Goldreich, Oded

Another motivation for reducing the randomness complexity of algorithms. (English)

Zbl 1291.68430

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, 555-560 (2011).

Summary: We observe that the randomness-complexity of an algorithm effects the time-complexity of implementing a version of it that utilizes a weak source of randomness (through a randomness-extractor). This provides an additional motivation for the study of the randomness complexity of randomized algorithms. We note that this motivation applies especially in the case that derandomization is prohibitingly costly.

For the entire collection see [Zbl 1220.68005].

MSC:

68W20 Randomized algorithms
60-08 Computational methods for problems pertaining to probability theory
94A20 Sampling theory in information and communication theory

Keywords:

randomness complexity; weak sources of randomness; randomness extractors; pseudorandom generators; sampling; property testing

Full Text: DOI

References:

[1] Bellare, M., Goldreich, O., Goldwasser, S.: Randomness in Interactive Proofs. Computational Complexity˜4(4), 319–354 (1993) · Zbl 0802.68053 · doi:10.1007/BF01275487

[2] Blum, M., Micali, S.: How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits. SIAM Journal on Computing˜13, 850–864 (1984); Preliminary Version in 23rd FOCS (1982) · Zbl 0547.68046 · doi:10.1137/0213053

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

[4] Goldreich, O.: A Brief Introduction to Property Testing. In: Goldreich, O., et al.: Studies in Complexity and Cryptography. LNCS, vol.˜6650, pp. 557–562. Springer, Heidelberg (2011) · Zbl 1343.68298

[5] Goldreich, O., Goldwasser, S., Micali, S.: How to Construct Random Functions. Journal of the ACM˜33(4), 792–807 (1986) · Zbl 0596.65002 · doi:10.1145/6490.6503

[6] Goldreich, O., Goldwasser, S., Ron, D.: Property testing and its connection to learning and approximation. Journal of the ACM, 653–750 (July 1998) · Zbl 1065.68575 · doi:10.1145/285055.285060

[7] Goldreich, O., Ron, D.: Property testing in bounded degree graphs. Algorithmica, 302–343 (2002) · Zbl 0990.68103 · doi:10.1007/s00453-001-0078-7

[8] Goldreich, O., Ron, D.: A sublinear bipartite tester for bounded degree graphs. Combinatorica˜19(3), 335–373 (1999) · Zbl 0932.68053 · doi:10.1007/s004930050060

[9] Goldreich, O., Sheffet, O.: On the randomness complexity of property testing. In: Charikar, M., Jansen, K., Reingold, O., Rolim, J.D.P. (eds.) RANDOM 2007 and APPROX 2007. LNCS, vol.˜4627, pp. 509–524. Springer, Heidelberg (2007) · Zbl 1171.68727 · doi:10.1007/978-3-540-74208-1$_3$7

[10] Ron, D.: Algorithmic and Analysis Techniques in Property Testing. Foundations and Trends in TCS˜5(2), 73–205 (2010) · Zbl 1184.68610

[11] Rubinfeld, R., Sudan, M.: Robust characterization of polynomials with applications to program testing. SIAM Journal on Computing˜25(2), 252–271 (1996) · Zbl 0844.68062 · doi:10.1137/S0097539793255151

[12] Sheffet, O.: M.Sc.Thesis, Weizmann Institute of Science (in preparation), http://www.wisdom.weizmann.ac.il/˜oded/msc-os.html

[13] Shaltiel, R.: Recent Developments in Explicit Constructions of Extractors. Bulletin of the EATCS ˜77, 67–95 (2002) · Zbl 1051.68070

[14] Shaltiel, R., Umans, C.: Simple Extractors for All Min-Entropies and a New Pseudo-Random Generator. In: 32nd IEEE Symposium on Foundations of Computer Science, pp. 648–657 (2001)· doi:10.1109/SFCS.2001.959941

[15] Ta-Shma, A., Zuckerman, D., Safra, S.: Extractors from Reed-Muller Codes. In: 32nd IEEE Symposium on Foundations of Computer Science, pp. 638–647 (2001) · Zbl 1094.68036 · doi:10.1109/SFCS.2001.959940

[16] Yao, A.C.: Theory and Application of Trapdoor Functions. In: 23rd IEEE Symposium on Foundations of Computer Science, pp. 80–91 (1982)· doi:10.1109/SFCS.1982.45