ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Март—апрель 2013. Том 20, № 2. С. 15–25

УДК 519.8

# О РАЗБИЕНИЯХ ДВОИЧНОГО ВЕКТОРНОГО ПРОСТРАНСТВА НА СОВЕРШЕННЫЕ КОДЫ

*Г. К. Гуськов*

**Аннотация.** С помощью свитчинговой конструкции $ijk$-компонент получена лучшая на сегодняшний день нижняя оценка числа разбиений двоичного векторного пространства на совершенные коды ранга, превосходящего ранг кода Хэмминга той же длины не более чем на 2.

**Ключевые слова:** совершенный двоичный код, разбиение двоичного векторного пространства на совершенные коды, ранг разбиения, нижняя оценка числа разбиений.

## Введение

Проблема исследования разбиений пространства $\mathbb{F}^n$ (векторного пространства длины $n$ над $GF(2)$ по отношению к метрике Хэмминга) тесно связана с проблемой построения совершенных кодов и изучения их свойств, поскольку асимптотики двойных логарифмов (если они существуют) числа различных совершенных кодов и числа различных разбиений на такие коды совпадают. Также следует упомянуть о том, что некоторые разбиения пространства $\mathbb{F}^n$ индуцируют раскраски векторов $\mathbb{F}^n$, связанные с оптоволоконными сетями (см., например, [15]). Кроме того, разбиения индуцируют совершенные раскраски, упоминаемые в литературе как полностью регулярные коды [11], partition designs, equitable partitions. Различные методы построения разбиений могут быть использованы для исследования нетривиальных свойств разбиений, а также для построения новых совершенных кодов.

Две конструкции (каскадная и свитчинговая) нетривиальных разбиений пространства $\mathbb{F}^n$ на совершенные коды предложены в [7], см. также [17]. В [2] с помощью известной конструкции Васильева [3] для совершенных двоичных кодов построен широкий класс разбиений на совершенные двоичные коды и получена следующая нижняя оценка числа $\mathcal{M}_n$ различных разбиений пространства $\mathbb{F}^n$ на совершенные коды длины $n$ для любого допустимого $n \geqslant 31$:

$$\mathcal{M}_n > 2^{2^{\frac{n-1}{2}}} \cdot 2^{2^{\frac{n-3}{4}}}. \tag{1}$$

С помощью приведённой в [16] классификации всех одиннадцати неэквивалентных разбиений длины 7 легко подсчитать число различных разбиений $\mathbb{F}^7$ на совершенные коды длины 7:

$$\mathcal{M}_7 = 27360 > 1.66 \cdot 2^{14}. \tag{2}$$

С использованием этих разбиений и конструкции из [2] в [4] показано, что

$$\mathcal{M}_{15} \geqslant 2^{147}. \tag{3}$$

Следовательно, с учётом (2) оценка (1) верна для любого $n \geqslant 7$.

Напомним, что нижняя оценка числа различных совершенных двоичных кодов, полученная в [14], является лучшей на сегодняшний день. Ниже приведены первые три сомножителя этой оценки:

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

здесь и далее log обозначает логарифм по основанию 2. Следует отметить, что (4) совпадает с нижней оценкой числа различных совершенных двоичных кодов, полученной в [6]. В [8] предложены конструкции разбиений пространства $\mathbb{F}^n$ на транзитивные коды, которые в дальнейшем развиты в [9] для построения 2-транзитивных и вершинно-транзитивных разбиений пространства $\mathbb{F}^n$ на совершенные двоичные коды. В [2] представлена конструкция разбиений пространства $\mathbb{F}^n$ на попарно не эквивалентные коды, а в [13] построен широкий класс разбиений на непараллельные коды Хэмминга. В [12] предложена каскадная конструкция разбиений и исследованы матрицы пересечений разбиений. В [10] предложено две конструкции разбиений множества всех $q$-значных векторов длины $n$ над $GF(q)$ на совершенные $q$-значные коды и приведена нижняя оценка числа различных разбиений на такие коды.

Заметим, что отдельное рассмотрение нижней оценки числа различных разбиений пространства $\mathbb{F}^N$, $N = n + 1$, на расширенные коды не имеет смысла, так как для перехода к этому случаю можно воспользоваться тем фактом, что преобразования, описанные конструкцией, рассматриваемой в работе, для разбиений на совершенные двоичные коды, могут быть применены к чётновесовым и нечётновесовым кодам независимо, т. е. если известна нижняя оценка числа различных разбиений пространства $\mathbb{F}^n$ на совершенные коды, то из неё легко получить нижнюю оценку числа различных разбиений пространства $\mathbb{F}^N$ на расширенные совершенные коды. Для этого достаточно оценку числа различных разбиений на совершенные коды длины $n$ возвести в квадрат. Очевидно, верно и обратное утверждение.

В [5] проведено дальнейшее исследование каскадного метода построения разбиений из [12]. Несмотря на то, что этот метод основан на конструкции совершенных двоичных кодов, дающей рекордную нижнюю оценку числа кодов ранга не больше $n - \log(n+1) + 2$, нижняя оценка числа различных разбиений пространства $\mathbb{F}^n$ на совершенные коды такого же ранга, полученная с его помощью, оказалась хуже чем (1) для $n > 15$. Но для $n = 15$ каскадный метод построения разбиений позволил получить следующую нижнюю оценку числа различных разбиений:

$$\mathcal{M}_{15} \geqslant 2^{120} \cdot 3^{48}, \tag{5}$$

что лучше оценок, найденных как с помощью конструкции Васильева, так и с помощью метода $ijk$-компонент.

В настоящей работе продолжается исследование свитчинговой конструкции $ijk$-компонент из [2] для построения разбиений пространства $\mathbb{F}^n$ на совершенные двоичные коды малого ранга (т. е. ранга не больше $n - \log(n+1)+2$). В разд. 1 приведены необходимые определения и понятия. Разд. 2 посвящён применению метода $ijk$-компонент для конструирования разбиений $\mathbb{F}^n$ на совершенные коды длины $n$. Этот метод позволил получить лучшую на сегодняшний день нижнюю оценку числа различных разбиений на совершенные двоичные коды малого ранга. Нетривиальные верхние оценки для числа разбиений на совершенные двоичные коды и для числа совершенных двоичных кодов пока не найдены.

## 1. Необходимые определения и понятия

*Расстояние Хэмминга* $d(x, y)$ между векторами $x$ и $y$ из $\mathbb{F}^n$ определяется как число координат, в которых различаются эти векторы. *Весом* вектора $x$ называется число $w(x) = d(x, 0^n)$, где $0^n$ — нулевой вектор длины $n$. *Двоичным кодом* называется произвольное подмножество $C$ из $\mathbb{F}^n$. Векторы пространства $\mathbb{F}^n$, принадлежащие $C$, называются кодовыми словами. *Совершенным двоичным кодом, исправляющим одиночные ошибки* (далее кратко *совершенным кодом*), называется такое подмножество $C$ из $\mathbb{F}^n$, что каждый вектор пространства $\mathbb{F}^n$ находится на расстоянии не больше 1 от некоторого единственного вектора из $C$. Хорошо известно, что такие коды существуют только при $n = 2^m - 1$, $m \geqslant 2$.

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

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

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 пространства $\mathbb{F}^n$ на коды называются *различными*, если найдутся два различных вектора из $\mathbb{F}^n$, принадлежащих одному коду первого разбиения и двум различным кодам второго разбиения. Далее будем говорить, что *разбиение имеет длину* $n$, если оно состоит из кодов длины $n$. Код длины $n$, содержащий $0^n$, называется *приведённым*.

*Рангом* приведённого кода $C$ называется размерность его линейной оболочки $r(C) = \dim(C)$. *Ранг разбиения* определим как наибольший из рангов всех приведённых кодов этого разбиения. Напомним, что ранг линейного совершенного кода длины $n$ — кода Хэмминга — равен $n - \log(n+1)$. Таким образом, ранг разбиения на коды Хэмминга (необязательно являющиеся классами смежности одного кода Хэмминга [13]) равен $n - \log(n+1)$. Очевидно, что ранг любого разбиения длины $n$ на совершенные коды, так же как и ранг произвольного совершенного кода длины $n$, варьируется от $n - \log(n+1)$ до $n$.

Пусть $C$ — произвольный совершенный код длины $n$, а $M$ — некоторое подмножество его кодовых слов. *Сдвигом множества* $M$ *в направлении* $i$, где $i \in \{1, 2, \ldots, n\}$, назовём множество $M' = M + e_i$, где $e_i$ — вектор веса 1 с единицей в $i$-й координате, т. е. $M'$ получено из $M$ инвертированием $i$-й координаты во всех его кодовых словах. Множество $M$ назовём *$i$-компонентой* совершенного кода $C$ длины $n$, если $C' = (C \setminus M) \cup (M + e_i)$ также является совершенным кодом длины $n$. Пусть $\alpha$ — произвольное подмножество множества $\{1, 2, \ldots, n\}$. Множество $M$ будем называть *$\alpha$-компонентой* кода $C$, если для любого элемента $i$ из $\alpha$ оно является $i$-компонентой $C$. Пусть $H$ — код Хэмминга длины $n$, через $R_i$ обозначим подпространство, порождённое совокупностью кодовых слов веса 3 кода $H$ с единичной $i$-й координатой. Через $R_{ij}$ обозначим подпространство, равное прямой сумме подпространств $R_i$ и $R_j$, а через $R_{ijk}$ — подпространство, равное прямой сумме подпространств $R_i$, $R_j$ и $R_k$. Если $e_i + e_k + e_k \in H$, то $R_{ij} = R_{ijk}$. Метод $ijk$-компонент предложен в [1].

## 2. Нижняя оценка числа разбиений на совершенные коды

Будучи применённым к коду Хэмминга, метод $ijk$-компонент позволяет строить богатые классы кодов, разбиений, а также выступает мощ-

ным инструментом для исследования свойств этих объектов [17]. В этом разделе покажем, что нижняя оценка (1) может быть значительно улучшена. Для этого приведём конструкцию разбиений пространства $\mathbb{F}^n$ на совершенные двоичные коды, основанную на методе $ijk$-компонент для построения совершенных кодов из [1]. Идея, лежащая в основе рассматриваемой конструкции, впервые предложена в [2] для построения разбиений на попарно не эквивалентные совершенные двоичные коды.

Изучим, какие многообразия разбиений можно получить, пользуясь методом из [2]. Пусть $P = \{H_0, \dots, H_n\}$ — разбиение пространства $\mathbb{F}^n$ на классы смежности кода Хэмминга $H$. Положим $H_0 = H + e_0$, где $e_0 = 0^n$, а $H_a = H + e_a$, $a = 0, \dots, n$, тогда $\mathbb{F}^n = \bigcup\limits_{a=0}^{n} (H + e_a)$.

В дальнейшем будем полагать, что $e_i + e_j + e_k \in H$. Классы смежности кода $H$ в разбиении $P$ перенумеруем аналогично [2], получим

$$\mathbb{F}^n = \bigcup_{l=0}^{\frac{n-3}{4}} (H_{4l} \cup (H_{4l} + e_i) \cup (H_{4l} + e_j) \cup (H_{4l} + e_k)).$$

Сделав замену $H_{4l} + e_p = H_{4l+p}$ для всех $p \in \{i, j, k\}$, сгруппируем коды разбиения в четвёрки $\{H_{4l}, H_{4l+i}, H_{4l+j}, H_{4l+k}\}$, $l = 0, 1, \dots, \frac{n-3}{4}$.

Разобьём код Хэмминга $H$ на $ijk$-компоненты. Согласно [1] в коде $H$ будет $N_2 = 2^{\frac{n+5}{4} - \log(n+1)}$ различных непересекающихся $ijk$-компонент. Каждую $ijk$-компоненту из $H$ можно разбить на $i$-, $j$- или $k$-компоненты. Согласно [1] их будет $N_1 = 2^{\frac{n-3}{4}}$. Аналогичные разбиения рассмотрим в каждом смежном классе по коду Хэмминга $H$. Все $ijk$-компоненты в коде $H$ пронумеруем индексами из $\{1, \dots, N_2\}$, а все $i$-компоненты ($j$- или $k$-компоненты) внутри каждой $ijk$-компоненты — индексами из $\{1, \dots, N_1\}$. Аналогично перенумеруем компоненты в остальных кодах разбиения. В результате каждый вектор $u$ из каждого кода разбиения будет иметь некоторую пару индексов $(r, s)$, $r \in \{1, \dots, N_2\}$, $s \in \{1, \dots, N_1\}$.

Рассмотрим следующие функции [1]:

$$\begin{aligned} &\sigma_l : \{1, \dots, N_2\} \times \{1, \dots, N_1\} \to \{0, 1\}, \\ &\xi_l : \{1, \dots, N_2\} \times \{1, \dots, N_1\} \to \{0, 1\}, \\ &\tau_l : \{1, \dots, N_2\} \to \{0, 1\}, \\ &\nu_l : \{1, \dots, N_2\} \to \{i, j, k\}, \end{aligned} \tag{6}$$

где $l = 0, 1, \dots, \frac{n-3}{4}$. Пусть $\pi = (i\, j\, k)$ — циклическая подстановка. Определим отображение $\varphi = (\sigma, \xi, \tau, \nu)$, где

$$\begin{aligned} &\sigma = (\sigma_0, \dots, \sigma_{\frac{n-3}{4}}), \quad \xi = (\xi_0, \dots, \xi_{\frac{n-3}{4}}), \\ &\tau = (\tau_0, \dots, \tau_{\frac{n-3}{4}}), \quad \nu = (\nu_0, \dots, \nu_{\frac{n-3}{4}}). \end{aligned} \tag{7}$$

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 $\sigma_l(t, s) \equiv \text{const}$ и $\xi_l(q, m) \equiv \text{const}$ для любых $s, m \in \{1, \ldots, N_1\}$. Отображение $\varphi$ будем называть *вырожденным*, если вырожденны все наборы $(\sigma_l, \xi_l, \tau_l, \nu_l)$. Разбиение, полученное с помощью $\varphi$ из разбиения $P$, будем обозначать через $\varphi(P)$.

Приведём описание конструкции. Каждой четвёрке $\{H_{4l}, H_{4l+i}, H_{4l+j}, H_{4l+k}\}$, $l = 0, 1, \ldots, \frac{n-3}{4}$, соответствует набор функций $(\sigma_l, \xi_l, \tau_l, \nu_l)$. Напомним, что каждый код из четвёрки можно разбить 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 $r$ — номер $ijk$-компоненты в коде $H_{4l}$.

Пусть $R_{ijk}$ — произвольная $ijk$-компонента кода $H_{4l}$. В зависимости от значения функции $\sigma_l(r, s)$ для каждой $i$-компоненты ($j$- или $k$-компоненты) из $R_{ijk}$ с индексом $s$ в $R_{ijk}$, где $r$ — 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 произвольной $i$-компоненты может быть осуществлён с соответствующей $i$-компонентой из $R_{ijk}+e_i$. Если $\nu_l(r) = j$, то свитчинг произвольной $j$-компоненты может быть выполнен с соответствующей $j$-компонентой из $R_{ijk} + e_j$. И, наконец, если $\nu_l(r) = k$, то свитчинг произвольной $k$-компоненты может быть произведён с соответствующей $k$-компонентой из $R_{ijk}+e_k$. Таким образом, всякий такой свитчинг в $R_{ijk}$ индуцирует также свитчинг в $ijk$-компоненте, определяемой направлением, по которому производится свитчинг в $R_{ijk}$. Легко подсчитать, что всего таких свитчингов будет $2^{N_1}$ в силу того, что в $R_{ijk}$ имеется $N_1$ компонент по направлению $i$ ($j$ или $k$).

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

Затем в зависимости от значения функции $\tau_l(r)$ либо производится свитчинг полученной $ijk$-компоненты по направлению $\pi(\nu_l(r))$ с $ijk$-компонентой с тем же индексом из соответствующего кода четвёрки, либо она не сдвигается. Для оставшейся пары $ijk$-компонент, чтобы среди ре-

зультирующих разбиений не было совпадений, это преобразование, в отличие от двух первых шагов, где операции были независимы, в точности дублируется.

Описанные для $R_{ijk}$ операции далее могут быть проделаны для остальных $ijk$-компонент из $H_{4l}$. В результате получаем $(2 \cdot 2)^{N_1 N_2} \cdot 2^{N_2}$ таких свитчингов.

**Лемма 1.** *Если невырожденные отображения* $\varphi' = (\sigma', \xi', \tau', \nu')$ *и* $\varphi'' = (\sigma'', \xi'', \tau'', \nu'')$ *различны, то разбиения* $\varphi'(P)$ *и* $\varphi''(P)$*, полученные в результате действий* $\varphi'$ *и* $\varphi''$ *на разбиение* $P$ *пространства* $\mathbb{F}^n$*, различны.*

Доказательство. Для доказательства различности результирующих разбиений покажем, что они отличаются по крайней мере в одной четвёрке кодов.

Пусть $\varphi'$ и $\varphi''$ различны. Без ограничения общности можем считать, что $\varphi' \neq \varphi''$ при $l = 0$. Рассмотрим первую четвёрку кодов из разбиения $P$ на классы смежности кода Хэмминга $H$: $\{H, H_i, H_j, H_k\}$.

Пусть $\nu'_0(r) \neq \nu''_0(r)$ для некоторого $r$. По определению конструкции $\varphi'$ и $\varphi''$ разобьют $ijk$-компоненту $R_{ijk}$ с индексом $r$ в коде $H$ на различные $\nu'_0(r)$- и $\nu''_0(r)$-компоненты соответственно (аналогичное разбиение будет произведено в остальных кодах четвёрки). Тогда в силу невырожденности $\varphi'$ и $\varphi''$ найдутся такие $s_1$ и $s_2$, что $\sigma''_0(r, s_1) = 0$ и $\sigma''_0(r, s_2) = 1$ или $\xi''_0(r, s_1) = 0$ и $\xi''_0(r, s_2) = 1$. Выбирая два кодовых слова в $R_{ijk}$ так, что они принадлежат одной $\nu'_0(r)$-компоненте с индексом $s$ в $R_{ijk}$, но двум разным $\nu''_0(r)$-компонентам с индексами $s_1$ и $s_2$ соответственно в $R_{ijk}$, получим, что после применения $\varphi'$ к разбиению $P$ эти слова будут принадлежать одному коду четвёрки первого разбиения $\varphi'(P)$, а после применения $\varphi''$ к разбиению $P$ — двум разным кодам. Следовательно, коды разбиений $\varphi'(P)$ и $\varphi''(P)$, полученные из исходной четвёрки $\{H, H_i, H_j, H_k\}$, будут различны, а потому и результирующие разбиения будут различны.

Пусть теперь $\nu'_0(r) \equiv \nu''_0(r)$. Поскольку $\varphi'$ и $\varphi''$ различны, найдётся такая пара индексов $(r, s)$, что

$$(\sigma'_0(r, s), \xi'_0(r, s), \tau'_0(r)) \neq (\sigma''_0(r, s), \xi''_0(r, s), \tau''_0(r)).$$

Рассмотрим случай, когда $\nu'_0(r) = \nu''_0(r) = k$ (случаи, когда $\nu'_0(r) = \nu''_0(r)$ равны $i$ или $j$, аналогичны). Найдём $ijk$-компоненту $R^u_{ijk}$ с индексом $r$ в коде $H$. Так как $\nu'_0(r) = \nu''_0(r) = k$, согласно конструкции $R^u_{ijk}$ разбивается на $k$-компоненты. Рассмотрим кодовое слово $u \in R^u_{ijk} \subset H$,

принадлежащее $k$-компоненте из $R^u_{ijk}$. Пусть $s$ — её индекс в $R^u_{ijk}$. Тогда $u + e_i \in H_i = H + e_i$, $u + e_k \in H_k = H + e_k$ и $u + e_j \in H_j = H + e_j$. Рассмотрим все значения, которые могут принимать функции $\sigma_0, \xi_0$ и $\tau_0$ из (6) для пары индексов $(r, s)$. Для этой цели рассмотрим таблицу, где в первом столбце содержатся все возможные значения вектора $(\sigma_0(r,s), \xi_0(r,s), \tau_0(r))$, а во втором — упорядоченные четвёрки элементов из множества $\{0, i, j, k\}$, обозначающие индексы кодов четвёрки $\{H, H_i, H_j, H_k\}$, в которых слова $u$, $u + e_i$, $u + e_k$ и $u + e_j$ окажутся под действием функций $\sigma_0, \xi_0, \tau_0$ (напомним, что $H = H_0$).

$$
\begin{array}{cc}
(\sigma_0(r,s), \xi_0(r,s), \tau_0(r)) & \\
(0,0,0) & (0,i,k,j) \\
(0,0,1) & (i,0,j,k) \\
(0,1,0) & (0,j,k,i) \\
(0,1,1) & (i,k,j,0) \\
(1,1,1) & (j,k,i,0) \\
(1,1,0) & (k,j,0,i) \\
(1,0,0) & (k,i,0,j) \\
(1,0,1) & (j,0,i,k)
\end{array}
\tag{8}
$$

Как видно из (8), упорядоченные четвёрки индексов в правом столбце попарно различны. Следовательно, четыре кодовых слова $u$, $u+e_i$, $u+e_k$ и $u+e_j$ под действием различных невырожденных отображений $\varphi'$ и $\varphi''$ окажутся в разных четвёрках кодов. А значит, четвёрки кодов, получаемые из $\{H, H_i, H_j, H_k\}$ в результате преобразований $\varphi'$ и $\varphi''$, различны, и никакой перенумерацией кодов разбиений $\varphi'(P)$ и $\varphi''(P)$ в силу невырожденности преобразований $\varphi'$ и $\varphi''$ нельзя добиться их совпадения. Отсюда заключаем, что разбиения $\varphi'(P)$ и $\varphi''(P)$ различны.

Так как все возможные случаи для двух различных невырожденных преобразований $\varphi'$ и $\varphi''$ исчерпываются рассмотренными выше, лемма 1 доказана.

Используя лемму 1, подсчитаем число $\mathcal{M}_n$ различных разбиений длины $n$. Для этой цели найдём число различных наборов $(\sigma_l, \xi_l, \tau_l, \nu_l)$. Нетрудно видеть, что значения функций $\sigma_l$ и $\xi_l$ можно задать $2^{N_1 N_2}$ способами для каждой из них, а значения функций $\tau_l$ и $\nu_l$ — $2^{N_2}$ и $3^{N_2}$ способами соответственно. По определению конструкции каждая из четырёх функций задаётся независимо, тем самым число различных наборов $(\sigma_l, \xi_l, \tau_l, \nu_l)$ будет равно $(2 \cdot 2)^{N_1 N_2} \cdot (2 \cdot 3)^{N_2}$. Так как в каждой четвёрке кодов преобразования производятся независимо, получаем не менее $(4^{N_1 N_2} \cdot 6^{N_2})^{\frac{n+1}{4}} = 2^{2^{\frac{n-1}{2}}} \cdot 6^{2^{\frac{n-3}{4}}}$ различных отображений $\varphi$.

Найдём верхнюю оценку числа вырожденных преобразований. По определению отображения $\varphi$ параметры $t$ и $q$ можно выбрать $N_2$ способами. Значения функций $\sigma(t,s)$ и $\xi(q,m)$ можно выбрать двумя способами для каждой, т. е. равными 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 $\varphi$ не превосходит

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

Оно является бесконечно малой величиной по сравнению с $(4^{N_1 N_2} \cdot 6^{N_2})^{\frac{n+1}{4}}$ (числом различных отображений $\varphi$ для достаточно большого $n$) и может быть компенсировано произволом выбора кодового слова $e_i + e_j + e_k$ в коде Хэмминга $H$. Таким образом, с учётом оценки (2) справедлива

**Теорема 1.** *Число $\mathcal{M}_n$ различных разбиений пространства $\mathbb{F}^n$ на совершенные коды длины $n$ удовлетворяет нижней оценке*

$$\mathcal{M}_n \geqslant 2^{2^{\frac{n-1}{2}}} \cdot 6^{2^{\frac{n-3}{4}}} \tag{9}$$

*для любого допустимого $n \geqslant 7$.*

Сравнение нижних оценок (1) и (9) для числа различных разбиений длины $n$ (обратим внимание на совпадение первых множителей), а также анализ всех известных нижних оценок числа различных совершенных кодов длины $n$ (см. [14, 17]) позволяют предположить, что первый множитель $2^{2^{\frac{n-1}{2}}}$ в нижней оценке числа различных разбиений пространства $\mathbb{F}^n$ на совершенные коды длины $n$ неулучшаем.

Напомним, что разбиения длины $n \geqslant 15$, полученные с помощью конструкции разбиений, основанной на конструкции Васильева, из кодов Хэмминга длины $(n-1)/2$, имеют ранг не больше $n - \log(n+1) + 1$. В свою очередь, разбиения, построенные с помощью метода $ijk$-компонент, описанного в данном разделе, имеют ранг не больше $n - \log(n+1) + 2$ для любой допустимой длины $n$. Это объясняется тем, что построение начинается с разбиения пространства $\mathbb{F}^n$ на классы смежности кода Хэмминга, а новые разбиения получаются из него свитчингами по трём направлениям $i$, $j$ и $k$, два из которых линейно независимы.

Следует отметить, что даже для разбиения на коды Хэмминга размерность линейной оболочки объединения всех приведённых кодов разбиения может быть равна $n$. Так, например, нетрудно проверить, что из одиннадцати неэквивалентных разбиений на коды Хэмминга длины 7 из [16] у трёх разбиений размерность линейной оболочки объединения

всех приведённых кодов равна 7, у пяти она равна 6, у двух равна 5 и у одного разбиения равна 4. Данный факт позволяет заключить, что класс разбиений, получаемых с помощью конструкции, основанной на конструкции Васильева (при $n = 15$ см. [2, 4, 7]), не совпадает с классом разбиений, получаемых с помощью каскадной конструкции [5] и изложенного выше метода. Также следует отметить, что размерность линейной оболочки объединения всех приведённых кодов разбиений, получаемых с помощью конструкции, основанной на конструкции Васильева, может расти с ростом итераций метода.

Отметим, что уже начиная с $n = 31$ метод $ijk$-компонент позволяет строить более богатые по мощности классы различных разбиений. При длине разбиения $n = 15$ нижние оценки числа различных разбиений, которые позволяют получить конструкция Васильева [4], метод $ijk$-компонент и каскадный метод [5], равны $2^{136} \cdot 3^6 < 2^{147} < 2^{136} \cdot 3^7$, $2^{136} \cdot 3^8$ и $2^{136} \cdot 3^{37} < 2^{120} \cdot 3^{48} < 2^{136} \cdot 3^{38}$ соответственно, см. также (3) и (5).

То, что в данном случае конструкция $ijk$-компонент уступает каскадному методу и не позволяет получить рекордных оценок на малых длинах, объясняется тем, что она основывается на разбиении на классы смежности линейного кода (кода Хэмминга) той же длины.

Автор выражает благодарность Ф. И. Соловьёвой, под руководством которой написана эта статья, и С. В. Августиновичу за полезные дискуссии.

## ЛИТЕРАТУРА

1. **Августинович С. В., Соловьёва Ф. И.** Построение совершенных двоичных кодов последовательными сдвигами $\alpha$-компонент // Пробл. передачи информ. — 1997. — Т. 33, № 3. — С. 15–21.
2. **Августинович С. В., Соловьёва Ф. И., Хеден У.** О разбиениях $n$-куба на неэквивалентные совершенные коды // Пробл. передачи информ. — 2007. — Т. 43, № 4. — С. 45–50.
3. **Васильев Ю. Л.** О негрупповых плотно упакованных кодах // Пробл. кибернетики. — 1962. — № 8. — С. 337–339.
4. **Гуськов Г. К.** О числе различных разбиений куба $E^{15}$ на совершенные двоичные коды // Мат. 47 междунар. науч. студ. конф. «Студент и научно-технический прогресс». — Новосибирск: Новосиб. гос. ун-т, 2009. — С. 160.
5. **Гуськов Г. К., Соловьёва Ф. И.** Об одной каскадной конструкции разбиений $n$-куба на совершенные двоичные коды // Тр. междунар. конф. «Информационные технологии и системы» (Россия, Петрозаводск, 19–25 августа 2012 г.). — М: ИППИ РАН, 2012. — С. 124–128.

6. **Кротов Д. С.** Нижние оценки числа $m$-квазигрупп порядка 4 и числа совершенных двоичных кодов // Дискрет. анализ и исслед. операций. — 2000. — Т. 7, № 2. — С. 47–53.
7. **Соловьёва Ф. И.** О двоичных негрупповых кодах // Методы дискретного анализа в изучении булевых функций и графов. — Новосибирск: Ин-т математики СО РАН, 1981. — № 37. — С. 65–76.
8. **Соловьёва Ф. И.** О транзитивных разбиениях $n$-куба на коды // Пробл. передачи информ. — 2008. — Т. 44, № 4. — С. 27–35.
9. **Соловьёва Ф. И., Гуськов Г. К.** О построении вершинно-транзитивных разбиений $n$-куба на совершенные коды // Дискрет. анализ и исслед. операций. — 2010. — Т. 17, № 3. — С. 84–100.
10. **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.
11. **Фон-Дер-Флаасс Д. Г.** Совершенные 2-раскраски гиперкуба // Сиб. мат. журн. — 2007. — Т. 48, № 4. — С. 923–930.
12. **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.
13. **Heden O., Solov'eva F. I.** Partitions of $\mathbb{F}^n$ into nonparallel Hamming codes // Adv. Math. Commun. — 2009. — Vol. 3, N 4. — P. 385–397.
14. **Krotov D. S., Avgustinovich S. V.** On the number of 1-perfect binary codes: a lower bound // IEEE Trans. Inf. Theory. — 2008. — Vol. 54, N 4. — P. 1760–1765.
15. **Östergård P. R. J.** On a hypercube coloring problem // J. Comb. Theory. Ser. A. — 2004. — Vol. 108, N 2. — P. 199–204.
16. **Phelps K. T.** An enumeration of 1-perfect binary codes // Australas. J. Comb. — 2000. — Vol. 21. — P. 287–298.
17. **Solov'eva F. I.** On perfect codes and related topics // *Com*$^2$*Mac* Lect. Notes Ser.13. — Pohang, Korea: Pohang Univ. Sci. Tech., 2004. — 80 p.


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

Статья поступила
27 апреля 2012 г.

Переработанный вариант —
4 февраля 2013 г.