О разбиениях n-куба на совершенные двоичные коды[1]

Г. К. Гуськов

Институт математики им. Соболева СО РАН,
e-mail: m1lesnsk@gmail.com

Ф. И Соловьёва

Институт математики им. Соболева СО РАН,
Новосибирский Государственный Университет,
e-mail: sol@math.nsc.ru

Аннотация

В работе предложена свитчинговая конструкция разбиений n-куба на совершенные двоичные коды, приведена нижняя оценка числа таких разбиений.

1 Введение

Проблеме исследования разбиений n-куба $\mathbb{F}^n$ (векторного пространства размерности n всех двоичных векторов длины n с метрикой Хэмминга) на совершенные двоичные коды посвящено значительно меньше статей, чем вопросам построения новых совершенных кодов и исследования их свойств, хотя две этих задачи тесно связаны, а именно, асимптотики двойных логарифмов числа различных совершенных кодов и числа различных разбиений на такие коды совпадают. Также следует упомянуть о связи разбиений $\mathbb{F}^n$ со следующими проблемами раскрасок вершин $\mathbb{F}^n$: разбиения n-куба индуцируют раскраски, связанные с оптоволоконными сетями, см. [1], кроме того, они индуцируют совершенные раскраски, упоминаемые в литературе как полностью регулярные коды (называемые также partition designs или equitable partitions) [2]. Две конструкции (каскадная и свитчинговая) нетривиальных разбиений n-куба на совершенные коды были предложены в [3]. В [4] была получена следующая нижняя оценка числа различных разбиений $\mathbb{F}^n$ на совершенные коды длины n (для любого допустимого $n \geq 31$):

$$2^{2^{\frac{(n-1)}{2}}}. \tag{1}$$

Приведём первые три фактора нижней оценки числа совершенных двоичных кодов, полученной С. В. Августиновичем и Д. С. Кротовым, см. [7], которая является лучшей на сегодняшний день:

$$2^{2^{\frac{n+1}{2}-\log(n+1)}} \cdot 3^{2^{\frac{n-3}{4}}} \cdot 2^{2^{\frac{n+5}{4}-\log(n+1)}}. \tag{2}$$

В статье [8] были предложены конструкции разбиений $\mathbb{F}^n$ на транзитивные коды, которые в дальнейшем были развиты в [9, 10] для построения 2-транзитивных и вершинно-транзитивных разбиений $\mathbb{F}^n$ на совершенные двоичные коды. В работе [11] С. В. Августиновичем и др. была представлена конструкция разбиений $\mathbb{F}^n$ на попарно неэквивалентные коды. В [12] С. В. Августиновичем и др. были исследованы матрицы пересечений разбиений. В статье [13] предложено две конструкции разбиений множества всех q-ичных векторов длины n на совершенные q-значные коды и приведена нижняя оценка числа различных разбиений на такие коды.

[1]Настоящая работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (проект 10-01-00424-а).

В настоящей работе приводится свитчинговый метод построения разбиений n-куба на совершенные двоичные коды и отвечающая ему нижняя оценка числа различных разбиений для любых допустимых $n \geq 7$. Нетривиальная верхняя оценка для числа таких разбиений пока не найдена.

2 Необходимые определения и понятия

Расстояние Хэмминга $d(x, y)$ между векторами x и y из $\mathbb{F}^n$ равно количеству координат, в которых различаются эти векторы. *Двоичным кодом* называется произвольное подмножество C из $\mathbb{F}^n$. *Совершенным двоичным кодом, исправляющим одиночные ошибки* (далее кратко *совершенным кодом*), называется такое подмножество из $\mathbb{F}^n$, что любой вектор пространства $\mathbb{F}^n$ находится на расстоянии не больше 1 от некоторого единственного вектора из C. Известно, что такие коды существуют только при $n = 2^m - 1,\ \ m \geq 2$.

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

$$\mathrm{Aut}(\mathbb{F}^n) = \{(v, \pi) \mid v \in \mathbb{F}^n,\ \pi \in S_n\},$$

где S_n — симметрическая группа подстановок длины n. *Группой автоморфизмов* $\mathrm{Aut}(C)$ кода C длины n называется группа изометрий пространства $\mathbb{F}^n$, переводящих код в себя. *Группой автоморфизмов произвольного разбиения* $P^n = \{C_0, C_1, \ldots, C_n\}$ *пространства* $\mathbb{F}^n$ *на совершенные коды* $C_0, C_1, \ldots, C_n$, назовём группу изометрий пространства $\mathbb{F}^n$, переводящих разбиение P^n в себя. Два разбиения $\mathbb{F}^n$ называются *различными*, если они различаются по меньшей мере в одном коде. Далее будем говорить, что *разбиение имеет длину* n, если оно состоит из кодов длины n.

В работе [14] К. Т. Фелпсом были классифицированы разбиения $\mathbb{F}^7$ на совершенные коды длины 7, а также описаны их группы автоморфизмов, всего было обнаружено 11 таких разбиений. Представим порядки их групп автоморфизмов в следующей таблице:

i	0	1	2	3	4	5	6	7	8	9	10
$\lvert Aut(P_i^7)\rvert$	768	1536	256	128	128	21504	384	256	336	1024	96

Используя эти данные, несложно подсчитать число различных разбиений $\mathbb{F}^7$ на совершенные коды длины 7.

Предложение 1. *Существует* $27360 = c \cdot 2^{14}$ *различных разбиений* $\mathbb{F}^7$ *на совершенные коды длины* 7, *где* $c > 1.66$.

3 Разбиения на совершенные коды длины 15

В этом параграфе покажем, что конструкция Васильева и результат Фелпса о классификации разбиений $\mathbb{F}^7$ позволяют получить нижнюю оценку числа разбиений $\mathbb{F}^{15}$ на совершенные коды. Заметим, см. [4], что этот случай оставался неизученным. Разбиения длины 15 представляют особенный интерес для исследований в силу того, что они зачастую выступают в качестве исходной точки для конструирования разбиений, а также кодов больших длин. В частности, совершенных кодов с определёнными свойствами, например, транзитивных кодов (см. [15]).

Пусть $\{C_0, \ldots, C_n\}$ некоторое разбиение $\mathbb{F}^n$ на совершенные двоичные коды $C_i,\ \ i = 0, 1, \ldots, n$. Рассмотрим следующую конструкцию разбиения куба $\mathbb{F}^{2n+1}$ (см. [4], также эта конструкция использовалась в [16]), на совершенные коды Васильева [17] длины $2n + 1$:

$$\begin{cases} C_i^{2n+1} = & \{(\tau(x)+y, |x|+\lambda_i(y), \sigma(x))\}, \\ C_{n+1+i}^{2n+1} = & \{(\tau(x)+y, |x|+\lambda_i(y)+1, \sigma(x))\}; \end{cases} \tag{3}$$

где $x \in \mathbb{F}^n$, $y \in C_i^n$, τ, σ – произвольные перестановки из S_n, $i = 0, 1, \ldots, n$, λ_i – произвольная двоичная функция, определённая на вершинах из C_i^n, такая что $\lambda_i(e_i) = 0,\ i = 0, \ldots, n$. Здесь e_i – вектор из $\mathbb{F}^n$ веса 1 с "1" на i-ой координатной позиции, $e_0 = \mathbf{0}^n$ – нулевой вектор длины n из $\mathbb{F}^n$, состоящий из нулей.
Через $\mathcal{M}_n$ и $\mathcal{M}'_n$ обозначим число различных и неэквивалентных разбиений $\mathbb{F}^n$ на совершенные коды, соответственно. Используя конструкцию (3) и применяя предложение 1, легко показать, что справедлива

Лемма 1. *Число $\mathcal{M}_{15}$ различных разбиений $\mathbb{F}^{15}$ на совершенные двоичные коды удовлетворяет следующей нижней оценке*

$$\mathcal{M}_{15} > 2^{159}. \tag{4}$$

Заметим, что число всех автоморфизмов куба $\mathbb{F}^{15}$ равно $15! \cdot 2^{15}$, что не превосходит 2^{56}. Таким образом, справедливо

Следствие 1. *Число $\mathcal{M}'_{15}$ неэквивалентных разбиений куба $\mathbb{F}^{15}$ на совершенные двоичные коды удовлетворяет следующей нижней оценке*

$$\mathcal{M}'_{15} > 2^{103}. \tag{5}$$

Замечание 1. Сравнивая оценку (5) для числа неэквивалентных разбиений куба $\mathbb{F}^{15}$ на совершенные двоичные коды длины 15 с оценкой числа неэквивалентных совершенных двоичных кодов длины 15, которых, согласно [19], существует ровно 5983, с учётом того, что $5983 < 2^{13}$, убеждаемся, что число неэквивалентных разбиений существенно больше числа неэквивалентных совершенных кодов.

В следующей теореме уточним оценку из [4] :

Теорема 1. *Число различных разбиений $\mathbb{F}^n$ на совершенные коды длины n не менее*

$$2^{2^{\frac{n-1}{2}}} \cdot 2^{2^{\frac{n-3}{4}}} \tag{6}$$

для любого $n = 2^m - 1,\ m \geq 3$.

Доказательство теоремы аналогично доказательству теоремы 3 из [4], с учётом предложения 1 и леммы 1. Заметим, что оценка (4) лучше, чем (6) при $n = 15$.

4 Нижняя оценка числа разбиений на совершенные коды, метод ijk-компонент

Будучи применённым к коду Хэмминга (линейному совершенному коду), метод ijk-компонент позволяет строить богатые классы кодов, разбиений, а также выступает мощным инструментом для исследования свойств этих объектов. В этом параграфе покажем, что нижняя оценка (6) может быть значительно улучшена. Для этой цели приведём конструкцию разбиений куба $\mathbb{F}^n$ на совершенные двоичные коды, основанную на методе ijk-компонент, который, в свою очередь, является частным случаем метода α-компонент из [18]. Рассмотрим следующие функции

$$\begin{array}{l} \sigma_l : \{1, \ldots, N_2\} \times \{1, \ldots, N_1\} \to \{0, 1\}; \\ \xi_l : \{1, \ldots, N_2\} \times \{1, \ldots, N_1\} \to \{0, 1\}; \\ \tau_l : \{1, \ldots, N_2\} \to \{0, 1\}; \\ \nu_l : \{1, \ldots, N_2\} \to \{i, j, k\}; \end{array} \tag{7}$$

где $N_1 = 2^{\frac{n-3}{4}}$, $N_2 = 2^{\frac{n+5}{4}-log_2(n+1)}$, $l = 0, 1, \ldots, \frac{n-3}{4}$, а также циклическую подстановку $\pi = (i\, j\, k)$. Определим отображение $\varphi = (\sigma, \xi, \tau, \nu)$, где

$$\sigma = (\sigma_0, \ldots, \sigma_{\frac{n-3}{4}}),\ \xi = (\xi_0, \ldots, \xi_{\frac{n-3}{4}}),\ \tau = (\tau_0, \ldots, \tau_{\frac{n-3}{4}}),\ \nu = (\nu_0, \ldots, \nu_{\frac{n-3}{4}}).$$

Набор функций $(\sigma_l, \xi_l, \tau_l, \nu_l)$, $l \in \{0, 1, \ldots, \frac{n-3}{4}\}$, будем называть *вырожденным*, если существуют $t, q \in \{1, \ldots, N_2\}$, такие что $\sigma_l(t, s) \equiv const$ и $\xi_l(q, m) \equiv const$ для любых $s, m \in \{1, \ldots, N_1\}$. Отображение φ будем называть *вырожденным*, если вырождены все наборы $(\sigma_l, \xi_l, \tau_l, \nu_l)$.

Идея, лежащая в основе предлагаемой конструкции, была впервые предложена в [11]. Рассмотрим разбиение $P = \{H_0, \ldots, H_n\}$ куба $\mathbb{F}^n$ на классы смежности кода Хэмминга, где $H_i = H + e_i$. Сгруппируем коды разбиения в четвёрки

$$\{H_{4l}, H_{4l+1}, H_{4l+2}, H_{4l+3}\},\ l = 0, 1, \ldots, \frac{n-3}{4}.$$

Разобьём H_{4l} на ijk-компоненты (согласно [11], их будет N_2). Это разбиение индуцирует разбиения остальных кодов четвёрки. Каждую ijk-компоненту из H_{4l} разобьём на i-, j- или k-компоненты (согласно [11], их будет N_1). Естественным образом это разбиение индуцирует разбиения в остальных кодах четвёрки. Все ijk-компоненты в H_{4l} пронумеруем индексами из $\{1, \ldots, N_2\}$, а все i-компоненты (j- или k-компоненты) внутри каждой ijk-компоненты – индексами из $\{1, \ldots, N_1\}$. Аналогично перенумеруем компоненты в остальных кодах разбиения. В результате любой вектор u из каждого кода разбиения будет иметь некоторую пару индексов (r, s), $r \in \{1, \ldots, N_2\}$, $s \in \{1, \ldots, N_1\}$.

Приведём описание конструкции. Каждой четвёрке $\{H_{4l}, H_{4l+1}, H_{4l+2}, H_{4l+3}\}$ соответствует набор функций $(\sigma_l, \xi_l, \tau_l, \nu_l)$. Каждый код разбивается на ijk-компоненты. Каждая ijk-компонента, в свою очередь, разбивается на i-, j- или k-компоненты, в зависимости от значения функции $\nu_l(r)$, где r – это индекс ijk-компоненты.

Выберем в коде H_{4l} произвольную ijk-компоненту R_{ijk}. В зависимости от значения функции $\sigma_l(r, s)$, для каждой i-компоненты (j- или k-компоненты) из R_{ijk}, где s – её индекс в R_{ijk}, а r – индекс R_{ijk} в коде H_{4l}, либо производится свитчинг этой компоненты по соответствующему направлению (i, j или k), либо она не сдвигается. При этом, используется следующее правило. Если R_{ijk} была разбита на i-компоненты (т.е. $\nu_l(r) = i$), то свитчинг производится с соответствующей i-компонентой из $R_{ijk} + e_1$. Если $\nu_l(r) = j$, то свитчинг производится с отвечающей ей j-компонентой из $R_{ijk} + e_3$. И, наконец, если $\nu_l(r) = k$, то с соответствующей k-компонентой из $R_{ijk} + e_2$. Таким образом, такой свитчинг в R_{ijk} порождает пару свитчингов – в самой R_{ijk} и в ijk-компоненте, определяемой направлением, по которому производится свитчинг. Легко видно, что всего таких свитчингов, в силу того, что в R_{ijk} имеется N_1 компонент по направлению i (j или k), будет 2^{N_1}.

Аналогичная процедура независимо проводится для функции ξ_l с тем лишь ограничением, что свитчинг производится между i-компонентами (j- или k-компонентами) из незадействованных на первом шаге пар ijk-компонент, в зависимости от значения ξ_l. А именно, при $\nu_l(r) = i$ обмениваются i-компонентами $R_{ijk} + e_3$ и $R_{ijk} + e_2$ (j-компонентами при $\nu_l(r) = j$ обмениваются $R_{ijk} + e_1$ и $R_{ijk} + e_2$, а k-компонентами при $\nu_l(r) = k$ обмениваются $R_{ijk} + e_1$ и $R_{ijk} + e_3$).

Затем, в зависимости от значения функции $\tau_l(r)$, либо производится свитчинг полученной из R_{ijk} в результате таких преобразований ijk-компоненты компоненты по направлению $\pi(\nu_l(r))$, либо она не сдвигается. Для оставшейся пары ijk-компонент это преобразование дублируется.

Описанные операции далее могут быть проделаны для остальных ijk-компонент из H_{4l}. Таким образом, получаем в точности $(2 \cdot 2)^{N_1 N_2} \cdot 2^{N_2}$ таких свитчингов.

Лемма 2. *Если отображения* $\varphi = (\sigma, \xi, \tau, \nu)$ *и* $\varphi' = (\sigma', \xi', \tau', \nu')$ *различны, то разбиения* $\mathcal{P} = \varphi(P)$ *и* $\mathcal{P}' = \varphi'(P)$ *куба* $\mathbb{F}^n$ *на совершенные двоичные коды различны.*

Используя лемму 2, подсчитаем число R_n различных разбиений длины n. Для этой цели найдём число различных наборов $(\sigma_l, \xi_l, \tau_l, \nu_l)$. Нетрудно видеть, что их будет $(2\cdot 2)^{N_1 N_2}\cdot(2\cdot 3)^{N_2}$. Так как в каждой четвёрке кодов преобразования производятся независимо, число R_n различных разбиений длины n удовлетворяет неравенству

$$R_n \geq (4^{N_1 N_2}\cdot 6^{N_2})^{\frac{n+1}{4}} = 2^{2^{\frac{n-1}{2}}}\cdot 6^{2^{\frac{n-3}{4}}}.$$

Найдём верхнюю оценку числа вырожденных преобразований. По определению, параметры t и q можно выбрать N_2 способами. Значения функций $\sigma(t,s)$ и $\xi(q,m)$ можно выбрать двумя способами для каждой, то есть "1" или "0". Оставшиеся значения для четвёрки $(\sigma_l, \xi_l, \tau_l, \nu_l)$ можно задать $4^{N_1(N_2-1)}\cdot 6^{N_2}$ способами. Следовательно, число вырожденных преобразований φ не больше

$$(4\cdot N_2\cdot N_2\cdot 4^{N_1(N_2-1)}\cdot 6^{N_2})^{\frac{n+1}{4}},$$

что является бесконечно малой величиной по сравнению с $(4^{N_1 N_2}\cdot 6^{N_2})^{\frac{n+1}{4}}$, числом различных отображений φ для достаточно большого n и может быть компенсировано произволом выбора тройки ijk в коде Хэмминга H_0. Таким образом, справедлива

Теорема 2. *Число* R_n *различных разбиений* $\mathbb{F}^n$ *на совершенные коды длины* n *удовлетворяет следующей нижней оценке*

$$R_n \geq 2^{2^{\frac{n-1}{2}}}\cdot 6^{2^{\frac{n-3}{4}}} \tag{8}$$

для любого допустимого, $n \geq 15$.

Сравнение полученных нижних оценок (6) и (8) для числа различных разбиений длины n (обратим внимание на совпадение первых факторов), а также анализ всех известных нижних оценок числа различных совершенных кодов длины n позволяют предположить, что *первый множитель* $2^{2^{\frac{n-1}{2}}}$ *в нижней оценке числа различных разбиений куба* $\mathbb{F}^n$ *на совершенные коды длины* n *неулучшаем.*

Замечание 2. При длине разбиения $n = 15$, конструкция Васильева позволяет получить нижнюю оценку числа различных разбиений примерно в 40 раз точнее, по сравнению с применением метода ijk-компонент: $2^{141}\cdot 3^8$ и 2^{159}, соответственно. Но, начиная с $n = 31$, оценка, полученная применением метода ijk-компонент, становится лучше.

Замечание 3. Конструкция (3) с функциями $\lambda_i \equiv 0,\ i = 0, \ldots, n$, использовалась в [16] для построения широкого класса различных разбиений на непараллельные коды Хэмминга.

Список литературы

[1] *Östergård P. R. J.* On a hypercube coloring problem // J. Combin. Theory Ser. A, **108**, 2004. P. 199–204.

[2] *Fon-Der-Flaas D. G.* Perfect colorings of a hypercube // Sib. Math. Journal, **48**, 2007. P. 923–930.

[3] *Соловьева Ф. И.* О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. Новосибирск: Ин-т математики СО АН СССР. 1981. Вып. 37. С. 65–76.

[4] *Solov'eva F. I.* On perfect codes and related topics // *Com*^{2}*Mac* Lecture Note Series13, Pohang 2004.

[5] *Кротов Д. С.* Конструкции плотно упакованных кодов и нижние оценки их числа // Канд. дисс., Новосибирск, 2000. 64 с.

[6] *Phelps K. T.* A General Product Construction for Error Correcting Codes // SIAM J. Algebraic Discrete Methods, 1984. V. 5. P. 224–228.

[7] *Krotov D. S., Avgustinovich S. V.* On the number of 1-perfect binary codes: A lower bound // IEEE Trans. Inf. Theory, 2008. V. 54, no. 4. P. 1760–1765.

[8] *Solov'eva F. I.* On transitive partitions of n-cube into codes // Problems of Inform. Transm., **45** (1), 2009. P. 27–35.

[9] *Solov'eva F. I., Guskov G. K.* On vertex-transitive and 2-transitive partitions of $\mathbb{F}^n$ into perfect codes // Proc. XII Int. Symposium on Problems of Redundancy in Information и Control Systems. St.-Petersburg, Russia, May, 26-30, 2009. P. 104–108.

[10] *Соловьёва Ф. И., Гуськов Г. К.* О построении вершинно-транзитивных разбиений n-куба на совершенные коды, Дискретный анализ и исследование операций, т.17, №3, 2010. С.84–100.

[11] *Avgustinovich S. V., Solov'eva F. I., Heden O.* Partitions of an n-Cube into Nonequivalent Perfect Codes // Problems Inform. Transmission, **43** (4), 2007. P. 310–315.

[12] *Avgustinovich S. V., Lobstein A. and Solov'eva F. I.* Intersection matrices for partitions by binary perfect codes // IEEE Trans. Inform. Theory, **47**, 2001. P. 1621–1624.

[13] *Solov'eva F. I., Los' A. V.* Constructions of partitions of $\mathbb{F}_q^n$ into perfect q-ary codes // Discrete Analysis and Oper. Research, **16** (3), 2009. P. 63–73.

[14] *Phelps K.T.* An enumeration of 1-perfect binary codes // Australas. J. Comb., **21**, (2000). P. 287–298.

[15] *Solov'eva F. I.* On the Construction of Transitive Codes // Problems of Inform. Transm.,**41**(3), 2005. P. 204–211.

[16] *Heden O., Solov'eva F. I.* Partitions of $\mathbb{F}^n$ into nonparallel Hamming codes // Advances in Math. of Communications, **3** (4), 2009. P. 385–397.

[17] *Васильев Ю. Л.* О негрупповых плотно упакованных кодах // Проблемы кибернетики. М: Физматгиз, 1962. Вып. 8. С. 337–339.

[18] *Августинович С. В., Соловьева Ф. И.* Построение совершенных бинарных кодов последовательными сдвигами α-компонент // Пробл. передачи информ. 1997. Т. 33. Вып. 3. С. 15–21.

[19] *Östergård P. R. J., Pottonen O.* The Perfect Binary One-Error-Correcting Codes of Length 15: Part I – Classification // IEEE Trans. Inform. Theory **55**, 2009. P. 4657–4660.

[20] *Гуськов Г. К.* О числе различных разбиений куба $\mathbb{F}^{15}$ на совершенные двоичные коды // *Материалы 47 Международной научной студенческой конференции "Студент и научно-технический прогресс": Математика. Новосиб. гос. ун-т. Новосибирск*, 2009. С. 160.