Electronic Colloquium on Computational Complexity, Report No. 56 (2004)

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

July 1, 2004

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 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 $\Sigma_2^p \cap \Pi_2^p$ with circuit complexity n^k. Kannan used diagonalization together with Karp-Lipton [KL80] collapse to prove his result. Recent improvements in the Karp-Lipton collapse result has improved Kannan's $\Sigma_2^p \cap \Pi_2^p$-bound [KW98, Cai01] to S_2^p; a complexity class which is contained in $\Sigma_2^p \cap \Pi_2^p$. Currently showing that there are languages in NP (or even MA) with super-linear circuit complexity is a significant open problem in the area. 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 with circuit complexity n^k. This result is incomparable with the lower bound for S_2^p since we do not know any direct relations between PP and S_2^p. While the proof of the theorem is simple and uses the standard line of argument, it does seem to require a combination of results from complexity theory. To best of our knowledge this result is not published.

1.1 Definitions

For standard complexity theoretic notations and definitions including those of complexity classes such as NP and PH, please refer to [Pap94]. Here we give definitions of probabilistic and nonuniform classes that we use in this note. A language L is in PP if there exists a probabilistic polynomial-time machine M so that for all inputs x,

$$x \in L \Leftrightarrow \Pr[M(x) \text{ accepts}] \geq \frac{1}{2}$$

ISSN 1433-8092

For any complexity class $\mathcal{C}$, we can define its bounded probabilistic version $\mathrm{BP}\cdot\mathcal{C}$ 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,

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

We will also use well-known interactive complexity classes AM and MA. AM can be defined using BP$\cdot$ 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,

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

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

Finally we consider circuit complexity classes. 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, $\mathrm{PH} \not\subseteq \mathrm{SIZE}(n^k)$, the theorem follows.

From [BFL91] 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 $\mathrm{NP} \subseteq \mathrm{PP}$, $\mathrm{NP} \subseteq \mathrm{P/poly}$. 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 $\mathrm{PP} \not\subseteq \mathrm{SIZE}(n^k)$. ■

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 for discussions, on the topic of this note.

References

[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.

[BFL91] L. Babai, L. Fortnow, and C. Lund. Nondeterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 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.

[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.

[KW98] J. Köbler and O. Watanabe. New collapse consequences of NP having small circuits. *SIAM Journal on Computing*, 28(1):311–324, 1998.

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

[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.

ECCC ISSN 1433-8092
http://www.eccc.uni-trier.de/eccc
ftp://ftp.eccc.uni-trier.de/pub/eccc
ftpmail@ftp.eccc.uni-trier.de, subject 'help eccc'