Computational Pseudo-Randomness

Avi Wigderson
Computer Science Institute
Hebrew University, Jerusalem

Abstract

One of the most important and fundamental discoveries of Theoretical Computer Science is the surprising connection between the computational power of randomness, and computational lower bounds on explicit functions. The currently strongest result of this form states [1]:

Theorem 1 *If EXP has no subexponentially small circuits*
then BPP had deterministic, pseudo-polynomial time algorithms.

The key mechanism behind this connection is called a pseudo-random generator. There are two different constructions known - the "classical" one of [2, 19], which uses the difficulty of computing functions whose inverse is easy, and the more recent one of [14, 15], which can use essentially any hard function.

The talk will motivate and define the notions above. Then it will survey the main ideas behind the constructions of both generators, the proofs that they are pseudo-random, and the theorem above. This will lead to several natural open problems and conjectures, of which the most important (and I believe, solvable with present technology) is

Conjecture 1 $EXP \neq BPP$

There will be no time to discuss the related (and equally interesting) topic of pseudo-random generators for restricted models, such as constant-depth circuits and log-space Turing machines.

References

[1] L. Babai, F. Fortnow, N. Nisan, and A. Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Computational Complexity*, 3:307–318, 1993.

[2] M. Blum and S. Micali. How to generate cryptographically strong sequences of pseudo-random bits. *SIAM Journal on Computing*, 13:850–864, 1984. First version in FOCS 1982.

[3] W. Diffie and M. E. Hellman. New directions in cryptography. IEEE Trans. Infor. Theory, IT-22:644–654, November 1976.

[4] O. Goldreich, S. Goldwasser, and S. Micali. How to construct random functions. *Journal of the ACM*, 33(4):792–807, 1986. Extended abstract in FOCS84.

[5] O. Goldreich and H. Krawczyk. Sparse pseudorandom distributions. In G. Brassard, editor, *Advances in Cryptology—CRYPTO '89*, volume 435 of *Lecture Notes in Computer Science*, Springer-Verlag, 1990.

[6] O. Goldreich, H. Krawczyk, and M. Luby. On the existence of pseudorandom generators. In *Twenty-Ninth Annual Symposium on Foundations of Computer Science*, pages 12–24, 1988.

[7] O. Goldreich and L.A. Levin. A hard-core predicate to any one-way function. In *Proceedings of the Twenty-First Annual ACM Symposium on Theory of Computing*, pages 25–32, 1989.

[8] S. Goldwasser and S. Micali. Probabilistic encryption. *Journal of Computer and System Sciences*, 28(2):270–299, 1984. Previous version in STOC 1982.

[9] J. Hastad. Pseudo-random generators with uniform assumptions. *Proceedings of the Twenty-Second Annual ACM Symposium on Theory of Computing*, pages 395–404, 1990.

[10] R. Impagliazzo, L.A. Levin, and M. Luby. Pseudorandom generation from one-way functions. In *Proceedings of the Twenty-First Annual ACM*

0-8186-6915-2/95 $04.00

Symposium on Theory of Computing, pages 12–24, 1989.

[11] Blum L., M. Blum, and M. Shub. A simple secure unpredictable pseudo-random number generator. *SIAM Journal on Computing*, 15:364–383, 1982. Preliminary version in Crypto82.

[12] L.A. Levin. One-way function and pseudorandom generators. In *Proceedings of the Eighteenth Annual ACM Symposium on Theory of Computing*, pages 363–365, 1985.

[13] M. Luby and C. Rackoff. How to construct pseudorandom permutations from pseudorandom functions. *SIAM Journal on Computing*, 17:373–386, 1988. Extended abstract in FOCS86.

[14] N. Nisan. Pseudorandom bits for constant depth circuits. *Combinatorica*, 11(1):63–70, 1991.

[15] N. Nisan and A. Wigderson. Hardness vs. randomness. In *29^{th} Annual Symposium on Foundations of Computer Science*, pages 2–11. IEEE, 1988.

[16] J.H. Reif and J.D. Tygar. Efficient parallel pseudo-random number generation. In Hugh C. Williams, editor, *Advances in Cryptology—CRYPTO '85*, volume 218 of *Lecture Notes in Computer Science*, pages 433–446. Springer-Verlag, 1985.

[17] A. Shamir. On the generation of cryptographically strong pseudorandom sequences. *ACM Transactions on Computer Systems*, 1(1):38–44, February 1983.

[18] U.V. Vazirani and V.V. Vazirani. Efficient and secure pseudo-random number generation. In *25^{th} Annual Symposium on Foundations of Computer Science*, pages 458–463. IEEE, 1984.

[19] A.C. Yao. Theory and applications of trapdoor functions. In *29^{rd} Annual Symposium on Foundations of Computer Science*, pages 80–91. IEEE, 1982.