# The Relativized Relationship between Probabilistically Checkable Debate Systems, IP and PSPACE

ALEXANDER RUSSELL*
Department of Mathematics

RAVI SUNDARAM†
Laboratory for Computer Science

Massachusetts Institute of Technology
Cambridge, MA 02139

September 3, 1993

**Abstract**

In 1990, **PSPACE** was shown to be identical to **IP**, the class of languages with interactive proofs [18, 20]. Recently, **PSPACE** was again recharacterized, this time in terms of *(Random) Probabilistically Checkable Debate Systems* [7, 8]. In particular, it was shown that $\mathbf{PSPACE} = \mathbf{PCDS}[\log n, 1] = \mathbf{RPCDS}[\log n, 1]$. We study the relativized behaviour of the classes defined by these debate systems in comparison with the classes **IP** and **PSPACE**. For the relationships between $(\mathbf{R})\mathbf{PCDS}[r(n), a(n)]$ and **IP** and $(\mathbf{R})\mathbf{PCDS}[r(n), a(n)]$ and **PSPACE** we determine a natural boundary (in terms of the parameters $r(n)$ and $a(n)$) separating direct-simulability and inequality (with probability 1). In addition, we show that if $\exists O, \mathbf{EXP}^O = \mathbf{PCDS}^O[\log n, \log n]$ then $\mathbf{P} \neq \mathbf{PSPACE}$.

**Keywords:** Computational complexity; interactive proofs; oracles

## 1 Introduction and Definitions

The notion of relativization was introduced by Baker, Gill, and Solovay [4] in an attempt to explain the difficulty of the famous $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ question. The attachment of oracles to different classes of machines, in general, is a method for exaggerating (perhaps small) differences in the computational ability of these classes. One way to lend credence to a conjectured relationship between two complexity classes is to exhibit an oracle relative to which the conjecture holds. Thus, the presentation of *contradictory relativizations* of a relationship between two complexity classes has been a standard tool for arguing the difficulty of precisely determining that relationship. The notion of relativization was strengthened by the consideration of random oracles [5]. In the words of Bennett and Gill:

*E-mail address: acr@theory.lcs.mit.edu. Supported by an NSF Graduate Fellowship and grants NSF 92-12184, AFOSR F49620-92-J-0125, and DARPA N00014-92-1799

†E-mail address: koods@theory.lcs.mit.edu. Supported by grants NSF 92-12184, AFOSR F49620-92-J-0125, and DARPA N00014-92-J-1799

> ... random oracles, by their very structurelessness, appear more benign and less likely to distort the relations among complexity classes than the other oracles used in complexity theory and recursive function theory, which are usually designed expressly to help or frustrate some class of computations.

This led them to formulate the RANDOM ORACLE HYPOTHESIS [5]: *the relationship between two natural complexity classes is preserved with probability 1 under relativization by a random oracle.* In this new framework, a conjectured relationship may be supported by showing that it holds with probability 1 relative to a random oracle. Clearly, this framework precludes the existence of contradictory (probability 1) relativizations.

Counter-examples to the random oracle hypothesis have been demonstrated and discussed in [12, 13, 14, 17, 19]. Recently, the random oracle hypothesis suffered a particularly crippling blow: the classes **IP** and **PSPACE** were shown to be equal [18, 20] despite separation with probability 1 [10, 6]. This proof that **IP** = **PSPACE** relies heavily on algebraic techniques, the cause of this nonrelativizing behavior. The class **PSPACE** has recently been given a new characterization in terms of *Probabilistically Checkable Debate Systems* [7, 8] also using such algebraic techniques. We examine the relativized behaviour of **IP** and **PSPACE** in comparison with the classes defined by these debate systems. We determine a natural boundary (in terms of certain parameters of the debate systems) separating direct-simulability and inequality (with probability 1). In addition to offering more evidence that these algebraic techniques do not relativize, these boundaries indicate that this new characterization of **PSPACE** is essentially stronger than the characterization of **PSPACE** by interactive proof systems–i.e., under relativization by a random oracle, the class of languages recognized by these debate systems is strictly smaller than that recognized by interactive proof systems. Finally, in the same vein as [9], we show that if $\exists O, \mathbf{EXP}^O = \mathbf{PCDS}^O[\log n, \log n]$ then $\mathbf{P} \neq \mathbf{PSPACE}$.

Oracles are attached to given enumerations of machines. When we speak of $\mathcal{C}^O$ where $\mathcal{C}$ is a complexity (language) class and $O$ an oracle, we will mean $\left\{\mathcal{L} \mid \mathcal{L} = L(M_i^O)\right\}$ where $\{M_i\}$ is an enumeration of machines such that $\{L(M_i)\} = \mathcal{C}$.

Fix an alphabet $\Sigma$. Let $\Lambda$ denote the empty word of $\Sigma^*$. $1^k$ denotes the concatenation of $k$ 1's. The result of running a probabilistic Turing machine $M$ on input $x$ with random string $R$ is denoted by $M[x;R]$. We reserve the variable $n$ for $|x|$, the length of the input in question.

**Definition 1.1 (IP)** *Let $\mathcal{P}$ be the class of interactive Turing machines ([11]). Define* **IP** *to be the class of languages $\mathcal{L}$ for which there exists a polynomial-time probabilistic interactive Turing machine $V$ so that*

- $x \in \mathcal{L} \Rightarrow \exists P \in \mathcal{P}, \Pr_{R \in coins}[(V \leftrightarrow P)[x;R] \ accepts] = 1$
- $x \notin \mathcal{L} \Rightarrow \forall P \in \mathcal{P}, \Pr_{R \in coins}[(V \leftrightarrow P)[x;R] \ accepts] < \frac{1}{3}$

*where $(V \leftrightarrow P)[x;R]$ denotes the interaction of verifier $V$ with prover $P$ on input $x$ and random coins $R$.*

After the definition of this class, it was shown that

**Theorem 1.2 ([10])** $\exists O, \mathbf{coNP}^O \not\subseteq \mathbf{IP}^O$ *(which implies that* $\mathbf{PSPACE}^O \neq \mathbf{IP}^O$*).*

and that, in fact, the above is a probability 1 result ([6]). Then, in a remarkable breakthrough, it was actually shown that

**Theorem 1.3 ([18, 20]) IP = PSPACE.**

Recently, using the machinery of [1], Condon *et. al.* gave a new characterization of **PSPACE** in terms of *Probabilistically Checkable Debate Systems*, defined below.

**Definition 1.4** *For a function* $f : \Sigma^* \to \Sigma^*$, *let* $f\langle x\rangle \stackrel{\text{def}}{=} f(x) \cdot x$. *A* $k$-player *is a function* $P : \Sigma^* \to \Sigma^k$. *Two* $k$*-players,* $P_1$ *and* $P_2$*, define an* $l$-debate $D_l(P_1, P_2) \stackrel{\text{def}}{=} \overbrace{P_1\langle P_2\langle P_1 \ldots \langle}^{l} \Lambda\rangle \ldots\rangle\rangle$.

**Definition 1.5 ([7, 8])** *Define* $\mathbf{PCDS}[r(n), a(n)]$ *to be the class of languages* $\mathcal{L}$ *for which there exists a probabilistic polynomial time Turing machine* $V$ *and polynomials* $q$ *and* $l$ *so that*

- $x \in \mathcal{L} \Rightarrow \exists P_1, \forall P_2, \Pr_{R\in coins}\left[V^{D(P_1,P_2)}[x; R] \text{ accepts}\right] = 1$
- $x \notin \mathcal{L} \Rightarrow \forall P_1, \exists P_2, \Pr_{R\in coins}\left[V^{D(P_1,P_2)}[x; R] \text{ accepts}\right] < \frac{1}{3}$

*where* $P_1$ *and* $P_2$ *are* $q(n)$*-players,* $D(P_1, P_2) = D_{l(n)}(P_1, P_2)$ *and, in either case, the verifier* $V$ *uses at most* $O(r(n))$ *random bits and examines at most* $O(a(n))$ *bits of* $D(P_1, P_2)$*, the debate generated by the two players* $P_1$ *and* $P_2$*. If we change the reject criteria so that the second player acts randomly, that is*

- $x \notin \mathcal{L} \Rightarrow \forall P_1, \Pr_{R\in coins, P_2}\left[V^{D(P_1,P_2)}[x; R] \text{ accepts}\right] < \frac{1}{3}$

*then we obtain the class of languages with Random Probabilistically Checkable Debate Systems [8] which we denote* $\mathbf{RPCDS}[r(n), a(n)]$.

As mentioned above, we have the following two theorems relating these debate systems and **PSPACE**.

**Theorem 1.6 ([7])** $\mathbf{PSPACE} = \mathbf{PCDS}[\text{poly } n, \text{poly } n] = \mathbf{PCDS}[\log n, 1]$.

**Theorem 1.7 ([8])** $\mathbf{PSPACE} = \mathbf{RPCDS}[\text{poly } n, \text{poly } n] = \mathbf{RPCDS}[\log n, 1]$.

# 2 Relativization Results

We concentrate on the behaviour of these classes with respect to a random oracle $O \in \Omega = 2^{\Sigma^*}$. The probability measure $\mu$ on $\Omega$ is defined by independently placing each string in the oracle with probability $\frac{1}{2}$. We begin by considering the relationship between $\mathbf{PCDS}[r(n), a(n)]$ and **PSPACE**.

## 2.1 The Relationship between $\mathbf{PCDS}[r(n), a(n)]$ and PSPACE

Since we are comparing **PSPACE** with smaller classes we consider **PSPACE** to be provided with the weak oracle-access mechanism, that is the oracle tape is a work tape.

**Theorem 2.1** $\forall O \subseteq \Sigma^*, \mathbf{PCDS}^O[0, \text{poly } n] = \mathbf{PSPACE}^O$.

*Proof:* By simulation. □

**Theorem 2.2** $\forall k, \Pr_{O\in\Omega}\left[\mathbf{PSPACE}^O = \mathbf{PCDS}^O[\text{poly } n, n^k]\right] = 0$.

*Proof:* We prove in the lemma below that with probability 1, $\mathbf{NP}^O$ is not even contained in $\mathbf{PCDS}^O[\text{poly}\, n, n^k]$. Since $\forall O, \mathbf{NP}^O \subseteq \mathbf{PSPACE}^O$, this shows that, with probability 1, $\mathbf{PCDS}^O[\text{poly}\, n, n^k]$ and $\mathbf{PSPACE}^O$ are different.

**Lemma 2.3** $\forall k$, $\Pr_{O\in\Omega}\left[\mathbf{NP}^O \subseteq \mathbf{PCDS}^O[\text{poly}\, n, n^k]\right] = 0$.

*Proof:* For an oracle $O$, define

$$\hat{O} = \left\{x \mid \forall t \in \{0, \ldots, |x|-1\}, x10^t \in O\right\}.$$

A polynomial-time machine with access to $O$ can efficiently sample from $\hat{O}$. If $O$ is a random oracle, then $\forall x$, $\Pr_{O\in\Omega}\left[x \in \hat{O}\right] = \frac{1}{2^{|x|}}$ so that $\forall n$, $\text{Exp}_{O\in\Omega}\left[\left|\hat{O}\cap\Sigma^n\right|\right] = 1$. For an oracle $A$, define

$$\mathcal{L}_\exists(A) = \left\{1^n \mid \exists y \in \Sigma^{n^{2k}} \cap A\right\}.$$

Clearly, $\forall O, \mathcal{L}_\exists(\hat{O}) \in \mathbf{NP}^O$. We show that $\Pr_{O\in\Omega}\left[\mathcal{L}_\exists(\hat{O}) \in \mathbf{PCDS}^O[\text{poly}\, n, n^k]\right] = 0$. Fix an enumeration of $\mathbf{PCDS}^O[\text{poly}\, n, n^k]$ verifiers $\{V_i \mid i \in \mathbb{N}\}$. Let $V_i$ be a verifier of this collection which, for $n \geq n_0$, takes at most $n^i$ time, queries at most $cn^k$ debate bits and uses some fixed polynomial, $r(n)$, amount of randomness. For $m, i \in \mathbb{N}$, define

$$\Omega_m^{(s)} = \left\{O \in \Omega \mid \left|\hat{O}\cap\Sigma^m\right| = s\right\}.$$

Then $\mu(\Omega_m^{(0)}) = (1 - \frac{1}{2^m})^{2^m} \approx \frac{1}{e}$. Let $n_1$ be large enough so that $\frac{2\cdot n_1^i \cdot 2^{cn_1^k}}{2^{n_1^{2k}}} < \frac{2}{3}$. Let $n > \tilde{n} \stackrel{\text{def}}{=} \max(n_0, n_1)$ and consider the behaviour of $V_i^O$ on $1^n$ with an oracle $O$ selected from $\Omega_{n^{2k}}^{(0)}$. One of the following three cases applies:

1. If $\Pr_{O\in\Omega_{n^{2k}}^{(0)}}\left[\exists P_1, \forall P_2, \Pr_{R\in\text{coins}}\left[V_i^{O,D(P_1,P_2)}[1^n; R] \text{ accepts}\right] = 1\right] \geq \frac{1}{4}$, then

$$\Pr_{O\in\Omega}\left[\exists P_1, \forall P_2, \Pr_{R\in\text{coins}}\left[V_i^{O,D(P_1,P_2)}[1^n; R] \text{ accepts}\right] = 1 \wedge 1^n \notin \mathcal{L}_\exists(\hat{O})\right] \geq \frac{1}{4}\Pr_{O\in\Omega}\left[O \in \Omega_{n^{2k}}^{(0)}\right] \approx \frac{1}{4e}. \quad (1)$$

   (Recall that $\mu(\Omega_{n^{2k}}^{(0)}) \approx \frac{1}{e}$.)

2. If

$$\Pr_{O\in\Omega_{n^{2k}}^{(0)}}\left[\exists P_1, \forall P_2, \Pr_{R\in\text{coins}}\left[V_i^{O,D(P_1,P_2)}[1^n; R] \text{ accepts}\right] \in [\frac{1}{3}, 1)\right] \geq \frac{1}{4e} \quad (2)$$

   then $V_i$ is behaving improperly, and evidently does not accept $L_\exists(\hat{O})$ for this $\frac{1}{4e}$ fraction of oracles.

3. If $\Pr_{O\in\Omega_{n^{2k}}^{(0)}}\left[\forall P_1, \exists P_2, \Pr_{R\in\text{coins}}\left[V_i^{O,D(P_1,P_2)}[1^n; R] \text{ accepts}\right] < \frac{1}{3}\right] \geq 1 - \frac{1}{2e}$, then we show that this set of oracles on which $V_i$ is successful induces a set of oracles on which $V_i$ errs. To begin with, we show that for any oracle $O$, most questions that $V_i$ asks of $O$ are asked on very few random strings. Fix an oracle $O$. Let us consider the behaviour of $V_i$ on a particular random

string $R$. Considering all of the possible $2^{cn^k}$ responses to $V_i$'s $cn^k$ queries[1] to $D(P_1, P_2)$ and noting that on any one path $V_i$ may only query $n^i$ strings of $O$, we have that on $R$ there are a total of at most $n^i \cdot 2^{cn^k}$ strings of $O$ that $V_i$ might query. We then have that

$$\Pr_{q \in \Sigma^{n^{2k}}} \left[ V_i^O[1^n; R] \text{ queries } q \right] \leq \frac{n^i \cdot 2^{cn^k}}{2^{n^{2k}}}.$$

Define

$$\mathcal{R}(Q, O) \stackrel{\text{def}}{=} \left\{ R \in \{0,1\}^{r(n)} \mid \exists q \in Q, \exists D \subseteq \Sigma^*, V_i^{O,D}[1^n; R]) \text{ queries } q \right\}.$$

Then

$$\operatorname*{Exp}_{q \in \Sigma^{n^{2k}}} \left[ |\mathcal{R}(\{q\}, O)| \right] \leq \frac{n^i \cdot 2^{r(n)} \cdot 2^{cn^k}}{2^{n^{2k}}}.$$

Invoking Markov's inequality yields

$$\forall O, \Pr_{q \in \Sigma^{n^{2k}}} \left[ |\mathcal{R}(\{q\}, O)| \geq \frac{2 \cdot n^i \cdot 2^{r(n)} \cdot 2^{cn^k}}{2^{n^{2k}}} \right] \leq \frac{1}{2}.$$

Define $S_q \stackrel{\text{def}}{=} \left\{ q1, q10, \ldots, q10^{|q|} \right\}$. Then, because $\forall q_1 \neq q_2 \in \Sigma^{2cn^k}, S_{q_1} \cap S_{q_2} = \emptyset$ we have that

$$\forall O, \Pr_{q \in \Sigma^{n^{2k}}} \left[ |\mathcal{R}(S_q, O)| > \frac{2 \cdot n^i \cdot 2^{r(n)} 2^{cn^k}}{2^{n^{2k}}} \right] \leq \frac{1}{2}.$$

Now, define $\Omega_m^{(1)} \stackrel{\text{def}}{=} \left\{ O \in \Omega \mid \left| \hat{O} \cap \Sigma^m \right| = 1 \right\}$. Then $\mu(\Omega_m^{(1)}) \approx \frac{1}{e}$. Let $E(O)$ be the event that $\forall P_1, \exists P_2, \Pr_{R \in \text{coins}} \left[ V_i^{O,D(P_1,P_2)}[1^n; R] \text{ accepts} \right] < \frac{1}{3}$. Then we may compute

$$\begin{aligned}
\Pr_{O \in \Omega^{(0)}_{n^{2k}}, q \in \Sigma^{n^{2k}}} \left[ E(O) \bigwedge |\mathcal{R}(S_q, O)| < \frac{2 \cdot n^i \cdot 2^{r(n)} \cdot 2^{cn^k}}{2^{n^{2k}}} \right] &\geq \\
\Pr_{O \in \Omega^{(0)}_{n^{2k}}} [E(O)] + \Pr_{O \in \Omega^{(0)}_{n^{2k}}, q \in \Sigma^{n^{2k}}} \left[ |\mathcal{R}(S_q, O)| < \frac{2 \cdot n^i \cdot 2^{r(n)} \cdot 2^{cn^k}}{2^{n^{2k}}} \right] - 1 &\geq \\
(1 - \frac{1}{2e}) + (1 - \frac{1}{2}) - 1 &\geq \\
\frac{1}{4}.
\end{aligned}$$

When the two above events occur we can conclude that

$$\forall P_1, \exists P_2, \Pr_{R \in \text{coins}} \left[ V_i^{O \cup S_q, D(P_1,P_2)}[1^n; R] \text{ accepts} \right] < \frac{1}{3} + \frac{2 \cdot n^i \cdot 2^{cn^k}}{2^{n^{2k}}}.$$

Notice that if $O$ and $q$ are chosen uniformly from $\Omega_m^{(0)}$ and $\Sigma^m$, respectively, then $O \cup S_q$ is uniform on $\Omega_m^{(1)}$. Therefore, for $n > \tilde{n}$,

$$\Pr_{O \in \Omega^{(1)}_{n^{2k}}} \left[ \forall P_1, \exists P_2, \Pr_{R \in \text{coins}} \left[ V_i^{O \cup S_q, D(P_1,P_2)}[1^n; R] \text{ accepts} \right] < 1 \right] \geq \frac{1}{4}.$$

[1]There are at most $2^{cn^k}$ responses to $V_i$'s queries even if $V_i$ is *adaptive* (so that the $i+1$st query may depend on the answer to the $i$th query).

Since $O \in \Omega_m^{(1)}$ implies $1^n \in \mathcal{L}_\exists(\hat{O})$,

$$\Pr_{O\in\Omega}\left[\forall P_1, \exists P_2 \Pr_{R\in\text{coins}}\left[V_i^{O,D(P_1,P_2)}[1^n; R] \text{ accepts}\right] \neq 1 \wedge 1^n \in \mathcal{L}_\exists(\hat{O})\right] \geq \frac{1}{4}\cdot\frac{1}{e}. \qquad (3)$$

Let $,_n$ be the event that $\exists P_1, \forall P_2, V_i^{O,D(P_1,P_2)}[1^n]$ accepts $\iff 1^n \in \mathcal{L}_\exists(\hat{O})$. From (1), (2) and (3) it follows that for $n > \tilde{n}$,

$$\Pr_{O\in\Omega}[,_n] < 1 - \frac{1}{4e}.$$

Furthermore, for $m > n^i$, $,_n$ and $,_m$ are independent (or use Lemma 1 of [5]). Hence, for any $V_i$,

$$\begin{aligned} \Pr_{O\in\Omega}\left[L(V_i^O) = \mathcal{L}_\exists(\hat{O})\right] &\leq \\ \prod_{j=\tilde{n}}^{\infty} \Pr_{O\in\Omega}\left[,_{2^{l^j}}\right] &= 0. \end{aligned}$$

Finally,

$$\Pr_{O\in\Omega}\left[\exists V_i^O, L(V_i^O) = \mathcal{L}_\exists(\hat{O})\right] \leq \sum_i \Pr_{O\in\Omega}\left[L(V_i^O) = \mathcal{L}_\exists(\hat{O})\right] = 0$$

so that

$$\Pr_{O\in\Omega}\left[\mathbf{NP}^O \subseteq \mathbf{PCDS}^O[\text{poly } n, n^k]\right] = 0.$$

□

Reiterating, from the fact that $\forall O, \mathbf{NP}^O \subseteq \mathbf{PSPACE}^O$ and the above lemma we have the desired theorem. □

## 2.2 The Relationship between $\mathbf{PCDS}[r(n), a(n)]$ and IP

**Theorem 2.4** *Consider the two classes* **IP** *and* $\mathbf{PCDS}[\text{poly } n, n^k]$. *We have*

1. $\Pr_{O\in\Omega}\left[\mathbf{IP}^O \subseteq \mathbf{PCDS}^O[\text{poly } n, n^k]\right] = 0$,
2. $\Pr_{O\in\Omega}\left[\mathbf{PCDS}^O[\text{poly } n, n^k] \subseteq \mathbf{IP}^O\right] = 0$.

*Proof:*

1. Using Lemma 2.3 and the fact that $\forall O \in \Omega, \mathbf{NP}^O \subseteq \mathbf{IP}^O$ we have the desired statement.
2. This follows from [6] and the fact that $\forall O, \mathbf{coNTIME}^O[n] \subseteq \mathbf{IP}^O \Rightarrow \mathbf{coNP}^O \subseteq \mathbf{IP}^O$.

□

## 2.3 The Relativized Relationship between $\mathbf{RPCDS}[r(n), a(n)]$ and IP, $\mathbf{PCDS}[r(n), a(n)]$

**Theorem 2.5** $\forall O, \mathbf{IP}^O = \mathbf{RPCDS}^O[\text{poly } n, \text{poly } n] = \mathbf{RPCDS}^O[0, \text{poly } n]$.

*Proof:* By simulation. □

Consider the classes $\mathbf{RPCDS}[\text{poly } n, n^k]$ and **IP**.

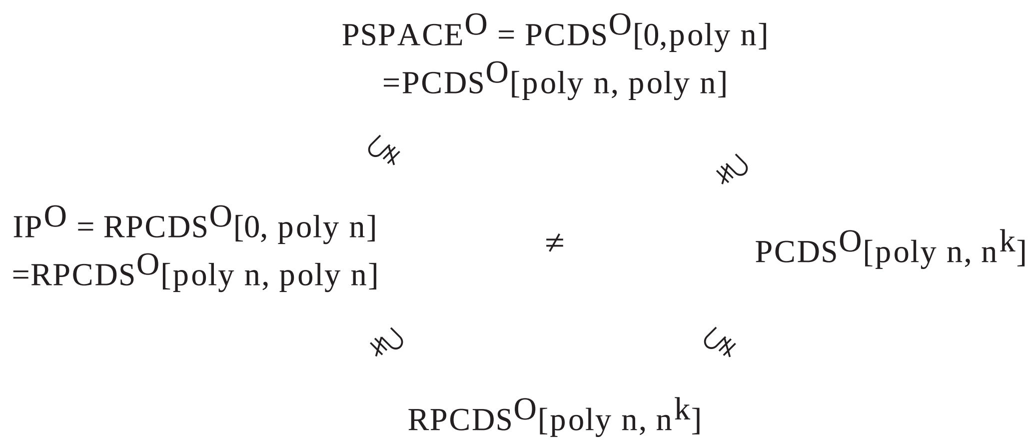


Figure 1: The Relativized World.

**Theorem 2.6** $\forall k, \Pr_{O\in\Omega}\left[\mathbf{RPCDS}^O[\text{poly } n, n^k] = \mathbf{IP}^O\right] = 0.$

*Proof:* We have that $\forall O, \mathbf{RPCDS}^O[\text{poly } n, n^k] \subseteq \mathbf{PCDS}^O[\text{poly}, n^k]$ so that Lemma 2.3 yields the desired result. $\square$

**Theorem 2.7** *For* $a(n) = \omega(\log n)$,

$$\Pr_{O\in\Omega}\left[\mathbf{PCDS}^O[r(n), a(n)] \subseteq \mathbf{RPCDS}^O[\text{poly } n, \text{poly } n]\right] = 0.$$

*Proof:* $\forall O, \mathbf{coNTIME}^O[a(n)] \subseteq \mathbf{PCDS}^O[r(n), a(n)]$ but, by argument similar to that of Lemma 2.3, one may show that

$$\Pr_{O\in\Omega}\left[\exists\mathcal{L} \in \mathbf{coNTIME}^O[a(n)] - \mathbf{RPCDS}^O[\text{poly } n, \text{poly } n]\right] = 1.$$

$\square$

Figure 1 shows the probability 1 relationships between these classes.

## 2.4 The Relationship between $\mathbf{PCDS}[r(n), a(n)]$ and EXPTIME

An oracle equating **NP** and **EXP** has been discovered by Heller [16].

**Theorem 2.8 ([16])** $\exists O \subseteq \Sigma^*$ *so that* $\mathbf{EXP}^O = \mathbf{NP}^O$.

Fortnow [9] has shown the following theorem relating the existence of an oracle equating $\mathbf{PCP}[\log n, 1]$ (see [1]) and **EXP** to the $\mathbf{P} \stackrel{?}{=} \mathbf{NP}$ question.

**Theorem 2.9 ([9])** *If* $\exists O \subseteq \Sigma^*$ *so that* $\mathbf{PCP}^O[\log n, 1] = \mathbf{EXP}^O$ *then* $\mathbf{P} \neq \mathbf{NP}$.

We prove a similar result for the class $\mathbf{PCDS}[\log n, \log n]$.

**Theorem 2.10** *If* $\exists O \subseteq \Sigma^*$ *so that* $\mathbf{PCDS}^O[\log n, \log n] = \mathbf{EXP}^O$ *then* $\mathbf{P} \neq \mathbf{PSPACE}$.

*Proof:* Let $O$ be an oracle so that $\mathbf{PCDS}^O[\log n, \log n] = \mathbf{EXP}^O$. Assume, for contradiction that $\mathbf{P} = \mathbf{PSPACE}$. Let $\mathcal{L}$ be a $\leq_p$-complete language for $\mathbf{EXP}^O$. We show that $\mathcal{L} \in \mathbf{P}^O$ and conclude that $\mathbf{P}^O = \mathbf{EXP}^O$, which contradicts the time hierarchy theorem [15]. Let $V$ be a $\mathbf{PCDS}^O[\log n, \log n]$ verifier for $\mathcal{L}$. We construct $D^O$, a deterministic polynomial time machine so that $L(D^O) = \mathcal{L}$. $D^O$, given input $w$, writes down the entire computation tree $\mathfrak{T}$ of $V[w]$, answering $V[w]$'s questions to $O$ by actual questions to $O$ and branching at those nodes where $V[w]$ receives debate tape answers. Notice that choice of a pair $(P_1, P_2)$ determines a path in $\mathfrak{T}$. This path is *satisified* if $V[w]$ accepts with these responses. Because $V[w]$ uses $O(\log n)$ random bits and receives $O(\log n)$ bits back from the debate tape, the total size of $\mathfrak{T}$ is polynomial in $|w|$. $\mathfrak{T}$ contains no queries to $O$. $D^O$ would now like to determine if $\exists P_1, \forall P_2$, the induced path in $\mathfrak{T}$ is satisfied. Fortunately, this is a $\mathbf{PSPACE}$ decision problem, which can be solved in polynomial time because $\mathbf{P} = \mathbf{PSPACE}$. Hence, $\mathcal{L} \in \mathbf{P}^O$ and $\mathbf{EXP}^O = \mathbf{P}^O$, contradicting the time hierarchy theorem. $\square$

## 3 Direction for Future Research

The discovery of simulation techniques which do not relativize (with probability 1) is astonishing. This leads us to question the meaning of relativization in general. One would like to distill the essential non-relativizing ingredient of these algebraic techniques. This may be done by presentation of (perhaps contrived) complexity classes with a somehow simpler (algebraic) proof of equality which exhibit this behaviour. Alternatively, this may be done by presentation of a new framework (perhaps just a new oracle-access mechanism [9]), analogous to relativization, in which these techniques behave well.

## 4 Acknowledgements

We would like to thank Joan Feigenbaum and Lance Fortnow for helpful discussions. We would also like to thank the anonymous referees, who gave an improved proof of Theorem 2.4(2) and improved the general presentation.

## References

[1] S. Arora, C. Lund, R. Motwani, M. Sudan, and M. Szegedy. Proof verification and the hardness of approximation problems. In *Proceedings of the Thirty Third Symposium on Foundations of Computer Science*, pages 14–23. IEEE, 1992.

[2] L. Babai. Trading group theory for randomness. In *Proceedings of the Seventeenth ACM Symposium on the Theory of Computing*, pages 421–429. ACM, 1985.

[3] 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(2):254–276, 1988.

[4] T. Baker, J. Gill, and R. Solovay. Relativizations of the P = NP question. *SIAM Journal on Computing*, 4(4):431–442, 1975.

[5] C. Bennett and J. Gill. Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \text{co-NP}^A$ with probability 1. *SIAM Journal on Computing*, 10(1):96–113, 1981.

[6] B. Chor, O. Goldreich, and J. Håstad. The random oracle hypothesis is false. Manuscript.

[7] A. Condon, J. Feigenbaum, C. Lund, and P. Shor. Probabilistically checkable debate systems and approximation algorithms for PSPACE-hard functions. In *Proceedings of the Twenty-Fifth ACM Symposium on Theory of Computing*, pages 305–314. ACM, 1993.

[8] A. Condon, J. Feigenbaum, C. Lund, and P. Shor. Random debators and the hardness of approximating stochastic functions. DIMACS Technical Report 93-79, Rutgers University, Piscataway, NJ, 1993.

[9] L. Fortnow. Oracles, proofs, and checking. Unpublished Manuscript, July 1993.

[10] L. Fortnow and M. Sipser. Are there interactive proofs for co-NP languages? *Information Processing Letters*, 28:249–251, 1988.

[11] S. Goldwasser, S. Micali, and C. Rackoff. The knowledge complexity of interactive proof systems. *SIAM Journal of Computing*, 18(1):186–208, 1989.

[12] J. Hartmanis. Solvable problems with conflicting relativizations. *Bulletin of the EATCS*, 27, 1985.

[13] J. Hartmanis, R. Chang, S. Chari, D. Ranjan, and P. Rohatgi. Relativization: A revisionistic retrospective. *Bulletin of the EATCS*, 47, 1992.

[14] J. Hartmanis, R. Chang, J. Kadin, and Mitchell. Some observations about relativization of space bounded computations. *Bulletin of the EATCS*, 35, 1988.

[15] J. Hartmanis and R. E. Stearns. On the computational complexity of algorithms. *Transactions of the American Mathematical Society*, 117:285–306, 1965.

[16] H. Heller. *Relativized Polynomial Hierarchy Extending Two Levels.* PhD thesis, Universität München, 1981.

[17] S. Kurtz. On the random oracle hypothesis. *Information and Control*, 57(1):40–47, April 1983.

[18] C. Lund, L. Fortnow, H. Karloff, and N. Nisan. Algebraic methods for interactive proof systems. *Journal of the ACM*, 39(4):859–868, 1992.

[19] M. O. Rabin and D. Scott. Finite automata and their decision problems. In E. F. Moore, editor, *Sequential Machines: Selected Papers*, pages 63–91. Addison-Wesley, 1964.

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