

### Пятиминутка №1

1. **Расстояние Хэмминга** - число несовпадающих координат векторов  $x, y \in E_q^n$ , обозначается через  $d(x, y) = |\{i \in \{1, \dots, n\} : x_i \neq y_i\}|$ .
2. **Вес Хэмминга** - число ненулевых координат вектора  $x$ , обозначается:  $\omega(x)$ ,  $\omega(x) = d(x, 0)$ .
3. **Код** - обозначается через  $C$  и является подмножеством кодовых слов:  $C \subseteq E_q^n$ .
4. **Параметры кода** -  $(n, |C|, d)$ , где:  $n$  - длина кода,  $|C|$  - мощность кода,  $d$  - минимальное кодовое расстояние, т.е. минимум расстояний по всем парам кодовых слов из  $C$ .
5. **Кодер** - биекция из множества информационных сообщений  $M$ ,  $M \subseteq E^k$  в множество кодовых слов  $C$ .
6. **Принцип максимума правдоподобия** - пусть для передачи использовался код  $C$ , если  $y$  - полученный вектор, то декодируем его в ближайшее кодовое слово  $x \in C$ .
7. **Число исправляемых ошибок** - пусть  $C$  код с кодовым расстоянием  $d$ , и пусть при передаче кодового слова  $x \in C$  возникло не более  $\lfloor (d-1)/2 \rfloor$  ошибок, тогда декодер восстановит сообщение.
8. **Число обнаруживаемых ошибок** - пусть  $C$  код с кодовым расстоянием  $d$ , и пусть при передаче кодового слова  $x \in C$  возникло не менее 1 и не более  $(d-1)$  и из канала связи получили вектор  $y$ . В этом случае кодер может запросить снова передачу данных, так как  $y$  - не кодовое слово. То есть код обнаруживает  $(d-1)$  ошибок.
9. **Линейный код** - код  $C$  называется линейным, если  $C$  является векторным подпространством  $E_q^n$ .
10. **Размерность линейного кода**  $C$  - число векторов в базисе  $C$ , обозначается через  $k$ .
11. **Параметры линейного кода** -  $[n, k, d]$ , где  $n$  - длина кода,  $k$  - размерность,  $d$  - минимальное кодовое расстояние.
12. **Кодовое расстояние линейного кода** - оно равно минимальному весу среди ненулевых кодовых слов.

13. **Порождающая матрица** - матрица  $G_{k \times n}$  строки которой образуют базис  $C$ , называется порождающей матрицей кода  $C$ .
14. **Проверочная матрица** - матрица  $H_{(n-k) \times n}$  имеющая  $n - k$  строк и  $n$  столбцов называется проверочной, если выполнено  $Hx^T = 0^{n-k} \Leftrightarrow x \in C$ .
15. **Порождающая матрица в каноническом виде** - порождающая матрица  $G$  называется заданной в каноническом виде, если  $G = [E_k | A]$ , где  $E_k$  - единичная матрица.
16. **Проверочная матрица в каноническом виде** - проверочная матрица  $H$  называется заданной в каноническом виде, если  $H = [A | E_{n-k}]$ , где  $E_{n-k}$  - единичная матрица.
17. **Теорема связывающая порождающую и проверочную матрицы** - если  $[E_k | A]$  - порождающая матрица в каноническом виде кода  $C$ , тогда  $[-A^T | E_{n-k}]$  - является проверочной матрицей в каноническом виде кода  $C$ . Верно и обратное.

## Пятиминутка №2

1. **Теорема о столбцах проверочной матрицы** Пусть  $H$  - проверочная матрица линейного кода  $C$ . Кодовое расстояние  $C$  равно  $d$  тогда и только тогда когда любые  $d - 1$  столбцов  $H$  линейно независимы и существует  $d$  линейно зависимых столбцов.

### Или кратко:

Пусть  $H$  - проверочная матрица линейного кода  $C$ , тогда  $d_C = d \Leftrightarrow \forall d - 1$  столбцов проверочной матрицы  $H$  линейно независимы, и  $\exists d$  линейно зависимых столбцов.

2. **Замечание 1**

\* двоичный код с проверочной матрицей  $H$ .

Кодовое расстояние  $C$  равно 1 тогда и только тогда когда в его проверочной матрице  $H$  существует нулевой столбец.

3. **Замечание 2** Кодовое расстояние  $C$  равно 2 тогда и только тогда когда в  $H$  нет нулевых столбцов и есть пара одинаковых столбцов.
4. **Замечание 3** Кодовое расстояние  $C$  равно 3 тогда и только тогда когда в  $H$  нет нулевых столбцов, столбцы попарно различны и есть столбец равный сумме двух других.

5. **Код Хэмминга** Пусть  $r \geq 2$ . Двоичным кодом Хэмминга (с  $r$  проверками на четность) называется код с проверочной матрицей  $H$ , столбцами которой являются все ненулевые векторы длины  $r$ . Параметры кода Хэмминга:

$n = 2^r - 1$  - длина кода;

$k = n - r$  - размерность кода;

$d = 3$  - минимальное кодовое расстояние (все векторы попарно различны, нет нулевых, сумма двух любых столбцов встречается в матрице.)

6. **Граница Хэмминга. Теорема** Пусть  $C$  - двоичный код длины  $n$  и кодовым расстоянием  $d$ . Тогда

$$|C| \leq \frac{2^n}{\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} C_n^i}$$

7. **Шар**  $B(x, j)$  радиуса  $j$  с центром в векторе  $x$  называется множество всех векторов, находящихся на расстоянии Хэмминга не более  $j$  от  $x$ .

**Или кратко:**

$$B(x, j) = \{y \in E_q^n : d(x, y) \leq j\}$$

8. **Граница Хэмминга для  $q$ -значных кодов** Пусть  $C$  -  $q$ -значный код длины  $n$  и кодовым расстоянием  $d$ . Тогда

$$|C| \leq \frac{q^n}{\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} C_n^i (q-1)^i}$$

9.  $q$ -значный код называется **совершенным** если его мощность достигает границы Хэмминга.

**Или кратко:**

$C \subseteq E_q^n$  - **совершенный** код, если

$$|C| = \frac{q^n}{\sum_{i=0}^{\lfloor (d-1)/2 \rfloor} C_n^i (q-1)^i}$$

10. Двоичный код Хэмминга является совершенным кодом с  $d = 3$ .

Длина  $n = 2^r - 1$

Мощность кода равна  $2^{n-r}$

Кодовое расстояние 3

Граница Хэмминга:  $2^{n-r} \leq 2^n / (1 + n) = 2^{n-r}$

11. **Теорема, Зиновьев, Леонтьев, Титвайнен, 1973** Пусть  $q = p^m$  тогда всякий совершенный код имеет параметры совпадающие с одним из следующих кодов:
1.  $q$ -значный код Хэмминга,
  2. Двоичный код Голя  $n = 23, k = 12, d = 7$ ,
  3. Троичный ( $q = 3$ ) код Голя  $n = 11, k = 6, d = 5$ .
12. **Теорема (Граница Синглтона)** Пусть  $C$  –  $q$ -значный код с параметрами  $n, |C|, d$ . Тогда  $\log_q |C| \leq n - d + 1$ .  
e.g.  $C = (000), (111)$
13. **Полный четновесовой код**  $\{x : x \in E^n, w(x) = 0(mod 2)\}$  Параметры  $n, |C| = 2^{n-1}, d = 2$
14. **Граница Плоткина** Пусть – двоичный код длины  $n$  с минимальным расстоянием  $d$ , и  $2d > n$ . Тогда справедливо неравенство

$$|C| \leq 2 \lfloor d/(2d - n) \rfloor$$