

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение
высшего образования
**«Национальный исследовательский
Нижегородский государственный университет им. Н.И. Лобачевского»
(ННГУ)**

Институт информационных технологий, математики и механики

Кафедра: алгебры, геометрии и дискретной математики

Направление подготовки: «Программная инженерия»
Профиль подготовки: «Разработка программно-информационных систем»

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА БАКАЛАВРА

на тему:
**«Алгоритмы для нахождения Эрмитовой нормальной формы и ближайшего
вектора решетки»**

Выполнил(а): студент(ка) группы

_____ Д.В. Огнев

Подпись

Научный руководитель:

Доцент, кандидат физико-
математических наук

_____ С.И. Весёлов

Подпись

Нижний Новгород
2022

Аннотация (ДОПИСАТЬ)

Тема выпускной квалификационной работы бакалавра – «Алгоритмы для нахождения Эрмитовой нормальной формы и ближайшего вектора решетки».

Ключевые слова: решетки, Эрмитова нормальная форма, проблема ближайшего вектора.

Данная работа посвящена изучению задач теории решеток и методов их решения. В работе изложены основные понятия, связанные с решетками, и разбор алгоритмов для нахождения Эрмитовой нормальной формы и ближайшего вектора решетки.

Целью работы является программная реализация алгоритмов для решения задач.

Объем работы - ...

Содержание

1. Список условных обозначений и сокращений (TODO)	4
2. Введение (TODO)	5
3. Основная часть (TODO)	6
3.1. Основные понятия	6
3.2. Обзор используемых инструментов.....	6
3.3. Алгоритм для нахождения ЭНФ для матриц с полным рангом строки.....	6
3.4. Алгоритм для нахождения ЭНФ для любых матриц.....	6
3.5. Применение ЭНФ	6
3.6. Проблема ближайшего вектора	6
3.7. Жадный метод (Greedy): алгоритм ближайшей плоскости Бабая.....	6
3.8. Метод ветвей и границ (Branch and Bound): алгоритм перечисления	6
3.9. Обзор программной реализации	6
4. Заключение (TODO)	7
5. Список источников (TODO)	8
Приложения (TODO)	9

1. Список условных обозначений и сокращений (TODO)

ПБВ (CVP) – проблема ближайшего вектора (Closest vector problem)

ЭНФ (HNF) – Эрмитова нормальная форма (Hermite normal form)

B&B – Branch and bound

2. Введение (TODO)

Текст введения

3. Основная часть (TODO)

3.1. Основные понятия

Решетка. Пусть $\mathbf{B} = [\mathbf{b}_1, \dots, \mathbf{b}_n] \in \mathbb{R}^{d \times n}$ - линейно независимые вектора из \mathbb{R}^d . Решетка, генерируемая от \mathbf{B} есть набор

$$\mathcal{L}(\mathbf{B}) = \{\mathbf{B}\mathbf{x} : \mathbf{x} \in \mathbb{Z}^n\} = \left\{ \sum_{i=1}^n x_i \cdot \mathbf{b}_i : \forall i \ x_i \in \mathbb{Z} \right\}$$

всех целочисленных линейных комбинаций столбцов матрицы \mathbf{B} . Матрица \mathbf{B} называется базисом для решетки $\mathcal{L}(\mathbf{B})$. Число n называется рангом решетки. Если $n = d$, то решетка $\mathcal{L}(\mathbf{B})$ называется решеткой полного ранга или полноразмерной решеткой в \mathbb{R}^d .

3.2. Обзор используемых инструментов

3.3. Алгоритм для нахождения ЭНФ для матриц с полным рангом строки

3.4. Алгоритм для нахождения ЭНФ для любых матриц

3.5. Применение ЭНФ

3.6. Проблема ближайшего вектора

3.7. Жадный метод (Greedy): алгоритм ближайшей плоскости Бабая

3.8. Метод ветвей и границ (Branch and Bound): алгоритм перечисления

3.9. Обзор программной реализации

4. Заключение (TODO)

В ходе выполнения выпускной квалификационной работы бакалавра были реализованы алгоритмы на языке C++ для нахождения ЭНФ и решения ПБВ.

Полученную программную реализацию можно использовать как библиотеку и подключать в другие проекты.

Был создан Github репозиторий, который содержит в себе все исходные файлы. Программная реализация использует CMake для автоматической сборки.

5. Список источников (TODO)

Тут будет список источников

Приложения (TODO)

Тут будет листинг кода