

УДК 519.72

## ОБ ОДНОМ СВОЙСТВЕ СОВЕРШЕННЫХ ДВОИЧНЫХ КОДОВ\*)

С. В. Августинович

Доказано, что любой совершенный двоичный  $(n, 3)$ -код однозначно восстанавливается по расположению его кодовых вершин в двух средних слоях единичного  $n$ -мерного куба. Получена нетривиальная верхняя оценка числа таких кодов.

Проблема описания совершенных двоичных кодов длины  $n$  с расстоянием 3 к настоящему времени не имеет удовлетворительного решения, поскольку величина  $2^{2^{(n-1)/2+\log(n+1)}}$ , ограничивающая, как хорошо известно (см. [1]), число таких кодов снизу, значительно отличается от величины  $2^{2^{n-\log n+\log \log(n+1)}}$ , фигурирующей в тривиальной верхней оценке

$$\left( \frac{2^n}{2^{n-(n-1)+1}} \right) < 2^{2^{n-\log n+\log \log(n+1)}};$$

здесь и всюду в дальнейшем  $\log$  означает логарифм по основанию 2. Последнюю оценку можно уточнить, благодаря полученному в данной статье результату о восстановимости совершенных кодов по их фрагментам.

Подмножество  $C$  вершин единичного  $n$ -мерного куба  $E^n$  называется совершенным двоичным  $(n, 3)$ -кодом, если

- 1) для любых различных вершин  $\alpha, \beta \in C$  справедливо неравенство  $\rho(\alpha, \beta) \geq 3$ , где  $\rho$  — расстояние Хэмминга,
- 2) для любой вершины  $\gamma \notin C$  существует единственная вершина  $\theta \in C$  такая, что  $\rho(\gamma, \theta) = 1$ .

Условия 1, 2 означают, что шары с единичным радиусом и центрами в кодовых вершинах не пересекаются и покрывают куб  $E^n$ .

Обозначим через  $P(n)$  число различных совершенных двоичных  $(n, 3)$ -кодов. Известно [1], что совершенные двоичные  $(n, 3)$ -коды существуют лишь для  $n = 2^k - 1$ ,  $k \in \mathbb{N}$ , причем число кодовых вершин

\*) Работа выполнена при финансовой поддержке Российского фонда фундаментальных исследований (код проекта 93-01-01484).

равно величине  $2^{n-k} = 2^{n-\log(n+1)}$ . Поэтому

$$P(n) < \binom{2^n}{2^{n-\log(n+1)}} < 2^{2^n - \log n + \log \log(n+1)}.$$

Подмножество  $M \subseteq E^n$  назовем *базовым*, если для любых различных кодов  $C_1, C_2$  найдется вершина  $\alpha \in M$  такая, что  $\alpha \in C_1$  и  $\alpha \notin C_2$ .

Нетрудно видеть, что если для кода  $C$  и базового множества  $M$  известно множество  $C \cap M$ , то можно восстановить весь код  $C$ .

Пусть  $n = 2^k - 1$ . Определим множества  $M_1, M_2, M_3$  вершин куба  $E^n$  следующим образом:

вершины из  $M_1$  имеют веса не более  $(n-3)/2$ ,  
 вершины из  $M_2$  — веса  $(n-1)/2$  и  $(n+1)/2$ ,  
 вершины из  $M_3$  — веса не менее  $(n+3)/2$ .

Очевидно, что  $E^n = M_1 \cup M_2 \cup M_3$ .

**Теорема.** Множество  $M_2$  является базовым.

**Доказательство.** Предположим, что множество  $M_2$  не базовое. Тогда найдутся два различных кода  $C_1$  и  $C_2$ , совпадающие на  $M_2$ . Введем обозначения:

$$\begin{aligned} C_1 \cap M_1 &= C_1^1, & C_1 \cap M_2 &= C_1^2, & C_1 \cap M_3 &= C_1^3, \\ C_2 \cap M_1 &= C_2^1, & C_2 \cap M_2 &= C_2^2, & C_2 \cap M_3 &= C_2^3. \end{aligned}$$

По предположению  $C_1^2 = C_2^2$ , но  $C_1^1 \neq C_2^1$ . Легко видеть, что множество  $C^* = C_2^1 \cup C_1^2 \cup C_1^3$  является совершенным  $(n, 3)$ -кодом, поскольку расстояние между  $C_2^1$  и  $C_1^3$  не меньше 3. Рассмотрим код  $C_1$ . Из [2] следует, что если  $\alpha \in C_1$ , то  $\bar{\alpha} \in C_1$ , где  $\bar{\alpha}$  — вершина, полученная из  $\alpha$  заменой единиц нулями и нулей единицами. Следовательно, множество  $C_1^1$  однозначно определяется по множеству  $C_1^3$ . Применяя аналогичное рассуждение к коду  $C^*$ , получим, что  $C_2^1$  определяется по  $C_1^3$ . Следовательно,  $C_1^1 = C_2^1$ , что приводит к противоречию.

Используя формулу Стирлинга, легко доказать неравенство

$$|M_2| < 2^{n - \frac{1}{2} \log n}.$$

Кроме того, согласно [1] имеет место неравенство

$$|M_2 \cap C| < |M_2|/n.$$

Таким образом, справедливо

**Следствие.** При любом  $n = 2^k - 1$ ,  $k \in \mathbb{N}$ ,

$$P(n) < \binom{2^{n - \frac{1}{2} \log n}}{2^{n - \frac{3}{2} \log n}} < 2^{2^{n - \frac{3}{2} \log n} + \log(en)}.$$

**ЛИТЕРАТУРА**

1. Васильев Ю. Л. О негрупповых плотно упакованных кодах // Проблемы кибернетики. М.: Наука, 1962. Вып. 8. С. 337–339.
2. 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.

Адрес автора:

РОССИЯ,  
630090, Новосибирск,  
Университетский пр., 4,  
Институт математики СО РАН

Статья поступила

14 декабря 1994 г.