

О РАССТОЯНИЯХ МЕЖДУ СОВЕРШЕННЫМИ ДВОИЧНЫМИ КОДАМИ

А. Ю. Васильева

Вводится понятие расстояния между двумя совершенными двоичными кодами и устанавливается нижняя оценка для этой величины, выражающаяся через разность количеств их вершин в произвольной k -мерной грани n -мерного куба. Доказано, что оценки являются достижимыми в случаях $k = 0$ и $k = (n - 1)/2$ (первая из них была получена в [4]).

Введение

Для описания всех совершенных двоичных кодов представляется важным изучение следующего вопроса: как различаются два кода во всем кубе, если известно, насколько они различаются в некоторой грани куба. В п. 1 вводится расстояние между двумя совершенными кодами и устанавливается нижняя оценка для расстояния между двумя кодами, если известны количества вершин из каждого кода в некоторой k -мерной грани куба (теорема 1).

Из этой теоремы при $k = 0$ вытекает достижимая оценка для расстояния двух различных кодов [4]. Эта оценка приводится в п. 2 (следствие 2) вместе с другим случаем теоремы 1 (следствие 3), который дает достижимую оценку расстояния между кодами при условии, что известно число вершин каждого кода в некоторой $(n - 1)/2$ -мерной грани.

1. Основной результат

Ниже используются следующие обозначения и понятия:

- n -мерный единичный куб (n -куб) — множество всех двоичных векторов длины n ;
- $\rho(\mathbf{x}, \mathbf{y}) = \sum_{i=1}^n |x_i - y_i|$ — расстояние Хемминга между вершинами \mathbf{x} и \mathbf{y} из E^n ;
- совершенный двоичный код длины $n = 2^m - 1$ — такое подмножество S вершин из E^n , что шары радиуса 1 с центрами из S

образуют разбиение n -куба (слово «двоичный» далее будем опускать);

- k -мерная грань n -куба — множество всех таких вершин из E^n , у которых $n - k$ координат фиксированы;
- $p_i(x; N) = \sum_{j=0}^i (-1)^j \binom{x}{j} \binom{N-x}{i-j}$ — многочлен Кравчука (см., например, [3]), где N — натуральное число и $0 \leq i \leq N$.

Пусть C_1 и C_2 — совершенные коды длины n . Величину

$$d(C_1, C_2) = |(C_1 \setminus C_2) \cup (C_2 \setminus C_1)| = 2|(C_1 \setminus C_2)|$$

назовем *расстоянием между кодами* C_1 и C_2 . Нетрудно проверить, что на множестве всех пар совершенных кодов длины n функция d удовлетворяет всем аксиомам расстояния.

Зафиксируем целое число k , $0 \leq k \leq n$. Обозначим через Γ^k произвольную k -мерную грань n -куба. Для данной пары совершенных кодов C_1 и C_2 обозначим

$$h(\Gamma^k) = ||C_1 \cap \Gamma^k| - |C_2 \cap \Gamma^k||.$$

Теорема 1. Если C_1 и C_2 — совершенные коды и $k \leq (n-1)/2$, то

$$d(C_1, C_2) \geq h(\Gamma^k) \sum_{i=0}^{n-k} \left| p_i \left(\frac{n+1}{2}; n-k \right) \right|. \quad (1)$$

Доказательство. Обозначим через $v^{(j)} = (v_0^{(j)}, v_1^{(j)}, \dots, v_{n-k}^{(j)})$ граневой спектр совершенного кода C_j , $j = 1, 2$, где по определению из [2]

$$v_i^{(j)} = \left| \left\{ \mathbf{x} \in C_j \mid \min_{\mathbf{y} \in \Gamma^k} \rho(\mathbf{x}, \mathbf{y}) = i \right\} \right|.$$

Очевидно, что

$$d(C_1, C_2) \geq \sum_{i=0}^{n-k} \left| v_i^{(1)} - v_i^{(2)} \right|. \quad (2)$$

В [2] доказано, что если $k \leq (n-1)/2$, то для любого i , $0 \leq i \leq n-k$, и $j = 1, 2$

$$v_i^{(j)} = \frac{2^k}{n+1} \binom{n-k}{i} + \left(v_0^{(j)} - \frac{2^k}{n+1} \right) p_i \left(\frac{n+1}{2}; n-k \right).$$

Следовательно,

$$v_i^{(1)} - v_i^{(2)} = (v_0^{(1)} - v_0^{(2)}) p_i \left(\frac{n+1}{2}; n-k \right). \quad (3)$$

Подставляя (3) в (2) и учитывая, что $|v_0^{(1)} - v_0^{(2)}| = h(\Gamma^k)$, получаем (1). Теорема 1 доказана.

Из теоремы 1 непосредственно вытекает

Следствие 1. Если C_1 и C_2 — совершенные коды, то

$$d(C_1, C_2) \geq \max_{0 \leq k \leq (n-1)/2} \left\{ \left(\max_{\Gamma^k \in E^n} h(\Gamma^k) \right) \sum_{i=0}^{n-k} \left| p_i \left(\frac{n+1}{2}; n-k \right) \right| \right\}.$$

2. Два частных случая

Первое из дальнейших утверждений (следствие 2) было получено в [4] в терминах пересечений совершенных кодов. Ясно, что если C_1 и C_2 — совершенные коды, то

$$d(C_1, C_2) + 2|C_1 \cap C_2| = |C_1| + |C_2| = 2^{n+1}/(n+1).$$

Следствие 2 [4]. Если C_1 и C_2 — различные совершенные коды, то

$$d(C_1, C_2) \geq 2^{(n+1)/2}. \quad (4)$$

Доказательство. Условие $C_1 \neq C_2$ означает, что существует такая нульмерная грань $\Gamma^0 = \{a\}$, что $h(\Gamma^0) = 1$. В формуле (1) положим $k = 0$. Поскольку

$$\sum_{i=0}^N p_i(x; N) z^i = (1-z)^x (1+z)^{N-x},$$

то при любом t , $0 \leq t \leq (n-1)/2$,

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

Значит,

$$d(C_1, C_2) \geq 2 \sum_{t=0}^{(n-1)/2} \binom{(n-1)/2}{t} = 2^{(n+1)/2}.$$

Следствие 2 доказано.

Следствие 3. Если C_1 и C_2 — совершенные коды и $k = (n-1)/2$, то

$$d(C_1, C_2) \geq h(\Gamma^{(n+1)/2}) 2^{(n+1)/2}. \quad (5)$$

Доказательство. Ясно, что для любого i , $0 \leq i \leq (n-1)/2$,

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

Значит,

$$d(C_1, C_2) \geq h(\Gamma^{(n+1)/2}) \sum_{i=0}^{(n+1)/2} \binom{(n+1)/2}{i} = h(\Gamma^{(n+1)/2}) 2^{(n+1)/2}.$$

Следствие 3 доказано.

В [4] установлено, что оценка (4) достижима. В [5] для любого натурального числа h , $0 \leq h \leq 2^{(n+1)/2}/(n+1)$, указаны такие совершенные коды C_1^* и C_2^* , что

$$d(C_1^*, C_2^*) = h 2^{(n+1)/2}. \quad (6)$$

Покажем, что на этих кодах достигается оценка (5), т. е. существует такая $(n-1)/2$ -мерная грань Γ , что $h = h(\Gamma)$.

Для произвольных $\mathbf{a} = (a_1, \dots, a_q)$ и $\mathbf{b} = (b_1, \dots, b_r)$ будем обозначать $(\mathbf{a}, \mathbf{b}) = (a_1, \dots, a_q, b_1, \dots, b_r)$ и $|\mathbf{a}| = a_1 \oplus a_2 \oplus \dots \oplus a_q$.

Пусть C_0 — произвольный совершенный код длины $n_0 = (n-1)/2$ и λ — произвольная булева функция на нем. Положим

$$C(\lambda) = \{(\mathbf{x}, \mathbf{x} \oplus \mathbf{y}, |\mathbf{x}| \oplus \lambda(\mathbf{y})) \mid \mathbf{x} \in E^{n_0}, \mathbf{y} \in C_0\}.$$

В [1] установлено, что $C(\lambda)$ является совершенным кодом длины n .

Пусть A — h -элементное подмножество вершин кода C_0 . Положим

$$C_1^* = C(\lambda_1), \quad C_2^* = C(\lambda_2),$$

где

$$\lambda_1 \equiv 0, \quad \lambda_2(\mathbf{y}) = \begin{cases} 1, & \text{если } \mathbf{y} \in A; \\ 0, & \text{если } \mathbf{y} \in C_0 \setminus A. \end{cases}$$

Рассмотрим $(n-1)/2$ -мерную грань

$$\Gamma = \{(\mathbf{0}, \mathbf{y}, 0) \mid \mathbf{y} \in E^{n_0}\} (\mathbf{0} = (0, \dots, 0) \in E^{n_0}).$$

Тогда

$$h(\Gamma) = \left| |\{(\mathbf{0}, \mathbf{y}, 0) \mid \mathbf{y} \in C_0\}| - |\{(\mathbf{0}, \mathbf{y}, 0) \mid \mathbf{y} \in C_0 \setminus A\}| \right| = |A|.$$

Пользуясь определением расстояния между кодами, находим

$$\begin{aligned} d(C_1^*, C_2^*) &= \left| \{(\mathbf{x}, \mathbf{x} \oplus \mathbf{y}, |\mathbf{x}| \oplus \delta) \mid \mathbf{x} \in E^{n_0}, \mathbf{y} \in A, \delta \in \{0, 1\}\} \right| \\ &= 2|A| 2^{(n-1)/2} = h(\Gamma) 2^{(n+1)/2}. \end{aligned}$$

Значит, для совершенных кодов C_1^* и C_2^* справедливо $h = h(\Gamma)$ и (6).

Автор выражает признательность С. В. Августиновичу за постановку задачи и обсуждение результатов и Ф. И. Соловьевой за 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. **Etzion T., Vardy A.** Perfect binary codes: constructions, properties and enumeration // IEEE Trans. Inform. Theory. 1994. V. 40, N 3. P. 754–763.
5. **Etzion T., Vardy A.** On perfect codes and tilings: problems and solutions // SIAM J. Discrete Math. 1998. V. 11, N 2. P. 205–223.

Адрес автора:

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

Статья поступила
5 мая 1998 г.