On the Power of Probabilistic Polynomial Time: (extended Abstract)

Richard Beigel
Lane A. Hemachandra
and
Gerd Wechsung

Department of Computer Science
Johns Hopkins University
Baltimore, MD 21218

June, 1989
Report JHU-89/07
On the Power of Probabilistic Polynomial Time:
\( \mathsf{P}^{\mathsf{NP}[\log]} \subseteq \mathsf{PP} \)
(Extended Abstract)

Richard Beigel \(^{*}\)  Lane A. Hemachandra \(^{†}\)  Gerd Wechsung \(^{†}\)

Abstract

We show that probabilistic polynomial time is closed under polynomial-time parity reductions. Therefore every set polynomial-time truth-table reducible to SAT (every set in the \( \Theta^p_2 \) level of the polynomial hierarchy) is accepted by a probabilistic polynomial-time Turing machine. Equivalently, \( \mathsf{P}^{\mathsf{NP}[\log]} \subseteq \mathsf{PP} \).

1 Main Results

Comparing the power of various computational paradigms is a core concern of computational complexity theory. In this paper, we study which classes in the polynomial hierarchy are contained in probabilistic polynomial time, \( \mathsf{PP} \).

Near the bottom of the polynomial hierarchy sits \( \mathsf{P}^{\mathsf{NP}[\log]} \), the class of languages accepted by polynomial-time Turing machines allowed \( O(\log n) \) calls to an NP oracle, which was first studied by Papadimitriou and Zachos in [PZ83]. Recently, the class has taken on new importance. The class \( \mathsf{P}^{\mathsf{NP}[\log]} \) defines the \( \Theta^p_2 \) level of Wagner’s refined polynomial hierarchy, has natural complete sets [Kre88, KSW86, Kad87, Wag87a], is equal to the class of sets polynomial-time truth-table reducible to SAT [Hem87, Wag87b, BH88], and is the level to which the polynomial hierarchy collapses under the assumption that \( \mathsf{NP} \) has sparse Turing-complete sets [Kad87].

In [Gil77], Gill showed that \( \mathsf{NP} \) is contained in \( \mathsf{PP} \). In [Rus85], Russo showed that the class \( \mathsf{PP} \) is closed under symmetric difference. Using this observation, Papadimitriou and Yannakakis [PY84] showed that \( \mathsf{DP} \subseteq \mathsf{PP} \), and Balcazar, Diaz, and Gabarro [BDG88] showed that the entire Boolean hierarchy is contained in \( \mathsf{PP} \).\(^1\)

In this paper we extend Russo’s approach, by showing that \( \mathsf{PP} \) is closed under polynomial-time truth-table reductions in which the truth-table implements the parity operation. This yields the corollary that \( \mathsf{P}^{\mathsf{NP}[\log]} \subseteq \mathsf{PP} \).

Definition 1 A set \( A \) is polynomial-time parity reducible to \( B \) (denoted \( A \leq^p_{\text{parity}} B \)) if \( A \leq^p_{\text{tt}} B \) via a truth-table that tests whether an odd number of its inputs belong to \( B \).

Theorem 2 \( \mathsf{PP} \) is closed under \( \leq^p_{\text{parity}} \) reductions.

Proof: Suppose that \( B \in \mathsf{PP} \) via Turing machine \( N \), and that \( A \leq^p_{\text{parity}} B \). We define a machine \( N' \) accepting \( A \) that behaves as follows on input \( x \).

i. Simulate the \( \leq^p_{\text{parity}} \)-reduction from \( A \) to \( B \), until it produces a list of strings \( x_1, \ldots, x_k \) such that \( x \in A \) if and only if an odd number of those strings belong to \( B \).

ii. Guess paths \( \rho_1, \ldots, \rho_k \) of machine \( N \). (This is possible because \( k \) is bounded by a polynomial in \( |x| \).)

iii. Compute the number of strings \( x \) such that \( \rho_i \) is an accepting path of machine \( N \) on input \( x \). Accept if that number is odd.

Though \( N' \) is defined in a most naive fashion, it nonetheless accepts the language \( A \). We proceed to prove this claim. By standard techniques [Gil77], we may assume that \( N \) accepts if more than one-half of

\(^1\)This improved on a result by Papadimitriou and Zachos, who showed that the Boolean hierarchy is contained in \( \mathsf{P}^{\mathsf{NP}[1]} \) [PZ83].

*Department of Computer Science, The Johns Hopkins University, Baltimore, MD 21218 USA. Research supported by NSF grant CCR-8808949.

†Department of Computer Science, University of Rochester, Rochester, NY 14627 USA. Research supported by NSF grant CCR-8809174 and a Hewlett-Packard Corporation equipment grant. This author performed some of this research while at Columbia University and while visiting Jen.

‡Sektion Mathematik, Friedrich-Schiller-Universität, Jena, German Democratic Republic.
its paths accept, and that \( N \) rejects if less than one-half of its paths accept. Let \( r_i = \frac{1}{2}(1 - p_i) \) denote the probability that a path of \( N \) accepts input \( x_i \). We define an operation on real numbers as follows

\[
r_1 \circ r_2 = r_1(1 - r_2) + r_2(1 - r_1).
\]

Note that \( r_1 \circ r_2 \) is the probability that exactly one of two randomly chosen paths \( p_1, p_2 \) of machine \( N \) accepts its input string \( x \). It is easily verified that

\[
\frac{1}{2}(1 - p_1) \circ \frac{1}{2}(1 - p_2) = \frac{1}{2}(1 - p_1 p_2).
\]

Hence \( \circ \) is isomorphic to real multiplication, and a simple induction shows that

\[
\frac{1}{2}(1 - p_1) \circ \cdots \circ \frac{1}{2}(1 - p_k) = \frac{1}{2}(1 - p_1 \cdots p_k).
\]

Moreover, that is the probability that a path of \( N \) accepts \( x \). Thus \( N \) accepts \( x \) if and only if an odd number of the real numbers \( p_i \) are negative. Equivalently, \( N \) accepts \( x \) if and only if an odd number of the probabilities \( r_i \) are greater than one-half. In other words \( N \) accepts \( x \) if and only if an odd number of the strings \( x_1, \ldots, x_k \) are accepted by \( N \). Thus \( N \) accepts the language \( A \).

Klaus Wagner has reported a clever proof of Corollary 3 (personal communication). That result can also be obtained as corollary to work by Toda [Tod88].

The results in this paper, [Tod88], and [Gil77] relativize, as do the results of Köbler, Schöning, Toda, and Torán[KSTTT9]. Therefore, Hoene has noted that \( \text{PP} \) contains \( \text{NP} \)-hardness.

\[
\{ A : (\exists B \in \text{P}^{\text{NP}^\text{Hierarchies}})[A \leq^p_{\text{parity}} B] \},
\]

and in particular \( \text{PP} \) contains \( \text{NP}^{\text{P}^\text{Hard}} \).

Acknowledgements

For helpful conversations we are very grateful to Gerhard Buntrock, Mike Fischer, Zvi Galil, Albrecht Hoene, and Dirk Siefkes.

References


[KSTTT9] Johannes Köbler, Uwe Schöning, Seinosuke Tada, and Jacobo Torán. Turing machines with few accepting computations and low sets for \( \text{PP} \).


