Теория Кодирования как введение в Алгебру и Арифметику

ЛИСТОК 2 (выдан 7 октября 2020)

Структуры, связанные с бинарным пространством

Задачи для письменного решения отмечены звездочкой $*$.

Задача 1. **Бинарный n-мерный куб и метрика Хэмминга** *(см. первую задачу Листка 1).*

Вершинами n-мерного куба являются точки бинарного метрического пространства $\mathbb{B}_2^n = (\mathbb{F}_2^n, \rho)$. Две вершины a и b соединены ребром, если расстояние Хэмминга между ними равно 1.

1) Постройте граф $\mathbb{B}_2^n$ для $n = 1$, 2, 3 и 4.

2) Сколько ребер имеется в n-мерном кубе?

3) Пусть $\mathbf{0} = (0, \ldots, 0)$ и $\mathbf{1} = (1, \ldots, 1)$. Постройте шары $V_{\mathbf{0}}(t)$, $V_{\mathbf{1}}(t)$ в графе четырехмерного куба для разных t. Найти $V_{\mathbf{0}}(2) \cap V_{\mathbf{1}}(2)$.

4) Пусть $a, b \in \mathbb{B}_2^n$ и $\rho(a, b) = 2t$. Найти число точек пересечения двух шаров $V_a(t) \cap V_b(t)$.

5) Убедиться, что наибольшее возможное расстояние между вершинами n-мерного куба равно n. Найти число различных пар вершин таких, что $\rho(a, b) = n$.

6*) Найти наибольшее число m такое, что в $\mathbb{B}_2^n$ существует равносторонний треугольник (a, b, c) с $\rho(a, b) = \rho(b, c) = \rho(a, c) = m$. (Можете рассмотреть $\mathbb{B}_2^4$.)

Задача 2*. **Линейные отображения и метрика Хэмминга.**

Во второй задаче Листка 1 мы установили, что автоморфизм метрического пространства $\mathbb{B}_2^n$ является линейным отображением пространства $\mathbb{F}_2^n$ тогда и только тогда, когда он является перестановкой координат.

Лабораторная работа: исследовать действие элементов группы $GL_3(\mathbb{F}_2)$ в метрическом пространстве $\mathbb{B}_2^3$.

Задача 3. **Булевы функции и пространство $\mathbb{B}_2^n$.**

1) Докажите, что множество булевых функций от m переменных со значениями в $\mathbb{F}_2$ изоморфно векторному пространству $\mathbb{F}_2^{2^m}$. Множество значений булевой функции $f(x_1, \ldots, x_m)$ есть вектор в $\mathbb{F}_2^{2^m}$. Вес Хэмминга этого вектора называется `весом` $w(f)$ `булевой функции` f.

2) Докажите, что каждую булеву функцию от m переменных можно однозначно представить как полиномиальную функцию над $\mathbb{F}_2$ от m переменных $x_1, \ldots, x_m$.

3*) `Степенью булевой функции` $\deg(f)$ $(f \not\equiv 0)$ называется наибольшая степень одночлена $x_{i_1} \cdot \ldots \cdot x_{i_k}$, входящего в полиномиальное представление. Пусть $f \not\equiv 0$ и $\deg(f) = d$. Доказать, что

$$2^{m-d} \leq w(f) \leq 2^m - 2^{m-d}.$$

Задача 4. **Булевы функции и код Рида-Маллера (Reed–Muller).**

Пусть $\mathcal{B}_m$ — линейное пространство над $\mathbb{F}_2$ всех булевых функций от m переменных, $0 \le r \le m$.

1) Доказать, что подмножество всех булевых функци таких, что $\deg(f) \le r$ образует подпространство $RM(r,m)$ в $\mathcal{B}_m$.

2) Доказать, что

$$\dim(RM(r,m)) = \sum_{k=0}^{r} C_m^k = |V_0(r)|.$$

3) Доказать, что $RM(r,m)^\perp = RM(m-r-1,m)$.

4*) Доказать, что минимальное расстояние кода $RM(r,m)$ равно 2^{m-r}.

5*) Описать порождающую матрицу кода Рида-Маллера $RM(1,m)$.

6*) *(Повторение линейной алгебры.)* `Аффинным подпространством` размерности m в $\mathbb{F}_2^n$ называется множество вида $V_m + u$, где V_m — m-мерное линейное подпространство, а $u \in \mathbb{F}_2^n$.

Дать короткое доказательство того, что каждое аффинное подпространство $\mathbb{F}_2^n$ задается (неоднородной) системой линейных уравнений типа

$$Ax = b.$$

Чему равен ранг матрицы A?

7*) В качестве приложения предыдущего результата найти число аффинных подпространств коразмерности k в $\mathbb{F}_2^n$. (Начните с $k = 1$, 2.)

8**) Слова минимального веса кода Рида-Маллера $RM(r,m)$ совпадают с векторами инциндентности в $\mathbb{F}_2^{2^m}$ аффинных подпространств коразмерности r.

9*) Найти группу автоморфизмов кода Рида-Маллера.