Alekhnovich, Michael

More on average case vs approximation complexity. (English) Zbl 1242.68109

Comput. Complexity 20, No. 4, 755-786 (2011).

Summary: We consider the problem to determine the maximal number of satisfiable equations in a linear system chosen at random. We make several plausible conjectures about the average case hardness of this problem for some natural distributions on the instances, and relate them to several interesting questions in the theory of approximation algorithms and in cryptography. Namely, we show that our conjectures imply the following facts:

- Feige's hypothesis about the hardness of refuting a random 3CNF is true, which in turn implies inapproximability within a constant for several combinatorial problems, for which no NP-hardness of approximation is known.
- It is hard to approximate the NEAREST CODEWORD within factor $n^{1-\epsilon}$.
- It is hard to estimate the rigidity of a matrix. More exactly, it is hard to distinguish between matrices of low rigidity and random ones.
- There exists a secure public-key (probabilistic) cryptosystem, based on the intractability of decoding of random binary codes.

Reviewer: Reviewer (Berlin)

MSC:

68Q17	Computational difficulty of problems (lower bounds, completeness, difficulty of approximation, etc.)
68Q30	Algorithmic information theory (Kolmogorov complexity, etc.)
68W25	Approximation algorithms
03F20	Complexity of proofs
68Q10	Modes of computation (nondeterministic, parallel, interactive, probabilistic, etc.)
94A60	Cryptography

Keywords:

cryptographic primitives; hardness of approximation

Software:

McEliece

Full Text: DOI

References:

[1] M. Alekhnovich, E. Ben-Sasson, A. Razborov, A. Wigderson. Pseudorandom generators in propositional complexity. In Proceedings of the 41st IEEE FOCS, 2000. Journal version to appear in SIAM Journal on Computing. · Zbl 1096.03070

[2] Arora S., Babai L., Stern J., Sweedy Z.: Hardness of Approximate Optima in Lattices, Codes, and Linear Systems. Journal of Computer and System Sciences 54(2), 317–331 (1997) · Zbl 0877.68067 · doi:10.1006/jcss.1997.1472

[3] M. Ajtai, C. Dwork. A Public-Key Cryptosystem with Worst-Case/Average-Case Equivalence. In Proc. on 29th Annual ACM Symposium on Theory of Computing, 284–293, 1997 · Zbl 0962.68055

[4] Arora S., Lund C., Motwani R., Sudan M., Szegedy M.: Proof Verification and Hardness of Approximation Problems. Journal of ACM 45(3), 501–555 (1998) · Zbl 1065.68570 · doi:10.1145/278298.278306

[5] Arora S., Safra S.: Probabilistic Checking of Proofs: A New Characterization of NP. Journal of ACM 45(1), 70–122 (1998) · Zbl 0903.68076 · doi:10.1145/273865.273901

[6] E. Ben-Sasson, P. Harsha \& S. Raskhodnikova. Some 3CNF Properties are Hard to Test. To appear in Proc. on 35th Annual ACM Symposium on Theory of Computing, 2003.

[7] U. Feige. Relations between average case complexity and approximation complexity. In Proc. on 34th Annual ACM Symposium on Theory of Computing, 534–543, 2002. · Zbl 1192.68358

[8] Feldman V.: Attribute-Efficient and Non-adaptive Learning of Parities and DNF Expressions. Journal of Machine Learning Research 8, 1431–1460 (2007) · Zbl 1222.68096

[9] A. Flaxman. A spectral technique for random satisfiable 3CNF formulas. In Proc. on 14th Annual ACM-SIAM Symposium on Discrete Algorithms, 2003. · Zbl 1094.68574

[10] Friedman J.: A note on matrix rigidity. Combinatorica 13(2), 235–239 (1993) · Zbl 0848.15005 · doi:10.1007/BF01303207

[11] Gollman D., Chambers W.: Clock-controlled shift registers: a review. IEEE Journal on Selected Areas in Communications 7(4), 525–533 (1989) · doi:10.1109/49.17716

[12] Goldreich O.: Foundations of Cryptography: Basic Applications. Cambridge University Press, Cambridge (2004) · Zbl 1068.94011

[13] O. Goldreich \& S. Goldwasser. On the Limits of Non-Approximability of Lattice Problems. In Proc. on 30th Annual ACM Symposium on the Theory of Computing, 1–9, 1998. · Zbl 1011.68512

[14] Goldwasser S., Micali S.: Probabilistic Encryption. Journal of Computer and System Sciences 28(2), 270–299 (1984) · Zbl 0563.94013 · doi:10.1016/0022-0000(84)90070-9

[15] Håstad J.: Dual Vectors and Lower Bounds for the Nearest Lattice Point Problem. Combinatorica 8((1), 75–81 (1988) · Zbl 0653.10026 · doi:10.1007/BF02122554

[16] Håstad J.: Some optimal inapproximability results. Journal of ACM 48, 798–859 (2001) · Zbl 1127.68405 · doi:10.1145/502090.502098

[17] Kashin B., Razborov A.: Improved lower bounds on the rigidity of Hadamard matrices. Mathematical Notes 63(4), 471–475 (1998) · Zbl 0917.15013 · doi:10.1007/BF02311250

[18] Lokam S.: Spectral Methods for Matrix Rigidity with Applications to Size-Depth Trade-offs and Communication Complexity. Journal of Computer and System Sciences 63(3), 449–473 (2001) · Zbl 1006.68051 · doi:10.1006/jcss.2001.1786

[19] Lagarias J., Lenstra H., Schnorr C.: Korkin-Zolotarev bases and successive minima of a lattice and its reciprocal lattice. Combinatorica 10(4), 333–348 (1990) · Zbl 0723.11029 · doi:10.1007/BF02128669

[20] R. McEliece. A Public-Key Cryptosystem Based on Algebraic Coding Theory. Deep Space Network Progress Report 42–44, Jet Propulsion Lab., California Institute of Technology, 114–116, 1978.

[21] Naor J., Naor M.: Small-Bias Probability Spaces: Efficient Constructions and Applications. SIAM Journal of Computing 22(4), 838–856 (1993) · Zbl 0776.60014 · doi:10.1137/0222053

[22] Pudlak P., Vavřin Z.: Computation of rigidity of order n/r for one simple matrix. Comm. Math. Univ. Carol. 32(2), 213–218 (1991)

[23] Pak I., Vu V.: On mixing of certain random walks, cutoff phenomenon and sharp threshold of random matroid processes. Discrete Applied Math. 110, 251–272 (2001) · Zbl 0983.60036 · doi:10.1016/S0166-218X(00)00201-8

[24] A. Razborov. On rigid matrices. Manuscript (in Russian), 1989.

[25] Razborov A., Rudich S.: Natural Proofs. Journal of Computer and System Sciences 55(1), 24–35 (1997) · Zbl 0884.68055 · doi:10.1006/jcss.1997.1494

[26] Shokrollahi M., Spielman D., Stemann V.: A Remark on Matrix Rigidity. Information Processing Letters 64(6), 283–285 (1997) · Zbl 1337.15004 · doi:10.1016/S0020-0190(97)00190-7

[27] 1968. Engl. translation: G. C. Tseitin, On the complexity of derivations in propositional calculus, in: Studies in mathematics and mathematical logic, Part II, ed. A. O. Slissenko, pp. 115–125.

[28] L. Valiant, Graph-Theoretic Arguments in Low-Level Complexity. In Proc. 6th Symposium on Mathematical Foundations of Computer Science, 162–176, 1977. · Zbl 0384.68046