Brakerski, Zvika; Goldreich, Oded

From absolute distinguishability to positive distinguishability. (English) Zbl 1343.68290

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, 141-155 (2011).

Summary: We study methods of converting algorithms that distinguish pairs of distributions with a gap that has an absolute value that is noticeable into corresponding algorithms in which the gap is always positive (and noticeable). Our focus is on designing algorithms that, in addition to the tested string, obtain a fixed number of samples from each distribution. Needless to say, such algorithms can not provide a very reliable guess for the sign of the original distinguishability gap, still we show that even guesses that are noticeably better than random are useful in this setting.

For the entire collection see [Zbl 1220.68005].

MSC:

68W20	Randomized algorithms
62E99	Statistical distribution theory

Cited in **2** Documents

Keywords:

computational indistinguishability; statistical indistinguishability

Full Text: DOI

References:

[1] Feller, W.: An Introduction to Probability Theory and Its Applications, 2nd edn., vol.~II. John Wiley & Sons, Chichester (1972) · Zbl 0039.13201

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

[3] Goldreich, O.: Foundation of Cryptography – Basic Applications. Cambridge University Press, Cambridge (2004) · Zbl 1068.94011