Random walks on Arakelov class groups

Boer, K. de

Summary

The main topic of this PhD thesis is the *Arakelov ray class group* of a number field, an algebraic object that contains both the ideal class group structure and the unit group structure. The main result consists of the fact that certain specific *random walks* on the Arakelov ray class group result in a target point that is uniformly distributed on this group, under the assumption of an extended version of the Riemann Hypothesis (Chapter 4). Almost all other results of this work are consequences of this fact.

As a first direct application, using these random walks on the Arakelov class group one can show that finding a short vector in a *arbitrarily chosen* ideal lattice is no harder than finding a short vector in a *random ideal lattice* of a fixed number field (Chapter 5). In other words, finding short vectors in the 'most difficult' ideal lattice is not much harder than finding short vectors in a random ideal lattice.

A second application uses these random walks to rigorously and efficiently sample elements from ideals of number fields, in such a way that the quotient of this element and the ideal lies in a pre-chosen ideal set. The success probability of this sampling procedure turns out to be proportional to the analytic number-theoretic *density* of this ideal set. One obtains a particularly interesting application of this result when one chooses the ideal set to be the set of prime ideals and when the number field equals a cyclotomic number field. In that case the theorem reads: one can efficiently sample elements in ideals of cyclotomic number fields such that the quotient of the concerning element and ideal is near-prime, i.e., a product of a large prime ideal and several very small prime ideals (Chapter 6).

The purpose of the above sampling algorithm is to transform heuristic arguments into rigorous proofs in certain number-theoretic algorithms, like ideal class group and unit group algorithms. We successfully achieve this goal for an algorithm that computes the power residue symbol: we give a formal proof of the polynomial running time of that algorithm. Before the writing of this thesis, this running time was only heuristically estimated to be polynomially bounded (Chapter 7).

A more self-contained part of this thesis consists of a quantum algorithm of the *continuous hidden subgroup problem* and a full, rigorous analysis thereof (Chapter 3). This algorithm can be applied to *compute* Arakelov ray class groups explicitly; though this is still a topic of research.