Теория Кодирования как введение в Алгебру и Арифметику

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

В. А. Гриценко, 17 сентября 2021

Более сложные задачи для индивидуального письменного решения отмечены звездочкой N^*.

Задача 1. **Вес бинарных слов (векторов).**

Пусть $v \in \mathbb{F}_2^n$ — элемент бинарного векторного пространства размерности n (или бинарное слово длины n). *Вес $w(v)$ равен числу ненулевых координат вектора v.* Перечислим простейшие свойства веса.

1) $0 \le w(v) \le n$, $w(v) = 0 \iff v = \bar{0} = (0, \dots, 0)$, $w(v) = n \iff v = \bar{1} = (1, 1, \dots, 1)$, $w(v + \bar{1}) = n - w(v)$,

$$w(u + v) = w(u) + w(v) - 2w(u \cap v),$$

где $u = (x_1, \dots, x_n)$, $v = (y_1, \dots, y_n)$ и $u \cap v = u * v = (x_1 y_1, \dots, x_n y_n)$.

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

Задача 2. **Метрика Хэмминга в $\mathbb{F}_2^n$.**

1) Пусть $a, b \in \mathbb{F}_2^n$. Определим *метрику Хэмминга* $\rho(a, b)$ как число попарно различных координат векторов a и b. Доказать, что это метрика и что определено бинарное метрическое пространство $\mathbb{B}_2^n = (\mathbb{F}_2^n, \rho)$.

a) $\rho(a, b) = 0 \iff a = b$,
b) $\rho(a, b) = \rho(b, a) = w(a - b) = w(a + b)$,
c) $\rho(a, c) \le \rho(a, b) + \rho(b, c)$.

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

$$\forall\, a, b, c \in \mathbb{F}_2^n : \quad \rho(a, b) = \rho(a + c, b + c).$$

3) Доказать, что перестановка координат в $\mathbb{F}_2^n$ является метрическим автоморфизмом пространства $\mathbb{B}_2^n$.

4) Пусть $V_t(a) = V_t^{(n)}(a)$ — шар радиуса t с центром в слове a метрического пространства $\mathbb{B}_2^n$

$$V_t(a) = V_t^{(n)}(a) = \{u \in \mathbb{F}_2^n \,:\, \rho(a, u) \le t\}.$$

Найти число элементов $|V_t^{(n)}(a)|$ в шаре.

5) Сколько попарно непересекающихся шаров радиуса t можно разместить в пространстве $\mathbb{B}_2^8$? Рассмотреть все возможные t.

6) Какое разбиение на шары задает код Хэмминга $H_4^{(7)} \subset \mathbb{F}_2^8$?

7) Доказать, что $V_t(\mathbf{0}) \sqcup V_{n-t-1}(\mathbf{1}) = \mathbb{F}_2^n$, где $\mathbf{0} = (0, \dots, 0)$, $\mathbf{1} = (1, \dots, 1)$.

8*) Пусть a, $c \in \mathbb{F}_2^n$. Описать все точки $b \in \mathbb{F}_2^n$ лежащие на "отрезке" $[ac]$, т.е. точки b, удовлетворяющие условию $\rho(a, b) + \rho(b, c) = \rho(a, c)$.

9*) Найти число точек пересечения двух шаров для произвольных $a, b \in \mathbb{F}_2^n$ и $t, s \in \mathbb{Z}_{\geq 0}$

$$|V_t(a) \cap V_s(b)| = ?$$

Задача 3*. **Группа автоморфизмов пространства $\mathbb{B}_2^n$.**

В Задаче 2 мы доказали, что параллельный перенос на любой вектор $a \in \mathbb{F}_2^n$ и перестановка координат $\mathbb{F}_2^n$ являются метрическими автоморфизмами пространства $\mathbb{B}_2^n$.

1) 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 π — перестановка координат в $\mathbb{F}_2^n$.

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

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

Задача 4. **Первые примеры кодов.**

1) Рассмотреть простейшие "повторяющиеся" коды

$$\mathbb{F}_2^2 \to \mathbb{F}_2^4, \qquad \mathbb{F}_2^2 \to \mathbb{F}_2^6,$$

определенные отображениями $(ab) \mapsto (aabb)$ и $(ab) \mapsto (aaabbb)$. Какой из этих кодов исправляет одну ошибку?

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

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

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

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

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

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

Задача 5. **Линейная алгебра: грассманиан $\mathbb{F}_2^n$.**

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

2) Найти число базисов n-мерного пространства $\mathbb{F}_2^n$. Аналогичный вопрос для пространства $\mathbb{F}_q^n$ над конечным полем $\mathbb{F}_q$.

3) Найти порядок группы обратимых матриц $GL_n(\mathbb{F}_2)$ ($GL_n(\mathbb{F}_q)$).

4) 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 $\dim(U_1 \cap U_2) = k - 1$.

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

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

7*) Аналогичный вопрос для графа $J_2(n,k)$. Исследовать свойства этого графа.

Задача 6. **Линейная алгебра: скалярное произведение.**
В пространстве $\mathbb{F}_2^n$ определена симметричная билинейная форма

$$v \cdot u = (v,u) = x_1y_1 + \ldots + x_ny_n \in \mathbb{F}_2.$$

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 $U \subset U^\perp$?

4) Аналогичный вопрос при условии $U = U^\perp$.

Задача 7. **Линейная алгебра: "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 8. **Единственность кода Хэмминга длины 7.**

1*) Доказать, что любой линейный совершенный код типе $[7,4;3]$ перестановкой координат переводится в код Хэмминга $H_4^{(7)} \subset \mathbb{F}_2^7$.

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

Задача 9. **Синдромы кода Хэмминга.** На лекции 20 сентября 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 10*. **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. Задачи 2 и 3.) Используя конечную проективную плоскость Фано при построение кода Хэмминга, доказать, что эта группа содержит подгруппу, изоморфную (простой) группе $GL_3(\mathbb{F}_2)$ порядка 168. Далее доказать, что группа перестановочных автоморфизмов $H_4^{(7)}$ изоморфна $GL_3(\mathbb{F}_2)$.

Задача 11*. **Группа $GL_3(\mathbb{F}_2)$.**

1) Найти порядок группы $GL_3(\mathbb{F}_2)$.

2) Найти её силовскую 2-подгруппу, элементы порядка 3 и 7.

3*) Найти все элементы порядка 3 и 7 в $GL_3(\mathbb{F}_2)$.

4*) Найти элемент максимального порядка в $GL_3(\mathbb{F}_2)$.

5*) Доказать, что группа $GL_3(\mathbb{F}_2)$ не содержит нетривиальных нормальных подгрупп.