**Теория Кодирования как введение в Алгебру и Арифметику**

# ЛИСТОК 1. Различные структуры на бинарном пространства $\mathbb{F}_2^n$

**В. А. Гриценко, 23 сентября 2020**

*Задачи для письменного решения, отмечены звездочкой $*$.*

Задача 1. **Простейшие свойства метрики Хэмминга.**
В курсе мы ввели бинарное метрическое пространство $\mathbb{B}_2^n = (\mathbb{F}_2^n, \rho)$ с метрикой Хэмминга $\rho(a, b)$, которая равна числу попарно различных координат векторов $a$ и $b \in \mathbb{F}_2^n$. Напомним, что вес бинарного вектора $w(a)$ равен числу его ненулевых координат.

1) Доказать, что $\rho(a, b) = w(a + b) = \rho(0, a + b)$,

$$w(a + b) \equiv w(a) + w(b) \mod 2, \qquad \rho(a, b) + \rho(b, c) \equiv \rho(a, c) \mod 2.$$

2) На первом занятии мы доказали неравенство треугольника для метрики Хэмминга. Как описать все точки $a$, $b$ и $c$, лежащие на одной "прямой", т.е. удовлетворяющие условию $\rho(a, b) + \rho(b, c) = \rho(a, c)$?

3) Показать, что в любом подпространстве $\mathbb{F}_2^n$ либо каждый вектор имеет четный вес, либо половина векторов имеет четные веса и половина — нечетные.

4) Пусть $V_t(a) = V_t^{(n)}(a)$ — шар радиуса $t$ с центром в слове $a$ метрического пространства $\mathbb{B}_2^n$. Сколько попарно непересекающихся шаров радиуса $t$ можно разместить в пространстве $\mathbb{B}_2^8$? Рассмотреть все возможные $t$.

5) Доказать, что $|V_t(\mathbf{0})| + |V_{n-t-1}(\mathbf{1})| = 2^n$, где $\mathbf{0} = (0, \ldots, 0)$, $\mathbf{1} = (1, \ldots, 1)$.

Задача 2. **Группа автоморфизмов метрического пространства $\mathbb{B}_2^n$.**

1) Доказать, что параллельный перенос на любой вектор $a \in \mathbb{F}_2^n$ является метрическим автоморфизмом пространства $\mathbb{B}_2^n$.

2) Доказать, что перестановка координат является метрическим автоморфизмом $\mathbb{B}_2^n$.

3$^*$) Доказать, что любой метрический автоморфизм $f$ пространства $\mathbb{B}_2^n$ есть композиция параллельного переноса и перестановки $f(v) = \pi(v) + a$, где $a \in \mathbb{F}_2^n$ и $\pi$ – перестановка координат $\mathbb{F}_2^n$.

4) Группа $\mathrm{Aut}(\mathbb{B}_2^n)$ есть полупрямое произведение абелевой группы $(\mathbb{F}_2^n, +)$ и группы перестановок $S_n$. В частности, $|\mathrm{Aut}(\mathbb{B}_2^n)| = 2^n \cdot n!$.

5$^*$) Найти элемент наибольшего порядка группы $\mathrm{Aut}(\mathbb{B}_2^8)$.

Задача 3. **Первые примеры кодов.**

1) Доказать, что не существует кода $f : \mathbb{F}_2^2 \to \mathbb{B}_2^4$, который исправляет одну ошибку. (См. лекцию 1.)

2) Построить линейный код $f : \mathbb{F}_2^2 \to \mathbb{F}_2^5$, исправляющий одну ошибку.

3) Найти все такие линейные коды с точностью до изоморфизма.

4$^{**}$) Найти, с точностью до изоморфизма, все коды (не обязательно линейные!) типа $f : \mathbb{F}_2^2 \to \mathbb{B}_2^5$, исправляющие одну ошибку.

5) Существует ли код $f : \mathbb{F}_2^2 \to \mathbb{B}_2^6$, исправляющий две ошибки?

6) Найти наименьшее $n$, для которого существует линейный код $f : \mathbb{F}_2^2 \to \mathbb{F}_2^n$, исправляющий две ошибки.

Задача 4. **Грассманиан $\mathbb{F}_2^n$.**

1) Найти число прямых и плоскостей в $\mathbb{F}_2^n$.

2) Найти число $k$-мерных подпространств пространства $\mathbb{F}_2^n$ (аналогичный вопрос для $\mathbb{F}_q^n$).

**Граф Грассмана** $J_2(n,k)$ — это граф, вершинами которого являются $k$-мерные подпространства пространства $\mathbb{F}_2^n$, а ребрами соединены только те вершины $V_1$ и $V_2$, для которых $\dim(U_1 \cap U_2) = k-1$.

3) Чем отличается граф $J_2(3,2)$ от конечной плоскости Фано?

4) Найти число вершин и ребер графа $J_2(4,k)$ для всех возможных $k$.

5$^*$) Аналогичный вопрос для графа $J_2(n,k)$. Проанализируйте свойства этого графа.

Задача 5. **Повторение линейной алгебры над полем $\mathbb{F}_2$.**

На пространстве $\mathbb{F}_2^n$ определена симметричная билинейная форма

$$v \cdot u = (v,u) = x_1y_1 + \ldots + x_ny_n.$$

Для любого подпространства $U \subset \mathbb{F}_2^n$ определим его ортогональное дополнение

$$U^\perp = \{v \in \mathbb{F}_2^n : \ \forall\, u \in U \ (u,v) = 0\}.$$

1) Доказать, что $(v,v) = 0$ тогда и только тогда, когда вес вектора $v$ чётен.

2) Доказать, что

$$\dim(U) + \dim(U^\perp) = n, \qquad (U^\perp)^\perp = U.$$

3) Что можно сказать о подпространстве $U \subset \mathbb{F}_2^n$ таком, что $U \subset U^\perp$? Аналогичный вопрос при условии $U = U^\perp$.

Задача 6. **“Лагранжианы” в $\mathbb{F}_2^n$.**

1) Найти число подпространств $U \subset \mathbb{F}_2^n$ для $n = 2$, 4 таких, что $U = U^\perp$.

2$^*$) Аналогичный вопрос для $n = 6$ и 8.

3$^*$) Найти число четырёхмерных подпространств $U \subset \mathbb{F}_2^8$ таких, что $U = U^\perp$ и вес любого вектора из $U$ делится на 4.

Задача 7. **Единственность кода Хэмминга длины 7.**

1$^*$) Доказать, что существует единственный, с точностью до перестановок координат, код Хэмминга $H_4^{(7)}$.

2$^{**}$) Найти, с точностью до изоморфизма, все (не обязательно линейные!) совершенные коды мощности 16 в $\mathbb{B}_2^7$, исправляющие одну ошибку.

Задача 8. **Синдромы кода Хэмминга.** На лекции мы разобрали все варианты возникших ошибок для всех возможных синдромов кода Хэмминга $H_4^{(7)}$. Рассмотреть аналогичную задачу для чётного расширения кода Хэмминга $H_4^{(8)}$.

Задача 9*. **Группа автоморфизмов кода Хэмминга.** Перестановочная группа автоморфизмов кода Хэмминга $H_4^{(7)}$ — это подгруппа группы перестановок координат $\mathbb{F}_2^8$, которые переводят подпространство $H_4^{(7)}$ в себя. (См. Задачу 2.) Используя конечную проективную плоскость Фано, мы доказали, что эта группа содержит подгруппу, изоморфную простой группе $GL_3(\mathbb{F}_2)$ порядка 168. Доказать, что группа перестановочных автоморфизмов $H_4^{(7)}$ совпадает с $GL_3(\mathbb{F}_2)$. Определить всю группу автоморфизмов кода Хэмминга.