List of Publications

Oded Goldreich

January 6, 2022

Contents

1 Theses 1

2 Original Papers in Refereed Journals 1

3 Original Papers in (Refereed) Conference Proceedings 7

4 Other Work 17
  4.1 Collected Works (LNCS Vol. 6650, 2011) ........................................... 17
  4.2 Collected Works (LNCS Vol. 12050, 2020) ........................................... 18
  4.3 Papers in Electronic Forum ................................................................. 19
  4.4 Reports and Unpublished Manuscripts ................................................. 20

5 Survey Papers 21
  5.1 Chapters in Books .......................................................... 21
  5.2 Published in Periodicals or Conference Proceedings ........................... 22
  5.3 Collected Works (LNCS Vol. 6650, 2011) ........................................... 23
  5.4 Electronic posting ............................................................... 23

6 Books, Lecture Notes, and Related Material 24
1 Theses


  Thesis adviser: Prof. S. Even, 1983.

2 Original Papers in Refereed Journals

Published


Accepted


### 3 Original Papers in (Refereed) Conference Proceedings

The paper are ordered by the date of the conferences, and not by the date of the publication of its proceedings. This comment is relevant with respect to the early Crypto’ conferences (i.e., of the 1980’s). Also, till the late 1980’s, simultaneous publication in various conferences was allowed (and even encouraged).


[C18] B. Chor and O. Goldreich, Unbiased Bits from Sources of Weak Randomness and Probabilistic Communication Complexity, Proc. of the 26th IEEE Symp. on Foundation of Computer Science (FOCS), 1985, pp. 429-442. (This is an extended abstract of No. J9.)


[C35] S. Ben-David, B. Chor, O. Goldreich, and M. Luby, On the Theory of Average Case Complexity, Proc. of the 4th conf. on Structure in Complexity Theory, (This is an abstract of No. C37.)


[C40] O. Goldreich, and H. Krawczyk, On Sparse Pseudorandom Ensembles, Advances in Cryptology – Crypto ’89 (Proceedings), Lecture Note in Computer Science (435) Springer Verlag, pp. 113–127, 1990. (This is an extended abstract of No. J22.)


[C66] S. Decatur, O. Goldreich, and D. Ron, Computational Sample Complexity, 10th COLT, pp. 130-142, 1997. (This is a preliminary version of No. J52.)

[C67] O. Goldreich and S. Safra, A Combinatorial Consistency Lemma with application to the PCP Theorem, proceedings of Random97, Springer LNCS, Vol. 1269, pp. 67–84. (This is a preliminary version of No. J53.)


[C70] O. Goldreich and S. Goldwasser, On the Limits of Non-Approximability of Lattice Problems, in Proc. of the 30th ACM Symp. on Theory of Computing (STOC), pp. 1–9, 1998. (This is an extended abstract of No. J54.)


[C74] O. Goldreich and M. Sudan, Computational Indistinguishability: A Sample Hierarchy, proceedings of 13th IEEE Conference on Computational Complexity, pages 24-33, 1998. (This is an extended abstract of No. J51.)


[C76] O. Goldreich, S. Goldwasser, E. Lehman and D. Ron, Testing Monotonicity, in 39th FOCS, pages 426–435, 1998. (This extended abstract has been merged with an improvement obtained in joint work with Alex Samorodnitsky to yield No. J56.)

[C77] O. Goldreich, D. Ron and M. Sudan, Chinese Remaindering with Errors, in 31st STOC, pages 225–234, 1999. (This is an extended abstract of No. J55.)


[C87] O. Goldreich and Y. Lindell, Session-Key Generation using Human Passwords Only, Proceedings of *Crypto01*, pages 408–432. (This is an extended abstract of No. J66.)

[C88] B. Barak, O. Goldreich, R. Impagliazzo, S. Rudich, A. Sahai, S. Vadhan and K. Yang, On the (Im)possibility of Software Obfuscation, Proceedings of *Crypto01*, pages 1–18. (This is an extended abstract of No. J80.)


[C95] O. Goldreich and M. Sudan, Locally Testable Codes and PCPs of Almost-Linear Length, in *Proc. of the 43rd FOCS*, pages 13–22, 2002. (This is an extended abstract of No. J67.)


[C99] E. Ben-Sasson, O. Goldreich, P. Harsha, M. Sudan, S. Vadhan. Robust PCPs of Proximity, Shorter PCPs and Applications to Coding, in Proc. of the 36th STOC, pages 1-10, 2004. (This is an extended abstract of No. J69.)


[C119] O. Goldreich and D. Ron. On Sample-Based Testers, in the proceedings of 6th ITCS, pages 337–345, 2015. (This is an extended abstract of No. J87.)


[C122] O. Goldreich, T. Gur, and R. Rothblum. Proofs of Proximity for Context-Free Languages and Read-Once Branching Programs, In 42nd ICALP (1), pages 666–677, 2015. (This is an extended abstract of No. J90.)


4 Other Work

This section only lists works that are not listed in the prior sections. Likewise, works are listed in the first relevant subsection. In all cases, these publications were not refereed.

4.1 Collected Works (LNCS Vol. 6650, 2011)

The works collected in this volume were competed at different times, and were revised towards this publication. The year of the original version is mentioned in square brackets.


[O6] O. Goldreich and D. Zuckerman, Another proof that BPP subseteq PH (and more) [1997]


[O10] O. Goldreich, Candidate One-Way Functions Based on Expander Graphs [2000]
4.2 Collected Works (LNCS Vol. 12050, 2020)

The works collected in this volume were completed at different times, and were revised towards this publication. The year of the original version is mentioned in square brackets.


[O22] O. Goldreich, Two Comments on Targeted Canonical Derandomizers [2011]


[O27] O. Goldreich and D. Ron, On the Relation between the Relative Earth Mover Distance and the Variation Distance (an exposition) [2016]

[O28] O. Goldreich, The Uniform Distribution is Complete with respect to Testing Identity to a Fixed Distribution [2016]
4.3 Papers in Electronic Forum

ECRC resides at https://eccc.weizmann.ac.il.

[O39] O. Goldreich, The Graph Clustering Problem has a Perfect Zero-Knowledge Proof, ECCC, TR96-054, November 1996. (See follow-up J47.)


4.4 Reports and Unpublished Manuscripts

Prior to the days of internet, these things were used.

Research Reports

[O56] O. Goldreich, Graph Partition into Equinumerous Connected Components is NP-Complete, TR No. 202, Computer Science Department, Technion, Haifa, Israel, 1981.


Unpublished Manuscripts (cited by other researchers)


5 Survey Papers

5.1 Chapters in Books


5.2 Published in Periodicals or Conference Proceedings


(A brief summary has appeared in *CryptoBytes*, the technical newsletter of RSA Laboratories, Vol. 3, No. 2, 1997.)

[S22] Pseudorandomness, in *Notices of AMS*, pages 1209–1216, November 1999. (This is an abbreviated version of No. S23.)


5.3 Collected Works (LNCS Vol. 6650, 2011)

In addition to the surveys listed next, surveys number S9, S11, S12, and S28 also appear in this collection. The surveys collected in this volume were completed at different times, and were revised towards this publication. The year of the original version is mentioned in square brackets.

[S32] On Yao’s XOR-Lemma (with N. Nisan and A. Wigderson) [1995]


[S34] A Sample of Samplers – A Computational Perspective on Sampling [1997]


[S37] On the complexity of computational problems regarding distributions (with S. Vadhan) [2003]


[S39] Average Case Complexity, Revisited [2008]

[S40] Basic Facts about Expander Graphs [2008]

[S41] A Brief Introduction to Property Testing [2010]

5.4 Electronic posting

ECCC resides at https://eccc.weizmann.ac.il.


6 Books, Lecture Notes, and Related Material

Books


Lecture Notes

[B8] Foundations of Cryptography – Class Notes, 1989. Computer Science Department, Technion, 184 pages. (Superseeded by B2 and B3.)


2. For a one-semester course, 104 pages, 2002.

Department of Computer Science and Applied Math., Weizmann Institute of Science. (Superseeded by B4.)

Other Material


Department of Computer Science and Applied Math., Weizmann Institute, 292 pages.

(This is a preliminary version of B2.)