Сибирский математический журнал
Март—апрель, 2013. Том 54, № 2

УДК 519.14

МНОГОМЕРНЫЕ ЛАТИНСКИЕ БИТРЕЙДЫ

В. Н. Потапов

Аннотация. Подмножество k-значного n-мерного гиперкуба называется *унитрейдом* (*объединенным битрейдом*), если мощности его пересечений с одномерными гранями гиперкуба принимают только два значения 0 и 2. Унитрейд называется *двудольным* (*гамильтоновым*), если соответствующий ему подграф гиперкуба является двудольным (гамильтоновым). Пара долей двудольного унитрейда называется *n-мерным латинским битрейдом.* Для троичного n-мерного гиперкуба определено число различных унитрейдов и получена экспоненциальная нижняя оценка числа неэквивалентных латинских битрейдов. Перечислены все возможные n-мерные латинские битрейды мощности, меньшей чем 2^{n+1}.

Подмножество k-значного n-мерного гиперкуба называется *t-кратным* МДР-*кодом*, если оно пересекается с каждой одномерной гранью гиперкуба ровно по t элементам. Симметрическая разность двух однократных МДР-кодов является двудольным унитрейдом. Каждая из компонент соответствующего латинского битрейда является свитчинговой компонентой одного из этих МДР-кодов. Исследованы вопросы о мощностях компонент МДР-кодов и возможности получения латинских битрейдов заданной мощности из МДР-кодов. Кроме того, доказано, что любой МДР-код вкладывается в гамильтонов двукратный МДР-код.

Ключевые слова: МДР-код, латинский битрейд, унитрейд, компонента.

Введение

Пусть $Q_k = \{0, 1, \dots, k-1\}$. Обозначим через Q_k^n множество упорядоченных k-ичных наборов (вершин) длины n. *Расстоянием Хэмминга* $d(x, y)$ между вершинами $x, y \in Q_k^n$ называется число позиций, в которых наборы x и y различаются. Через ΓQ_k^n обозначим граф минимальных расстояний метрического пространства $\left(Q_k^n, d\right)$. *Гранью размерности* k называется подмножество гиперкуба Q_k^n, состоящее из вершин с одинаковыми фиксированными значениями некоторых $n-k$ координат. В частности, *одномерная грань направления* i, проходящая через вершину $(a_1, \dots, a_n) \in Q_k^n$, определяется как множество $\{(a_1, \dots, a_{i-1}, x, a_{i+1}, \dots, a_n) \mid x \in Q_k\}$.

МДР-*кодом с расстоянием* d называется множество $M \subset Q_k^n$, пересекающееся с каждой $(d-1)$-мерной гранью ровно по одному элементу. Множество W называется *t-кратным* МДР-*кодом*, если оно пересекается с каждой одномерной гранью ровно по t элементам. Понятие кратного МДР-кода с расстоянием d совпадает с понятием корреляционно-иммунной функции порядка $n-d+1$ в Q_k^n. Нетрудно видеть, что множество $M \subset Q_k^n$ является МДР-кодом с расстоянием d тогда и только тогда, когда оно имеет мощность k^{n-d+1} и расстояние между

Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (коды проектов 11–01–00997, 10–01–00616) и ФЦП «Научные и научно-педагогические кадры инновационной России» на 2009–2013 гг. (гос. контракт № 02.740.11.0362).

любыми двумя различными элементами из M не менее d. t-Кратный МДР-код называется *расщепляемым*, если он является объединением t однократных МДР-кодов. Кратные нерасщепляемые МДР-коды с расстоянием 2 рассматриваются в [1]. В дальнейшем в статье рассматриваются МДР-коды (в том числе кратные) только с расстоянием 2.

Граф называется *гамильтоновым*, если он содержит простой цикл, проходящий через все вершины графа. Для однократного МДР-кода M можно определить граф минимальных расстояний $\Gamma_2 M$, в котором соединены ребром вершины, находящиеся на расстоянии 2. Из определения МДР-кода нетрудно получить, что граф $\Gamma_2 M$ всегда является гамильтоновым. Рассмотрим двукратный МДР-код $D \subset Q_k^n$, через ΓD обозначим граф минимальных расстояний множества D, т. е. соединим ребрами вершины, находящиеся на расстоянии 1. Доказано (§ 3), что любой МДР-код вкладывается в гамильтонов двукратный МДР-код. Заметим, что двукратный МДР-код D расщепляем тогда и только тогда, когда граф ΓD является двудольным.

Множество $B \subset Q_k^n$ будем называть *унитрейдом*[1)], если мощности его пересечений с одномерными гранями принимают только два значения 0 и 2. Унитрейд $B \subset Q_k^n$ будем называть *двудольным*, если подграф ΓB графа ΓQ_k^n, порожденный множеством вершин B, двудольный. Ясно, что симметрическая разность двух МДР-кодов является двудольным унитрейдом.

Поскольку в каждой одномерной грани МДР-кода содержится только одна точка, можно считать, что МДР-код в Q_k^n неявно задает некоторую функцию от $n-1$ переменной. Таблица значений этой функции является латинским $(n-1)$-мерным кубом порядка k (латинским квадратом при $n = 3$), а МДР-код можно рассматривать как график функции. *Латинским битрейдом* называют пару частичных латинских квадратов, объединение графиков которых является двудольным унитрейдом. Мы распространяем название «латинский битрейд» на многомерный случай. Кроме того, в тех случаях, когда двудольный унитрейд однозначно разделяется на доли (состоит из одной компоненты связности), будем называть *латинским битрейдом* не только пару долей, но и сам унитрейд.

Двудольный унитрейд (латинский битрейд) B будем называть *полученным* из МДР-кода M_1 (возможно, кратного), если найдется такой МДР-код M_2 (той же кратности), что $B = M_1 \triangle M_2$. В этом случае множество $B \cap M_1$ будем называть *компонентой* МДР-кода M_1 в соответствии с общим представлением о свитчинговой компоненте кода как о подмножестве кода, замена которого равномощным множеством сохраняет кодовое расстояние. Свитчинговым компонентам МДР-кодов M_1 и M_2 соответствуют доли компонент связности графа ΓB — компоненты латинского битрейда, соответствующего унитрейду B.

В статье рассматриваются вопросы о числе унитрейдов и латинских битрейдов в гиперкубе Q_k^n, о возможности получения латинских битрейдов из МДР-кодов и о мощностях компонент МДР-кодов. В § 2 для троичного n-мерного гиперкуба определено число различных унитрейдов (2^{2^n}) и получена асимптотическая (при $n \to \infty$) нижняя оценка[2)] $e^{\Omega(\sqrt{n})}$ числа неэквивалентных латинских битрейдов. Нетривиальные верхние оценки числа латинских битрейдов неизвестны. При $k \geq 4$ число и даже асимптотика двойного логарифма числа унитрейдов и латинских битрейдов также остаются неизвестными. Связь вопроса о числе латинских битрейдов в гиперкубе Q_k^n с другими комбинаторными

[1)] В [2] использовался термин «2-код».

[2)] Равенство $f(n) = \Omega(g(n))$ означает, что $f(n) \geq cg(n)$ для некоторого $c > 0$ при $n \to \infty$.

задачами обсуждается в [3].

В § 1 перечислены все возможные n-мерные унитрейды мощности, меньшей чем 2^{n+1}, и доказано, что для каждого $s \in \{0, \dots, n-1\}$ имеется единственный с точностью до эквивалентности n-мерный латинский битрейд мощности $2^{n+1} - 2^{s+1}$. В § 3 доказана возможность получения этих латинских битрейдов из двукратных МДР-кодов и тем самым частично определен спектр мощностей компонент двукратных МДР-кодов.

В [1, 4] имеется конструкция, позволяющая получать из t-кратных МДР-кодов t-кратные двоичные совершенные коды. Вопросы, связанные с мощностями компонент совершенных двоичных кодов и гамильтоновости графов этих кодов, рассматриваются в [5, 6]. Полученные в данной работе результаты относительно мощностей компонент МДР-кодов и гамильтоновости графов МДР-кодов могут быть использованы при исследовании свойств других классов кодов.

§ 1. Мощности унитрейдов

Предложение 1. (a) *Декартово произведение двух унитрейдов является унитрейдом.*

(b) *Декартово произведение двух двудольных унитрейдов является двудольным унитрейдом.*

Доказательство п. (a) непосредственно вытекает из определений, при доказательстве п. (b) пользуемся тем, что декартово произведение двудольных графов является двудольным графом.

Следующие два утверждения доказаны в [3] при $k = 4$, однако их можно доказать точно так же при произвольном $k \geq 2$.

Предложение 2. *Пусть $B \subset Q_k^n$ — непустой унитрейд, тогда $|B| \geq 2^n$.*

Предложение 3. *Пусть $B \subset Q_k^n$ — унитрейд. Следующие условия эквивалентны:*

(a) $|B| = 2^n$,

(b) *для любой m-мерной грани мощность ее пересечения с B равняется* 0 *или* 2^m,

(c) *унитрейд B пересекается только с двумя гипергранями каждого направления,*

(d) *подграф графа ΓB изоморфен булеву кубу ΓQ_2^n.*

Из предложения 2 непосредственно вытекает, что в Q_2^n существует единственный унитрейд, совпадающий со всем множеством Q_2^n.

Рассмотрим вопрос о спектре мощностей унитрейдов.

Предложение 4. *Пусть $B \subset Q_k^n$ — унитрейд и $2^{n+1} > |B| \geq 2^n$. Тогда $|B| = 2^{n+1} - 2^{s+1}$, где $s \in \{0, \dots, n-1\}$.*

Доказательство проведем индукцией по n. При $n = 1$ утверждение очевидно, предположим, что оно верно при $n - 1$. Если унитрейд $B \subset Q_k^n$ содержится в объединении двух гиперграней каждого направления, то $|B| = 2^n$ по предложению 3.

Если унитрейд B пересекается с четырьмя гипергранями одного направления, то по предложению 3 его мощность больше или равна 2^{n+1}. Пусть унитрейд B пересекается с тремя гипергранями одного направления. Если пересечение хотя бы с одной из них имеет мощность, большую либо равную 2^n, то по предложению 2 имеем $|B| \geq 2^{n+1}$. В противном случае по предположению индукции имеем $|B| = 3 \cdot 2^n - 2^{s_1} - 2^{s_2} - 2^{s_3}$. Поскольку неравенство $2^{s_1} + 2^{s_2} + 2^{s_3} > 2^n$ выполнено, только когда как минимум два из трех s_i равняются $n-1$, имеем $|B| = 2^{n+1} - 2^s$.

Как видно из доказательства предложения 4, унитрейд $B \subset Q_k^n$ мощности, меньшей чем 2^{n+1}, пересекается не более чем с тремя гипергранями любого направления, следовательно, может быть вложен в троичный гиперкуб.

Предложение 5. (a) *Симметрическая разность двух унитрейдов в гиперкубе Q_3^n является унитрейдом.*

(b) *Если симметрическая разность двух двудольных унитрейдов в гиперкубе Q_k^n является унитрейдом, а их пересечение порождает связный подграф в Q_k^n, то симметрическая разность является латинским битрейдом.*

Доказательство п. (a) непосредственно вытекает из определений, при доказательстве п. (b) пользуемся тем, что связный двудольный граф однозначно разделяется на доли.

Предложение 6. *Для любого $s \in \{0, \dots, n-1\}$ существует единственный (с точностью до эквивалентности) унитрейд $B_s \subset Q_3^n$ такой, что $|B_s| = 2^{n+1} - 2^{s+1}$. Унитрейды B_s являются латинскими битрейдами.*

Доказательство. Согласно предложению 5 множество $B_s = (\{0,1\}^{n-s} \triangle \{1,2\}^{n-s}) \times \{0,1\}^s$ является латинским битрейдом. Очевидно, $|B| = 2^s(2^{n-s} + 2^{n-s} - 2)$.

Перейдем к доказательству единственности. Рассмотрим унитрейд $B \subset Q_3^n$, $|B| < 2^{n+1}$. Аналогично доказательству предложения 4 получаем, что пересечения множества B с гипергранями некоторого направления имеют мощности 2^{n-1}, 2^{n-1}, $2^n - 2^s$. По предположению 3 два пересечения эквивалентны булевым кубам, тогда из определения унитрейда следует, что третье пересечение является симметрической разностью двух булевых кубов.

§ 2. Число унитрейдов в Q_3^n

Рассмотрим множество функций $g : Q_3^n \to \{0,1\}$ как векторное пространство $\mathbb{V}(n)$ над полем $GF(2)$. Характеристические функции унитрейдов образуют в $\mathbb{V}(n)$ линейное подпространство $\mathscr{B}(n)$, в котором в качестве базиса можно выбрать характеристические функции χ^B гиперкубов вида $B = \{\alpha_1, 2\} \times \dots \times \{\alpha_n, 2\}$, где $\alpha_i \in \{0,1\}$. Набор коэффициентов в разложении функции g по базису $\{\chi^B\}$ является булевой функцией от набора $(\alpha_1, \dots, \alpha_n)$. Далее в явной форме определим преобразование, которое каждой булевой функции ставит в соответствие элемент из $\mathscr{B}(n)$.

Определим частичный порядок на Q_3: $0 < 2$, $1 < 2$, а символы 0 и 1 несравнимы. Пусть $(x_1, \dots, x_n), (y_1, \dots, y_n) \in Q_3^n$. Введем обозначение $(x_1, \dots, x_n) \leq (y_1, \dots, y_n)$, если для любого $i \in \{1, \dots, n\}$ верно, что $x_i < y_i$ или $x_i = y_i$. Отметим, что множество $\{x \in \{0,1\}^n \mid x \leq y\}$ является гранью булева n-мерного гиперкуба размерности $wt(y)$, равной числу символов 2 в наборе y. Более того, множество граней находится во взаимно однозначном соответствии с множеством наборов $y \in Q_3^n$.

Пусть f — некоторая булева функция. Определим функцию $U[f] : Q_3^n \to \{0,1\}$ равенством $U[f](y) = \bigoplus\limits_{x \leq y} f(x)$. Заметим, что булева функция $U[f]|_{\{0,2\}^n}$

является преобразованием Мёбиуса от функции f.

Предложение 7. (a) *Пусть* $A \subseteq \{0,1\}^n$, *тогда* $U[\chi^A] \in \mathscr{B}(n)$.
(b) *Пусть* $g \in \mathscr{B}(n)$, *тогда* $U[g|_{\{0,1\}^n}] = g$.

Доказательство. (a) Пусть $f = \chi^A$. Из определения преобразования U имеем равенство

$$U[f](a_1,\ldots,a_{i-1},2,a_{i+1},\ldots,a_n)$$
$$= U[f](a_1,\ldots,a_{i-1},0,a_{i+1},\ldots,a_n) \oplus U[f](a_1,\ldots,a_{i-1},1,a_{i+1},\ldots,a_n)$$

для любых $a_j \in Q_3$. Следовательно, функция $U[f]$ имеет четное число единиц в каждой одномерной грани гиперкуба Q_3^n и $U[f] \in \mathscr{B}(n)$.

(b) Равенство $U[g|_{\{0,1\}^n}](y) = g(y)$ для любого $y \in Q_3^n$ нетрудно показать методом индукции по числу символов 2 в наборе y.

Из предложения 7 вытекает, что подпространство $\mathscr{B}(n)$ имеет размерность 2^n. Следовательно, справедливо следующее

Предложение 8. *В гиперкубе* Q_3^n *имеется ровно* 2^{2^n} *различных унитрейдов.*

Рассмотрим множество функций $g : Q_3^n \to R$ как векторное пространство $\mathbb{V}_R(n)$ над полем R вещественных чисел и линейное подпространство $\mathscr{B}_R(n)$, состоящее из функций, сумма значений которых по любой одномерной грани равняется 0. Пусть $B \subset Q_3^n$ — двудольный унитрейд. Определим функцию $h_B : Q_3^n \to \{-1,0,1\}$, которая принимает значение 1 на первой доле унитрейда, -1 — на второй и 0 — в остальных вершинах гиперкуба. Ясно, что $h_B \in \mathscr{B}_R(n)$. Определим оператор U_R для вещественнозначных функций аналогично оператору U. Пусть $f : Q_2^n \to R$, тогда

$$U_R[f](y) = (-1)^{wt(y)} \sum_{x \le y} f(x). \tag{1}$$

Следующее предложение аналогично предложению 7.

Предложение 9. (a) *Для любой функции* $f : Q_2^n \to R$ *имеем* $U_R[f] \in \mathscr{B}_R(n)$.
(b) *Пусть* $g \in \mathscr{B}_R(n)$, *тогда* $U_R[g|_{\{0,1\}^n}] = g$.

Пусть множество $\mathscr{F}(n)$ состоит из функций $f : Q_2^n \to \{-1,0,1\}$, сумма значений которых в любой грани равна одному из трех чисел: $-1,0,1$. *Счетчиком четности* называется булева функция $\delta(x_1,x_2,\ldots,x_n) = \bigoplus_{i=1}^{n} x_i$. Нетрудно видеть, что $(-1)^{\delta(x)} \in \mathscr{F}(n)$.

Справедливо следующее

Предложение 10. (a) *Пусть* B *— двудольный унитрейд, тогда* $h_B|_{\{0,1\}^n} \in \mathscr{F}(n)$.
(b) *Если* $f \in \mathscr{F}(n)$, *то* $U_R[f] = h_B$ *для некоторого двудольного унитрейда* $B \subset Q_3^n$.

Доказательство. (a) По предложению 9(b) имеем $U_R[|h_B|_{\{0,1\}^n}] = h_B$. Тогда для любой грани $\{x \in \{0,1\}^n \mid x \le y\}$

$$\sum_{x \le y} h_B|_{\{0,1\}^n}(x) = (-1)^{wt(y)} h_B(y) \in \{-1,0,1\}.$$

(b) По предложению 9(a) имеем $U_R[f] \in \mathscr{B}_R(n)$. Из условия $f \in \mathscr{F}(n)$ и определения оператора U_R следует, что $U_R[f](Q_3^n) \subseteq \{-1,0,1\}$. Тогда в каждой одномерной грани функция $U_R[f]$ либо трижды принимает значение 0, либо по одному разу значения $-1,0,1$.

Рассмотрим некоторые конструкции функций из $\mathscr{F}(n)$.

Предложение 11. (a) *Пусть $f \in \mathscr{F}(n)$, тогда $f \cdot \chi^\gamma \in \mathscr{F}(n)$ для любой грани γ.*

(b) *Пусть γ_1, γ_2 — грани в Q_2^n и $\gamma_1 \cap \gamma_2 \neq \varnothing$. Определим функцию f равенством*

$$f(x_1,\dots,x_n,x_{n+1}) = \begin{cases} \chi^{\gamma_1}(-1)^{\delta(x_1,\dots,x_n)} & \text{при } x_{n+1}=0, \\ \chi^{\gamma_2}(-1)^{\delta(x_1,\dots,x_n)\oplus 1} & \text{при } x_{n+1}=1. \end{cases}$$

Тогда $f \in \mathscr{F}(n+1)$.

Предложение 12. *Пусть $f \in \mathscr{F}(n)$, $g \in \mathscr{F}(m)$ и $F(x,y) = f(x)g(y)$. Тогда $F \in \mathscr{F}(n+m)$.*

Доказательства предложений 11 и 12 нетрудно получить непосредственной проверкой.

Заметим, что все унитрейды в Q_3^n состоят из одной компоненты связности, поэтому двудольные унитрейды являются латинскими битрейдами.

Далее получим нижнюю оценку числа неэквивалентных латинских битрейдов. Две определенные на гиперкубе функции называются *эквивалентными*, если они переходят друг в друга посредством изометрий гиперкуба. Рассмотрим гиперкуб Q_2^n как векторное пространство над полем $GF(2)$. Будем называть *носителем* вектора $x \in Q_2^n$ множество позиций, на которых в векторе x находятся единицы. Рассмотрим набор векторов $z^1,\dots,z^k$ с попарно не пересекающимися носителями. Пусть $V \subset Q_2^n$ — подпространство, натянутое на векторы $z^1,\dots,z^k$, $V = \{\bigoplus \alpha_i z^i \mid \alpha \in Q_2^k\}$. Пусть $f : Q_2^k \to \{-1,0,1\}$. Определим функцию $G_V[f] : Q_2^n \to \{-1,0,1\}$ равенствами

$$G_V[f](x) = \begin{cases} f(\alpha) & \text{при } x = \bigoplus \alpha_i z^i, \\ 0 & \text{при } x \notin V. \end{cases}$$

Теорема 1. (a) *Если $f \in \mathscr{F}(k)$, то $G_V[f] \in \mathscr{F}(n)$.*

(b) *Множество $\mathscr{F}(n)$ содержит не менее $e^{\Omega(\sqrt{n})}$ неэквивалентных функций.*

(c) *В гиперкубе Q_3^n имеется не менее $e^{\Omega(\sqrt{n})}$ неэквивалентных латинских битрейдов.*

Доказательство. (a) Поскольку носители векторов $z^1,\dots,z^k$ попарно не пересекаются, сумма значений функции $G_V[f]$ по грани гиперкуба Q_2^n совпадает с суммой значений функции f по некоторой грани гиперкуба Q_2^k. Тогда $G_V[f](Q_3^n) \subseteq \{-1,0,1\}$.

(b) Известно (см., например, [8]), что имеется $e^{\Omega(\sqrt{n})}$ различных разбиений числа n на целые неотрицательные слагаемые. Каждое такое разбиение порождает некоторый набор векторов $z^1,\dots,z^k$ с попарно не пересекающимися носителями и соответствующее набору подпространство V. Функции $G_V[\delta]$ неэквивалентны для различных разбиений, поскольку расстояния Хэмминга между базисными векторами не меняются при изометриях гиперкуба.

(c) По предложению 10(b) каждая функция $U_R[G_V[\delta]]$ порождает латинский битрейд B. Рассмотрим случай, когда все носители векторов $z^1,\dots,z^k$

имеют мощность не менее трех и сумма этих мощностей равна n. Покажем, что пересечения битрейда B с гипергранями вида $\gamma = \{x \in Q_3^n \mid x_i = 2\}$ обладают некоторым инвариантным относительно изометрии свойством $(*)$, которым не обладают пересечения битрейда B с гипергранями вида $\{x \in Q_3^n \mid x_i = 0\}$ и $\{x \in Q_3^n \mid x_i = 1\}$. Тогда для любой изометрии φ по битрейду $\varphi(B)$ можно определить множество $\varphi(B \cap \{0,1\}^n)$. Следовательно, неэквивалентность битрейдов $U_R[G_V[\delta]]$ при различных V является следствием п. (b).

$(*)$ Пусть $\gamma = \{x \in Q_3^n \mid x_i = a\}$. Неравенство $a \neq 2$ справедливо тогда и только тогда, когда найдется такая гипергрань $\gamma' = \{x \in Q_3^n \mid x_j = b\}$, $b \in Q_3$, $j \neq i$, что пересечение $\gamma \cap \gamma' \cap B$ пусто.

Без ограничения общности полагаем, что $i = 1$ и носитель вектора z^1 содержит 1 и 2. Тогда

$$\{x \in Q_3^n \mid x_1 = 0\} \cap \{x \in Q_3^n \mid x_2 = 1\} \cap B = \varnothing,$$

$$\{x \in Q_3^n \mid x_1 = 1\} \cap \{x \in Q_3^n \mid x_2 = 0\} \cap B = \varnothing,$$

в то время как из формулы (1) имеем

$$y = (2,0,\dots,0) \in \{x \in Q_3^n \mid x_1 = 2\} \cap \{x \in Q_3^n \mid x_j = 0\} \cap B,$$

$$y' = (2,0,\dots,0,2,0\dots) \in \{x \in Q_3^n \mid x_1 = 2\} \cap \{x \in Q_3^n \mid x_j = 2\} \cap B,$$

поскольку

$$\begin{aligned}\{\overline{0}\} = \{x \in \{0,1\}^n \mid x \le y\} \cap \{x \in \{0,1\}^n \mid G_V[\delta](x) \neq 0\}\\ = \{x \in \{0,1\}^n \mid x \le y'\} \cap \{x \in \{0,1\}^n \mid G_V[\delta](x) \neq 0\}.\end{aligned}$$

Кроме того,

$$y'' = (2,0,\dots,0,1,\dots,1,0\dots) \in \{x \in Q_3^n \mid x_1 = 2\} \cap \{x \in Q_3^n \mid x_j = 1\} \cap B,$$

так как

$$\begin{aligned}\{x \in \{0,1\}^n \mid x \le y''\} \cap \{x \in \{0,1\}^n \mid G_V[\delta](x) \neq 0\}\\ = \{(0,\dots,0,1,\dots,1,0\dots)\} = \{z^k\},\end{aligned}$$

где носитель вектора z^k содержит позицию j.

Отметим, что латинский битрейд B_s (см. предложение 6) можно задать также функцией $h_{B_s} = U_R[G_V[\delta]]$, где базис подпространства V состоит из одного вектора z с носителем мощности $n - s$.

§ 3. МДР-коды

Методом индукции по размерности n нетрудно доказать, что любой МДР-код в гиперкубе Q_3^n продолжается до МДР-кода в гиперкубе Q_3^{n+1} ровно двумя способами, причем при каждом $n \ge 1$ все МДР-коды в гиперкубе Q_3^n эквивалентны (см. [9, упражнение 13.15]). Характеризация всех МДР-кодов в гиперкубе Q_4^n имеется в [10]. Как указано выше, симметрическая разность $M_1 \triangle M_2$ двух МДР-кодов M_1 и M_2 является двудольным унитрейдом, причем каждая из долей $M_1 \cap (M_1 \triangle M_2)$ и $M_2 \cap (M_1 \triangle M_2)$ — компонента соответствующего МДР-кода. Таким образом, в предложении 4 получены ограничения на возможные мощности компонент МДР-кодов. Отметим (см., например, [2]), что в гиперкубах Q_k^n при $k \ge 4$ имеются МДР-коды с компонентами мощности, кратной 2^{n-1}, и соответствующие им унитрейды мощности, кратной 2^n. Более того, в [3] показано, что любой унитрейд, содержащийся в двукратном МДР-коде в Q_4^n, имеет мощность, кратную 2^n. Ниже рассмотрен вопрос о возможности получения из МДР-кодов (в том числе кратных) унитрейдов других мощностей.

Для произвольной функции $f : Q_k^n \to Q_k$ обозначим ее график через $\mathscr{M}\langle f\rangle = \{(x, f(x)) : x \in Q_k^n\}$. Если множество $\mathscr{M}\langle f\rangle$ является МДР-кодом, то функция f называется *n-арной квазигруппой порядка k*. Соответственно *частичной n-арной квазигруппой порядка k* называется функция, график которой пересекается с любой одномерной гранью не более чем по одной вершине.

В [11] доказано, что любая частичная n-арная квазигруппа конечного порядка есть сужение n-арной квазигруппы некоторого большего порядка. Отсюда следует

Предложение 13. *Любой латинский битрейд $B \subset Q_k^n$ может быть получен из некоторого* МДР-кода *$M \subset Q_m^n$, где $m \geq k$.*

Предложение 14. *Латинский битрейд $B \subset Q_k^n$ такой, что $2^{n+1} > |B| > 2^n$, не может быть получен из* МДР-кода *$M \subset Q_k^n$ при $k \in \{3, 4\}$.*

Доказательство. Поскольку все МДР-коды в Q_3^n эквивалентны при любом n, достаточно рассмотреть произвольный МДР-код в Q_3^n, например, $M = \{x \in Q_3^n \mid x_1 + \dots + x_n = 0 \bmod 3\}$. Нетрудно видеть, что любой полученный из M унитрейд содержит весь МДР-код M и имеет мощность $2 \cdot 3^{n-1}$.

Пусть $k = 4$. Рассмотрим трехмерные латинские битрейды. Полным перебором нетрудно убедиться, что если полученный из МДР-кода $M \subseteq Q_4^3$ битрейд B имеет пересечение мощности не менее 6 с некоторой двумерной гранью, то найдется еще одна двумерная грань, параллельная первой, пересечение с которой также имеет мощность не менее 6. Кроме того, полным перебором можно проверить, что в этом случае $|B| \geq 16 = 2^4$.

Рассмотрим латинский битрейд B', полученный из МДР-кода в Q_4^n. Применяя метод индукции, выводим, что если битрейд $B' \subseteq Q_4^n$ имеет пересечение мощности не менее 6 с какой-либо двумерной гранью, то $|B'| \geq 2^{n+1}$. Из предложения 3 следует, что если пересечение латинского битрейда с любой двумерной гранью имеет мощность меньше 6, т. е. равную 0 или 4, то граф, порожденный битрейдом B', является булевым n-кубом.

Рассмотрим возможность получения латинских битрейдов малой мощности из двукратных МДР-кодов.

Предложение 15. *Любой n-мерный латинский битрейд мощности меньше 2^{n+1} может быть получен из двукратных* МДР-кодов *в Q_4^n.*

Доказательство. Вначале покажем, что битрейд $B_0^k = \{0,1\}^k \triangle \{1,2\}^k$ может быть получен из некоторого двукратного МДР-кода в Q_4^k. Пусть функция $g : Q_k^n \to \{0,1\}$ определена равенством $g(a_1, \dots, a_k) = \sum_{i=1}^{k} a_i \bmod 2$. Нетрудно видеть, что функции g, $g_1 = g \oplus \chi^{\{1,2\}^k}$ и $g_2 = g \oplus \chi^{\{0,1\}^k}$ являются характеристическими функциями некоторых двукратных МДР-кодов M_0, M_1 и M_2. Поскольку $g_1 \oplus g_2 = \chi^{\{1,2\}^k} \oplus \chi^{\{0,1\}^k}$, имеем $B_0^k = M_1 \triangle M_2$.

Рассмотрим булевозначные функции

$$f_1(a_1,\dots,a_k,y)=\begin{cases} g_1(a_1,\dots,a_k) & \text{при } y=0,\\ g_2(a_1,\dots,a_k) & \text{при } y=1,\\ g_1(a_1,\dots,a_k)\oplus 1 & \text{при } y=2,\\ g_2(a_1,\dots,a_k)\oplus 1 & \text{при } y=3; \end{cases} \tag{2}$$

$$f_2(a_1,\dots,a_k,y)=\begin{cases} g_2(a_1,\dots,a_k) & \text{при } y=0,\\ g_1(a_1,\dots,a_k) & \text{при } y=1,\\ g_1(a_1,\dots,a_k)\oplus 1 & \text{при } y=2,\\ g_2(a_1,\dots,a_k)\oplus 1 & \text{при } y=3. \end{cases} \tag{3}$$

Легко видеть, что f_1 и f_2 являются характеристическими функциями двукратных МДР-кодов, причем $f_1\oplus f_2=\chi^{B_0^k\times\{0,1\}}$.

Подставляя в формулы (2), (3) функции f_1 и f_2 вместо g_1 и g_2, обнаружим, что латинский битрейд $B_0^k\times\{0,1\}^2$ также может быть получен из некоторого двукратного МДР-кода в Q_4^{k+2}, и т. д. Для окончания доказательства остается сослаться на предложения 4 и 6.

Приведем таблицы функций g, g_1, g_2 при $n=2$:

$$\begin{pmatrix}0&1&0&1\\1&0&1&0\\0&1&0&1\\1&0&1&0\end{pmatrix},\quad \begin{pmatrix}0&1&0&1\\1&1&0&0\\0&0&1&1\\1&0&1&0\end{pmatrix},\quad \begin{pmatrix}1&0&0&1\\0&1&1&0\\0&1&0&1\\1&0&1&0\end{pmatrix}.$$

Можно показать, что построенные в предложении 15 двукратные МДР-коды нерасщепляемы при $n\ge 3$.

Далее исследуем вопрос о гамильтоновости графов минимальных расстояний двукратных МДР-кодов.

Предложение 16. *Для любого* МДР-*кода $M\subset Q_k^n$ найдется двукратный* МДР-*код D такой, что $M\subset D$ и граф минимальных расстояний ΓD гамильтонов.*

Доказательство. Определим МДР-код $M'\subset Q_k^n$ равенством

$$M'=\{(x_1+1 \bmod k, x_2,\dots,x_n)\mid (x_1,\dots,x_n)\in M\}.$$

Рассмотрим двукратный МДР-код $D=M\cup M'$. Докажем по индукции, что граф ΓD гамильтонов, причем для любого ребра найдется проходящий через него гамильтонов цикл. При $n=2$ граф ΓD представляет собой гамильтонов цикл, состоящий из чередующихся ребер двух направлений.

Пусть предположение индукции доказано при $n-1$. Рассмотрим произвольное ребро в графе ΓD, например ребро v, соединяющее точки $(0,\dots,0,c)$ и $(0,\dots,0,c')$. Граф $\Gamma D'$, где $D'=\{(x_1,x_n)\mid (x_1,0,\dots,0,x_n)\in D\}$, является простым циклом H' и содержит ребро v. По предположению индукции граф ΓD_a, где $D_a=\{(x_1,\dots,x_{n-1})\mid (x_1,\dots,x_{n-1},a)\in D\}$, содержит гамильтонов цикл H_a для любого $a\in Q_k$, причем гамильтонов цикл H_a можно выбрать проходящим через ребро, принадлежащее циклу H'.

Если два простых цикла пересекаются ровно по одному ребру, то, удалив из объединения двух циклов это ребро, получим простой цикл. Таким образом, граф $H=H'\triangle\bigcup_a H_a$ является простым циклом. Кроме того, цикл H проходит через все вершины графа ΓD и содержит ребро v.

ЛИТЕРАТУРА

1. *Кротов Д. С., Потапов В. Н.* О кратных МДР- и совершенных кодах, не расщепляемых на однократные // Пробл. передачи информации. 2004. Т. 40, № 1. С. 6–14.
2. *Krotov D. S.* On decomposability of 4-ary distance 2 MDS codes, double-codes, and n-quasigroups of order 4 // Discrete Math. 2008. V. 308, N 15. P. 3322–3334.
3. *Кротов Д. С., Потапов В. Н.* О числе n-арных квазигрупп конечного порядка // Дискрет. математика. 2012. Т. 24, № 1. С. 60–69.
4. *Phelps K.* A general product construction for error correcting codes // SIAM J. Algebraic Discrete Methods. 1984. V. 5, N 2. P. 224–228.
5. *Потапов В. Н.* Спектр мощностей компонент корреляционно-иммунных функций, бент-функций, совершенных раскрасок и кодов // Пробл. передачи информации. 2012. Т. 48, № 1. С. 54–63.
6. *Романов А. М.* О комбинаторных кодах Грея с расстоянием 3 // Дискрет. математика. 2009. Т. 21, № 3. С. 73–78.
7. *Потапов В. Н., Кротов Д. С.* Асимптотика числа n-квазигрупп порядка 4 // Сиб. мат. журн. 2006. Т. 47, № 4. С. 873–887.
8. *Эндрюс Г.* Теория разбиений. М.: Наука, 1982.
9. *Laywine C. F., Mullen G. L.* Discrete mathematics using Latin squares. New York: Wiley, 1998.
10. *Krotov D. S., Potapov V. N.* n-Ary quasigroups of order 4 // SIAM J. Discrete Math. 2009. V. 23, N 2. P. 561–570.
11. *Cruse A. B.* On the finite completion of partial latin cubes // J. Comb. Theory, Ser. A. 1974. V. 17. P. 112–119.

Статья поступила 17 марта 2012 г.

Потапов Владимир Николаевич
Новосибирский гос. университет,
ул. Пирогова, 2, Новосибирск 630090
potapov@math.nsc.ru