Babai, László

On Lovász' lattice reduction and the nearest lattice point problem (shortened version). (English) Zbl 0569.10015

Theoretical aspects of computer science, 2nd ann. Symp., Saarbrücken/Ger. 1985, Lect. Notes Comput. Sci. 182, 13-20 (1985).

[For the entire collection see Zbl 0561.00020.]

Answering a question of Vera Sós, we show how Lovász' lattice reduction can be used to find a point of a given lattice, nearest within a factor of c^d ($c = const$) to a given point in $\mathbb{R}^d$. We prove that each of two straightforward fast heuristic procedures achieves this goal when applied to a lattice given by a Lovász-reduced basis. The verification of one of them requires proving a geometric feature of Lovász-reduced bases: a c_1^d lower bound on the angle between any member of the basis and the hyperplane generated by the other members, where $c_1 = \sqrt{2/3}$.

As an application, we obtain a solution to the nonhomogeneous simultaneous diophantine approximation problem, optimal within a factor of C^d. In another application, we improve the Grötschel-Lovász- Schrijver version of H. W. Lenstra's integer linear programming algorithm. The algorithms, when applied to rational input vectors, run in polynomial time. For lack of space, most proofs are omitted. A full version will appear in Combinatorica.

MSC:

11H06 Lattices and convex bodies (number-theoretic aspects)
11H55 Quadratic forms (reduction theory, extreme forms, etc.)
68W99 Algorithms in computer science
52C07 Lattices and convex bodies in n dimensions (aspects of discrete geometry)
90C10 Integer programming

Keywords:

computational number theory; Lovász-reduced basis; nonhomogeneous simultaneous diophantine approximation; Grötschel-Lovász-Schrijver version; Lenstra's integer linear programming algorithm; polynomial time