БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

МЕХАНИКО-МАТЕМАТИЧЕСКИЙ ФАКУЛЬТЕТ

Кафедра дифференциальных уравнений и системного анализа

Аннотация к дипломной работе

LLL-алгоритм

Гирис Анастасия Олеговна

Научный руководитель:
кандидат физ.-мат. наук,
доцент Д.Н.Чергинец

2014

В дипломной работе 35 страниц, 10 источников, одно приложение.

РЕШЕТКИ, БАЗИС, ОРТОГОНАЛИЗАЦИЯ ГРАМА-ШМИДТА, LLL-ПРИВЕДЕННЫЙ БАЗИС, ЗАДАЧА О РЮКЗАКЕ, РЮКЗАЧНАЯ КРИПТОСИСТЕМА, КРИПТОАНАЛИЗ, ЯДРО МАТРИЦЫ, ОБРАЗ МАТРИЦЫ, ЛИНЕЙНАЯ ЗАВИСИМОСТЬ.

В дипломной работе рассмотрен алгоритм построения LLL-приведенного базиса целочисленной решетки за полиномиальное время.

Цель работы – изучить и реализовать LLL-алгоритм, рассмотреть его применение в криптографии и других областях математики и информатики.

В дипломной работе получены следующие результаты:

1) построена функция, которая приводит произвольный базис решетки к LLL-приведенному;

2) проведен криптоанализ шифра Меркля-Хеллмана при помощи LLL-алгоритма;

3) реализованы функции вычисления ядра и образа линейного отображения евклидова пространства и нахождения целочисленной линейной зависимости заданных действительных чисел, использующие LLL-алгоритм;

4) рассмотрен ряд примеров, показывающих корректность работы всех построенных функций.

Дипломная работа написана на основе комплексного исследования работ зарубежных и российских авторов. Практическая основа исследования заключается в реализации алгоритмов в пакете Wolfram Mathematica, изученных в теоретической части работы.

Дипломная работа выполнена автором самостоятельно.

Thesis project is presented in the form of an explanatory note of 35 pages, 10 references, 1 application.

LATTICE, BASIS, GRAM-SCHMIDT ORTHOGONALIZATION, LLL-REDUCED BASIS, THE KNAPSACK PROBLEM, KNAPSACK CRYPTOSYSTEMS, CRYPTANALYSIS, KERNEL OF THE MATRIX, LINEAR DEPENDENCE.

In the thesis project the algorithm of creation of the LLL-reduced basis of an integer lattice for polynomial time is considered.

The work purpose – to study and realize LLL algorithm, to consider its application in cryptography and other areas of mathematics and informatics.

The main results of the thesis projects are as follows:

1) function, which leads any basis of a lattice to the LLL-reduced is constructed;

2) cryptoanalysis of the code of Merklya-Hellman using LLL algorithm is carried out;

3) functions of calculation of a kernel and image of linear mapping of Euclidean space and finding of integer linear dependence of the set real numbers, using LLL algorithm are realized;

4) a number of the examples showing a correctness of work of all constructed functions is considered.

The thesis project is written on the basis of complex research of works of foreign and Russian authors. The practical basis of research consists in realization algorithms in the Wolfram Mathematica package, studied in theoretical part of work.

The thesis project was done solely by the author.