Goldreich, Oded; Zuckerman, David

Another proof that $\mathcal{BPP} \subseteq \mathcal{PH}$ (and more). (English) Zbl 1343.68085

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, 40-53 (2011).

Summary: We provide another proof of the Sipser-Lautemann Theorem by which $\mathcal{BPP} \subseteq \mathcal{MA}$ ($\subseteq \mathcal{PH}$). The current proof is based on strong results regarding the amplification of $\mathcal{BPP}$, due to *D. Zuckerman* [Algorithmica 16, No. 4–5, 367–391 (1996; Zbl 0857.68121)]. Given these results, the current proof is even simpler than previous ones. Furthermore, extending the proof leads to two results regarding $\mathcal{MA}$: $\mathcal{MA} \subseteq \mathcal{ZPP}^{\mathcal{NP}}$ (which seems to be new), and that two-sided error $\mathcal{MA}$ equals $\mathcal{MA}$. Finally, we survey the known facts regarding the fragment of the polynomial-time hierarchy that contains $\mathcal{MA}$.

For the entire collection see [Zbl 1220.68005].

MSC:

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

Cited in **5** Documents

Keywords:

BPP; polynomial-time hierarchy; interactive proof systems (AM and MA); randomness-efficient error reduction (amplification)

Full Text: DOI

References:

[1] Babai, L.: Trading Group Theory for Randomness. In: 17th STOC, pp. 421–429 (1985)· doi:10.1145/22145.22192

[2] Babai, L., Fortnow, L., Nisan, N., Wigderson, A.: BPP has Subexponential Time Simulations unless EXPTIME has Publishable Proofs. Complexity Theory~3, 307–318 (1993) · Zbl 0802.68054

[3] Boppana, R., Håstad, J., Zachos, S.: Does Co-NP Have Short Interactive Proofs? IPL~25, 127–132 (1987) · Zbl 0653.68037 · doi:10.1016/0020-0190(87)90232-8

[4] Canetti, R.: On BPP and the Polynomial-time Hierarchy. IPL~57, 237–241 (1996) · Zbl 0875.68425 · doi:10.1016/0020-0190(96)00016-6

[5] Fürer, M., Goldreich, O., Mansour, Y., Sipser, M., Zachos, S.: On Completeness and Soundness in Interactive Proof Systems. In: Micali, S. (ed.) Advances in Computing Research (Randomness and Computation), vol.~5, pp. 429–442 (1989)

[6] Goldreich, O.: A Sample of Samplers – A Computational Perspective on Sampling. This volume. See also ECCC, TR97-020, TR97-020 (May 1997)

[7] Goldreich, O.: Computational Complexity: A Conceptual Perspective. Cambridge University Press, Cambridge (2008) · Zbl 1154.68056 · doi:10.1017/CBO9780511804106

[8] Goldwasser, S., Micali, S., Rackoff, C.: The knowledge Complexity of Interactive Proofs. SIAM J. on Computing~18(1), 186–208 (1989) · Zbl 0677.68062 · doi:10.1137/0218012

[9] Goldwasser, S., Sipser, M.: Private Coins versus Public Coins in Interactive Proof Systems. In: Micali, S. (ed.) Advances in Computing Research (Randomness and Computation), vol.~5, pp. 73–90 (1989)

[10] 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

[11] Lautemann, C.: BPP and the Polynomial Hierarchy. IPL~17, 215–217 (1983) · Zbl 0515.68042 · doi:10.1016/0020-0190(83)90044-3

[12] Miltersen, P.B., Vinodchandran, N.V.: Derandomizing Arthur-Merlin Games using Hitting Sets. Computational Complexity~14(3), 256–279 (2005); Preliminary version in 40th FOCS (1999) · Zbl 1085.68058 · doi:10.1007/s00037-005-0197-7

[13] Russell, A., Sundaram, R.: Symmetric Alternation Captures BPP. Journal of Computational Complexity (1995) (to appear); Preliminary version in Technical Report MIT-LCS-TM-54

[14] Sipser, M.: A Complexity Theoretic Approach to Randomness. In: 15th STOC, pp. 330–335 (1983)· doi:10.1145/800061.808762

[15] Zachos, S., Fürer, M.: Probabilistic Quantifiers vs.~Distrustful Adversaries. In: Nori, K.V. (ed.) FSTTCS 1987. LNCS,

vol.~287, pp. 443–455. Springer, Heidelberg (1987) · Zbl 0647.68052 · doi:10.1007/3-540-18625-5$_6$7

[16] Zachos, S., Heller, H.: A decisive characterization of BPP. Information and Control~69(1-3), 125–135 (1986) · Zbl 0616.68049 · doi:10.1016/S0019-9958(86)80044-4

[17] Zuckerman, D.: Simulating BPP Using a General Weak Random Source. Algorithmica~16, 367–391 (1996) · Zbl 0857.68121 · doi:10.1007/BF01940870

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.