Project 3
Lattices

KG

February 13, 2024

1 Introduction

In this project, we will implement algorithms for lattices, in particular algorithms for the closest vector problem.

2 Tasks

You will write a report using LaTeX. The report should include an explanation of what you have done, a description of your implementation, the theoretical analysis, any experimental results with explanations and a code listing.

For this project, you should probably rely on any linear algebra libraries available to you, though any implementation of lattice-specific algorithms should not be used.

Throughout this project, you may make reasonable assumptions about the lattices you will work with (such as restricting to integral lattices).

1. Implement: Estimating the closest lattice point Implement Babai's rounding method or Babai's nearest plane algorithm for using a lattice basis to make an estimate for the closest lattice point.

2. Implement: Searching for the closest lattice point Implement an algorithm for searching for the closest vector in a lattice (that is, enumerating all points near a given point).

3. Implement: LLL algorithm Implement the LLL algorithm.

4. Optional: Implement: BKZ algorithm Implement an algorithm to find a BKZ basis.

5. Run: Finding closest vectors Find a suitable sequence of lattices (each lattice described by a lattice basis) of increasing dimension, together with target vectors not in the lattices. (Starting with the LWE problem, as in the lectures, is one way.)

For each lattice in your sequence, run the LLL algorithm from Task 3 to get a better basis, then use the methods from Task 1 to estimate the closest lattice vector to your target vector. Then use the methods from Task 2 to find the closest lattice vector to your target vector. Is there any difference in your results.

Given no more computational resources than 24 single-core hours, how large dimensions can your code handle? Plot the runtime cost of the algorithms. Do they correspond to the theoretical estimates?

If you did Task 4, redo the above using BKZ-reduced bases with suitable parameters. Does anything change?