Electronic Colloquium on Computational Complexity, Report No. 105 (2010)

A note on circuit lower bounds from derandomization

Scott Aaronson [*]
MIT
aaronson@csail.mit.edu

Dieter van Melkebeek[†]
University of Wisconsin-Madison
dieter@cs.wisc.edu

June 28, 2010

Abstract

We present an alternate proof of the result by Kabanets and Impagliazzo that derandomizing polynomial identity testing implies circuit lower bounds. Our proof is simpler, scales better, and yields a somewhat stronger result than the original argument.

1 Introduction

It is well-known that the standard approach for derandomizing BPP, namely via quick pseudorandom generators for circuits, requires proving superpolynomial circuit lower bounds for EXP. For the larger class of promise-BPP, Impagliazzo, Kabanets and Wigderson [IKW02] showed that *any* derandomization – using pseudorandom generators or not – implies superpolynomial circuit lower bounds for NEXP. Building on [IKW02], Kabanets and Impagliazzo [KI04] proved that *any* derandomization of BPP *proper* implies superpolynomial circuit lower bounds of some kind. More specifically, they showed that if polynomial identities over the integers can be decided deterministically (or even nondeterministically) in subexponential time, then either NEXP does not have Boolean circuits of polynomial size or else the permanent over $\mathbb{Z}$ does not have arithmetic circuits of polynomial size.

The proof in [KI04] hinges on the result from [IKW02] that NEXP $\subseteq$ P/poly $\Rightarrow$ NEXP = MA, which itself involves the use of multi-prover interactive proofs for EXP (through Nisan's result that EXP $\subseteq$ P/poly $\Rightarrow$ EXP = MA [BFNW93]), average-case to worst-case reductions for EXP (as in [BFNW93]), and the Nisan-Wigderson hardness-based pseudorandom generator construction [NW94]. Some versions of the proof also use Toda's Theorem that the polynomial-time hierarchy reduces to counting [Tod91]. We developed a number of alternate proofs that particularly avoid the most involved ingredient of the original proof, namely the result from [IKW02]. In this note

[*] This material is based upon work supported by the National Science Foundation under Grant No. 0844626. Also supported by a DARPA YFA grant and the Keck Foundation.

[†] This material is based upon work supported by the National Science Foundation under Grant No. 0728809.

ISSN 1433-8092

we present the simplest of the proofs we came up with. It does not involve any of the ingredients mentioned above and is completely elementary modulo the use of the #P-completeness of the permanent [Val79].

Apart from its simplicity and possible didactic value, our argument also yields a somewhat stronger result. It essentially gives the same lower bound for NEXP $\cap$ coNEXP as [KI04] does for NEXP. More importantly, our argument scales better than the original one. We defer the discussion of these issues until after the presentation of the original and the new argument.

2 Notation

We adopt the following notation for the rest of this note. PIT stands for "polynomial identity testing" and is formalized as the language of all arithmetic circuits that compute the zero polynomial over $\mathbb{Z}$, where arithmetic circuits consist of internal nodes representing addition, subtraction, and multiplication, and leaves representing variables and the constants 0 and 1. $\textsc{Perm}$ symbols the permanent of matrices over $\mathbb{Z}$. NSUBEXP is a shorthand for $\cap_{\epsilon>0}\mathrm{NTIME}(2^{n^\epsilon})$. For any function $s(n)$ we denote by $\mathrm{SIZE}(s(n))$ the class of languages L such that L at length n can be decided by a Boolean circuit of size $s(n)$ for all but finitely many input lengths n. We denote by $\mathrm{ASIZE}(a(n))$ the class of families $(p_n)_{n\in\mathbb{N}}$ of polynomials over $\mathbb{Z}$ where p_n has n variables and can be computed by an arithmetic circuit of size $a(n)$ for all but finitely many $n \in \mathbb{N}$.

Using the above notation we can state the result from [KI04] as follows.

Theorem 1 ([KI04]). *If* PIT $\in$ NSUBEXP *then*

(i) NEXP $\not\subseteq$ SIZE(poly(n)) *or*

(ii) $\textsc{Perm} \notin \mathrm{ASIZE}(\mathrm{poly}(n))$.

3 The Arguments

We now present the argument from [KI04] and our new argument for Theorem 1. Both arguments share a common part, which we first describe. In order to maximize the commonality, we present the argument from [KI04] slightly differently[1] than in that paper.

3.1 A Common Lemma

Lemma 1. *If* PIT $\in$ NSUBEXP *and* $\textsc{Perm} \in \mathrm{ASIZE}(\mathrm{poly}(n))$*, then* $\Sigma_2^{\mathrm{p}} \subseteq$ NSUBEXP.

The proof of Lemma 1 relies on the following claim, which shows how checking the correctness of a purported arithmetic circuit for the permanent reduces to PIT.

Claim 1. *There exists a polynomial-time algorithm that takes an arithmetic circuit C and an integer m, and produces an arithmetic circuit $\tilde{C}$ such that C computes the permanent of m-by-m matrices over $\mathbb{Z}$ iff $\tilde{C} \in$ PIT.*

[1] The difference is that [KI04] states and uses Lemma 1 for $\mathrm{P}^{\#\mathrm{P}}$ instead of Σ_2^{p}, but the rest of the argument can be adapted to work with the latter.

Claim 1 follows from viewing the Laplace expansion of the permanent as a downward self-reduction. For completeness we include a proof in the appendix.

Proof (of Lemma 1). Assuming the hypotheses of the lemma, we will show that coNP $\subseteq$ NSUBEXP, which implies that $\Sigma_2^{\mathrm{p}} \subseteq$ NSUBEXP.

For any language $L \in$ coNP there exists a function $f \in$ #P such that for any input x, $x \in L$ iff $f(x) = 0$. Valiant's proof that the permanent is #P-complete [Val79] implies that for any $f \in$ #P there exists a polynomial-time computable mapping g onto square matrices with entries in $\{-1, 0, 1, 2, 3\}$ such that $f(x) = 0$ iff $\textsc{Perm}(g(x)) = 0$. Thus, it suffices to develop an NSUBEXP-algorithm to decide whether a given m-by-m matrix M with entries in $\{-1, 0, 1, 2, 3\}$ is zero over the integers. We use the following procedure.

1. Guess a polynomial-sized candidate arithmetic circuit C for $\textsc{Perm}$ on matrices of dimension m.
2. Verify the correctness of C. Halt and reject if the test fails.
3. Use the circuit C to determine the permanent of M and accept iff the result is 0.

The circuit in step 1 exists by virtue of the hypothesis that $\textsc{Perm}$ has polynomial-size arithmetic circuits. The combination of Claim 1 and the hypothesis that PIT $\in$ NSUBEXP shows how to do step 2 in NSUBEXP. In order to execute step 3 in deterministic polynomial time, we can evaluate the arithmetic circuit C on the given input M and perform the arithmetic modulo $m!3^m + 1$. The latter quantity exceeds $\textsc{Perm}(M)$ in absolute value, so the outcome of the computation is zero iff $\textsc{Perm}(M)$ is. Overall, the above 3-step procedure correctly decides whether $\textsc{Perm}(M) = 0$ in NSUBEXP. ∎

3.2 The Original Argument

Assume by way of contradiction that the hypothesis of Theorem 1 holds but that (i) and (ii) fail. We have that

$$\text{NEXP} \subseteq \text{MA} \subseteq \text{NSUBEXP}. \tag{1}$$

The first inclusion in (1) follows from [IKW02] by our second hypothesis (NEXP $\subseteq$ SIZE(poly(n))). The second inclusion follows from Lemma 1 by our first hypothesis (PIT $\in$ NSUBEXP) and third hypothesis ($\textsc{Perm} \in$ ASIZE(poly(n))) and the fact that MA $\subseteq \Sigma_2^{\mathrm{p}}$. Combined (1) yields a contradiction to the nondeterministic time hierarchy theorem[2].

3.3 The New Argument

Assume by way of contradiction that the hypothesis of Theorem 1 holds but that (i) and (ii) fail. We have that

$$\Sigma_2^{\mathrm{p}} \subseteq \text{NE} \subseteq \text{SIZE}(n^c) \tag{2}$$

for some constant c. The first inclusion in (2) follows from Lemma 1 by our first hypothesis (PIT $\in$ NSUBEXP) and our third hypothesis ($\textsc{Perm} \in$ ASIZE(poly(n))). The second inclusion follows

[2] Alternately, since NEXP $\subseteq$ MA implies that NEXP = EXP and thus NEXP $\subseteq$ coMA, one can obtain the contradiction that NEXP $\subseteq$ coNSUBEXP, which is somewhat easier to refute than NEXP $\subseteq$ NSUBEXP.

from our second hypothesis (NEXP $\subseteq$ SIZE(poly(n))) and the fact that NE $\doteq$ NTIME($2^{O(n)}$) has a complete problem under linear-time reductions, e.g., $\{\langle M, x, t\rangle \mid M$ is a nondeterministic Turing machine that accepts x in at most t steps$\}$. All together (2) yields a contradiction to the result of Kannan's that for every fixed constant c there exists a language in Σ_2^{p} that does not have Boolean circuits of size n^c [Kan82].

4 Strenghtening and Parameterized Statement

Kannan actually showed that $\Sigma_2^{\mathrm{p}} \cap \Pi_2^{\mathrm{p}}$ (rather than Σ_2^{p}) is not in SIZE(n^c) for any constant c. Incorporating that fact into our argument leads to a strengthening that essentially[3] allows us to replace NEXP in part (i) of Theorem 1 by NEXP $\cap$ coNEXP.

Both the original and the new argument can trade the running time of the nondeterministic algorithm for PIT and the size of the arithmetic circuits for Perm in part (ii). However, due to the use of the implication NEXP $\subseteq$ SIZE(poly(n)) $\Rightarrow$ NEXP = MA from [IKW02], the original argument does not accommodate changes to either the right-hand side or the left-hand side of (i), whereas the new argument allows us to play with both sides. On the left-hand side, the proof in [IKW02] can only handle time bounds that are at least exponential.[4] This is true even when the running time of the nondeterministic algorithm for PIT is polynomial, in which case our argument only needs the time bound on the left-hand side of (i) to be superpolynomial. On the right-hand side, the proof in [IKW02] can only handle circuit sizes that are polynomial;[5] our proof gives nontrivial results for circuit sizes ranging from linear to linear-exponential.

We can further improve the parameterized version of Theorem 1 by slightly modifying our argument and incorporating Toda's Theorem [Tod91]. The strengthening and improved parameterization are captured in the following statement, which appears in the full version of [KvMS09]. We use (N $\cap$ coN)TIME(τ) as a shorthand for NTIME(τ) $\cap$ coNTIME(τ).

Theorem 2 ([KvMS09]). *Let $\gamma(n)$ denote the maximum circuit complexity of Boolean functions on n inputs. There exists a constant $c > 0$ such that the following holds for any functions $a(n)$, $s(n)$, and $t(n)$ such that $a(n)$ and $s(n)$ are constructible, $a(n)$ and $t(n)$ are monotone, and $n \leq s(n) < \gamma(n)$.*

If PIT $\in$ NTIME($t(n)$) *then*

(i) $(\mathrm{N} \cap \mathrm{coN})\mathrm{TIME}\left(t((s(n))^c \cdot a((s(n))^c))\right) \not\subseteq \mathrm{SIZE}(s(n))$, *or*

(ii) Perm $\notin$ ASIZE($a(n)$).

[3] More precisely, this modification allows us to replace NEXP by NEXP $\cap$ coNEXP under the slighly stronger hypothesis that PIT $\in$ NTIME($t(n)$) for some constructible $t(n)$ that is $O(2^{n^\epsilon})$ for every positive ϵ. Issues of uniformity make the argument somewhat tedious. For that reason and the fact that modification using Toda's Theorem (discussed next) avoids those issues as well as the need for the slightly stronger hypothesis, we do not spell out the proof.

[4] This is because of the use of the implication EXP $\subseteq$ SIZE(poly(n)) $\Rightarrow$ EXP = MA, in which we do not know whether we can replace EXP by $\mathcal{C}$ = DTIME($t(n)$) for subexponential $t(n)$, as the argument needs multiple-prover interactive proofs for $\mathcal{C}$ with honest provers computable in $\mathrm{P}^{\mathcal{C}}$.

[5] This is because the argument in [IKW02] first shows that the hypothesis implies that NEXP = EXP and then resorts to the implication EXP $\subseteq$ SIZE(poly(n)) $\Rightarrow$ EXP = MA. The first step involves cycling over all circuits of the size given by the right-hand side of the premise. This can be done in EXP only when that size is polynomial.

The instantiation of Theorem 2 to the setting of Theorem 1 yields the following statement.

Corollary 1. *If* PIT $\in$ NSUBEXP *then*

(i) NEXP $\cap$ coNEXP $\not\subseteq$ SIZE(poly(n)) *or*

(ii) Perm $\notin$ ASIZE(poly(n)).

We refer to (the full version of) [KvMS09] for the detailed analysis and formal proof of Theorem 2. Here we suffice with a sketch of the modifications to our proof of Theorem 1 and an explanation of how Toda's Theorem helps. We point out that the focus in [KvMS09] lies on so-called typically-correct derandomization. In particular, [KvMS09] shows that Theorem 1 holds even under the weaker hypothesis that for every positive ϵ there exists a nondeterminstic algorithm that runs in time 2^{n^ϵ} and decides PIT correctly on all but 2^{n^ϵ} of the inputs of length n for all but finitely many n.

The weakness of the argument without Toda's Theorem stems from the use of Kannan's result that $\Sigma_2^{\mathrm{p}} \not\subseteq \mathrm{SIZE}(n^c)$ for any constant c, a result that does not scale as well as one might hope (see [MVW99] for a discussion). The issue disappears when we go higher up in the polynomial-time hierarchy, where Kannan's argument generalizes to $\Sigma_3^{\mathrm{p}}\mathrm{TIME}((s(n))^2 \log^a s(n)) \not\subseteq \mathrm{SIZE}(s(n))$ and $\Sigma_4^{\mathrm{p}}\mathrm{TIME}(s(n) \log^a s(n)) \not\subseteq \mathrm{SIZE}(s(n))$ for some constant a and any constructible bound $s(n)$ less than the maximum circuit complexity. By Toda's Theorem there exists a constant b and a problem $A \in \#\mathrm{P}$ such that $\Sigma_4^{\mathrm{p}}\mathrm{TIME}(t(n)) \subseteq \mathrm{DTIME}^A((t(n))^b)$ for any constructible bound $t(n)$. The proof of Lemma 1 shows that its statement holds even when we replace Σ_2^{p} by $\mathrm{P}^{\#\mathrm{P}}$, and the argument scales optimally. The fact that $\mathrm{P}^{\#\mathrm{P}}$ is closed under complementation automatically leads to a simulation in $(\mathrm{N} \cap \mathrm{coN})\mathrm{TIME}(\cdot)$ in the generalization of Lemma 1. Combining all the ingredients in a similar way as in our proof of Theorem 1 yields the statement of Theorem 2.

Acknowledgements

We would like to thank Valentine Kabanets for encouraging us to write this note. DvM is grateful to Jeff Kinne and Ronen Shaltiel for helpful discussions and comments and for the related joint work in [KvMS09].

References

[BFNW93] László Babai, Lance Fortnow, Noam Nisan, and Avi Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. *Computational Complexity*, 3:307–318, 1993.

[IKW02] Russell Impagliazzo, Valentine Kabanets, and Avi Wigderson. In search of an easy witness: exponential time vs. probabilistic polynomial time. *Journal of Computer and System Sciences*, 65(4):672–694, 2002.

[Kan82] Ravi Kannan. Circuit-size lower bounds and nonreducibility to sparse sets. *Information and Control*, 55(1):40–56, 1982.

[KI04] Valentine Kabanets and Russell Impagliazzo. Derandomizing polynomial identity tests means proving circuit lower bounds. *Computational Complexity*, 13(1/2):1–46, 2004.

[KvMS09] Jeff Kinne, Dieter van Melkebeek, and Ronen Shaltiel. Pseudorandom generators and typically-correct derandomization. In *Proceedings of the International Workshop on Randomization and Computation (RANDOM)*, pages 574–587, 2009.

[MVW99] Peter Bro Miltersen, N. V. Vinodchandran, and Osamu Watanabe. Super-polynomial versus half-exponential circuit size in the exponential hierarchy. In *Proceedings of the 5th Annual International Conference on Computing and Combinatorics (COCOON)*, pages 210–220, 1999.

[NW94] Noam Nisan and Avi Wigderson. Hardness vs. randomness. *Journal of Computer and System Sciences*, 49(2):149–167, 1994.

[Tod91] Seinosuke Toda. PP is as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 20(5):865–877, 1991.

[Val79] Leslie Valiant. The complexity of computing the permanent. *Theoretical Computer Science*, 8:189–201, 1979.

Appendix

For completeness we include a proof that deciding the correctness of an arithmetic circuit for the permanent over $\mathbb{Z}$ reduces to PIT.

Proof (of Claim 1). We use the following notation. Let M be an m-by-m matrix M. For $0 \leq k \leq m$ and $1 \leq i, j \leq k$, we let $M^{(k)}$ denote the matrix obtained by taking the m-by-m identity matrix and replacing the top left k-by-k submatrix by the corresponding submatrix of M. Let $M^{(k-1)}_{-i,-j}$ denote the same for $k-1$ but starting from the matrix M with the i-th row and j-th column deleted.

We have that C correctly computes the permanent of m-by-m matrices over $\mathbb{Z}$ iff for each $1 \leq k \leq m$, the polynomial

$$\tilde{C}_k = C(X^{(k)}) - \sum_{j=1}^{k} C(X^{(k-1)}_{-k,-j}) \cdot x_{kj}$$

is identically zero, as well as the polynomial $\tilde{C}_0 = C(X^{(0)}) - 1$, where X denotes an m-by-m matrix of variables $(x_{ij})_{i,j=1}^{m}$. By introducing one more variable x_0, those conditions can be expressed equivalently as whether the following polynomial is identically zero: $\tilde{C} = \sum_{k=0}^{m} \tilde{C}_k \cdot x_0^k$. The straightforward implementation of $\tilde{C}$ given C yields an arithmetic circuit that consists of $O(m^2)$ copies of C and some simple additional circuitry. That arithmetic circuit is in PIT iff C correctly computes the permanent on m-by-m matrices over $\mathbb{Z}$. ■

ECCC ISSN 1433-8092

http://eccc.hpi-web.de