Solving SVP (and CVP) in $2^n$ Time via Discrete Gaussian Sampling

Abstract:

We show a $2^{n+o(n)}$-time algorithm for the Shortest Vector Problem on n-dimensional lattices (improving on the previous best-known algorithm of Micciancio and Voulgaris, which runs in time $4^{n+o(n)}$). The algorithm uses the elementary yet powerful observation that, by properly combining samples from a Gaussian distribution over the lattice, we can produce exact samples from a narrower Gaussian distribution on the lattice. We use such a procedure repeatedly to obtain samples from an arbitrarily narrow Gaussian distribution over the lattice, allowing us to find a shortest vector.

Both the algorithm and the analysis are quite simple in hindsight. (The main technical tool is an identity on Gaussian measures with a simple geometric proof originally due to Riemann.) If time allows and interest merits, we will discuss a more technical variant of this algorithm that solves the Closest Vector Problem (a seemingly harder problem) in the same asymptotic running time.


Email: dana.kalderon@weizmann.ac.il * Phone: (08)9343349 * Fax: (08)9344308