

ЛОКАЛЬНЫЕ СПЕКТРЫ СОВЕРШЕННЫХ ДВОИЧНЫХ КОДОВ

А. Ю. Васильева

Для произвольного совершенного двоичного $(n, 3)$ -кода вводится понятие локального спектра как локального аналога весового спектра. Устанавливается связь локальных спектров произвольного кода на паре ортогональных k - и $(n - k)$ -мерной граней n -куба и обнаруживаются некоторые свойства рассматриваемых спектров.

В работе изучаются числовые характеристики произвольного совершенного двоичного $(n, 3)$ -кода, относящиеся к расположению вершин кода в произвольной грани n -куба и называемые в совокупности локальным спектром кода. Такого рода характеристики привлекают внимание в силу того, что они помогают понять многообразие геометрического строения кодов, что в свою очередь может способствовать решению задачи описания всех совершенных кодов. Так, в теории корректирующих кодов для доказательства неэквивалентности кодов часто используется несовпадение их весовых спектров. Локальный же спектр внутри грани является аналогом весового спектра кода, который согласно [5] одинаков для любых двух совершенных кодов, содержащих нулевую вершину куба. Однако уже для локальных спектров наблюдается большое разнообразие: если есть грани, содержащие различное количество вершин совершенного кода, то заведомо и локальные спектры в этих гранях будут различны (комбинируя результаты из [7] и [1], можно получить весьма много значений мощности пересечения совершенного кода с гранью заданной размерности, не превосходящей $(n - 1)/2$).

В разделе 1 доказывается вспомогательная лемма 1, необходимая для доказательства основной теоремы 1 из раздела 2, утверждающей, что локальный спектр кода в грани, ортогональной к данной, однозначно определяется локальным спектром в исходной грани (указывается вид этой связи).

В разделе 3 устанавливаются содержательные следствия основной теоремы. Например, оказывается, что локальные спектры можно применить для изучения систематичности совершенного кода, точнее,

систематические совершенные коды можно характеризовать в терминах локальных спектров (следствие 4). Кроме того, в этом разделе показывается, что множество вершин кода в произвольной грани куба определяет локальные спектры (а как следствие этого, количество вершин кода) во всех гранях, ортогональных к исходной. В следствии 6 устанавливается, что в отличие от граней небольших размерностей в гранях размерности не менее $(n+1)/2$ (которые обладают тем свойством, что количество кодовых вершин в них зависит только от размерности грани [4, 6]) локальные спектры однозначно определяются лишь частью своих компонент.

1. Предварительные сведения

Введем следующие обозначения и понятия:

$E^n = \{\mathbf{x} = (x_1, x_2, \dots, x_n) \mid x_i \in \{0, 1\}, 0 \leq i \leq n\}$ — n -мерный единичный куб (n -куб);

$\rho(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n |x_i - y_i|$ — расстояние Хэмминга между вершинами \mathbf{x} и \mathbf{y} из E^n ;

C — совершенный двоичный $(n, 3)$ -код — такое подмножество вершин из E^n , что шары радиуса 1 с центрами из C не пересекаются и в совокупности покрывают n -куб (иногда будем говорить просто «код», так как другие коды здесь упоминаться не будут);

t -мерная грань n -куба — множество всех таких вершин из E^n , у которых данные $n - t$ координат фиксированы;

две t -мерные грани γ и γ' назовем *параллельными*, если

$$\begin{aligned}\gamma &= \{\mathbf{x} = (x_1, x_2, \dots, x_n) \in E^n \mid x_i = a_i, i \notin \{i_1, \dots, i_m\}\}, \\ \gamma' &= \{\mathbf{x} = (x_1, x_2, \dots, x_n) \in E^n \mid x_i = b_i, i \notin \{i_1, \dots, i_m\}\};\end{aligned}$$

t -мерную грань γ и $(n - t)$ -мерную грань γ^\perp назовем *ортогональными*, если

$$\begin{aligned}\gamma &= \{\mathbf{x} = (x_1, x_2, \dots, x_n) \in E^n \mid x_i = a_i, i \notin \{i_1, \dots, i_m\}\}, \\ \gamma^\perp &= \{\mathbf{x} = (x_1, x_2, \dots, x_n) \in E^n \mid x_i = a_i, i \in \{i_1, \dots, i_m\}\},\end{aligned}$$

где $\mathbf{a} = (a_1, a_2, \dots, a_n)$ — их единственная общая вершина;

$$p_i(x; N) = \sum_{j=0}^i (-1)^j \binom{x}{j} \binom{N-x}{i-j} \text{ — многочлен Кравчука (см., например, [3]), где } N \text{ — натуральное число и } 0 \leq i \leq N.$$

Для произвольной грани γ и произвольной вершины \mathbf{a} из γ обозначим через $A_i^{\mathbf{a}}(\gamma)$ множество всех вершин грани γ , находящихся на расстоянии i от вершины \mathbf{a} , а через $v_i^{\mathbf{a}}(\gamma)$ количество кодовых вершин в грани γ , находящихся на расстоянии i от вершины \mathbf{a} . Вектор

$$v^{\mathbf{a}}(\gamma) = (v_0^{\mathbf{a}}(\gamma), v_1^{\mathbf{a}}(\gamma), \dots, v_{\dim \gamma}^{\mathbf{a}}(\gamma))$$

назовем *локальным спектром кода C в грани γ относительно вершины \mathbf{a}* , или, короче, (γ, \mathbf{a}) -*локальным спектром кода C* .

Предварительно обозначим через \mathbf{e}_i вершину $(0, \dots, 0, 1, 0, \dots, 0)$, где единица находится на i -м месте, а для любого множества M из n -куба обозначим через $M \oplus \mathbf{x}$ множество $\{\mathbf{y} \oplus \mathbf{x} \mid \mathbf{y} \in M\}$, где $\mathbf{y} \oplus \mathbf{x} = (y_1 \oplus x_1, y_2 \oplus x_2, \dots, y_n \oplus x_n)$ — сложение по модулю 2.

Положим

$$\begin{aligned} \gamma &= \{\mathbf{x} = (0, \dots, 0, x_{n-m+1}, \dots, x_n) \in E^n\}; \\ \gamma_i &= \gamma \cup (\gamma \oplus \mathbf{e}_i), \quad 1 \leq i \leq n - m. \end{aligned}$$

Введем дополнительно $v_{-1}^{\mathbf{a}}(\gamma)$ и $v_{m+1}^{\mathbf{a}}(\gamma)$, положив их равными нулю.

Лемма 1. При любом j , $0 \leq j \leq m$, справедливо равенство

$$(2m - n - j + 1)v_{j-1}^0(\gamma) + v_j^0(\gamma) + (j + 1)v_{j+1}^0(\gamma) + \sum_{i=1}^{n-m} v_j^{\mathbf{e}_i}(\gamma_i) = \binom{m}{j}. \quad (1)$$

ДОКАЗАТЕЛЬСТВО. Пусть j — произвольное число такое, что $0 \leq j \leq m$. Так как код C — совершенный, то любая некодовая вершина n -куба находится на расстоянии 1 от одной кодовой. Поэтому $A_j^0(\gamma)$ разбивается на четыре подмножества согласно следующим условиям:

- 1) $\mathbf{x} \in C$;
 - 2) ближайшая к \mathbf{x} вершина кода C принадлежит множеству $A_{j-1}^0(\gamma)$;
 - 3) ближайшая к \mathbf{x} вершина кода C принадлежит множеству $A_{j+1}^0(\gamma)$;
 - 4) ближайшая к \mathbf{x} вершина кода C принадлежит множеству $A_j^{\mathbf{e}_i}(\gamma)$
- для некоторого i , $1 \leq i \leq n - m$.

Нетрудно убедиться, что мощности таких подмножеств равны соответственно $v_j^0(\gamma)$, $(m - j + 1)v_{j-1}^0(\gamma)$, $(j + 1)v_{j+1}^0(\gamma)$ и $\sum_{i=1}^{n-m} v_j^{\mathbf{e}_i}(\gamma \oplus \mathbf{e}_i)$. Остается заметить, что для любого i , $1 \leq i \leq n - m$,

$$v_{j-1}^0(\gamma) + v_j^{\mathbf{e}_i}(\gamma \oplus \mathbf{e}_i) = v_j^{\mathbf{e}_i}(\gamma_i).$$

Поскольку наши подмножества образуют разбиение $A_j^0(\gamma)$, то, учитывая последнее равенство, получим (1). Лемма 1 доказана.

2. Связь между локальными спектрами совершенного кода в ортогональных гранях n -куба

Пусть Γ — произвольная k -мерная грань n -куба. Обозначим через Γ^\perp грань размерности $n - k$, ортогональную к грани Γ . Пусть грани Γ и Γ^\perp пересекаются по вершине \mathbf{a} . Следующая теорема, устанавливающая связь локальных спектров произвольного совершенного кода в гранях Γ и Γ^\perp относительно вершины \mathbf{a} , является основной в этом разделе.

Теорема 1. $(\Gamma^\perp, \mathbf{a})$ -локальный спектр совершенного кода однозначно определяется (Γ, \mathbf{a}) -локальным спектром этого кода и задается коэффициентами разложения по степеням x функции

$$f_\Gamma(x) = \frac{1}{n+1}(1+x)^{n-k} + (1-x)^{(n+1)/2-k} \times (1+x)^{(n-1)/2-k} \sum_{q=0}^k (-1)^q \left(v_q^{\mathbf{a}}(\Gamma) - \frac{1}{n+1} \binom{k}{q} \right) x^q. \quad (2)$$

Доказательство. Пусть $h_\Gamma = \sum_{j=0}^{n-k} v_j^{\mathbf{a}}(\Gamma^\perp) x^j$. Индукцией по k (размерности грани Γ), каждый раз составляя дифференциальное уравнение с начальным условием для функции h_Γ , покажем, что $h_\Gamma = f_\Gamma$.

Базис индукции. $k = 0$, т. е. $\Gamma = \{\mathbf{a}\}$. В этом случае $\Gamma^\perp = E^n$ и $(\Gamma^\perp, \mathbf{a})$ -локальный спектр кода является весовым спектром относительно вершины \mathbf{a} и поэтому (см. [5, 2])

$$h_{\{\mathbf{a}\}}(x) = \frac{1}{n+1}(1+x)^n + \left(v_0^{\mathbf{a}}(\{\mathbf{a}\}) - \frac{1}{n+1} \right) (1-x)^{(n+1)/2} (1+x)^{(n-1)/2}.$$

Очевидно, что эта формула совпадает с формулой (2) при $k = 0$.

Шаг индукции. Предположим, что утверждение теоремы верно при $\dim \Gamma = k - 1$. Докажем его истинность при $\dim \Gamma = k$.

Без ограничения общности можно считать, что

$$\begin{aligned} \Gamma &= \{\mathbf{x} = (x_1, \dots, x_k, 0, \dots, 0) \in E^n\}, \\ \Gamma^\perp &= \{\mathbf{x} = (0, \dots, 0, x_{k+1}, \dots, x_n) \in E^n\} \end{aligned}$$

и точка их пересечения $\mathbf{a} = 0 = (0, \dots, 0) \in E^n$.

По лемме 1 при любом j , $0 \leq j \leq n - k$, верно соотношение

$$\begin{aligned} (n - 2k - j + 1)v_{j-1}^0(\Gamma^\perp) \\ + v_j^0(\Gamma^\perp) + (j + 1)v_{j+1}^0(\Gamma^\perp) + \sum_{i=1}^k v_j^{e_i}(\Gamma_i^\perp) = \binom{n-k}{j}, \end{aligned} \quad (3)$$

где $\Gamma_i^\perp = \Gamma^\perp \cup (\Gamma^\perp \oplus \mathbf{e}_i)$, $1 \leq i \leq k$, и $v_{-1}^0(\Gamma^\perp) = v_{n-k+1}^0(\Gamma^\perp) = 0$.

Эта система из $n-k+1$ линейных алгебраических уравнений относительно $v^0(\Gamma^\perp)$ при каждом значении $v_0^0(\Gamma^\perp)$ имеет единственное решение, которое можно получить, последовательно вычисляя компоненты спектра из уравнений системы.

Умножим j -е уравнение системы (3) на x^j и просуммируем по j . Преобразовав, получим

$$h'_\Gamma(x) = \frac{(n-2k)x+1}{x^2-1} h_\Gamma(x) + \frac{1}{x^2-1} \left(\sum_{i=1}^k h_{\Gamma_i}(x) - (1+x)^{n-k} \right), \quad (4)$$

где $\Gamma_i = \{\mathbf{x} = (x_1, \dots, x_{i-1}, 1, x_{i+1}, \dots, x_k, 0, \dots, 0) \in E^n\}$ является $(k-1)$ -мерной гранью. Поэтому по предположению индукции $h_{\Gamma_i} = f_{\Gamma_i}$.

Так как $v_0^0(\Gamma^\perp) = v_0^0(\Gamma)$, то должно выполняться начальное условие

$$h_\Gamma(0) = v_0^0(\Gamma), \quad (5)$$

что обеспечивает единственность решения задачи Коши (4), (5).

Остается убедиться, что функция (2) является решением этой задачи. Очевидно, что для функции f_Γ начальное условие (5) выполняется. Для проверки выполнения уравнения (4) для функции f_Γ заметим, что любая вершина из $A_{r+1}^0(\Gamma)$ находится на расстоянии r ровно от $r+1$ вершин из $A_1^0(\Gamma) = \{\mathbf{e}_1, \dots, \mathbf{e}_k\}$ и поэтому покрывается ровно $r+1$ множествами из совокупности $\{A_r^{e_i}(\Gamma_i), 1 \leq i \leq k\}$. Следовательно,

$$(r+1)v_{r+1}^0(\Gamma) = \sum_{i=1}^k v_r^{e_i}(\Gamma_i)$$

и $\sum_{i=1}^k f_{\Gamma_i}(x)$ можно выразить через $(\Gamma, \mathbf{0})$ -локальный спектр:

$$\begin{aligned} \sum_{i=1}^k f_{\Gamma_i}(x) &= \frac{k}{n+1} (1+x)^{n-k-1} + (1-x)^{(n-1)/2-k} \\ &\times (1+x)^{(n-3)/2-k} \sum_{r=0}^{k-1} (-1)^r \left((r+1)v_{r+1}^0(\Gamma) - \frac{k}{n+1} \binom{k-1}{r} \right) x^r. \end{aligned}$$

После этого, вычислив $f_\Gamma^l(x)$ и подставив $f_\Gamma(x)$, $f_\Gamma^l(x)$ и $\sum_{i=1}^k f_{\Gamma_i}(x)$ в уравнение (4), после преобразований убедимся, что имеем тождество, а значит, функция $f_\Gamma(x)$ является решением задачи (4), (5). Теорема 1 доказана.

Формулу (2) из теоремы 1 приведем к более наглядному и симметричному виду. Предварительно для произвольного множества M из n -куба введем величину $V(M)$, определяемую условием

$$\frac{V(M)}{|M|} = \frac{|C|}{|E^n|}, \quad \text{т. е. } V(M) = \frac{|M|}{n+1}.$$

Для произвольной грани γ и вершины \mathbf{a} из γ положим

$$\Delta_i^{\mathbf{a}}(\gamma) = v_i^{\mathbf{a}}(\gamma) - V(A_i^{\mathbf{a}}(\gamma)), \quad 0 \leq i \leq \dim \gamma.$$

Так как $V(A_i^{\mathbf{a}}(\gamma)) = \frac{1}{n+1} \binom{\dim \gamma}{i}$, то из (2) непосредственно получаем

Следствие 1.

$$\sum_{j=0}^{n-k} \Delta_j^{\mathbf{a}}(\Gamma^{\perp}) x^j = (1-x)^{(n+1)/2-k} (1+x)^{(n-1)/2-k} \sum_{q=0}^k (-1)^q \Delta_q^{\mathbf{a}}(\Gamma) x^q. \quad (6)$$

Следствие 2. Если $\dim \Gamma = k \leq (n-1)/2$, то

$$\Delta_j^{\mathbf{a}}(\Gamma^{\perp}) = \sum_{q+r=j} (-1)^q \Delta_q^{\mathbf{a}}(\Gamma) p_r\left(\frac{n+1}{2} - k; n - 2k\right).$$

Отметим, что присутствующие в формуле значения многочленов Кравчука вычисляются довольно просто в результате рассмотрения их эквивалентной формы. Поскольку $\sum_{i=0}^N p_i(x; N) z^i = (1-z)^x (1+z)^{N-x}$, то при любом t , $0 \leq t \leq (n-1)/2$, имеем

$$p_{2t}\left(\frac{n+1}{2}; n\right) = -p_{2t+1}\left(\frac{n+1}{2}; n\right) = (-1)^t \binom{(n-1)/2}{t}.$$

3. Свойства локальных спектров

Для произвольной вершины $\mathbf{a} \in E^n$ обозначим через $\Gamma^{\perp}(\mathbf{a})$ грань, ортогональную к Γ и содержащую вершину \mathbf{a} .

Сначала рассмотрим два случая, иллюстрирующие смысл теоремы 1. Первый касается граней, не имеющих общих с кодом вершин.

Следствие 3. Грань Γ не содержит вершин кода C тогда и только тогда, когда $(\Gamma^{\perp}(\mathbf{a}), \mathbf{a})$ -локальный спектр совершенного кода C не зависит от выбора вершины \mathbf{a} в грани Γ .

Действительно, в этом случае (Γ, \mathbf{a}) -локальный спектр не зависит от выбора вершины $\mathbf{a} \in \Gamma$, а значит, по теореме 1 аналогичное верно и для $(\Gamma^{\perp}(\mathbf{a}), \mathbf{a})$ -локального спектра.

Второй случай касается систематических совершенных кодов, т. е. совершенных кодов, у которых существует такая $\log(n+1)$ -мерная грань, что во всех параллельных ей гранях содержится только по одной кодовой вершине. Следствие 4 вытекает из теоремы 1, если в качестве грани Γ взять именно такую грань.

Следствие 4. Совершенный код C является систематическим тогда и только тогда, когда существует такая $\log(n+1)$ -мерная грань Γ , что $(\Gamma^\perp(\mathbf{a}), \mathbf{a})$ -локальный спектр совершенного кода C не зависит от выбора вершины \mathbf{a} кода C .

Заметим, что, используя формулу (2), нетрудно указать конкретные выражения для упомянутых в следствиях 3 и 4 локальных спектров.

Если известно, какие вершины грани Γ принадлежат коду C , то для любой вершины $\mathbf{a} \in \Gamma$ можно посчитать (Γ, \mathbf{a}) -локальный спектр этого кода, а из теоремы 1 вытекает, что в этом случае можно вычислить $(\Gamma^\perp(\mathbf{a}), \mathbf{a})$ -локальный спектр, т. е. верно следующее

Следствие 5. Для любой вершины $\mathbf{a} \in \Gamma$ $(\Gamma^\perp(\mathbf{a}), \mathbf{a})$ -локальный спектр совершенного кода C однозначно определяется множеством кодовых вершин в грани Γ , т. е. множеством $C \cap \Gamma$.

Продолжим анализ формулы (2). В случае размерности исходной грани $k \leq (n-1)/2$ следствие 2 дает явное выражение для локального спектра в ортогональной к ней грани. В случае же $k \geq (n+1)/2$ мы не можем указать аналогичную формулу, однако именно этот факт дает возможность обнаружить внутренние связи в локальном спектре грани большой размерности.

Следствие 6. Пусть $\dim \Gamma = k \geq (n+1)/2$ и \mathbf{a} — произвольная вершина грани Γ . Тогда (Γ, \mathbf{a}) -локальный спектр совершенного кода для любой вершины $\mathbf{a} \in \Gamma$ однозначно определяется значениями своих первых $n-k+1$ компонент $v_0^{\mathbf{a}}(\Gamma), \dots, v_{n-k}^{\mathbf{a}}(\Gamma)$.

Доказательство. Зависимость спектра $v^{\mathbf{a}}(\Gamma^\perp)$ от $v^{\mathbf{a}}(\Gamma)$ описывается теоремой 1. Из того, что коэффициенты в разложении функции $f_\Gamma(x)$ по степеням x представляют собой $(\Gamma^\perp, \mathbf{a})$ -локальный спектр, следует, что эта функция является многочленом степени, не превосходящей $n-k$. В случае $k \geq (n+1)/2$ из формулы (2) вытекает, что функция $f_\Gamma(x)$ будет многочленом только тогда, когда многочлен

$$S(x) = \sum_{q=0}^k (-1)^q \Delta_q^{\mathbf{a}}(\Gamma) x^q$$

делится на многочлен $G(x) = (1-x)^{k-(n+1)/2} (1+x)^{k-(n-1)/2}$, т. е. по следствию 1

$$S(x) = G(x) \sum_{j=0}^{n-k} \Delta_j^{\mathbf{a}}(\Gamma^\perp) x^j. \quad (7)$$

Рассмотрим матрицу $P = (P_{qj})$ размера $k \times (n - k)$ такую, что элемент P_{qj} равен коэффициенту при x^{q-j} в многочлене $G(x)$, т. е.

$$P_{qj} = \begin{cases} p_{q-j}(k - (n + 1)/2; 2k - n) & \text{при } q \geq j, \\ 0 & \text{при } q < j. \end{cases}$$

Тогда из (7) следует, что

$$Ph = s, \quad (8)$$

где векторы $h = (h_0, h_1, \dots, h_{n-k})^T$ и $s = (s_0, s_1, \dots, s_k)^T$ таковы, что

$$h_j = \Delta_j^a(\Gamma^\perp), \quad 0 \leq j \leq n - k, \quad \text{и } s_q = (-1)^q \Delta_q^a(\Gamma), \quad 0 \leq q \leq k.$$

Заметим, что нижняя треугольная квадратная матрица $\tilde{P} = (P_{qj})$ размера $(n - k) \times (n - k)$, где $0 \leq q \leq n - k$ и $0 \leq j \leq n - k$, — невырожденная, так как все ее диагональные элементы равны 1. Поэтому, зная $v_0^a(\Gamma), \dots, v_{n-k}^a(\Gamma)$, а значит, и $\tilde{s} = (s_0, \dots, s_{n-k})$, из системы

$$\tilde{P}h = \tilde{s}$$

можно однозначно вычислить вектор h : $h = \tilde{P}^{-1}\tilde{s}$.

Отсюда и из системы (8) получим $s = P\tilde{P}^{-1}\tilde{s}$.

Следовательно, компоненты $v_{n-k+1}^a(\Gamma), \dots, v_k^a(\Gamma)$ (Γ, \mathbf{a}) -локального спектра однозначно вычисляются по компонентам $v_0^a(\Gamma), \dots, v_{n-k}^a(\Gamma)$. Следствие 6 доказано.

Автор выражает признательность С. В. Августиновичу и Ф. И. Соловьевой за постановку задачи и ценные замечания.

ЛИТЕРАТУРА

1. Васильев Ю. Л. О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Наука, 1962. Вып. 8. С. 337–339.
2. Васильева А. Ю. Спектральные свойства совершенных двоичных $(n, 3)$ -кодов // Дискрет. анализ и исслед. операций. 1995. Т. 2, № 2. С. 16–25.
3. Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А. Теория кодов, исправляющих ошибки. М.: Связь, 1979.
4. Пулатов А. К. К структуре плотно упакованных $(n, 3)$ -кодов // Методы дискретного анализа в теории кодов и схем: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1976. Вып. 29. С. 53–60.
5. Шапиро Г. С., Злотник Д. Л. К математической теории кодов с исправлением ошибок // Кибернетический сб. М.: Изд-во иностр. лит., 1962. Вып. 5. С. 7–32.

-
6. **Delsarte P.** Bounds for unrestricted codes by linear programming // Philips Res. Reports. 1972. V. 27. P. 272–289.
 7. **Etzion T., Vardy A.** Perfect binary codes: constructions, properties and enumeration // IEEE Trans. Inform. Theory. 1994. V. 40, N 3. P. 754–763.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск, Россия.
E-mail: vasilan@math.nsc.ru

Статья поступила

11 декабря 1997 г.,
переработанный вариант —
11 декабря 1998 г.