Preface to SICOMP's Special Issue on Randomness and Complexity

Oded Goldreich
Department of Computer Science
Weizmann Institute of Science
Rehovot, Israel.
oded.goldreich@weizmann.ac.il

Madhu Sudan
Laboratory for Computer Science
Massachusetts Institute of Technology
Cambridge, MA 02139.
madhu@mit.edu

March 28, 2006

The idea of a SICOMP special issue on "Randomness and Complexity" occurred to us, when we were in residence at the Radcliffe Institute for Advanced Study of Harvard University during the academic year 2003-2004. We were part of a "Science Cluster" in Theoretical Computer Science at the Radcliffe Institute, whose other members were Eli Ben-Sasson, Dana Ron, Ronitt Rubinfeld, and Salil Vadhan. The focus of this cluster was "Randomness and Computation". The extensive interaction within the cluster members as well as with frequent visitors (most notably Irit Dinur, Shafi Goldwasser and Tali Kaufman) made us more aware than ever of the richness of the area, and the idea of editing a special issue on "Randomness and Complexity" emerged naturally.

The interplay of randomness and complexity is at the heart of modern cryptography and plays a fundamental role in the design of algorithms and in complexity theory at large. Specifically, this interplay is pivotal to several intriguing notions of probabilistic proof systems (e.g., interactive proofs, zero-knowledge proofs, and PCP), is the focal of the computational approach to randomness, and is essential for various types of sub-linear time algorithms. All these areas were at the focus of extensive research in the last two decades, but each "research generation" brings its own new perspective (and/or focus) to them. This special issue report some of the recent progress achieved in these related areas. Following are some of its main themes.

Cryptography. The paper of Applebaum, Ishai and Kushilevitz provides strong evidence that many Cryptographic primitives and tasks can be implemented at very low complexity. For example, they show that the existence of one-way functions that can be evaluated in $\mathcal{NC}1$ implies the existence of one-way functions that can be evaluated in $\mathcal{NC}0$. Whereas the former are widely believed to exist (e.g., based on the standard factoring assumption), most researchers have previously believed that the latter do not exist. We stress that evaluation in $\mathcal{NC}0$ means that each output bit only depends on a constant number of input bits. The new work further shows that dependence on *four* input bits suffices (whereas dependence on at least *three* input bits is definitely necessary).

Probabilistically Checkable Proofs (PCPs). Current research in the area is marked by a renewed attention to aspects such as the following:

1. Achieving constructs of almost-linear length that can be tested by very few (say constant number of) queries.

2. Obtaining a combinatorial proof of the PCP Theorem.
3. Exploration of the relationship between PCP and coding theory (e.g., locally testable codes).
4. Applications of PCPs to obtaining new inapproximability results regarding long-standing problems such as min-Bisection.

Specifically, the paper of Ben-Sasson *et. al.* presents significant improvements to the trade-off between proof-length and the number of queries. The paper of Dinur and Reingold makes a major step in the project of obtaining combinatorial proofs of the PCP Theorem. Both papers share a reformulation of the proof-composition paradigm, where "proximity testing" and "robustness" play a central role. Lastly, Khot's paper puts forward new PCP parameters and introduces new PCP constructions that are used to provide evidence that min-Bisection is not approximable up-to some constant.

Randomness Extraction. The construction of randomness extractors has received much attention in the last two decades. Much of the past work (especially in the 1990's) has focused on extracting randomness from a single weak source, while using an auxiliary short (uniformly distributed) seed. The focus was on using the weakest possible form of a source (i.e., a min-entropy source). In contrast, the current era is marked by a focus on stronger sources, while disallowing the use of an auxiliary (uniformly distributed) seed. The paper of Gabizon, Raz and Shaltiel studies bit-fixing sources, whereas the paper of Barak, Impagliazzo and Wigderson studies extraction from a constant number of independent sources of linear min-entropy (which may be viewed as a single source consisting of a constant number of independent blocks). Indeed, each of these papers revisits problems raised in the mid 1980's, which were neglected in the 1990's (due to the focus of that era on obtaining the best results for seed-assisted extraction from a single min-entropy source). Needless to say, we believe that the renewed interest in these problems (especially the second one) is highly justified.

We wish to seize the opportunity to say a few words regarding seed-assisted versus seedless randomness extraction. Seed-assisted randomness extraction found many applications (via direct and indirect connections to other important problems), but still one may ask what do they mean for the original problem of implementing a randomized procedure using a weak source of randomness. One answer is that the seed can be obtained from an expensive high-quality auxiliary source, and that one wishes to minimize the use of this source (and thus uses a cheaper low-quality random source for the bulk of the randomness required). Another answer is that if the seed is short enough then one may afford to try all possible seeds, invoke the procedure with the corresponding randomness extracted (from the same source output and varying seeds), and rule by majority. This suggestion is adequate for the implementation of standard randomized algorithms, but not in "adversarial" settings (e.g., cryptography) in which a randomized procedure is invoked in order to protect against some (adversarial) party. Thus, seedless randomness extraction is essential in many applications.

Worst-Case to Average-Case Reductions. The question of whether worst-case to average-case reductions or even merely "hardness amplification" exist for $\mathcal{NP}$ has received much interest recently. The first part of the question is studied in the paper of Bogdanov and Trevisan which provides a negative indication, restricted to non-adaptive reductions. The second part of the question is unfortunately not represented in this special issue (and the interested reader is directed to [1]).

Zero-Knowledge. Vadhan's paper presents an *unconditional* study of *computational* zero-knowledge, yielding valuable transformations between various forms of zero-knowledge (e.g., from a weak form of zero-knowledge to the standard form). This work builds on studies of *statistical* zero-knowledge that were conducted in the late 1990's, thus fulfilling a prophecy made at the time.

Low-Degree Tests. The celebrated low-degree tests have been revisited recently with a focus on derandomization and on low-degree tests over small finite fields. The first direction is represented by the work of Shpilka and Wigderson that seem to provide a "proof from The Book" for (a derandomized version of) the linearity test. The second direction is unfortunately not represented in this special issue (and the interested reader is directed to [2, 3]).

Acknowledgments

We are grateful to the contributing authors for accepting our invitation to publish in this special issue. In some cases, they had to decline other competitive invitations in order to do so.

We are grateful to Eva Tardos for handling the refereeing process of the paper of Ben-Sasson, Goldreich, Harsha, Sudan, and Vadhan.

References

[1] A. Healy, S. Vadhan and E. Viola. Using nondeterminism to amplify hardness. In *36th STOC*, pages 192–201, 2004.

[2] C.S. Jutla, A.C. Patthak, A. Rudra, D. Zuckerman. Testing Low-Degree Polynomials over Prime Fields. In *45th FOCS*, pages 423–432, 2004.

[3] T. Kaufman and D. Ron. Testing Polynomials over General Fields. In *45th FOCS*, pages 413–422, 2004.