DOI:10.1145/3065468

To view the accompanying paper, visit doi.acm.org/10.1145/3065470 rh

Technical Perspective
Low-Depth Arithmetic Circuits

By Avi Wigderson

THE COMPUTATIONS OF polynomials (over a field, which we shall throughout assume is of zero or large enough characteristic) using arithmetic operations of addition and multiplication (and possibly division) are of course as natural as the computation of Boolean functions via logical gates, and capture many natural important tasks including Fourier transforms, linear algebra, matrix computations and more generally symbolic algebraic computations arising in many settings. Arithmetic circuits are the natural computational model for understanding the computational complexity of such tasks just like Boolean circuits are for Boolean functions. The presence of algebraic structure and mathematical tools supplied by centuries of work in algebra were a source of hope that understanding arithmetic circuits will be much faster and easier than their Boolean siblings. And while we generally know more about arithmetic circuits, their power is far from understood, and in particular, the arithmetic analog VP vs. VNP of the Boolean P vs. NP problem as formulated by Valiant[8] is wide open.

The past few years have seen a revolution in our understanding of arithmetic circuits. Surprising new upper bounds, combined with new powerful techniques of proving lower bounds, have brought us to recognize the mysterious importance of very shallow circuits to capture the long-term goals of the field, and to pinpointing with uncommon precision the complexity of natural problems in this model. These developments have rejuvenated the hope, and give a concrete program, to the possible separation of Valiant's classes VP and VNP. The following paper of Gupta et. al. on the "chasm at depth 3" is one of the culminations of this new understanding. I will now briefly explain the "chasm" phenomenon, and some of these developments, on which the authors of the paper elaborate.

A series of important works in the 1980s on constant-depth Boolean circuits gives a very good picture of their limitations, including tight exponential lower bounds on extremely simple functions like the symmetric functions. The basic message is that constant-depth (and polynomial size) is an extremely weak class of algorithms. Strangely (and specifically over large enough fields) this intuition fails completely for arithmetic circuits. In 1980, Ben-Or already made the important simple observation that the symmetric polynomials can be computed in depth-3 by a quadratic size formula! So, the challenge to prove exponential lower bounds for this simple model was on. Such bounds were proved under further restrictions (like homogeneity) by Nisan-Wigderson,[6] who introduced important techniques of partial derivatives and random restrictions to the study arithmetic circuits. While the best general lower bound is quadratic (matching Ben-Or's result for symmetric polynomials), there was still a belief that constant depth is a weak model and we should easily prove much better bounds, for harder functions like permanent and even determinant. Still, no such progress followed for over a decade.

A surprising and influential paper by Agrawal and Vinay,[1] which they called a "chasm at depth 4" appeared in 2008. Its clear message: proving lower bounds for (even homogeneous) depth-4 circuits is as hard (or, for optimists, as useful) as proving lower bounds on general circuits. Extending the celebrated depth reduction technique of Valiant, Skyum, Berkowitz and Rackoff,[9] this paper (with subsequent improvements of Tavenas and Koiran) shows that any arithmetic circuit of size s computing a degree d polynomial can also be computed by a homogeneous depth-4 circuit of size $s^{O(\sqrt{d})}$. For example, proving a subexponential $n^{\omega(\sqrt{n})}$ lower bound for computing the permanent on $n \times n$ matrices, on such a weak constant-depth circuit would separate VP from VNP! But recall, even for depth-3 we were stuck.

While we generally know more about arithmetic circuits, their power is far from understood.

Next, a series of papers, mainly by subsets of the present authors and a few others got us extremely close to this goal! Using deep ideas and results from algebraic geometry originating from the work of Hilbert in commutative algebra, they have extended the method of partial derivatives to the much stronger "shifted partial derivatives" and combined with other ideas including very fine combinatorial analysis were able to reach the chasm, but not cross it. More precisely they proved lower bounds of $n^{\Omega(\sqrt{n})}$ or both determinant and permanent. Note that for the determinant this lower bound is tight, and changing the Ω to ω in this expression for the permanent would thus separate the two and hence separate VP from VNP.

So far for depth 4. The following paper proves that the very same chasm actually exists in depth 3, at least over fields of characteristic 0 like the rational numbers. More precisely, as above, every size s arithmetic circuit computing a polynomial of degree d can be computed by a depth-3 circuit of size $s^{O(\sqrt{d})}$ (which un-

Association for Computing Machinery

ACM Conference Proceedings Now Available via Print-on-Demand!

Did you know that you can now order many popular ACM conference proceedings via print-on-demand?

Institutions, libraries and individuals can choose from more than 100 titles on a continually updated list through Amazon, Barnes & Noble, Baker & Taylor, Ingram and NACSCORP: CHI, KDD, Multimedia, SIGIR, SIGCOMM, SIGCSE, SIGMOD/PODS, and many more.

For available titles and ordering info, visit: librarians.acm.org/pod

fortunately are not homogeneous anymore and actually have very large degrees). It is difficult to explain to non-experts why this is so unexpected, but as before it carries the same message: proving $n^{\omega(\sqrt{n})}$ lower bound for computing the permanent even on depth-3 arithmetic circuits would separate VP from VNP.

Again, for optimists, this means that we are extremely close to resolving a major goal of the field. For pessimists, this may be simply an indication of how strong are depth-3 circuits and how hopeless proving lower bounds is even for them. I am on the optimists' side. As far as we know, in the arithmetic setting we have no barriers (aka excuses) of the "natural proofs" or "relativization" varieties, which seem to explain our failure so far to prove lower bounds in the Boolean setting. Moreover, the arithmetic setting is making good on the promise of providing mathematical techniques, which may help resolve its major problems, as the line of work here indicates. Another indication, of course, the Geometric Complexity Theory (GCT) approach of Mulmuley and Sohoni,[5] which approaches the VP vs. VNP question from a different direction, based on invariant theory and representation theory. Indeed, some relations and connections between the two approaches were discovered, and the growing interests of pure mathematicians in these computational complexity questions is encouraging.

As we have grown to expect of computational complexity, there are myriad connections of this research in arithmetic complexity to other seemingly distinct subareas of the field. One important connection to pseudorandomness, in particular the intimate relationship between derandomizing the probabilistic algorithm for Polynomial Identity Testing (PIT) and arithmetic lower bounds discovered by Kabanets and Impagliazzo.[4] Subsequently, Dvir and Shpilka[2] initiated a program to understand this question for very shallow circuits, making connections to locally decodable and correctable codes on the one hand and to combinatorial geometry (mainly incidence theory) on the other. This has lead to a long sequence of papers obtaining both new lower bounds and new identity testing algorithms for larger and larger classes of low-depth and other circuit models. Yet another exciting connection was recently made by Grochow and Pitassi[3] between arithmetic complexity, PIT and proof complexity, in what will surely develop and possibly lead to lower bounds in that field.

Let me conclude with a riddle: Can depth-3 lower bounds on Boolean circuits lead to "real" lower bounds, as they do in the arithmetic setting? Yes! The positive answer in Valiant's[7] predates all of these developments. In this paper Valiant shows that any function requiring $\exp(n)$ size depth-3 Boolean circuits cannot be computed by a linear-size, logarithmic depth circuit. The state-of-art in Boolean circuit lower bounds is so pathetic that the latter remained one of its major goals since Valiant's paper, and can be achieved via strong enough depth-3 lower bounds.

On to proving real lower bounds! C

References

1. Agrawal, M. and Vinay, V. Arithmetic circuits: A chasm at depth four. In *Proceedings of the Annual Symposium on Foundations of Computer Science*. IEEE, 2008, 67–75.
2. Dvir, Z. and Shpilka, A. Locally decodable codes with two queries and polynomial identity testing for depth 3 circuits. *SIAM Journal on Computing 36*, 5 (2007), 1404–1434.
3. Grochow, J. et al. Circuit complexity, proof complexity, and polynomial identity testing. In *Proceedings of IEEE 55th Annual Symposium Foundations of Computer Science*. IEEE, 2014, 110–119.
4. Kabanets, V. and Impagliazzo, R. Identity tests means proving circuit lower bounds. *Comput. Complexity 13*, 1–2 (2004), 1–46.
5. Mulmuley, K. and Sohoni, M. Geometric complexity theory I: An approach to the *P* vs. *NP* and related problems. *SIAM J. Comput. 31*, 2 (201), 496–526.
6. Nisan, N. and Wigderson, A. Lower bounds on arithmetic circuits via partial derivatives. *Computational Complexity 6*, 3 (1996), 217–234.
7. Valiant, L.G. Graph-theoretic arguments in low-level complexity. Springer, 1977.
8. Valiant L.G. Completeness classes in algebra. In *Proceedings of the 11th Annual ACM Symposium on Theory of Computing*, (1979), 249–261.
9. Valiant. L.G., Skyum, S., Berkowitz S., and Rackoff, C. Fast parallel computation of polynomials using few processors. *SIAM Journal on Computing 12*, 4 (1983), 641–644.

Avi Wigderson is a professor in the School of Mathematics, Institute for Advanced Study, at Princeton University, Princeton, NJ.

Copyright held by author.