Euclidean Lattice Reduction

Chee Yap

Courant Institute, New York University
251, Mercer Street
New York, NY 10012
email: yap@cs.nyu.edu

Techniques from the geometry of numbers was first introduced into algorithmics by A.K. Lenstra. In particular, the lattice reduction algorithm (LLL) of Lenstra-Lenstra-Lovász has proved very useful in many areas. The related problem of computing the shortest lattice vector can be seen as the higher dimensional analogue of the GCD problem. In the plane, there is a shortest vector algorithm attributed to Gauss that is analogous to the Euclidean GCD algorithm. We show that in this planar case, the shortest vector problem has complexity $O(n \log^2 n \log\log n)$, matching the known integer GCD bound. This extends Schönhage's GCD technique to a higher dimension.

The extension is interesting because unlike integer GCD where the reduction terminates with the value 0, the Gaussian algorithm terminates in a non-zero vector in general. This causes difficulty for the usual Half-GCD idea. We introduce the "coherent remainder sequence" in our algorithm and analysis. We note that the Half-GCD technique is different from several other techniques that has been used to speed up the lattice reduction algorithm of LLL.

We describe extensions to related problems in recent joint work with Tom Dubé: First, the problem of Gaussian integer GCD. This is simpler than planar lattice reductions in that we have a Euclidean domain, but has added complications because the reduction group is not the classical modular group. Still, we can achieve the same complexity as integer GCD. Second, we discuss the Euclidean lattice reduction method in higher dimensions.