

### 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 (Граница Синглтона)** Пусть  $C$  –  $q$ -значный код с параметрами  $n, |C|, d$ . Тогда  $\log_q |C| \leq n - d + 1$ .  
e.g.  $C = (000), (111)$
12. **Полный четновесовой код**  $\{x : x \in E^n, w(x) = 0 \pmod{2}\}$  Параметры  $n, |C| = 2^{n-1}, d = 2$
13. **Граница Плоткина** Пусть – двоичный код длины  $n$  с минимальным расстоянием  $d$ , и  $2d > n$ . Тогда справедливо неравенство

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

### Пятиминутка №3

1. **Код Адамара** Рассмотрим код, столбцы порождающей матрицы  $G$  которого состоят из всех ненулевых векторов длины  $k$ :

$$G = \begin{pmatrix} 0 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix}, \text{ этот код называется кодом Адамара.}$$

Его параметры:  $[2^k - 1, k, 2^k - 1]$

2. **Утверждение(Код Адамара)** Код Адамара имеет параметры  $[2^k - 1, k, 2^k - 1]$  и достигает границы Плоткина.
3. **Граница Варшавова - Гилберта** Пусть  $\sum_{i=0}^{d-2} C_{n-1}^i < 2^r$ . Тогда существует линейный код длины  $n, k \geq n - r, d' \geq d$ .
4. **Оптимальный код** Код, имеющий максимальную мощность среди всех кодов той же длины и кодовым расстоянием называется **оптимальным**.

### Пятиминутка №4

1. **Теорема (Конструкция Плоткина)** Пусть  $C$  и  $D$  коды одинаковой длины  $n$  с кодовым расстоянием  $d_1$  и  $d_2$  соответственно. Тогда код  $C^{2n} = \{(x, x + y) : x \in C, y \in D\}$  имеет длину  $2n$ , мощность  $|C| * |D|$ , кодовое расстояние  $\min\{2d_1, d_2\}$ .
2. **Расширение кода** Пусть  $C$  – двоичный код с кодовым расстоянием  $d$ ,  $d$  – нечетное. Рассмотрим код:

$$\bar{C} = \{(x, \omega(x) \pmod{2}) : x \in C\}$$

Параметры:  $\bar{C} : \bar{n} = n + 1, |\bar{C}| = |C|, \bar{d} = d + 1$ .

3. **Выкалывание в коде** Выкалывание кодовых координат представляет собой удаление символа в одной координате во всех кодовых словах. Если исходный код  $C$  имел параметры:  $(n, |C|, d)$ , то код  $C'$ , полученный выкалыванием из  $C$ , имеет следующие параметры:  $(n-1, |C'|, d')$ , где  $|C'| \leq |C|, d-1 \leq d' \leq d$  (заметим, что  $|C| = |C'|$ , если  $d > 1$ ).

4. **Укорочение кода** Укорочение кода состоит в следующем:

- Выбираем все кодовые слова, у которых  $i$ -й символ равен 0 (либо 1). Как правило, выбирается более мощная часть кодовой матрицы с фиксированной координатой  $i$ , если таковой нет, у которых символ в координате  $i$  равен 0;
- Удаляем символы в выбранных словах.

Из кода  $C$  с параметрами  $(n; |C|; d)$  получается  $(n-1; |C'|; d')$  – код  $C'$ , где  $|C'| \geq |C| = 2; d' \geq d$ .

5. **Утверждение (эквивалентность кода Хэмминга)** Всякий линейный совершенный код с кодовым расстоянием 3 есть код Хэмминга и наоборот.

6. **Эквивалентные двоичные коды** Двоичные коды  $C$  и  $D$  длины  $n$  называются *эквивалентными*, если существует перестановка координатных позиций  $\pi$  и вектор  $x \in E^n$ , такие что

$$x + \pi(C) = D,$$

где  $x + \pi(C)$  определяется как следующий код:

$$\{x + (y_{\pi(1)}, \dots, y_{\pi(n)}) : y \in C\}$$

Обозначим  $(y_{\pi(1)}, \dots, y_{\pi(n)})$  через  $\pi(y)$ .

Перестановка  $\pi$  и сдвиг на  $x$  сохраняют расстояние между любыми словами:

$$d(x + \pi(y), x + \pi(y')) = d(\pi(y), \pi(y')) = d(y, y')$$

Поэтому эквивалентные коды имеют одинаковые параметры.

7. **Смежный класс по коду** Если  $C$  – линейный код длины  $n$ , то *смежным классом* по коду  $C$  называется:

$$x + C = \{(x_1, \dots, x_n) + y : y \in C\}$$

для некоторого  $x \in E^n$ .

8. **Замечание (смежные классы кода Хэмминга)** Коды, эквивалентные коду Хэмминга - все коды Хэмминга (содержащие  $0^n$ ) и смежные классы по ним, не содержащие  $0^n$ .
9. **Теорема Васильев, 1962** Пусть  $C$  - произвольный двоичный совершенный код длины  $n$  с кодовым расстоянием 3 и  $\lambda$  - произвольная функция из кода  $C$  в множество  $\{0, 1\}$ . И пусть  $|x| \doteq \omega(x) \bmod 2$ . Множество:

$$V_{C,\lambda} = \{(x + y, |x| + \lambda(y), x) : x \in E^n, y \in C\}$$

является совершенным двоичным кодом длины  $2 \cdot n + 1$  с кодовым расстоянием 3.

10. **Следствие из теоремы Васильева** Двоичные совершенные коды, не эквивалентные кодам Хэмминга, существуют для любой длины  $n$ ,  $n \geq 15$ .
11. **Теорема, Зиновьев, Леонтьев, Титвайнен, 1973** Пусть  $q = p^m$  тогда всякий нетривиальный (то есть отличный от всего пространства и имеющий мощность больше 2) совершенный код имеет параметры совпадающие с одним из следующих кодов:
1.  $q$ -значный код Хэмминга,
  2. Двоичный код Голея  $n = 23, k = 12, d = 7$ ,
  3. Троичный ( $q = 3$ ) код Голея  $n = 11, k = 6, d = 5$ .
12. **Вектор ошибок** -  $c \in C$  передавали,  $y$  получили, тогда  $e = c + y$  - единицы в позициях, где произошли ошибки.
13. **Лидер смежного класса** - любой вектор наименьшего веса в этом классе.
14. **Утверждение о векторе ошибок** Пусть  $y = c + e$  - полученный вектор,  $c \in C$ . тогда вектор ошибок  $e$  принадлежит тому же смежному классу что и  $y$ .

### Пятиминутка №5

1. **Синдром вектора, его длина (для  $[n,k,d]$  кода)**

Пусть используется линейный двоичный код длины  $n$  размерности  $k$  с проверочной матрицей  $H$  для передачи сообщений. Синдромом вектора  $y \in E^n$  называется вектор  $H y^T$ .

Свойства синдрома:

1. Синдром вектор длины  $n - k$ .
2. Синдром кодового слова равен  $0^{n-k}$ .
3. Синдромы и смежные классы находятся во взаимно однозначном соответствии.
4. Синдром полученного вектора  $u$  равен сумме столбцов проверочной матрицы с номерами в позициях где произошли ошибки.

2. **Вероятностью ошибки декодирования** кода  $C$  называется средняя вероятность ошибки декодирования по всем словам, то есть

$$P_{mistake} = \frac{\sum_{c \in C} (1 - P(c|c))}{|C|}$$

3. **Пропускная способность канала и скорость кода**

Пусть  $p$  - вероятность искажения символа при передаче в канале связи. Пропускной способностью канала называется

$$C(p) = 1 + p \log(p) + (1 - p) \log(1 - p)$$

где  $\log = \log_2$ .

Скоростью кода  $C$  называется  $\frac{\log|C|}{n}$  (если  $C$ -линейный, то процент информационных символов).

4. **Теорема Шеннона**

Для всякого канала с пропускной способностью  $C(p)$  и всяких  $\epsilon, R > 0, R < C(p)$  существует код достаточной большой длины  $n$  скорости  $R$ , что действуя по принципу максимума правдоподобия вероятность ошибки декодирования  $P_{mistake} < \epsilon$ .

5. **Поле**

Поле называется алгебраическая система  $\langle F, +, * \rangle$ :

1.  $\langle F, + \rangle$  - коммутативная группа с  $0$
2.  $\langle F \setminus \{0\}, * \rangle$  - коммутативная группа с  $1$
3. Для любых трех элементов  $a, b, c \in F$  выполнено  $a(b+c) = ab+ac$

6. **Порядок поля**

Порядком поля называется число его элементов.

## 7. Поле Галуа

Конечным полем или полем Галуа называется поле конечного порядка.

## 8. Характеристика поля

Характеристикой поля  $F$  называется минимальное неотрицательное число  $r$ , такое что сумма  $\underbrace{1 + 1 + \dots + 1 + 1}_r = 0$

## 9. Теорема о порядке поля Галуа

Если порядок поля Галуа равен  $q$ , то  $q = p^m$ , где  $m \geq 1$  и  $p$ -простое число, равное характеристике поля.

### Дополнительно к 5 пятиминутке

1. Пусть дан линейный код с параметрами  $[n, k, d]$ ,  $q=2$ . Опишите кратко структуру таблицы стандартного расположения (что собой представляют строки и столбцы, сколько их).
2. Пусть дан линейный код и его смежный класс. Может ли так случиться, что в смежном классе кодовых слов меньше, чем в коде? Ответ поясните.
3. Пусть дан линейный код с параметрами  $[n, k, d]$ . Напишите и объясните, сколько существует различных смежных классов этого кода.
4. Верно ли, что синдромы двух слов из различных смежных классов линейного кода должны иметь разные синдромы? Ответ поясните.

### Пятиминутка №6

#### 1. Идеал

Пусть  $K$  - кольцо, подкольцо  $I$  кольца  $K$  называется **идеалом**, если  $\forall i \in I, \forall k \in K : ik \in I$

#### 2. Неприводимый многочлен

Многочлен  $f(x) \in F_p[x]$  называется **неприводимым**, если он **нормированный** (старший коэффициент равен 1) и не раскладывается в произведение многочленов меньшей степени из  $F_p[x]$ .

#### 3. Теорема

Пусть  $f(x)$  - неприводимый многочлен из  $F_p[x]$  степени  $m$ . Тогда  $F_p[x]/(f(x))$  - поле Галуа  $GF(p^m)$ .



#### 4. Порядок элемента группы

Порядком элемента  $\alpha$  группы называется наименьшее положительное число  $l$ :  $\alpha^l = 1$ .

#### 5. Примитивный элемент поля

Примитивным элементом  $\alpha$  поля  $GF(p^m)$  называется элемент порядка  $p^m - 1$ . То есть выполнено:

$$GF(p^m) \setminus \{0\} = \{1, \alpha, \alpha^2, \dots, \alpha^{p^m-2}\}$$

#### 6. Лемма 1

Пусть  $G$  - коммутативная группа, тогда если  $\alpha$  - элемент порядка  $l$ , то  $\alpha^k$  - элемент порядка  $\frac{l}{(k,l)}$

#### 7. Лемма 2

Пусть  $G$  - коммутативная группа,  $\alpha$  - элемент порядка  $l$ ,  $\beta$  - элемент порядка  $k$ ,  $(k, l) = 1$ , тогда  $\alpha\beta$  - элемент порядка  $kl$ .

#### 8. Теорема

Во всяком поле Галуа  $GF(p^m)$  существует **примитивный** элемент.

#### 9. Следствие (Теорема Ферма)

Для всякого элемента  $\beta$  поля  $GF(p^m)$  выполнено:  $\beta^{p^m-1} - \beta = 0$

#### 10. Следствие (Теорема Ферма, другая формулировка)

В  $GF(p^m)$  выполнено:

$$\prod_{\beta \in GF(p)} (x - \beta) = x^{p^m} - x$$

#### 11. Следствие

Пусть  $\alpha$  - **примитивный** элемент поля Галуа  $GF(p^m)$ . Тогда  $\alpha^i$  - **примитивный** элемент  $\Leftrightarrow (i, p^m - 1) = 1$