$\mathrm{AM_{exp}} \not\subseteq (\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$

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

August 27, 2003

Abstract

In this note we show that $\mathrm{AM_{exp}} \not\subseteq (\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$, where $\mathrm{AM_{exp}}$ denotes the exponential version of the class AM. Since there are oracles relative to which $\mathrm{AM_{exp}} \subseteq \mathrm{P}/\mathrm{poly}$, our result is an instance of very few nonrelativizable separation results.

Keywords: computational complexity, nonuniform computation, lower bound, relativization.

1 Introduction

Investigating the power of Turing machine based computations, in comparison with nonuniform computations, is of considerable importance in complexity theory. In particular, the question whether there are functions computable in exponential time with super polynomial circuit complexity is one of the most fundamental open problems with significant implications on other central questions in complexity theory. While it is widely believed that the answer to the above question is affirmative, researchers are yet to find a proof for it. One major bottleneck in finding a proof is that there are oracles relative to which exponential time has polynomial size circuits [Hel86]. Hence any proof should have a nonrelativizable component in it.

A fruitful approach towards the $\mathrm{EXP} - \mathrm{P}/\mathrm{poly}$ problem has been to obtain weaker upper bounds on the uniform complexity of functions which require Boolean circuits of certain size. There are a number of papers following this theme [Kan82, KW98, BFT98, MVW99]. In particular, Buhrman et. al. [BFT98] show that there are functions in $\mathrm{MA_{exp}}$ with super polynomial circuit complexity: that is $\mathrm{MA_{exp}} \not\subseteq \mathrm{P}/\mathrm{poly}$. An important aspect of the result $\mathrm{MA_{exp}} \not\subseteq \mathrm{P}/\mathrm{poly}$ is that it is nonrelativizable. Indeed, Buhrman et. al. construct an oracle under which even $\mathrm{MIP_{exp}}$ has polynomial size circuits. In fact, this is the *only* reasonable separation result known until now that is nonrelativizable. Currently, proving more nonrelativizable separation results remains one of the major challenges in complexity theory.

In this note, we separate the uniform class $\mathrm{AM_{exp}}$, the exponential version of AM, from the nonuniform nondeterministic class $(\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$. That is, we show the following theorem.

*Part of the work done while the author was with BRICS, University of Aarhus, Denmark, and later with NEC Research Institute, Princeton, NJ, USA.

Theorem 1 $\mathrm{AM_{exp}} \not\subseteq (\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$

Since $\mathrm{AM_{exp}} \subseteq \mathrm{MIP_{exp}}$, we have that relative to the oracle of Buhrman et. al., $\mathrm{AM_{exp}} \subseteq \mathrm{P/poly} \subseteq (\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$. Hence our result provides another instance of a separation result which is not relativizable.

The line of argument used in the proofs of all of the above-mentioned results is: first show, using diagonalization, a weak upper bound on functions with super polynomial circuit complexity; and then use a collapse result in order to bring down the uniform complexity of such functions. We follow similar arguments to prove our result. We first show that there are functions in Δ_4^{exp} (4^{th} level of exponential hierarchy) which are not in NP/poly. In order to improve the bound of Δ_4^{exp} to $\mathrm{AM_{exp}}$, we observe the following collapse result: if $\mathrm{EXP} \subseteq (\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$ then $\mathrm{EXP} = \mathrm{AM}$. Although this collapse result is easy to show following the techniques used for proving $\mathrm{EXP} \subseteq \mathrm{P/poly} \Rightarrow \mathrm{EXP} \subseteq \mathrm{MA}$ [BFL91], we give a proof here; partly to note the following interesting point. In order to show the collapse $\mathrm{EXP} \subseteq \mathrm{P/poly} \Rightarrow \mathrm{EXP} \subseteq \mathrm{MA}$, Babai et. al. use the powerful multi-prover interactive protocol for EXP that they develop in their paper. While it appears that the protocol for EXP is necessary for proving the above-mentioned collapse, we notice that in fact we only need the well-known LFKN-Shamir [LFKN92, Sha92] interactive protocol for PSPACE in order to prove this collapse. This is because, if $\mathrm{EXP} \subseteq \mathrm{P/poly}$ then we already know from [KL80] that $\mathrm{EXP} \subseteq \mathrm{PSPACE}$, and then we can use the interactive protocol for PSPACE in order to show the collapse. The proof we present here follows this double-collapse argument.

Recently, using derandomization, Impagliazzo et. al. [IKW01] show that if $\mathrm{NEXP} \subseteq \mathrm{P/poly}$ then $\mathrm{NEXP} = \mathrm{MA}$. Here, we also observe that the techniques of [IKW01] can be used to show that if $\mathrm{NEXP} \subseteq (\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$ then $\mathrm{NEXP} = \mathrm{AM}$.

In the next section we introduce some notations and definitions necessary for this paper. In Section 3 we prove our main separation result, and in Section 4 we prove the collapse result for NEXP.

Intermediate results that we establish to prove Theorem 1 is also independently shown by others. In particular, Theorems 4 and 8 are proved in [AK02]. Theorem 5 is shown in [KW98]. This paper studies the nonuniform class $(\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$ in relation to uniform classes above EXP. For an investigation of $(\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$ in relation to classes upto and including PSPACE, we refer the reader to Cai et. al. [CCHO03].

2 Notations and Definitions

We assume the necessary complexity theoretic notations and definitions, including the definitions of standard complexity classes such as P, NP, PSPACE, EXP, 2-EXP (double exponential time). Refer to [Pap94] for these definitions. Δ_4^{exp} denotes the class $\mathrm{EXP}^{\Sigma_3^{\mathrm{P}}}$.

Following [KL80], for any complexity class $\mathcal{C}$, the corresponding nonuniform class, denoted by $\mathcal{C}/\mathrm{poly}$ is defined as follows.

A language $L \in \mathcal{C}/\mathrm{poly}$ if there exists an interpreter language $A \in \mathcal{C}$ and a function $f : \mathbf{N} \to \Sigma^*$ (f is called the *advice*), such that $|f(n)| \leq n^k$ for some k and for all x,

$$x \in L \Leftrightarrow \langle x, f(|x|) \rangle \in A$$

We consider nonuniform classes $(\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly}$, NP/poly, and PSPACE/poly. The inclusion $(\mathrm{NP} \cap \mathrm{coNP})/\mathrm{poly} \subseteq \mathrm{NP/poly} \subseteq \mathrm{PSPACE/poly}$ holds among these classes.

A language L is defined to be in AM if there is a language $A \in \mathrm{P}$ and a polynomial p, so that for all $x \in \{0,1\}^n$,

$$x \in L \Rightarrow \Pr_{y \in \{0,1\}^{p(n)}} (\exists z \in \{0,1\}^{p(n)}\ (x,y,z) \in A) \geq \frac{2}{3}$$

$$x \notin L \Rightarrow \Pr_{y \in \{0,1\}^{p(n)}} (\exists z \in \{0,1\}^{p(n)}\ (x,y,z) \in A) \leq \frac{1}{3}$$

The exponential version of the class, denoted by $\mathrm{AM}_{\mathrm{exp}}$, can be defined analogously by allowing y and z to be of length exponential in n.

3 $\mathbf{AM_{exp}} \not\subseteq$ (NP∩coNP)/poly

For proving our main result, we first show the collapse EXP $\subseteq$ (NP $\cap$ coNP)/poly $\Rightarrow$ EXP $\subseteq$ AM. The result is proved by a double-collapse argument, namely, first a collapse of EXP to PSPACE and then to AM. The first collapse is a result from [KL80] which we state below.

Theorem 2 ([KL80]) *If* EXP $\subseteq$ PSPACE/poly *then* EXP $\subseteq$ PSPACE.

For the second collapse, we need the well-known interactive proof for PSPACE [LFKN92, Sha92]. Although it is not essential, for a more rigorous argument, it will be useful to state the PSPACE protocol in the language of PCP (Probabilistically Checkable Proofs). We refer the reader to [ALM+98] for exact definition of this notation. In this notation, we have that PSPACE $\subseteq$ PCP$(n^{O(1)}, n^{O(1)})$. It is also known that for $L \in$ PSPACE, for any instance x, the PCP-proof of the fact that $x \in L$ (or $x \notin L$) can be computed by a Turing machine using PSPACE. In addition to these, we also require the fact that the locations of the PCP-proof probed by the verifier depends only on the random bits she makes; that is the verifier does not use the contents that he previously read to compute the locations that he subsequently wishes to read. We state these facts in the following theorem.

Theorem 3 ([LFKN92, Sha92]) *For any $L \in$ PSPACE, $L \in$ PCP$(n^{O(1)}, n^{O(1)})$ such that,*

1. *The verifier makes all the random coin tosses in the beginning of the protocol and then decides on $n^{O(1)}$ locations where she is going to probe the proof.*
2. *There is a Turing machine running in polynomial space which takes as input $\langle x, i\rangle$ and outputs the ith bit of the* PCP *proof of the fact that $x \in L$ (or $x \notin L$).*

Theorem 4 *If* EXP $\subseteq$ (NP $\cap$ coNP)/poly *then* EXP $\subseteq$ AM.

Proof Since (NP $\cap$ coNP)/poly $\subseteq$ PSPACE/poly, the assumption implies that EXP $\subseteq$ PSPACE/poly. Hence, from Theorem 2 we have that actually EXP $\subseteq$ PSPACE. We now have the assumption that PSPACE $\subseteq$ (NP $\cap$ coNP)/poly. We will show that if PSPACE $\subseteq$ (NP $\cap$ coNP)/poly, then PSPACE $\subseteq$ AM.

Let $L \in$ PSPACE. Let V be the verifier for L guaranteed by Theorem 3. Let L' be the language $\{\langle x, i\rangle \| i^{th}\text{bit of the PCP proof for } x \text{ is } 1\}$. L' is in PSPACE. Also, by assumption L' is in (NP $\cap$ coNP)/poly. Let A be the language in (NP $\cap$ coNP) witnessing this, where M and $\overline{M}$ be the nondeterministic Turing machines accepting A and $\overline{A}$ respectively. For length n, let f_n be the correct advice for L'.

We will show that there is a constant round Arthur-Merlin protocol for accepting L, this will show that $L \in$ AM [Bab85, BM88]. The protocol works as follows. Merlin first sends the advice f_n to Arthur. Arthur then makes the random coin tosses and computes the queries on which he needs the entries of the proof, by simulating V. For a query $\langle x, i\rangle$, if $\langle x, i\rangle \in L'$, Merlin gives an accepting path of M and if $\langle x, i\rangle \notin L'$ Merlin gives an accepting path of $\overline{M}$. Using these Arthur can verify that the bits are indeed correct given the correct advice and the correct witnesses. Finally Arthur simulates the verifier V and accepts if and only if V accepts.

It is easy to see that this is a 3 round Arthur-Merlin protocol for L. ■

Remark 1: Instead of relying on (1) of Theorem 3 explicitly, it is possible to use the more powerful theorem PSPACE $\subseteq$ PCP$(n^{O(1)}, O(1))$ for showing the above result.

Now we can use this collapse to show the lower bound. We first note the following upper bound for languages not in NP/poly. We can use diagonalization argument similar to that in [Kan82] to get the following theorem.

Theorem 5 $\Delta_4^{\mathrm{exp}} \not\subseteq$ NP/poly

Proof We can adapt the proof given in [MVW99] for the deterministic case to actually show that there are functions in Δ_4^{exp} that has maximum *nondeterministic* circuit complexity. A nondeterministic circuit has, in addition to usual input gates, *guess* gates with fanin 0. A circuit C accepts an input x if and only if there exists a set of guess bits y, so that $C(x, y)$ outputs one. Using standard arguments, it is easy to show that nondeterministic circuits of polynomial size corresponds to NP/poly.

Consider the language $L = \{\langle 0^{2^n}, F, C\rangle | C$ is a nondeterministic circuit, F is the truth-table of a n-ary Boolean function, and $\exists x \in \{0,1\}^n$ so that $F(x) \neq C(x)\}$. It is easy to see that L is a language in $\Pi_2^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}}$. Let M be a Π_2-machine accepting L. Consider the language $L' = \{\langle 0^{2^n}, Y, s\rangle | \exists Z$ so that $YZ \in \{0,1\}^{2^n}$, YZ is the truth-table of an n-ary function with nondeterministic circuit complexity $s\}$. Using M, we can construct a Σ_3-machine M' accepting L', showing that $L' \in \Sigma_3^{\mathrm{P}}$. Now, an EXP machine on input x, can use L' to prefix search for the lexicographically first truth-table of a function f with maximum nondeterministic circuit complexity and output $f(x)$.

■

Theorem 1 $\mathrm{AM_{exp}} \not\subseteq$ (NP $\cap$ coNP)/poly

Proof Suppose EXP $\not\subseteq$ (NP $\cap$ coNP)/poly. Then, since EXP $\subseteq \mathrm{AM_{exp}}$, we are done. Otherwise EXP $\subseteq$ (NP $\cap$ coNP)/poly. Then from Theorem 1, EXP $\subseteq$ AM. By padding we have 2-EXP $\subseteq \mathrm{AM_{exp}}$. Then $\Delta_4^{\mathrm{exp}} \subseteq$ 2-EXP $\subseteq \mathrm{AM_{exp}}$. It follows from Theorem 5 that $\mathrm{AM_{exp}} \not\subseteq$ (NP $\cap$ coNP)/poly. ■

4 Collapsing NEXP if NEXP is in (NP$\cap$coNP)/poly

Recently, using derandomization [IKW01] show that if NEXP $\subseteq$ P/poly then NEXP $\subseteq$ MA. Their techniques can be used to prove that NEXP $\subseteq$ (NP $\cap$ coNP)/poly then NEXP $\subseteq$ AM.

For this section we use the following notations and definitions. NSIZE$(g(n))$ denotes the class of Boolean functions $f : \{0,1\}^n \to \{0,1\}$ having nondeterministic circuits of size at most $g(n)$. For any complexity class $\mathcal{C}$, let io-$\mathcal{C}$ denotes the class of Boolean functions f for which there is a Boolean function $f' \in \mathcal{C}$ such that $f_n = f'_n$ for infinitely many n, where f_n (respectively f'_n) denotes the restriction of f (respectively f') on $\{0,1\}^n$.

We need the following result from [IKW01].

Theorem 6 *If* NEXP $\neq$ EXP, *then for every* $\epsilon > 0$, AM $\subseteq$ io-NTIME$(2^{n^\epsilon})/n^\epsilon$.

Theorem 7 *If* NEXP $\subseteq$ (NP $\cap$ coNP)/poly, *then* NEXP = EXP.

Proof We can argue as in [IKW01]. Suppose NEXP $\subseteq$ (NP$\cap$coNP)/poly but NEXP $\neq$ EXP. Then, we have from Theorem 6 that AM $\subseteq$ io-NTIME$(2^{n^\epsilon})/n^\epsilon$. In particular, under the assumption we have AM $\subseteq$ io-NTIME$(2^n)/n$. But under the assumption, from Theorem 4, we have EXP = AM. Hence we have EXP $\subseteq$ io-NTIME$(2^n)/n$. Moreover, since NEXP $\subseteq$ (NP $\cap$ coNP)/poly, we have that NEXP $\subseteq$ NP/poly. Hence there is a fixed constant c such that io-NTIME$(2^n)/n \subseteq$ io-NSIZE(n^c). But this is a contradiction, since we can construct languages in EXP that are not in io-NSIZE(n^c) by diagonalization. ∎

Combining the above theorem with Theorem 4, we have the following.

Theorem 8 *If* NEXP $\subseteq$ (NP $\cap$ coNP)/poly, *then* NEXP = AM

5 Conclusions

We conclude this paper with a brief discussion on the difference between (NP $\cap$ coNP)/poly and NP/poly$\cap$coNP/poly. The technical difference between these two classes is the following. For a language L to be in (NP$\cap$coNP)/poly, the nondeterministic machine accepting the interpreter language should be an NP $\cap$ coNP-machine (strong nondeterministic machine [Lon82]) for all inputs. Such a restriction is not there for a language L to in NP/poly $\cap$ coNP/poly: only for the correct advice string the machine should behave like a strong machine. From the definitions it follows that (NP $\cap$ coNP)/poly $\subseteq$ NP/poly $\cap$ coNP/poly and whether the containment is proper or not is open. Since if NP = coNP these nonuniform classes coincide, separating them is at least as difficult as separating NP from coNP. Fortnow et. al. [FFKL03] constructed an oracle relative to which the containment is proper. There are alternative ways to characterize these classes. Gavaldà and Balcázar[GB91] characterize these classes as closure of certain nondeterministic reductions to sparse sets. It is also possible to characterize them using Selman's[Sel94] nondeterministic function classes[AK02].

Is $\mathrm{AM}_{\mathrm{exp}} \cap \mathrm{coAM}_{\mathrm{exp}} \not\subseteq$ NP/poly$\cap$coNP/poly? This remains an important open question. Proof of Theorem 4 will not go though for NP/poly$\cap$coNP/poly, since in this case the prover can cheat by sending a wrong advice string and the verifier will not be able to detect this.

Acknowledgments

I would like to thank Lance Fortnow for answering my questions regarding relativization, Peter Bro Miltersen and Johannes Köbler for very helpful discussions, V. Arvind for bringing [AK02] to my notice, and Lane Hemaspaandra for exchanging papers with me. I would like to thank Anna Gál and Amnon Ta-Shma for discussions which motivated me to submit the result of this note for publication. I would like to thank anonymous reviewers for helpful comments and pointers.

References

[AK02] V. Arvind and Johannes Köbler. New lowness results for ZPP(NP) and other complexity classes. *Journal of Computer and System Sciences*, 65(2):257–277, 2002.

[ALM+98] Sanjeev Arora, Carsten Lund, Rajeev Motwani, Madhu Sudan, and Mario Szegedy. Proof verification and the hardness of approximation problems. *Journal of the ACM*, 45(3):501–555, May 1998.

[Bab85] László Babai. Trading group theory for randomness. In *Proc. 17th Ann. ACM Symp. on Theory of Computing*, pages 421–429, 1985.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Nondeterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991.

[BFT98] H. Buhrman, L. Fortnow, and T. Thierauf. Nonrelativizing separations. In *Proceedings of the 13th Annual IEEE Conference on Computational Complexity*, pages 8–12, 1998.

[BM88] László Babai and Shlomo Moran. Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes. *Journal of Computer and System Sciences*, 36:254–276, 1988.

[CCHO03] J. Y. Cai, V. T. Chakaravarthy, L. A. Hemaspaandra, and M. Ogihara. Competing provers yield improved Karp-Lipton collapse results. In *Proceedings of the 20th Annual Symposium on Theoretical Aspects of Computer Science*, volume 2607 of *Lecture Notes in Computer Science*, pages 535–546, 2003.

[FFKL03] Stephen Fenner, Lance Fortnow, Stuart Kurtz, and Lide Li. An oracle builder's toolkit. *Information and Computation*, 182(2):95–136, 2003.

[GB91] Ricard Gavaldà and José Luis Balcázar. Strong and robustly strong polynomial-time reducibilities to sparce sets. *Theoretical Computer Science*, 88:1–14, 1991.

[Hel86] H. Heller. On relativized exponential and probabilistic complexity classes. *Information and Control*, 71:231–243, 1986.

[IKW01] R. Impagliazzo, V. Kabanets, and A. Wigderson. In search of an easy witness: Exponential time vs. probabilistic polynomial time. In *Proceedings of the 16th Annual IEEE Conference on Computational Complexity*, pages 2–12, 2001.

[Kan82] Ravi 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.

[LFKN92] Carsten Lund, Lance Fortnow, Howard Karloff, and Noam Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, oct 1992.

[Lon82] Tim Long. Strong nondeterministic polynomial time reducibilities. *Theoretical Computer Science*, 21:1–25, 1982.

[MVW99] P. B. Miltersen, N. V. Vinodchandran, and O. Watanabe. Super-polynomial versus half-exponential circuit size in the exponential hierarchy. In *Proceedings of 5th Annual International Conference on Computing and Combinatorics*, volume 1627 of *Lecture Notes in Computer Science*, pages 210–220, 1999.

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

[Sel94] Alan L. Selman. A taxonomy of complexity classes of functions. *Journal of Computer and System Sciences*, 48(2):357–381, 1994.

[Sha92] Adi Shamir. IP=PSPACE. *Journal of the ACM*, 39(4):869–877, 1992.