Babai, L.

On Lovász' lattice reduction and the nearest lattice point problem. (English) Zbl 0593.68030

Combinatorica 6, 1-13 (1986).

This is the full version of the author's paper announced in Lect. Notes Comput. Sci. 182, 13-20 (1985; Zbl 0569.10015).

MSC:

68Q25	Analysis of algorithms and problem complexity
90C10	Integer programming
11J99	Diophantine approximation, transcendental number theory
11H06	Lattices and convex bodies (number-theoretic aspects)
11H55	Quadratic forms (reduction theory, extreme forms, etc.)

Keywords:

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

Full Text: DOI

References:

[1] L. Adleman, On breaking the iterated Merkle–Hellman public key cryptosystem,Proc. 15th ACM Symp. on Theory of Computing, Boston (1983), 402–412. · Zbl 0543.94011

[2] J. W. S. Cassels,An introduction to the geometry of numbers, Springer, New York, (1971). · Zbl 0209.34401

[3] P. van Emde Boas, Another NP-complete partition problem and the complexity of computing short vectors in a lattice,Rep. MI/UVA 81-04, Amsterdam (1981).

[4] M. Grötschel, L. Lovász andA. Schrijver, The ellipsoid method and its consequences in combinatorial optimization,Combinatorica 1 (1981), 186–197.

[5] M. Grötschel, L. Lovász andA. Schrijver, Geometric methods in combinatorial optimization, in: Progress in Combinatorial Optimization (W. R. Pulleyblank, ed.),Proc. Silver Jubilee Conf. on Comb., Univ. Waterloo, Vol. 1, 1982, Acad. Press, N. Y. (1984), 167–183. · Zbl 0541.90075

[6] B. Helfrich, An algorithm to construct Minkowski-reduced lattice-bases, in:Proc. 2nd Ann. Symp. on Theoretical Aspects of Comp. Sci. (STACS 85),Springer Lect. Notes. in Comp. Sci. 182 (1985), 173–179. · Zbl 0569.10014 · doi:10.1007/BFb0024006

[7] R. Kannan, Improved algorithms for integer programming and related lattice problems,in: Proc. 15th ACM Symp. on Theory of Comp., (1983), 193–206.

[8] R. Kannan, A. K. Lenstra andL. Lovász, Polynomial factorization and nonrandomness of bits of algebraic and some transcendental numbers,in: Proc. 16th Ann. ACM Symp. on Theory of Computing, Washington, D. C. (1984), 191–200.

[9] J. Lagarias andA. M. Odlyzko, Solving low density subset sum problems,in: Proc. 24th IEEE Symp. on Foundations of Comp. Sci., (1983), 1–10. · Zbl 0632.94007

[10] A. K. Lenstra, Lattices and factorization of polynomials,Report IW 190/81, Mathematisch Centrum, Amsterdam (1981). · Zbl 0477.12002

[11] A. K. Lenstra, H. W. Lenstra, Jr. andL. Lovász, Factoring polynomials with rational coefficients,Math. Ann. 261 (1982), 515–534. · Zbl 0488.12001 · doi:10.1007/BF01457454

[12] H. W. Lenstra, Jr., Integer programming with a fixed number of variables.Math. Oper. Res. 8 (1983), 538–548. · Zbl 0524.90067 · doi:10.1287/moor.8.4.538

[13] L. Lovász,private communications, 1981–1982.

[14] A. M. Odlyzko andH. te Riele, Disproof of the Mertens conjecture,J. reine angew. Math. 357 (1985), 138–160. · Zbl 0544.10047 · doi:10.1515/crll.1985.357.138

[15] A. Shamir, A polynomial time algorithm for breaking the Merkle–Hellman cryptosystem,Proc. 23rd IEEE Symp. on Foundations of Comp. Sci., Chicago, Illinois (1982), 145–152.

[16] C. P. Schnorr, A hierarchy of polynomial time basis reduction algorithms,in: Theory of Algorithms, Proc. Conf. Pécs (Hungary) 1984,Coll. Soc. J. Bolyai, to appear. · Zbl 0642.10030

[17] Vera T. Sós, On the theory of diophantine approximation II,Acta Math. Acad. Sci. Hung. (1958), 229–241. · Zbl 0086.03902

[18] Vera T. Sós, Irregularities of partitions: Ramsey theory, uniform distribution,in: Surveys in Combinatorics, Proc. 9th British

Combinatorial Conference, 1983 (E. Keith Lloyd, ed.) London Math. Soc. Lect. Notes 82, Cambridge Univ. Press 1983.