О построении разбиений $p+1$-мерного пространства всех p-значных векторов на совершенные коды

А. В. Лось, К. И. Бурнаков

Аннотация

Для любого числа простого числа p предложена конструкция разбиения $p+1$-мерного пространства всех p-значных векторов на совершенные коды. Найдена нижняя оценка числа неэквивалентных таких кодов.

1. Введение

Через 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 предложены два метода построения разбиений пространства F_q^N на различные совершенные q-значные коды длины N с кодовым расстоянием 3, здесь $N = (q^m-1)/(q-1)$. В первом методе построения разбиений используется некоторая модификация хорошо известной конструкции Шонхайма, см. [10]. Этот метод является обобщением аналогичного результата для совершенных двоичных кодов, см. [11], а также [1], где установлено, что для любого допустимого $N > 15$ число различных разбиений множества всех двоичных векторов F_2^N на совершенные коды длины N не меньше, чем

$$2^{2^{(N-1)/2}}.$$

Недавно стало известно, что эта оценка верна для любого допустимого $N \geq 7$. Во второй конструкции используются свитчинги простых компонент (см. [5]) смежных классов q-значного кода Хэмминга в пространстве F_q^N, где $q > 2$.

Проблема перечисления всех разбиений пространства F_q^N на совершенные q-значные коды тесно связана с классической проблемой перечисления всех совершенных q-значных кодов. В настоящей статье рассматриваются различные разбиения, поскольку, зная оценку снизу числа различных разбиений, легко оценить снизу число неэквивалентных таких разбиений с учетом порядка группы автоморфизмов F_q^N. Конструкции разбиений могут также быть полезны для построения новых классов q-значных кодов и, в частности, совершенных. В книге [8], гл. 11, описано несколько конструкций совершенных q-значных кодов, в основе которых лежат разбиения пространства F_q^N на совершенные коды. Следует отметить, что для $q > 2$ известно не так много работ, посвященных построению разбиений пространства F_q^N на совершенные коды, двоичный же случай исследован гораздо глубже.

Напомним некоторые необходимые определения. Произвольное подмножество C пространства F_q^N называется *совершенным q-значным кодом длины N с кодовым расстоянием 3* (далее кратко *совершенным кодом*), если для любого вектора $x \in F_q^N$ 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, 12]. Код называется *линейным*, если он образует линейное подпространство в пространстве F_q^N. Совершенный линейный код $\mathcal{H}_q^N$ называется *кодом Хэмминга*. Далее будем обозначать его через $\mathcal{H}$. Два кода $C, C' \subset F_q^N$ называются *изоморфными*, если существует такая перестановка σ на N координатных позициях, что $C' = \sigma(C)$. Код Хэмминга единственен с точностью до изоморфизма. Всюду далее $N = qn + 1$, $n = (q^{m-1} - 1)/(q-1)$ и $m \geq 2$.

2. Конструкция разбиений $(p+1)$-мерных пространств на p-значные коды

В этом параграфе описана конструкция класса нетривиальных разбиений пространства F_p^n на совершенные p-значные, p — простое, коды длины $n = p+1$ с помощью выбора по некоторым правилам кодов, эквивалентных коду Хэмминга и способных составлять такое разбиение.

Рассмотрим произвольное разбиение пространства F_p^n на совершенные p-значные коды. Нетрудно проверить следующее

Утверждение 1. *Разбиение пространства всех p-значных векторов длины $n = \frac{p^m-1}{p-1}$ состоит из p^m совершенных кодов с кодовым расстоянием 3.*

Доказательство. Рассмотрим произвольный p-значный код Хэмминга длины $n = \frac{p^m-1}{p-1}$. Поскольку такой код имеет кодовое расстояние 3 и является плотноупакованным, то шары радиуса 1 с центрами в кодовых словах не пересекаются и образуют покрытие всего пространства F_p^n. Очевидно, что для произвольного разбиения такого пространства на совершенные коды верно, что в каждом шаре покрытия пространства F_p^n содержится по одному кодовому слову из каждого кода разбиения. Таким образом, число кодов в разбиении пространства F_p^n равно объему шара радиуса 1, то есть $1 + C_n^1(p-1)^1 = 1 + n(p-1) = p^m$. □

Поскольку вопрос о существовании совершенных p-значных кодов, неэквивалентных кодам Хэмминга длины $p+1$, остается открытым, то для конструирования разбиений будем рассматривать только коды Хэмминга и эквивалентные им. Для дальнейших оценок числа разбиений найдем нижнюю

оценку числа p-значных совершенных кодов длины $p+1$.

Утверждение 2. *В пространстве всех p-значных векторов длины $n = p+1$ существует по крайней мере $((p-1)!)^p((p-2)!)^2$ различных приведенных совершенных кодов.*

Доказательство. Поскольку коды Хэмминга линейные и содержат нулевое кодовое слово, то число приведенных совершенных кодов не меньше, чем кодов эквивалентных коду Хэмминга, содержащих нулевой вектор. Для того чтобы найти коды эквивалентные коду Хэмминга, содержащие нулевой вектор, требуется рассмотреть преобразования, оставляющие нулевое слово на месте, то есть группу симметрий кода Хэмминга. Известно, что порядок группы симметрий кода Хэмминга длины $n\frac{p^m-1}{p-1}$ совпадает с порядком общей линейной группы $GL_m(p)$, см. [**?**], то есть

$$|Sym(\mathcal{H}_p^n)| = (p^m - p^{m-1}) \cdots (p^m - p^0).$$

Тогда число приведенных кодов, эквивалентных коду Хэмминга, можно вычислить из отношения порядков групп симметрий всего пространства и кода Хэмминга. Учитывая, что группу симметрий n мерного пространства всех p-значных векторов составляют пары преобразований (π, σ), где π принадлежит симметрической группе перестановок S_n, а σ является конфигурацией длины n, состоящей из n перестановок элементов поля $GF(p)$, оставляющих нулевой элемент неподвижным, то есть $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n)$, где $\sigma_i \in S_{p-1}$, $i \in \{1, 2, \ldots, n\}$, получаем, что $|Sym(F_p^n)| = n!((p-1)!)^n$. Тогда число приведенных кодов, эквивалентных коду Хэмминга, равно

$$\frac{|Sym(F_p^n)|}{|Sym(\mathcal{H}_p^n)|} = \frac{n!((p-1)!)^n}{(p^m - p^{m-1}) \cdots (p^m - p^0)}.$$

Отсюда получаем, что число приведенных совершенных p-значных кодов $\mathcal{N}_p^{p+1}$ длины $p+1$ не меньше, чем

$$\frac{|Sym(F_p^{p+1})|}{|Sym(\mathcal{H}_p^{p+1})|} = \frac{(p+1)!((p-1)!)^{p+1}}{(p^2-p)(p^2-1)} = \frac{((p-1)!)^{p+2}}{(p-1)^2}.$$

□

Рассмотрим разбиение пространства F_p^n всех p-значных векторов длины $n = \frac{p^m-1}{p-1}$ на классы смежности приведенного совершенного кода, такое разбиение называется *тривиальным*. Несложно показать, что

Утверждение 3. *Размерность пересечения кодов Хэмминга, классы смежности которых составляют нетривиальное разбиение пространства* F_p^{p+1}, *равна* $p-2$.

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 $k = p-1$ имеем, что размерность пересечения кодов совпадает с размерностью самих кодов. Данная ситуация характерна только для тривиального разбиения, когда разбиение состоит из классов смежности одного кода Хэмминга.

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

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

Но, согласно утверждению 1, разбиение пространства F_p^{p+1} состоит из p^2 совершенных кодов. Тогда любой класс смежности кода $\mathcal{H}_2$ 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 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 F_p^{p+1}. Объединение этих p классов смежности кода $\mathcal{H}_2$ совпадает с объединением некоторых p классов смежности кода $\mathcal{H}_1$, и тогда тривиальное разбиение пространства F_p^{p+1} на классы смежности кода $\mathcal{H}_2$ позволяет заменить некоторые p кодов на классы смежности кода $\mathcal{H}_1$, что в результате дает разбиение, не являющееся тривиальным. □

Для доказательства следующего утверждения предположим, что существует разбиение пространства F_p^{p+1} на классы смежности двух различных кодов Хэмминга $\mathcal{H}_1$ и $\mathcal{H}_2$. Поскольку размерность таких кодов равна $p-1$, и, согласно утверждению 3, размерность их пересечения равна $p-2$, то размерность подпространства U, порожденного объединением этих кодов Хэмминга равна p. Если рассмотреть разбиение пространства F_p^{p+1} в виде объединения разбиений p классов смежности подпространства U на классы смежности кодов $\mathcal{H}_1$ и $\mathcal{H}_2$, то очевидно, что произвольный класс смежности подпространства U представим в виде разбиения на классы смежности только одного из кодов Хэмминга $\mathcal{H}_1$ или $\mathcal{H}_2$. Если представить разбиение пространства F_p^{p+1} в виде объединения кодов, составляющих его, то последний факт можно записать в виде:

$$F_p^{p+1} = \bigcup_{i=1}^{p} U_i, \tag{1}$$

где U_i — i-ый смежный класс подпространства U и

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

здесь $\mathcal{H}_t^{(ij)}$ — некоторый смежный класс кода $\mathcal{H}_{t_i}$, $t_i \in \{1, 2\}$.

Утверждение 4. *Одно разбиение пространства F_p^{p+1} могут составлять классы смежности до $p-1$ различных p-значных кодов Хэмминга длины $p+1$ включительно.*

Доказательство. Рассмотрим два кода Хэмминга $\mathcal{H}_1$ и $\mathcal{H}_2$ классы смежности которых, составляют нетривиальное разбиение пространства F_p^{p+1}. Согласно утверждению 3, размерность пересечения этих кодов Хэмминга равна $p-2$. Обозначим порождающие матрицы рассматриваемых кодов через G_1 и G_2 соответственно. Согласно утверждению 3, размерность пересечения этих кодов Хэмминга равна $p-2$. 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 утверждению 3, 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 $GF(p)$.

Рассмотрим порождающую матрицу G_2. Поскольку она порождает код Хэмминга с кодовым расстоянием 3, то произвольная линейная комбинация последней строки матрицы G_2 должна быть удалена от остальных строк матрицы по крайней мере на 3. Обозначим последнюю строку матрицы G_2 через c_2 и рассмотрим следующую ее линейную комбинацию:

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

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

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

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 любого числа кодов с порождающей матрицей вида (2). Для этого рассмотрим три кода Хэмминга с порождающими матрицами, определенного выше вида, у которых последние строки 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, а значит смежные классы любого числа кодов Хэмминга с порождающими матрицами вида (2) могут составлять одно разбиение пространства F_p^{p+1}.

Остается показать, что смежные классы кодов Хэмминга, не имеющих порождающих матриц вида (2), не могут составлять одного разбиения пространства F_p^{p+1} вместе с кодами $\mathcal{H}_1$ и $\mathcal{H}_2$ одновременно. Рассмотрим код Хэмминга $\mathcal{H}_3$, порождающая матрица которого, не теряя всеобщности рассмотрения, 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 $\delta \in GF^*(p)$. Легко видеть, что порядок пересечения данного кода с кодом $\mathcal{H}_1$ также равен $p-2$, что удовлетворяет требованию утверждения 3. Но подпространство, порожденное объединением матриц G_2 и G_3 совпадает с пространством F_p^{p+1}, что противоречит утверждению 3 и, следовательно, смежные классы кодов $\mathcal{H}_2$ и $\mathcal{H}_3$ не могут составлять одно разбиение. □

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 утверждению 4 классы смежности таких кодов могут составлять одно разбиение. Линейная оболочка объединение таких кодов Хэмминга как множеств векторов является некоторым подпространством $U \subseteq F_p^{p+1}$ 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 через U_i i-ый смежный класс подпространства U, а через $\mathcal{H}_t^{ij}$ — смежные

классы кода Хэмминга $\mathcal{H}_t$, $t \in \{1, 2, \ldots, p-1\}$, объединение которых

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

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 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 получается из утверждений 1 и 4, а также из того факта, что все задействованные в разбиении классы смежности кодов Хэмминга не пересекаются между собой. □

3. Нижняя оценка числа неэквивалентных разбиений $(p+1)$-мерных пространств на p-значные совершенные коды

Два разбиения пространства F_p^{p+1} на совершенные коды называются эквивалентными, если существует такой автоморфизм пространства, что все коды первого разбиения под действием данного автоморфизма перейдут в коды второго.

Используя конструкцию разбиений, заданную теоремой 2, можно оценить снизу число неэквивалентных разбиений.

Утверждение 5. *Если спектры двух разбиений содержат различные значения, то такие разбиения неэквивалентны.*

Доказательство. Рассмотрим два разбиения пространства F_p^{p+1} с различными спектрами. Предположим, что одно разбиение под действием некоторого автоморфизма $(\pi, \sigma) \in Aut(F_p^{p+1})$ 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.

□

Утверждение 6. *Если спектры двух разбиений содержат различные значения, то такие разбиения неэквивалентны.*

Доказательство. □

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

$$f(p) \cdot \frac{((p-1)!)^{p+2}}{(p-1)^2},$$

где

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

Доказательство. □

Список литературы

[1] **Августинович 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 // Проблемы кибернетики. М: Наука, 1962. Вып. 8. С. 337–339.

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

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

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

[6] **Соловьева Ф. И., Гуськов Г. К.** Частное сообщение.

[7] **Тимашёв А. Н.** О перманентах случайных дважды стахастических матриц и асимптотических оценках чисел латинских прямоугольников и латинских квадратов // Дискретная математика. 2002. Т. 14. Вып. 4. С. 65–86.

[8] **Cohen G., Honkala I., Lobstein A., Litsyn S.,** Covering codes, Elsevier, 1998.

[9] **Phelps K. T., Villanueva M.** Ranks of q-ary 1 perfect codes // Des. Codes Cryptogr. 2002. V. 27. P. 139–144.

[10] **Schönheim J.** On linear and nonlinear single-error-correcting q-nary 1 perfect codes // Inform. Control. 1986. V. 12. P. 23–26.

[11] **Solov'eva F. I.** On perfect codes and related topics, Com^{2}Mac Lecture Note Series 13, Pohang 2004. 80 P.

[12] **Tietäväinen A.** On the nonexistence of perfect codes over finite fields // SIAM J. Appl. Math. 1973. V. 24. P. 88–96.

Бурнаков Константин Игоревич
Новосибирский государственный университет, ул. Пирогова, 2,
Новосибирск 630090
@gmail.com

Лось Антон Васильевич
Институт математики им. С. Л. Соболева СО РАН, пр. Коптюга, 4,
Новосибирский государственный университет, ул. Пирогова, 2,
Новосибирск 630090
sozercatel@gmail.com