BRICS

Basic Research in Computer Science

BRICS RS-00-19 V. N. Variyam: A Note on $\mathrm{NP} \cap \mathrm{coNP}/\mathrm{poly}$

A Note on $\mathrm{NP} \cap \mathrm{coNP}/\mathrm{poly}$

Vinodchandran N. Variyam

BRICS Report Series **RS-00-19**

ISSN 0909-0878 **August 2000**

BRICS
Department of Computer Science
University of Aarhus
Ny Munkegade, building 540
DK–8000 Aarhus C
Denmark
Telephone: +45 8942 3360
Telefax: +45 8942 3255
Internet: BRICS@brics.dk

BRICS publications are in general accessible through the World Wide Web and anonymous FTP through these URLs:

`http://www.brics.dk`
`ftp://ftp.brics.dk`
This document in subdirectory `RS/00/19/`

A Note on $\mathbf{NP} \cap \mathbf{coNP}$/poly

N. V. Vinodchandran
BRICS, Department of Computer Science,
University of Aarhus, Denmark.
vinod@brics.dk

August, 2000

Abstract

In this note we show that $\mathbf{AM_{exp}} \not\subseteq \mathbf{NP} \cap \mathbf{coNP}$/poly, where $\mathbf{AM_{exp}}$ denotes the exponential version of the class $\mathbf{AM}$. The main part of the proof is a collapse of $\mathbf{EXP}$ to $\mathbf{AM}$ under the assumption that $\mathbf{EXP} \subseteq \mathbf{NP} \cap \mathbf{coNP}$/poly

1 Introduction

The issue of how powerful circuit based computation is, in comparison with Turing machine based computation has considerable importance in complexity theory. There are a large number of important open problems in this area. In particular, are there functions in $\mathbf{EXP}$ those do not have Boolean circuits of polynomial size? While it is highly likely that the answer to this question is affirmative, proving such a lower bound is considered beyond the current techniques in complexity theory. A fruitful approach towards this problem has been to obtain uniform upper bounds on the complexity of languages those do not have circuits of certain size. There are a number of papers addressing this issue, including [Kan82, KW95, BFT98, MVW99]. In particular, it is shown in [BFT98] that there are languages in $\mathbf{MA_{exp}}$ those require super polynomial circuit size; that is $\mathbf{MA_{exp}} \not\subseteq \mathbf{P}$/poly. The line of argument that is used in the proofs of these results is; first show a weaker upper bound on the languages requiring super polynomial circuits, and then use a collapse result in order to bring down the complexity of such languages.

In [BFT98], the authors use a collapse result based on certain results from interactive proof systems[BFL91].

In this note, investigating the computational power of nonuniform computations further, we show that the exponential version of **AM** (the class $\mathbf{AM}_{\mathbf{exp}}$) has languages not in $\mathbf{NP} \cap \mathbf{coNP}/\text{poly}$.

A weak upper bound of Σ_4^e (4^{th} level of exponential hierarchy) on languages not in $\mathbf{NP} \cap \mathbf{coNP}/\text{poly}$ can be proved using a counting argument along the lines of [Kan82]. In order to improve the bound of Σ_4^e to $\mathbf{AM}_{\mathbf{exp}}$, we prove the following collapse result; if $\mathbf{EXP} \subseteq \mathbf{NP} \cap \mathbf{coNP}/\text{poly}$ then $\mathbf{EXP} = \mathbf{AM}$. The technique that we use to show this result is similar to the technique of [BFL91] for showing that if $\mathbf{EXP} \subseteq \mathbf{P}/\text{poly}$ then $\mathbf{EXP} \subseteq \mathbf{MA}$. However, for the proof to work in the nondeterministic setting we need to make use of some additional property of LFKN-Shamir interactive protocol for **PSPACE**.

In order to show the collapse (if $\mathbf{EXP} \subseteq \mathbf{P}/\text{poly}$ then $\mathbf{EXP} \subseteq \mathbf{MA}$), in [BFL91], the authors use the powerful multiprover interactive protocol for **EXP** that they develop in their paper. Since the contents of the interactive proof in this protocol can be computed in **EXP**, if **EXP** is in $\mathbf{P}/\text{poly}$, Merlin can first send the polynomial advice to Arthur. Arthur can then compute the bits of the proof by himself as and when required, and simulate the verifier in the protocol for deciding the language.

While it appears that the protocol for **EXP** is necessary for proving the above-mentioned collapse, we notice that in fact one only needs the well-known LFKN-Shamir[LFKN92, Sha92] interactive protocol for **PSPACE** for showing this collapses. This is because, if $\mathbf{EXP} \subseteq \mathbf{P}/\text{poly}$ then we already know from [KL80] that $\mathbf{EXP} \subseteq \mathbf{PSPACE}$. Then one can use the interactive protocol for **PSPACE** insted of the protocol for **EXP** in order to show the collapse. We also make use of certain property of the interactive proof for **PSPACE**, that the locations of the proof probed by the verifier depends only on the random bits he/she makes. The verifier does not use the contents that he/she previously read to compute the locations that he/she subsequently wishes to read.

In the next section we introduce some notations and definitions necessary for this paper.

2 Notations and Definitions

We assume the necessary complexity theoretic notations and definitions, including the definitions of standard complexity classes like **P**, **NP**, **PSPACE**, **E**, **EXP**. Please refer to [BDG95, BDG90, Pap94] for these definitions. Σ_4^e denotes the fourth level of the exponential hierarchy.

For any complexity class $\mathcal{C}$, the corresponding nonuniform class, denoted by $\mathcal{C}$/poly is defined as follows.

A language $L \in \mathcal{C}/\text{poly}$ if there exists a 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,

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

The nonuniform classes that we consider are $\mathbf{NP} \cap \mathbf{coNP}$/poly and **PSPACE**/poly. The inclusion $\mathbf{NP} \cap \mathbf{coNP}/\text{poly} \subseteq \mathbf{PSPACE}/\text{poly}$ holds between these classes.

A language L is defined to be in **AM** if there is a language $A \in \mathbf{P}$ 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 $\mathbf{AM_{exp}}$, can be defined analogously.

3 Main Theorem

We show the main theorem. For proving this, we first show a collapse result, namely if $\mathbf{EXP} \subseteq \mathbf{NP} \cap \mathbf{coNP}/\text{poly}$, then $\mathbf{EXP} \subseteq \mathbf{AM}$. 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 1 ([KL80]) *If* $\mathbf{EXP} \subseteq \mathbf{PSPACE}/\text{poly}$ *then* $\mathbf{EXP} \subseteq \mathbf{PSPACE}$.

For the second collapse, we need the well-known interactive proof for **PSPACE** [LFKN92, Sha92]. It will be useful to state it 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 he 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 2 ([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 3 *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 1 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 2. 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 non-deterministic 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 acepting path of M and if $\langle x, i\rangle \notin L'$ Merlin gives an acepting 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: We would like to mention that insted of relying on (1) of Theorem 2 explicitly, it is possible to use the fact that **PSPACE** $\subseteq$ PCP$(n^{O(1)}, O(1))$ for showing the above result.

Now we can use this collapse to show the lower bound. The proof is very similar to the proof of the fact that $\mathbf{MA_{exp}}$ does not have polynomial circuits[BFT98]. We first note the following upper bound for languages not in $\mathbf{NP}\cap\mathbf{coNP}$/poly. We can use counting argument similar to that in [Kan82] to get the following theorem.

Theorem 4 $\Sigma_4^e \not\subseteq \mathbf{NP} \cap \mathbf{coNP}$/poly.

Theorem 5 $\mathbf{AM_{exp}} \not\subseteq \mathbf{NP} \cap \mathbf{coNP}$/poly.

Proof Suppose $\mathbf{EXP} \not\subseteq \mathbf{NP} \cap \mathbf{coNP}$/poly. Then, since $\mathbf{EXP} \subseteq \mathbf{AM_{exp}}$, we are done. Otherwise $\mathbf{EXP} \subseteq \mathbf{NP} \cap \mathbf{coNP}$/poly. Then from Theorem 5, $\mathbf{EXP} \subseteq \mathbf{AM}$. By padding we have $\mathbf{EEXP} \subseteq \mathbf{AM_{exp}}$. Then $\Sigma_4^e \subseteq \mathbf{EEXP} \subseteq \mathbf{AM_{exp}}$. It follows from Theorem 4 $\mathbf{AM_{exp}} \not\subseteq \mathbf{NP}\cap\mathbf{coNP}$/poly. ■

Acknowledgements

I would like to thank Peter Bro Miltersen and Johannes Köbler for very helpful discussions.

References

[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.

[BDG90] José Luis Balcázar, Josep Díaz, and Joaquim Gabarró. *Structural Complexity* I. Number 11 in EATCS Monographs on Theoretical Computer Science. Springer, Berlin-Heidelberg-New York, 1990.

[BDG95] José Luis Balcázar, Josep Díaz, and Joaquim Gabarró. *Structural Complexity* II. Number 22 in EATCS Monographs on Theoretical Computer Science. Springer, Berlin-Heidelberg-New York, 1995.

[BFL91] László Babai, Lance Fortnow, and Carsten Lund. Nondeterministic exponential time has two-prover interactive protocols. *Computational Complexity*, 1(1):3–40, 1991. (Preliminary version in Proc. 31st FOCS.).

[BFT98] Harry Buhrman, Lance Fortnow, and Thomas Thierauf. Nonrelativizing separations. In *Proceedings of the 13th Annual IEEE Conference on Computational Complexity (CCC-98)*, pages 8–12, Los Alamitos, June 15–18 1998. IEEE Computer Society.

[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.

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

[KL80] Richard M. Karp and Richard J. Lipton. Some connections between uniform and non-uniform complexity classes. In *Proc. 12th ACM Symp. on Theory of Computing*, pages 302–309, 1980.

[KW95] Johannes Köbler and Osamu Watanabe. New collapse consequences of NP having small circuits. *Lecture Notes in Computer Science*, 944:196–207, 1995.

[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.

[MVW99] Peter Bro Miltersen, N. V. Vinodchandran, and Osamu Watanabe. Super-polynomial versus half-exponential circuit size in the exponential hierarchy. *Lecture Notes in Computer Science*, 1627:210–220, 1999.

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

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

Recent BRICS Report Series Publications

RS-00-19 **Vinodchandran N. Variyam.** ***A Note on*** $\mathrm{NP} \cap \mathrm{coNP/poly}$**. August 2000. 7 pp.**

RS-00-18 **Federico Crazzolara and Glynn Winskel.** ***Language, Semantics, and Methods for Cryptographic Protocols*****. August 2000. ii+42 pp.**

RS-00-17 **Thomas S. Hune.** ***Modeling a Language for Embedded Systems in Timed Automata*****. August 2000. 26 pp. Earlier version entitled** ***Modelling a Real-Time Language*** **appeared in Gnesi and Latella, editors,** ***Fourth International ERCIM Workshop on Formal Methods for Industrial Critical Systems*****, FMICS '99 Proceedings of the FLoC Workshop, 1999, pages 259–282.**

RS-00-16 **Jiří Srba.** ***Complexity of Weak Bisimilarity and Regularity for BPA and BPP*****. June 2000. 20 pp. To appear in Aceto and Victor, editors,** ***Expressiveness in Concurrency: Fifth International Workshop EXPRESS '00 Proceedings*****, ENTCS, 2000.**

RS-00-15 **Daniel Damian and Olivier Danvy.** ***Syntactic Accidents in Program Analysis: On the Impact of the CPS Transformation*****. June 2000. Extended version of an article to appear in** ***Proceedings of the fifth ACM SIGPLAN International Conference on Functional Programming*****, 2000.**

RS-00-14 **Ronald Cramer, Ivan B. Damgård, and Jesper Buus Nielsen.** ***Multiparty Computation from Threshold Homomorphic Encryption*****. June 2000. ii+38 pp.**

RS-00-13 **Ondřej Klíma and Jiří Srba.** ***Matching Modulo Associativity and Idempotency is NP-Complete*****. June 2000. 19 pp. To appear in** ***Mathematical Foundations of Computer Science: 25th International Symposium*****, MFCS '00 Proceedings, LNCS, 2000.**

RS-00-12 **Ulrich Kohlenbach.** ***Intuitionistic Choice and Restricted Classical Logic*****. May 2000. 9 pp.**

RS-00-11 **Jakob Pagter.** ***On Ajtai's Lower Bound Technique for*** R***-way Branching Programs and the Hamming Distance Problem*****. May 2000. 18 pp.**

RS-00-10 **Stefan Dantchev and Søren Riis.** ***A Tough Nut for Tree Resolution*****. May 2000. 13 pp.**