

УДК 519.8

О ПОСТРОЕНИИ ВЕРШИННО-ТРАНЗИТИВНЫХ РАЗБИЕНИЙ n -КУБА НА СОВЕРШЕННЫЕ КОДЫ ^{*)}

Ф. И. Соловьёва, Г. К. Гуськов

Аннотация. Приводятся два метода построения вершинно-транзитивных и 2-транзитивных разбиений n -куба на совершенные коды, а также нижние оценки числа неэквивалентных транзитивных, вершинно-транзитивных и 2-транзитивных разбиений n -куба на совершенные коды.

Ключевые слова: совершенный двоичный код, вершинно-транзитивное разбиение, k -транзитивное разбиение n -куба.

Введение

Исследование разбиений n -куба E^n (множества всех двоичных векторов длины n) на совершенные коды освещено в небольшом количестве статей. Две конструкции (свитчинговая и каскадная) предложены в [3], первая из них позволила получить нетривиальную нижнюю оценку $2^{2^{(n-1)/2}}$ числа разбиений пространства E^n на совершенные двоичные коды длины $n > 15$ [1, 14].

В [1] показано, что для каждого $n = 2^k - 1$, $k \geq 5$, существует разбиение множества всех двоичных векторов длины n на попарно не эквивалентные совершенные двоичные коды длины n с кодовым расстоянием 3. В [11] предложено несколько конструкций разбиений E^n на попарно не параллельные коды Хэмминга длины n для любого $n \geq 15$. В [14] Фелпсом классифицированы все неэквивалентные разбиения E^7 на коды Хэмминга, их оказалось 11.

Исследование разбиений n -куба на совершенные коды представляется важным, в частности, из-за тесной связи с задачей перечисления всех совершенных двоичных кодов. Известно, что между количеством таких разбиений и числом различных совершенных двоичных кодов существует следующая зависимость: предел отношения двойных логарифмов этих чисел равен 1, хотя число разбиений заведомо больше числа

^{*)}Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект № 10-01-00424)

неэквивалентных кодов. Другими мотивациями исследования и построения разбиений E^n на коды (необязательно совершенные) является связь разбиений со следующими проблемами раскрасок вершин E^n : разбиение E^n на коды индуцирует раскраски, связанные с оптоволоконными сетями [13], или совершенные раскраски, именуемые также полностью регулярными кодами, partition designs, equitable partitions [7]. В [5, 16] предложено несколько конструкций транзитивных разбиений n -куба E^n на двоичные коды, в частности, на совершенные коды. Исследованию матриц пересечения совершенных двоичных кодов посвящена статья [8]. О построении разбиений n -мерного q -значного куба E_q^n , $q > 2$, на совершенные коды см. [6, 8]. В [6] приведена нижняя оценка числа разбиений E_q^n на совершенные коды, являющаяся на сегодняшний день лучшей.

В настоящей статье продолжено исследование и конструирование транзитивных разбиений на совершенные двоичные коды [5, 16]. Ниже приводятся две конструкции вершинно-транзитивных и 2-транзитивных разбиений E^n на совершенные двоичные коды, вычисляются нижние оценки числа неэквивалентных транзитивных, вершинно-транзитивных и 2-транзитивных разбиений E^n на совершенные коды.

1. Необходимые определения и понятия

Множество E^n образует n -мерное метрическое пространство по отношению к метрике Хэмминга. Расстояние Хэмминга $d(x, y)$ между векторами x и y из E^n равно количеству координат, в которых различаются эти векторы. Двоичным кодом называется произвольное подмножество C из E^n . Совершенным двоичным кодом, исправляющим одиночные ошибки, (далее кратко совершенным кодом) называется такое подмножество C из E^n , что любой вектор пространства E^n находится на расстоянии не больше 1 от некоторого единственного вектора из C .

Известно, что группа автоморфизмов пространства E^n исчерпывается всеми изометриями E^n , каждая такая изометрия определяется подстановкой π на множестве координат и сдвигом на произвольный вектор $v \in E^n$. Группа автоморфизмов $\text{Aut}(E^n)$ пространства E^n определяется как

$$\text{Aut}(E^n) = \{(v, \pi) \mid v \in E^n, \pi \in S_n\},$$

где S_n — симметрическая группа подстановок длины n . Группой автоморфизмов $\text{Aut}(C)$ кода C длины n назовём группу изометрий пространства E^n , переводящих код в себя. Код называется транзитивным, если его группа автоморфизмов действует транзитивно на всех его кодовых словах. Группой автоморфизмов произвольного разбиения $P^n =$

$\{C_0, C_1, \dots, C_n\}$ пространства E^n на совершенные коды C_0, C_1, \dots, C_n , $\bigcup_{i=0}^n C_i = E^n$, называется группа изометрий пространства E^n , переводящих разбиение P^n в себя. Каждый такой автоморфизм индуцирует подстановку γ на элементах множества индексов $I = \{0, 1, \dots, n\}$, переставляющую коды в разбиении P^n :

$$\gamma(\{C_0, C_1, \dots, C_n\}) = \{C_{\gamma(0)}, C_{\gamma(1)}, \dots, C_{\gamma(n)}\},$$

т.е. группа автоморфизмов разбиения P^n изоморфна некоторой подгруппе группы S_{n+1} . Семейство кодов P^n называется k -транзитивным, $1 \leq k \leq n$, если для любой пары упорядоченных подмножеств $\{i_1, \dots, i_k\}$ и $\{j_1, \dots, j_k\}$ из I существует автоморфизм σ из $\text{Aut}(P^n)$ такой, что $\sigma(C_{i_t}) = C_{j_t}$, $t = 1, \dots, k$. При $k = 1$ семейство кодов P^n называется транзитивным. Семейство кодов P^n назовём вершинно-транзитивным, если для любых двух вершин $u \in C_i$, $v \in C_j$ существует автоморфизм σ из $\text{Aut}(P^n)$ такой, что $\sigma(u) = v$. При этом если $i = j$ для любого $i \in I$, то получим вершинно-транзитивное разбиение на транзитивные коды (например, на классы смежности кода Хэмминга). Далее будем говорить, что разбиение имеет длину n , если оно состоит из кодов длины n .

2. Вспомогательные утверждения

В дальнейшем нам понадобятся разбиения куба E^7 на коды Хэмминга. Несмотря на то, что в E^7 существует единственный, с точностью до изоморфизма, совершенный код — линейный код Хэмминга, таких разбиений согласно классификации Фелпса [14] оказалось 11.

Лемма 1. Среди 11 неэквивалентных разбиений пространства E^7 на коды Хэмминга имеется семь транзитивных разбиений, шесть из которых — вершинно-транзитивные, два разбиения из этих семи являются 2-транзитивными; при $k \geq 3$ в E^7 не существует k -транзитивных разбиений.

Лемма доказана с помощью компьютерных исследований, таблица, отвечающая этим разбиениям, с учётом нумерации разбиений, приведённой в [14], выглядит следующим образом:

Разбиения в E^7	P_0	P_1	P_2	P_3	P_4	P_5	P_6	P_7	P_8	P_9	P_{10}
транзитивность	—	+	+	—	—	+	+	+	+	+	—
2-транзитивность	—	—	—	—	—	+	—	—	+	—	—
вершинная транзитивность	—	+	+	—	—	+	+	+	—	+	—

Отметим, что разбиение под номером 5 в таблице на классы смежности кода Хэмминга является транзитивным, а также вершинно-транзитивным и 2-транзитивным, а разбиение под номером 8 — 2-транзитивным, но не вершинно-транзитивным.

Рассмотрим произвольное разбиение $P^n = \{H_0^n, \dots, H_n^n\}$ куба E^n на коды Хэмминга H_0^n, \dots, H_n^n . Введём для любого такого разбиения понятие *матрицы пересечений разбиения* — это симметричная матрица $M(P^n)$ порядка $n+1$ с элементами $m_{ij} = |\overline{H}_i^n \cap \overline{H}_j^n|$, где $\overline{H}_i^n = x + H_i^n$ для некоторого кодового слова $x \in H_i^n$, т.е. нулевое кодовое слово $\mathbf{0}^n$ принадлежит коду \overline{H}_i^n , $i, j \in \{0, 1, \dots, n\}$. Поскольку код Хэмминга линейен, число m_{ij} не зависит от выбора вектора x .

Заметим, что в случае разбиения на нелинейные коды (именно по причине их нелинейности), в отличие от случая разбиения на классы смежности линейных кодов, может возникнуть уже не одна матрица пересечений с точностью до эквивалентности, а целый класс таких матриц.

Матрицы $M(P_1^n)$ и $M(P_2^n)$ двух разбиений P_1^n и P_2^n назовём *эквивалентными*, если эти матрицы совпадают с точностью до перестановки столбцов и строк. Из того простого факта, что если P_1^n и P_2^n эквивалентны, то матрицы $M(P_1^n)$ и $M(P_2^n)$ также эквивалентны, легко вытекает следующая

Лемма 2. *Если матрицы $M(P_1^n)$ и $M(P_2^n)$ двух разбиений P_1^n и P_2^n не эквивалентны, то эти разбиения не эквивалентны.*

В приложении приведены матрицы пересечений $M(P_i^7)$, $i = 0, \dots, 10$, для всех одиннадцати разбиений из [14] куба E^7 на коды Хэмминга длины 7. В таблицах $S(P_i^7)$, $i = 0, 1, \dots, 10$, проиллюстрирован *состав матриц* выше главной диагонали, т.е. сколько раз на пересечении i -й и j -й строк, $i < j$, встречаются числа из множества $\{2, 4, 8, 16\}$ (других чисел быть не может, так как коды Хэмминга длины 7 могут пересекаться только по 2, 4, 8 или 16 векторам, см. [10]). Заметим, что таблицы составов у всех одиннадцати матриц пересечений разбиения куба E^7 разные. Отсюда, в частности, следует, что все эти разбиения неэквивалентны.

Следует отметить, что вследствие леммы 2 матрицы пересечений можно использовать наравне с такими уже известными инструментами доказательства неэквивалентности кодов и разбиений на коды, как, например, ранги и размерности ядер кодов.

3. Конструкции вершинно-транзитивных разбиений

Для построения вершинно-транзитивных разбиений E^n на совершенные коды используем две конструкции, введённые в [5] для построения

транзитивных разбиений на двоичные коды, необязательно совершенные.

3.1. Конструкция А. В этом разделе покажем, используя конструкцию Васильева [2], что можно строить вершинно-транзитивные (2-транзитивные) разбиения E^n на совершенные коды любой допустимой длины $n \geq 15$.

Пусть $P^n = \{C_0^n, C_1^n, \dots, C_n^n\}$ — произвольное разбиение E^n на совершенные коды длины n , e_s — вектор веса 1 длины n с единичной s -й координатой. Тогда совокупность кодов

$$C_i^{2n+1} = \{(x, |x|, x + y) \mid x \in E^n, y \in C_i^n\}, \quad C_{n+i+1}^{2n+1} = C_i^{2n+1} + e_{n+1}, \\ i = 0, 1, \dots, n,$$

задаёт разбиение P^{2n+1} , названное в [5] *конструкцией А*.

Для доказательства вершинной транзитивности разбиения P^{2n+1} докажем сначала транзитивность этого разбиения. Доказательство аналогично доказательству теоремы 1 из [5], однако приведём его для полноты изложения.

Лемма 3. Пусть $P^n = \{C_0^n, C_1^n, \dots, C_n^n\}$ является произвольным вершинно-транзитивным разбиением E^n на совершенные коды длины n . Тогда разбиение P^{2n+1} транзитивно.

Доказательство. Из того, что P^n вершинно-транзитивно, следует, что оно транзитивно, а значит, для любых $0 \leq s, r \leq n$ существует автоморфизм δ разбиения P^n такой, что $\delta(C_s^n) = C_r^n$, где $\delta = (y, \pi)$, $\pi \in S_n$, $y \in E^n$. Пусть $\pi = \begin{pmatrix} 1 & 2 & \dots & n \\ \pi_1 & \pi_2 & \dots & \pi_n \end{pmatrix}$. Используя π , зададим перестановку σ_π следующим образом [4]:

$$\sigma_\pi = \begin{pmatrix} 1 & 2 & \dots & n & n+1 & n+2 & n+3 & \dots & 2n+1 \\ \pi_1 & \pi_2 & \dots & \pi_n & n+1 & n+1+\pi_1 & n+1+\pi_2 & \dots & n+1+\pi_n \end{pmatrix}.$$

Зафиксируем произвольный вектор $x \in E^n$. Определим следующее преобразование φ разбиения P^{2n+1} :

$$\varphi = ((x, |x| + \alpha + \beta, x + y), \sigma_\pi), \quad (1)$$

где

$$\alpha = \begin{cases} 0, & \text{если } 0 \leq i \leq n, \\ 1, & \text{если } n < i \leq 2n+1; \end{cases} \quad (2)$$

$$\beta = \begin{cases} 0, & \text{если } 0 \leq j \leq n, \\ 1, & \text{если } n < j \leq 2n + 1. \end{cases} \quad (3)$$

Покажем, что φ — автоморфизм разбиения P^{2n+1} , т. е. $\varphi(P^{2n+1}) = P^{2n+1}$.

Пусть $0 \leq i, j \leq n$ и $i = s$, $j = r$. Рассмотрим код C_i^{2n+1} из P^{2n+1} :

$$C_i^{2n+1} = \{(x', |x'|, x' + y') \mid x' \in E^n, y' \in C_i^n\}.$$

Покажем, что $\varphi(C_i^{2n+1}) = C_j^{2n+1}$. Согласно (1) получим

$$\begin{aligned} \varphi(C_i^{2n+1}) &= (x, |x|, x + y) + \sigma_\pi(C_i^{2n+1}) \\ &= (x, |x|, x + y) + \{(\pi(x'), |\pi(x')|, \pi(x' + y'))\} \\ &= \{(x + \pi(x'), |x + \pi(x')|, x + \pi(x') + y + \pi(y'))\}. \end{aligned} \quad (4)$$

Ясно, что вектор $x'' = x + \pi(x')$ принадлежит E^n , а в силу выбора δ и того, что $y' \in C_s^n$, получаем, что $y'' = y + \pi(y') \in C_r^n$. Следовательно, $(x'', |x''|, x'' + y'') \in C_j^{2n+1}$, где $j = r$. Учитывая, что φ является автоморфизмом куба E^{2n+1} , получим $\varphi(C_i^{2n+1}) = C_j^{2n+1}$.

Аналогично доказываются и остальные случаи. Например, если рассматриваются два произвольных кода C_i^{2n+1} и C_j^{2n+1} , $i = n + s + 1$, $j = n + r + 1$, т. е. $n < i, j \leq 2n + 1$, то для преобразования, построенного согласно (1), верно

$$\varphi(C_{n+s+1}^{2n+1}) = C_{n+r+1}^{2n+1},$$

т. е. φ — автоморфизм разбиения P^n , переводящий код C_i^{2n+1} в код C_j^{2n+1} . Следовательно, для любых i, j , $0 \leq i, j \leq 2n + 1$, найдётся преобразование, переводящее код C_i^{2n+1} в код C_j^{2n+1} . Будучи автоморфизмом куба E^{2n+1} , это преобразование переводит различные коды из P^{2n+1} в различные коды из P^{2n+1} , а значит, является автоморфизмом разбиения P^{2n+1} . Лемма 3 доказана.

Теорема 1. Если разбиение P^n вершинно-транзитивно, то семейство кодов P^{2n+1} , построенное с помощью конструкции A , является вершинно-транзитивным разбиением куба E^{2n+1} на совершенные коды.

Доказательство теоремы можно разбить на доказательство двух утверждений:

1. Для любого отображения из $\text{Aut}(P^n)$ можно построить отображение φ такое, что $\varphi \in \text{Aut}(P^{2n+1})$.
2. Полученное разбиение P^{2n+1} является вершинно-транзитивным.

Первое утверждение вытекает из леммы 3. Для доказательства второго рассмотрим произвольные вершины

$$u = (x', |x'| + \alpha, x' + y'), \quad v = (x'', |x''| + \beta, x'' + y'')$$

из E^{2n+1} , принадлежащие кодам C_i^{2n+1} , C_j^{2n+1} соответственно, где $y' \in C_s^n$, $y'' \in C_r^n$, $x', x'' \in E^n$, $0 \leq i, j \leq 2n+1$, $0 \leq s, r \leq n$.

Пусть $i = s$, $j = r$. Из вершинной транзитивности P^n следует, что существует автоморфизм $\delta = (y, \pi)$, $\pi \in S_n$, $y \in E^n$, такой, что

$$\delta(y') = y + \pi(y') = y'' \in y + \pi(C_s^n) = C_r^n.$$

Используя снова преобразование φ , определённое в (1), и выбрав вектор x из E^n так, чтобы выполнялось $x + \pi(x') = x''$, положим

$$\varphi = ((x, |x| + \alpha + \beta, x + y), \sigma_\pi).$$

Подействуем преобразованием φ на кодовое слово u :

$$\begin{aligned} \varphi(u) &= (x, |x| + \alpha + \beta, x + y) + \sigma_\pi(u) \\ &= (x + \pi(x'), |x| + |\pi(x')| + \alpha + \alpha + \beta, x + y + \pi(x' + y')) \\ &= (\pi(x') + x, |\pi(x') + x| + \beta, \pi(x') + x + \pi(y') + y). \end{aligned}$$

В силу выбора вектора x имеем $x'' = x + \pi(x')$, а из определения δ следует, что $y + \pi(y') = y''$. Следовательно, $\varphi(u) = (x'', |x''| + \beta, x'' + y'') = v$, т. е. для любых двух вершин из кодов C_i^{2n+1} , $C_j^{2n+1} \in P^{2n+1}$ соответственно, где $i = s$, $j = r$, существует автоморфизм разбиения (тот факт, что $\varphi \in \text{Aut}(P^{2n+1})$, доказан в лемме 3), переводящий вершины u и v друг в друга. В случаях $i = s$, $j = n+1+r$; $i = n+1+s$, $j = r$, а также $i = n+1+s$, $j = n+1+r$ доказательство аналогично. Отсюда следует вершинная транзитивность разбиения P^{2n+1} . Теорема 1 доказана.

Аналогично доказывается

Теорема 2. Если P^n — 2-транзитивное разбиение на совершенные коды длины n , то семейство кодов P^{2n+1} , построенное с помощью конструкции А, является 2-транзитивным разбиением куба E^{2n+1} на совершенные коды длины $2n+1$.

3.2. Конструкция В. Рассмотрим метод построения транзитивных разбиений, основанный на конструкции Моллара [12] для двоичных кодов. Он является обобщением конструкции А, точно так же, как и конструкция Моллара является обобщением конструкции Васильева для

двоичных кодов, исправляющих одну ошибку. Следует отметить, что в отличие от конструкции В конструкция А позволяет строить транзитивные коды с большими кодовыми расстояниями [4, 5]. Для полноты изложения напомним конструкцию Моллара. Пусть C^t и D^m — произвольные приведённые (т. е. содержащие нулевые векторы) двоичные коды длин t и m соответственно, имеющие кодовые расстояния не менее 3. Пусть $x = (x_{11}, x_{12}, \dots, x_{1m}, x_{21}, \dots, x_{2m}, \dots, x_{t1}, \dots, x_{tm}) \in E^{tm}$. В дальнейшем будем использовать матричную запись вектора x : i -я строка матрицы X равна $x_{i1} \ x_{i2} \ \dots \ x_{im}$, где $i = 1, \dots, t$. Функции $p_1(x)$ и $p_2(x)$, определённые как

$$p_1(x) = \left(\sum_{j=1}^m x_{1j}, \dots, \sum_{j=1}^m x_{tj} \right) \in E^t,$$

$$p_2(x) = \left(\sum_{i=1}^t x_{i1}, \dots, \sum_{i=1}^t x_{im} \right) \in E^m,$$

называются *обобщёнными проверками на чётность*. Множество

$$C^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in E^{tm}, y \in C^t, z \in D^m\}$$

является двоичным кодом Моллара длины $n = tm + t + m$ с кодовым расстоянием 3 [12].

Пусть $P^t = \{C_0^t, \dots, C_t^t\}$ и $P^m = \{C_0^m, \dots, C_m^m\}$ — произвольные разбиения E^t и E^m на совершенные двоичные коды соответственно. Тогда семейство кодов

$$C_{ij}^n = \{(x, y + p_1(x), z + p_2(x)) \mid x \in E^{tm}, y \in C_i^t, z \in C_j^m\},$$

$$0 \leq i \leq t, 0 \leq j \leq m, \quad (5)$$

задаёт разбиение P^n куба E^n на совершенные двоичные коды [5], где $n = tm + t + m$. Назовём эту конструкцию, следуя [5], конструкцией В. Доказательство следующей леммы является аналогом доказательства теоремы 3 из [5], приведём его для полноты изложения.

Лемма 4. Пусть разбиения P^t и P^m являются вершинно-транзитивными разбиениями E^t и E^m на совершенные двоичные коды соответственно. Тогда разбиение P^n транзитивно.

Доказательство. Вершинная транзитивность P^t и P^m по определению предполагает транзитивность этих разбиений, а значит, для любых $0 \leq i, k \leq t$ и $0 \leq j, s \leq m$ существуют такие автоморфизмы ϑ и ψ

разбиений P^t и P^m соответственно, что $\vartheta(C_i^t) = C_k^t$ и $\psi(C_j^m) = C_s^m$, где $\vartheta = (\pi, v)$, $\pi \in S_t$, $v \in E^t$ и $\psi = (\tau, u)$, $\tau \in S_m$, $u \in E^m$.

Пусть $\pi = \begin{pmatrix} 1 & 2 & \dots & t \\ \pi_1 & \pi_2 & \dots & \pi_t \end{pmatrix}$ и $\tau = \begin{pmatrix} 1 & 2 & \dots & m \\ \tau_1 & \tau_2 & \dots & \tau_m \end{pmatrix}$. Рас-

смотрим заданное выше разбиение P^n на коды

$$C_{ij}^n = \{(x', y + p_1(x'), z + p_2(x')) \mid x' \in E^{tm}, y \in C_i^t, z \in C_j^m\}$$

из (5), $0 \leq i \leq t$, $0 \leq j \leq m$. Определим преобразование φ , переводящее код C_{ij}^n в код C_{ks}^n . Для этого определим подстановки π' и τ' следующим образом:

$$\pi' = \begin{pmatrix} tm+1 & tm+2 & \dots & tm+t \\ tm+\pi_1 & tm+\pi_2 & \dots & tm+\pi_t \end{pmatrix},$$

$$\tau' = \begin{pmatrix} tm+t+1 & tm+t+2 & \dots & tm+t+m \\ tm+t+\tau_1 & tm+t+\tau_2 & \dots & tm+t+\tau_m \end{pmatrix}.$$

Рассмотрим преобразование φ вида

$$\varphi = ((x, v + p_1(x), u + p_2(x)), \sigma_{\pi\tau}), \quad (6)$$

где $\sigma_{\pi\tau} = (\pi \circ \tau, \pi', \tau') \in S_n$. Действие композиции $\pi \circ \tau$ подстановок π и τ на матрицу X заключается в перестановке строк согласно перестановке π , а столбцов — согласно перестановке τ .

Покажем, что φ — автоморфизм разбиения P^n , переводящий код C_{ij}^n в код C_{ks}^n . Для этого рассмотрим произвольное кодовое слово $\mathbf{x} = (x', y + p_1(x'), z + p_2(x'))$ кода C_{ij}^n и покажем, что под действием преобразования φ оно перейдёт в некоторое кодовое слово кода C_{ks}^n :

$$\begin{aligned} \varphi(\mathbf{x}) &= (x, v + p_1(x), u + p_2(x)) + \sigma_{\pi\tau}(x', y + p_1(x'), z + p_2(x')) \\ &= (x, v + p_1(x), u + p_2(x)) + (x'', \pi(y) + p_1(x''), \tau(z) + p_2(x'')) \\ &= (x + x'', v + \pi(y) + p_1(x) + p_1(x''), u + \tau(z) + p_2(x) + p_2(x'')) \\ &= (x + x'', v + \pi(y) + p_1(x + x''), u + \tau(z) + p_2(x + x'')), \end{aligned}$$

где $x'' = \sigma_{\pi\tau}(x')$. Очевидно, что $x + x'' \in E^{tm}$. Поскольку $(x + x'', p_1(x + x''), p_2(x + x'')) \in E^n$, $y \in C_i^t$, $z \in C_j^m$, $v + \pi(y) \in C_k^t$ и $u + \tau(z) \in C_s^m$ в силу вершинной транзитивности разбиений P^t и P^m соответственно, полученный вектор $\varphi(\mathbf{x})$ согласно конструкции (5) принадлежит коду C_{ks}^n . Так как φ является автоморфизмом E^n , различные кодовые слова кода C_{ij}^n под действием φ переходят в различные кодовые слова кода C_{ks}^n , следовательно, $\varphi(C_{ij}^n) = C_{ks}^n$. Более того, в силу произвольности выбора

i и j , $0 \leq i \leq t$, $0 \leq j \leq m$, с учётом выбора отображений ϑ и ψ , отображение φ , будучи автоморфизмом куба E^n , переводит различные коды из множества P^n в различные коды из P^n . Следовательно, отображение φ является автоморфизмом разбиения P^n , т. е. $\varphi(P^n) = P^n$. Лемма 4 доказана.

Используя эту лемму, нетрудно показать рассуждениями, аналогичными проведённым в теореме 1, что можно итеративно строить вершинно-транзитивные разбиения куба E^n , т. е. справедлива

Теорема 3. Если разбиения P^t и P^m вершинно-транзитивны, то семейство кодов P^n , построенное с помощью конструкции B , вершинно-транзитивно.

Теорема 4. Если разбиения P^t и P^m 2-транзитивны, то семейство кодов P^n , построенное с помощью конструкции B , 2-транзитивно.

ДОКАЗАТЕЛЬСТВО. Из леммы 4 следует, что для любых отображений $\vartheta \in \text{Aut}(P^t)$ и $\psi \in \text{Aut}(P^m)$ можно построить отображение φ такое, что $\varphi \in \text{Aut}(P^n)$, т. е. разбиение P^n транзитивно.

Из того, что разбиения P^t и P^m по условию являются 2-транзитивными, следует существование преобразований $\vartheta \in \text{Aut}(P^t)$ и $\psi \in \text{Aut}(P^m)$ таких, что $(\vartheta(C_i^t), \vartheta(C_{i'}^t)) = (C_k^t, C_{k'}^t)$ и $(\psi(C_j^m), \psi(C_{j'}^m)) = (C_s^m, C_{s'}^m)$, для любых $0 \leq i, i', k, k' \leq t$ и $0 \leq j, j', s, s' \leq m$, где $\vartheta = (\pi, v)$, $\pi \in S_t$, $v \in E^t$ и $\psi = (\tau, u)$, $\tau \in S_m$, $u \in E^m$. Используя их, построим отображение φ согласно (6) и приведём схему доказательства того факта, что полученное разбиение P^n является 2-транзитивным.

Рассмотрим произвольные пары кодов $(C_{ij}^n, C_{i'j'}^n)$ и $(C_{ks}^n, C_{k's'}^n)$, построенных согласно (5), и произвольные вершины x, y из кодов C_{ij}^n и $C_{i'j'}^n$ соответственно.

Подействуем преобразованием φ на векторы x и y . В предыдущей лемме было рассмотрено действие преобразования, построенного согласно (6), на произвольный код разбиения P^n . Учитывая свойства преобразований ϑ и ψ , с помощью рассуждений, аналогичных рассмотренным в лемме 4, нетрудно видеть, что $\varphi(x) \in C_{ks}^n$ и $\varphi(y) \in C_{k's'}^n$, а также

$$\varphi(C_{ij}^n, C_{i'j'}^n) = (\varphi(C_{ij}^n), \varphi(C_{i'j'}^n)) = (C_{ks}^n, C_{k's'}^n),$$

т. е. для любых двух пар кодов из разбиения P^n существует преобразование, переводящее одну пару этих кодов в другую, откуда следует 2-транзитивность разбиения P^n . Теорема 4 доказана.

4. Нижние оценки

Используя лемму 2, а также тот факт, что согласно [14] существует всего 11 неэквивалентных разбиений длины 7, получим нижние оценки числа разбиений, построенных с помощью конструкций В и А. В дальнейшем понадобятся следующие утверждения.

Лемма 5. Пусть Q — матрица пересечений разбиения P^n куба E^n на коды Хэмминга с элементами q_{rs} , $0 \leq r, s \leq n$. Тогда для элементов r_{ij} матрицы пересечений R разбиения P^{2n+1} , которое получено с помощью конструкции А из P^n , справедливо

$$r_{ij} = \begin{cases} 2^n q_{ij}, & \text{если } 0 \leq i, j \leq n; \\ 2^n q_{i-n-1, j-n-1}, & \text{если } n < i, j \leq 2n+1; \\ 0, & \text{если } 0 \leq i \leq n, n < j \leq 2n+1 \\ & \text{либо } n < i \leq 2n+1, j \leq n. \end{cases} \quad (7)$$

ДОКАЗАТЕЛЬСТВО. Для доказательства рассмотрим два произвольных вектора u и v из E^{2n+1} :

$$u = (x_1, |x_1| + \alpha, x_1 + y_1) \in C_i^{2n+1}, \quad v = (x_2, |x_2| + \beta, x_2 + y_2) \in C_j^{2n+1},$$

где α и β определены выше (см. (2), (3)). Очевидно, что для совпадения u и v необходимо выполнение следующих равенств:

$$x_1 = x_2, \quad |x_1| + \alpha = |x_2| + \beta, \quad x_1 + y_1 = x_2 + y_2. \quad (8)$$

Поскольку $x_1 = x_2$, имеем $|x_1| = |x_2|$. Отсюда, учитывая (8), можно заключить, что для равенства двух данных векторов необходимо $\alpha = \beta$. Но при

$$i \leq n, \quad n < j \leq 2n+1 \quad \text{либо} \quad n < i \leq 2n+1, \quad j \leq n \quad (9)$$

это невозможно, следовательно, $\alpha \neq \beta$, а значит, можно заключить, что если i, j удовлетворяют (9), то коды C_i и C_j пересекаются по пустому множеству, т. е. $r_{ij} = 0$. Если же $0 \leq i, j \leq n$ (случай $n < i, j \leq 2n+1$ аналогичен, только следует принять во внимание, что Q — это $(n+1) \times (n+1)$ -матрица), то, используя определение конструкции А, несложно показать, что мощность r_{ij} пересечения кодов C_i^{2n+1} и C_j^{2n+1} будет удовлетворять равенству

$$r_{ij} = |C_i^{2n+1} \cap C_j^{2n+1}| = |E^n| q_{ij} = 2^n q_{ij}.$$

Отсюда следует справедливость (7). Лемма 5 доказана.

Докажем аналогичную лемму для конструкции В.

Лемма 6. Пусть Q_t — матрица пересечений разбиения P^t куба E^t на коды Хэмминга, а Q_m — матрица пересечений разбиения P^m куба E^m на коды Хэмминга. Тогда для элементов матрицы пересечений R разбиения P^n , $n = tm + t + m$, полученного с помощью конструкции В из P^t и P^m , справедливо равенство $r_{lskr} = 2^{tm} p_{lk} q_{sr}$, где r_{lskr} — элемент матрицы пересечений разбиения P^n , отвечающий пересечению кодов C_{ls}^n и C_{kr}^n , т. е.

$$r_{lskr} = |C_{ls}^n \cap C_{kr}^n|.$$

ДОКАЗАТЕЛЬСТВО. Пусть $Q_t = (p_{lk})$ и $Q_m = (q_{sr})$ — матрицы пересечений разбиений P^t и P^m соответственно, т. е. $p_{lk} = |C_l^t \cap C_k^t|$, $q_{sr} = |C_s^m \cap C_r^m|$. Нетрудно видеть, что согласно конструкции В разбиению P^n соответствует матрица пересечений с элементами

$$r_{lskr} = |E^{ts}| \cdot |C_l^t \cap C_k^t| \cdot |C_s^m \cap C_r^m| = 2^{tm} p_{lk} q_{sr}.$$

Лемма 6 доказана.

Через $R_{n;\text{trans}}$, $R_{n;\text{vertex-trans}}$, $R_{n;2\text{-trans}}$ обозначим число неэквивалентных транзитивных, вершинно-транзитивных, 2-транзитивных разбиений E^n на совершенные двоичные коды соответственно. Используя изложенные выше факты, докажем следующее утверждение.

Теорема 5. Для любого $n \geq 2^k - 1$, $k > 20$, число неэквивалентных транзитивных разбиений E^n на совершенные коды удовлетворяет нижней оценке $R_{n;\text{trans}} > n + 1$.

ДОКАЗАТЕЛЬСТВО. Докажем теорему индукцией по $k \geq 6$, где $n_k = 2^{3+3k} - 1$ является длиной разбиения. Подчеркнём, что из лемм 5, 6 и 2 вытекает, что разбиения одинаковой длины, построенные с помощью конструкций А и В и имеющие разные матрицы состава, будут неэквивалентны. Как можно видеть из приложения, все одиннадцать разбиений из [14] имеют различные матрицы состава (см. определение в конце разд. 3), т. е. матрицы пересечений попарно не эквивалентны, а следовательно, согласно лемме 2 эти разбиения попарно не эквивалентны. Отсюда, используя конструкции А и В для разбиения длины $n_k = tm + t + m$, с учётом того, что конструкция А (в отличие от конструкции В) оставляет число разбиений прежним, имеем следующую оценку для числа неэквивалентных разбиений длины n_k :

$$R_{n_k} \geq R_7 \cdot R_{\frac{n_k-7}{8}} + \frac{1}{2} \sum_{t \neq 7, \frac{n_k-t}{t+1} \neq t} (R_t \cdot R_{\frac{n_k-t}{t+1}}) + R' + R_{n_k-1},$$

где

$$R' = \begin{cases} 0 & \text{при } k \equiv 0 \pmod{2}, \\ \frac{R_{t'}(R_{t'}+1)}{2} & \text{при } k \equiv 1 \pmod{2}, \end{cases} \quad (10)$$

где $t' = \sqrt{n_k + 1} - 1$. Ограничимся неравенством вида

$$R_n > R_7 \cdot R_{\frac{n_k-7}{8}} + R_{n_{k-1}}, \quad (11)$$

так как вклад остальных слагаемых в общую сумму незначителен по сравнению с (11). Изначально согласно лемме 1 имеем 7 транзитивных разбиений пространства E^7 .

БАЗА ИНДУКЦИИ: при $k = 6$ имеем $R_{n_6;\text{trans}} = 2409344 > 2097151 + 1$, $n_1 = 2097151$.

ШАГ ИНДУКЦИИ. Пусть для $n_{k-1} = 2^{3+3(k-1)} - 1$, $k > 6$, существует не менее $R_{n_{k-1};\text{trans}}$ различных разбиений, т. е. $R_{n_{k-1};\text{trans}} > n_{k-1} + 1$. Тогда, применив конструкцию В к этим разбиениям, получим для $n_k = 2^{3+3k}$ неравенство

$$R_{n_k;\text{trans}} > 8 \cdot R_{n_{k-1};\text{trans}}. \quad (12)$$

Выражая n_{k-1} через n_k , имеем $\log_2 n_{k-1} + 1 = \log_2 n_k + 1 - 3$, откуда

$$n_{k-1} + 1 = (n_k + 1)/8.$$

Используя это выражение, из формулы (12) получим требуемую оценку:

$$R_{n_k;\text{trans}} > 8 \cdot (n_{k-1} + 1) = n_k + 1.$$

Теорема 5 доказана.

С использованием того же метода легко доказываются

Следствие 1. Для любого $n \geq 2^m - 1$, $m > 20$, число $R_{n;\text{vertex-trans}}$ неэквивалентных вершинно-транзитивных разбиений E^n на совершенные коды длины n удовлетворяет нижней оценке

$$R_{n;\text{vertex-trans}} > \frac{n+1}{2}.$$

Следствие 2. Для любого $n \geq 2^m - 1$, $m > 20$, число $R_{n;2\text{-trans}}$ неэквивалентных 2-транзитивных разбиений E^n на совершенные коды длины n удовлетворяет нижней оценке

$$R_{n;2\text{-trans}} > \frac{n+1}{3}.$$

Для малых значений длин кодов $n \leq 2^{20} - 1$ этот метод позволяет получить только следующие оценки.

Следствие 3. Для любого $n \geq 2^m - 1$, где $3 \leq m \leq 20$, числа неэквивалентных транзитивных, вершинно-транзитивных и 2-транзитивных разбиений E^n на совершенные коды удовлетворяют следующим нижним оценкам:

- (i) $R_{n;\text{trans}} \geq \frac{n+1}{2}$;
- (ii) $R_{n;\text{vertex-trans}} \geq \frac{n+1}{3}$;
- (iii) $R_{n;2\text{-trans}} \geq \frac{n+1}{4}$.

5. Приложение

Ниже, как и в разд. 3, $M(P_i^7)$ обозначает матрицу пересечений i -го разбиения пространства E^7 на коды Хэмминга длины 7 из классификации Фелпса [14]. Каждая матрица симметрична, поэтому элементы ниже главной диагонали опущены, на главной диагонали, очевидно, должно стоять только 16. Таблица $S(P_i)$ обозначает состав матрицы, т. е. сколько раз в данной матрице выше главной диагонали встречаются числа 4, 8 и 16, $i = 0, 1, \dots, 10$.

$M(P_0^7):$		0	1	2	3	4	5	6	7
	0		16	16	16	16	16	8	8
	1			16	16	16	16	8	8
	2				16	16	16	8	8
	3					16	16	8	8
	4						16	8	8
	5							8	8
	6								16
	7								
$M(P_1^7):$		0	1	2	3	4	5	6	7
	0		16	16	16	4	4	4	4
	1			16	16	4	4	4	4
	2				16	4	4	4	4
	3					4	4	4	4
	4						16	16	16
	5							16	16
	6								16
	7								

$S(P_0^7):$	4	8	16
	0	12	16

$S(P_1^7):$	4	8	16
	16	0	12

$M(P_2^7):$

	0	1	2	3	4	5	6	7
0		16	8	8	4	4	8	8
1			8	8	4	4	8	8
2				16	8	8	4	4
3					8	8	4	4
4						16	8	8
5							8	8
6								16
7								

 $S(P_2^7):$

4	8	16
8	16	4

 $M(P_3^7):$

	0	1	2	3	4	5	6	7
0		16	8	4	8	4	8	8
1			8	4	8	4	8	8
2				8	16	8	16	16
3					8	16	8	8
4						8	16	16
5							8	8
6								16
7								

 $S(P_3^7):$

4	8	16
4	16	8

 $M(P_4^7):$

	0	1	2	3	4	5	6	7
0		16	16	16	4	8	4	8
1			16	16	4	8	4	8
2				16	4	8	4	8
3					4	8	4	8
4						8	16	8
5							8	16
6								8
7								

 $S(P_4^7):$

4	8	16
8	12	8

 $M(P_5^7):$

	0	1	2	3	4	5	6	7
0		16	16	16	16	16	16	16
1			16	16	16	16	16	16
2				16	16	16	16	16
3					16	16	16	16
4						16	16	16
5							16	16
6								16
7								

 $S(P_5^7):$

4	8	16
0	0	28

 $M(P_6^7):$

	0	1	2	3	4	5	6	7
0		16	4	4	4	4	4	4
1			4	4	4	4	4	4
2				4	4	16	4	4
3					4	4	16	4
4						4	4	16
5							4	4
6								4
7								

 $S(P_6^7):$

4	8	16
24	0	4

$M(P_7^7):$		0	1	2	3	4	5	6	7
	0		16	8	8	4	8	4	8
	1			8	8	4	8	4	8
	2				16	8	4	8	4
	3					8	4	8	4
	4						8	16	8
	5							8	16
	6								8
	7								
$M(P_8^7):$		0	1	2	3	4	5	6	7
	0		4	4	4	4	4	4	4
	1			4	4	4	4	4	4
	2				4	4	4	4	4
	3					4	4	4	4
	4						4	4	4
	5							4	4
	6								4
	7								
$M(P_9^7):$		0	1	2	3	4	5	6	7
	0		16	8	8	16	16	8	8
	1			8	8	16	16	8	8
	2				16	8	8	16	16
	3					8	8	16	16
	4						16	8	8
	5							8	8
	6								16
	7								
$M(P_{10}^7):$		0	1	2	3	4	5	6	7
	0		16	8	4	4	4	8	4
	1			8	4	4	4	8	4
	2				8	8	8	16	8
	3					4	16	8	4
	4						4	8	16
	5							8	4
	6								8
	7								

 $S(P_7^7):$

4	8	16
8	16	4

 $S(P_8^7):$

4	8	16
28	0	0

 $S(P_9^7):$

4	8	16
0	16	12

 $S(P_{10}^7):$

4	8	16
12	12	4

ЛИТЕРАТУРА

1. Августинovich С. В., Соловьева Ф. И., Хеден У. О разбиениях n -куба на неэквивалентные совершенные коды // Пробл. передачи информ. — 2007. — Т. 43, № 4. — С. 45–50.
2. Васильев Ю. Л. О негрупповых плотно упакованных кодах // Пробл. кибернетики. Вып. 8. — М: Физматгиз, 1962. — С. 337–339.
3. Соловьева Ф. И. О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. Вып. 37. — Новосибирск: Ин-т математики СО РАН, 1981. — С. 65–76.

4. Соловьёва Ф. И. О построении транзитивных кодов // Пробл. передачи информ. — 2005. — Т. 41, № 3. — С. 23–31.
5. Соловьёва Ф. И. О транзитивных разбиениях n -куба на коды // Пробл. передачи информ. — 2008. — Т. 44, вып. 4. — С. 27–35.
6. Соловьёва Ф. И., Лось А. В. О построении разбиений на совершенные q -значные коды // Дискрет. анализ и исслед. операций. — 2009. — Т. 16, № 3. — С. 63–73.
7. Фон-дер-Флаасс Д. Г. Совершенные 2-раскраски гиперкуба // Сиб. мат. журн. — 2007. — Т. 48. — С. 923–930.
8. Avgustinovich S. V., Lobstein A., Solov'eva F. I. Intersection matrices for partitions by binary perfect codes // IEEE Trans. Inform. Theory. — 2001. — Vol. 47, N 4. — P. 1621–1624.
9. Cohen G., Honkala I., Lobstein A., Litsyn S. Covering codes. — Amsterdam, Lausanne, New York, Oxford, Shannon, Tokyo: Elsevier, 1998. — 542 p.
10. Etzion T., Vardy A. Perfect binary codes and tilings: problems and solutions // SIAM J. Discrete Math. — 1998. — Vol. 11, N 2. — P. 205–223.
11. Heden O., Solov'eva F. I. On partitions of n -cube into Hamming codes // Adv. Math. Commun. — 2009. — Vol. 3, N 4. — P. 385–397.
12. Mollard M. A generalized parity function and its use in the construction of perfect codes // SIAM J. Alg. Discrete Math. — 1986. — Vol. 7, N 1. — P. 113–115.
13. Östergård P. R. J. On a hypercube coloring problem // J. Combin. Theory. Ser. A. — 2004. — Vol. 108. — P. 199–204.
14. Phelps K. T. An enumeration of 1-perfect binary codes // Australasian J. Combin. — 2000. — Vol. 21. — P. 287–298.
15. Solov'eva F. I. On perfect codes and related topics, Com²Mac // Lect. Note. Ser. 13. — Pohang: Pohang Univ. Sci. Technology, 2004. — 80 p.
16. Solov'eva F. I. Existence of transitive partitions into binary codes // Proc. 11th Int. Workshop Algebr. Comb. Coding Theory (Pamporovo, Bulgaria, June 2008). — Pamporovo: Institute of Mathematics and Informatics, Bulgarian Academy of Sciences, 2008. — P. 267–272.

Соловьёва Фаина Ивановна,
e-mail: sol@math.nsc.ru

Гуськов Георгий Константинович,
e-mail: m1lesnsk@gmail.com

Статья поступила
11 февраля 2010 г.

Переработанный вариант —
10 марта 2010 г.