Computer Science > Computational Complexity

Deterministic Construction of an Approximate M-Ellipsoid and its Application to Derandomizing Lattice Algorithms

Daniel Dadush, Santosh Vempala

(Submitted on 27 Jul 2011)

We give a deterministic O(log n)^n algorithm for the {\em Shortest Vector Problem (SVP)} of a lattice under {\em any} norm, improving on the previous best deterministic bound of n^O(n) for general norms and nearly matching the bound of 2^O(n) for the standard Euclidean norm established by Micciancio and Voulgaris (STOC 2010). Our algorithm can be viewed as a derandomization of the AKS randomized sieve algorithm, which can be used to solve SVP for any norm in 2^O(n) time with high probability. We use the technique of covering a convex body by ellipsoids, as introduced for lattice problems in (Dadush et al., FOCS 2011).

Our main contribution is a deterministic approximation of an M-ellipsoid of any convex body. We achieve this via a convex programming formulation of the optimal ellipsoid with the objective function being an n-dimensional integral that we show can be approximated deterministically, a technique that appears to be of independent interest.

Subjects:	**Computational Complexity (cs.CC)**; Functional Analysis (math.FA)
MSC classes:	52C07, 68Q25
Cite as:	**arXiv:1107.5478 [cs.CC]**
	(or **arXiv:1107.5478v1 [cs.CC]** for this version)

Submission history

From: Santosh Vempala [view email]

[v1] Wed, 27 Jul 2011 14:05:55 GMT (25kb)

Which authors of this paper are endorsers?