De-randomizing BPP: The State of the Art

Avi Wigderson
The Hebrew University, Jerusalem
avi@cs.huji.ac.il

The introduction of randomization into efficient computation has been one of the most fertile and useful ideas in computer science. In cryptography and asynchronous computing, randomization makes possible tasks that are impossible to perform deterministically. Even for function computation, many examples are known in which randomization allows considerable savings in resources like space and time over deterministic algorithms, or even "only" simplifies them.

But to what extent is this seeming power of randomness over determinism real? The most famous concrete version of this question regards the power of BPP, the class of problems solvable by probabilistic polynomial time algorithms making small constant error. What is the relative power of such algorithms compared to deterministic ones? This is largely open. On the one hand, it is possible that $P = BPP$, i.e., randomness is useless for solving new problems in polynomial time. On the other, we might have $BPP = EXP$, which would say that randomness would be a nearly omnipotent tool for algorithm design.

The only viable path towards resolving this problem was initiated in the seminal papers [4, 14], from which developed the concept of "pseudorandom generators", and the "hardness vs randomness" paradigm: BPP can be nontrivially simulated by deterministic algorithms, if some hard function is available.

While the hard functions above needed in fact to be one-way functions, completely different pseudo-random generators [9, 10] allowed the use of any hard function in EXP for such nontrivial simulation. Further progress considerably weakened the hardness requirement, and considerably strengthened the deterministic simulation. The state of the art results are summarized (informally) below.

Theorem 1 *[3] If $EXP \not\subseteq P/poly$ then BPP has sub-exponential deterministic algorithms.*

Theorem 2 *[6] If $E \not\subseteq SIZE(2^{o(n)})$ then BPP=P.*

Theorem 3 *[7] If $EXP \neq BPP$ then BPP has subexpoenntial deterministic algorithms on average (for any efficiently samplable distribution).*

The first two results give the two extremes of the hardness vs randomness trade-offs under nonuniform (circuit) lower bounds. The last result gives the best simulation under uniform (probabilistic Turing machine) lower bounds. These leave little doubt in the following conjecture:

Conjecture 4 *$BPP \neq EXP$*

The talk will concentrate on the most recent, uniform result, of [7]. It will focus on the major ideas that led to the best nonuniform results, the difficulties in making them uniform, and how to overcome these difficulties. Some new directions and open problems suggested by this result will be presented, as well as a discussion if we are closer to resolving the conjecture above.

This area of research has been extremely active in the last few years, and several important ideas arose which we will have only little time to touch. Among them are

- The surprising possibility of using hitting sets (which are natural for de-randomizing RP) to de-randomize BPP [1, 2].
- The recent optimal hardness-amplification methods of [12], generalizing those of [6].
- The extension of the de-randomization techniques from BPP to AM, of [8].

- The amazing use of these computational methods for the information theoretic construction of extractors by [13].

The bibliography below is far from complete. All of [6, 7, 12] contain a good overview of the historical development as well as a comprehensive bibliography. For a more general survey of pseudorandomness, the reader is referred to the excellent recent monograph [5].

References

[1] A. Andreev, A. Clementi and J. Rolim, "Hitting Sets Derandomize BPP", in *XXIII International Colloquium on Algorithms, Logic and Programming (ICALP'96)*, 1996.

[2] A. Andreev, A. Clementi, and J. Rolim, "Hitting Properties of Hard Boolean Operators and its Consequences on BPP", manuscript, 1996.

[3] L. Babai, L. Fortnow, N. Nisan and A. Wigderson, "BPP has Subexponential Time Simulations unless EXPTIME has Publishable Proofs", *Complexity Theory*, Vol 3, pp. 307–318, 1993.

[4] M. Blum and S. Micali. "How to Generate Cryptographically Strong Sequences of Pseudo-Random Bits", *SIAM J. Comput.*, Vol. 13, pages 850–864, 1984.

[5] O. Goldreich, "Modern Cryptography, Probabilistic Proofs and Pseudorandomness", Algorithms and Combinatorics Series, Springer-Verlag 1999.

[6] R. Impagliazzo and A. Wigderson, "P=BPP unless E has sub-exponential circuits: Derandomizing the XOR Lemma", Proc. of the *29th STOC*, pp. 220–229, 1997.

[7] R. Impagliazzo and A. Wigderson, "Randomness vs. Time': De-randomization under a uniform assumption", Proc. of the *36th FOCS* , 1998.

[8] A. Klivans, D. van Melkebeek, "Graph Nonisomorphism has Subexponential Size Proofs Unless the Polynomial-Time Hierarchy Collapses", ECCC report TR98-075, 1998.

[9] N. Nisan, "Pseudo-random bits for constant depth circuits", *Combinatorica 11* (1), pp. 63-70, 1991.

[10] N. Nisan, and A. Wigderson, "Hardness vs Randomness", *J. Comput. System Sci.* 49, 149-167, 1994

[11] A. Shamir, "On the generation of cryptographically strong pseudo-random sequences", *8th ICALP, Lecture Notoes in Computer Science* 62, Springer-Verlag, pp. 544–550, 1981.

[12] M. Sudan, L. Trevisan and S. Vadhan, "Pseudorandom generators without the XOR Lemma", ECCC Report TR98-074, 1998.

[13] L. Trevisan, "Construction of Extractors Using Pseudo-Random Generators", Proc of the *31st STOC*, 1999.

[14] A.C. Yao, "Theory and Application of Trapdoor Functions", in *23st FOCS*, pages 80–91, 1982.