S©MR ISSN 1813-3304

СИБИРСКИЕ ЭЛЕКТРОННЫЕ
МАТЕМАТИЧЕСКИЕ ИЗВЕСТИЯ

Siberian Electronic Mathematical Reports
http://semr.math.nsc.ru

Том 8, стр. 372–380 (2011) УДК 512.5
MSC 13A99

О ПОСТРОЕНИИ РАЗБИЕНИЙ $(p+1)$-МЕРНОГО ПРОСТРАНСТВА ВСЕХ P-ЗНАЧНЫХ ВЕКТОРОВ НА КОДЫ ХЭММИНГА

А. В. Лось, К. И. Бурнаков

Abstract. We suggest the construction of a partition of the set of all p-ary vectors of length $p+1$ into perfect p-ary codes, where p is a prime. The construction yields the lower bound $N(p) > (e^{\pi\sqrt{2p/3}})/(4p\sqrt{3})$ on the number of nonequivalent such partitions for any prime p.

Keywords: perfect q-ary code, Hamming code, partition into codes, switchings.

1. Введение

Через $\mathbb{F}_q^n$ обозначим n-мерное метрическое пространство над полем Галуа $GF(q)$, где $q = p^r$, p — простое число, по отношению к метрике Хэмминга. В настоящей работе для любого простого числа p предложена конструкция разбиения $(p+1)$-мерного пространства всех p-значных векторов на совершенные коды. Найдена нижняя оценка числа неэквивалентных таких разбиений.

Задача построения и изучения свойств новых разбиений n-мерных векторных пространств над $GF(q)$ на совершенные коды тесно связана с классической проблемой перечисления всех совершенных кодов над конечными полями. Новые конструкции разбиений могут быть полезны для построения новых классов q-значных кодов и, в частности, совершенных. В книге [11], гл. 11, приведено описание ряда различных конструкций совершенных q-значных кодов, в основе которых лежат разбиения пространства $\mathbb{F}_q^n$ на совершенные коды.

Los, A.V., Burnakov, K.I., Construction of partitions of the set of all p-ary vectors of length p+1 into Hamming codes.

Работа выполнена при частичной финансовой поддержке Российского фонда фундаментальных исследований (проект 10-01-00424-а).

Поступила 18 ноября 2011 г., опубликована 24 декабря 2011 г.

Следует отметить, что существуют работы, посвященные построению разбиений пространства $\mathbb{F}_q^n$ на совершенные коды для произвольных допустимых $n = (q^m - 1)/(q - 1)$ и $q = p^r$, где p — простое, а m и r — целые числа (см., например, [6, 7]). Отдельно и более глубоко исследован двоичный случай (см. [14, 2]). В работе [9] предложены конструкции разбиений пространства $\mathbb{F}_2^n$ на смежные классы попарно различных двоичных кодов Хэмминга. Для кодов малой размерности выполнена классификация разбиений пространства $\mathbb{F}_2^7$ на совершенные коды длины 7 и пространства $\mathbb{F}_2^8$ на расширенные коды длины 8. Всего построено 11 неэквивалентных разбиений пространства $\mathbb{F}_2^7$ и 10 неэквивалентных разбиений пространства $\mathbb{F}_2^8$, см. [13].

Напомним некоторые необходимые определения. Произвольное подмножество C пространства $\mathbb{F}_q^n$ называется *совершенным q-значным кодом длины n с кодовым расстоянием 3* (далее кратко *совершенным кодом*), если для любого вектора $x \in \mathbb{F}_q^n$ существует единственное кодовое слово y из кода C такое, что расстояние Хэмминга $d(x, y)$ между ними удовлетворяет $d(x, y) \leq 1$. Хорошо известно, что такие коды существуют только для $n = (q^m - 1)/(q - 1)$, $m \geq 2$, см. [3, 4, 15]. Код называется *линейным*, если он образует линейное подпространство в пространстве $\mathbb{F}_q^n$. Совершенный линейный код называется *кодом Хэмминга*. Далее код Хэмминга длины n над полем $GF(q)$ будем обозначать через $\mathcal{H}$, напомним, что размерность такого кода равна $n - m$, где $n = (q^m - 1)/(q - 1)$.

Разбиением пространства на совершенные коды называется множество непересекающихся кодов, объединение которых совпадает с этим пространством. *Изометрия* — это преобразование метрического пространства, сохраняющее расстояние между любыми двумя его элементами. Два разбиения пространства $\mathbb{F}_q^n$ на совершенные коды называются эквивалентными, если существует такая изометрия пространства $\mathbb{F}_q^n$, что все коды первого разбиения под действием данного автоморфизма перейдут в коды второго. А. А. Марков в 1956 году показал [8], что группа изометрий пространства $\mathbb{F}_q^n$ представляет собой полупрямое произведение

$$\mathrm{Aut}(\mathbb{F}_q^n) = S_n \leftthreetimes S_q^n = \left\{(\pi, \sigma) | \pi \in S_n, \sigma \in S_q^n\right\}.$$

Иначе говоря, изометрия пространства $\mathbb{F}_q^n$ представима в виде пары преобразований (π, σ), где подстановка $\pi \in S_n$ переставляет координаты вектора $x \in \mathbb{F}_q^n$, в то время как σ является *конфигурацией* длины n, состоящей из набора n перестановок элементов поля $GF(q)$, то есть $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$, где $\sigma_i \in S_q$, $i \in \{1, 2, \ldots, n\}$.

2. Конструкция разбиений

Перед описанием конструкции класса нетривиальных разбиений пространства $\mathbb{F}_p^n$ на совершенные p-значные коды, где p — простое, а размерность пространства $n = p + 1$, докажем ряд утверждений характеризующих такие разбиения.

Рассмотрим произвольное разбиение пространства $\mathbb{F}_p^{p+1}$ на совершенные p-значные коды. Нетрудно проверить следующее

Лемма 1. *Разбиение пространства всех p-значных векторов длины $n = p+1$ состоит из p^2 совершенных кодов с кодовым расстоянием 3.*

Доказательство. Рассмотрим пространство над полем $GF(p)$ размерности $n = \frac{p^m-1}{p-1}$, где $m = 2$. Поскольку совершенный линейный код в таком пространстве имеет размерность $n-m = p-1$, то из мощностных соображений получаем, что число совершенных кодов, составляющих разбиение такого пространства, равно p^2. $\square$

Поскольку вопрос о существовании совершенных p-значных кодов длины $n = p+1$, неэквивалентных кодам Хэмминга, остается открытым, то для конструирования разбиений будем рассматривать только коды Хэмминга и коды эквивалентные им. Два кода называются *эквивалентными*, если существуют изометрии пространства $\mathbb{F}_p^n$, отображающие эти коды друг в друга.

Разбиение пространства $\mathbb{F}_p^n$ всех p-значных векторов длины n на классы смежности кода Хэмминга назовем *тривиальным*. Несложно показать, что

Лемма 2. *Если классы смежности двух кодов Хэмминга составляют некоторое нетривиальное разбиение пространства $\mathbb{F}_p^{p+1}$ на совершенные коды, то мощность пересечения этих кодов Хэмминга равна p^{p-2}.*

Доказательство. Рассмотрим два произвольных p-значных кода Хэмминга $\mathcal{H}_1$ и $\mathcal{H}_2$ длины $n = p+1$. Обозначим размерность пересечения этих кодов через k: $k = dim(\mathcal{H}_1 \cap \mathcal{H}_2)$. Поскольку проверочные матрицы этих кодов H_1 и H_2 состоят из двух строк, то проверочная матрица их пересечения

$$H = \left[\frac{H_1}{H_2}\right],$$

состоящая из объединения строк матриц H_1 и H_2, имеет 4 строки. Тогда $rank(H) \in \{2,3,4\}$, то есть $k \in \{p-1, p-2, p-3\}$.

Рассмотрим все возможные значения для k.

При $k = p-1$ размерность пересечения кодов совпадает с размерностью самих кодов. Данная ситуация имеет место в том случае, когда разбиение состоит из классов смежности только одного кода Хэмминга.

Пусть $k = p-3$. Рассмотрим разложение кода $\mathcal{H}_1$ на классы смежности по пересечению исходных кодов $\mathcal{H}_1 \cap \mathcal{H}_2$, число таких классов смежности равно

$$\frac{|\mathcal{H}_1|}{|\mathcal{H}_1 \cap \mathcal{H}_2|} = \frac{p^{p-1}}{p^{p-3}} = p^2.$$

Таким образом, код Хэмминга $\mathcal{H}_1$ будет пересекаться с p^2 классами смежности кода $\mathcal{H}_2$. Но, согласно лемме 1, разбиение пространства $\mathbb{F}_p^{p+1}$ состоит из p^2 совершенных кодов. Тогда любой класс смежности кода $\mathcal{H}_2$, составляющий некоторое разбиение будет пересекаться с кодом $\mathcal{H}_1$. Следовательно, коды Хэмминга с пересечением мощности p^{p-3} ра́вно как и их классы смежности не могут составлять одно разбиение пространства $\mathbb{F}_p^{p+1}$ на коды.

В случае, когда $k = p-2$ код $\mathcal{H}_1$ можно разложить на

$$\frac{|\mathcal{H}_1|}{|\mathcal{H}_1 \cap \mathcal{H}_2|} = \frac{p^{p-1}}{p^{p-2}} = p$$

классов смежности пересечения $\mathcal{H}_1 \cap \mathcal{H}_2$. Тогда код $\mathcal{H}_1$ пересекает некоторые p классов смежности кода $\mathcal{H}_2$, составляющих тривиальное разбиение пространства $\mathbb{F}_p^{p+1}$. Объединение U этих p классов смежности кода $\mathcal{H}_2$ совпадает с объединением некоторых p классов смежности кода $\mathcal{H}_1$, и тогда тривиальное разбиение пространства $\mathbb{F}_p^{p+1}$ на классы смежности кода $\mathcal{H}_2$ позволяет заменить

коды, составляющие объединение U на p некоторых классов смежности кода $\mathcal{H}_1$, что в результате дает разбиение отличное от тривиального. $\square$

Отметим, что в доказательстве леммы 2 в случае при $k = p-2$ рассмотрен пример построения нового разбиения пространства на коды с помощью замены части кодов исходного тривиального разбиения на другие коды, имеющие такое же объединение что и заменяемые. Данный способ построения является методом свитчинга, в котором один комбинаторный объект получается из другого при помощи замены части исходного объекта на новую с сохранением некоторых свойств. Чаще всего данный метод применяется при построении новых совершенных кодов с помощью свитчингов компонент кода Хэмминга, см. [1, 5].

Рассмотрим подробнее подобные преобразования тривиального разбиения пространства $\mathbb{F}_p^{p+1}$ на классы смежности кодов Хэмминга. Пусть коды $\mathcal{H}_1$ и $\mathcal{H}_2$ пересекаются по p^{p-2} кодовым словам. Рассмотрим объединение p классов смежности кода $\mathcal{H}_2$, пересекающихся с кодом $\mathcal{H}_1$, как и ранее обозначим его через U. Нетрудно показать, что объединение U является линейным кодом размерности p. Кроме того, очевидно, что существуют p некоторых классов смежности кода $\mathcal{H}_1$, объединение которых совпадает с U. Используя данное совпадение мы вправе осуществить свитчинг в тривиальном разбиении пространства $\mathbb{F}_p^{p+1}$ на классы смежности кода $\mathcal{H}_2$, заменяя коды, составляющие объединение U, на выбранные классы смежности кода $\mathcal{H}_1$. Более того, подобные свитчинги правомерны и для любого класса смежности объединения U, поскольку для каждого класса смежности U также найдутся p подходящих классов смежности кода $\mathcal{H}_1$.

Если представить разбиение пространства $\mathbb{F}_p^{p+1}$ в виде объединения кодов, составляющих его, то последние размышления можно записать следующим образом:

$$\mathbb{F}_p^{p+1} = \bigcup_{i=1}^{p} U_i, \tag{1}$$

где U_i — i-ый смежный класс подпространства U и $U_1 = U$. В свою очередь, множество U_i является объединением некоторых смежных классов $\mathcal{H}_{t_i}^{ij}$ кода $\mathcal{H}_{t_i}$, здесь $t_i \in \{1, 2\}$, $i \in \{1, 2, \ldots, p\}$, то есть

$$U_i = \bigcup_{j=1}^{p} \mathcal{H}_{t_i}^{ij}.$$

Следующее утверждение призвано обозначить какое количество кодов Хэмминга может составлять одно разбиение пространства $\mathbb{F}_p^{p+1}$.

Лемма 3. *Существует разбиение пространства $\mathbb{F}_p^{p+1}$, состоящее из k классов смежности различных p-значных кодов Хэмминга длины $p+1$, где $k \in \{2, \ldots, p-1\}$.*

Доказательство. Рассмотрим два кода Хэмминга $\mathcal{H}_1$ и $\mathcal{H}_2$, классы смежности которых составляют нетривиальное разбиение пространства $\mathbb{F}_p^{p+1}$. Обозначим порождающие матрицы рассматриваемых кодов через G_1 и G_2 соответственно. Не теряя общности, положим, что порождающая матрица кода $\mathcal{H}_1$

задана в каноническом виде и имеет вид:

$$G_1 = \left(\begin{array}{cccc|c|cc} 1 & & & 0 & 0 & p-1 & p-1 \\ & 1 & & & 0 & p-1 & p-2 \\ & & \ddots & & \vdots & \vdots & \vdots \\ 0 & & & 1 & 0 & p-1 & 2 \\ \hline 0 & 0 & \cdots & 0 & 1 & p-1 & 1 \end{array}\right).$$

Согласно лемме 2, размерность пересечения кодов $\mathcal{H}_1$ и $\mathcal{H}_2$ равна $p-2$, тогда, не теряя общности, можно предположить, что эти коды пересекаются по подпространству, порождённому первыми $p-2$ строками порождающей матрицы G_1. Следовательно, порождающая матрица кода $\mathcal{H}_2$ может быть задана в следующем каноническом виде:

$$G_2 = \left(\begin{array}{cccc|c|cc} 1 & & & 0 & 0 & p-1 & p-1 \\ & 1 & & & 0 & p-1 & p-2 \\ & & \ddots & & \vdots & \vdots & \vdots \\ 0 & & & 1 & 0 & p-1 & 2 \\ \hline 0 & 0 & \cdots & 0 & 1 & \alpha & \beta \end{array}\right),$$

где α и β — некоторые ненулевые элементы поля $GF(p)$ не равные $p-1$ и 1 соответственно.

Рассмотрим порождающую матрицу G_2. Поскольку она порождает код Хэмминга с кодовым расстоянием 3, то вектор, полученный произведением последней строки матрицы G_2 на произвольный ненулевой элемент поля, должен быть удален от остальных строк матрицы по крайней мере на расстояние 3. Обозначим последнюю строку матрицы G_2 через c_2 и рассмотрим следующий вектор:

$$\frac{p-1}{\alpha} \cdot c_2 = \frac{p-1}{\alpha} \cdot (0, \ldots, 0, 1, \alpha, \beta) = \left(0, \ldots, 0, \frac{p-1}{\alpha}, p-1, \frac{(p-1)\beta}{\alpha}\right).$$

Для того чтобы полученный вектор принадлежал коду $\mathcal{H}_2$ необходимо, чтобы его последняя координата была равна 1. Тогда получаем, что $\beta = \alpha/(p-1)$ и

$$G_2 = \left(\begin{array}{cccc|c|cc} 1 & & & 0 & 0 & p-1 & p-1 \\ & 1 & & & 0 & p-1 & p-2 \\ & & \ddots & & \vdots & \vdots & \vdots \\ 0 & & & 1 & 0 & p-1 & 2 \\ \hline 0 & 0 & \cdots & 0 & 1 & \alpha & \frac{\alpha}{p-1} \end{array}\right), \tag{2}$$

где $\alpha \neq p-1$. Таким образом, произвольная пара кодов Хэмминга с порождающими матрицами заданного выше вида (2) могут составлять разбиение (1), а поскольку в кодовом слове c_2 фигурирует произвольный ненулевой элемент поля $\alpha \in GF^*(p)$, то такая пара кодов Хэмминга может быть выбрана среди $p-1$ различных кодов Хэмминга.

Покажем, что разбиение (1) может состоять из классов смежности произвольного кода Хэмминга с порождающей матрицей вида (2). Для этого рассмотрим три кода Хэмминга с порождающими матрицами определенного выше вида, последние строки которых равны

$$c_1 = \left(0, \ldots, 0, 1, \alpha, \frac{\alpha}{p-1}\right),$$

$$c_2 = \left(0, \ldots, 0, 1, \beta, \frac{\beta}{p-1}\right),$$

$$c_3 = \left(0, \ldots, 0, 1, \gamma, \frac{\gamma}{p-1}\right)$$

соответственно, где α, β и γ различные ненулевые элементы поля $GF(p)$. Очевидно, что ранг матрицы, состоящей из строк c_1, c_2 и c_3, равен 2. Следовательно, объединение любой пары из рассматриваемых кодов порождает одно и то же подпространство U. Таким образом, объединение любой пары кодов Хэмминга с порождающими матрицами вида (2) порождает одно и то же подпространство U. Это означает, что каждый класс смежности подпространства U может быть представлен в виде объединения классов смежности одного из $p-1$ кодов Хэмминга с порождающей матрицей заданного вида (2).

Остается показать, что смежные классы кодов Хэмминга, не имеющих порождающих матриц вида (2), не могут составлять одно разбиение пространства $\mathbb{F}_p^{p+1}$ вместе с кодами $\mathcal{H}_1$ и $\mathcal{H}_2$ одновременно. Не теряя общности, рассмотрим код Хэмминга $\mathcal{H}_3$, порождающая матрица которого может быть задана в следующем виде:

$$G_3 = \left(\begin{array}{cccc|c|cc} 1 & & & 0 & 0 & p-1 & p-1 \\ & 1 & & & 0 & p-1 & p-2 \\ & & \ddots & & \vdots & \vdots & \vdots \\ 0 & & & 1 & 0 & \delta & \frac{2\delta}{p-1} \\ \hline 0 & 0 & \cdots & 0 & 1 & p-1 & 1 \end{array}\right),$$

где δ — ненулевой элемент поля $GF(p)$ не равный $p-1$. Легко видеть, что размерность пересечения данного кода с кодом $\mathcal{H}_1$ также равна $p-2$, что удовлетворяет требованию леммы 2 и позволяет использовать смежные классы кода $\mathcal{H}_3$ в одном разбиении вместе со смежными классами кода $\mathcal{H}_1$. Теперь проверим возможность составления одного разбиения со смежными классами кода $\mathcal{H}_2$. Рассмотрим подпространство, порожденное объединением матриц G_2 и G_3. Оно совпадает с пространством $\mathbb{F}_p^{p+1}$. А поскольку размерность линейной оболочки двух подпространств равна сумме размерностей этих подпространств минус размерность их пересечения, то размерность пересечения кодов, порожденных матрицами G_2 и G_3, равна $p-3$, что противоречит условию леммы 2. Следовательно, смежные классы кодов $\mathcal{H}_2$ и $\mathcal{H}_3$ не могут составлять одно разбиение. $\square$

Рассмотрим семейство, состоящее из $p-1$ кодов Хэмминга длины $p+1$, у которых найдутся порождающие матрицы, отличающиеся только в одной строке, обозначим его $\mathcal{P}$. По лемме 3 классы смежности таких кодов могут составлять одно разбиение. Линейная оболочка объединения таких кодов Хэмминга как множеств векторов является некоторым подпространством $U \subseteq \mathbb{F}_p^{p+1}$ размерности p. А значит произвольный класс смежности подпространства U может быть представлен в виде объединения классов смежности любого кода Хэмминга из семейства $\mathcal{P}$.

Пусть $\mathcal{H}_1$, $\mathcal{H}_2$, …, $\mathcal{H}_{p-1}$ — коды Хэмминга одного семейства $\mathcal{P}$. Обозначим i-ый смежный класс подпространства U через U_i, где $U_1 = U$, а через $\mathcal{H}_{t_i}^{ij}$ —

смежные классы кода Хэмминга $\mathcal{H}_{t_i}$, $t_i \in \{1, 2, \ldots, p-1\}$, объединение которых

$$\bigcup_{j=1}^{p} \mathcal{H}_{t_i}^{ij}$$

совпадает с U_i.

Теорема 1. *Коды, входящие в объединение*

$$\bigcup_{i=1}^{p} \bigcup_{j=1}^{p} \mathcal{H}_{t_i}^{ij}$$

составляют разбиение пространства $\mathbb{F}_p^{p+1}$ на совершенные p-значные коды длины $p+1$, где $\mathcal{H}_{t_i}^{ij}$ — некоторый смежный класс кода Хэмминга $\mathcal{H}_{t_i}$.

Доказательство. Доказательство непосредственно следует из леммы 1 и леммы 3, а также из того факта, что все задействованные в разбиении классы смежности кодов Хэмминга не пересекаются между собой. □

3. Нижняя оценка числа неэквивалентных разбиений

Рассмотрим произвольное разбиение пространства $\mathbb{F}_p^{p+1}$ на совершенные коды, построенное с помощью описанной выше конструкции. Согласно утверждению 3 такое разбиение состоит из классов смежности не более чем $p-1$ различных кодов Хэмминга, тогда разбиение может характеризовать вектор длины $p-1$, компоненты которого соответствуют количеству подмножеств U_i разбиения (1), составленных из классов смежности одного кода Хэмминга. Очевидно, что сумма компонент этого вектора соответствует числу подмножеств U_i разбиения (1), то есть равна p. Назовем описанный вектор *спектром разбиения*. Очевидно, что спектр тривиального разбиения содержит одну ненулевую компоненту, равную p. Отметим, что в нашем случае у понятия спектр разбиения порядок следования его компонент не является существенным, то есть будем считать, что два спектра совпадают, если существует перестановка компонент первого спектра, переводящая его во второй.

Используя конструкцию разбиений, заданную теоремой 1, можно оценить снизу число неэквивалентных разбиений.

Лемма 4. *Если спектры двух разбиений содержат различные значения, то такие разбиения неэквивалентны.*

Доказательство. Рассмотрим два разбиения пространства $\mathbb{F}_p^{p+1}$ с различными спектрами. Предположим, что одно разбиение под действием некоторого автоморфизма $(\pi, \sigma) \in Aut(\mathbb{F}_p^{p+1})$ перешло в другое. Тогда в первом разбиении найдутся классы смежности кода Хэмминга, которые под действием автоморфизма (π, σ) перейдут в классы смежности двух или более различных кодов Хэмминга.

Рассмотрим два класса смежности $\mathcal{H}_1'$ и $\mathcal{H}_1''$ некоторого кода Хэмминга $\mathcal{H}_1$, составляющие первое разбиение, которые под действием автоморфизма $(\pi, \sigma) \in Aut(\mathbb{F}_p^{p+1})$ перешли в коды $\mathcal{H}_2'$ и $\mathcal{H}_3'$ второго разбиения, являющиеся классами смежности двух различных кодов Хэмминга $\mathcal{H}_2$ и $\mathcal{H}_3$ соответственно. Так как любой код Хэмминга $\mathcal{H}_1$ имеет кодовое расстояние 3, то его классы смежности можно представить в виде $\mathcal{H}_1' = \mathcal{H}_1 + \alpha \cdot e_i$ и $\mathcal{H}_1'' = \mathcal{H}_1 + \beta \cdot e_j$, где e_i — вектор с одним ненулевым элементом в i-й позиции, равным 1, а α и β — ненулевые

элементы поля $GF(p)$. Очевидно, что кодовые матрицы кодов $\mathcal{H}_1'$ и $\mathcal{H}_1''$ различаются в тех же координатных позициях, что и коды $\mathcal{H}_1$ и $\mathcal{H}_1 + \alpha \cdot e_i - \beta \cdot e_j$. А поскольку кодовые слова веса 3 кода Хэмминга образуют обобщенную систему троек Штейнера, то для некоторых $k \in \{1, 2, \ldots, p+1\}$ и ненулевого элемента γ поля $GF(p)$ существует кодовое слово $c = \alpha \cdot e_i - \beta \cdot e_j + \gamma \cdot e_k$, принадлежащее коду $\mathcal{H}_1$. Следовательно, кодовые матрицы кодов $\mathcal{H}_1'$ и $\mathcal{H}_1''$ различаются только в одной координатной позиции k. Заметим, что под действием автоморфизма (π, σ) пространства $\mathbb{F}_p^{p+1}$ совпадающие столбцы кодовых матриц различных кодов перейдут в совпадающие, а различные — в различные. Таким образом, кодовые матрицы кодов $\mathcal{H}_2'$ и $\mathcal{H}_3'$ второго разбиения также отличаются только в одной координатной позиции, а поскольку они являются классами смежности кодов Хэмминга $\mathcal{H}_2$ и $\mathcal{H}_3$, то несложно показать, что коды $\mathcal{H}_2$ и $\mathcal{H}_3$ должны совпадать. □

Теорема 2. *Число неэквивалентных разбиений пространства $\mathbb{F}_p^{p+1}$ на совершенные p-значные коды длины $p+1$ не меньше чем*

$$f(p) \sim \frac{1}{4p\sqrt{3}} e^{\pi\sqrt{2p/3}}.$$

Доказательство. Согласно утверждению 4, если разбиения пространства $\mathbb{F}_p^{p+1}$ на совершенные коды имеют различные спектры, то эти разбиения неэквивалентны. Тогда число попарно неэквивалентных разбиений совпадает с числом различных спектров, которое можно оценить снизу количеством различных разложений $f(p)$ числа p на слагаемые. Асимптотическая формула такого числа при $p \to \infty$ имеет, согласно [10], следующий вид:

$$f(p) \sim \frac{1}{4p\sqrt{3}} e^{\pi\sqrt{2p/3}}. \qquad \square$$

Авторы выражают благодарность Ф. И. Соловьевой за ценные замечания, позволившие существенно улучшить изложение статьи.

Список литературы

[1] С. В. Августинович, Ф. И. Соловьева, *Построение совершенных бинарных кодов последовательными сдвигами $\widetilde{\alpha}$-компонент* Пробл. передачи информ. 1997. Т. 33. Вып. 3. С. 15–21. MR1476367

[2] С. В. Августинович, Ф. И. Соловьева, У. Хеден, *О разбиениях n-куба на неэквивалентные совершенные коды*, Пробл. передачи информ. 2007. Т. 43. № 4. С. 45–50. MR2406143

[3] В. А. Зиновьев, В. К. Леонтьев, *О совершенных кодах*, (Препринт/ ИППИ АН СССР). 1972. Вып. 1. С. 26–35. MR0325263

[4] В. А. Зиновьев, В. К. Леонтьев, *Несуществование совершенных кодов над полями Галуа*, Проблемы управления и теории информации. 1973. Вып. 2. С. 123–132. MR0401330

[5] А. В. Лось, *Построение совершенных q-ичных кодов свитчингами простых компонент* Пробл. передачи информ. 2006. Т. 42. № 1. С. 34–42. MR2214510

[6] Ф. И. Соловьева, А. В. Лось, *О построении разбиений $\mathbb{F}_q^N$ на совершенные q-значные коды*, Дискрет. анализ и исслед. операций. 2009. Т. 16. № 3. С. 63–73. MR2588620

[7] А. В. Лось, Ф. И. Соловьева, *О разбиениях пространства $\mathbb{F}_q^N$ на аффинно неэквивалентные совершенные q-значные коды*, Сиб. электрон. матем. известия. 2010. Т. 7. С. 425–434. MR2770863

[8] А. А. Марков, *О перобразованиях, не распространяющих искажения*, Избранные труды. Т. II. Теория алгоритмов и конструктивная математика, математическая логика, информатика и смежные вопросы. — М.: МЦНМО, 2003. С. 70–93. MR2086689

[9] O. Heden, F. I. Solov'eva, *Partitions of $\mathbb{F}^n$ into non-parallel Hamming codes*, Advanced in Mathematics of Communications V. 13, No. 4, 2009. P 385–397. MR2559136
[10] Г. Эндрюс, *Теория разбиений*, Перв. с англ. М.: Наука. Главная редакция физико-математической литературы, 1982. — 256 С.
[11] G. Cohen, I. Honkala, A. Lobstein, S. Litsyn, *Covering codes*, Elsevier, 1998.
[12] W. C. Huffman, *Codes and groups*, Handbook of coding theory. Amsterdam – New York: Elsevier. 1998. MR1667953
[13] K. T. Phelps, *An enumeration of 1-perfect binary codes*, Australas. J. Comb., **21**, 2000. P. 287–298. MR1758278
[14] F. I. Solov'eva, *On perfect codes and related topics*, Com^{2}Mac Lecture Note Series 13, Pohang 2004. 80 P.
[15] A. Tietäväinen, *On the nonexistence of perfect codes over finite fields*, SIAM J. Appl. Math. 1973. V. 24. P. 88–96. MR0325260

Лось Антон Васильевич
Институт математики им. С. Л. Соболева СО РАН,
пр. академика Коптюга 4,
630090, Новосибирск, Россия
E-mail address: sozercatel@gmail.com

Бурнаков Константин Игоревич
Институт математики им. С. Л. Соболева СО РАН,
пр. академика Коптюга 4,
630090, Новосибирск, Россия
E-mail address: eresyyl@gmail.com