ДИСКРЕТНЫЙ АНАЛИЗ И ИССЛЕДОВАНИЕ ОПЕРАЦИЙ
Апрель—июнь 1995. Том 2, № 2, 16–25

УДК 519.72

СПЕКТРАЛЬНЫЕ СВОЙСТВА СОВЕРШЕННЫХ ДВОИЧНЫХ $(n,3)$-КОДОВ

А. Ю. Васильева

Для произвольного совершенного двоичного $(n,3)$-кода рассматривается распределение кодовых вершин по членам некоторых разбиений n-мерного единичного куба. Основное внимание уделяется случаю, относящемуся к множеству параллельных граней одинаковой размерности. На этой основе исследуется граневое строение дополнения к коду, и в этих терминах устанавливаются два характеристических свойства нелинейных кодов.

В работе исследуется строение совершенных (плотно упакованных) двоичных $(n,3)$-кодов (т. е. кодов длины n с расстоянием 3), строение которых, как известно, обладает большой симметрией. В частности, согласно свойству, найденному Г. С. Шапиро и Д. Л. Злотником [1], весовые спектры всех совершенных $(n,3)$-кодов, которым принадлежит нулевая вершина куба, совпадают. Известно также, что кодовые вершины равномерно распределены по граням большой размерности. В случае произвольного q-ичного кода П. Дельсартом [2, 3] найден минимальный размер граней с этим свойством. Позднее А. К. Пулатов [4] независимо установил такой размер для q-ичных ($q = 2, 3, \dots$) совершенных $(n,3)$-кодов.

В § 1 сформулировано и доказано обобщение теоремы Шапиро — Злотника, а его частный случай, относящийся к распределению кодовых вершин по граням, рассмотрен в § 2. Из полученного результата вытекает простое новое доказательство теоремы Дельсарта — Пулатова (§ 2).

Кроме того, обобщение оказалось полезным для изучения вопроса о строении множества граней дополнения к коду. В § 3 выяснено, что свойства кода Хэмминга [5], относящиеся к таким граням, присущи только этому коду, и, таким образом, установлены признаки, по которым можно разграничивать множества линейных и нелинейных совершенных кодов.

§ 1. Обобщение теоремы Шапиро — Злотника

Предварительно введем следующие обозначения и понятия:

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

— число единичных компонент вектора $\mathbf{x}$ обозначается $w(\mathbf{x})$ и называется *весом* вершины $\mathbf{x}$;

— $\rho(\mathbf{x}, \mathbf{y}) = \Sigma|x_i - y_i|$ — расстояние между вершинами $\mathbf{x}$ и $\mathbf{y}$;

— $S_i^n(\mathbf{x}) = \{\mathbf{y} \in E^n \mid \rho(\mathbf{x}, \mathbf{y}) = i\}$ — n-мерная сфера радиуса i с центром в вершине $\mathbf{x} \in E^n$;

— произвольный совершенный двоичный (далее слово «двоичный» будем опускать) $(n,3)$-код C — это такое подмножество вершин из E^n, находящихся друг от друга на расстоянии не менее 3, что множество шаров радиуса 1 с центрами из C покрывает куб.

Пусть $A_0, A_1, \dots, A_p$ — произвольная система попарно не пересекающихся подмножеств из E^n, причем $A_0 \cup \dots \cup A_p = E^n$. Систему множеств $\{A_i\}$ назовем *расслоением*, множества A_i — *слоями*, а множество A_0 — *начальным слоем* в E^n, если

$$A_i = \{\mathbf{x} \in E^n \mid \rho(\mathbf{x}, A_0) = i\} \quad \text{при любом} \quad i,\ i \leqslant i \leqslant p,$$

где $\rho(\mathbf{x}, A_0) = \min\limits_{\mathbf{y} \in A_0} \rho(\mathbf{x}, \mathbf{y})$.

Обозначим через a_i мощность слоя A_i, а через v_i — число кодовых вершин в слое A_i, т. е. $a_i = |A_i|$ и $v_i = |A_i \cap C|$. Вектор $(v_0, v_1, \dots, v_p)$ назовем *спектром* кода C относительно расслоения $\{A_i\}$.

Расслоение $\{A_i\}$ назовем *правильным*, если

а) при любом i, $0 \leqslant i \leqslant p$, для любых вершин $\mathbf{x}, \mathbf{y} \in A_i$ справедливо равенство $|S_1^n(\mathbf{x}) \cap A_i| = |S_1^n(\mathbf{y}) \cap A_i| =: k_i$;

б) при любом i, $0 \leqslant i \leqslant p-1$, для любых вершин $\mathbf{x}$, $\mathbf{y} \in A_i$ справедливо равенство $|S_1^n(\mathbf{x}) \cap A_{i+1}| = |S_1^n(\mathbf{y}) \cap A_{i+1}| =: u_i$.

В этих терминах утверждение Шапиро — Злотника можно сформулировать следующим образом.

Пусть $\mathbf{x}$ — некоторая вершина совершенного $(n,3)$-кода C и $\{A_i\}$ — такое правильное расслоение куба E^n, что $A_0 = \{\mathbf{x}\}$. Тогда спектр кода C относительно расслоения $\{A_i\}$ не зависит ни от выбора вершины $\mathbf{x}$, ни от выбора кода C.

Это утверждение допускает следующее обобщение на случай произвольного правильного расслоения.

Теорема 1. *Спектр любого совершенного $(n,3)$-кода относительно правильного расслоения куба E^n однозначно определяется числом кодовых вершин, принадлежащих начальному слою.*

Доказательство. Пусть C — совершенный $(n,3)$-код, $\{A_i\}$ — правильное расслоение куба E^n и $v_0 = \tilde{v}$. Зафиксируем произвольное i, $1 \leqslant i \leqslant p-1$.

Заметим, что при любом $\mathbf{x} \in A_i$ справедливо включение $S_1^n(\mathbf{x}) \subset A_{i-1} \cup A_i \cup A_{i+1}$. Кроме того, из определения правильного расслоения непосредственно следует, что каждая вершина $\mathbf{x} \in A_i$ имеет фиксированное число соседних вершин, принадлежащих слою A_{i-1}; это число равно $d_i = n - k_i - u_i$.

Для любой вершины $\mathbf{x} \in A_i$ выполняется одно из следующих условий, причем в каждом случае нетрудно подсчитать число таких вершин.

1. $\mathbf{x} \in C$. Число вершин равно v_i.

2. Вершина $\mathbf{x}$ не является кодовой и находится на расстоянии 1 от некоторой кодовой вершины из этого же слоя. Нетрудно проверить, что число вершин, удовлетворяющих этому условию, равно $v_i k_i$.

3. Вершина $\mathbf{x}$ не является кодовой и находится на расстоянии 1 от некоторой кодовой вершины из слоя A_{i-1}. Число таких вершин равно $v_{i-1}u_{i-1}$.

4. Вершина $\mathbf{x}$ не является кодовой и находится на расстоянии 1 от некоторой кодовой вершины из слоя A_{i+1}. Число таких вершин равно $v_{i+1}d_{i+1}$.

Таким образом,

$$a_i = v_i + v_i k_i + v_{i-1}u_{i-1} + v_{i+1}d_{i+1} = u_{i-1}v_{i-1} + (k_i + 1)v_i + d_{i+1}v_{i+1}.$$

Это равенство справедливо при любом i, $1 \leqslant i \leqslant p - 1$.

При $i = 0$ и $i = p$ соотношения для a_i принимают вид

$$a_0 = (k_0 + 1)v_0 + d_1 v_1, \quad a_p = u_{p-1}v_{p-1} + (k_p + 1)v_p.$$

В результате получаем следующую систему уравнений с неизвестными $v_0, v_1, \ldots, v_p$:

$$\begin{cases} a_0 = (k_0 + 1)v_0 + d_1 v_1; \\ a_i = u_{i-1}v_{i-1} + (k_i + 1)v_i + d_{i+1}v_{i+1}, \quad 1 \leqslant i \leqslant p - 1; \\ a_p = u_{p-1}v_{p-1} + (k_p + 1)v_p. \end{cases} \tag{1}$$

Кроме того, $v_0 = \tilde{v}$. Поэтому система (1) фактически является системой из $p + 1$ уравнений с p неизвестными. Она имеет решение, так как существует совершенный $(n, 3)$-код C, спектр которого удовлетворяет этой системе. Легко видеть, что это решение единственное. Итак, каков бы ни был совершенный $(n, 3)$-код, его спектр относительно правильного расслоения определяется числом кодовых вершин, принадлежащих начальному слою. Теорема 1 доказана.

§ 2. Граневой спектр совершенного $(n, 3)$-кода

Зафиксируем целое число k, $0 \leqslant k \leqslant n$, и пусть $m = n - k$. Пусть Γ — произвольная грань размерности k из E^n. Семейство всех граней размерности k, параллельных Γ, обозначим через $F(\Gamma)$. Пусть $A_0 = \Gamma$ и множество A_i состоит из граней семейства $F(\Gamma)$, находящихся на расстоянии i от грани Γ, т. е.

$$A_i = \cup\{\Gamma' \in F(\Gamma) \mid \rho(\Gamma, \Gamma') = i\}, \quad 0 \leqslant i \leqslant p,$$

где $\rho(A, B) := \min\limits_{x \in A,\, y \in B} \rho(\mathbf{x}, \mathbf{y})$.

Лемма 1. *Система множеств $\{A_i\}$ является правильным расслоением.*

Доказательство. Из определения расслоения непосредственно следует, что $\{A_i\}_{i=0}^{p}$ — расслоение, причем $p = m$.

Теперь выясним, что расслоение $\{A_i\}$ правильное. Действительно, для любых i и $\mathbf{x} \in A_i$ имеем $k_i = |A_i \cap S_1^n(\mathbf{x})| = k$ и $u_i = m - i$. Лемма 1 доказана.

Правильное расслоение $\{A_i\}_{i=0}^{m}$, определенное выше, назовем *граневым*, грань $\Gamma = A_0$ — *начальной гранью* и спектр $(v_0, \dots, v_p)$ совершенного $(n, 3)$-кода относительно такого расслоения — *граневым спектром* кода.

Следствие. *Граневой спектр произвольного совершенного $(n, 3)$-кода определяется числом вершин, принадлежащих начальной грани.*

Заметим, что в случае граневого расслоения $|A_i| = \binom{m}{i} 2^k$ и $d_i = n - k_i - u_i = i$. Тогда из леммы 1 и формул (1) получаем систему линейных уравнений

$$\begin{cases} 2^k = (k+1)v_0 + v_1; \\ 2^k \binom{m}{i} = (m - i + 1)v_{i-1} + (k+1)v_i + (i+1)v_{i+1}, \quad 1 \leqslant i \leqslant m - 1; \\ 2^k = v_{m-1} + (k+1)v_m. \end{cases} \tag{2}$$

Теорема 2. *Пусть C — совершенный $(n, 3)$-код, $\{A_i\}$ — граневое расслоение куба E^n и v_0 — число кодовых вершин, принадлежащих начальному слою. Тогда граневой спектр кода C относительно граневого расслоения $\{A_i\}$ задается коэффициентами разложения в степенной ряд функции*

$$p(x) = \frac{2^k}{n+1}(1 - x)^m + \left(v_0 - \frac{2^k}{n+1}\right)(1 + x)^{(n-1)/2-k}(1 - x)^{(n+1)/2}. \tag{3}$$

Доказательство. Пусть

$$p(x) = \sum_{j=0}^{m} v_j x^j$$

— производящая функция системы (2). Введя дополнительно v_{-1}, v_{m+1}, v_{m+2}, $\binom{m}{m+1}$ и положив их равными нулю, перепишем систему (2):

$$(m-i+1)v_{i-1}+(k+1)v_i+(i+1)v_{i+1}=2^k\binom{m}{i}, \quad 0\leqslant i\leqslant m+1. \quad (4)$$

Тогда функцию $p(x)$ можно записать в виде

$$p(x)=\sum_{j=0}^{m+1} v_j x^j,$$

а ее производную — в виде

$$p'(x)=\sum_{j=0}^{m+1} j v_j x^{j-1}=\sum_{j=1}^{m} j v_j x^{j-1}.$$

Умножая i-е уравнение системы (4) на x^i и суммируя уравнения по i, получаем

$$m\sum_{i=0}^{m+1} v_{i-1}x^i-\sum_{i=0}^{m+1}(i-1)v_{i-1}x^i \\ +(k+1)\sum_{i=0}^{m+1} v_i x^i+\sum_{i=0}^{m+1}(i+1)v_{i+1}x^i=2^k\sum_{i=0}^{m+1}\binom{m}{i}x^i.$$

Тогда

$$mxp(x)-x^2p'(x)+(k+1)p(x)+p'(x)=2^k(1+x)^m,$$
$$p'(x)=\frac{mx+k+1}{x^2-1}p(x)+\frac{2^k(1+x)^m}{1-x^2}. \quad (5)$$

Таким образом, решение алгебраической системы (2) свелось к решению линейного дифференциального уравнения (5) с начальным условием $p(0)=v_0$.

Решая задачу Коши (например, интегрируя это уравнение методом вариации произвольной постоянной [6]), получаем, что функция $p(x)$ имеет указанный вид и коэффициенты ее разложения представляют собой граневой спектр. Теорема 2 доказана.

Из теоремы 2 следует

Теорема Дельсарта — Пулатова для совершенных $(n,3)$-кодов. *Пусть C — совершенный $(n,3)$-код и $k\geqslant(n+1)/2$. Тогда в любой k-мерной грани из E^n содержится $2^k/(n+1)$ кодовых вершин.*

Доказательство. Пусть Γ — произвольная грань размерности k из E^n. Рассмотрим граневое расслоение $\{A_i\}_{i=0}^{n-k}$ такое, что $A_0 = \Gamma$. Тогда числа $v_i = |C \cap A_i|$ есть коэффициенты функции $p(x)$ из формулы (3). Так как число слоев равно $n-k$, то $p(x)$ — многочлен степени, не превосходящей $n-k$.

Предположим, что $|C \cap \Gamma| \neq 2^k/(n+1)$, т. е. $v_0 - 2^k/(n+1) \neq 0$. Тогда из (3) следует, что $p(x)$ не является многочленом, так как $(1+x)^{(n-1)/2-k}$ — дробно-рациональная функция, разлагающаяся в бесконечный ряд по степеням x. Противоречие. Значит, $|C \cap \Gamma| = 2^k/(n+1)$. Теорема доказана.

Таким образом, установлен граневой спектр произвольного совершенного $(n,3)$-кода в случае $k \geqslant (n+1)/2$. Кроме того, из формулы (3) можно получить явную формулу для граневого спектра в случае меньших размерностей начальной грани.

Следствие теоремы 2. *Пусть $k \leqslant (n-1)/2$ и начальная грань граневого расслоения имеет размерность k. Тогда граневой спектр любого совершенного $(n,3)$-кода имеет вид*

$$v_i = \frac{2^k}{n+1}\binom{n-k}{i} + \left(v_0 - \frac{2^k}{n+1}\right) \times \sum_{j+l=i} (-1)^l \binom{(n-1)/2-k}{j}\binom{(n+1)/2}{l}, \quad 1 \leqslant i \leqslant n-k. \qquad (6)$$

§ 3. К строению дополнений совершенных $(n,3)$-кодов

Пусть $f(\mathbf{x})$ — булева функция на кубе E^n и Γ — k-мерная грань. Как обычно, грань Γ будем называть *максимальной* (нерасширяемой) гранью функции $f(\mathbf{x})$, если $f(\mathbf{x}) = 1$ для любой вершины $\mathbf{x} \in \Gamma$ и в любой $(k+1)$-мерной грани $\Gamma' \supset \Gamma$ существует такая вершина $\mathbf{y} \in \Gamma'$, что $f(\mathbf{y}) = 0$.

Пусть $C \subseteq E^n$ — совершенный $(n,3)$-код. Обозначим через D_C дополнение к коду C и через $d_C(\mathbf{x})$ — характеристическую функцию множества D_C, т. е.

$$D_C = E^n \setminus C, \quad d_C(\mathbf{x}) = \begin{cases} 1, & \mathbf{x} \in D_C, \\ 0, & \mathbf{x} \in C. \end{cases}$$

Доказательство утверждений § 3 основано на разбиении куба E^n на такие граневые слои, что начальной гранью является некоторая максимальная грань функции $d_C(\mathbf{x})$.

Лемма 2. *Пусть $n > 3$ и k-мерная грань Γ — максимальная грань функции $d_C(\mathbf{x})$. Тогда $\log(n+1) \leqslant k \leqslant (n-1)/2$.*

Здесь и далее log означает логарифм по основанию 2.

Доказательство. Неравенство $k \leqslant (n-1)/2$ непосредственно следует из теоремы Дельсарта — Пулатова.

Покажем, что $k \geqslant \log(n+1)$. Рассмотрим граневое расслоение $\{A_i\}$ с начальной гранью Γ: $A_0 = \Gamma$. Грани, параллельные Γ и соседние с ней, образуют первый слой A_1. Число таких граней равно $n-k$. Поскольку Γ является максимальной гранью функции $d_C(\mathbf{x})$, в каждой соседней грани содержится хотя бы одна кодовая вершина, а значит, $v_1 \geqslant n-k$. Кроме того, из первого уравнения системы (2) следует, что $v_1 = 2^k - (k+1)v_0 = 2^k$ (так как $v_0 = 0$). Поэтому $n - k \leqslant 2^k$, откуда нетрудно получить неравенство $k \geqslant \log(n+1)$. Лемма 2 доказана.

Далее будем предполагать, что нулевая вершина куба E^n принадлежит коду C.

Пусть Γ — k-мерная грань. Число кодовых вершин в этой грани не превосходит $2^k/(k+1)$. Будем говорить, что вершины кода C *плотно упакованы в грани* Γ, если Γ покрывается шарами радиуса 1 с центрами из множества $C \cap \Gamma$. Легко видеть, что в этом и только в этом случае $|\Gamma \cap C| = 2^k/(k+1)$.

Лемма 3. *Пусть C — совершенный $(n,3)$-код, $\mathbf{0} \in C$, Γ — максимальная грань функции $d_C(\mathbf{x})$, размерность грани Γ равна k, $m = n-k$; $\{A_i\}$ — такое граневое расслоение, что $A_0 = \Gamma$; $\{B_i\}$ — такое граневое расслоение, что $B_0 \in F(\Gamma)$ и $\mathbf{0} \in B_0$.*

Тогда эквивалентны следующие утверждения:

(a) *$k = (n-1)/2$;*

(b) *четные слои $\{A_i\}$ целиком лежат в множестве D_C, а нечетные слои состоят из граней $\Gamma' \in F(\Gamma)$, в которых плотно упакованы вершины кода C;*

(c) *нечетные слои $\{B_i\}$ целиком лежат в множестве D_C, а четные слои состоят из граней $\Gamma' \in F(\Gamma)$, в которых плотно упакованы вершины кода C;*

(d) *$A_2 \cap C = \varnothing$.*

Доказательство. 1. Докажем, что (a) $\Rightarrow$ (b). Из формул (6) получаем, что граневой спектр $(v_0, \ldots, v_m)$ кода C относительно расслоения $\{A_i\}$ имеет следующий вид (так как $v_0 = 0$):

$$v_{2r} = 0, \quad v_{2r-1} = \frac{2^k}{k+1}\binom{m}{2r-1}, \quad r = 1, 2, \ldots, (n+1)/4.$$

Число граней из семейства $F(\Gamma)$, образующих слой A_i, равно $\binom{m}{i}$. Поэтому в каждой грани из семейства $F(\Gamma)$, лежащей в нечетном слое, находится $2^k/(k+1)$ кодовых вершин, т. е. кодовые вершины плотно упакованы в такой грани. Кроме того, во всех четных слоях кодовые вершины отсутствуют.

2. Легко проверить, что (b) $\Leftrightarrow$ (c).

3. Очевидно, что (b) $\Rightarrow$ (d).

4. Докажем, что (d) $\Rightarrow$ (a). Из первого уравнения системы (2) следует, что $v_1 = 2^k - (k+1)v_0 = 2^k$. В силу условия (d) $v_0 = v_2 = 0$. Следовательно, из второго уравнения системы (2) имеем $2^k m = (k+1)v_1 = (k+1)2^k$. Значит, $m = k+1$, $k = (n-1)/2$. Лемма 3 доказана.

Известно [5], что размерности всех максимальных граней функции $d_H(\mathbf{x})$, где H — код Хэмминга (единственный линейный, с точностью до изоморфизма), одинаковы и равны $(n-1)/2$. Справедливо обратное утверждение.

Теорема 3. *Пусть C — совершенный $(n,3)$-код и $\mathbf{0} \in C$. Если все максимальные грани булевой функции $d_C(\mathbf{x})$ имеют размерность $(n-1)/2$, то код C линеен.*

Доказательство. Обозначим $k = (n-1)/2$ и $m = (n+1)/2$. Предположим, что C — нелинейный код, т. е. $\mathbf{z} = \mathbf{x} + \mathbf{y} \notin C$ для некоторых $\mathbf{x}, \mathbf{y} \in C$. Тогда вершина $\mathbf{z}$ лежит в некоторой максимальной грани Γ функции $d_C(\mathbf{x})$. По условию размерность грани Γ равна k. Рассмотрим граневое расслоение $\{B_i\}_{i=0}^m$ такое, что $B_0 \in F(\Gamma)$ и $\mathbf{0} \in B_0$. Из леммы 3 следует, что грань Γ содержится в некотором слое с нечетным номером, а вершины кода C располагаются в слоях с четными номерами.

Каждую вершину $\mathbf{x} \in E^n$ запишем в блочном виде: $\mathbf{x} = (\mathbf{ab})$, где $\mathbf{b} = (b_1, \ldots, b_k)$ — проекция $\mathbf{x}$ на грань B_0, а $\mathbf{a} = (a_1, \ldots, a_m)$ — координаты вершины $\mathbf{x}$ по оставшимся m направлениям. В этом представлении

$$\begin{array}{lll}
\mathbf{x} = (\mathbf{a}_x\mathbf{b}_x), & \text{где } w(\mathbf{a}_x) = 2p, & p \in \{0, 1, \ldots, (n+1)/4\}; \\
\mathbf{y} = (\mathbf{a}_y\mathbf{b}_y), & \text{где } w(\mathbf{a}_y) = 2q, & q \in \{0, 1, \ldots, (n+1)/4\}; \\
\mathbf{z} = (\mathbf{a}_z\mathbf{b}_z), & \text{где } w(\mathbf{a}_z) = 2r-1, & r \in \{1, \ldots, (n+1)/4\};
\end{array}$$

Так как $\mathbf{x} + \mathbf{y} = \mathbf{z}$, то $\mathbf{a}_x + \mathbf{a}_y = \mathbf{a}_z$. Поэтому $w(\mathbf{a}_x + \mathbf{a}_y) = w(\mathbf{a}_z)$ — нечетное число. Но, с другой стороны,

$$w(\mathbf{a}_x + \mathbf{a}_y) = w(\mathbf{a}_x) + w(\mathbf{a}_y) - 2w(\mathbf{a}_x \wedge \mathbf{a}_y) = 2(p + q - w(\mathbf{a}_x \wedge \mathbf{a}_y)),$$

т. е. всегда четно, а $w(\mathbf{a}_z)$ нечетно. Противоречие. Значит, наше предположение было неверным. Следовательно, сумма любых двух кодовых вершин также принадлежит коду, т. е. код линеен. Теорема 3 доказана.

Замечание. В частности, из леммы 2 и теоремы 3 следует известный факт линейности любого совершенного $(7,3)$-кода: здесь размерность всех максимальных граней дополнения к коду равна $(n-1)/2$, так как $\log(n+1) = (n-1)/2 = 3$, и поэтому код линеен.

Ясно, что $S_1^n(\mathbf{x}) \subset D_C$ и $S_2^n(\mathbf{x}) \subset D_C$ для любого $\mathbf{x} \in C$.

Для линейного кода H верно следующее утверждение (см. [5]): сфера радиуса 2 с центром в любой кодовой вершине покрывается теми и только теми максимальными гранями функции d_H, что и сфера радиуса 1 с центром в той же вершине. Оказывается, это свойство также является характеристическим для линейного кода, т. е. верна следующая

Теорема 4. *Пусть C — совершенный $(n,3)$-код, $\mathbf{0} \in C$ и сфера радиуса 2 с центром в произвольной кодовой вершине покрывается теми и только теми максимальными гранями функции d_C, что и сфера радиуса 1 с тем же центром. Тогда C — линейный код.*

Доказательство. Пусть Γ — некоторая максимальная грань функции $d_C(\mathbf{x})$. Обозначим $k = \dim \Gamma$ и $m = n - k$. Рассмотрим граневое расслоение $\{A_i\}_{i=0}^m$ такое, что $A_0 = \Gamma$; $(v_0, \ldots, v_m)$ — спектр относительно этого расслоения.

Сначала покажем, что $v_2 = 0$. Предположим, что слою A_2 принадлежит некоторая кодовая вершина $\mathbf{x}$. Тогда сфера радиуса 2 с центром $\mathbf{x}$ имеет непустое пересечение с гранью $\Gamma = A_0$: $\Gamma \cap S_2^n(\mathbf{x}) \neq \varnothing$, хотя сфера радиуса 1 с тем же центром не пересекается с этой гранью, т. е. $\Gamma \cap S_1^n(\mathbf{x}) = \varnothing$. Противоречие с условием. Значит, $v_0 = v_2 = 0$, и из леммы 3 получаем $\dim \Gamma = k = (n-1)/2$.

Это верно для любой максимальной грани функции $d_C(\mathbf{x})$. Следовательно, размерности всех максимальных граней функции $d_C(\mathbf{x})$ равны $(n-1)/2$ и по теореме 3 код C линеен. Теорема 4 доказана.

Из теорем 3 и 4 вытекает

Следствие. *Для нелинейных совершенных $(n,3)$-кодов являются характеристическими следующие свойства:*

1) *размерность хотя бы одной максимальной грани, не содержащей кодовые вершины, строго меньше $(n-1)/2$;*

2) *существует хотя бы одна кодовая вершина $\mathbf{x}$, находящаяся на расстоянии 2 от некоторой максимальной грани, не содержащей кодовые вершины.*

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

ЛИТЕРАТУРА

1. **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.

2. **Мак-Вильямс Ф. Дж., Слоэн Н. Дж. А.** Теория кодов, исправляющих ошибки. М.: Связь, 1979.
3. **Delsarte P.** Bounds for unrestricted codes by linear programming // Philips Res. Reports. 1972. V. 27. P. 272–289.
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. **Романов А. М.** Оценка длины кратчайшей дизъюнктивной нормальной формы для отрицания характеристической функции кода Хэмминга // Методы дискретного анализа в исследовании экстремальных структур: Сб. науч. тр. Новосибирск: Ин-т математики СО АН СССР, 1983. Вып. 39. С. 88–97.
6. **Петровский И. Г.** Лекции по теории обыкновенных дифференциальных уравнений. М.: Наука, 1964.

Адрес автора:

Россия,
630090 Новосибирск,
ул. Пирогова, 2,
Новосибирский государственный университет

Статья поступила

15 декабря 1994 г.