Randomness – A Computational Complexity Perspective

Avi Wigderson

Institute for Advanced Study,
School of Mathematics,
1 Einstein Drive, Princeton, NJ 08540, USA

Abstract. Man has grappled with the meaning and utility of randomness for centuries. Research in the Theory of Computation in the last thirty years has enriched this study considerably. This lecture will describe two main aspects of this research on randomness, demonstrating its power and weakness respectively.

Randomness is paramount to computational efficiency: The use of randomness seems to dramatically enhance computation (and do other wonders) for a variety of problems and settings. In particular, examples will be given of probabilistic algorithms (with tiny error) for natural tasks in different areas, which are exponentially faster than their (best known) deterministic counterparts.

Computational efficiency is paramount to understanding randomness: We will explain the computationally-motivated definition of "pseudorandom" distributions, namely ones which cannot be distinguished from the uniform distribution by any efficient procedure from a given class. Using this definition, we show how such pseudorandomness may be generated deterministically, from (appropriate) computationally difficult problems. Consequently, randomness is probably not as powerful as it seems above.

We conclude with the power of randomness in other computational settings, such as space complexity and probabilistic proof systems. In particular we'll discuss the remarkable properties of Zero-Knowledge proofs and of Probabilistically Checkable proofs.

The bibliography contains several useful books and surveys in which material pertaining to the computational randomness may be found. In particular, we include surveys on topics not covered in the lecture, including *extractors* (designed to purify weak random sources) and *expander graphs* (perhaps the most useful "pseudorandom" object).

Keywords: randomness, complexity, pseudorandom, derandomnization.

E.A. Hirsch et al. (Eds.): CSR 2008, LNCS 5010, pp. 1–2, 2008.
© Springer-Verlag Berlin Heidelberg 2008

References

1. Goldreich, O.: Modern Cryptography, Probabilistic Proofs and Pseudorandomness. Algorithms and Combinatorics, vol. 17. Springer, Heidelberg (1998)
2. Motwani, R., Raghavan, P.: Randomized Algorithms. Cambridge University Press, Cambridge (1995)
3. Shaltiel, R.: Recent Developments in Explicit Constructions of Extractors. Bull. EATCS 77, 67–95 (2002)
4. Wigderson, A.: P, NP and Mathematics — A computational complexity perspective. In: Proceedings of the ICM 2006, Madrid, vol. I, pp. 665–712. EMS Publishing House, Zurich (2007), http://www.icm2006.org/proceedings/Vol_I/29.pdf