Summary

Algorithms for Finding Short Vectors in Algebraic Lattices

E. Kirshanova

October 12, 2019

A Euclidean lattice is a finitely generated additive subgroup in $\mathbb{R}^n$. The Shortest Vector Problem (SVP) is the core computational task on Euclidean lattices. Given a lattice (often compactly) represented by its basis, SVP asks to find a non-zero vector in the lattice. The problem has a long history and appears in many areas of mathematics and computer science including algorithmic number theory, cryptography and communication theory.

Although the algorithmic aspects of generic lattices are quite well-understood, so-called algebraic lattices corresponding to modules over the ring of integers of a number field have been much less studied. This is unsatisfactory as finding short vectors in such lattices is important in number theory (algorithms for class group computations) and cryptography. Designing more efficient SVP algorithms for algebraic lattices is the purpose of this research proposal.

First, we design a lattice-basis reduction algorithm that would build on carefully crafted sieving algorithms for rank-2 module lattices. We do so by extending ideas from the recent work of Lee, Pellet–Mary, Stehle, and Wallet (AsiaCrypt 2019) that aims at finding pairs of vectors in order to find relatively short vector in rank-2 modules. The challenges here include extending their techniques to different target norms (we would like to find much shorter vectors) and possibly to higher-rank lattices. The ultimate goal is to develop and analyse lattice basis reduction algorithms for module lattices that operate on pseudo-bases (i.e., that take into account the algebraic nature of the lattice).

Second, we consider special families of lattices that admit asymptotically faster algorithms than generic lattices of the same rank. One example of such fields are multiquadratic fields. It was recently shown (Bauch, Bernstein, de Valence , Lange, and van Vredendaal, 2017) that these fields admit fast algorithms for finding short generators of principal ideals. We extend these results to non-principal ideals and to modules of higher ranks by analysing geometric properties of generators of Stickelberger ideal of the ring of integers of multiquadratic extensions and by using our above results on basis reduction for modules.

Our results can be used as tools in computational number theory and in cryptanalysis of modern lattice-based constructions.