Goldreich, Oded

In a world of P = BPP. (English) Zbl 1343.68084

Goldreich, Oded (ed.), Studies in complexity and cryptography. Miscellanea on the interplay between randomness and computation. In collaboration with Lidor Avigad, Mihir Bellare, Zvika Brakerski, Shafi Goldwasser, Shai Halevi, Tali Kaufman, Leonid Levin, Noam Nisan, Dana Ron, Madhu Sudan, Luca Trevisan, Salil Vadhan, Avi Wigderson, David Zuckerman. Berlin: Springer (ISBN 978-3-642-22669-4/pbk). Lecture Notes in Computer Science 6650, 191-232 (2011).

Summary: We show that proving results such as $\mathcal{BPP} = \mathcal{P}$ essentially necessitate the construction of suitable pseudorandom generators (i.e., generators that suffice for such derandomization results). In particular, the main incarnation of this equivalence refers to the standard notion of uniform derandomization and to the corresponding pseudorandom generators (i.e., the standard uniform notion of "canonical derandomizers"). This equivalence bypasses the question of which hardness assumptions are required for establishing such derandomization results, which has received considerable attention in the last decade or so (starting with [*R. Impagliazzo* and *A. Wigderson*, J. Comput. Syst. Sci. 63, No. 4, 672–688 (2001; Zbl 1052.68034)]).

We also identify a natural class of search problems that can be solved by deterministic polynomial-time reductions to $\mathcal{BPP}$. This result is instrumental to the construction of the aforementioned pseudorandom generators (based on the assumption $\mathcal{BPP} = \mathcal{P}$), which is actually a reduction of the "construction problem" to $\mathcal{BPP}$.

Caveat: Throughout the text, we abuse standard notation by letting $\mathcal{BPP}$, $\mathcal{P}$ etc denote classes of promise problems. We are aware of the possibility that this choice may annoy some readers, but believe that promise problem actually provide the most adequate formulation of natural decisional problems.

For the entire collection see [Zbl 1220.68005].

MSC:

68Q15 Complexity classes (hierarchies, relations among complexity classes, etc.)
68W20 Randomized algorithms

Keywords:

BPP; derandomization; pseudorandom generators; promise problems; search problems; FPTAS; randomized constructions

Full Text: DOI

References:

[1] Aydinlioglu, B., Gutfreund, D., Hitchcock, J.M., Kawachi, A.: Derandomizing Arthur-Merlin Games and Approximate Counting Implies Exponential-Size Lower Bounds. Computational Complexity (to appear) · Zbl 1230.68076

[2] Blum, M., Micali, S.: How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. In: SICOMP, vol.˜13, pp. 850–864 (1984); Preliminary version in 23rd FOCS, pp. 80–91 (1982) · Zbl 0547.68046

[3] Chor, B., Goldreich, O.: On the Power of Two–Point Based Sampling. Jour.˜of Complexity˜5, 96–106 (1989) · Zbl 0672.60105 · doi:10.1016/0885-064X(89)90015-0

[4] Even, S., Selman, A.L., Yacobi, Y.: The Complexity of Promise Problems with Applications to Public-Key Cryptography. Inform. and Control˜61, 159–173 (1984) · Zbl 0592.94012 · doi:10.1016/S0019-9958(84)80056-X

[5] Fortnow, L.: Comparing Notions of Full Derandomization. In: 16th CCC, pp. 28–34 (2001)

[6] Friedman, J.: A Proof of Alon's Second Eigenvalue Conjecture. In: 35th STOC, pp. 720–724 (2003) · Zbl 1192.05087 · doi:10.1145/780542.780646

[7] Gauss, C.F.: Untersuchungen Über Höhere Arithmetik, 2nd edn. Chelsea publishing company, New York (1981) (reprinted)

[8] Goldreich, O.: Foundation of Cryptography: Basic Tools. Cambridge University Press, Cambridge (2001) · Zbl 1007.94016 · doi:10.1017/CBO9780511546891

[9] Goldreich, O.: Computational Complexity: A Conceptual Perspective. Cambridge University Press, Cambridge (2008) · Zbl

1154.68056 · doi:10.1017/CBO9780511804106

[10] Goldreich, O., Wigderson, A.: On Pseudorandomness with respect to Deterministic Observers. In: RANDOM 2000, Proceedings of the Satellite Workshops of the 27th ICALP. Carleton Scientific (Proc. in Inform. 8), pp. 77–84 (2000); See also ECCC, TR00-056

[11] Goldwasser, S., Micali, S.: Probabilistic Encryption. JCSS˜28(2), 270–299 (1984); Preliminary version in 14th STOC (1982) · Zbl 0563.94013

[12] Grollmann, J., Selman, A.L.: Complexity Measures for Public-Key Cryptosystems. In: SICOMP, vol.˜17(2), pp. 309–335 (1988) · Zbl 0644.94016 · doi:10.1137/0217018

[13] Hochbaum, D. (ed.): Approximation Algorithms for NP-Hard Problems. PWS (1996) · Zbl 1368.68010

[14] Huxley, M.N.: On the Difference Between Consecutive Primes. Invent. Math.˜15, 164–170 (1972) · Zbl 0241.10026 · doi:10.1007/BF01418933

[15] Impagliazzo, R., Kabanets, V., Wigderson, A.: In Search of an Easy Witness: Exponential Time vs Probabilistic Polynomial Time. JCSS˜65(4), 672–694 (2002); Preliminary version in 16th CCC (2001) · Zbl 1059.68047

[16] Impagliazzo, R., Wigderson, A.: P=BPP if E requires exponential circuits: Derandomizing the XOR Lemma. In: 29th STOC, pp. 220–229 (1997) · Zbl 0962.68058

[17] Impagliazzo, R., Wigderson, A.: Randomness vs.˜Time: De-randomization under a uniform assumption. JCSS˜63(4), 672–688 (2001); Preliminary version in 39th FOCS (1998) · Zbl 1052.68034

[18] Jerrum, M., Valiant, L., Vazirani, V.V.: Random Generation of Combinatorial Structures from a Uniform Distribution. In: TCS, vol.˜43, pp. 169–188 (1986) · Zbl 0597.68056

[19] Kabanets, V., Impagliazzo, R.: Derandomizing Polynomial Identity Tests Means Proving Circuit Lower Bounds. Computational Complexity˜13, 1–46 (2003); Preliminary version in 35th STOC (2003) · Zbl 1089.68042 · doi:10.1007/s00037-004-0182-6

[20] Nisan, N., Wigderson, A.: Hardness vs Randomness. JCSS˜49(2), 149–167 (1994); Preliminary version in 29th FOCS (1988) · Zbl 0821.68057

[21] Ostrovsky, R., Wigderson, A.: One-Way Functions are Essential for Non-Trivial Zero-Knowledge. In: 2nd Israel Symp. on Theory of Computing and Systems, pp. 3–17. IEEE Comp. Soc. Press, Los Alamitos (1993)· doi:10.1109/ISTCS.1993.253489

[22] Reingold, O., Trevisan, L., Vadhan, S.: Pseudorandom walks on regular digraphs and the RL vs. L problem. In: 38th STOC, pp. 457–466 (2006); See details in ECCC, TR05-022 · Zbl 1301.05317

[23] Shaltiel, R., Umans, C.: Low-end Uniform Hardness vs Randomness Tradeoffs for AM. SICOMP˜39(3), 1006–1037 (2009); Preliminary version in 39th STOC (2007) · Zbl 1194.68120 · doi:10.1137/070698348

[24] Trevisan, L., Vadhan, S.: Pseudorandomness and Average-Case Complexity Via Uniform Reductions. Computational Complexity˜16(4), 331–364 (2007); Preliminary version in 17th CCC (2002) · Zbl 1133.68023

[25] Umans, C.: Pseudo-random Generators for all Hardness. JCSS˜67(2), 419–440 (2002); Preliminary version in 34th STOC (2002) · Zbl 1072.68129

[26] Vadhan, S.: An Unconditional Study of Computational Zero Knowledge. SICOMP˜36(4), 1160–1214 (2006); Preliminary version in 45th FOCS (2004) · Zbl 1129.94037 · doi:10.1137/S0097539705447207

[27] Yao, A.C.: Theory and Application of Trapdoor Functions. In: 23rd FOCS, pp. 80–91 (1982)· doi:10.1109/SFCS.1982.45