Fortnow, Lance; **Santhanam, Rahul**

Infeasibility of instance compression and succinct PCPs for NP. (English) Zbl 1233.68144

J. Comput. Syst. Sci. 77, No. 1, 91-106 (2011).

A question by *H. L. Bodlaender, R. G. Downey, M. R. Fellows* and *D. Hermelin* ["On problems without polynomial kernels", J. Comput. Syst. Sci. 75, No. 8, 423–434 (2009; Zbl 1192.68288)] asks if there is a polynomial-time computable function that, given a sequence of m Boolean formulae each of length at most n, computes a formula of length bounded by a polynomial in n such that the computed formula is satisfiable if and only if at least one of the given formulae is satisfiable. This paper settles the question in the negative, under the assumption that the polynomial-time hierarchy does not collapse. A number of consequences of this result, the maybe most prominent of which concerns kernalizability of certain graph problems, are shown.

Reviewer: Heribert Vollmer (Hannover)

MSC:

68Q25 Analysis of algorithms and problem complexity
68Q15 Complexity classes (hierarchies, relations among complexity classes, etc.)
68Q17 Computational difficulty of problems (lower bounds, completeness, difficulty of approximation, etc.)
68Q10 Modes of computation (nondeterministic, parallel, interactive, probabilistic, etc.)

Keywords:

satisfiability problem; probabilistically checkable proof; parameterized complexity; compressibility

Full Text: DOI

References:

[1] Leonard Adleman, Two theorems on random polynomial time, in: Proceedings of the 20th Annual IEEE Symposium on the Foundations of Computer Science, 1978, pp. 75-83.

[2] Arora, Sanjeev; Lund, Carsten; Motwani, Rajeev; Sudan, Madhu; Szegedy, Mario, Proof verification and the hardness of approximation problems, J. ACM, 45, 3, 501-555, (1998) · Zbl 1065.68570

[3] Yonatan Aumann, Michael Rabin, Information theoretically secure communication in the limited storage space model, in: Proceedings of CRYPTO '99, 1999, pp. 65-79. · Zbl 0940.94007

[4] Arora, Sanjeev; Safra, Shmuel, Probabilistic checking of proofs: A new characterization of NP, J. ACM, 45, 1, 70-122, (1998) · Zbl 0903.68076

[5] Alon, Noga; Spencer, Joel, The probabilistic method, Wiley-intersci. ser. discrete math. optim., (2008), Wiley · Zbl 1148.05001

[6] Hans Bodlaender, Rod Downey, Michael Fellows, Danny Hermelin, On problems without polynomial kernels, in: Proceedings of 35th International Colloquium on Automata, Languages and Programming, 2008, pp. 563-574. · Zbl 1153.68554

[7] Harry Buhrman, John Hitchcock, NP-complete sets are exponentially dense unless NP ⊠ co-NP/poly, in: Proceedings of 23rd Annual IEEE Conference on Computational Complexity, 2008, in press.

[8] Cai, Liming; Chen, Jianer; Downey, Rodney; Fellows, Michael, Advice classes of parameterized tractability, Ann. pure appl. logic, 84, 1, 119-138, (1997) · Zbl 0873.68071

[9] Yijia Chen, Jörg Flum, Moritz Müller, Lower bounds for kernelizations and other preprocessing procedures, in: Proceedings of Computability in Europe 2009, in: Lecture Notes in Comput. Sci., Springer-Verlag, 2009, in press. · Zbl 1268.68084

[10] Stephen Cook, The complexity of theorem-proving procedures, in: Proceedings of the 3rd Annual ACM Symposium on Theory of Computing, 1971, pp. 151-158. · Zbl 0253.68020

[11] Downey, Rodney; Fellows, Michael, Parameterized complexity, (1999), Springer-Verlag · Zbl 0961.68533

[12] Bella Dubrov, Yuval Ishai, On the randomness complexity of efficient sampling, in Proceedings of the 38th Annual ACM Symposium on Theory of Computing, 2006, pp. 711-720. · Zbl 1301.68261

[13] Dinur, Irit, The PCP theorem by gap amplification, J. ACM, 54, 3, (2007) · Zbl 1292.68074

[14] Yan Zong Ding, Michael Rabin, Hyper-encryption, everlasting security, in: Annual Symposium on Theoretical Aspects of Computer Science, 2002, pp. 1-26. · Zbl 1054.68049

[15] Flum, Jorg; Grohe, Martin, Parameterized complexity theory, (2006), Springer · Zbl 1143.68016

[16] Fortnow, L.; Santhanam, R., Infeasibility of instance compression and succinct PCPs for NP, (), 133-142 · Zbl 1231.68133

[17] Garey, Michael; Johnson, David, Approximation algorithms for combinatorial problems: an annotated bibliography, (1976), Academic Press New York, pp. 41-52

[18] Guo, Jiong; Niedermeier, Rolf, Invitation to data reduction and problem kernelization, ACM SIGACT news, 38, 1, 31-45, (2007)

[19] Danny Harnik, Moni Naor, On everlasting security in the hybrid bounded storage model, in: Proceedings of the 33rd International Colloquium on Automata, Languages and Programming, 2006, pp. 192-203. · Zbl 1133.94320

[20] Danny Harnik, Moni Naor, On the compressibility of NP instances and cryptographic applications, in: Proceedings of the 47th Annual IEEE Symposium on Foundations of Computer Science, 2006, pp. 719-728. · Zbl 1207.68162

[21] Russell Impagliazzo, Avi Wigderson, P = BPP if E requires exponential circuits: Derandomizing the XOR lemma, in: Proceedings of the 29th Annual ACM Symposium on the Theory of Computing, 1997 pp. 220-229. · Zbl 0962.68058

[22] Karp, Richard; Lipton, Richard, Turing machines that take advice, Enseign. math., 28, 2, 191-209, (1982) · Zbl 0529.68025

[23] Tauman Kalai, Yael; Raz, Ran, Interactive PCP, Electronic colloquium on computational complexity, 7, 31, (2007) · Zbl 1155.68504

[24] Klivans, Adam; van Melkebeek, Dieter, Graph nonisomorphism has subexponential size proofs unless the polynomial hierarchy collapses, SIAM J. comput., 31, 5, 1501-1526, (2002) · Zbl 1016.68060

[25] Mahaney, Stephen, Sparse complete sets for NP: solution of a conjecture of berman and hartmanis, J. comput. system sci., 25, 2, 130-143, (1982) · Zbl 0493.68043

[26] Daniel Márx, Parameterized complexity and approximation algorithms, The Computer Journal (2006), in press.

[27] Maurer, Ueli, Conditionally-perfect secrecy and a provably-secure randomized cipher, J. cryptology, 5, 1, 53-66, (1992) · Zbl 0746.94013

[28] Niedermeier, Rolf, Invitation to fixed-parameter algorithms, (2006), University Press Oxford · Zbl 1095.68038

[29] Simon, Daniel, Finding collisions on a one-way street: can secure hash functions be based on general assumptions?, (), 334-345 · Zbl 0919.94032

[30] Ronen Shaltiel, Christopher Umans, Simple extractors for all min-entropies and a new pseudo-random generator, in: Proceedings of the 42nd IEEE Symposium on Foundations of Computer Science, 2001. · Zbl 1317.68132

[31] Vadhan, Salil, Constructing locally computable extractors and cryptosystems in the bounded storage model, J. cryptology, 17, 1, 43-77, (2004) · Zbl 1071.94016

[32] Dieter van Melkebeek, Personal communication, 2009.

[33] Yap, Chee-Keng, Some consequences of non-uniform conditions on uniform classes, Theoret. comput. sci., 26, 287-300, (1983) · Zbl 0541.68017