Cracks in the Defenses: Scouting Out Approaches on Circuit Lower Bounds

Eric Allender

Department of Computer Science, Rutgers University, Piscataway, NJ 08855,
allender@cs.rutgers.edu

Abstract. Razborov and Rudich identified an imposing barrier that stands in the way of progress toward the goal of proving superpolynomial lower bounds on circuit size. Their work on "natural proofs" applies to a large class of arguments that have been used in complexity theory, and shows that no such argument can prove that a problem requires circuits of superpolynomial size, even for some very restricted classes of circuits (under reasonable cryptographic assumptions). This barrier is so daunting, that some researchers have decided to focus their attentions elsewhere. Yet the goal of proving circuit lower bounds is of such importance, that some in the community have proposed concrete strategies for surmounting the obstacle. This lecture will discuss some of these strategies, and will dwell at length on a recent approach proposed by Michal Koucký and the author.

1 Introduction and Ancient History

More than a decade ago, the author wrote a survey of results in circuit complexity [7]. That survey is still depressingly up-to-date. Despite some interesting recent progress on circuit lower bounds (see, for example [16, 22, 40, 21, 17]), it is fairly accurate to say that only modest progress has been made in the field of circuit lower bounds since the dramatic results of the 1980s [5, 20, 42, 25, 34, 41].

Already in the mid-1990s, Razborov and Rudich identified a reason that explained this lack of progress [33]. They examined the known lower bound arguments showing that some function f is not computed by a class $\mathcal{C}$ of circuits, and showed that such arguments all implied the existence of a combinatorial property Q such that

- Q *is large*: That is, most of the Boolean functions f on n input variables have property Q.
- Q *is constructive*: That is, given a truth-table of size $N = 2^n$ representing a Boolean function t on n input variables, determining whether t has property Q takes time only polynomial in N. (The main conclusions of [33] carry over unchanged if this is weakened to time $N^{\log^{O(1)} N}$.)
- Q *is useful* for proving that f is not computed by circuits in $\mathcal{C}$, in the sense that f has property Q, but no function computed by circuits in the class $\mathcal{C}$ has property Q.

Razborov and Rudich call any such argument a *natural proof*.

Razborov and Rudich showed in [33] that if there is a secure pseudorandom function generator computable in the class $\mathcal{C}$, then there can be no natural proof showing that f

is not in $\mathcal{C}$. Since Naor and Reingold [31] show that there are pseudorandom function generators computable in TC^0 (assuming that factoring Blum integers requires circuits of size 2^{n^ϵ} for some $\epsilon > 0$) this means that, in the likely case that factoring Blum integers is hard, no natural proof can show that any function lies outside of TC^0.

2 Tried and True Techniques

Of course, we do know that there *are* some problems that lie outside of TC^0. Indeed, the only arguments currently known showing that certain functions do not lie in TC^0 make use of *diagonalization*, which was already identified by Razborov and Rudich as a "non-natural" proof technique. Usually diagonalization applies only to *uniform* complexity classes (such as the arguments of [8, 15] showing that dlogtime-uniform TC^0 is properly contained in $C_=P$ and PP). However, even non-uniform classes such as P/poly can be separated from large enough classes by means of diagonalization. Diagonalization combined with "arithmetization[1]" yields the best-known result along these lines: the result of Buhrman, Fortnow and Thierauf [14] that MA_{EXP} is not contained in P/poly (and hence is also not contained in (non-uniform) TC^0). Is there hope that these techniques might lead to better lower bounds for TC^0?

Perhaps there is hope – but it is tempered by the recognition that diagonalization and arithmetization also have severe limitations when it comes to proving circuit lower bounds. Diagonalization is the canonical example of a "relativizing" proof technique, and even when when combined with arithmetization techniques the known separation results "algebrize" (using the terminology introduced by Aaronson and Wigderson [1]). Aaronson and Wigderson show that algebrizing proof techniques are not strong enough to prove that NEXP is not in P/poly (so that the lower bound of [14] mentioned above is close to the best that can be obtained using these techniques).

It is true that this does not directly address the question of using diagonalization and arithmetization to prove lower bounds for "small" subclasses of P/poly (such as TC^0), and indeed it is debatable whether it is even relevant to talk about "relativized" or "algebrized" subclasses of P. This issue has been discussed in several papers [10, 19, 24, 23]; see also Section 9 of [1]. Thus there is (as yet) no strong argument why diagonalization and arithmetization cannot prove separations from TC^0 – but there is also scant reason for optimism that this will be a promising avenue of attack. After all, there is no evidence that these techniques can provide alternative proofs of known separations (such as the result that PARITY is not in AC^0 [5, 20, 42, 25]).

We are left to wonder what other approaches have been proposed, for obtaining circuit lower bounds.

3 The Mulmuley-Sohoni Approach

TC^0 is a class defined by Boolean circuits, but it also has appealing characterizations in terms of arithmetic circuits [2]. Specifically, TC^0 is the class of Boolean functions that can be represented as the sign of a function $\{0,1\}^n \to \mathbb{Z}$ that is computed by

[1] For more information on what terms such as "arithmetization mean, consult [1].

polynomial-size constant-depth unbounded-fan-in arithmetic circuits with $+$ and $\times$ gates, and constants from $\{0, 1, -1\}$. This class of arithmetic circuits (arithmetic AC^0 circuits) has enough restrictions so that existing lower bound techniques suffice to show that several functions cannot be computed by such circuits [2, 9] (although they do not suffice to say much about what can be represented as the *sign* of such functions.) The natural proofs framework of Razborov and Rudich is not known to extend in a direct way to *arithmetic* circuits. Might this not offer an avenue of attack?

As it turns out, there is a fairly sophisticated plan of attack that is based on (a somewhat different model of) arithmetic circuits. Mulmuley and Sohoni proposed a program for using the techniques of algebraic geometry in order to prove lower bounds on the size of arithmetic formulae computing the permanent (and eventually for addressing the P vs NP question) [30]. The question of whether their approach might circumvent the natural proofs barrier was discussed briefly by Mulmuley and Sohoni [30] and subsequently was discussed at more length by Regan [37]. Regan reaches the conclusion that the approach proposed by Mulmuley and Sohoni holds the promise of being an "un-natural" proof technique, by violating the requirement of *constructivity*. That is, it seems that the proof might give rise to a useful and large combinatorial property Q with the property that, given a truth table t determining if the function represented by t has property Q might be very complex.

3.1 Other Nonconstructive Approaches

The call for lower bound arguments that violate the "constructivity" requirement of Razborov and Rudich is echoed in the current draft of the textbook by Arora and Barak [12]. Arora and Barak describe how improved circuit lower bounds could conceivably be based on the combinatorial property Q consisting of those functions that have high discrepancy. They observe that computing the discrepancy, given the truth table of a function, is hard for coNP, and thus this is a good candidate for violating the "constructivity" condition. It also might suggest that this is too complicated a notion to hope to analyze usefully in the context of a lower bound proof – but Arora and Barak go on to give examples of elegant and understandable proofs in the literature that rely on computing values that are NP-hard to compute in general, but which yield to analysis in such a way that does not yield an efficient algorithm. Quoting from Arora and Barak:

> *This suggests we should not blindly trust the intuition that "nonconstructive $\equiv$ difficult."*

4 Lower Bounds via Derandomization

Let us turn again to the topic of arithmetic circuits. The *Identity Testing* problem is to determine, given an arithmetic circuit C, if the polynomial represented by the circuit is the identically zero polynomial. It is well known that this problem has an efficient probabilistic algorithm (see, e.g., [27, 18, 39, 43]), and thus it is a tempting target for those seeking to derandomize probabilistic algorithms. Note that there have been some very impressive successes in the last decade in the campaign to transform probabilistic algorithms to efficient deterministic algorithms [3, 38].

Unfortunately, anyone seeking to derandomize the Identity Testing problem will need to contend with the results of Kabanets and Impagliazzo [29], who showed that Identity Testing is in P only if one of the following two conditions hold:

- NEXP $\not\subseteq$ P/poly
- The Permanent does not have arithmetic circuits of polynomial size.

Conversely, sufficiently strong circuit lower bounds imply that Identity Testing can be derandomized. Thus derandomizing the Identity Testing problem is in some sense *equivalent* to proving circuit lower bounds.

There are two ways to view this state of affairs. The pessimist might conclude that derandomizing Identity Testing is hopeless. The optimist might conclude that this is *exactly* the problem to work on, in order to prove circuit lower bounds. (The optimist might take additional inspiration from the observation that it suffices to deal with arithmetic circuits that have *no input variables*; simply *evaluating* an arithmetic circuit to determine if it evaluates to zero is already as hard as the general problem [6].)

In fact, Agrawal has proposed a multi-step program to separate P from NP that proceeds by building progressively better pseudorandom generators, with the goal of proving lower bounds via derandomization [4]. Agrawal does cite the work of Razborov and Rudich, but he does not explicitly state how his program would circumvent the obstacle of Natural Proofs. I would characterize his approach to Natural Proofs as saying, in essence: "First, let's prove the lower bound, and afterward we can figure out why Natural Proofs posed no obstacle."

This is a reasonable stance to take, because, in Agrawal's own words, "In the sequence of steps proposed to prove arithmetic and Boolean circuit lower bounds, perhaps the most important one is step 1" – and step 1 in Agrawal's program does *not* seem to involve proving anything that Razborov and Rudich say should be hard to prove.

Step 1 in Agrawal's program involves improving the Nisan-Wigderson pseudorandom generator for probabilistic AC^0 circuits [32]. The Nisan-Wigderson generator shows that any problem solvable by probabilistic AC^0 circuits can be solved in time $2^{\log^{O(1)} n}$. Agrawal proposes improving the parameters, in a way that would yield a polynomial-time algorithm. As he observes, such a construction would also show that there is a problem in DTIME($2^{O(n)}$) that requires AC^0 circuits of size $2^{\epsilon n}$ for some $\epsilon > 0$. This would be a significant advance beyond what is currently known; it is not even known if there is any problem in DTIME($2^{O(n)}$) that requires *depth three* circuits of this size. Perhaps there are significant barriers that prevent us from proving such lower bounds – but there seems to be nothing in the Natural Proofs framework that explains why this should be difficult.

5 Amplifying Modest Lower Bounds

This section describes work performed jointly by Michal Koucký and the author [11].

The work of Razborov and Rudich highlights a significant obstacle to proving *superpolynomial* lower bounds – but there is nothing in their framework that prevents "natural" proofs of quadratic or cubic lower bounds. Indeed, there are examples of proofs of this sort. Håstad showed that a certain function requires formulae of size

nearly n^3 [26], and it is known that certain problems in P require branching programs of size nearly $n \log \log n$ [13]. Impagliazzo, Paturi, and Saks showed that any depth d TC^0 circuit for PARITY must have $n^{1+\Omega(1/(2.5)^d)}$ wires [28].

Thus we know of no reason why a natural proof cannot show that, say, the Boolean Formula Evaluation problem (a standard complete problem for NC^1) requires TC^0 circuits of size $n^{1.01}$.

It turns out that this would have significant consequences. It is shown in [11] that, if $NC^1 = TC^0$, then for every $\epsilon > 0$, the Boolean Formula Evaluation problem has TC^0 circuits of size $n^{1+\epsilon}$. That is, proving even a size lower bound of $n^{1.01}$ would separate TC^0 from NC^1.

The reason for this "amplification" effect is that many of the well-studied problems in NC^1 (such as the Boolean Formula Evaluation problem) have a very strong self-reducibility property. Namely, there are very efficient reductions that reduce the problem for instances of length n to instances of length n^ϵ.

How does this relate to the Natural Proofs framework? Consider the combinatorial property Q consisting of all truth-tables of n-variate Boolean functions that are *not* computed by threshold circuits of depth $\log^* n$ and size $n^{1.01}$. This property certainly satisfies the largeness criterion. It is also easy to see that, given a truth table of size $N = 2^n$, it can be determined in time $N^{O \log^{.01} N}$ whether property Q holds. Thus, although this does not seem to be recognizable in polynomial time, it certainly is recognizable in quasipolynomial time, and thus is "constructive" enough to qualify as "natural" in most of the theorems presented by Razborov and Rudich. Thus we have an example of a large and constructive combinatorial property that is useful against TC^0 circuits of size $n^{1.01}$. Yet we know of no way to conclude from this (using the machinery of [33] or using any other argumentation) that factoring Blum integers is computable by circuits of size $2^{n^{o(1)}}$ – although this *would* be the case if we had a large constructive combinatorial property Q' that is useful not only against TC^0 circuits of size $n^{1.01}$ but against TC^0 circuits of polynomial size.

Of course, we don't know that the Boolean Formula Evaluation problem satisfies this property Q. But we do know that it satisfies the strong self-reducibility property mentioned earlier, which in turn implies that it satisfies property Q only if it does not lie in TC^0. However, only a *tiny fraction* of all functions on n variables satisfy this self-reducibility property. Thus if one were able to establish that the Boolean Formula Evaluation problem satisfies property Q, we see no obvious way that this would give rise to a "large" combinatorial property useful against TC^0, and thus this could provide a way to perform an end-run around the Natural Proofs barrier.

Although this provides a rough plan of attack for separating NC^1 from TC^0, it is interesting (or frustrating) to note that it does not provide a similar plan of attack for separating TC^0 from NP or NEXP. That is, if SAT is in TC^0, we do not know how to conclude that SAT has TC^0 circuits of size $n^{1.01}$; indeed, we do not know how to find any fixed k such that SAT has TC^0 circuits of size n^k, assuming only that NP = TC^0.

5.1 Other Evidence that Lower Bounds Are Hard

There is more than one way to explain our inability to prove lower bounds in circuit complexity. Razborov [36] has shown, under cryptographic assumptions, that certain

circuit lower bounds are independent of certain theories of bounded arithmetic. (He also argues in [35] that these same theories capture the types of reasoning that have been used in lower bound arguments thus far.) It would be interesting to determine if these same logics are unable to prove that the Boolean Formula Evaluation problem requires TC^0 circuits of size $n^{1.00001}$, under similar cryptographic assumptions.

Acknowledgments

I thank Nikolay Vereshchagin and Michal Koucký for encouraging me to choose this topic for my CSR lecture. I also thank Michal Koucký for numerous discussions that have refined and clarified my view of this material, and I thank Alexander Razborov for raising some thought-provoking points. The research of the author is supported in part by NSF Grants CCF-0514155 and DMS-0652582.

References

1. Scott Aaronson and Avi Wigderson. Algebrization: A new barrier in complexity theory. In *STOC*, 2008. To appear.
2. M. Agrawal, E. Allender, and S. Datta. On TC^0, AC^0, and arithmetic circuits. *Journal of Computer and System Sciences*, 60:395–421, 2000.
3. M. Agrawal, N. Kayal, and N. Saxena. PRIMES is in P. *Annals of Mathematics*, 160:781–793, 2004.
4. Manindra Agrawal. Proving lower bounds via pseudo-random generators. In *Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS)*, volume 3821 of *Lecture Notes in Computer Science*, pages 92–105, 2005.
5. M. Ajtai. Σ^1_1-formulae on finite structures. *Annals of Pure and Applied Logic*, 24:1–48, 1983.
6. E. Allender, P. Bürgisser, Johan Kjeldgaard-Pedersen, and Peter Bro Miltersen. On the complexity of numerical analysis. In *Proc. 21st Ann. IEEE Conf. on Computational Complexity (CCC '06)*, pages 331–339, 2006.
7. Eric Allender. Circuit complexity before the dawn of the new millennium. In *Conference on Foundations of Software Technology and Theoretical Computer Science (FST&TCS)*, volume 1180 of *Lecture Notes in Computer Science*, pages 1–18, 1996.
8. Eric Allender. The permanent requires large uniform threshold circuits. *Chicago J. Theor. Comput. Sci.*, 1999.
9. Eric Allender, Andris Ambainis, David A. Mix Barrington, Samir Datta, and Huong LêThanh. Bounded depth arithmetic circuits: Counting and closure. In *International Conference on Automata, Languages, and Programming (ICALP)*, volume 1644 of *Lecture Notes in Computer Science*, pages 149–158, 1999.
10. Eric Allender and Vivek Gore. On strong separations from AC^0. In Jin-Yi Cai, editor, *Advances in Computational Complexity Theory*, volume 13 of *DIMACS Series in Discrete Mathematics and Theoretical Computer Science*, pages 21–37. AMS Press, 1993.
11. Eric Allender and Michal Koucký. Amplifying lower bounds by means of self-reducibility. In *IEEE Conference on Computational Complexity*, 2008. To appear.
12. Sanjeev Arora and Boaz Barak. Complexity theory: A modern approach. Draft currently available at http://www.cs.princeton.edu/theory/complexity/.
13. P. Beame, M. Saks, X. Sun, and E. Vee. Super-linear time-space tradeoff lower bounds for randomized computation. *Journal of the ACM*, 50:154–195, 2003.

14. Harry Buhrman, Lance Fortnow, and Thomas Thierauf. Nonrelativizing separations. In *IEEE Conference on Computational Complexity*, pages 8–12, 1998.
15. H. Caussinus, P. McKenzie, D. Thérien, and H. Vollmer. Nondeterministic NC^1 computation. *Journal of Computer and System Sciences*, 57:200–212, 1998.
16. Arkadev Chattopadhyay and Kristoffer Arnsfelt Hansen. Lower bounds for circuits with few modular and symmetric gates. In *International Conference on Automata, Languages, and Programming (ICALP)*, volume 3580 of *Lecture Notes in Computer Science*, pages 994–1005, 2005.
17. Dmitriy Cherukhin. Lower bounds of complexity for depth-2 and depth-3 Boolean circuits with arbitrary gates. In *CSR*, 2008. In these proceedings.
18. R. DeMillo and R. Lipton. A probabilistic remark on algebraic program testing. *Information Processing Letters*, 7:193–195, 1978.
19. Lance Fortnow. The role of relativization in complexity theory. *Bulletin of the EATCS*, 52:229–243, 1994.
20. M. Furst, J. Saxe, and M. Sipser. Parity, circuits, and the polynomial-time hierarchy. *Mathematical Systems Theory*, 17:13–27, 1984.
21. Frederic Green. The correlation between parity and quadratic polynomials mod 3. *J. Comput. Syst. Sci.*, 69(1):28–44, 2004.
22. Kristoffer Arnsfelt Hansen and Peter Bro Miltersen. Some meet-in-the-middle circuit lower bounds. In *Symposium on Mathematical Foundations of Computer Science (MFCS)*, volume 3153 of *Lecture Notes in Computer Science*, pages 334–345, 2004.
23. J. Hartmanis, R. Chang, S. Chari, D. Ranjan, and P. Rohatgi. Relativization: A revisionistic perspective. In G. Rozenberg and A. Salomaa, editors, *Current Trends in Theoretical Computer Science*, volume 40 of *World Scientific Series in Computer Science*, pages 537–548. World Scientific Press, 1993.
24. J. Hartmanis, R. Chang, J. Kadin, and S. Mitchell. Some observations about relativizations of space bounded computations. In G. Rozenberg and A. Salomaa, editors, *Current Trends in Theoretical Computer Science*, volume 40 of *World Scientific Series in Computer Science*, pages 423–433. World Scientific Press, 1993.
25. J. Håstad. *Computational Limitations for Small Depth Circuits*. MIT Press, Cambridge, MA, 1987.
26. Johan Håstad. The shrinkage exponent of de Morgan formulas is 2. *SIAM J. Comput.*, 27(1):48–64, 1998.
27. O.H. Ibarra and S. Moran. Equivalence of straight-line programs. *Journal of the ACM*, 30:217–228, 1983.
28. Russell Impagliazzo, Ramamohan Paturi, and Michael E. Saks. Size-depth tradeoffs for threshold circuits. *SIAM J. Comput.*, 26:693–707, 1997.
29. Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1-2):1–46, 2004.
30. Ketan Mulmuley and Milind A. Sohoni. Geometric complexity theory I: An approach to the P vs. NP and related problems. *SIAM J. Comput.*, 31(2):496–526, 2001.
31. Moni Naor and Omer Reingold. Number-theoretic constructions of efficient pseudo-random functions. *J. ACM*, 51(2):231–262, 2004.
32. N. Nisan and A. Wigderson. Hardness vs. randomness. *Journal of Computer and System Sciences*, 49:149–167, 1994.
33. A. Razborov and S. Rudich. Natural proofs. *Journal of Computer and System Sciences*, 55:24–35, 1997.
34. A. A. Razborov. Lower bounds on the size of bounded depth networks over a complete basis with logical addition. *Mathematicheskie Zametki*, 41:598–607, 1987. English translation in Mathematical Notes of the Academy of Sciences of the USSR 41:333-338, 1987.

35. A. A. Razborov. Bounded arithmetic and lower bounds. In P. Clote and J. Remmel, editors, *Feasible Mathematics II,*, volume 13 of *Progress in Computer Science and Applied Logic*, pages 344–386. Birkhäuser, 1995.
36. A. A. Razborov. Unprovability of lower bounds on circuit size in certain fragments of bounded arithmetic. *Izvestiya Math.*, 59:205–227, 1995.
37. Kenneth W. Regan. Understanding the Mulmuley-Sohoni approach to P vs. NP. *Bulletin of the EATCS*, 78:86–99, 2002.
38. O. Reingold. Undirected st-connectivity in log-space. In *IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 376–385. IEEE Computer Society Press, 2005.
39. J.T. Schwartz. Fast probabilistic algorithms for verification of polynomial identities. *Journal of the ACM*, 27:701–717, 1980.
40. Alexander A. Sherstov. Separating AC^0 from depth-2 majority circuits. In *ACM Symposium on Theory of Computing (STOC)*, pages 294–301, 2007.
41. R. Smolensky. Algebraic methods in the theory of lower bounds for Boolean circuit complexity. In *ACM Symposium on Theory of Computing (STOC)*, pages 77–82, 1987.
42. A. Yao. Separating the polynomial-time hierarchy by oracles. In *IEEE Symposium on Foundations of Computer Science (FOCS)*, pages 1–10, 1985.
43. R.E.B. Zippel. Simplification of radicals with applications to solving polynomial equations. Master's thesis, M.I.T., 1977.