

## Goldreich, Oded

**On the average-case complexity of property testing.** (English) Zbl 1343.68296

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, 124-135 (2011).

Summary: Motivated by a study of *M. Zimand* [“On derandomizing probabilistic sublinear-time algorithms”, in: Proceedings of the 22th annual IEEE conference on computational complexity, CCC 2007. Washington DC: IEEE Computer Society. 1–9 (2007; doi:10.1109/CCC.2007.19)], we consider the average-case complexity of property testing (focusing, for clarity, on testing properties of Boolean strings). We make two observations:

1. In the context of average-case analysis with respect to the uniform distribution (on all strings of a fixed length), property testing is trivial. Specifically, either the yes-instances (i.e., instances having the property) or the no-instances (i.e., instances that are far from having the property) are exponentially rare, and thus the tester may just reject (resp., accept) obliviously of the input.
2. Turning to average-case derandomization with respect to distributions that assigns noticeable probability mass to both yes-instances and no-instances, we identify a natural class of distributions and testers for which average-case derandomization results can be obtained directly (i.e., without using randomness extractors). Furthermore, the resulting deterministic algorithm may preserve the non-adaptivity of the original tester. (In contrast, Zimand’s argument utilizes a strong type of randomness extractors and introduces adaptivity into the testing process.)

For the entire collection see [\[Zbl 1220.68005\]](#).

### MSC:

[68W20](#) Randomized algorithms  
[68Q25](#) Analysis of algorithms and problem complexity

Cited in 1 Document

### Keywords:

[property testing](#); [average-case complexity](#)

**Full Text:** [DOI](#)

### References:

- [1] Alon, N.: Testing subgraphs of large graphs. *Random Structures and Algorithms* 21, 359–370 (2002) · [Zbl 1027.68095](#) · [doi:10.1002/rsa.10056](#)
- [2] Alon, N., Spencer, J.H.: *The Probabilistic Method*, 2nd edn. John Wiley & Sons, Inc., Chichester (2000) · [Zbl 0996.05001](#) · [doi:10.1002/0471722154](#)
- [3] Ergun, F., Kannan, S., Kumar, S.R., Rubinfeld, R., Viswanathan, M.: Spot-Checkers. In: 30th STOC, pp. 259–268 (1998) · [Zbl 1027.68514](#) · [doi:10.1145/276698.276757](#)
- [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] Frieze, A., Kanan, R.: Quick approximation to matrices and applications. *Combinatorica* 19(2), 175–220 (1999) · [Zbl 0933.68061](#) · [doi:10.1007/s004930050052](#)
- [6] Goldreich, O.: A Brief Introduction to Property Testing. In: Goldreich, O., et al. (eds.) *Studies in Complexity and Cryptography*. LNCS, vol. 6650, pp. 467–471. Springer, Heidelberg (2011) · [Zbl 1343.68298](#)
- [7] Goldreich, O., Goldwasser, S., Lehman, E., Ron, D., Samorodnitsky, A.: Testing Monotonicity. *Combinatorica* 20(3), 301–337 (2000) · [Zbl 0964.68148](#) · [doi:10.1007/s004930070011](#)
- [8] 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](#)
- [9] Goldreich, O., Kaufman, T.: Proximity Oblivious Testing and the Role of Invariances. *ECCC*, TR10-058 · [Zbl 1343.68301](#)
- [10] Goldreich, O., Ron, D.: Property testing in bounded degree graphs. *Algorithmica*, 302–343 (2002) · [Zbl 0990.68103](#) · [doi:10.1007/s00453-001-0078-7](#)

- [11] 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](#)
- [12] Goldreich, O., Sheffet, O.: On the randomness complexity of property testing. *Computational Complexity* 19(1), 99–133 (2010); Extended abstract in *Proc. of RANDOM 2007* (2007) · [Zbl 1204.68097](#) · [doi:10.1007/s00037-009-0282-4](#)
- [13] Goldreich, O., Trevisan, L.: Three theorems regarding testing graph properties. *Random Structures and Algorithms* 23(1), 23–57 (2003) · [Zbl 1048.68062](#) · [doi:10.1002/rsa.10078](#)
- [14] Goldreich, O., Wigderson, A.: Derandomization that is rarely wrong from short advice that is typically good. In: Rolim, J.D.P., Vadhan, S.P. (eds.) *RANDOM 2002*. LNCS, vol. 2483, pp. 209–223. Springer, Heidelberg (2002) · [Zbl 1028.68225](#) · [doi:10.1007/3-540-45726-7\\_17](#)
- [15] Kaufman, T., Sudan, M.: Algebraic Property Testing: The Role of Invariances. In: *40th STOC*, pp. 403–412 (2008) · [Zbl 1231.68290](#)
- [16] Ron, D.: Algorithmic and Analysis Techniques in Property Testing. *Foundations and Trends in TCS* 5(2), 73–205 (2010) · [Zbl 1184.68610](#)
- [17] 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](#)
- [18] Zimand, M.: On derandomizing probabilistic sublinear-time algorithms. In: *The Proc. of the 22nd IEEE Conference on Computational Complexity*, pp. 1–9 (2007) · [doi:10.1109/CCC.2007.19](#)

This reference list is based on information provided by the publisher or from digital mathematics libraries. Its items are heuristically matched to zbMATH identifiers and may contain data conversion errors. It attempts to reflect the references listed in the original paper as accurately as possible without claiming the completeness or perfect precision of the matching.