The Power and Weakness of Randomness in Computation

Avi Wigderson

Institute for Advanced Study, Princeton

Humanity 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. We 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 can 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) which are exponentially faster than their (best known) deterministic counterparts, and probabilistic algorithms which achieve significant space savings over deterministic ones. Other settings include distributed algorithms where randomness (provably) achieves exponentially smaller congestion than deterministic ones. Finally we'll show that using randomness, proof systems can be enhanced to allow properties unattainable without it. Letting the verifier and prover toss coins, proof systems can allow spot checking of proofs (PCPs - a central tool in the theory of approximation), as well as zero-knowledge proofs (proofs revealing nothing except their validity - a central tool in cryptography).

Computational Efficiency is Paramount to Understanding Randomness. We explain the computationally-motivated definition of randomness, and try to argue its merits as the "right" definition. The central idea is "computational indistinguishability" - declaring a distribution pseudorandom if it cannot be distinguished from the uniform distribution by any efficient procedure (in a given class, say time or space bounded algorithms). It is evident, almost by definition, that such pseudorandom distributions are as good as uniform as sources of randomness for probabilistic algorithms in the given class. We then demonstrate the remarkable fact, known as the "hardness vs. randomness paradigm" that such pseudorandomness may be generated deterministically and efficiently, from (appropriate) computationally difficult problems. This leads to a deterministic "derandomization" of any given probabilistic algorithm, which is not much slower. Consequently, randomness is probably not as powerful as it seems above.

For a comprehensive text on probabilistic algorithms the reader is refered to [MR]. For a thorough discussion of both probabilistic proof systems, as well as pseudorandomness, the reader is refered to [G].

J.R. Correa, A. Hevia, and M. Kiwi (Eds.): LATIN 2006, LNCS 3887, pp. 28–29, 2006.
© Springer-Verlag Berlin Heidelberg 2006

References

[MR] Motwani, Rajeev and Raghavan, Prabhakar Randomized Algorithms, Cambridge University Press, 1995.

[G] Goldreich, Oded Modern Cryptography, Probabilisitc Proofs and Pseudorandomness, Springer Verlag, Algorithms and Combinatorics, Vol 17, 1998.