A note on the circuit complexity of PP

N. V. Vinodchandran
Department of Computer Science and Engineering
University of Nebraska-Lincoln, USA
vinod@cse.unl.edu

June 28, 2005

Abstract

In this short note we show that for any integer k, there are languages in the complexity class PP that do not have Boolean circuits of size n^k.

1 Introduction and Definitions

Proving circuit lower bounds for specific problems such as SAT is one of the most fundamental and difficult problems in complexity theory. In particular, establishing a super-linear circuit lower bound for SAT is far from being settled.

A more tractable approach is to prove circuit lower bounds for *some* language in a uniform complexity class. In the early eighties Kannan [Kan82] showed that for any integer k there are languages in $\Sigma_2^{\mathrm{p}} \cap \Pi_2^{\mathrm{p}}$ with circuit complexity n^k. Kannan used diagonalization together with the Karp-Lipton [KL80] collapse to prove his result. Recent improvements in the Karp-Lipton collapse result have improved Kannan's $\Sigma_2^{\mathrm{p}} \cap \Pi_2^{\mathrm{p}}$-bound to $\mathrm{S}_2^{\mathrm{p}}$ [Cai01], a complexity class which is contained in $\Sigma_2^{\mathrm{p}} \cap \Pi_2^{\mathrm{p}}$. Currently showing that there are languages in NP (or even MA) with super-linear circuit complexity is a significant open problem in the area. The existence of oracles relative to which NP has circuits of size $3n$ adds to the difficulty of this problem [Wil85].

In this short note we show that for any fixed k, there are languages in PP that do not have Boolean circuits of size n^k. This result is incomparable with the $\mathrm{S}_2^{\mathrm{p}}$ result since we do not know whether $\mathrm{S}_2^{\mathrm{p}}$ is contained in PP or not. Note that such a containment will require nonrelativizing techniques since there are oracles relative to which $\mathrm{S}_2^{\mathrm{p}} \not\subseteq \mathrm{PP}$ (since $\mathrm{P}^{\mathrm{NP}} \subseteq \mathrm{S}_2^{\mathrm{p}}$, an oracle due to Beigel [Bei94] which separates P^{NP} from PP also separates $\mathrm{S}_2^{\mathrm{p}}$ from PP).

While the proof of the theorem is short and simple, it does seem to require a combination of results from complexity theory.

1.1 Definitions

For standard complexity-theoretic notations and definitions including those of complexity classes such as NP and PH, refer to [Pap94, BDG88]. We next give definitions of the probabilistic and nonuniform classes that we use here. A language L is in PP if there exists a probabilistic polynomial-time machine M so that for all inputs x, x is in L if and only if M accepts x with probability $\geq \frac{1}{2}$ [Gil77].

We will use the BP operator defined by Schöning [Sch88]. For any complexity class $\mathcal{C}$, its bounded probabilistic version $\mathrm{BP} \cdot \mathcal{C}$ is defined as follows: a language $L \in \mathrm{BP} \cdot \mathcal{C}$ if there exist a polynomial p and a language $A \in \mathcal{C}$ so that for all inputs x,

$$\begin{aligned} x \in L &\Rightarrow \Pr_{y \in \{0,1\}^{p(|x|)}}[\langle x, y\rangle \in A] \geq 2/3 \\ x \notin L &\Rightarrow \Pr_{y \in \{0,1\}^{p(|x|)}}[\langle x, y\rangle \in A] \leq 1/3 \end{aligned}$$

We will also use well-known interactive complexity classes AM and MA. AM can be characterized using BP operator as $\mathrm{BP} \cdot \mathrm{NP}$. A language $L \in \mathrm{MA}$ if there exist a polynomial p and a probabilistic polynomial-time machine M such that for all inputs x,

$$\begin{aligned} x \in L &\Rightarrow \exists y \in \{0,1\}^{p(|x|)} \Pr[M(x,y) \text{ accepts}] \geq 2/3 \\ x \notin L &\Rightarrow \forall y \in \{0,1\}^{p(|x|)} \Pr[M(x,y) \text{ accepts}] \leq 1/3 \end{aligned}$$

The containment $\mathrm{MA} \subseteq \mathrm{PP}$ is known [Ver92]. By applying the BP operator to the class MA we get the class $\mathrm{BP} \cdot \mathrm{MA}$. But this class is known to be equal to AM [Bab85].

Finally we consider circuit complexity classes. For a Boolean circuit with AND, OR and NOT gates, its size is the number of gates in the circuit. Let $\mathrm{SIZE}(n^k)$ denote the class of languages accepted by Boolean circuit families of size bounded by n^k. Then $\mathrm{P/poly} = \bigcup_k \mathrm{SIZE}(n^k)$. Kannan showed that for any fixed k, $\Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}} \not\subseteq \mathrm{SIZE}(n^k)$ [Kan82].

2 Main Result

We now prove that for any k, PP has languages with circuit complexity n^k. This lower bound result is a corollary to the following theorem.

Theorem 1 *One of the following holds:*

(a) $\mathrm{PP} \not\subseteq \mathrm{P/poly}$.

(b) *For any integer k,* $\mathrm{MA} \not\subseteq \mathrm{SIZE}(n^k)$.

Proof

Suppose (a) is not true and $\mathrm{PP} \subseteq \mathrm{P/poly}$. In this case we will show that actually $\mathrm{PH} = \mathrm{MA}$. Since for any integer k, $\mathrm{PH} \not\subseteq \mathrm{SIZE}(n^k)$ [Kan82], the theorem will follow.

From [LFKN92] we know that $\mathrm{PP} \subseteq \mathrm{P/poly} \Rightarrow \mathrm{PP} \subseteq \mathrm{MA}$. From an extension of Toda's theorem for a number of counting classes including PP, we know that $\mathrm{PH} \subseteq \mathrm{BP} \cdot \mathrm{PP}$ [TO92]. Hence we have $\mathrm{PH} \subseteq \mathrm{BP} \cdot \mathrm{MA} = \mathrm{AM}$ [Bab85]. Since $\mathrm{NP} \subseteq \mathrm{PP}$, under our assumption we have $\mathrm{NP} \subseteq \mathrm{P/poly}$. From [AKSS95] we have, $\mathrm{NP} \subseteq \mathrm{P/poly} \Rightarrow \mathrm{AM} = \mathrm{MA}$. Therefore $\mathrm{PH} = \mathrm{MA}$. ■

Corollary 2 (Main Result) *For any integer k,* $\mathrm{PP} \not\subseteq \mathrm{SIZE}(n^k)$.

Proof

If $\mathrm{PP} \not\subseteq \mathrm{P/poly}$ then the result holds. Otherwise from the above theorem $\mathrm{MA} \not\subseteq \mathrm{SIZE}(n^k)$. But we know that $\mathrm{MA} \subseteq \mathrm{PP}$ [Ver92] and hence $\mathrm{PP} \not\subseteq \mathrm{SIZE}(n^k)$. ■

3 Concluding Remarks

Can we prove circuit lower bounds for other counting classes such as $\oplus$P? Since it is known that $\oplus\mathrm{P} \subseteq \mathrm{P/poly} \Rightarrow \oplus\mathrm{P} \subseteq \mathrm{MA}$ [BF91], a result identical to Theorem 1 can be proved for $\oplus$P using the same reasoning. But we do not know whether $\mathrm{MA} \subseteq \oplus\mathrm{P}$. This is an interesting open problem. We are using non-relativizing techniques in our proofs. Is our main result non-relativizing? Indeed in a very recent work Aaronson constructed an oracle relative to which PP has circuits with linear size thus showing that our result is non-relativizing [Aar05]. This gives a very strong indication that current techniques may be sufficient to prove super-linear circuit lower bound for some language in NP.

Acknowledgments

I would like to thank Peter Bro Miltersen for exciting and encouraging discussions about the result. A first version of this note was written while I was visiting Peter. I would like to thank V. Arvind for email exchanges, and A. Pavan and John Hitchcock for discussions, on the topic of this note. I would like to thank Lance Fortnow, Valentine Kabanets, Sambudha Roy, and D. Sivakumar for valuable comments on the ECCC Technical report version of this note (ECCC TR04-056). I would like to thank National Science Foundation, USA for supporting my research through the grant CCF-0430991.

References

[Aar05] S. Aaronson. Oracles are subtle but not malicious. Technical Report TR05-040, *Electronic Colloquium on Computational Complexity*, 2005. Available at `http://www.eccc.uni-trier.de/eccc/`.

[AKSS95] V. Arvind, J. Köbler, U. Schöning, and R. Schuler. If NP has polynomial-size circuits then MA=AM. *Theoretical Computer Science*, 137(2):279–282, 1995.

[Bab85] L. Babai. Trading group theory for randomness. In *Proceedings of the 17th ACM Symposium on Theory of Computing*, pages 421–429, 1985.

[BDG88] J. Balcázar, J. Díaz, and J. Gabarró. *Structural Complexity – I & II.* Springer Verlag, 1988.

[Bei94] R. Beigel. Perceptrons, PP, and the polynomial hierarchy. *Computational Complexity*, 4(4):339–349, 1994.

[BF91] L. Babai and L. Fortnow. Arithmetization: A new method in structural complexity theory. *Computational Complexity*, 1:41–66, 1991.

[Cai01] J-Y. Cai. $\mathrm{S}_2^{\mathrm{P}} \subseteq \mathrm{ZPP}^{\mathrm{NP}}$. In *Proceedings of the 42nd Annual IEEE Symposium on Foundations of Computer Science*, pages 620–629, 2001.

[Gil77] J. Gill. Computational complexity of probabilistic complexity classes. *SIAM Journal on Computing*, 6:675–695, 1977.

[Kan82] R. Kannan. Circuit-size lower bounds and non-reducibility to sparse sets. *Information and Control*, 55:40–56, 1982.

[KL80] R. Karp and R. Lipton. Some connections between uniform and non-uniform complexity classes. In *Proceedings of the 12th Annual ACM Symposium on Theory of Computing*, pages 302–309, 1980.

[LFKN92] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.

[Pap94] C. Papadimitriou. *Computational Complexity.* Addison-Wesley, 1994.

[Sch88] U. Schöning. Probabilistic complexity classes and lowness. *Journal of Computer and System Sciences*, 39:84–100, 1988.

[TO92] S. Toda and M. Ogiwara. Counting classes are at least as hard as the polynomial-time hierarchy. *SIAM Journal on Computing*, 21(2):316–328, 1992.

[Ver92] N. K. Vereshchagin. On the power of PP. In *Proceedings of the 7th IEEE Annual Conference on Structure in Complexity Theory*, pages 138–143, Boston, MA, USA, 1992.

[Wil85] C. B. Wilson. Reltivized circuit complexity. *Journal of Computer and System Sciences*, 31(2):169–181, 1985.