COMBINATORICA 6 (1) (1986) 1—13

ON LOVÁSZ' LATTICE REDUCTION AND THE NEAREST LATTICE POINT PROBLEM

L. BABAI

Received 11 June 1984
Revised 20 August 1985

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 $\mathbf{R}^d$. 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.

1. Introduction

A *lattice* in $\mathbf{R}^d$, defined by the basis $B=\{b_1, \ldots, b_d\}$ of $\mathbf{R}^d$, is the set $L=\sum_{i=1}^{d} \mathbf{Z}b_i$ of all integral linear combinations of B. Finding the shortest non-zero vector in L is a fundamental algorithmic problem, and lies at the heart of the solution of many diophantine problems in arithmetics, including integer programming (H. W. Lenstra, Jr. [12]), finding irreducible factors of polynomials (A. K. Lenstra [10]), minimal polynomials of algebraic numbers (Kannan, Lenstra, Lovász [8]) and simultaneous diophantine approximation in the first place (Lovász, see [11]).

Although the shortest vector problem may be NP-hard for integral input vectors (it is known to be NP-hard with respect to maximum norm, P. van Emde Boas [3]), a vector at most C^d times the shortest one suffices for most applications. These applications include those mentioned above as well as applications to the ellipsoid method in linear programming (Lovász [13]; cf. [5]), recent attacks on knapsack-based crypto-systems (Adleman [1], Shamir [15], Lagarias and Odlyzko [9]), and the disproof of Mertens' century-old conjecture in number theory (Odlyzko and te Riele,

AMS subject classification (1980): 68 C 25, 10 F 10, 10 F 15, 90 C 10

[14]). All these applications were made possible by *Lovász' lattice reduction* algorithm (see [11]), originally designed to give nearly optimal simultaneous diophantine approximation which, in turn, arose, as far as Lovász was concerned, from the need to eliminate the annoying full-dimensionality condition from the ellipsoid method in linear programming ([13], see Grötschel, Lovász, Schrijver [5]). Odlyzko reports that Lovász' algorithm performs substantially better in practice than predicted by the C^d theoretical worst-case bound. This observation was crucial for the number theoretic application [14].

Diophantine problems usually come in homogeneous and nonhomogeneous versions, and usually both have similar answers but the nonhomogeneous cases are more difficult to handle (cf. Cassels [2]).

In the case of the short lattice vector problem (a *homogeneous* approximation problem: we approximate zero), the corresponding *nonhomogeneous* problem is to find *the nearest lattice point to a given point in* $\mathbf{R}^d$. This problem is known to be NP-hard even in the Euclidean case (P. van Emde Boas [3]). However, as we shall see, a lattice point within C^d times the distance from the nearest one can be found efficiently (in polynomial time if the basis vectors have rational coordinates). Here, C is an absolute constant, and d is the dimension. We prove that each of two trivial heuristic procedures (Section 3) achieve this goal if we start from a Lovász-reduced basis.

The most important and immediate application of Lovász' lattice reduction algorithm was his (homogeneous) diophantine approximation algorithm, previously solved only in dimension one by the classical method of continued fractions. Vera Sós [17] gave a method, based on continued fractions, to solve the one-dimensional nonhomogeneous case optimally. We shall show how the approximate nearest lattice point procedure leads to nearly optimal nonhomogeneous simultaneous diophantine approximation (Section 7).

In Section 8, we improve the Grötschel—Lovász—Schrijver version of H. W. Lenstra's integer linear programming algorithm.

We note that R. Kannan [7] considered some of the problems discussed here (cf. Sect. 8 of this paper). He solved the nearest lattice point problem in d^{cd} arithmetic operations. He also showed that a shortest vector oracle can be used to find, in polynomial time, a lattice point nearest within a factor d to a given point in d-space.

Let me remark that I don't see any a priori reason why the nonhomogeneous approximation problem could not actually be *easier* than the homogeneous one.

Problem. Suppose we are given an oracle which solves the nearest lattice point problem within a constant factor, i.e., on an input (L, x) $(x \in \mathbf{R}^d$, L a lattice in $\mathbf{R}^d)$ the oracle outputs $w \in L$ such that $|w-x| \leqq C|u-x|$ for any $u \in L$. Can such an oracle be used to solve, in polinomial time, the shortest vector problem within a factor of $\exp(d^{1-\varepsilon})$ for some fixed $\varepsilon > 0$? (That is, on an input L, a lattice in $\mathbf{R}^d$, output a nonzero vector $w \in L$ such that $|w| \leqq |u| \exp(d^{1-\varepsilon})$ for any $u \in L$, $u \neq 0$.)

Acknowledgements. I am indebted to Vera Sós for drawing my attention to the importance of nonhomogeneous diophantine approximation and the approximately nearest lattice point problems. I would like to thank László Lovász for telling me about his lattice reduction algorithm and its numerous consequences, immediately after he had made the discovery at the end of 1981. Excellent seminar lectures by Éva