

2 Линейные коды

- Двоичным кодом называется произвольное подмножество E^n .
 - Кодовые параметры кода C — тройка $(n, |C|, d)$, где
 - n — длина;
 - $|C|$ — мощность кода;
 - d — кодовое расстояние кода, $d = \min_{x, y \in C, x \neq y} d(x, y)$.
 - Код называется линейным, если он образует подпространство в E^n , его параметры обозначаются также $[n, k, d]$ (или кратко $[n, k]$), где k — размерность кода, т.е. $|C| = 2^k$.
 - Два вектора $x, y \in E^n$ ортогональны, если $x \cdot y = x_1y_1 \oplus \dots \oplus x_ny_n = 0$.
-

2.1 Найти число баз в E^n .

2.2 Найти число различных линейных $[n, k]$ -кодов.

2.3 Показать, что кодовое расстояние линейного кода равно минимальному из весов его ненулевых векторов.

2.4 Показать, что в двоичном линейном коде либо каждый кодовый вектор имеет четный вес, либо половина кодовых векторов имеет четные веса и половина — нечетные.

2.5 Доказать, что ненулевой столбец кодовой матрицы линейного $[n, k]$ -кода содержит ровно 2^{k-1} единиц.

2.6 Показать, что кодовое расстояние линейного $[n, k]$ -кода не превосходит $\lfloor \frac{n \cdot 2^{k-1}}{2^k - 1} \rfloor$.

2.7 Найти число векторов, ортогональных к данному ненулевому вектору x из E^n .

2.8 Разобрать способы задания линейного кода с помощью:

- а) кодовой матрицы;
- б) проверочной матрицы;
- в) порождающей матрицы.

2.9 Построить коды с помощью проверочных матриц

$$a) H = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}; \quad b) H = \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 0 \end{pmatrix}.$$

Найти порождающие матрицы для этих кодов. Определить кодовые параметры.

2.10 Пусть H, G — проверочная и порождающая матрицы линейного кода соответственно. Доказать, что $H \cdot G^T = \mathbf{0}$ и $G \cdot H^T = \mathbf{0}$. Исследуя связь между H и G , найти число проверочных и порождающих матриц для данного $[n, k]$ -кода.

Теория к Семинару 3 "Границы объёмов кодов. Коды Хэмминга".

Границы Хэмминга, Синглтона, Варшамова-Гилберта, Плоткина. Коды Хэмминга, исправляющие одну ошибку. Совершенные коды.