If NP has Polynomial-Size Circuits, then MA = AM

Vikraman Arvind[a], Johannes Köbler[b], Uwe Schöning[b], Rainer Schuler[b]

[a] *The Institute of Mathematical Sciences, Taramani, Madras 600 113, India*

[b] *Abteilung Theoretische Informatik, Universität Ulm, 89069 Ulm, Germany*

Abstract

It is shown that the assumption of NP having polynomial-size circuits implies (apart from a collapse of the polynomial-time hierarchy as shown by Karp and Lipton) that the classes AM and MA of Babai's Arthur-Merlin hierarchy coincide. This means that also a certain inner collapse of the remaining classes of the polynomial-time hierarchy occurs.

It is well known [KL80] that the assumption of NP having polynomial-size circuits (in symbols $\mathrm{NP} \subseteq \mathrm{P/poly}$) implies that the polynomial-time hierarchy collapses to level two (in symbols $\mathrm{PH} = \Sigma_2^\mathrm{P} = \Pi_2^\mathrm{P}$). The textbooks [BDG, KST93, BC93, Pa94] can be consulted for the basic notations and results.

Furthermore, this collapse level was shown to be optimal, up to relativization, in [He86]. There it is shown that under a suitable oracle, the collapse cannot go down to the next lower level of the polynomial-time hierarchy, $\Delta_2^\mathrm{P} = \mathrm{P}^{\mathrm{NP}}$.

What we show here is, under the same assumption, an additional "inner collapse", namely of the two classes AM and MA which are not known to be equal to each other, and which are not known to be equal to Σ_2^P. Figure 1 shows the known inclusion structure of the classes in the polynomial-time hierarchy, whereas Figure 2 shows these inclusions under the assumption $\mathrm{NP} \subseteq \mathrm{P/poly}$. The proof is not difficult and just a combination of known techniques, but the result as such has not been observed before, and we think it has some significance.

In both figures the relative position of the classes $\mathrm{NP}^{\mathrm{BPP}}$ and $\mathrm{BPP}^{\mathrm{NP}}$ is also outlined. By [La83, Si83] (used in a relativized version) $\mathrm{BPP}^{\mathrm{NP}}$ is included in the class $(\Sigma_2^\mathrm{P} \cap \Pi_2^\mathrm{P})^{\mathrm{NP}} = \Sigma_3^\mathrm{P} \cap \Pi_3^\mathrm{P}$. By the fact that $\mathrm{PH} = \Sigma_2^\mathrm{P} = \Pi_2^\mathrm{P}$ holds under the assumption $\mathrm{NP} \subseteq \mathrm{P/poly}$, the class $\mathrm{BPP}^{\mathrm{NP}}$ is a subset of $\Sigma_2^\mathrm{P} = \Pi_2^\mathrm{P}$ in Figure 2. It is still open whether the classes $\mathrm{NP}^{\mathrm{BPP}}$ and $\mathrm{BPP}^{\mathrm{NP}}$ are also affected by the collapse.

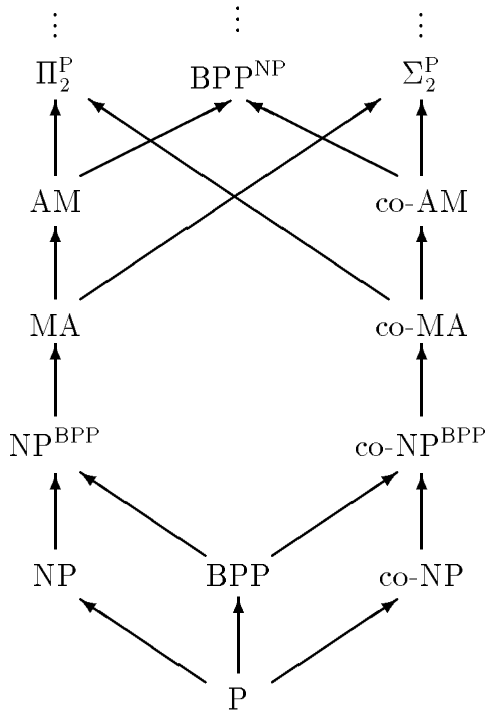

Figure 1: Classes of the polynomial-time and the Arthur-Merlin hierarchy.

The classes MA and AM have been introduced in [BM88] as classes of the "Arthur-Merlin" hierarchy. Their definition can be stated as follows. A set A is in MA if there is a predicate $B \in \mathrm{P}$ such that for all strings x the following holds:

$$x \in A \;\Rightarrow\; \exists y\, Pr[\, \langle x, y, z\rangle \in B\,] > 3/4,$$
$$x \notin A \;\Rightarrow\; \forall y\, Pr[\, \langle x, y, z\rangle \in B\,] < 1/4.$$

A set A is in AM if there is a predicate $B \in \mathrm{P}$ such that for all strings x the following holds:

$$x \in A \;\Rightarrow\; Pr[\, \exists y\, \langle x, y, z\rangle \in B\,] > 3/4,$$
$$x \notin A \;\Rightarrow\; Pr[\, \exists y\, \langle x, y, z\rangle \in B\,] < 1/4.$$

In both definitions all strings y, z are of some polynomial length in $|x|$, say $p(|x|)$, where z is chosen uniformly at random from all the strings of that length. The following inclusion relations are known: $\mathrm{NP}^{\mathrm{BPP}} \subseteq \mathrm{MA} \subseteq \mathrm{AM} \subseteq \Pi_2^{\mathrm{P}}$, and $\mathrm{MA} \subseteq \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}}$ [BM88]. Figure 1 contains all known inclusions.

As preparation to the forthcoming proof, we observe (as in [Ho81]) that any (non-uniform) family of circuits for the NP-complete set SAT can be converted into a new (non-uniform) circuit family in which the circuits are still polynomial in their input

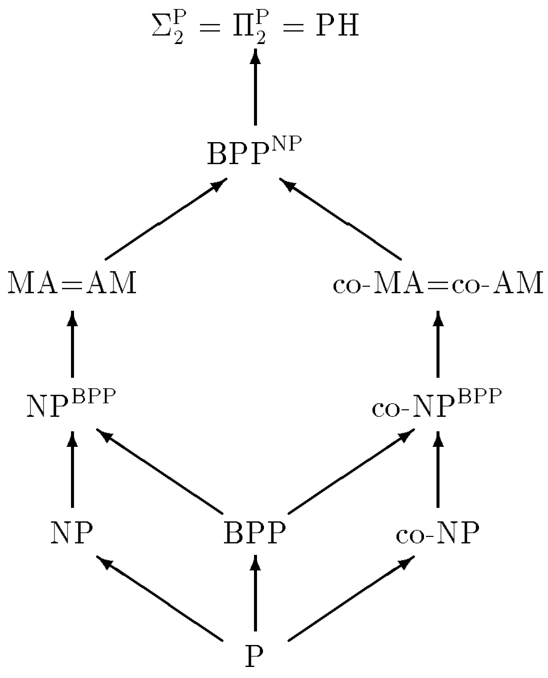

Figure 2: The classes under the assumption NP $\subseteq$ P/poly.

size, and not only output a binary value depending on whether the input formula F is satisfiable, but also output a "witness" for satisfiability, i.e. a satisfying assignment (if one exists). Such witness-constructing circuits can be obtained via the self-reducibility of SAT by building a cascade of several original circuits, as illustrated in Figure 3. The triangles indicate original circuits with binary output, whereas the boxes indicate a circuit that transforms (the binary encoding of) $F = F(x_1, \ldots, x_n)$, where the x_i are Boolean variables, into (the encoding of) $F(a_1, \ldots, a_k, x_{k+1}, \ldots, x_n)$. The binary values $a_i, \ldots, a_k$ are given by the side inputs.

Theorem. If NP has polynomial-size circuits (i.e. NP $\subseteq$ P/poly), then MA = AM.

Proof: The assumption implies that SAT has polynomial-size circuits, and by the above discussion, SAT has polynomial-size witness-constructing circuits. Let A be a set in AM, i.e. there is a predicate $B \in \mathrm{P}$ such that for all strings x the following holds:

$$x \in A \;\Rightarrow\; Pr[\,\exists y\ \langle x, y, z\rangle \in B\,] > 3/4,$$

$$x \notin A \;\Rightarrow\; Pr[\,\exists y\ \langle x, y, z\rangle \in B\,] < 1/4.$$

The set

$$C = \{\langle x, z\rangle \mid \exists y\ \langle x, y, z\rangle \in B\}$$

is in NP. Therefore it is reducible to SAT, say with some reduction function f. We can

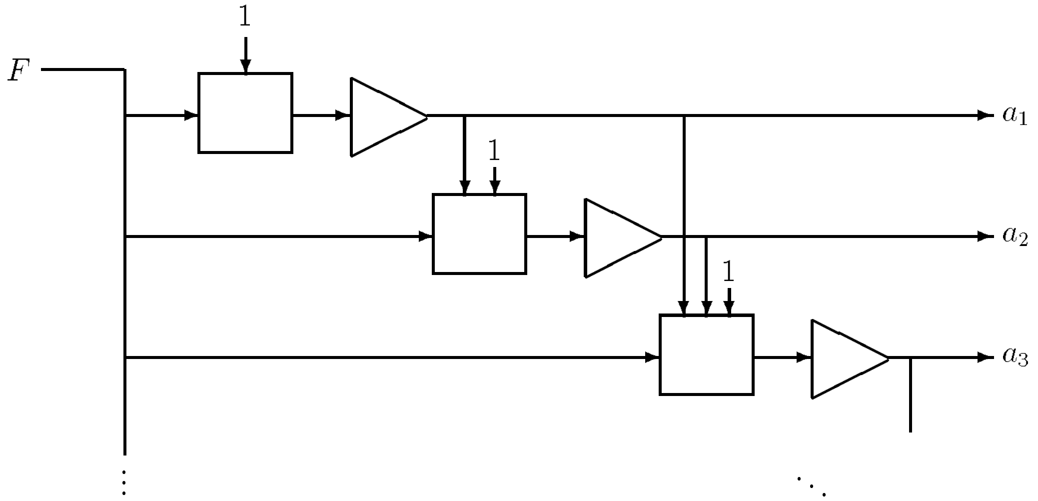

Figure 3: A witness-constructing circuit for SAT.

restate the above characterization of A as

$$x \in A \Rightarrow Pr[\ f(\langle x, z\rangle) \in \mathrm{SAT}\ ] > 3/4,$$

$$x \notin A \Rightarrow Pr[\ f(\langle x, z\rangle) \in \mathrm{SAT}\ ] < 1/4.$$

Here z is chosen uniformly at random over strings of length $p(n)$. Finally, this can be rewritten as follows where $\mathrm{OK}(F, a)$ is the polynomial-time predicate that is true if and only if a is a satisfying assignment for F.

$$x \in A \Rightarrow \exists \text{ circuit } c: \ Pr[\ \mathrm{OK}(f(\langle x, z\rangle),\ c(f(\langle x, z\rangle)))\ ] > 3/4,$$

$$x \notin A \Rightarrow \forall \text{ circuits } c: \ Pr[\ \mathrm{OK}(f(\langle x, z\rangle),\ c(f(\langle x, z\rangle)))\ ] < 1/4.$$

Here the quantifiers range over circuits of suitable polynomial size. This proves that A is in MA. □

This proof is similar in spirit to the one used in [BFNW93] to show that EXPTIME $\subseteq$ P/poly implies EXPTIME $\subseteq$ MA, and also similar to the one in [LT93, KST93] used to prove that if graph isomorphism were in P/poly, then its complement is in MA.

Note added in proof: As O. Watanabe pointed out to us, it can be shown, using techniques from (Bshouty, Cleve, Kannan, and Tamon: Oracles and queries that are sufficient for exact learning; COLT'94), that NP $\subseteq$ P/poly implies a collapse of PH to ZPP(NP).

References

[BFNW93] L. Babai, L. Fortnow, N. Nisan, A. Wigderson. BPP has subexponential time simulations unless EXPTIME has publishable proofs. Computational

Complexity **3** (1993) 307–318.

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

[BDG] J.L. Balcázar, J. Díaz, J. Gabarró. *Structural Complexity Theory I + II.* (Springer, Berlin, 1988, 1990).

[BC93] D.P. Bovet, P. Crescenzi. *Introduction to the Theory of Complexity.* (Prentice-Hall, Englewood Cliffs, NJ, 1993).

[He86] H. Heller. On relativized exponential and probabilistic complexity classes. *Information and Control* **71** (1986) 231–243.

[Ho81] J.E. Hopcroft. Recent directions in algorithmic research. *Proc. Theoretical Computer Science*, Lecture Notes in Computer Science, vol. 104 (Springer, Berlin, 1981) 123–134.

[KL80] R.M. Karp, R.J. Lipton. Some connections between nonuniform and uniform complexity classes. *Proc. 12th ACM Symp. Theory of Computer Science*, (1980) 302–309. Also: Turing machines that take advice. In: *Logic and Algorithmic*, Monographie No. 30 de l'Enseignement Mathematique, Université de Genève (1982) 255–274.

[KST93] J. Köbler, U. Schöning, J. Torán. *The Graph Isomorphism Problem: Its Structural Complexity.* (Birkhäuser, Boston, 1993).

[La83] C. Lautemann. BPP and the polynomial hierarchy. *Information Processing Letters* **14** (1983) 215–217.

[LT93] A. Lozano, J. Torán. On the non-uniform complexity of the graph isomorphism problem. In *Complexity Theory, Current Research*, Cambridge University Press (1993) 245–273.

[Pa94] C.H. Papadimitriou. *Computational Complexity* (Addison-Wesley, Reading, MA, 1994).

[Si83] M. Sipser. A complexity theoretic approach to randomness. *Proc. 15th ACM Symp. Theory of Computer Science* (1983) 330–335.