ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Октябрь—декабрь 2002. Серия 1. Том 9, № 4, 33–40

УДК 519.72

СИЛЬНАЯ ДИСТАНЦИОННАЯ ИНВАРИАНТНОСТЬ СОВЕРШЕННЫХ ДВОИЧНЫХ КОДОВ*)

А. Ю. Васильева

Введено понятие межвесового спектра кода, исследованы некоторые его свойства в случае совершенных двоичных кодов с расстоянием 3. Как следствие получено новое метрическое свойство совершенных двоичных кодов с расстоянием 3 — их сильная дистанционная инвариантность.

1. Постановка задачи и формулировка результата

Множество всех двоичных наборов длины n называется *n-мерным булевым кубом* (или *n-кубом*) и обозначается через E^n. Для двух вершин n-куба введем специальные обозначения: $(0,\dots,0)=\mathbf{0}$ и $(1,\dots,1)=\mathbf{1}$. *Расстоянием Хемминга* $\rho(\mathbf{x},y)$ между вершинами $\mathbf{x}$ и $\mathbf{y}$ из E^n называется число координат, в которых эти вершины различаются. *Весом Хемминга* $w(\mathbf{x})$ вершины $\mathbf{x}$ называется число ее ненулевых координат. Через W_i обозначается множество всех вершин веса i из n-куба. *Совершенным двоичным кодом с расстоянием* 3 называется такое множество C вершин из E^n, что шары радиуса 1 с центрами из C не пересекаются и в совокупности покрывают n-куб. В дальнейшем будем рассматривать только такие коды и их спектры.

Весовым спектром кода $C\subseteq E^n$ относительно вершины $\mathbf{a}\in E^n$ называется $(n+1)$-мерный вектор

$$v(\mathbf{a})=(v_0(\mathbf{a}),\dots,v_n(\mathbf{a})),$$

в котором i-я координата $(0\leqslant i\leqslant n)$ равна числу вершин кода C, находящихся на расстоянии i от вершины $\mathbf{a}$. Код C называется *дистанционно инвариантным*, если его весовые спектры относительно всех вершин кода совпадают. Известно, что совершенные коды являются дистанционно инвариантными [3, 5].

*) Исследование выполнено при финансовой поддержке Российского фонда фундаментальных исследований (проект 00–01–00822).

Теперь введем некоторые обобщения понятий весового спектра и дистанционной инвариантности. Пусть $\mathbf{a}$ — произвольная вершина n-куба. Обозначим через $T^d_{i,j}(\mathbf{a})$ число таких неупорядоченных пар $\{\mathbf{x},\mathbf{y}\}$ вершин кода C, что $\rho(\mathbf{a},\mathbf{x})=i$, $\rho(\mathbf{a},\mathbf{y})=j$ и $\rho(\mathbf{x},\mathbf{y})=d$. Назовем (i,j)-*весовым спектром* кода C относительно вершины $\mathbf{a}$ вектор

$$T_{i,j}(\mathbf{a})=(T^0_{i,j}(\mathbf{a}),\dots,T^n_{i,j}(\mathbf{a})).$$

Совокупность всех (i,j)-весовых спектров относительно вершины $\mathbf{a}$ будем называть *межвесовым спектром* кода относительно вершины $\mathbf{a}$. Код назовем *сильно дистанционно инвариантным,* если его межвесовые спектры относительно всех вершин кода совпадают.

В дальнейшем для краткости будем обозначать

$$v_i=v_i(\mathbf{0}),\quad T_{i,j}=T_{i,j}(\mathbf{0}).$$

Ключевой является следующая

Теорема 1. *Межвесовой спектр произвольного совершенного кода относительно нулевой вершины n-куба однозначно определяется величиной v_0.*

В качестве следствия из этой теоремы получаем основное утверждение.

Теорема 2. *Произвольный совершенный код является сильно дистанционно инвариантным.*

Поясним причины возникновения такой постановки задачи. Код C называется *дистанционно регулярным*, если выполнено следующее условие: если вершины $\mathbf{x},\mathbf{y}\in C$ находятся на расстоянии k, то число таких вершин $\mathbf{z}\in C$, что $\rho(\mathbf{x},\mathbf{z})=i$ и $\rho(\mathbf{y},\mathbf{z})=j$, зависит только от i, j, k и не зависит от выбора вершин $\mathbf{x}$ и $\mathbf{y}$. Все совершенные коды длины 15 и более не являются дистанционно регулярными [1]. Дистанционная регулярность является более сильным свойством, чем сильная дистанционная инвариантность. Действительно, рассмотрим такие тройки $\{\mathbf{a},\mathbf{b},\mathbf{c}\}$ вершин данного кода C, что $\rho(\mathbf{a},\mathbf{b})=i$, $\rho(\mathbf{a},\mathbf{c})=j$ и $\rho(\mathbf{a},\mathbf{b})=d$. Дистанционная регулярность кода C означает, что число $r^d_{ij}(\mathbf{a},\mathbf{b})$ таких троек кодовых вершин, у которых зафиксированы две вершины $\mathbf{a}$ и $\mathbf{b}$, не зависит от выбора этой пары вершин. По определению межвесового спектра

$$T^d_{i,j}(\mathbf{a})=\sum_{\mathbf{b}\in E^n,\ \rho(\mathbf{a},\mathbf{b})=i} r^d_{ij}(\mathbf{a},\mathbf{b}),$$

а независимость этих величин от выбора вершины $\mathbf{a}$ означает, что код C сильно дистанционно инвариантен.

Цель данной статьи состоит в установлении метрического свойства, промежуточного между дистанционной инвариантностью и дистанционной регулярностью, причем такого, что ему удовлетворяют все исследуемые коды.

2. Некоторые соотношения между компонентами локальных и межвесовых спектров

Сначала напомним некоторые понятия и факты, которые необходимы для дальнейшего изложения.

Множество всех вершин из n-куба, совпадающих в фиксированных $n-m$ координатах, называется *m-мерной гранью* n-куба.

Пусть γ — произвольная m-мерная грань и $\mathbf{x}$ — произвольная вершина из γ. *Локальным спектром кода C в грани γ относительно вершины* $\mathbf{x}$ называется $(m+1)$-мерный вектор, в котором i-я компонента $(0 \leqslant i \leqslant m)$ равна числу вершин кода C, лежащих в грани γ и находящихся на расстоянии i от вершины $\mathbf{x}$.

Пусть γ — m-мерная грань и $\gamma^{\perp}$ — $n-m$-мерная грань. Грани γ и $\gamma^{\perp}$ называются *ортогональными*, если множество координат, в которых совпадают все вершины из $\gamma^{\perp}$, является дополнением множества координат, в которых совпадают все вершины из γ. Ясно, что пересечение граней γ и $\gamma^{\perp}$ состоит из одной вершины, а сумма их размерностей равна n.

Для произвольной вершины $\mathbf{a} \in E^n$ через $\gamma_{\mathbf{a}}$ будем обозначать грань, состоящую из всех вершин, предшествующих вершине $\mathbf{a}$, а через $\gamma_{\mathbf{a}}^{\perp}$ — грань, состоящую из всех вершин, следующих за вершиной $\mathbf{a}$. Нетрудно понять, что грани $\gamma_{\mathbf{a}}$ и $\gamma_{\mathbf{a}}^{\perp}$ ортогональны и $\dim \gamma_{\mathbf{a}} = w(\mathbf{a})$. Обозначим через $l_i(\mathbf{a}), 0 \leqslant i \leqslant w(\mathbf{a})$, компоненты локального спектра кода C в грани $\gamma_{\mathbf{a}}$ относительно вершины $\mathbf{a}$, а через $l_i^{\perp}(\mathbf{a})$, $0 \leqslant i \leqslant n - w(\mathbf{a})$, — компоненты локального спектра кода C в грани $\gamma_{\mathbf{a}}^{\perp}$ относительно вершины $\mathbf{a}$.

Пусть N — натуральное число и $0 \leqslant i \leqslant N$. Пусть

$$p_i(t; N) = \sum_{j=0}^{i} (-1)^j \binom{t}{j} \binom{N-t}{i-j} -$$

многочлен от переменной t, называемый *многочленом Кравчука* (см., например, [4]), и обозначим

$$p_r^k = p_r\Big(\frac{n+1}{2} - k; n - 2k\Big).$$

В работе [2] была доказана следующая теорема, касающаяся связи локальных спектров совершенного кода в ортогональных гранях.

Теорема 3. *Пусть* $\mathbf{a} \in E^n$ *— произвольная вершина веса* k, $k \leqslant (n-1)/2$. *Тогда для любого* j, $0 \leqslant j \leqslant n-k$, *справедливо равенство*

$$l_j^{\perp}(\mathbf{a}) = \frac{1}{n+1}\binom{n-k}{j} + \sum_{q+r=j} (-1)^q p_r^k \left(l_q(\mathbf{a}) - \frac{1}{n+1}\binom{k}{q} \right). \qquad (1)$$

Теперь сформулируем и докажем три леммы о связи межвесового спектра совершенного кода с его весовым и локальными спектрами. В четвертой лемме (i,j)-весовой спектр будет выражен через (i',j')-весовые спектры, $i', j' \leqslant i$.

Лемма 1. *Пусть* $q \leqslant k$. *Тогда*

$$\sum_{\mathbf{a} \in W_k} l_q(\mathbf{a}) = \binom{n-k+q}{q} v_{k-q}. \qquad (2)$$

Доказательство. В левой части равенства (2) учитываются все вершины $\mathbf{x}$ кода C, имеющие вес $k-q$, их число равно v_{k-q}, при этом каждая такая вершина $\mathbf{x}$ учитывается столько раз, в скольких гранях $\gamma_{\mathbf{a}}$, $\mathbf{a} \in W_k$ она содержится. Число таких граней равно

$$|\{\mathbf{a} \in W_k \mid \mathbf{x} \in \gamma_{\mathbf{a}}\}| = |\{\mathbf{a} \in W_k \mid \mathbf{a} \in \gamma_{\mathbf{x}}^{\perp}\}| = \binom{n-k+q}{q}.$$

Лемма 1 доказана.

Лемма 2. *Пусть* $0 \leqslant k \leqslant i \leqslant j$. *Тогда*

$$\sum_{\mathbf{a} \in W_k} l_{i-k}^{\perp}(\mathbf{a}) l_{j-k}^{\perp}(\mathbf{a}) = \sum_{d=j-i}^{i+j-2k} \binom{(i+j-d)/2}{k} T_{i,j}^d. \qquad (3)$$

Доказательство. Нетрудно видеть, что в левой части равенства (3) учитываются, возможно, по нескольку раз, все такие пары $\{\mathbf{x},\mathbf{y}\}$ вершин совершенного кода C, что $\mathbf{x} \in W_i$, $\mathbf{y} \in W_j$ и $\rho(\mathbf{x},\mathbf{y}) \leqslant i+j-2k$. Ясно также, что $\rho(\mathbf{x},\mathbf{y}) \geqslant j-i$. Подсчитаем, сколько раз учитывается пара $\{\mathbf{x},\mathbf{y}\}$, если $\rho(\mathbf{x},\mathbf{y}) = d$, где $j-i \leqslant d \leqslant i+j-2k$. Поскольку в каждом слагаемом левой части (3) любая пара $\{\mathbf{x},\mathbf{y}\}$ учитывается не более одного раза, то надо определить число слагаемых, в которые дает ненулевой вклад эта пара, т. е. число $t_{\mathbf{x},\mathbf{y}}$ таких вершин $\mathbf{a} \in W_k$, что $\mathbf{x},\mathbf{y} \in \gamma_{\mathbf{a}}^{\perp}$. Обозначим через $\mathbf{b}(\mathbf{x},\mathbf{y})$ вершину максимального веса в пересечении граней $\gamma_{\mathbf{x}}$ и $\gamma_{\mathbf{y}}$. Нетрудно видеть, что $w(\mathbf{b}(\mathbf{x},\mathbf{y})) = (i+j-d)/2$. Поэтому

$$t_{\mathbf{x},y} = |\{\mathbf{a} \in W_k \mid \mathbf{x},\mathbf{y} \in \gamma_{\mathbf{a}}^{\perp}\}| = |\{\mathbf{a} \in W_k \mid \mathbf{b}(\mathbf{x},\mathbf{y}) \in \gamma_{\mathbf{a}}^{\perp}|$$
$$= |\{\mathbf{a} \in W_k \mid \mathbf{a} \in \gamma_{\mathbf{b}(\mathbf{x},\mathbf{y})}\}| = \binom{(i+j-d)/2}{k}.$$

Следовательно, формула (3) верна. Лемма 2 доказана.

Лемма 3. *Пусть* $0 \leqslant h \leqslant m \leqslant k$. *Тогда*

$$\sum_{\mathbf{a}\in W_k} l_h(\mathbf{a}) l_m(\mathbf{a}) = \sum_{d=m-h}^{h+m} \binom{n-(h+m-d)/2}{n-k} T^d_{k-h,k-m}. \tag{4}$$

Доказательство этой леммы мы не приводим, поскольку оно аналогично доказательству предыдущей леммы.

Теперь рассмотрим произвольный совершенный код и установим связь его (i,j)-весового спектра, где $0 \leqslant i \leqslant j \leqslant n$, с теми его (i',j')-весовыми спектрами, для которых $i', j' \leqslant i$. Для этого кроме лемм 1–3 будет существенно привлекаться аналитическая запись связи локальных спектров совершенного кода в ортогональных гранях. Грубо говоря, (i,j)-весовой спектр выражается через локальные спектры во всех гранях, содержащих вершину $\mathbf{1}$ и имеющих непустое пересечение с i-м и j-м уровнями n-куба. По теореме 3 о взаимосвязи локальных спектров в ортогональных гранях эти выражения записываются через локальные спектры в гранях, все вершины которых имеют вес, строго меньший i и j.

Для сокращения записи обозначим

$$\psi_{ik} = \frac{1}{n+1}\left(\binom{n-k}{i-k} + \sum_{q+r=i-k} (-1)^q p^k_r \binom{k}{q}\right),$$

$$v[k] = (v_0, v_1, \ldots, v_k) \quad \text{и} \quad T[i] = \left(T^d_{i',j'} \mid i', j' \leqslant i\right).$$

Лемма 4. *Пусть* $i \leqslant j$ *и* $i \leqslant (n-1)/2$. *Тогда для любого* k, $0 \leqslant k \leqslant i$,

$$\sum_{d=j-i}^{i+j-2k} \binom{(i+j-d)/2}{k} T^d_{i,j} = F_{ijk}\left(v[k], T[k]\right), \tag{5}$$

где $F_{ijk}\left(v[k], T[k]\right)$ — *некоторая линейная функция векторов* $v[k]$ *и* $T[k]$.

Доказательство. Согласно лемме 2 имеем

$$\sum_{d=j-i}^{i+j-2k} \binom{(i+j-d)/2}{k} T^d_{i,j} = \sum_{\mathbf{a}\in W_k} l^{\perp}_{i-k}(\mathbf{a}) l^{\perp}_{j-k}(\mathbf{a}). \tag{6}$$

Поскольку в правой части последнего равенства стоит сумма по всем вершинам веса k и по условию $k \leqslant i \leqslant (n-1)/2$, согласно теореме 3 компоненты локальных спектров в грани $\gamma_{\mathbf{a}}$ можно выразить через локальный спектр в грани $\gamma^{\perp}_{\mathbf{a}}$. По формуле (1) получаем, что последняя сумма равна

$$\sum_{\mathbf{a}\in W_k} \left(\psi_{ik} + \sum_{q+r=i-k} (-1)^q p^k_r l_q(\mathbf{a})\right)\left(\psi_{jk} + \sum_{Q+R=j-k} (-1)^Q p^k_R l_Q(\mathbf{a})\right).$$

Раскрывая скобки и меняя порядок суммирования, получаем:

$$\psi_{ik}\psi_{jk}\binom{n}{k} + \sum_{q+r=i-k}\sum_{Q+R=j-k}(-1)^{q+Q}p_r^k p_R^k \sum_{\mathbf{a}\in W_k} l_q(\mathbf{a})l_Q(\mathbf{a})$$
$$+ \psi_{jk}\sum_{q+r=i-k}(-1)^q p_r^k \sum_{\mathbf{a}\in W_k} l_q(\mathbf{a}) + \psi_{ik}\sum_{Q+R=j-k}(-1)^Q p_R^k \sum_{\mathbf{a}\in W_k} l_Q(\mathbf{a}).$$

Преобразовав с помощью лемм 1 и 3 стоящие в выражении суммы по множеству вершин веса k, приведем формулу к виду

$$\psi_{ik}\psi_{jk}\binom{n}{k} + \sum_{q+r=i-k}\sum_{Q+R=j-k}(-1)^{q+Q}p_r^k p_R^k$$
$$\times \sum_{t=|Q-q|}^{Q+q}\binom{n+(q+Q-t)/2}{n-k}T^t_{k-q,k-Q}$$
$$+ \psi_{jk}\sum_{q+r=i-k}(-1)^q p_r^k\binom{n-k+q}{q}v_{k-q}$$
$$+ \psi_{ik}\sum_{Q+R=j-k}(-1)^Q p_R^k\binom{n-k+Q}{Q}v_{k-Q} = F_{ijk}\left(v[k],T[k]\right).$$

Лемма 4 доказана.

3. Инвариантность межвесового спектра

Предварительно заметим, что для произвольной вершины $\mathbf{a}\in E^n$ величина $T^d_{i,j}(\mathbf{a})$ равна нулю, если числа $j-i$ и d имеют разную четность. Напомним, что для произвольного i, $0\leqslant i\leqslant n$, величина v_i определяется как число кодовых вершин веса i.

Доказательство теоремы 1. Надо доказать, что для произвольных целых i и j, $0\leqslant i,j\leqslant n$, (i,j)-весовой спектр совершенного кода зависит только от принадлежности коду нулевой вершины n-куба. Проведем доказательство индукцией по минимальному из чисел i и j. Предположим, что $i\leqslant j$. Без ограничения общности будем считать, что $i\leqslant(n-1)/2$, поскольку очевидно совпадение (i,j)- и $(n-j,n-i)$-весовых спектров совершенного кода.

Пусть $i=0$. Очевидно, что для произвольного j равенство $T^d_{0,j}=0$ справедливо в том случае, если $\mathbf{0}\notin C$, и

$$T^d_{0,j}(C) = \begin{cases} v_j, & \text{если } d=j,\\ 0, & \text{если } d\neq j,\end{cases} \text{ в случае, если } \mathbf{0}\in C.$$

Из теоремы Шапиро — Злотника следует, что величина v_j зависит только от v_0, т. е. факта принадлежности нулевой вершины коду. Следовательно, для $(0,j)$-весового спектра утверждение теоремы верно.

На i-м шаге предположим, что утверждение теоремы верно для всех (i', j')-весовых спектров при $i' < i$ (в частности, для $T[i-1]$ — «начального отрезка» межвесового спектра), и докажем, что оно выполняется для всех (i, j)-весовых спектров при $j \geqslant i$. При этом, в частности, получим, что утверждение выполняется для совокупности $T[i]$.

Сначала покажем, что утверждение теоремы выполняется для (i, i)-весового спектра. Ясно, что

$$T^0_{i,i} = v_i. \tag{7}$$

Пользуясь леммой 4, запишем равенства

$$\sum_{d=0}^{2(i-k)} \binom{i - d/2}{k} T^d_{i,i} = F_{iik}\left(v[k], T[k]\right), \quad i - 1 \geqslant k \geqslant 0. \tag{8}$$

Система (7), (8) из $i+1$ линейных алгебраических уравнений с $i+1$ неизвестными $T^d_{i,i}$, где d четно и $0 \leqslant d \leqslant 2i$, разрешима, поскольку существуют совершенные коды. Решение этой системы единственно, поскольку матрица системы треугольная с диагональными элементами, равными единице. Рассмотрим правую часть этой системы. По предположению индукции все (i', j')-весовые спектры при $i', j' \leqslant i-1$, являются функциями от v_0 (а значит, и все $T[k]$ при $k < i$). Поскольку все компоненты весового спектра совершенного кода тоже зависят только от принадлежности коду нулевой вершины куба, правые части уравнений этой системы однозначно определяются значением v_0. Для произвольного четного d число $T^d_{i,i}$ является функцией от правых частей системы уравнений (7), (8), а следовательно, зависит только от v_0. Так как $T^d_{i,i} = 0$ при нечетном d, то (i, i)-весовой спектр однозначно определяется фактом принадлежности нулевой вершины куба данному кубу.

Теперь можно перейти к случаю $j > i$. Для доказательства теоремы в этом случае надо рассмотреть систему $i+1$ линейных алгебраических уравнений относительно $i+1$ неизвестных $T^d_{i,j}$, где $j - i \leqslant d \leqslant i + j - 2k$ и $d \equiv (j-i) \bmod 2$,

$$\sum_{d=j-i}^{i+j-2k} \binom{(i+j-d)/2}{k} T^d_{i,j} = F_{ijk}\left(v[k], T[k]\right), \quad 0 \leqslant k \leqslant i,$$

и почти дословно повторить предыдущие рассуждения. Для этого надо заметить, что система имеет решение, притом единственное, а правые части уравнений зависят только от весового спектра кода, однозначно определяемого величиной v_0, и совокупности $T[i]$, т. е. тех (i', j')-весовых спектров, для которых утверждение теоремы выполнено в силу доказанного выше и предположения индукции. В результате получаем, что (i, j)-весовой спектр совершенного кода для произвольного $j > i$ зависит только от v_0.

Итак, (i,j)-весовой спектр совершенного кода C для произвольного j, $j \geqslant i$, однозначно определяется величиной v_0. Теорема 1 доказана.

Рассматривая для произвольной вершины $\mathbf{a} \in E^n$ код $C \oplus \mathbf{a}$ и его межвесовой спектр относительно нулевой вершины, из теоремы 1 получаем

Следствие 1. *Межвесовой спектр произвольного совершенного кода относительно произвольной вершины* $\mathbf{a} \in E^n$ *однозначно определяется величиной* $v_0(\mathbf{a})$.

Непосредственно из этого утверждения, а также из определения сильной дистанционной инвариантности следует

Теорема 4. *Произвольный совершенный код является сильно дистанционно инвариантным.*

Изложенные в статье результаты были анонсированы в [6].

Автор выражает глубокую признательность С. В. Августиновичу за постановку задачи и полезные обсуждения результатов. Автор также благодарит рецензента за замечания, позволившие улучшить изложение.

ЛИТЕРАТУРА

1. **Августинович С. В., Соловьева Ф. И.** О дистанционной регулярности совершенных двоичных кодов // Проблемы передачи информации. 1998. Т. 34, вып. 3. С. 247–249.
2. **Васильева А. Ю.** Локальные спектры совершенных двоичных кодов // Дискрет. анализ и исслед. операций. Сер. 1. 1999. Т. 6, № 1. С. 3–11.
3. **Ллойд С. П.** Бинарное блочное кодирование // Кибернетический сб. М.: Изд-во иностр лит., 1960. Вып. 1. С. 206–226.
4. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
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. **Vassilieva A. Yu.** Local and interweight spectra of perfect binary codes // Proc. of Intern. Sympos. on Information Theory ISIT-2000. Sorrento, Italy, 2000. P. 474.

Адрес автора:

Институт математики
им. С. Л. Соболева СО РАН,
пр. Академика Коптюга, 4,
630090 Новосибирск,
Россия

Статья поступила
7 марта 2002 г.