On the Power of Small-Depth Computation

On the Power of Small-Depth Computation

Emanuele Viola

Northeastern University
440 Huntington Ave.
Boston, MA 02115
USA

viola@ccs.neu.edu

the essence of knowledge

Boston – Delft

Foundations and Trends® in Theoretical Computer Science

Published, sold and distributed by:
now Publishers Inc.
PO Box 1024
Hanover, MA 02339
USA
Tel. +1-781-985-4510
www.nowpublishers.com
sales@nowpublishers.com

Outside North America:
now Publishers Inc.
PO Box 179
2600 AD Delft
The Netherlands
Tel. +31-6-51115274

The preferred citation for this publication is E. Viola, On the Power of Small-Depth Computation, Foundation and Trends® in Theoretical Computer Science, vol 5, no 1, pp 1–72, 2009

ISBN: 978-1-60198-300-8

Foundations and Trends® in Theoretical Computer Science
Volume 5 Issue 1, 2009

Editorial Board

Editorial Scope

Foundations and Trends® in Theoretical Computer Science will publish survey and tutorial articles in the following topics:

- Algorithmic game theory
- Computational algebra
- Computational aspects of combinatorics and graph theory
- Computational aspects of communication
- Computational biology
- Computational complexity
- Computational geometry
- Computational learning
- Computational Models and Complexity
- Computational Number Theory
- Cryptography and information security
- Data structures
- Database theory
- Design and analysis of algorithms
- Distributed computing
- Information retrieval
- Operations Research
- Parallel algorithms
- Quantum Computation
- Randomness in Computation

Information for Librarians
Foundations and Trends® in Theoretical Computer Science, 2009, Volume 5, 4 issues. ISSN paper version 1551-305X. ISSN online version 1551-3068. Also available as a combined paper and online subscription.

Foundations and Trends® in
Theoretical Computer Science
Vol. 5, No. 1 (2009) 1–72

DOI: 10.1561/0400000033

now
the essence of knowledge

On the Power of Small-Depth Computation

Emanuele Viola

Northeastern University, 440 Huntington Ave., Boston, MA 02115, USA, viola@ccs.neu.edu

Abstract

In this monograph we discuss selected topics on small-depth computation, presenting a few unpublished proofs along the way. The four sections contain:

(1) A unified treatment of the challenge of exhibiting explicit functions that have small correlation with low-degree polynomials over $\{0,1\}$.
(2) An unpublished proof that small bounded-depth circuits (AC^0) have exponentially small correlation with the parity function. The proof is due to Klivans and Vadhan; it builds upon and simplifies previous ones.
(3) Valiant's simulation of log-depth linear-size circuits of fan-in 2 by sub-exponential size circuits of depth 3 and unbounded fan-in. To our knowledge, a proof of this result has never appeared in full.
(4) Applebaum, Ishai, and Kushilevitz's cryptography in bounded depth.

Supported by NSF grant CCF-0845003.

Contents

1

Introduction

The NP-completeness of SAT is a celebrated example of the power of bounded-depth computation: the core of the argument is a depth reduction establishing that any small non-deterministic circuit — an arbitrary NP computation on an arbitrary input — can be simulated by a small non-deterministic circuit of depth 2 with unbounded fan-in — a SAT instance.

Many other examples permeate theoretical computer science. In this monograph we discuss a selected subset of them and include a few unpublished proofs.

We start in Section 2 with considering low-degree polynomials over the fields with two elements $\{0,1\}$ (a.k.a. GF(2)). Polynomials are a bounded-depth computational model: they correspond to depth-2 unbounded fan-in circuits whose output gate is a sum (in our case, modulo 2). Despite the apparent simplicity of the model, a fundamental challenge has resisted decades of attacks from researchers: exhibit explicit functions that have small correlation with low-degree polynomials. The section is a unified treatment of the state-of-the-art on this challenge. We discuss long-standing results and recent developments, related proof techniques, and connections with pseudorandom

generators. We also suggest several research directions. Along the way, we present previously unpublished proofs of certain correlation bounds.

In Section 3 we consider unbounded fan-in circuits of small depth with $\wedge$ (and), $\vee$ (or), and $\neg$ (not) gates, known as AC^0. Here, we present an unpublished proof of the well-known result that small AC^0 circuits have exponentially small correlation with the parity function. The proof is due to Klivans and Vadhan; it builds upon and simplifies previous ones.

In Section 4 we present a depth-reduction result by Valiant [72, 73] whose proof to our knowledge has never appeared in full. The result is that log-depth linear-size circuits of fan-in 2 can be simulated by sub-exponential size circuits of depth 3 and unbounded fan-in (again, the gates are $\wedge, \vee, \neg$). Although the parameters are more contrived, this result is in the same spirit of the NP-completeness of SAT mentioned at the beginning of this introduction. The latter depth-reduction crucially exploits *non-determinism*; interestingly, we have to work harder to prove Valiant's *deterministic* simulation.

Finally, in Section 5 we present the result by Applebaum, Ishai, and Kushilevitz [7] that shows that, under standard complexity theoretic assumptions, many cryptographic primitives can be implemented in very restricted computational models. Specifically, one can implement those primitives by functions such that each of their output bits only depends on a constant number of input bits. In particular, each output bit can be computed by a circuit of constant size and depth.

Of course, many exciting works on small-depth computation are not covered here. Recent ones include Rossman's lower bound [68] and the pseudorandom generators for small-depth circuits by Bazzi, Razborov, and Braverman [21].

Publishing note. Section 2 appeared in ACM SIGACT News Volume 40, Issue 1 (March 2009). The other sections are a polished version of the notes of Lectures 4, 5, 6, 7, 10, 12, 13, and 14 of the author's class "Gems of Theoretical Computer Science," taught at Northeastern University in Spring 2009 [78]. I thank the audience of the class, Rajmohan Rajaraman, and Ravi Sundaram for their useful feedback. I am grateful to Aldo Cassola, Dimitrios Kanoulas, Eric Miles, and Ravi Sundaram for scribing the above lectures.

References

[1] S. Aaronson and A. Wigderson, "Algebrization: A new barrier in complexity theory," in *40th Annual ACM Symposium on the Theory of Computing (STOC)*, pp. 731–740, 2008.

[2] M. Agrawal and V. Vinay, "Arithmetic circuits: A chasm at depth four," in *49th Annual IEEE Symposium on Foundations of Computer Science (FOCS)*, pp. 67–75, 2008.

[3] M. Ajtai, "Σ_1^1-formulae on finite structures," *Annals of Pure and Applied Logic*, vol. 24, no. 1, pp. 1–48, 1983.

[4] N. Alon and R. Beigel, "Lower bounds for approximations by low degree polynomials over Z_m," in *16th Annual Conference on Computational Complexity*, pp. 184–187, IEEE, June 18–21 2001.

[5] N. Alon, O. Goldreich, J. Håstad, and R. Peralta, "Simple constructions of almost k-wise independent random variables," *Random Structures & Algorithms*, vol. 3, no. 3, pp. 289–304, 1992.

[6] N. Alon, T. Kaufman, M. Krivelevich, S. Litsyn, and D. Ron, "Testing low-degree polynomials over GF(2)," in *7th International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, vol. 2764 of *Lecture Notes in Computer Science*, pp. 188–199, Springer, 2003.

[7] B. Applebaum, Y. Ishai, and E. Kushilevitz, "Cryptography in NC^0," *SIAM Journal of Computing*, vol. 36, no. 4, pp. 845–888, 2006.

[8] S. Arora and B. Barak, *Computational Complexity: A Modern Approach*. Cambridge University Press, January 2007.

[9] J. Aspnes, R. Beigel, M. Furst, and S. Rudich, "The expressive power of voting polynomials," *Combinatorica*, vol. 14, no. 2, pp. 135–148, 1994.

[10] L. Babai, N. Nisan, and M. Szegedy, "Multiparty protocols, pseudorandom generators for logspace, and time-space trade-offs," *Journal of Computer System and Sciences*, vol. 45, no. 2, pp. 204–232, 1992.

[11] T. Baker, J. Gill, and R. Solovay, "Relativizations of the P=?NP question," *SIAM Journal of Computing*, vol. 4, no. 4, pp. 431–442, 1975.

[12] P. Beame, S. A. Cook, and H. J. Hoover, "Log depth circuits for division and related problems," *SIAM Journal of Computing*, vol. 15, no. 4, pp. 994–1003, 1986.

[13] R. Beigel, "The polynomial method in circuit complexity," in *8th Annual Structure in Complexity Theory Conference*, pp. 82–95, IEEE, 1993.

[14] R. Beigel, "When do extra majority gates help? polylog(N) majority gates are equivalent to one," *Computational Complexity*, vol. 4, no. 4, pp. 314–324, 1994. Special issue devoted to the 4th Annual McGill Workshop on Complexity Theory.

[15] I. Ben-Eliezer, R. Hod, and S. Lovett, "Random low degree polynomials are hard to approximate," Manuscript, 2008.

[16] E. Ben-Sasson, M. Sudan, S. Vadhan, and A. Wigderson, "Randomness-efficient low degree tests and short PCPs via epsilon-biased sets," in *35th Annual Symposium on Theory of Computing (STOC)*, pp. 612–621, ACM, 2003.

[17] N. Bhatnagar, P. Gopalan, and R. J. Lipton, "Symmetric polynomials over Z_m and simultaneous communication protocols," *Journal of Computer and System Sciences*, vol. 72, no. 2, pp. 252–285, 2006.

[18] A. Bogdanov and E. Viola, "Pseudorandom bits for polynomials," in *48th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 41–51, IEEE, 2007. To appear in *SIAM Journal on Computing*.

[19] R. B. Boppana and M. Sipser, "The complexity of finite functions," in *Handbook of Theoretical Computer Science*, vol. A, pp. 757–804, Amsterdam: Elsevier, 1990.

[20] J. Bourgain, "Estimation of certain exponential sums arising in complexity theory," *Comptes Rendus Mathematique Academy of Sciences Paris*, vol. 340, no. 9, pp. 627–631, 2005.

[21] M. Braverman, "Poly-logarithmic independence fools AC^0 circuits," in *24th Conference on Computational Complexity (CCC)*, IEEE, 2009.

[22] J.-Y. Cai, "With probability one, a random oracle separates PSPACE from the polynomial-time hierarchy," *Journal of Computer and System Sciences*, vol. 38, no. 1, pp. 68–85, 1989.

[23] J.-Y. Cai, F. Green, and T. Thierauf, "On the Correlation of Symmetric Functions," *Mathematical Systems Theory*, vol. 29, no. 3, pp. 245–258, 1996.

[24] A. Chattopadhyay, "Discrepancy and the power of bottom fan-in in depth-three circuits," in *48th Annual Symposium on Foundations of Computer Science (FOCS)*, pp. 449–458, IEEE, 2007.

[25] F. R. K. Chung and P. Tetali, "Communication complexity and quasi randomness," *SIAM Journal on Discrete Mathematics*, vol. 6, no. 1, pp. 110–123, 1993.

[26] P. Clote and E. Kranakis, *Boolean Functions and Computation Models*. Springer, 2002.

[27] T. M. Cover and J. A. Thomas, *Elements of Information Theory (Wiley Series in Telecommunications and Signal Processing)*. Wiley-Interscience, 2006.

[28] D. Dubhashi and A. Panconesi, *Concentration of Measure for the Analysis of Randomized Algorithms*. Cambridge University Press, 2009.

[29] Y. Freund, "Boosting a weak learning algorithm by majority," *Information and Computation*, vol. 121, no. 2, pp. 256–285, 1995.

[30] M. L. Furst, J. B. Saxe, and M. Sipser, "Parity, circuits, and the polynomial-time hierarchy.," *Mathematical Systems Theory*, vol. 17, no. 1, pp. 13–27, 1984.

[31] A. Gál and V. Trifonov, "On the correlation between parity and modular polynomials," in *31st International Symposium on Mathematical Foundations of Computer Science (MFCS)*, vol. 4162 of *Lecture Notes in Computer Science*, pp. 387–398, Springer, 2006.

[32] M. Goldmann, J. Håstad, and A. A. Razborov, "Majority gates vs. general weighted threshold gates," *Computational Complexity*, vol. 22, pp. 277–300, 1992.

[33] O. Goldreich, "Candidate one-way functions based on expander graphs," Technical Report, Electronic Colloquium on Computational Complexity, 2000.

[34] O. Goldreich, *Foundations of Cryptography: Volume 1, Basic Tools*. Cambridge: Cambridge University Press, 2001.

[35] O. Goldreich, N. Nisan, and A. Wigderson, "On Yao's XOR lemma," Techncial Report TR95–050, *Electronic Colloquium on Computational Complexity*, www.eccc.uni-trier.de/, March 1995.

[36] T. Gowers, "A new proof of Szemerédi's theorem for arithmetic progressions of length four," *Geometric and Functional Analysis*, vol. 8, no. 3, pp. 529–551, 1998.

[37] T. Gowers, "A new proof of Szemerédi's theorem," *Geometric and Functional Analysis*, vol. 11, no. 3, pp. 465–588, 2001.

[38] A. Granville and Z. Rudnick, "Uniform distribution," in *Equidistribution in Number Theory, An Introduction*, vol. 237 of *NATO Science Series II: Mathematics, Physics and Chemsitry*, pp. 1–13, Springer, 2007.

[39] B. Green and T. Tao, "The distribution of polynomials over finite fields, with applications to the Gowers norms," arXiv:0711.3191v1, 2007.

[40] B. Green and T. Tao, "An inverse theorem for the Gowers $U^3(G)$ norm," *Proceedings of the Edinburgh Mathematical Society (Series 2)*, vol. 51, no. 01, pp. 73–153, 2008.

[41] F. Green, "The correlation between parity and quadratic polynomials mod 3," *Journal of Computer System and Sciences*, vol. 69, no. 1, pp. 28–44, 2004.

[42] F. Green and A. Roy, "Uniqueness of Optimal Mod 3 Circuits for Parity," in *Dagstuhl Seminar Proceedings, Algebraic Methods in Computational Complexity*, vol. 07411, 2007.

[43] F. Green, A. Roy, and H. Straubing, "Bounds on an exponential sum arising in Boolean circuit complexity," *Comptes Rendus Mathematique Academy of Sciences Paris*, vol. 341, no. 5, pp. 279–282, 2005.

[44] V. Grolmusz, "Separating the communication complexities of MODm and MODp circuits," *Journal of Computer System and Sciences*, vol. 51, no. 2, pp. 307–313, 1995.

[45] D. Gutfreund and E. Viola, "Fooling parity tests with parity gates," in *8th International Workshop on Randomization and Computation (RANDOM)*, pp. 381–392, Springer, 2004.

[46] J. Håstad and M. Goldmann, "On the power of small-depth threshold circuits," *Computational Complexity*, vol. 1, no. 2, pp. 113–129, 1991.

[47] A. Hajnal, W. Maass, P. Pudlák, M. Szegedy, and G. Turán, "Threshold circuits of bounded depth," *Journal of Computer System and Sciences*, vol. 46, no. 2, pp. 129–154, 1993.

[48] K. A. Hansen, "Lower bounds for circuits with few modular gates using exponential sums," *Electronic Colloquium on Computational Complexity*, 2006. Technical Report TR06-079, www.eccc.uni-trier.de/.

[49] J. Håstad, *Computational Limitations of Small-depth Circuits*. MIT Press, 1987.

[50] A. Healy, "Randomness-efficient sampling within NC^1," *Computational Complexity*, vol. 17, pp. 3–37, April 2008.

[51] A. Healy and E. Viola, "Constant-depth circuits for arithmetic in finite fields of characteristic two," in *23rd International Symposium on Theoretical Aspects of Computer Science (STACS)*, pp. 672–683, Springer, 2006.

[52] R. Impagliazzo and M. Naor, "Efficient cryptographic schemes provably as secure as subset sum," *Journal of Cryptology*, vol. 9, pp. 199–216, Fall 1996.

[53] R. Impagliazzo and A. Wigderson, "$P = BPP$ if E requires exponential circuits: Derandomizing the XOR lemma," in *29th Annual Symposium on Theory of Computing (STOC)*, pp. 220–229, ACM, 1997.

[54] K. Iwama and H. Morizumi, "An explicit lower bound of $5n - o(n)$ for Boolean circuits," in *Mathematical Foundations of Computer Science (MFCS)*, pp. 353–364, 2002.

[55] A. R. Klivans, "On the derandomization of constant depth circuits," in *5th International Workshop on Randomization and Approximation Techniques in Computer Science (RANDOM)*, Springer 2001.

[56] E. Kushilevitz and N. Nisan, *Communication complexity*. Cambridge: Cambridge University Press, 1997.

[57] S. Lovett, "Unconditional pseudorandom generators for low degree polynomials," in *40th Annual Symposium on the Theory of Computing (STOC)*, pp. 557–562, ACM, 2008.

[58] S. Lovett, R. Meshulam, and A. Samorodnitsky, "Inverse conjecture for the Gowers norm is false," in *40th Annual Symposium on the Theory of Computing (STOC)*, pp. 547–556, ACM, 2008.

[59] M. Luby, B. Veličković, and A. Wigderson, "Deterministic approximate counting of depth-2 circuits," in *2nd Israeli Symposium on Theoretical Computer Science (ISTCS)*, pp. 18–24, 1993.

[60] J. Naor and M. Naor, "Small-bias probability spaces: Efficient Constructions and Applications," *SIAM Journal of Computing*, vol. 22, no. 4, pp. 838–856, 1993.

[61] V. A. Nepomnjaščiĭ, "Rudimentary predicates and Turing calculations," *Soviet Mathematics-Doklady*, vol. 11, no. 6, pp. 1462–1465, 1970.

[62] N. Nisan, "Pseudorandom bits for constant depth circuits," *Combinatorica*, vol. 11, no. 1, pp. 63–70, 1991.
[63] N. Nisan and A. Wigderson, "Hardness vs Randomness," *Journal of Computer and Systems Sciences*, vol. 49, no. 2, pp. 149–167, 1994.
[64] R. Raz, "The BNS-Chung criterion for multi-party communication complexity," *Computational Complexity*, vol. 9, no. 2, pp. 113–122, 2000.
[65] A. Razborov, "Lower bounds on the dimension of schemes of bounded depth in a complete basis containing the logical addition function," *Matematicheskie Zametki*, vol. 41, no. 4, pp. 598–607, 623, 1987.
[66] A. Razborov and S. Rudich, "Natural Proofs," *Journal of Computer and System Sciences*, vol. 55, pp. 24–35, August 1997.
[67] A. Razborov and A. Wigderson, "$n^{\Omega(\log n)}$ lower bounds on the size of depth-3 threshold circuits with AND gates at the bottom," *Information Processing Letters*, vol. 45, no. 6, pp. 303–307, 1993.
[68] B. Rossman, "On the constant-depth complexity of k-clique," in *40th Annual Symposium on the Theory of Computing (STOC)*, ACM, 2008.
[69] A. Samorodnitsky, "Low-degree tests at large distances," in *39th Annual Symposium on Theory of Computing (STOC)*, pp. 506–515, ACM, 2007.
[70] R. Shaltiel and E. Viola, "Hardness amplification proofs require majority," in *40th Annual Symposium on the Theory of Computing (STOC)*, pp. 589–598, ACM, 2008.
[71] R. Smolensky, "Algebraic methods in the theory of lower bounds for Boolean circuit complexity," in *19th Annual Symposium on Theory of Computing*, pp. 77–82, ACM, 1987.
[72] L. G. Valiant, "Graph-theoretic arguments in low-level complexity," in *6th Symposium on Mathematical Foundations of Computer Science*, vol. 53 of *Lecture Notes in Computer Science*, pp. 162–176, Springer, 1977.
[73] L. G. Valiant, "Exponential lower bounds for restricted monotone circuits," in *15th annual ACM symposium on Theory of computing (STOC)*, pp. 110–117, ACM, 1983.
[74] E. Viola, "The complexity of hardness amplification and derandomization," PhD thesis, Harvard University, www.eccc.uni-trier.de/ 2006.
[75] E. Viola, "New correlation bounds for GF(2) polynomials using Gowers uniformity," *Electronic Colloquium on Computational Complexity*, Technical Report TR06-097, www.eccc.uni-trier.de/ 2006.
[76] E. Viola, "On Constructing Parallel Pseudorandom Generators from One-Way Functions," in *20th Annual Conference on Computational Complexity (CCC)*, pp. 183–197, IEEE, 2005.
[77] E. Viola, "Pseudorandom bits for constant-depth circuits with few arbitrary symmetric gates," *SIAM Journal on Computing*, vol. 36, no. 5, pp. 1387–1403, 2007.
[78] E. Viola, "Gems of theoretical computer science," Lecture notes of the class taught at Northeastern University. Available at http://www.ccs.neu.edu/home/viola/classes/gems-08/index.html, 2009.
[79] E. Viola, "The sum of d small-bias generators fools polynomials of degree d," *Computational Complexity*, vol. 18, no. 2, pp. 209–217, 2009.

[80] E. Viola and A. Wigderson, "Norms, XOR lemmas, and lower bounds for GF(2) polynomials and multiparty protocols," *Theory of Computing*, vol. 4, pp. 137–168, 2008.

[81] A. C.-C. Yao, "Separating the polynomial-time hierarchy by oracles," in *Proceedings of the 26th annual symposium on Foundations of computer science*, pp. 1–10, IEEE Press, 1985.