Теория Кодирования как введение в Алгебру и Арифметику

ЛИСТОК 3 (27 октября 2020)

Целочисленные квадратичные решётки и их расширения

Задача 1. **Решётки A_n и D_n.** Положим

$$A_n = \{(x_1, \ldots, x_{n+1}) \in \mathbb{Z}^{n+1} : x_1 + \ldots + x_{n+1} = 0\},$$

$$D_n = \{(x_1, \ldots, x_n) \in \mathbb{Z}^n : x_1 + \ldots + x_n \in 2\mathbb{Z}\}.$$

1) Показать, что A_n и D_n – чётные квадратичные решётки для любого n.

2) Пусть $(e_1, \ldots, e_n)$ евклидов базис решётки $\mathbb{Z}^n \subset \mathbb{R}^n$. Доказать, что векторы $e_1 - e_2$, $e_2 - e_3$, …, $e_n - e_{n+1}$ образуют базис решётки A_n для $n \geq 1$, а векторы $e_1 - e_2$, $e_2 - e_3$, …, $e_{n-1} - e_n$ и $e_{n-1} + e_n$ – базис решётки D_n для $n > 1$. Найти базис D_1.

3) Доказать, что решётка D_2 изоморфна ортогональной сумме двух решёток $A_1 \perp A_1$, а D_3 изоморфна A_3. Сравните две решётки A_1 и D_1 ранга один.

4) Найти матрицы Грама решёток A_n и D_n в базисах из пункта 2. Можете ли вы найти детерминанты этих матриц Грама?

5) **Корнями** (или 2-корнями) целочисленной квадратичной решётки L называются элементы $v \in L$ такие, что $v^2 = (v, v) = 2$. Найти число корней решёток A_n и D_n. Доказать, что A_n и D_n не являются изоморфными для $n \geq 4$.

6) Дать описание ортогональной группы $O(\mathbb{Z}^n)$ целочисленной евклидовой решётки $\mathbb{Z}^n$.

7) Пусть $v \in L$ и $v^2 = (v, v) = 2$. Доказать, что отражение $\sigma_v(l) = l - \frac{2(l,v)}{(v,v)}v$ относительно гиперплоскости ортогональной вектору v переводит решётку L в себя, т.е. $\sigma_v \in O(L)$.

8*) Исследовать отражения σ_v относительно корней в решётках A_n и D_n. Найти ортогональные группы $O(D_n)$ и $O(A_n)$ этих решёток.

Задача 2. **Четная унимодулярная решётка E_8.**

1) Показать, что векторы e_i и $\frac{1}{2}(e_1 + e_2 + \ldots + e_n)$ принадлежат решётке D_n^*, двойственной D_n. Построить какой-нибудь базис двойственной решётки D_n^*. Построить базис решетки D_n^*, двойственный к базису из Задачи 1-2.

2) Найти дискриминант D_n, рассматривая следующие вложения решёток

$$D_n < \mathbb{Z}^n = (\mathbb{Z}^n)^* < D_n^*.$$

3) Доказать, что расширение

$$E_8 =< D_8, \ \frac{1}{2}(e_1 + \ldots + e_8) >$$

является четной целочисленной квадратичной решеткой.

4) Доказать, используя идею из пункта 2, что четная решетка E_8 является унимодулярной: $E_8^* = E_8$.

5) Дать координатное описание чётной унимодулярной решётки E_8 и доказать, что она содержит ровно 240 корней.

Задача 3. **Дискриминантная группа решётки D_n.**

1) Найти конечную абелеву группу D_n^*/D_n.

2) Дать полное описание конечной квадратичной формы дискриминантной группы $D(D_n)$ для любого $n \geq 1$. Какая периодичность возникает?

3) Исследовать тотально изотропные подгруппы дискриминантной группы $D(D_n)$ в смысле конечной билинейной формы b_{D_n} и в смысле конечной квадратичной формы q_{D_n}.

4) Решётка D_n – подрешётка нечётной решётки $\mathbb{Z}^n$. Для какого ранга n решётка D_n является максимальной чётной решёткой?

5) Построить чётные унимодулярные решётки D_{8n}^+.

6) Найти число корней (векторов v таких, что $(v,v) = 2$) в решётках D_{8n}^+ при $n > 1$. Сравнить с результатом Задачи 2-5.

7*) Доказать, что чётные унимодулярные решётки D_{16}^+ и $E_8 \perp E_8$ не являются изоморфными.

8*) Доказать, что чётные унимодулярные решетки D_{24}^+, $D_{16}^+ \perp E_8$ и $E_8 \perp E_8 \perp E_8$ не являются попарно изоморфными квадратичными решетками ранга 24.

Задача 4. **Унимодулярные надрешётки и код Хэмминга.**

1) Показать, что решётка $4A_1 = A_1 \perp A_1 \perp A_1 \perp A_1$ не является максимальной в классе чётных целочисленных квадратичных решёток. Доказать, что любое ее чётное расширение изоморфно решётке D_4.

2) Построить чётную унимодулярную надрешётку решётки $8A_1$, используя четное расширение $H_4^{(8)}$ кода Хэмминга.

Построить чётные унимодулярные надрешётки, указаных ниже решёток:

3*) $D_4 \perp D_4$, $D_3 \perp D_5$, $D_2 \perp D_6$, $D_1 \perp D_7$.

4*) $2A_4 = A_4 \perp A_4$.

5*) $A_3 \perp A_5$.

6*) $6A_2 = A_2 \perp A_2 \perp A_2 \perp A_2 \perp A_2 \perp A_2$.

Примеры 3–6 иллюстрируют элементы теории кодирования над кольцами.