[Gup90] S. Gupta. A note on the counting hierarchy. Technical Report OSU-CISRC-8/90-TR24, The Ohio State University, Col, OH, August 1990.

[Gup91] S. Gupta. The power of witness reduction. In *Proceedings of 6th Annual Structure in Complexity Theory Conference*, pages 43–59. IEEE Computer Society Press, 1991.

[Sch89] U. Schöning. Probabilistic complexity classes and lowness. *Journal of Computer and System Sciences*, 480:238–250, 1989.

[Tar91] J. Tarui. Randomized polynomials, threshold circuits, and the polynomial hierarchy. In *Proceedings of Symposium on Theoretical Aspects of Computer Science*, 1991.

[TO90] S. Toda and M. Ogiwara. Counting classes are at least as hard as the the polynomial-time hierarchy. In *Proceedings of 6th Structure in Complexity Theory Conference*, pages 2–12. IEEE Computer Society Press, 1990.

[Tor88] J. Torán. An oracle characterization of the counting hierarchy. In *Proceedings of 3rd Structure in Complexity Theory Conference*, pages 213–223. IEEE Computer Society Press, 1988.

[ZH86] S. Zachos and H. Heller. A decisive characterization of BPP. *Information and Control*, 69:125–135, 1986.

2. It is easy to see that $(\exists^+/\forall)\mathrm{C}_=\mathrm{P} \subseteq (\exists^+\forall/\forall\exists^+)\mathrm{C}_=\mathrm{P}$. Now, let $L \in (\exists^+\forall/\forall\exists^+)\mathrm{C}_=\mathrm{P}$. Then there exists polynomials p_1 and p_2 and a set $A \in \mathrm{C}_=\mathrm{P}$ such that $x \in L \Rightarrow \exists^+ y \forall z \langle x, y, z\rangle \in A$ and $x \notin L \Rightarrow \forall y \exists^+ z \langle x, y, z\rangle \notin A$, where $|y| = p_1(|x|)$ and $|z| = p_2(|x|)$. As $A \in \mathrm{C}_=\mathrm{P}$ there exists $f \in \mathcal{Z}\#\mathrm{P}$ such that $\langle x, y, z\rangle \in A \Leftrightarrow f(\langle x, y, z\rangle) = 0$. Define g as follows: $g(\langle x, y\rangle) = \sum_{z,|z|=p_2(|x|)} f^2(\langle x, y, z\rangle)$. Then $g \in \mathcal{Z}\#\mathrm{P}$ as the machine for g guesses z and runs the machine for f on each of the guesses. Define a set $B \in \mathcal{Z}\mathrm{C}_=\mathrm{P}$ as follows: $\langle x, y\rangle \in B \Leftrightarrow g(\langle x, y\rangle) = 0$. Thus, $x \in L \Rightarrow \exists^+ y, |y| = p_1(|x|)\langle x, y\rangle \in B$ and $x \notin L \Rightarrow \forall y, |y| = p_1(|x|)\langle x, y\rangle \notin B$ proving that $L \in (\exists^+/\forall)\mathrm{C}_=\mathrm{P} = \mathrm{RP} \cdot \mathrm{C}_=\mathrm{P}$.

□

Corollary 3.5

1. $\widehat{\mathrm{BP}} \cdot \mathrm{C}_=\mathrm{P} = \mathrm{RP} \cdot \mathrm{C}_=\mathrm{P}$.
2. $\widehat{\mathrm{BP}} \cdot \mathrm{C}_=\mathrm{P} \cap \text{co-}(\widehat{\mathrm{BP}} \cdot \mathrm{C}_=\mathrm{P}) = \mathrm{ZP} \cdot \mathrm{C}_=\mathrm{P}$.

Now we show that Toda and Ogiwara's result, that $\mathrm{PH} \subseteq \widehat{\mathrm{BP}} \cdot \mathrm{C}_=\mathrm{P}$, implies that $\mathrm{PH} \subseteq \mathrm{ZP} \cdot \mathrm{C}_=\mathrm{P}$.

Proposition 3.6 $\mathrm{PH} \subseteq \mathrm{ZP} \cdot \mathrm{C}_=\mathrm{P}$, *with arbitrarily low error probability.*

Proof. $\mathrm{PH} \subseteq \widehat{\mathrm{BP}} \cdot \mathrm{C}_=\mathrm{P}$ implies that $\mathrm{PH} \subseteq \text{co-}(\widehat{\mathrm{BP}} \cdot \mathrm{C}_=\mathrm{P})$. Thus, $\mathrm{PH} \subseteq \widehat{\mathrm{BP}} \cdot \mathrm{C}_=\mathrm{P} \cap \text{co-}\widehat{\mathrm{BP}} \cdot \mathrm{C}_=\mathrm{P} = \mathrm{ZP} \cdot \mathrm{C}_=\mathrm{P}$. As $\mathrm{C}_=\mathrm{P}$ is closed under AND and OR reductions, therefore by Proposition 2.8 the error probability can be made arbitrarily small. □

Open Questions: The important question whether PH is contained in PP still remains open. Of course, $\mathrm{PH} \subseteq \mathrm{ZP} \cdot \mathrm{PP}$ as $\mathrm{C}_=\mathrm{P} \subseteq \mathrm{PP}$.

Acknowledgment: I am extremely grateful to Professor T.J. Long for his constant support and encouragement without which this paper could never have been written.

References

[BRS90] R. Beigel, N. Reingold, and D. Spielman. PP is closed under intersection. Technical Report YALEU/DOS/TR-803, Yale University, Department of Computer Science, New Haven, CT, 1990.

Define $B = \{\langle x, u_1, \ldots, u_{p(|x|)}, v\rangle \mid |u_1| = \ldots = |u_{p(|x|)}| = |v| = p(|x|), \wedge_{i=1}^{p(|x|)}\langle x, u_i \oplus v\rangle \in A\}$. As K is closed under AND reduction, therefore $B \in K$. Using Lemma 3.1 it is easy to see that $x \in L \Rightarrow \forall u_1, \ldots, u_{p(|x|)} \exists^+ v \langle x, u_1, \ldots, u_{p(|x|)}, v\rangle \in B$ and $x \notin L \Rightarrow \exists^+ u_1, \ldots, u_{p(|x|)} \forall v \langle x, u_1, \ldots, u_{p(|x|)}, v\rangle \notin B$; that is, $L \in (\forall\exists^+/\exists^+\forall)K$.

3. The proof of Part 3 is similar to Part 2.

□

Note that closure under MAJORITY reduction implies closure under OR and AND reductions. Furthermore, if a class K is closed under MAJORITY reduction then $\widehat{\mathrm{BP}} \cdot K = \mathrm{BP} \cdot K$. This immediatly gives the following corollary to Theorem 3.2.

Corollary 3.3 *If K is closed under* MAJORITY *reduction then* $\widehat{\mathrm{BP}} \cdot K = (\exists^+\forall/\forall\exists^+)K = (\forall\exists^+/\exists^+\forall)K = \mathrm{BP} \cdot K$.

We will apply Theorem 3.2 to the class C$_=$P to show that $\widehat{\mathrm{BP}} \cdot \mathrm{C}_=\mathrm{P} = \mathrm{RP} \cdot \mathrm{C}_=\mathrm{P}$. First, we need the following proposition.

Proposition 3.4

1. C$_=$P *is closed under* AND *reduction and* OR *reduction.*

2. $(\exists^+\forall/\forall\exists^+)\mathrm{C}_=\mathrm{P} = (\exists^+/\forall)\mathrm{C}_=\mathrm{P}$.

Note: $(\exists^+/\forall)\mathrm{C}_=\mathrm{P} = \mathrm{RP} \cdot \mathrm{C}_=\mathrm{P}$.

Proof.

1. Let $A \leq^P_{AND} B$, where $B \in \mathrm{C}_=\mathrm{P}$ by a function $f \in \mathrm{PF}$. Then, $x \in A \Leftrightarrow \wedge_{i=1}^n y_i \in B$, where $f(x) = \langle y_1, \ldots, y_n\rangle$ for some n. As $B \in \mathrm{C}_=\mathrm{P} = \mathcal{Z}\mathrm{C}_=\mathrm{P}$[Gup91], there exists a function $g \in \mathcal{Z}\#\mathrm{P}$ such that $x \in B \Leftrightarrow g(x) = 0$. Let $h(x) = g^2(y_1) + \ldots + g^2(y_n)$, where $f(x) = \langle y_1, \ldots, y_n\rangle$ for some n. Using the constructions given implicitly in [BRS90] and explicitly in [Gup90], $h \in \mathcal{Z}\#\mathrm{P}$. Therefore, $x \in A \Leftrightarrow h(x) = 0$ and $A \in \mathcal{Z}\mathrm{C}_=\mathrm{P} = \mathrm{C}_=\mathrm{P}$. This shows that C$_=$P is closed under AND reduction.

   Similarly, letting $h(x) = \prod_{i=1}^n g(y_i)$ we can show that C$_=$P is closed under OR reduction.

1. Suppose not. Then, there exists $u_1, u_2, \ldots, u_m$ such that $\|\{v \in \Sigma^m \mid \exists i \leq m, u_i \oplus v \notin E\}\| > (\frac{1}{4})2^m$. Thus, there exists an i such that for at least $\frac{1}{m}(\frac{2^m}{4})$ v's, $v \oplus u_i \notin E$. Therefore, $|E| < 2^m(1 - \frac{1}{4m}) \leq 2^m(1 - \frac{1}{2^k})$ which is a contradiction.

2. $\text{Prob}[\|\{v \in \Sigma^m \mid \exists i \leq m, u_i \oplus v \in E\}\| = 2^m] = 1 - \text{Prob}\,[\exists v, |v| = m, \forall i \leq m, u_i \oplus v \notin E]$ $\geq 1 - \sum_v \text{Prob}\,[\forall i \leq m u_i \oplus v \notin E] = 1 - \sum_v \prod_i \text{Prob}\,[u_i \oplus v \notin E] \geq 1 - \sum_v \prod_i 2^{-k} = 1 - 2^{-m(k-1)}$.

□

Now we generalize the results of Zachos and Heller[ZH86] to classes defined by using the $\widehat{\text{BP}}$ operator.

Theorem 3.2

1. $(\forall\exists^+/\exists^+\forall)K \cup (\exists^+\forall/\forall\exists^+)K \subseteq \text{BP} \cdot K$.

2. *If K is closed under* AND *reductions then,* $\widehat{\text{BP}} \cdot K \subseteq (\forall\exists^+/\exists^+\forall)K$.

3. *If K is closed under* OR *reductions then,* $\widehat{\text{BP}} \cdot K \subseteq (\exists^+\forall/\forall\exists^+)K$.

Proof.

1. We show that $(\forall\exists^+/\exists^+\forall)K \subseteq \text{BP} \cdot K$. Let $L \in (\forall\exists^+/\exists^+\forall)K$. Then there exists a set $A \in K$ and polynomials p_1 and p_2 such that $x \in L \Rightarrow \forall y \exists^+ z \langle x, y, z\rangle \in A$ and $x \notin L \Rightarrow \exists^+ y \forall z \langle x, y, z\rangle \notin A$, where $|y| = p_1(|x|)$ and $|z| = p_2(|x|)$. Let $B = \{\langle x, w\rangle \mid w = yz, |y| = p_1(|x|), |z| = p_2(|x|), \langle x, y, z\rangle \in A\}$. Clearly, $B \leq^P_{AND} A$, and hence $B \in K$. Thus, $x \in L \Rightarrow \exists^+ w \langle x, w\rangle \in B$ and $x \notin L \Rightarrow \exists^+ w \langle x, w\rangle \notin B$, where $|w| = p_1(|x|) + p_2(|x|)$; that is, $L \in \text{BP} \cdot K$. The proof that $(\exists^+\forall/\forall\exists^+)K \subseteq \text{BP} \cdot K$ is similar.

2. Consider $L \in \widehat{\text{BP}} \cdot K$. Then, for each polynomial e there exists a set $A \in K$ and a polynomial p such that $\text{Prob}[x \in L \Leftrightarrow \langle x, y\rangle \in A] \geq 1 - \frac{1}{2^{e(|x|)}}$, where y is chosen uniformly from $\{0,1\}^{p(|x|)}$. Let $E_x = \{y \mid |y| = p(|x|), \langle x, y\rangle \in A\}$. Thus, $x \in L \Rightarrow |E_x| \geq (1 - \frac{1}{2^{e(|x|)}})2^{p(|x|)}$ and $x \notin L \Rightarrow |\bar{E}_x| \geq (1 - \frac{1}{2^{e(|x|)}})2^{p(|x|)}$; that is, Lemma 3.1 is applicable, for sufficiently large x, for both E_x and $\bar{E}_x$.

1. This follows directly from the second amplification lemma [Sch89].

2. Repeat the computation of a machine M accepting $L \in \mathrm{RP} \cdot K$ exactly $e(|x|)$ times on input x. Accept if and only if at least one of the computations accept.

3. The proof is similar to the one in part 2.

□

3 Main Results

In this section we show that $\widehat{\mathrm{BP}} \cdot \mathrm{C_=P} = \mathrm{RP} \cdot \mathrm{C_=P}$, which implies that $\widehat{\mathrm{BP}} \cdot \mathrm{C_=P} \cap \text{co-}(\widehat{\mathrm{BP}} \cdot \mathrm{C_=P}) = \mathrm{ZP} \cdot \mathrm{C_=P}$. Zachos and Heller[ZH86] gave a "decisive characterization" of BPP showing that $\mathrm{BPP} = (\exists^+\forall/\forall\exists^+)\mathrm{P}$. Their proof uses the fact that the error probability for BPP can be made exponentially small using only polynomial number of repetitions. This idea of making error probability exponentially small is built into the definition of the $\widehat{\mathrm{BP}}$ operator introduced by Toda and Ogiwara[TO90]. We show that the result of Zachos and Heller, that $\mathrm{BPP} = (\exists^+\forall/\forall\exists^+)\mathrm{P}$, immediately generalizes to $\widehat{\mathrm{BP}} \cdot K$ for classes K satisfying certain basic criterian. Using this result, we show that Tarui's result[Tar91], that $\mathrm{PH} \subseteq \mathrm{ZP} \cdot \mathrm{C_=P}$, is an immediate corollary of Toda and Ogiwara's result that $\mathrm{PH} \subseteq \widehat{\mathrm{BP}} \cdot \mathrm{C_=P}$. In fact, our result shows that the improvement from double-sided error to zero-sided error can be obtained merely by the interesting interaction of the operator $\widehat{\mathrm{BP}}$ with $\mathrm{C_=P}$.

For the sake of completeness we prove the following lemma which is implicitly proven in [ZH86]. Our presentation of the proof is adapted from [Sch89]. Here, $u \oplus v$ denotes exclusive-or of the bit vectors u and v.

Lemma 3.1 *Let m and k be some non-zero integers such that $4m \leq 2^k$. Let $E \subseteq \Sigma^m$ be a set with $|E| \geq (1 - \frac{1}{2^k})2^m$. Let $u_1, u_2, \ldots, u_m$ be chosen independently and uniformly from Σ^m. Then, the following statements hold:*

1. $Prob\Big[\|\{v \in \Sigma^m \mid \forall i \leq m, u_i \oplus v \in E\}\| \geq \frac{3}{4}2^m\Big] = 1$

2. $Prob[\|\{v \in \Sigma^m \mid \exists i \leq m, u_i \oplus v \in E\}\| = 2^m] \geq (1 - \frac{1}{2^{m(k-1)}})$

Proof.

5. $\mathrm{ZP} \cdot K = \mathrm{RP} \cdot K \cap \text{co-}(\mathrm{RP} \cdot K)$.

It is easy to see that $\text{co-}(\widehat{\mathrm{BP}} \cdot K) = \widehat{\mathrm{BP}} \cdot \text{co-}K$. However, $\text{co-}(\mathrm{RP} \cdot K)$ can be a different class than $(\text{co-RP}) \cdot K$ if the class K is not closed under complement. In fact, $(\text{co-RP}) \cdot \mathrm{C_=P} = \mathrm{C_=P}$ while it is not known if $\text{co-}(\mathrm{RP} \cdot \mathrm{C_=P})$ is equal to $\mathrm{C_=P}$.

Next, we define three special types of reducibilities used in this paper.

Definition 2.7

1. $A \leq^P_{AND} B$ *iff there exists a* $f \in \mathrm{PF}$ *such that for all* x, $f(x) = \langle y_1, y_2, \ldots, y_n \rangle$, *for some* n, *and such that* $x \in A \Leftrightarrow \wedge_{i=1}^n y_i \in B$. *We say that a class* K *is closed under* AND *reductions if for all* $B \in K$, $A \leq^P_{AND} B \Rightarrow A \in K$.

2. $A \leq^P_{OR} B$ *iff there exists a* $f \in \mathrm{PF}$ *such that for all* x, $f(x) = \langle y_1, y_2, \ldots, y_n \rangle$, *for some* n, *and such that* $x \in A \Leftrightarrow \vee_{i=1}^n y_i \in B$. *We say that a class* K *is closed under* OR *reductions if for all* $B \in K$, $A \leq^P_{OR} B \Rightarrow A \in K$.

3. $A \leq^P_{MAJ} B$ *iff there exists a* $f \in \mathrm{PF}$ *such that for all* x, $f(x) = \langle y_1, y_2, \ldots, y_n \rangle$, *for some* n, *and such that* $x \in A \Leftrightarrow$ *majority (at least* $\lceil \frac{n}{2} \rceil$*) of* $y_i \in B$. *We say that a class* K *is closed under* MAJORITY *reductions if for all* $B \in K$, $A \leq^P_{MAJ} B \Rightarrow A \in K$.

The reductions $A \leq^P_{AND} B$ and $A \leq^P_{OR} B$ are called $A \leq^P_{conj} B$ and $A \leq^P_{disj} B$, respectively, in literature. Also, Schöning[Sch89] defined the majority reduction only for odd n.

The following proposition follows from the definitions of various quantifiers by using "repeated computation".

Proposition 2.8

1. *If* K *is closed under* MAJORITY *reductions then,* $\widehat{\mathrm{BP}} \cdot K = \mathrm{BP} \cdot K$.

2. *If* K *is closed under* OR *reductions then, the error probability of* $\mathrm{RP} \cdot K$ *can be reduced from* $\frac{1}{2} - \epsilon$ *to* $\frac{1}{2^{e(|x|)}}$ *for any polynomial* e.

3. *If* K *is closed under* AND *reductions then, the error probability of* $(\text{co-RP}) \cdot K$ *can be reduced from* $\frac{1}{2} - \epsilon$ *to* $\frac{1}{2^{e(|x|)}}$ *for any polynomial* e.

Proof.

The following definition is the "operator" form of the definition from Zachos and Heller[ZH86]. The motivation here is that some complexity classes are defined so that the "rejection criterion" is not the logical negation of the "acceptance criterion". Hence, different quantifiers are needed to describe the acceptance and the rejection criterion.

Definition 2.5 *Let $Q_i, Q_i', i = 1, 2, \ldots k$, be polynomially bounded quantifiers from among $\exists, \forall, \exists^+$. Then, $L \in (Q_1, \ldots, Q_k / Q_1', \ldots, Q_k')K$ iff there exist polnomials $p_1, p_2, \ldots, p_k$ and a set $A \in K$ such that, $x \in L \Rightarrow Q_1 y_1\ Q_2 y_2 \ldots Q_k y_k\ \langle x, y_1, \ldots, y_k \rangle \in A$ and $x \notin L \Rightarrow Q_1' y_1\ Q_2' y_2 \ldots Q_k' y_k\ \langle x, y_1, \ldots, y_k \rangle \notin A$, where $|y_i| = p_i(|x|), i = 1, 2, \ldots, k$.*

Next, we define the various bounded-probability operators used in this paper. The operator BP was first introduced as a generalization of BPP in [Sch89], while $\widehat{\mathrm{BP}}$ was first defined in [TO90]. $\widehat{\mathrm{BP}}$ is an immediate generalization of BP with "free amplification" built into the definition. The notation of RP as an operator was introduced in [Tar91]; the similar quantifier is denoted $\exists^+$ in [ZH86].

Definition 2.6

1. *A language $L \in \mathrm{BP} \cdot K$ iff there exists a polynomial p, an $\epsilon > 0$ and a set $A \in K$ such that, $Prob[x \in L \Leftrightarrow \langle x, y \rangle \in A] \geq \frac{1}{2} + \epsilon$, where y is chosen uniformly from $\{0,1\}^{p(|x|)}$; that is, $\mathrm{BP} \cdot K = (\exists^+ / \exists^+)K$.*

2. *A language $L \in \widehat{\mathrm{BP}} \cdot K$ iff for each polynomial e there exists a polynomial p and a set $A \in K$ such that, $Prob[x \in L \Leftrightarrow \langle x, y \rangle \in A] \geq 1 - \frac{1}{2^{e(|x|)}}$, where y is chosen uniformly from $\{0,1\}^{p(|x|)}$.*

3. *A language $L \in \mathrm{RP} \cdot K$[1] iff there exists a polynomial p, an $\epsilon > 0$ and a set $A \in K$ such that, $x \in L \Rightarrow Prob[\langle x, y \rangle \in A] \geq \frac{1}{2} + \epsilon$ and $x \notin L \Rightarrow Prob[\langle x, y \rangle \notin A] = 1$ where y is chosen uniformly from $\{0,1\}^{p(|x|)}$; that is, $\mathrm{RP} \cdot K = (\exists^+ / \forall)K$.*

4. *A language $L \in (\text{co-RP}) \cdot K$ iff there exists a polynomial p, an $\epsilon > 0$ and a set $A \in K$ such that, $x \in L \Rightarrow Prob[\langle x, y \rangle \in A] = 1$ and $x \notin L \Rightarrow Prob[\langle x, y \rangle \notin A] \geq \frac{1}{2} + \epsilon$ where y is chosen uniformly from $\{0,1\}^{p(|x|)}$; that is, $(\text{co-RP}) \cdot K = (\forall / \exists^+)K$.*

[1] This definition is slightly different from that of Tarui's due to the presence of ϵ. However, with our definition the RP operator is easily defined using notation used by Zachos and Heller as, $\mathrm{RP} \cdot K = (\exists^+ / \forall)K$. If the class K is closed under OR reductions, then the two definitions are equivalent.

to normal nondeterministic oracle Turing machines which may ask several queries on the same computation path, and the new queries may depend on the answers to the previous queries. The reader is referred to [Tor88] for an excellent exposition on some of the techniques that can be used to show this equivalence.

All languages are over the fixed alphabet $\Sigma = \{0,1\}$. The set of natural numbers is denoted by $\mathcal{N}$. We denote by PF the class of polynomial time computable functions and by P the set of polynomial time recognizable languages. We use $\langle \cdot, \cdot \rangle$ to denote a standard polynomial time computable pairing function. Furthermore, we use $\langle \cdot, \cdot, \cdot \rangle$ to denote $\langle \langle \cdot, \cdot \rangle, \cdot \rangle$.

We now define some standard operators.

Definition 2.1

1. *A language $L \in \exists \cdot K$ iff there exists a polynomial p and a set $A \in K$ such that, $x \in L \Leftrightarrow \|\{y \mid |y| = p(|x|), \langle x, y \rangle \in A\}\| \geq 1$.*

2. *A language $L \in \forall \cdot K$ iff there exists a polynomial p and a set $A \in K$ such that, $x \in L \Leftrightarrow \|\{y \mid |y| = p(|x|), \langle x, y \rangle \in A\}\| = 2^{p(|x|)}$.*

3. *A language $L \in \mathrm{C}_{=} \cdot K$ iff there exists a function $f \in \mathrm{PF}$, $f : \Sigma^* \longmapsto \mathcal{N}$, a polynomial p and a set $A \in K$ such that, $x \in L \Leftrightarrow \|\{y \mid |y| = p(|x|) \langle x, y \rangle \in A\}\| = f(x)$.*

Using the above notation the polynomial-time hierarchy can be defined to be $\mathrm{PH} = \cup_{k>0} \underbrace{\exists \forall \ldots}_{k>0} \mathrm{P}$.

The class $\mathrm{C}_{=}\mathrm{P} = \mathrm{C}_{=} \cdot \mathrm{P}$. The following alternate characterization of $\mathrm{C}_{=}\mathrm{P}$ will be useful in this paper.

Definition 2.2 *A function from strings to integers is in $\mathcal{Z}\#\mathrm{P}$ if there exists a nondeterministic Turing machine M such that $f(x) =$Number of accepting paths of M on x $-$ Number of rejecting paths of M on x. $L \in \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$ iff there exists a $f \in \mathcal{Z}\#\mathrm{P}$ such that $x \in L \Leftrightarrow f(x) = 0$.*

Proposition 2.3 *[Gup91]* $\mathrm{C}_{=}\mathrm{P} = \mathcal{Z}\mathrm{C}_{=}\mathrm{P}$.

Zachos and Heller[ZH86] introduced the quantifier $\exists^+$ to denote that "most" of the choices satfisfy a predciate.

Definition 2.4 *Let $P(y)$ be a predicate. Then $\exists^+ y P(y)$ is true iff there exists an $\epsilon > 0$ and a polynomial p such that Prob$[P(y)] \geq \frac{1}{2} + \epsilon$, where y is chosen uniformly from $\{0,1\}^{p(|x|)}$.*

Keywords: Computational Complexity, Probabilistic classes, Polynomial-time hierarchy

1 Introduction

Toda and Ogiwara [TO90] showed that PH $\subseteq \widehat{\mathrm{BP}} \cdot \mathrm{C_{=}P}$; that is, the polynomial-time hierarchy is contained in $\mathrm{C_{=}P}$ with arbitrarily low double-sided error probability. Tarui[Tar91] independently proved and improved this result to show that PH $\subseteq \mathrm{ZP} \cdot \mathrm{C_{=}P}$; that is, the polynomial-time hierarchy is contained in $\mathrm{C_{=}P}$ with zero-sided error probability. It may appear that the improved result PH $\subseteq \mathrm{ZP} \cdot \mathrm{C_{=}P}$ requires an understanding of the algorithm by which a language in PH can be accepted by a $\mathrm{C_{=}P}$ machine with some error probability. In this paper we show that this is not the case; the result PH $\subseteq \widehat{\mathrm{BP}} \cdot \mathrm{C_{=}P}$ is sufficient to show that PH $\subseteq \mathrm{ZP} \cdot \mathrm{C_{=}P}$.

We prove that $\widehat{\mathrm{BP}} \cdot \mathrm{C_{=}P} = \mathrm{RP} \cdot \mathrm{C_{=}P}$ which implies that $\widehat{\mathrm{BP}} \cdot \mathrm{C_{=}P} \cap \text{co-}\widehat{\mathrm{BP}} \cdot \mathrm{C_{=}P} = \mathrm{ZP} \cdot \mathrm{C_{=}P}$. Thus, PH $\subseteq \widehat{\mathrm{BP}} \cdot \mathrm{C_{=}P}$ implies that PH $\subseteq \mathrm{ZP} \cdot \mathrm{C_{=}P}$ in a straight forward fashion. Besides providing an alternate characterization of the class $\mathrm{ZP} \cdot \mathrm{C_{=}P}$, our result shows that the improvement from double-sided error to zero-sided error can be obtained merely by the interesting interaction of the operator $\widehat{\mathrm{BP}}$ with $\mathrm{C_{=}P}$.

Our result, that $\widehat{\mathrm{BP}} \cdot \mathrm{C_{=}P} = \mathrm{RP} \cdot \mathrm{C_{=}P}$, uses an immediate generalization of the results of Zachos and Heller[ZH86]. They gave a "decisive characterization" of BPP showing that BPP $= (\exists^{+}\forall/\forall\exists^{+})\mathrm{P}$. Their proof uses the fact that the error probability for BPP can be made exponentially small using only a polynomial number of repetitions. This idea of making the error probability exponentially small is built into the definition of the $\widehat{\mathrm{BP}}$ operator introduced by Toda and Ogiwara[TO90]. We show that the result of Zachos and Heller, that BPP $= (\exists^{+}\forall/\forall\exists^{+})\mathrm{P}$, immediately generalizes to $\widehat{\mathrm{BP}} \cdot K$, for classes K closed under certain basic reductions.

This paper is organized as follows: in the next section we introduce the operators and complexity classes used in this paper. We also state some easy properties of these operators. In Section 3 we present our main results: first we generalize the results of [ZH86], and using this we show that the main theorem in [Tar91] follows directly from the theorem in [TO90].

2 Preliminaries

Our model of computation is weak nondeterministic oracle Turing machines(NTMs). For such machines, each computation path always ends by writing a string on the query tape and accepts if and only if the query answer is "yes". For most important classes, this model is equivalent

On Bounded-Probability Operators and $C_{=}P$[1]

Sanjay Gupta
sgupta@cis.ohio-state.edu
Department of Computer and Information Science
The Ohio State University
Columbus, Ohio 43210

[1]This work was supported in part by NSF Grant CCR-8909071.