# ЗАЩИТА КАНАЛОВ ПЕРЕДАЧИ И ХРАНЕНИЯ ДАННЫХ НА ОСНОВЕ АЛГЕБРАИЧЕСКИХ РЕШЕТЧАТЫХ КОДОВ

*Алисеенко М.А.*

*Белорусский государственный университет информатики и радиоэлектроники*
*г. Минск, Республика Беларусь*

*Саломатин С.Б. – канд. тех. наук, доцент*

Рассмотрены алгебраические решетки, задачи кратчайшего и ближайшего векторов решетки. Приведены выражения кратчайшего вектора решетки и порождающая матрица решетки. Рассмотрен алгоритм преобразования кратчайшего ортогонального базиса решетки.

Алгебраическая решетка является конечно порожденной аддитивной подгруппой множества $R^n$. Решетку L можно представить как множество целочисленных линейных комбинаций n линейно независимых базисных векторов в m-мерном евклидовом пространстве, где m и n – размерность и ранг решетки соответственно. Решетки, у которых размерность m и ранг n равны, называются полноразмерными [1]. Определитель решетки равен объему фундаментального параллелотопа, образованного базисом $B = b_1,\ldots,b_n$, рисунок 1. Базис решетки не единственен: матрица перехода от одного базиса решетки к произвольному другому унимодулярна, т. е. ее определитель равен ±1, поэтому детерминант решетки не зависит от выбора базиса [2]. Произведение базисной и унимодулярной матрицы даст новый базис решетки.

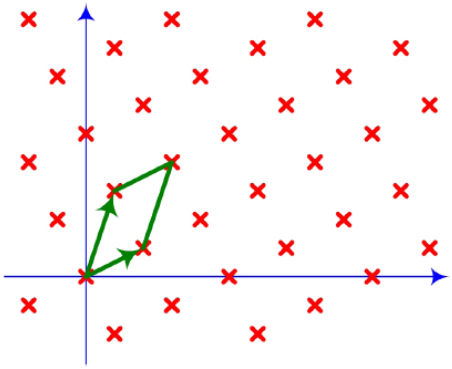

Рисунок 1 – Фундаментальный параллелотоп решетки, образованный базисом

Некоторые задачи теории решеток используются для создания схем стойкой криптографии, которые устойчивы для квантовых вычислений. Задача нахождения кратчайшего вектора (SVP, Shortest Vector Problem) подразумевает нахождение в заданном базисе решетки ненулевой вектор по отношению к определенной нормали. Математическая запись кратчайшего вектора:

$$a^* = \underset{a\in Z^n\setminus\{0\}}{\arg.\min}\|Aa\|^2 = \underset{a\in Z^n\setminus\{0\}}{\arg.\min} a^T G a, \quad (1)$$

где A – полноранговая матрица, являющаяся базисом решетки,

$G = A^T A$ – матрица Грамма решетки.

Задача нахождения ближайшего вектора (CVP, Closest Vector Problem) – нахождение вектора в решетке по заданному базису и некоторому вектору, не принадлежащему решетке, при этом максимально схожего по длине с заданным вектором. Математическая запись ближайшего вектора к произвольному вектору y:

$$a^* = \underset{a\in Z^n}{\arg.\min}\|Aa - y\|^2 = \underset{a\in Z^n}{\arg.\min}(a^T G a - 2y^T A a + y^T y). \quad (2)$$

По аналогии с линейными кодами решетка может быть выражена через порождающую матрицу и целочисленный коэффициент, что показано в выражении:

$$\Lambda = \{\lambda = \underbrace{[b_1 \vdots \cdots \vdots b_n]}_{G} a : a \in Z^n\}. \quad (3)$$

Под кратчайшим вектором решетки понимается вектор, длина которого:

$$\lambda(\Lambda) = \min_{x,y\in\Lambda, x\neq y}\|x - y\| = \min_{x\in\Lambda, x\neq 0}\|x\|. \quad (4)$$

Первый последовательный минимум, под которым понимается наименьший радиус окружности (шара), соответствует длине кратчайшего вектора решетки, рисунок 2.

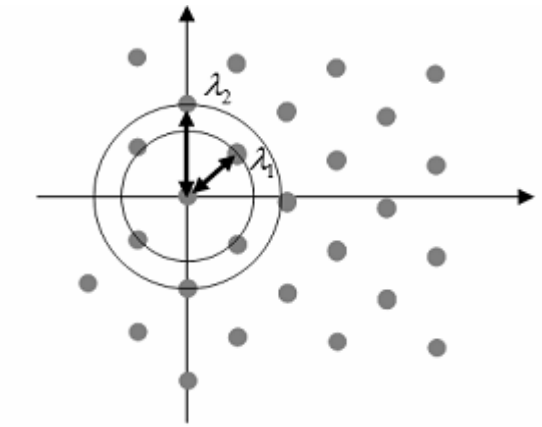


Рисунок 2 – Кратчайший базис-радиус решетки

Задачи теории решеток можно решить, если базис решетки редуцирован, т.е. состоит из относительно коротких почти ортогональных векторов. На сегодняшний день эффективным алгоритмом редукции базиса решетки является алгоритм LLL (Ленстры-Ленстры-Ловаса).

За полиномиальное время алгоритм преобразует базис на решетке в кратчайший почти ортогональный базис на этой же решетке. Для векторного пространства $R^n$ процесс Грама-Шмидта позволяет преобразовать произвольный базис в ортонормированный («идеал», к которому стремится LLL-алгоритм), но не гарантирует того, что на выходе каждый из векторов будет целочисленной линейной комбинацией исходного базиса. Таким образом, полученный в результате набор векторов может и не являться базисом исходной решётки [3]. Необходима проверка на соблюдение условий нормы и Ловаса, при необходимости поменять местами вычисляемые векторы и пересчитать редуцированные векторы и их коэффициенты.

Алгоритм построения LLL-приведенного базиса делает $O(n^4 \log B)$ арифметических операций. При этом целые числа, встречающиеся в ходе работы алгоритма, имеют двоичную длину $O(n \log B)$ битов.

**Список использованных источников:**

1. Программный комплекс приведения базиса целочисленных решеток / О.В. Кузьмин, В.С. Усатюк // Программые продукты и системы №4, 2012. – С.180-183.

2. Использование ортогонализации Грама-Шмидта в алгоритме приведения базиса решетки для протоколов безопасности / А.В. Пискова, А.А. Менщиков,А.Г. Коробейников // Вопросы о кибербезопасности №1(14), 2016. – С.47-52.

3. Lattice Reduction / S. Galbraith // Mathematics of Public Key Cryptography, 2012. – P. 365-381.