – битрейд, имеем $f = \ell$ и $|U^{n+1}| = |U[f]| = 2 \cdot 3^n$. ▲

4.4. Битрейды и расстояния между мономами. Пусть $B \subset Q_k^n$ – битрейд. В § 2 была определена функция $b[B]\colon Q_k^n \to \{0, \pm 1\}$, которая принимает значение 1 на одной доле битрейда B, -1 на другой его доле и 0 в остальных вершинах. В этом пункте мы будем рассматривать $b[B]$ как функцию, действующую в $\mathbb{R}$, т.е. $b[B] \in \in \mathbb{V}_{n,3}(\mathbb{R})$. В случае $k = 3$ такую функцию можно определить ровно двумя способами: $b[B]$ и $-b[B]$, поскольку граф ΓB связен. В дальнейшем мы рассматриваем только такой случай и обычно не уточняем, каким из двух способов выбран знак функции $b[B]$. Для краткости введем обозначения $b_v = b[U[x^v]]$ и $b_V = b[U[f^V]]$, где $v \in Q_3^n$, $V \subset Q_3^n$.

Предложение 13. *Пусть $B, B' \subset Q_3^n$ – битрейды и $b[B](x)b[B'](x) \neq 1$ для любого $x \in Q_3^n$. Тогда $S = \operatorname{supp}(b[B] + b[B'])$ – битрейд и $b[S] = b[B] + b[B']$.*

Доказательство. Если $b[B], b[B'] \in \mathbb{V}_{n,3}(\mathbb{R})$, то $b[B]+b[B'] \in \mathbb{V}_{n,3}(\mathbb{R})$. По условию $b[B]b[B'] \neq 1$, следовательно, $(b[B]+b[B'])(Q_3^n) \subseteq \{0, \pm 1\}$. Тогда по определению $S = \mathrm{supp}(b[B] + b[B'])$ – битрейд. ▲

Будем говорить, что функции b_v и b_u *согласованы*, если $b_u(x)b_v(x) \neq 1$ для любого $x \in Q_3^n$.

Предложение 14. *Пусть $v, u \in Q_3^n$. Если найдется вершина $x \in Q_3^n$, такая что $b_v(x)b_u(x) = -1$, то пара функций b_u и b_v согласована.*

Доказательство. Пересечение битрейдов $U[x^u]$ и $U[x^v]$ является булевым подкубом в грани, соответствующей совпадающим координатам наборов u и v. Из связности пересечения $U[x^u] \cap U[x^v]$ следует, что унитрейд $U[x^u \oplus x^v]$ является битрейдом. Как было замечено выше, любой битрейд разделяется на доли единственным образом. ▲

Следствие 4. *Любой унитрейд ранга 2 является битрейдом.*

Предложение 15. *Унитрейд $U[f^V]$ является битрейдом, если для каждого $v \in V$ можно выбрать функции (знак функции) b_v так, чтобы функция $g = \sum\limits_{v \in V} b_v$ принимала значения только из множества $\{0, \pm 1\}$.*

Доказательство. Поскольку $b_v \in \mathbb{V}_{n,3}(\mathbb{R})$ для любого $v \in V$, то и $g \in \mathbb{V}_{n,3}(\mathbb{R})$. Тогда из условия следует, что $\mathrm{supp}(g)$ – унитрейд. Очевидно, $U[f^V] \subset \mathrm{supp}(g)$. Тогда из предложения 4(b) имеем $\mathrm{supp}(g) = U[f^V]$, т.е. $g = \pm b_V$. ▲

Предложение 16. *Пусть $V \subset Q_3^n$ и $|V| = 3$ (т.е. $\mathrm{rank}(U[f^V]) \leqslant 3$). Если все вершины множества V различаются только в двух координатах либо две вершины множества V различаются только в одной координате, то $U[f^V]$ – битрейд.*

Доказательство. Пусть $V = \{u, v, w\}$ и вершины множества V различаются только в двух координатах. Тогда с помощью предложения 12 можно перейти к двумерному случаю, когда все унитрейды являются битрейдами.

Если $d(v, u) = 1$, то $x^v \oplus x^u = x^o$, т.е. $\mathrm{rank}(U[f^V]) = 2$, и требуемое вытекает из следствия 4. ▲

Будем говорить, что три вершины $\{u, v, w\} \subset Q_3^n$ *находятся в общем положении*, если найдется координата, в которой они попарно различаются. В этом случае найдутся точки $a, a', a'' \in Q_3^n$, в которых носители битрейдов b_u, b_v, b_w пересекаются только попарно, т.е. $a \in (\mathrm{supp}(b_v) \cap \mathrm{supp}(b_u)) \setminus \mathrm{supp}(b_w)$, $a' \in (\mathrm{supp}(b_v) \cap \mathrm{supp}(b_w)) \setminus \setminus \mathrm{supp}(b_u)$, $a'' \in (\mathrm{supp}(b_w) \cap \mathrm{supp}(b_u)) \setminus \mathrm{supp}(b_v)$.

Вначале рассмотрим унитрейды $U[f^V]$ ранга 3, когда три вершины $V = \{u, v, w\}$ не находятся в общем положении.

Предложение 17. *Пусть $V = \{u, v, w\} \subset Q_3^n$.*

(a) *Если любая координата набора w совпадает с соответствующей координатой набора u или набора v, то $U[f^V]$ – битрейд.*

(b) *Если любая координата на наборах u, v, w принимает не более двух значений и не выполнено условие* (a)*, то $U[f^V]$ не является битрейдом.*

Доказательство. (a) Рассмотрим случай, когда нет координаты, в которой все три вершины u, v, w совпадают. Без ограничения общности можно считать, что $u = \bar{0}$, $v = \bar{1}$, $w \in \{0, 1\}^n$. По предложению 14 функции b_v и b_u можно выбрать так, чтобы вещественные суммы $b_v + b_w$ и $b_u + b_w$ принимали значения только из множества $\{0, \pm 1\}$. Из условия видно, что $U[x^{\bar{0}}] \cap U[x^{\bar{1}}] = \{\bar{1}\} \subset U[x^w]$. Поэтому $(b_v + b_w)(\bar{1}) = 0$. Следовательно, функция $b_v + b_u + b_w$ принимает значения только из множества $\{0, \pm 1\}$. Требуемое следует из предложения 15.

Случай, когда все три вершины u, v, w совпадают в некоторой координате, сводится к рассмотренному с помощью предложения 12.

(b) Если любая тройка координат в наборах u, v, w удовлетворяет условию (a), то наборы u, v, w также удовлетворяют этому условию. Без ограничения общности можно считать, что условию (a) не удовлетворяют первые тройки координат наборов u, v, w и они равны, соответственно, $e_1 = (1, 0, 0)$, $e_2 = (0, 1, 0)$ и $e_3 = (0, 0, 1)$. Поскольку в каждой координате наборы u, v, w принимают только два значения, то найдется трехмерная грань, на которой $x^v \oplus x^u \oplus x^w = x_1 \oplus x_2 \oplus x_3 = f'$. Непосредственная проверка показывает, что $U[f']$ эквивалентен унитрейду (1) и не является битрейдом. Тогда из предложения 1 следует, что и $U[f^V]$ не является битрейдом. ▲

Теперь рассмотрим унитрейды $U[f^V]$ ранга 3, когда три вершины $V = \{u, v, w\}$ находятся в общем положении.

Предложение 18. *Пусть* $V = \{u, v, w\} \subset Q_3^n$.

(a) *Если сумма попарных расстояний между вершинами множества* V *нечетна, то они находятся в общем положении.*

(b) *Если вершины множества* V *находятся в общем положении, то из согласованности пары* b_v, b_u *и пары* b_v, b_w *следует согласованность пары* b_u, b_w *тогда и только тогда, когда сумма попарных расстояний между вершинами множества* V *нечетна.*

Доказательство. Если вершины u, v, w не находятся в общем положении, то каждая координата дает вклад 0 или 2 в сумму $d(u, v) + d(v, w) + d(u, v)$. Поэтому в этом случае сумма расстояний четная. Пункт (a) доказан.

Рассмотрим случай, когда $V = \{\bar{0}, \bar{1}, \overline{-1}\}$. Нетрудно видеть, что унитрейды $U[x^{\bar{0}}]$ и $U[x^{\bar{1}}]$ пересекаются по одной точке $\bar{1}$. Разделим битрейд $U[x^{\bar{0}} \oplus x^{\bar{1}}]$ на две доли. Вершины той же четности, что и $\bar{1}$, в гиперкубах $U[x^{\bar{0}}]$ и $U[x^{\bar{1}}]$ должны принадлежать разным долям. Следовательно, вершины $\bar{0}$ и $\overline{-1}$ оказываются в разных долях. Рассмотрим гиперкуб $U[x^{\overline{-1}}]$. Ясно, что вершины $\bar{0}$ и $\overline{-1}$ оказываются в разных долях, если и только если n нечетно. Тогда из согласованности пары $b_{\bar{0}}, b_{\bar{1}}$ и пары $b_{\bar{0}}, b_{\overline{-1}}$ следует согласованность пары $b_{\bar{1}}, b_{\overline{-1}}$ при нечетном n и несогласованность пары $b_{\bar{1}}, b_{\overline{-1}}$ при четном n.

Проведем дальнейшее доказательство по индукции. Предположим, что при $n-1$ утверждение доказано.

Пусть вершины u, v, w попарно различаются в каждой координате. Тогда утверждение следует из рассмотренного выше случая. В противном случае найдется координата, в которой не все вершины u, v, w попарно различаются. После удаления этой координаты укороченные наборы v', u', w' также находятся в общем положении. Без ограничения общности можно полагать, что удаленная координата была последней. Очевидно, $d(u', v') + d(v', w') + d(u', v') = d(u, v) + d(v, w) + d(u, v)$, если $u_n = v_n = w_n$, и $d(u', v') + d(v', w') + d(u', v') = d(u, v) + d(v, w) + d(u, v) - 2$ в противном случае. Тогда утверждение верно для функций $b_{v'}$, $b_{u'}$ и $b_{w'}$ по предположению индукции. Поскольку последняя координата не принимает одно из значений $\{0, \pm 1\}$ на наборах u, v, w, то найдется гипергрань $x_n = \delta$ по последнему направлению, такая что $b_v(x\delta) = b_{v'}(x)$, $b_u(x\delta) = b_{u'}(x)$, $b_w(x\delta) = b_{w'}(x)$ для всех $x \in Q_3^{n-1}$. Тогда для функций b_v, b_u и b_w требуемое следует из предложения 14. ▲

Следствие 5. *Если сумма попарных расстояний между вершинами множества* $V = \{u, v, w\} \subset Q_3^n$ *нечетна, то* $U[f^V]$ *– битрейд.*

Следствие 6. *Если вершины множества* $V = \{u, v, w\} \subset Q_3^n$ *находятся в общем положении, различаются не менее чем в трех координатах и сумма попарных расстояний между вершинами множества* V *четна, то* $U[f^V]$ *не является битрейдом.*

Доказательство. Из предложения 18 следует, что набор функций b_u, b_v, b_w не может быть попарно согласованным. Если две из трех вершин находятся на расстоянии 1 и три вершины находятся в общем положении, то в некоторой координате

все три вершины различаются, и сумма попарных расстояний между ними нечетна. Из условия, что никакие две из вершин u, v, w не находятся на расстоянии 1, следует, что пересечения $\mathrm{supp}(b_v) \cap \mathrm{supp}(b_u)$, $\mathrm{supp}(b_v) \cap \mathrm{supp}(b_w)$ и $\mathrm{supp}(b_u) \cap \mathrm{supp}(b_w)$ эквивалентны граням булева гиперкуба размерности как минимум на 2 меньше размерности гиберкуба, а из условия, что вершины u, v, w различаются не менее чем в трех координатах, следует, что если ровно на 2, то грани, соответствующие разным пересечениям, не параллельны. Поэтому множества $\mathrm{supp}(b_w) \setminus (\mathrm{supp}(b_v) \cup \mathrm{supp}(b_u))$, $\mathrm{supp}(b_u) \setminus (\mathrm{supp}(b_v) \cup \mathrm{supp}(b_w))$, $\mathrm{supp}(b_v) \setminus (\mathrm{supp}(b_w) \cup \mathrm{supp}(b_u))$ являются связными. Тогда из несогласованности следует недвудольность унитрейда. ▲

Если вершины множества $V = \{u, v, w\} \subset Q_3^n$ находятся в общем положении и сумма попарных расстояний между вершинами множества V четна, то они не могут различаться только в одной координате, а если они различаются только в двух координатах, то ранг унитрейда $U[f^V]$ равен 2.

Предложение 19. *Если все попарные расстояния между различными точками множества $V \subset Q_3^n$ нечетны, то $U[f^V]$ – битрейд.*

Доказательство. Покажем по индукции, что можно так выбрать функции b_v, $v \in V$, что все функции b_v будут попарно согласованы. При $|V| = 3$ требуемое следует из предложения 18. Пусть для множеств $V \subset Q_3^n$, $|V| = k$, утверждение верно. Рассмотрим $u \notin V$, находящуюся на нечетном расстоянии от любой точки из V. Выберем функцию b_u согласовано с b_v для некоторого $v \in V$. Тогда из предложения 18 следует, что b_u согласовано с b_w для любого $w \in V$. Таким образом, функции b_v, $v \in V$, попарно согласованы при $|V| = k + 1$. Если все функции b_v, $v \in V$, согласованы, то $\sum\limits_{v \in V} b_v$ принимает значения только из множества $\{0, \pm 1\}$. Тогда $U[f^V]$ – битрейд по предложению 15. ▲

4.5. Вычислительные результаты. В этом пункте мы приведем результаты вычислений числа $N(n)$ троичных битрейдов с помощью ЭВМ. Удалось вычислить число различных битрейдов до размерности $n = 7$, а число неэквивалентных – до размерности $n = 6$. Метод перечисления не сильно отличается от прямого перебора, поэтому мы не будем описывать алгоритм в подробностях. Для перечисления всех битрейдов в Q_3^n в качестве одного из ретрактов подставлялись по одному представителю каждого из $N'(n-1)$ классов эквивалентности функций, найденных на предыдущем шаге. После этого для параллельного ретракта проводился поточечный перебор значений функции с очевидной проверкой выполнимости условия на сумму по одномерной грани. Полученное число решений умножалось на число представителей в классе эквивалентности первого ретракта. Вычисление $N(7)$ заняло два года процессорного времени (в расчете на одно ядро процессора); вычисление проводилось на кластере ИВЦ НГУ. Результаты вычислений до $n = 6$ проверены с помощью следующей техники двойного подсчета (см. [22]): мощность каждого класса эквивалентности, вычисленная через мощность группы автоморфизмов его представителя, совпадает с числом представителей, найденных в процессе полного перебора. В таблице приведены следующие величины: $N(n)$ – число различных (включая тождественно нулевую) $\{-1, 0, 1\}$-функций на Q_3^n, у которых сумма по каждой одномерной грани равна 0 (т.е. все три значения в грани либо нулевые, либо попарно различные); $N'(n)$ – число неэквивалентных таких функций. Последняя колонка отражает среднюю половинную мощность (число элементов -1) битрейда (в скобках приведено среднеквадратичное отклонение); из этой статистики исключен пустой битрейд.

Далее мы приведем распределение битрейдов по мощностям. Для каждого n указано число битрейдов (именно двудольных унитрейдов, т.е. число функций будет вдвое больше) мощности $2^n, 2^n + 2, 2^n + 4, \ldots, 2 \cdot 3^{n-1}$.

$n = 1$: 3.

$n = 2$: 9, 6.

Таблица

n	$N'(n)$	$N(n)$	$\ln N(n)$	$\ln\ln N(n)$	
0	2	3	1,098	0,094	
1	2	7	1,945	0,665 (+0,571)	1
2	3	31	3,433	1,233 (+0,567)	2,4 ($\pm$0,490)
3	5	403	5,998	1,791 (+0,557)	$6{,}448 = 2{,}539^2$ ($\pm$1,188)
4	13	29875	10,304	2,332 (+0,541)	$17{,}960 = 2{,}619^3$ ($\pm$2,342)
5	92	32184151	17,286	2,849 (+0,517)	$50{,}527 = 2{,}666^4$ ($\pm$4,776)
6	25493	1488159817231	28,028	3,333 (+0,483)	$142{,}25 = 2{,}695^5$ ($\pm$10,07)
7	$>$ 2187260868	6171914027409468739	43,266	3,767 (+0,434)	$398{,}17 = 2{,}712^6$ ($\pm$22,59)

$n = 3$: 27, 0, 54, 108, 0, 12.

$n = 4$: 81, 0, 0, 0, 324, 0, 1296, 648, 0, 3888, 2844, 0, 4536, 1296, 0, 0, 0, 0, 0, 24.

$n = 5$: 243, 0, 0, 0, 0, 0, 0, 0, 1620, 0, 0, 0, 9720, 0, 9720, 3888, 0, 0, 58320, 0, 41580, 77760, 0, 116640, 301320, 0, 259200, 660960, 0, 480816, 1368576, 0, 1156680, 2468880, 0, 1415232, 2721600, 0, 1148040, 2185056, 0, 583200, 816480, 0, 90720, 104976, 0, 10800, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 48.

$n = 6$: 729, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 7290, 0, 0, 0, 0, 0, 0, 0, 58320, 0, 0, 0, 87480, 0, 69984, 23328, 0, 0, 0, 0, 524880, 0, 0, 0, 370980, 0, 1399680, 0, 0, 699840, 2099520, 0, 4811400, 466560, 0, 2799360, 7290000, 0, 16562880, 2099520, 0, 6998400, 15244848, 0, 49968576, 19012320, 0, 46889280, 48114000, 0, 149999040, 48988800, 0, 173560320, 158793696, 0, 431451360, 203303520, 0, 593464320, 402077520, 0, 1226726208, 655983360, 0, 1759957632, 1275108480, 0, 3455693280, 1610681760, 0, 4922674560, 3332579760, 0, 8667868320, 4840793280, 0, 12263996160, 7124630400, 0, 19261521360, 10458292320, 0, 25982259840, 15546805632, 0, 37437240960, 17859890880, 0, 44159904000, 26492909760, 0, 56014493760, 28054486080, 0, 58200653952, 29447634240, 0, 63563901120, 30536701920, 0, 53914973760, 27520508160, 0, 44905723488, 18151205760, 0, 28971976320, 13573863360, 0, 17778852000, 6267067200, 0, 7903992960, 2932269264, 0, 2917632960, 1190894400, 0, 772623360, 243544320, 0, 299531520, 100077120, 0, 33592320, 41290560, 0, 5598720, 6298560, 0, 0, 1179360, 0, 3079296, 3429216, 0, 0, 0, 0, 0, 77760, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 96.

$n = 7$: 2187, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 30618, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 306180, 0, 0, 0, 0, 0, 0, 0, 612360, 0, 0, 0, 734832, 0, 489888, 139968, 0, 0, 0, 0, 0, 0, 0, 3674160, 0, 0, 0, 0, 0, 0, 0, 2585520, 0, 0, 0, 14696640, 0, 0, 0, 0, 0, 14696640, 0, 22044960, 5878656, 0, 0, 48376440, 0, 9797760, 0, 0, 0, 58786560, 0, 105325920, 9797760, 0, 29393280, 252292320, 0, 48988800, 19595520, 0, 0, 264539520, 0, 258660864, 39191040, 0, 58786560, 849465792, 0, 417384576, 64665216, 0, 118599552, 1102248000, 0, 1026927720, 440899200, 0, 117573120, 3241833840, 0, 1646023680, 881798400, 0, 411505920, 5472048960, 0, 4595639328, 1293304320, 0, 1175731200, 13190234400, 0, 6642881280, 4967464320, 0, 2792361600, 23992754688, 0, 14767655616, 8897345856, 0, 5232003840, 48779617824, 0, 29422673280, 19428958080, 0, 13418032320, 86712135552, 0, 56942131680, 43070952960, 0, 29628426240, 174586285440, 0, 108140326560, 100338860160, 0, 60767667072, 333349188480, 0, 211194390960, 197052549120, 0, 133406300160, 633974103504, 0, 394756649280, 437915782080, 0, 284879669760, 1184769633600, 0, 732195313920, 918265662720, 0, 553710608640, 2237431905072, 0, 1396486980000, 1839642114240, 0, 1166266563840, 4133841505920, 0, 2463586985664, 3699825232320, 0, 2436508916352, 7740828063360, 0, 4633391621376, 7373480647680, 0, 4422630481920, 14095095607296, 0, 9008038009152, 14256009258624, 0, 8787284896320, 25936010563680, 0, 15056472533760, 27127920314880, 0, 17656455116160, 46489296385728, 0, 28595219380560, 51865158776256, 0, 30807273127680, 84076043325120, 0, 53419783072320, 96717020198400, 0, 59173324616448, 151123241747520, 0, 87927292938240, 177969306401280, 0, 112318130615040, 267008385528864, 0, 160800706809792, 321325302945024, 0, 188053645282560, 466481709832320, 0, 291050421480000, 570238841894400, 0, 343218104712000, 806560729743456, 0, 464604287555520, 996450456984192, 0, 620225396784000, 1373638417522560, 0, 816009087669552, 1708948701149760, 0, 982341376894080, 2305937678879520, 0,

1414154728014336, 2868447898270080, 0, 1691741075976000, 3783164938709184, 0, 2145564791750016, 4708186964144640, 0, 2866434717250944, 6089563693805760, 0, 3543718526510400, 7547844801104640, 0, 4235506218558720, 9574787807964288, 0, 5748041164944960, 11803431065489280, 0, 6789801853310400, 14687203311950400, 0, 8100416661309504, 17888868241614720, 0, 10588066580077056, 21840361606638720, 0, 12363491876450400, 26269417255213440, 0, 14285288100787200, 31462082237108160, 0, 18299032850230272, 37233543050766720, 0, 20709927455180544, 43720111582963200, 0, 23313370728464640, 50763763455713280, 0, 28924064989464960, 58412989843236000, 0, 31813638206316480, 66303578484210816, 0, 34565462372004480, 74583100623265920, 0, 41520901293714528, 82545422286942720, 0, 43826073580183104, 90590698165121280, 0, 45970461276122880, 97356175759100160, 0, 52673395505996160, 103853217900781440, 0, 53561231066238336, 108100043912367360, 0, 53128915099827840, 111570541229580480, 0, 58350442395913920, 112097875912081920, 0, 55765902028032000, 111406452367500864, 0, 52657506351233280, 107575556428968768, 0, 53994455165468160, 102377410528901760, 0, 48778189150406400, 94582347577421760, 0, 42669649619928576, 85745409629443200, 0, 40987358888555520, 75337864538158080, 0, 34117558361470080, 64695169565885376, 0, 27623026142341056, 53722349499008448, 0, 24230050550665344, 43420216983171840, 0, 18493690067425440, 33854862632935680, 0, 13546143606925440, 25584444523483776, 0, 10783563464378880, 18568192776336000, 0, 7350295708661760, 13016846960075520, 0, 4835426179046400, 8727631849641600, 0, 3393591789458304, 5646375105114240, 0, 2053100209063680, 3458776067268480, 0, 1173620938855680, 2041794442509696, 0, 728670130929216, 1138311067888512, 0, 375048142382592, 609672959421120, 0, 191348768439360, 307095833018880, 0, 99253170374400, 152237238241536, 0, 46874958318720, 69750838786176, 0, 19948807630080, 31988971163520, 0, 10729375110720, 13802819748480, 0, 3921475057920, 6002269439040, 0, 1657927958400, 2388145213440, 0, 1007425278720, 1073677731840, 0, 520179426144, 484107321600, 0, 144614937600, 245492674560, 0, 205312060800, 136090886400, 0, 89050752000, 73071694080, 0, 20222576640, 49468890240, 0, 45500797440, 28217548800, 0, 15872371200, 12433357440, 0, 3174474240, 2821754880, 0, 12580323840, 4938071040, 0, 3853785600, 1058158080, 0, 0, 529079040, 0, 1410877440, 0, 0, 1162667520, 0, 0, 0, 0, 0, 235146240, 0, 0, 264539520, 0, 0, 0, 0, 0, 0, 0, 0, 12700800, 0, 0, 0, 0, 0, 129330432, 120932352, 0, 71197056, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 520128, 0, 192.

4.6. Уточнение мощностного спектра битрейдов.

Предложение 20. *Пусть* $\operatorname{rank}(U) \geqslant 4$ *и* $U \subset Q_3^n$ *– неразложимый унитрейд размерности* n*. Тогда* $|U| > 2{,}5 \cdot 2^n$*.*

Доказательство. Рассмотрим ранги ретрактов унитрейда U по некоторой координате. По следствию 1 суммы рангов двух ретрактов не меньше 4.

1) Если унитрейд U имеет пустой ретракт, то по предложению 12 унитрейд U разложим.

2) Если унитрейд U имеет два ретракта ранга не меньше 3 и еще один ранга не меньше 1, то $|U| > 2 \cdot 2^n + 2^{n-1}$ (см. предложение 8 и следствие 3).

3) Пусть теперь все ретракты унитрейда U по любой координате имеют ранг 2 и $\operatorname{rank}(U) = 4$. Тогда $U = U[f]$, где $f = x^a \oplus x^b \oplus x^c \oplus x^e$ и попарные расстояния между наборами a, b, c, e не меньше 2. При этом в любом ретракте расстояния между двумя непересекающимися парами наборов равны 1, поэтому в каждой координате два набора из a, b, c, e принимают одно значение, а два другие – другое. Без ограничения общности можно считать, что $a_i = 1$ и $(b_i, c_i, e_i) \in \{(0,0,1), (0,1,0), (1,0,0)\}$ для всех $i = 1, \dots, n$.

Если какой-то элемент из $E = \{(0,0,1), (0,1,0), (1,0,0)\}$ не встречается среди векторов (b_i, c_i, e_i), то унитрейд $U[f]$ разложим. А именно, $f = (x^u \oplus 1)(x^v \oplus 1)$ для некоторых наборов u и v.

Если все элементы множества E встречаются по одному разу, то унитрейд U эквивалентен унитрейду (1) и имеет ранг 3. Если все элементы множества E встречаются среди векторов (b_i, c_i, e_i) и какой-то из них встречается в координатах i и i', $i \neq i'$, то ретракт по координате i имеет ранг не менее 3. ▲

Для набора векторов $W \subset Q_3^n$ определим $r(W)$ как число позиций, в которых все наборы из W совпадают, если в каждой позиции наборы из W имеют не более двух различных значений. Если же найдется позиция, в которой присутствуют все три различных символа, то положим $r(W) = -\infty$, т.е. $2^{r(W)} = 0$.

Предложение 21. *Пусть* $f(x) = \bigoplus\limits_{v \in V} x^v$, *где* $V \subset Q_3^n$. *Тогда*

$$|U[f]| = \sum_{t=1}^{|V|} (-2)^{t-1} \sum_{W \subset V,\, |W|=t} 2^{r(W)}.$$

Доказательство. Известна формула, подобная формуле включения-исключения:

$$|\mathrm{supp}(\chi_{A_1} \oplus \ldots \oplus \chi_{A_s})| =$$
$$= \sum_i |A_i| - 2\sum_{i \neq j} |A_i \cap A_j| + 2^2 \sum_{i \neq j \neq k} |A_i \cap A_j \cap A_k| - \ldots + (-2)^{s-1} |A_1 \cap \ldots \cap A_s|.$$

Как было отмечено в § 3, справедливы равенства $U[x^{v^1} \oplus x^{v^2} \oplus \ldots \oplus x^{v^s}] = U[x^{v^1}] \oplus \oplus \ldots \oplus U[x^{v^s}]$ и $U[x^v] = \chi_{\{0,\pm 1\}_v}$.

Нетрудно видеть, что $|\{0,\pm 1\}_{v^1} \cap \ldots \cap \{0,\pm 1\}_{v^s}| = 2^{r(\{v^1,\ldots,v^s\})}$. Тогда требуемая формула следует из подстановки этого равенства в первую формулу. ▲

Пусть $v^i \in \{0,\pm 1\}^n$. Рассмотрим матрицу $\{v_j^i\}$ размера $3 \times n$, строками которой являются векторы $v^i \in V$, $|V| = 3$. Пусть матрица содержит $k_1(V)$ столбцов вида *acc*, $k_2(V)$ – *cac*, $k_3(V)$ – *cca* и $k_4(V)$ столбцов, состоящих из всех различных символов. Тогда из предложения 21 вытекает

Предложение 22. *Пусть* $V \subset Q_3^n$, $\mathrm{rank}(U[f^V]) = 3$ *и все три монома не совпадают ни в какой координате. Тогда* $|U[x^{v^1} \oplus x^{v^2} \oplus x^{v^3}]| = 3 \cdot 2^n - 2(2^{k_1(V)} + + 2^{k_2(V)} + 2^{k_3(V)}) + 4\delta(k_4(V))$, *где* $\delta(k) = 0$, *если* $k > 0$, *и* $\delta(k) = 1$, *если* $k = 0$.

Рассмотрим все возможные битрейды ранга 3 мощности до $2{,}5 \cdot 2^n$ включительно.

Заметим, что если $d(u,v) = 1$, то $x^u \oplus x^v = x^w$ для некоторого w. Поэтому достаточно рассматривать случай, когда $k_i \leqslant n-2$, где $i = 1,2,3$ и $n = k_1+k_2+k_3+k_4$.

1. Пусть $k_1 = \max\limits_{i=1,2,3} k_i = n-2$. Тогда возможны следующие наборы

1.1. $(k_1,k_2,k_3,k_4) = (n-2,2,0,0)$. Битрейд по предложению 17(a). Мощность битрейда $3 \cdot 2^n - 2(2^{n-2}+4+1)+4 = 2{,}5 \cdot 2^n - 6$. При $n = 3$ ранг битрейда равняется 2.

1.2. $(k_1,k_2,k_3,k_4) = (n-2,1,1,0)$. Не битрейд по предложению 17(b).

1.3. $(k_1,k_2,k_3,k_4) = (n-2,0,0,2)$. Не битрейд по следствию 6.

1.4. $(k_1,k_2,k_3,k_4) = (n-2,1,0,1)$. Битрейд по следствию 5. Мощность битрейда $3 \cdot 2^n - 2(2^{n-2}+2+1) = 2{,}5 \cdot 2^n - 6$. При $n = 3$ ранг битрейда равняется 2.

2. Пусть $k_1 = \max\limits_{i=1,2,3} k_i = n-3$. Тогда возможны следующие наборы.

2.1. $(k_1,k_2,k_3,k_4) = (n-3,3,0,0)$. Битрейд по предложению 17(a). Мощность битрейда $3 \cdot 2^n - 2(2^{n-3}+8+1)+4 = 2{,}5 \cdot 2^n + 2^{n-2} - 14$. При $n = 4$ битрейд имеет ранг 2, при $n = 5$ совпадает со случаем 1.1, при $n > 5$ мощность больше $2{,}5 \cdot 2^n$.

2.2. $(k_1,k_2,k_3,k_4) = (n-3,2,1,0)$. Не битрейд по предложению 17(b).

2.3. $(k_1, k_2, k_3, k_4) = (n-3, 2, 0, 1)$. Битрейд по следствию 5. Мощность битрейда $3 \cdot 2^n - 2(2^{n-3} + 4 + 1) = 2{,}5 \cdot 2^n + 2^{n-2} - 10$. При $n = 4$ совпадает со случаем 1.4, при $n = 5$ имеем мощность $2{,}5 \cdot 2^n - 2$, при $n > 5$ мощность больше $2{,}5 \cdot 2^n$.

2.4. $(k_1, k_2, k_3, k_4) = (n-3, 1, 1, 1)$. Битрейд по следствию 5. Мощность битрейда $3 \cdot 2^n - 2(2^{n-3} + 2 + 2) = 2{,}5 \cdot 2^n + 2^{n-2} - 8$. При $n = 4$ имеем мощность $2{,}5 \cdot 2^n - 4$, при $n = 5$ имеем мощность $2{,}5 \cdot 2^n$, при $n > 5$ мощность больше $2{,}5 \cdot 2^n$.

2.5. $(k_1, k_2, k_3, k_4) = (n-3, 0, 1, 2)$. Не битрейд по следствию 6.

2.6. $(k_1, k_2, k_3, k_4) = (n-3, 0, 0, 3)$. Битрейд по следствию 5. Мощность битрейда $3 \cdot 2^n - 2(2^{n-3} + 1 + 1) = 2{,}5 \cdot 2^n + 2^{n-2} - 4$. При $n = 3$ имеем мощность $2{,}5 \cdot 2^n - 2$, при $n = 4$ имеем мощность $2{,}5 \cdot 2^n$, при $n > 4$ мощность больше $2{,}5 \cdot 2^n$.

Если $\max\limits_{i=1,2,3} k_i < n - 3$, то мощность унитрейда больше $2{,}5 \cdot 2^n$.

Теперь рассмотрим разложимые битрейды (см. предложение 11).

3. Если оба сомножителя в декартовом произведении не являются булевыми гиперкубами, то по предложению 8 их мощности могут принимать значение $\frac{3}{2}2^n$, $\frac{7}{4}2^n$ и т.д. Поскольку $\frac{3}{2}\frac{7}{4} > \frac{5}{2}$, мощность не более 2,5 от минимальной, а именно $2{,}25 \cdot 2^n$, $n \geqslant 4$, имеют только произведения битрейдов мощности вида $\frac{3}{2}2^{n_1}$.

Суммируя проведенный выше перебор и учитывая возможность декартова умножения на булев гиперкуб (см. предложение 8), делаем вывод, что справедлива

Теорема 5 (мощности малых троичных битрейдов). *В гиперкубе Q_3^{n+m} при любом $m \geqslant 0$ имеются только следующие битрейды мощности более 2^{n+m+1} и не более $5 \cdot 2^{n+m-1}$:*

i) $2^m(2{,}5 \cdot 2^n - 6)$ *при любых* $n \geqslant 4$ (1.1 *и* 1.4);
ii) $2^m(2{,}5 \cdot 2^5 - 2)$ *при* $n = 5$ (2.3);
iii) $2^m(2{,}5 \cdot 2^3 - 2)$ *при* $n = 3$ (2.4, 2.6 *и* 3);
iv) $2^m(2{,}5 \cdot 2^4)$ *при* $n = 4$ (2.4 *и* 2.6).

Рассмотрим унитрейд U мощности не более $2{,}5 \cdot 2^n$ в Q_k^n, $k > 3$. Если по одному из направлений он пересекается не менее чем с четырьмя гиперплоскостями, то пересечение с каждой гиперплоскостью имеет мощность 2^{n-1} или $3 \cdot 2^{n-2}$ (см. предложение 8). Тогда мощность унитрейда U может равняться $2 \cdot 2^n$, $2{,}25 \cdot 2^n$ или $2{,}5 \cdot 2^n$. Как показано выше, битрейды мощностей $2{,}25 \cdot 2^n$ и $2{,}5 \cdot 2^n$ имеются в троичных гиперкубах. Помимо них в гиперкубах Q_k^n при $k > 3$ имеются битрейды той же мощности, состоящие из двух непересекающихся компонент; а также битрейды вида $U = U' \times \{0,1\}^{n-2}$, где $U' \subset Q_k^2$ – цикл длины 8 или 10. В Q_4^3 нетрудно построить битрейд мощности $2{,}25 \cdot 2^3 = 18$. Аналогично доказательству предложения 12 нетрудно получить, что в гиперкубах Q_4^n, $n \geqslant 3$, имеются битрейды мощности $9 \cdot 2^{n-2}$.

Из сказанного выше имеем

Следствие 7 (мощности малых битрейдов). *Возможные малые мощности (не более $2{,}5 \cdot 2^n$) битрейдов в гиперкубах Q_k^n при $k > 3$ исчерпываются тем же списком, что в теореме* 5, *и дополнительной возможной мощностью 2^{n+1}.*

§ 5. Число битрейдов

5.1. Нижняя оценка числа битрейдов. Вначале выясним, какова максимальная мощность подмножества гиперкуба Q_k^n, если все попарные расстояния между его элементами нечетные. Начнем с рассуждений, касающихся набора вершин в евклидовом пространстве.

Пусть $\{v_1, \ldots, v_n\} \subset \mathbb{R}^m$ и квадраты попарных евклидовых расстояний между векторами v_i и v_j равны $d_{ij} = \|v_i - v_j\|_2^2$. Определителем Кэли – Менгера называется

$$\det\begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & d_{11} & d_{12} & \dots & d_{1n} \\ 1 & d_{21} & d_{22} & \dots & d_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & d_{n1} & d_{n2} & \dots & d_{nn} \end{pmatrix} = (-1)^{n+1}2^n(n!)^2(\mathrm{Vol}_{n-1})^2,$$

где Vol_{n-1} – $(n-1)$-мерный объем выпуклой оболочки множества $\{v_1, \dots, v_n\}$. Доказательство этой формулы объема через определитель можно найти, например, в монографиях [23, § 40; 24, § 4.7]. Нам важно, что при $n-1 > m$ определитель равен нулю, поскольку $\mathrm{Vol}_{n-1} = 0$. Из свойств определителя можно вывести следующую известную лемму.

Лемма. *Пусть $A \subset \mathbb{R}^m$, все попарные квадраты евклидовых расстояний между точками множества A целые нечетные и $|A| = m+2$. Тогда $(m+2) \equiv 0 \bmod 4$.*

Доказательство. Пусть $n = |A| = m+2$. Проведем несколько операций сложения строк и столбцов, не меняющих определитель. Вычтем первую строку матрицы из остальных. Получим равенство

$$\det\begin{pmatrix} 0 & 1 & 1 & \dots & 1 \\ 1 & -1 & c_{12} & \dots & c_{1n} \\ 1 & c_{21} & -1 & \dots & c_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & c_{n1} & c_{n2} & \dots & -1 \end{pmatrix} = 0,$$

где числа $c_{ij} = d_{ij} - 1$ четные. Теперь прибавим сумму столбцов от второго до $(n+1)$-го к первому столбцу, а затем сумму строк от второй до $(n+1)$-й к первой строке. Получим равенство

$$\det\begin{pmatrix} b & a_1 & a_2 & \dots & a_n \\ a_1 & -1 & c_{12} & \dots & c_{1n} \\ a_2 & c_{21} & -1 & \dots & c_{2n} \\ \dots & \dots & \dots & \dots & \dots \\ a_n & c_{n1} & c_{n2} & \dots & -1 \end{pmatrix} = 0,$$

где $a_i = \sum\limits_j c_{ij} = \sum\limits_j c_{ji}$ и $b = n + \sum\limits_i a_i = n + 2\sum\limits_{i<j} c_{ij}$. Любая диагональ матрицы, кроме главной, содержит как минимум два четных числа, поэтому произведение элементов диагонали кратно 4. Следовательно, произведение элементов главной диагонали также должно делиться на 4. Тогда $n \equiv b \equiv 0 \bmod 4$. ▲

Следствие 8. *Пусть $A \subset \mathbb{R}^m$ и все попарные квадраты евклидовых расстояний между точками множества A целые нечетные. Тогда $|A| \leqslant m+2$.*

Доказательство. Докажем от противного. Пусть имеется такой набор из $m+3$ точек в $\mathbb{R}^m$. Тогда он также содержится в $\mathbb{R}^{m+1}$ и удовлетворяет условию леммы, т.е. $m+3 \equiv 0 \bmod 4$. Кроме того, его поднабор из $m+2$ точек в $\mathbb{R}^m$ также удовлетворяет условию леммы и $m+2 \equiv 0 \bmod 4$. ▲

Следствие 9. (a) *Пусть $A \subset Q_k^m$ и все попарные расстояния Хэмминга между точками множества A нечетны. Тогда $|A| \leqslant (q-1)m+2$.*

(b) *Пусть $A \subset Q_k^m$ и для любых трех точек из A сумма попарных расстояний нечетна. Тогда $|A| \leqslant (q-1)m+3$.*

Доказательство. (a) Закодируем элементы Q_k наборами действительных чисел длины $k-1$ с попарными евклидовыми расстояниями 1 (вершинами симплекса). При этом словам из Q_k^m будут сопоставлены векторы $(q-1)m$-мерного евклидова пространства, причем расстояние Хэмминга между словами равно квадрату евклидова расстояния между соответствующими векторами.

(b) Рассмотрим произвольную точку $a \in A$ и обозначим через A' множество точек из A на нечетном расстоянии от a и через A'' множество точек из $A \setminus \{a\}$ на четном расстоянии от a. Легко видеть, что расстояние между b и c нечетно, если $b, c \in A'$ или $b, c \in A''$, и четно, если $b \in A'$, $c \in A''$ или $c \in A'$, $b \in A''$. Всем наборам из $A' \cup \{a\}$ припишем в конце 0, а наборам из A'' припишем в конце 1. Получим множество $B \subset Q_k^m \times Q_2$ с попарно нечетными расстояниями. Применяя далее технику, аналогичную (a), получаем множество точек в евклидовом пространстве с попарно нечетными квадратами расстояний. Поскольку для кодирования значений последней координаты достаточно всего одной евклидовой координаты, оценка получается на 1 больше, чем в случае (a). ▲

Для случая, когда q – степень простого числа, общеизвестно

Предложение 23. *В гиперкубе Q_q^m при $m = \dfrac{q^t - 1}{q - 1}$ имеется эквидистантный код H_t мощности $(q-1)m + 1 = q^t$ с кодовым расстоянием q^{t-1}, дуальный к коду Хэмминга.*

Теорема 6. (a) *При $n = \dfrac{3^t - 1}{2}$ найдется множество $V \subset Q_3^n$, такое что для любого $W \subseteq V$ унитрейд $U[f^W]$ является битрейдом и $|V| = 2n + 1$.*

(b) *Пусть $V \subset Q_3^n$, $n \geqslant 3$, и для любого $W \subseteq V$ унитрейд $U[f^W]$ является битрейдом. Тогда* $\operatorname{rank}(U[f^V]) \leqslant 3n$.

Доказательство. Утверждение (a) следует из предложений 19 и 23. Докажем утверждение (b).

Без ограничения общности полагаем, что $|V| = \operatorname{rank}(U[f^V])$. Положим $\pi(1) = 3$ и $\pi(2) = 6$. Обозначим через $\pi(n)$, $n \geqslant 3$, максимальную мощность множества $V \subset Q_3^n$, в котором любая тройка вершин порождает битрейд. Будем доказывать неравенство $\pi(n) \leqslant 3n$ по индукции. При $n = 3$ неравенство можно проверить непосредственно. Если любая тройка вершин в множестве V находится в общем положении, то требуемое следует из предложения 18(b) и следствия 9(b). Теперь докажем несколько вспомогательных предложений о структуре множества V, когда не все тройки в нем находятся в общем положении.

По предложению 17 любая тройка вершин из V, не находящаяся в общем положении, должна удовлетворять условию предложения 17(a), т.е. одна из вершин должна находится между двумя другими. Это свойство будем называть упорядоченностью тройки.

Рассмотрим максимальный набор $v^0, \ldots, v^m \in V$, такой что любая тройка вершин из него упорядочена. Без ограничения общности (применяя, если нужно, изометрии гиперкуба) можно считать[3], что $v^0 = \bar{0}$, $v^i = (2 \ldots 20 \ldots 0)$ и $v^0 \prec v^1 \prec \ldots \prec v^m$, где $m > 1$. Множество координат j, в которых $v_j^m = 2$, обозначим через M. Множество координат, в которых вершина v^i отличается от v^{i+1}, обозначим через M_i.

В множестве $V \setminus V_0$, где $V_0 = \{v^0, \ldots, v^m\}$, нет вершин, имеющих только 0 и 2 на позициях из множества M, поскольку это противоречит либо максимальности набора V_0, либо предложению 17.

Пусть найдется вершина $u \in V$, такая что все три тройки вершин $\{v^{i_1}, v^{i_2}, u\}$, $\{v^{i_1}, v^{i_3}, u\}$ и $\{v^{i_2}, v^{i_3}, u\}$ находятся в общем положении. Поскольку $d(v^{i_1}, v^{i_2}) + d(v^{i_2}, v^{i_3}) = d(v^{i_1}, v^{i_3})$, нетрудно убедиться, что сумма длин сторон в одном из трех треугольников четна. По следствию 6 имеем противоречие. Будем ссылаться на это замечание как на свойство $(*)$.

Покажем, что вершина $u \in V \setminus V_0$ содержит 1 только в одном из блоков M_i, $i = 0, \ldots, m-1$. Если вершина u содержит 1 в двух координатах, из M_i и из M_j,

[3] Здесь удобнее использовать алфавит $\{0, 1, 2\}$ с определенным в начале статьи частичным порядком $0 \prec 2$ и $1 \prec 2$.

$i < j$, то u находится в общем положении с любыми двумя из трех вершин v^0, v^i, v^m. Получили противоречие по свойству $(*)$. Обозначим через U_i множество вершин из V, имеющих хотя бы одну 1 в блоке M_i.

Покажем, что любая вершина u из U_j имеет в координатах каждого блока M_i, $i < j$, одинаковые символы, либо нули, либо двойки. Действительно, в противном случае тройка вершин v^0, v^{j-1}, u не в общем положении, но не упорядочена, поэтому по предложению 17(b) не порождает битрейд. Аналогично, любая вершина u из U_j имеет в координатах каждого из блоков M_i, $i > j$, одинаковые символы (достаточно рассмотреть тройку v^m, v^j, u).

Пусть вершина $u^0 \in U_0$ содержит 2 в координате из некоторого блока M_i, $i > 0$. Тогда тройка вершин v^1, v^m, u^0 не в общем положении и не упорядочены, поэтому по предложению 17(b) не порождает битрейд. Значит, $u^0 \in U_0$ содержит только нули в координатах из любых блоков M_i, $i > 0$. Покажем, что никакая вершина $u^j \in U_j$, $j > 0$, не содержит 0 в блоке M_0. Действительно, в этом случае вершина u^j находится в общем положении с любыми двумя из трех вершин u^0, v^1, v^m. Получили противоречие по свойству $(*)$. Аналогично, рассмотрев случай, когда вершина $u^{m-1} \in$ $\in U_{m-1}$ содержит 0 в координате из некоторого блока M_i, $i < m-1$, а также случаи когда вершина $u^j \in U_j$, $m-1 > j > 0$ содержит символ 0 в блоках M_i, $i < j$, или символ 2 в блоках M_i, $i > j$, приходим к выводу, что единственной непротиворечивой возможностью является следующая: вершина $u^j \in U_j$, $j = 0, \ldots, m-1$, содержит только двойки в блоках M_i при $i < j$ и только нули в блоках M_i при $i > j$.

Покажем от противного, что две вершины $u^i \in U_i$, $u^j \in U_j$, $i < j$, не могут иметь две разные ненулевые k-е координаты при $k > |M|$. Пусть $u^i(k) = 1$, $u^j(k) = 2$. Рассмотрим тройку вершин v^0, v^i, u^j. Она упорядочена (выполнено условие предложения 17(a)), но любая пара из вершин этой тройки находится в общем положении с вершиной u^i. Получили противоречие по свойству $(*)$.

Мы показали, что $u^i(k) = u^j(k)$ или $u^i(k) = 0$, или $u^j(k) = 0$ при $k > |M|$. Теперь покажем, что и случай $u^i(k) = u^j(k) \neq 0$ для некоторого $k > |M|$ невозможен. Действительно, в этом случае тройка вершин v^i, u^i, u^j, $i < j$, не в общем положении и не упорядочена, поэтому по предложению 17(b) не порождает битрейд. Таким образом, координаты в дополнении к множеству M можно разделить на не пересекающиеся группы $N_0, \ldots, N_{m-1}$ так, что для любой вершины $u^i \in U_i$ ненулевыми являются только координаты из множества N_i.

Рассмотрим сужение набора вершин $W_i = \{v^0, v^m\} \cup U_i$ на координаты $M_i \cup N_i$. Нетрудно видеть, что некоторая тройка вершин из W_i находится в общем положении тогда и только тогда, когда в общем положении находится ее сужение на координаты $M_i \cup N_i$. При этом четность суммы расстояний между вершинами тройки на всех координатах и только на множестве $M_i \cup N_i$ совпадают. Если же сужение тройки вершин на $M_i \cup N_i$ находится не в общем положении и не упорядочено, то тройка вершин не упорядочена и на множестве всех координат. Следовательно, тройка вершин из W_i порождает битрейд, только если она порождает битрейд на сужении.

Отсюда следует, что мощность множества $W_i = \{v^0, v^m\} \cup U_i$ не превышает $\pi(|M_i| + |N_i|)$, если $|M_i| + |N_i| \geqslant 3$. При $|M_i| + |N_i| = 1$ неравенство $|W_i| \leqslant 3 = \pi(1)$ очевидно. Если $|M_i| + |N_i| = 2$, то неравенство $|W_i| \leqslant 6 = \pi(2)$ нетрудно доказать, рассматривая сужения вершин на набор из трех координат, включающий множества N_i и M_i. Тогда по предположению индукции имеем

$$|V| = |V_0| + \sum_{i=0}^{m-1} |U_i| \leqslant m + 1 + \sum_{i=0}^{m-1} (\pi(|M_i| + |N_i|) - 2) \leqslant 3n. \quad \blacktriangle$$

Далее нам понадобится код H_t при $q = 3$. Будем оценивать снизу число неэквивалентных битрейдов, выбирая наборы вершин из кода с попарно нечетными расстo-

яниями для порождения битрейдов. Теорема 6 показывает, что наша оценка почти исчерпывает возможности этого способа построения множества битрейдов большой мощности.

Предложение 24. *Пусть D – кодовое расстояние множества $V_i \subset Q_3^n$ и $|V_i| \leqslant 2^{D-3}$ при $i = 1, 2$. Тогда из эквивалентности унитрейдов $U[f^{V_1}]$ и $U[f^{V_2}]$ следует эквивалентность множеств V_1 и V_2.*

Доказательство. Пусть унитрейд $U[f^V]$ эквивалентен унитрейду U'. Тогда $U' = U[f^{V'}]$, где множество V' эквивалентно множеству V. Однако соответствие неоднозначно, т.е. в общем случае имеются другие множества $W \subset Q_3^n$, для которых $U' = U[f^W]$.

Достаточно показать, что если $2^{n-2} > |V|2^{n-D+1}$, то множество V с кодовым расстоянием D восстанавливается однозначно по унитрейду $U[f^V]$. Рассмотрим произвольный подкуб $U[x^v]$. Имеем $v \in V$, если и только если $|U[f^V] \cap U[x^v]| \geqslant 2^n - 2^{n-2}$. Действительно, поскольку $|U[x^w] \cap U[x^v]| = 2^{n-d(v,w)}$ для любого $w \in Q_3^n$, справедливы неравенства

1) $|U[f^V] \cap U[x^v]| \geqslant 2^n - |V|2^{n-D}$ при $v \in V$;
2) $|U[f^V] \cap U[x^w]| < 2^{n-1} + |V|2^{n-D+1}$ при $w \notin V$.

Имеем $2^n - |V|2^{n-D} \geqslant 2^{n-1} + |V|2^{n-D+1}$ при $|V| \leqslant 2^{D-3}$. ▲

Обозначим через $\mathrm{sp}(v)$ состав вектора v, например, $\mathrm{sp}(0, 1, 1, 0, -1) = (2, 2, 1)$. Будем говорить, что состав вектора *уникальный* для некоторого линейного пространства, если в нем нет других векторов с тем же составом.

Предложение 25. *Пусть $W \subset Q_k^n$ – линейное подпространство над $\mathrm{GF}(k)$ и в W имеется базис B, состоящий из векторов с уникальным составом. Тогда в W имеется не менее $2^{|W|-\dim W-1}/|W|$ неэквивалентных подмножеств векторов.*

Доказательство. Рассмотрим подмножества $C \subset W$, которые содержат нулевой вектор и базис, т.е. $B \subset C$ и $\bar{0} \in C$. Пусть $\varphi_{\pi,a}$ – изометрия, переводящая одно такое множество C в другое C', т.е. $\varphi_{\pi,a}(C) = \pi(C) + a = C'$. Поскольку $\pi(\bar{0}) = \bar{0}$, имеем $a \in C' \subset W$. Рассмотрим базисный вектор $v \in C \cap C'$ с уникальным составом. Из равенства $\mathrm{sp}(\pi(v)) = \mathrm{sp}(v)$ и уникальности состава имеем $\pi(v) = v$. Из линейности автотопии π, т.е. из равенства $\pi(\alpha u + \beta w) = \alpha\pi(u) + \beta\pi(w)$, следует, что π действует тождественно на W. Тогда $\varphi_{\pi,a}(u) = u + a$, где $a \in W$. Очевидно, что число подможеств в W, содержащих некоторый базис и нулевой вектор, равно $2^{|W|-\dim W-1}$, причем любой класс эквивалентности подмножеств содержит не больше элементов, чем $|W|$. ▲

Рассмотрим порождающую матрицу A кода H_t размерности $t > 1$ (см. предложение 23). Матрица A содержит единичную подматрицу. Проведем следующее преобразование порождающей матрицы A: добавим к ней столбцы единичной матрицы в количестве 2^{k-1} копий k-го столбца при $k = 2, \ldots, t$. Линейный код, порожденный преобразованной таким способом матрицей, обозначим через H'_t. Все векторы кода H_t (за исключением нулевого) имеют одинаковый нечетный вес, поэтому разность между числом координат равных 1 и -1 нечетная, а значит, добавление четного числа столбцов в порождающую матрицу не может привести к одинаковому составу у пар коллинеарных векторов из H'_t. Неколлинеарные векторы из H'_t имеют разный вес по построению. Поэтому код H'_t имеет базис (строки порождающей матрицы A) из векторов с уникальным составом. Расстояние между любой парой векторов из кода H_t нечетно. Поскольку в порождающую матрицу A было добавлено четное число копий единичных столбцов, расстояния между любой парой векторов из кода H'_t также нечетно. Длина кода H'_t равна $2^t - 2 + \dfrac{3^t - 1}{2}$.

Теорема 7 (нижняя граница). *Число неэквивалентных битрейдов размерности n не меньше $2^{(2/3-o(1))n}$ при $n \to \infty$.*

Доказательство. При $2^t - 2 + \dfrac{3^t-1}{2} \leqslant n < 2^{t+1} - 2 + \dfrac{3^{t+1}-1}{2}$ рассмотрим множество H'_t. По предложению 23 кодовое расстояние множества H'_t равно $D = 3^t$. Для достаточно больших t имеем $|H'_t|2^{n-D+1} = 3^t 2^{n-D+1} \leqslant 3^t 2^{2^t - 1 - \frac{3^t+1}{2}} < 2^{n-2}$. Из предложения 24 следует, что эквивалентность двух битрейдов $U(f^V)$ и $U(f^W)$ равносильна эквивалентности множеств $V, W \subset H'_t$. Из предложения 25 следует требуемая оценка числа таких подмножеств. ▲

5.2. Верхняя оценка числа битрейдов. Семейство функций $\mathcal{A} = \bigcup\limits_{n=1}^{\infty} \mathcal{A}_n$, $\mathcal{A}_n \subseteq \{f\colon Q_k^n \to S\}$, $n \in \mathbb{N}$, будем называть *наследственным*, если любое множество функций $\mathcal{A}_n$ замкнуто относительно действия изометрий пространства Q_k^n на аргументы функций и любой ретракт любой функции из $\mathcal{A}_n$ лежит в $\mathcal{A}_{n-1}$. Множество $T \subset Q_k^m$ называется *тестирующим* для множества функций $\mathcal{A}_m$, если для любых $f, g \in \mathcal{A}_m$ из $f|_T = g|_T$ следует $f = g$. Множество T является тестирующим для множества функций $\mathcal{A}_m$ тогда и только тогда, когда $\operatorname{supp}(f-g) \cap T \neq \varnothing$ для любых f и g из $\mathcal{A}_m$, т.е. его дополнение $Q_k^m \setminus T$ не включает носитель разности никаких двух функций из $\mathcal{A}_m$. Поскольку разность двух характеристических функций некоторых комбинаторных конфигураций является битрейдом (в широком смысле), то поиск тестирующих множеств эквивалентен нахождению множеств, не включающих битрейдов.

Предложение 26. *Пусть семейство* $\mathcal{A} = \bigcup\limits_{n=1}^{\infty} \mathcal{A}_n$, $n \in \mathbb{N}$, *наследственное. Пусть* $T \subset Q_k^m$ *– тестирующее множество для* $\mathcal{A}_m$. *Тогда декартово произведение тестирующих множеств* $T^\ell \subset Q_k^{\ell m}$ *является тестирующим для* $\mathcal{A}_{\ell m}$.

Доказательство. Докажем утверждение по индукции. Пусть $f|_{T^\ell} = g|_{T^\ell}$. Тогда по предположению индукции для любого $v \in T$ из $f|_{T^{\ell-1}\times\{v\}} = g|_{T^{\ell-1}\times\{v\}}$ следует, что $f|_{Q_k^{(\ell-1)m}\times\{v\}} = g|_{Q_k^{(\ell-1)m}\times\{v\}}$. Следовательно для любого $w \in Q_k^{(\ell-1)m}$ имеем $f|_{\{w\}\times T} = g|_{\{w\}\times T}$. Множество $\{w\}\times T$ является тестирующим для ретрактов на $\{w\} \times Q_k^m$, поскольку семейство $\mathcal{A}_n$ наследственное. Тогда $f|_{\{w\}\times Q_k^m} = g|_{\{w\}\times Q_k^m}$ для любого $w \in Q_k^{(\ell-1)m}$. ▲

Из определения тестирующего множества и предложения 26 следует

Предложение 27. *Пусть* $\mathcal{A} = \bigcup\limits_{n=1}^{\infty} \mathcal{A}_n$ *– наследственное семейство функций и* $T \subset Q_k^m$ *– тестирующее множество для* $\mathcal{A}_m$. *Тогда* $|\mathcal{A}_{\ell m}| \leqslant |S|^{|T|^\ell}$.

Ниже мы не будем различать унитрейды и их характеристические функции. Семейства битрейдов и унитрейдов являются наследственными (см. предложения 1 и 2). Как следует из формулы (2), тестирующим множеством для семейства троичных унитрейдов (и битрейдов) является любое подмножество в Q_3^n, индуцирующее подграф, изоморфный булеву гиперкубу. Пусть T – тестирующее множество для семейства унитрейдов в Q_3^n. Поскольку число унитрейдов в Q_3^n равняется 2^{2^n}, из предложения 27 следует, что $|T| \geqslant 2^n$. Отметим, что для любого тестирующего множества T его дополнение $Q_3^n \setminus T$ не включает (непустой) унитрейд, и наоборот, если $Q_3^n \setminus T$ включает унитрейд, то множество T не является тестирующим для унитрейдов. Поэтому максимальная мощность подмножества в Q_3^n, не включающего унитрейды, равна $3^n - 2^n$. Для семейства битрейдов аналогичный вопрос остается открытым. Ниже мы по существу доказываем, что найдется подмножество в Q_3^n мощности больше $3^n - 2^n$, не включающее симметрические разности битрейдов.

Предложение 28. *Если найдется унитрейд* $U \subset Q_3^m$, *характеристическая функция которого не является суммой* (*по модулю* 2) *двух битрейдов*, *то для битрейдов в* Q_3^m *найдется тестирующее множество мощности* $2^m - 1$.

Доказательство. Каждой вершине $v \in Q_3^m$ поставим в соответствие переменную x_v. Рассмотрим следующую систему булевых уравнений, однозначно задающих унитрейд U:

(i) $x_a \oplus x_b \oplus x_c = 0$ – для любой одномерной грани $\{a, b, c\}$ в Q_3^m;

(ii) $x_v = 0$ – для любой v из $Q_3^m \setminus U$.

Выберем из уравнений типа (i) независимую подсистему (I), а затем из уравнений типа (ii) – максимальную независимую подсистему (II), которая независима и с уравнениями типа (i). Множество решений подсистемы (I) уравнений типа (i) имеет размерность 2^m, а совместная система – размерность 1, поскольку (см. предложение 4) ни один унитрейд не является подмножеством другого, т.е. нули одной функции не могут быть подмножеством нулей другой характеристической функции унитрейда. Поэтому имеется $2^m - 1$ уравнений в подсистеме (II), которые задаются точками v некоторого множества $T \subset Q_3^m$, $|T| = 2^m - 1$.

Покажем, что T есть тестирующее множество для битрейдов в Q_3^m. Пусть две характеристические функции χ_A и χ_B различных битрейдов A и B совпадают на множестве T, тогда $\chi_U = \chi_A \oplus \chi_B$, поскольку функция $\chi_A \oplus \chi_B$ является решением системы уравнений, задающей унитрейд U. Это противоречит условию. ▲

Вычислительный эксперимент (см. таблицу из п. 4.5) показывает, что число битрейдов в Q_3^7 не больше, чем $2^{2^6} = \sqrt{2^{2^7}}$, т.е. квадратный корень из числа унитрейдов в Q_3^7. Тогда пар битрейдов в Q_3^7 меньше, чем унитрейдов. Таким образом, при $n = 7$ выполнены условия предложения 28. Отсюда получаем

Следствие 10. *Число битрейдов в $Q_3^{7\ell}$ не выше $2^{\alpha^{7\ell}}$, где $\alpha = (2^7 - 1)^{1/7} < 2$.*

Пусть $\beta(n)$ – число битрейдов в Q_3^n. Тогда $\beta(n + m) \leqslant (\beta(n))^{2^m}$, $m = 1, \ldots, 6$. Следовательно, имеется аналогичная оценка числа битрейдов при произвольных $n > 7$.

Теорема 8 (верхняя граница). *Число битрейдов в Q_3^n не выше $2^{\alpha_1^n}$, где $\alpha_1 < 2$.*

Авторы выражают благодарность Информационно-вычислительному центру Новосибирского государственного университета (ИВЦ НГУ) за предоставленные вычислительные ресурсы, участникам семинара "N-арные квазигруппы и смежные вопросы" ИМ СО РАН за плодотворные обсуждения и рецензенту за полезные замечания.

СПИСОК ЛИТЕРАТУРЫ

1. *Кротов Д.С.* Трейды в комбинаторных конфигурациях // Материалы XII Международного семинара "Дискретная математика и ее приложения" им. академика О.Б. Лупанова (Москва, 20–25 июня 2016 г.). М.: Изд-во механико-математического факультета МГУ, 2016. С. 84–96.
2. *Hedayat A.S., Khosrovshahi G.B.* Trades // Handbook of Combinatorial Designs. Boca Raton: Chapman & Hall, 2007. P. 644–648.
3. *Khosrovshahi G.B., Maimani H.R., Torabi R.* On Trades: An Update // Discrete Appl. Math. 1999. V. 95. № 1–3. P. 361–376.
4. *Krotov D.S.* On the Gaps of the Spectrum of Volumes of Trades // J. Combin. Des. 2018. V. 26. № 3. P. 119–126.
5. *Krotov D.S., Mogilnykh I.Yu., Potapov V.N.* To the Theory of q-ary Steiner and Other-Type Trades // Discrete Math. 2016. V. 339. № 3. P. 1150–1157.
6. *Ghorbani E., Kamali S., Khosrovshahi G.B., Krotov D.S.* On the Volumes and Affine Types of Trades // Electron. J. Combin. (to appear).
7. *Cavenagh N.J.* The Theory and Application of Latin Bitrades: A Survey // Math. Slovaca. 2008. V. 58. № 6. P. 691–718.
8. *Cho S.* On the Support Size of Null Designs of Finite Ranked Posets // Combinatorica. 1999. V. 19. № 4. P. 589–595.

9. *Августинович С.В., Соловьева Ф.И.* Построение совершенных двоичных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент // Пробл. передачи информ. 1997. Т. 33. № 3. С. 15–21.
10. *Östergård P.R.J.* Switching Codes and Designs // Discrete Math. 2012. V. 312. № 3. P. 621–632.
11. *Потапов В.Н.* Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Пробл. передачи информ. 2012. Т. 48. № 1. С. 54–63.
12. *Krotov, D.S., Potapov, V.N., Sokolova, P.V.* On Reconstructing Reducible n-ary Quasigroups and Switching Subquasigroups // Quasigroups Relat. Syst. 2008. V. 16. № 1. P. 55–67.
13. *Потапов В.Н., Кротов Д.С.* О числе n-арных квазигрупп конечного порядка // Дискретная математика. 2012. Т. 24. № 1. С. 60–69.
14. *Riener H., Ehlers R., Schmitt B.O., De Micheli G.* Exact Synthesis of ESOP Forms // Advanced Boolean Techniques: Selected Papers from the 13th International Workshop on Boolean Problems. Cham: Springer, 2020. P. 177–194.
15. *Винокуров С.Ф., Казимиров А.С.* О сложности одного класса булевых функций // Изв. Иркутского гос. ун-та. Сер. Математика. 2010. Т. 3. № 4. С. 2–6.
16. *Потапов В.Н.* Многомерные латинские битрейды // Сиб. мат. журн. 2013. Т. 54. № 2. С. 407–416.
17. *Krotov D.S., Potapov V.N.* n-ary Quasigroups of Order 4 // SIAM J. Discrete Math. 2009. V. 23. № 2. P. 561–570.
18. *Ellenberg J.S., Gijswijt D.* On Large Subsets of F_q^n with No Three-Term Arithmetic Progression // Ann. Math. (2). 2017. V. 185. № 1. P. 339–343.
19. *Потапов В.Н.* О булевых функциях, почти уравновешенных в гранях // Прикладная дискретная математика. Приложение. 2012. № 5. С. 23–25.
20. *Kasami T., Tokura N.* On the Weight Structure of Reed–Muller Codes // IEEE Trans. Inform. Theory. 1970. V. 16. № 6. P. 752–759.
21. *Kasami T., Tokura N., Azumi S.* On the Weight Enumeration of Weights Less than $2.5d$ of Reed–Muller Codes // Inform. Control. 1976. V. 30. № 4. P. 380–395.
22. *Kaski P., Östergård, P.R.J.* Classification Algorithms for Codes and Designs. Berlin: Springer, 2006.
23. *Blumenthal L.* Theory and Applications of Distance Geometry. Oxford: Clarendon Press, 1953.
24. *Pak I.* Lectures on Discrete and Polyhedral Geometry. Book draft, 2010. Available at `http://www.math.ucla.edu/~pak/book.htm`.

Кротов Денис Станиславович
Потапов Владимир Николаевич
Институт математики им. С.Л. Соболева СО РАН, Новосибирск
`krotov@math.nsc.ru`
`vpotapov@math.nsc.ru`

Поступила в редакцию
24.12.2018
После доработки
19.09.2019
Принята к публикации
12.11.2019