Theoretical Computer Science 81 (1991) 35-47
Elsevier

Polynomial-time reducibilities and "almost all" oracle sets*

Shouwen Tang

Department of Theoretical Computer Science, Beijing Computer Institute, Beijing 100040, People's Rep. China

Ronald V. Book

Department of Mathematics, University of California, Santa Barbara, CA 93106, USA

Communicated by J. Diaz
Received May 1988
Revised November 1988, February 1989

Abstract

Tang, S. and R.V. Book, Polynomial-time reducibilities and "almost all" oracle sets, Theoretical Computer Science 81 (1991) 35-47.

It is shown for every $k>0$ and for almost every tally set T, $\{A \mid A \leqslant^{\mathrm{P}}_{k\text{-tt}} T\} \neq \{A \mid A \leqslant^{\mathrm{P}}_{(k+1)\text{-tt}} T\}$. In contrast, it is shown that for every set A, the following holds: (a) for almost every set B, $A \leqslant^{\mathrm{P}}_{\mathrm{m}} B$ if and only if $A \leqslant^{\mathrm{P}}_{(\log n)\text{-T}} B$; and (b) for almost every set B, $A \leqslant^{\mathrm{P}}_{\mathrm{tt}} B$ if and only if $A \leqslant^{\mathrm{P}}_{\mathrm{T}} B$.

1. Introduction

The subject of this paper is the properties of polynomial-time reducibilities with respect to "almost all oracle sets". There are two parts. In the first part we study the classes of sets reducible *to* oracle sets by different reducibilities computed in polynomial time, and in the second part we study the classes of oracle sets reducible *from* arbitrary sets by different reducibilities.

In computational complexity theory, the study of reducibilities to almost all oracle sets appears to have first been studied by Bennett and Gill [3] in their work on the "random oracle hypothesis" and, more generally, on probabilistic arguments about complexity classes. (We make no claims about the random-oracle hypothesis, which has been refuted in several different ways.) More recently, arguments about

* The research reported in this paper was supported in part by the National Science Foundation under Grant CCR-8611980. This paper was written while the first author visited the Department of Mathematics, University of California, Santa Barbara.

reducibilities to almost all oracle sets have arisen in the study of interactive proof systems and in attempts to connect that work with more traditional approaches to computational complexity theory, e.g., structural complexity theory. In this context the work of Babai and Moran [2], Schöning [7], and Tang and Watanabe [9] has provided motivation for the present paper. Of particular importance for the questions studied here is the paper of Ambos-Spies [1].

Recall that the class of sets with polynomial-size circuits has been characterized as the class of sets that are Turing reducible in polynomial time to sparse sets or to tally sets. For any type R of reducibility and any class $\mathbf{C}$ of sets, $P_R(\mathbf{C})$ denotes $\{A \mid \text{there exists } C \in \mathbf{C} \text{ such that } A \leq_R^{\mathrm{P}} C\}$; thus, if we let SPARSE denote the class of all sparse sets and TALLY denote the class of all tally sets, then the class of sets with polynomial-size circuits is precisely $P_{\mathrm{T}}(\text{SPARSE}) = P_{\mathrm{T}}(\text{TALLY})$. Book and Ko [4] showed that the class of sets with polynomial-size circuits can be decomposed into a properly infinite hierarchy when considering the class SPARSE and the various bounded truth-table reducibilities computed in polynomial time: for every $k > 0$, $P_{k\text{-tt}}(\text{SPARSE})$ is properly included in $P_{(k+1)\text{-tt}}(\text{SPARSE})$. On the other hand, reducing sets to tally sets results in a collapse if only the bounded truth-table reducibilities are considered: $P_{\mathrm{m}}(\text{TALLY}) = P_{\mathrm{btt}}(\text{TALLY})$. In the latter case, Book and Ko observed that for every set A, if T_1 is a tally set (i.e., a set on a one-letter alphabet) such that $A \leq_{\mathrm{btt}}^{\mathrm{P}} T_1$, then there is a tally set T_2 such that $A \leq_{\mathrm{m}}^{\mathrm{P}} T_2$. This does not mean that for every tally set T, $P_{\mathrm{btt}}(T) = P_{\mathrm{m}}(T)$; in fact, we show that for almost every tally set T, this equality is false.

We show that when considering the polynomial-time reductions to almost every tally oracle set, the crucial parameter is the number of questions asked in nonadaptive reducibilities. We make this formal by showing that for every $k > 0$ and for almost every tally set T, there is a set A such that $A \leq_{(k+1)\text{-tt}}^{\mathrm{P}} T$ but $A \not\leq_{k\text{-tt}}^{\mathrm{P}} T$, that is, $P_{k\text{-tt}}(T) \neq P_{(k+1)\text{-tt}}(T)$. Hence, for almost every tally set T, the classes $P_{\mathrm{m}}(T)$, $P_{1\text{-tt}}(T), \ldots, P_{k\text{-tt}}(T), \ldots$ form a properly infinite hierarchy of classes. The analogous result holds for sets over an arbitrary alphabet (instead of a one-letter alphabet); essentially the same proof method can be used.

Having studied the classes of sets that are polynomial reducible to a given set, we consider the classes of sets reducible from a given set. This theme appears to have been considered first by Simon and Gill [8], who studied "upwards diagonalizations" and showed that if $A \notin \mathrm{P}$, then for any two types R, S of reducibilities from $\{1\text{-tt}, \ldots, k\text{-tt}, \ldots, \text{btt}, \text{tt}, \mathrm{T}\}$, the classes $\{B \mid A \leq_R^{\mathrm{P}} B\}$ and $\{B \mid A \leq_S^{\mathrm{P}} B\}$ are different, i.e., there exists a witness to the inequality $\{B \mid A \leq_R^{\mathrm{P}} B\} \neq \{B \mid A \leq_S^{\mathrm{P}} B\}$. We study the following question: for a given set A, how many sets witness the inequality $\{B \mid A \leq_R^{\mathrm{P}} B\} \neq \{B \mid A \leq_S^{\mathrm{P}} B\}$?

We consider the polynomial-time reductions from a set over the alphabet $\{0, 1\}$ to almost every oracle set, and we show that there is no difference between the adaptive and the nonadaptive polynomial-time reducibilities (and no difference between random oracle sets that are from the alphabet $\{0, 1\}$ and random tally oracle sets). The only parameter that plays a role is whether there is a $\mathrm{O}(\log n)$ bound or a polynomial bound on the number of oracle queries. We make this formal by proving that for every set A, the following hold:

(a) for almost every set B, $A \leq_{\mathrm{m}}^{\mathrm{P}} B$ if and only if $A \leq_{(\log n)\text{-T}}^{\mathrm{P}} B$;

(b) for almost every set B, $A \leq_{\mathrm{tt}}^{\mathrm{P}} B$ if and only if $A \leq_{\mathrm{T}}^{\mathrm{P}} B$.

Part (a) is related to a result of Ambos-Spies characterizing membership in the class P, while part (b) is related to a result of Bennett and Gill and of Ambos-Spies characterizing membership in BPP.

We conclude from this result that for any set A, the sets witnessing $\{B \mid A \leq_{\mathrm{m}}^{\mathrm{P}} B\} \neq \{B \mid A \leq_{(\log n)\text{-T}}^{\mathrm{P}} B\}$ are very rare since this collection has measure 0; the same thing is true for any other pair of different bounded truth-table reducibilities. In addition, we see that for any set A, the sets witnessing $\{B \mid A \leq_{\mathrm{tt}}^{\mathrm{P}} B\} \neq \{B \mid A \leq_{\mathrm{T}}^{\mathrm{P}} B\}$ are very rare since this collection has measure 0; but the situation is different if we restrict attention to tally sets since for *every* tally set T, $A \leq_{\mathrm{tt}}^{\mathrm{P}} T$ if and only if $A \leq_{\mathrm{T}}^{\mathrm{P}} T$.

There is an apparent exception to the remarks made above to the effect that it is only the $\mathrm{O}(\log n)$ bound or polynomial bound on the number of oracle queries that makes the difference. We show that for every set A, $A \in \mathrm{P}$ if and only if for almost every set B, $A \leq_{\mathrm{ctt}}^{\mathrm{P}} B$ if and only if for almost every set B, $A \leq_{\mathrm{dtt}}^{\mathrm{P}} B$; where ctt and dtt denote (unbounded) conjunctive and disjunctive truth-table reducibilities, respectively. However, the proof shows that in each case these reducibilities may be taken to be bounded.

To prove the results described in the last paragraphs, we use results on "random-oracle sets" developed by Bennett and Gill [3] and Ambos-Spies [1]. Much of the work in the present paper is motivated by the recent results of Tang and Watanabe [9].

2. Preliminaries

In this section we review some definitions and establish notation.

We wi'' consider strings over the alphabet $\Sigma = \{0, 1\}$. The set of all finite strings over Σ is denoted by Σ^* and the set of all one-way infinite sequences over Σ is denoted by Σ^ω. We assume an enumeration $e = w_0 < w_1 < w_2 < \cdots$ of Σ^* based on the dyadic representation of the nonnegative integers. The length of a string x will be denoted by $|x|$. The cardinality of a set S will be denoted by $\|S\|$. For a set S and an integer n, $S^n = \{x \in S \mid |x| = n\}$ and $S^{\leq n} = \{x \in S \mid |x| \leq n\}$. For a set S, χ_S denotes the characteristic function of S, and $\bar{S} = \Sigma^* - S$. A *tally* set is any subset of $\{0\}^*$; let TALLY denote the class of all tally sets.

Let $B \subseteq \Sigma^*$. The *characteristic sequence* $\alpha_B = b_0 b_1 \ldots$ of B is an element of Σ^ω such that $b_n = 1$ if and only if $w_n \in B$ (where Σ^* is enumerated as $w_0, w_1, \ldots$). For an element $\alpha \in \Sigma^\omega$, B_α is the set with characteristic function α.

Let T be a tally set. The *tally characteristic sequence* $\tau_T = b_0 b_1 \ldots$ of T is an element in Σ^ω such that $b_n = 1$ if and only if $0^n \in T$. For an element $\alpha \in \Sigma^\omega$, T_α is the tally set with tally characteristic function α.

We will identify a (tally) set with its (tally) characteristic sequence.

For $z \in \Sigma^*$, let $R_z = \{z\}\Sigma^\omega = \{T \in \text{TALLY} \mid \tau_T = z\delta \text{ for some } \delta \in \Sigma^\omega\}$. Thus, R_z is a "rectangular" infinite product in Σ^ω; such an infinite product will be referred to as a *basic rectangle.*

We denote by $\langle\ ,\ \rangle$ some pairing function $\Sigma^* \times \Sigma^* \to \Sigma^*$ that can be computed in polynomial time and has the property that when restricted to $\{0\}^* \times \{0\}^*$ takes values in $\{0\}^*$. Abusing the notation, we also use $\langle\, ,\dots,\rangle$ to denote tuples of objects; this should cause no difficulty for the reader since it will be clear from the context what is intended.

Define $\lambda(0) = \lambda(1) = \frac{1}{2}$ on Σ, making Σ into a probability space. By taking the completion of the infinite product on this probability space, we have the measure λ on Σ^ω. Two measures ν and μ are defined so that for any class $\boldsymbol{C}$ of sets ($\boldsymbol{T}$ of tally sets), $\nu(\boldsymbol{C})$ ($\mu(\boldsymbol{T})$) is a real number in the interval $[0, 1]$; these measures on Σ^ω correspond to the measure λ on Σ, which can be interpreted as the Lebesgue measure on the interval $[0, 1]$ if one identifies the element in Σ^ω with the real number in $[0, 1]$ in the usual way. That is, for a class $\boldsymbol{C}$ of sets, $\nu(\boldsymbol{C}) = \lambda(\{\alpha \mid B_\alpha \in \boldsymbol{B}\})$, and for a class $\boldsymbol{T}$ of tally sets, $\mu(\boldsymbol{T}) = \lambda(\{\alpha \mid B_\alpha \in \boldsymbol{T}\})$. The different notations, ν and μ, are used to emphasize the difference between the notion of a characteristic sequence and a tally characteristic sequence.

It will be useful to have notation for the conditional probability of a property of sets (or sets of strings). We will use the following: For a predicate P and natural number m, $\Pr_m[y : P(y)]$ is the conditional probability $\Pr[P/\Sigma^m] = 2^{-m} \times \|\{y \mid |y| = m \text{ and } P(y)\}\|$.

Bennett and Gill [3] used a version of the 0-1 law from probability theory. In this context we use the following version: if a measurable class of sets is closed under finite variation, then its measure is either 0 or 1. This provides justification for claiming that if $\boldsymbol{T}$ is a class of tally sets such that $\mu(\boldsymbol{T}) = 1$, we say that the property identifying $\boldsymbol{T}$ holds for *almost every tally set.* Similar comments will be made when referring to a class of subsets of Σ^*.

For an oracle machine M, $L(M, A)$ denotes the set of strings accepted by M relative to oracle set A, and $L(M) = L(M, \emptyset)$ denotes the set of strings accepted by M when no oracle queries are made (or allowed). For every set A, the collection $\{L(M, A) \mid M$ is a deterministic oracle machine that runs in polynomial time$\}$ is denoted by $P(A)$. Set B is *Turing-reducible* to set A in polynomial time, denoted $A \leqslant^{\mathrm{P}}_{\mathrm{T}} B$, if $A \in P(B)$.

Let PF denote the class of functions computable in polynomial time by deterministic machines.

We are concerned with "bounded truth-table reducibilities" that are computed in polynomial time [6]:

(i) set A is *many-one reducible* to set B, $A \leqslant^{\mathrm{P}}_{\mathrm{m}} B$, if there is a function $f \in \text{PF}$ such that for all x, $x \in A$ if and only if $f(x) \in B$;

(ii) for each $k > 0$, set A is *k-truth-table reducible* to set B, $A \leqslant^{\mathrm{P}}_{k\text{-tt}} B$, if there exist f and g in PF such that for all x, $f(x)$ is a list of k strings, $g(x)$ is a truth-table with k variables, and $x \in A$ if and only if the truth-table $g(x)$ evaluates to **true** on the k-tuple $\langle \chi_B(y_1), \ldots, \chi_B(y_k) \rangle$ where $f(x) = \langle y_1, \ldots, y_k \rangle$;

(iii) set A is *bounded truth-table reducible* to set B, $A \leq_{\mathrm{btt}}^{\mathrm{P}} B$, if there is an integer k such that $A \leq_{k\text{-tt}}^{\mathrm{P}} B$;

(iv) set A is *truth-table reducible* to set B if there exist f and g in PF such that for all x, $f(x)$ is a list of strings, say k many strings, $g(x)$ is a Boolean circuit with k inputs, and $x \in A$ if and only if the truth-table $g(x)$ evaluates to **true** on the k-tuple $\langle \chi_B(y_1), \ldots, \chi_B(y_k) \rangle$ where $f(x) = \langle y_1, \ldots, y_k \rangle$.

For any reducibility R and any class $\boldsymbol{C}$ of sets, let $P_R(\boldsymbol{C}) = \{A \mid \text{there exists } C \in \boldsymbol{C} \text{ such that } A \leq_R^{\mathrm{P}} C\}$.

We will use the following facts.

Lemma 2.1. *For any set A and any reducibility R, $\mu(\{T \in \mathrm{TALLY} \mid A \leq_R^{\mathrm{P}} T\}) = 1$ implies $\nu(\{B \subseteq \Sigma^* \mid A \leq_R^{\mathrm{P}} B\}) = 1$, that is, if for almost every tally set T, $A \leq_R^{\mathrm{P}} T$, then for almost every set B, $A \leq_R^{\mathrm{P}} B$.*

Proof (*sketch*). Notice that for any $\alpha \in \Sigma^\omega$, $A \leq_R^{\mathrm{P}} T_\alpha$ implies that $A \leq_R^{\mathrm{P}} B_\alpha$. □

Lemma 2.2. *If $\boldsymbol{T}$ is a class of tally sets such that $\mu(\boldsymbol{T}) > 0$, then there is a basic rectangle R_z such that $\mu(\boldsymbol{T} \cap R_z) > \frac{3}{4}\mu(R_z)$.*

For this paper, the appropriate references for the facts about random sets and measurability of sets are [3, 9].

3. Reductions to a set

It seems reasonable to assume that asking more questions of an oracle set will produce more information. Book and Ko showed that this is not true if one considers the sets reducible to the class of tally sets, i.e., $P_{\mathrm{m}}(\mathrm{TALLY}) = P_{\mathrm{btt}}(\mathrm{TALLY})$. The proof of Book and Ko showed that for every set A and every tally set T_1, if $A \leq_{\mathrm{btt}}^{\mathrm{P}} T_1$, then there is a tally set T_2 such that $A \leq_{\mathrm{m}}^{\mathrm{P}} T_2$.

In this section we show that for almost every tally set, the assumption holds: for almost every tally set T, the class of sets that are bounded truth-table reducible to T in polynomial time forms a properly infinite hierarchy depending on the number of questions asked. This is the main result of this section. There is no similar result concerning truth-table vs. Turing reducibilities to tally sets since for every set A and every tally set T, $A \leq_{\mathrm{tt}}^{\mathrm{P}} T$ if and only if $A \leq_{\mathrm{T}}^{\mathrm{P}} T$.

We begin with a result that is more restricted than the main result but has the advantage of being constructive.

Theorem 3.1. *There is a recursive tally set T such that $P_{\mathrm{m}}(T) \neq P_{1\text{-tt}}(T)$ and for every $k>0$, $P_{k\text{-tt}}(T) \neq P_{(k+1)\text{-tt}}(T)$.*

Proof. Let $f_j^{(0)}$, $j=0,1,2,\ldots$, be an effective enumeration of all many-one reductions, i.e., all functions in PF. Then $A \leqslant_{\mathrm{m}}^{\mathrm{P}} B$ if and only if there exists a j such that for all x, $x \in A$ if and only if $f_j^{(0)}(x) \in B$.

For each integer $k>0$, let $(f_j^{(k)}, g_j^{(k)})$, $j=0,1,2,\ldots$ be an effective enumeration of all pairs of k-tt generators $f_j^{(k)} \in \mathrm{PF}$ and all k-tt evaluators $g_j^{(k)} \in \mathrm{PF}$. We say that $A \leqslant_{k\text{-tt}}^{\mathrm{P}} B$ via $(f_j^{(k)}, g_j^{(k)})$ if for all x, $x \in A$ if and only if $g_j^{(k)}(x, B(y_1), B(y_2), \ldots, B(y_k)) = 1$, where $(y_1, y_2, \ldots, y_k) = f_j^{(k)}(x)$. We say that $A \leqslant_{k\text{-tt}}^{\mathrm{P}} B$ if there exists a j such that $A \leqslant_{k\text{-tt}}^{\mathrm{P}} B$ via $(f_j^{(k)}, g_j^{(k)})$. For each j and k, we assume that the running time of a machine computing $f_j^{(k)}$ and $g_j^{(k)}$ is bounded above by a polynomial p_j.

We will define a sequence $A^{(0)}, A^{(1)}, A^{(2)}, \ldots$ of sets so that $A^{(0)} \in P_{1\text{-tt}}(T) - P_{\mathrm{m}}(T)$ and for each $k>0$, $A^{(k)} \in P_{(k+1)\text{-tt}}(T) - P_{k\text{-tt}}(T)$. For each $k>0$, we will define $A_\pi^{(k)}$, $\pi=0,1,2,\ldots$ with $A_\pi^{(k)} \subseteq A_{\pi+1}^{(k)}$, and then define $A^{(k)} := \bigcup_{\pi>0} A_\pi^{(k)}$. In addition, we will define a sequence T_π, $\pi=0,1,2,\ldots$, with $T_\pi \subseteq T_{\pi+1}$, and then define $T := \bigcup_{\pi>0} T_\pi$.

A pairing function $\langle\ ,\ \rangle$ allows for the enumeration of all pairs (k,m), $k \geqslant 0$, $m \geqslant 0$. Without loss of generality, assume that $\langle 0,0\rangle \neq 0$, $k+m \leqslant \langle k,m\rangle$, and $p_j(\langle n,n\rangle) < 2^n$.

Let $n[0]=1$ and $n[m+1]=2^{n[m]}$.

Stage 0: Let $A_0^{(i)} := \emptyset$ for every $i>0$, and let $T_0 := \emptyset$.

Stage π: Let $\pi = \langle k,j\rangle > 0$.

Case 1: $k \geqslant 1$. Consider the pair $(f_j^{(k)}, g_j^{(k)})$ acting on input $0^{\langle n[\pi],k\rangle}$. Let $(y_1, y_2, \ldots, y_k) = f_j^{(k)}(0^{\langle n[\pi],k\rangle})$. For each i, $1 \leqslant i \leqslant k$, let $b_i = T_{\pi-1}(y_i)$. (Once again, we identify a set with its characteristic function.)

If $g_j^{(k)}(0^{\langle n[\pi],k\rangle}, b_1, \ldots, b_k) = 1$, then let $T_\pi := T_{\pi-1}$, and let $A_\pi^{(i)} := A_{\pi-1}^{(i)}$ for every $i>0$.

If $g_j^{(k)}(0^{\langle n[\pi],k\rangle}, b_1, \ldots, b_k) = 0$, then let $T_\pi := T_{\pi-1} \cup \{0^{\langle n[\pi],t\rangle}\}$ where t is the minimal t' such that $1 \leqslant t' \leqslant k+1$ and $0^{\langle n[\pi],t'\rangle} \notin \{y_1, \ldots, y_k\}$, let $A_\pi^{(i)} := A_{\pi-1}^{(i)}$ for every $i>0$ with $i \neq k$, and let $A_\pi^{(k)} := A_{\pi-1}^{(k)} \cup \{0^{\langle n[\pi],k\rangle}\}$.

Case 2: $k=0$. If $f_j^{(0)}(0^{\langle n[\pi],0\rangle}) \in T_{\pi-1}$, then let $T_\pi := T_{\pi-1} \cup \{0^{\langle n[\pi],0\rangle}\}$, and let $A_\pi^{(i)} := A_{\pi-1}^{(i)}$ for each $i>0$. If $f^{(0)}(0^{\langle n[\pi],0\rangle}) \notin T_{\pi-1}$, then let $T_\pi := T_{\pi-1}$, and let $A_\pi^{(i)} := A_{\pi-1}^{(i)}$ for each $i>0$. (*End of stage* π).

Let $A^{(0)} = \bar{T}$, i.e., $A^{(0)} = \{0\}^* - T$. There are some simple points to observe.

(1) It is clear that $T \subseteq \{0\}^*$ and that for every $i>0$, $A^{(i)} \subseteq \{0\}^*$.

(2) For every $k>0$, each string in $A^{(k)}$ has the form $0^{\langle n,k\rangle}$, where for some π, $n = n[\pi]$. In addition, $0^{\langle n,k\rangle} \in A^{(k)}$ if and only if there exists j, $1 \leqslant j \leqslant k+1$, such that $0^{\langle n,j\rangle} \in T$; thus, $A^{(k)} \leqslant_{(k+1)\text{-tt}}^{\mathrm{P}} T$.

(3) The set T is recursive since the list of functions $f_j^{(k)}$, $j \geqslant 0$, and the list of functions $g_j^{(k)}$, $k \geqslant 0$, are effective enumerations.

These facts and the following claims yield the desired result.

Claim 1. *For all* $k>0$, $A^{(k)} \not\leq^{\mathrm{P}}_{k\text{-tt}} T$.

Proof. Assume to the contrary that there is an m such that $A^{(k)} \leq^{\mathrm{P}}_{k\text{-tt}} T$ via $(f^{(k)}_m, g^{(k)}_m)$. Let $\pi=\langle k, m\rangle$. Let $f^{(k)}_m(0^{\langle n[\pi],k\rangle})=(y_1,\ldots,y_k)$, and let $b_i=T(y_i)$ for each i, $1\leq i\leq k$. Then, by the definition of $A^{(k)} \leq^{\mathrm{P}}_{k\text{-tt}} T$ via $(f^{(k)}_m, g^{(k)}_m)$, it is the case that $0^{\langle n[\pi],k\rangle}\in A^{(k)}$ if and only if $g^{(k)}_m(0^{\langle n[\pi],k\rangle}, b_1,\ldots,b_k)=1$.

However, the construction in Case 1 of Stage π yields the fact that $0^{\langle n[\pi],k\rangle}\in A^{(k)}$ if and only if $g^{(k)}_m(0^{\langle n[\pi],k\rangle}, b_1,\ldots,b_k)=0$, a contradiction. □ (*Claim* 1).

Claim 2. *Then* $A^{(0)} \leq^{\mathrm{P}}_{\mathrm{1\text{-}tt}} T$ *but* $A^{(0)} \not\leq^{\mathrm{P}}_{m} T$.

Proof. Assume to the contrary that $A^{(0)} \leq^{\mathrm{P}}_{\mathrm{m}} T$ via $f^{(0)}_m$. Let $\pi=\langle 0, m\rangle$. It is immediate from the definition that $0^{\langle n[\pi],0\rangle}\in A^{(0)}=\bar{T}$ if and only if $f^{(0)}_m(0^{\langle n[\pi],0\rangle})\in T$.

However, the construction in Case 2 of Stage π yields the fact that $0^{\langle n[\pi],0\rangle}\in T$ if and only if $f^{(0)}_m(0^{\langle n[\pi],0\rangle})\in T$, a contradiction. □ (*Claim* 2).

This completes the proof of the theorem. □

The reader may observe that the witness $A^{(k)}\in P_{(k+1)\text{-tt}}(T)-P_{k\text{-tt}}(T)$ is such that $A^{(k)}\in P_{(k+1)\text{-dtt}}(T)$, where dtt denotes disjunctive truth-table reducibility.

Now we have the main result of this section. It should be observed that Theorem 3.2 gives a nonconstructive proof of Theorem 3.1.

Theorem 3.2. *For every* $k>0$ *and for almost every tally set* T, $P_{k\text{-tt}}(T)\neq P_{(k+1)\text{-tt}}(T)$. *That is, for every* $k>0$, $\mu(\{T\in \mathrm{TALLY} \mid P_{k\text{-tt}}(T)\neq P_{(k+1)\text{-tt}}(T)\})=1$.

Proof. Let $k>0$ be fixed. For every tally T, let

$$\mathrm{ODD}_T=\{0^n \mid \|\{0^n, 0^{n+1},\ldots,0^{n+k}\}\cap T\| \text{ is odd}\}.$$

It is clear that for every tally set T, $\mathrm{ODD}_T \leq^{\mathrm{P}}_{(k+1)\text{-tt}} T$. We will show that for almost every set T, $\mathrm{ODD}_T\notin P_{k\text{-tt}}(T)$.

Let (f, g) be a k-tt reduction that is computed in polynomial time; let $f=(f_1,\ldots,f_k)$. For every tally set T and every n, let $(f,g)^T(0^n)$ denote $g(0^n, T(f_1(0^n)),\ldots,T(f_k(0^n)))$. Observe that $(f,g)^T(0^n)$ is the result of the reduction in the sense that for any tally sets T_1, T_2, (f,g) witnesses $T_1 \leq^{\mathrm{P}}_{k\text{-tt}} T_2$ if and only if for all n, $T_1(0^n)=(f,g)^{T_2}(0^n)$.

For any n, if $\mathrm{ODD}_T(0^n)=(f,g)^T(0^n)$, then we say that ODD_T and $(f,g)^T$ *agree on* 0^n.

In order to prove the theorem, we will show the following.

(1) For any fixed k-tt reduction (f,g), the set $\{T\in\mathrm{TALLY} \mid (f,g)$ witnesses $\mathrm{ODD}_T \leq^{\mathrm{P}}_{k\text{-tt}} T\}$ has measure 0.

Since (f,g) is a fixed k-tt reduction, it is clear that the question of whether ODD_T and $(f,g)^T$ agree on some 0^n depends on only a finite subset of T. Let q be a polynomial with the properties that for all n, $|f_i(0^n)|\leq q(n)$ for each i, $1\leq i\leq k$, and

$n+k\leq q(n)$. Thus, $\{T\in \text{TALLY}\,|\,\text{ODD}_T$ and $(f,g)^T$ agree on $0^n\}\subseteq R_{y(1)}\cup\cdots\cup R_{y(m)}$, where for each i, $R_{y(i)}$ is the basic rectangle $y(i)\Sigma^{\omega}$, $m\geq 1$, the $y(i)$'s are distinct, and $|y(1)|=\cdots=|y(m)|=q(n)$. Hence, for any finite set $S\subset\{0\}^*$, $\{T\in \text{TALLY}\,|\,\text{ODD}_T$ and $(f,g)^T$ agree on each word in $S\}$ is a union of finitely many basic rectangles.

Claim. *Let n be fixed and let y be a string such that $|y|<n$. Then $\mu(\{T\in \text{TALLY}\,|\,\text{ODD}_T$ and $(f,g)^T$ agree on $0^n\}\cap R_y)=\frac{1}{2}\mu(R_y)$.*

Proof. Notice that $0^n\in \text{ODD}_T$ if and only if $\|\{0^n,0^{n+1},\ldots,0^{n+k}\}\cap T\|$ is odd. Because $(f,g)^T(0^n)$ queries T about only k words, there exists some word in $\{0^n,0^{n+1},\ldots,0^{n+k}\}$ that is not queried; we lose no generality by assuming that 0^{n+k} is such a word, that is, $0^{n+k}\notin\{f_1(0^n),\ldots,f_k(0^n)\}$. For any tally set $T\in R_y$, if T' and T differ only on 0^{n+k} (i.e., $T'=T\triangle\{0^{n+k}\}$), then $T'\in R_y$ and $(f,g)^T(0^n)=(f,g)^{T'}(0^n)$ but $\text{ODD}_{T'}(0^n)\neq\text{ODD}_T(0^n)$. Hence, exactly one of T and T' is in $\{T\in \text{TALLY}\,|\,\text{ODD}_T$ and (f,g) agree on $0^n\}\cap R_y$.

Let $R_y=R_{yz(1)}\cup\cdots\cup R_{yz(t)}$, where $|yz(1)|=\cdots=|yz(t)|=q(n)$ and $i\neq j$ implies $R_{yz(i)}\cap R_{yz(j)}=\emptyset$.

Since both $\text{ODD}_T(0^n)$ and $(f,g)^T(0^n)$ depend only on $T^{\leq q(n)}$, we have that for each i, either $R_{yz(i)}\subseteq\{T\,|\,\text{ODD}_T$ and $(f,g)^T$ agree on $0^n\}$ or $R_{yz(i)}\cap\{T\,|\,\text{ODD}_T$ and $(f,g)^T$ agree on $0^n\}=\emptyset$.

Suppose that for all j, $1\leq j\leq\frac{1}{2}t$, $yz(2j)$ and $yz(2j-1)$ differ only on the $(n+k)$th bit (so that $T\in R_{yz(2j-1)}$ if and only if $T\triangle\{0^{n+k}\}\in R_{yz(2j)}$).

By the analysis above we have $R_{yz(2j-1)}\subseteq\{T\in \text{TALLY}\,|\,\text{ODD}_T$ and $(f,g)^T$ agree on $0^n\}$ if and only if

$$R_{yz(2j)}\cap\{T\in \text{TALLY}\,|\,\text{ODD}_T \text{ and } (f,g)^T \text{ agree on } 0^n\}=\emptyset.$$

Thus, among the basic rectangles $R_{yz(1)},\ldots,R_{yz(t)}$, exactly one half are in $\{T\in \text{TALLY}\,|\,\text{ODD}_T$ and $(f,g)^T$ agree on $0^n\}$; each of the others is disjoint with that class.

This completes the proof of the Claim. □ (*Claim*).

Continuing with the proof of (1), choose $n_1<n_2<\cdots$ such that for each i, $n_{i+1}>q(n_i)$ and $n_{i+1}>n_i+k$. Let $C_i=\{T\in \text{TALLY}\,|\,\text{ODD}_T$ and $(f,g)^T$ agree on each of $0^{n_1},0^{n_2},\ldots,0^{n_i}\}$. This implies that $C_1\supseteq C_2\supseteq\cdots\supseteq\{T\in \text{TALLY}\,|\,(f,g)$ witnesses $\text{ODD}_T\leq^{\text{P}}_{k\text{-tt}}T\}$. By the Claim, we have $\mu(C_{i+1})=\frac{1}{2}\mu(C_i)$. Thus, $\mu(\{T\in \text{TALLY}\,|\,(f,g)$ witnesses $\text{ODD}_T\leq^{\text{P}}_{k\text{-tt}}T\})\leq\frac{1}{2}^i$ for all $i>0$, and so $\mu(\{T\in \text{TALLY}\,|\,(f,g)$ witnesses $\text{ODD}_T\leq^{\text{P}}_{k\text{-tt}}T\})=0$ as desired. Thus, (1) is established.

Notice that $\{T\in \text{TALLY}\,|\,\text{ODD}_T\leq^{\text{P}}_{k\text{-tt}}T\}=\bigcup\{T\in \text{TALLY}\,|\,(f,g)$ witnesses $\text{ODD}_T\leq^{\text{P}}_{k\text{-tt}}T\}$ where the union is taken over all pairs (f,g) that witness a k-tt reduction computed in polynomial time. From (1) we see that each set on the right-hand side of the equation has measure 0 and so $\{T\in \text{TALLY}\,|\,\text{ODD}_T\leq^{\text{P}}_{k\text{-tt}}T\}$ has measure 0, that is, $\mu(\{T\in \text{TALLY}\,|\,\text{ODD}_T\leq^{\text{P}}_{k\text{-tt}}T\})=0$. Hence, for almost every tally set T, $\text{ODD}_T\notin P_{k\text{-tt}}(T)$.

This completes the proof of the theorem. □

Using a similar argument it is easy to see that for almost every tally set T, $P_{\mathrm{m}}(T) \neq P_{1\text{-tt}}(T)$. Hence, we have the following result.

Corollary 3.3. *For almost every tally set T, the classes $P_{\mathrm{m}}(T)$, $P_{1\text{-tt}}(T), \ldots, P_{k\text{-tt}}(T), \ldots$ form a properly infinite hierarchy of classes.*

If one looks carefully at the proof of Theorem 3.2, then one can see that the $(k+1)$-tt reduction of ODD_T to T can be carried out by a machine that uses only $\log n$ work space. Thus, we note that restricting the work space in this way does not overcome the additional power gained by making one additional oracle query

A different (and more complicated) argument can be applied to show that for almost every tally set T, $P_{k\text{-tt}}(T) \neq P_{(k+1)\text{-ctt}}(T)$ for $k > 0$, where ctt denotes conjunctive truth-table reducibility.

In addition, the proof of Theorem 3.2 can be modified to show that the analogous result holds when sets over the alphabet $\{0, 1\}$ are used instead of sets over the alphabet $\{0\}$; that is, for almost every set B, $P_{k\text{-tt}}(B) \neq P_{(k+1)\text{-tt}}(B)$ for $k > 0$. The idea is to use the measure ν instead of μ and, for $A \subseteq \{0, 1\}^*$, to define ODD_A by $\{w_n \mid \|\{w_n, w_{n+1}, \ldots, w_{n+k}\} \cap A\| \text{ is odd}\}$. In addition, the notion of basic rectangle must be interpreted as $R_z = \{B \subseteq \Sigma^* \mid \alpha_B = z\delta \text{ for some } \delta \in \Sigma^{\omega}\}$.

While our interest here is in reducibilities computable in polynomial time, the proofs of Theorems 3.1 and 3.2 yield precisely the same results for the corresponding reducibilities computable in polynomial space.

4. Reductions from a set

In Section 3 we showed that for almost every tally set T, the class of sets that are bounded truth-table reducible to T in polynomial time forms a properly infinite hierarchy depending on the number of questions asked. This shows that for almost every tally set the "downward" reductions associated with the different bounded truth-table reducibilities are different. In this section we consider the "upward" reductions. We will concentrate on results concerning almost every set; but every theorem remains true if one changes "almost every set" to "almost every tally set."

Simon and Gill [8] showed that if $A \notin \mathrm{P}$, then for any two types r, s of reducibilities from $\{1\text{-tt}, \ldots, k\text{-tt}, \ldots, \text{btt}, \text{tt}, \text{T}\}$, the classes $\{B \mid A \leq_r^{\mathrm{P}} B\}$ and $\{B \mid A \leq_s^{\mathrm{P}} B\}$ are different, $\{B \mid A \leq_r^{\mathrm{P}} B\} \neq \{B \mid A \leq_s^{\mathrm{P}} B\}$; their proof involves constructing witnesses for the inequality. We consider the following question: for a given set A, how many sets witness the inequality $\{B \mid A \leq_r^{\mathrm{P}} B\} \neq \{B \mid A \leq_s^{\mathrm{P}} B\}$? We provide different answers to this question depending on the reducibilities. The single parameter that makes the difference in the answer is whether the number of oracle queries is $O(\log n)$ bounded or is bounded only by the polynomial running time.

Ambos-Spies [1] first observed that $A \in \mathrm{P}$ if and only if for almost every set B, $A \leq_{\mathrm{m}}^{\mathrm{P}} B$. We strengthen this in the first result.

Suppose that there is a deterministic polynomial-time bounded oracle machine M such that $L(M, B) = A$, and such that for some $c > 0$ and every input x, relative to any oracle set in M's computation on x there are at most $c \cdot \log n$ oracle queries. Then we write $A \leqslant^{\mathrm{P}}_{(\log n)\text{-T}} B$.

Theorem 4.1. *For every set A, $A \in \mathrm{P}$ if and only if for almost every set B, $A \leqslant^{\mathrm{P}}_{(\log n)\text{-T}} B$.*

Proof. Let $M_1, M_2, \ldots$ be an enumeration of the deterministic polynomial time-bounded oracle machines that witness $\leqslant^{\mathrm{P}}_{(\log n)\text{-T}}$.

Suppose that for almost every set B, $A \leqslant^{\mathrm{P}}_{(\log n)\text{-T}} B$, so that $\nu(\{B \mid A \leqslant^{\mathrm{P}}_{(\log n)\text{-T}} B\}) = 1$. Since $\{B \mid A \leqslant^{\mathrm{P}}_{(\log n)\text{-T}} B\} = \bigcup_i \{B \mid A = L(M_i, B)\}$, there is a fixed j such that $\nu(\{B \mid A = L(M_j, B)\}) > 0$. By usual amplification accompanying the 0-1 law, this means that we can assume that M_j is such that $\nu(\{B \mid A = L(M_j, B)\} > \frac{3}{4}$. We will write M for M_j.

We lose no generality by assuming that in any single computation, M never queries the oracle about the same string twice, and there is a fixed c such that for any input x every computation of M on x makes exactly $c \cdot \log|x|$ oracle queries.

Let $D = \{\langle x, y\rangle \mid y \in \{0,1\}^*,\ |y| = c \cdot \log|x|$, and y represents the answers to the sequence of queries made in an accepting computation of M on $x\}$. It is clear that $D \in \mathrm{P}$.

For any x and y with $|y| = c \cdot \log|x|$, let $C(x, y) = \{B \mid y$ represents the sequence of answers to the oracle queries in M's computation on input x relative to $B\}$. Thus, for any two sets B_1, B_2 in $C(x, y)$, M's computation on x relative to B_1 is exactly the same as M's computation on x relative to B_2. This means that for any fixed x and any y with $|y| = c \cdot \log|x|$, either $C(x, y) \subseteq \{B \mid A$ and $L(M, B)$ agree on $x\}$ or $C(x, y) \cap \{B \mid A$ and $L(M, B)$ agree on $x\} = \emptyset$. Hence, for any given x, $\{B \mid A$ and $L(M, B)$ agree on $x\} = C(x, y_1) \cup \cdots \cup C(x, y_m)$ for some $m > 0$ and some $y_1, \ldots, y_m$, where for each i, $|y_i| = c \cdot \log|x|$ and $i \neq j$ implies $y_i \neq y_j$.

It is easy to see that in the equation $\{B \mid A$ and $L(M, B)$ agree on $x\} = C(x, y_1) \cup \cdots \cup C(x, y_m)$, $y_i \neq y_j$ implies $C(x, y_i) \cap C(x, y_j) = \emptyset$ and for each i, $\nu(C(x, y_i)) = 2^{-(c \cdot \log|x|)}$. In addition, $\{B \mid A = L(M, B)\} \subseteq \{B \mid A$ and $L(M, B)$ agree on $x\}$. Hence, we have the following:

$$\begin{aligned} m \cdot 2^{-(c \cdot \log|x|)} &= \nu(\{B \mid A \text{ and } L(M, B) \text{ agree on } x\}) \\ &\geqslant \nu(\{B \mid A = L(M, B)\}) > \tfrac{3}{4}. \end{aligned}$$

Now, $\{y \mid A(x) = D(\langle x, y\rangle)\} \supseteq \{y_1, \ldots, y_m\}$ since if $B \in C(x, y_i)$, then $D(\langle x, y_i\rangle)$ agrees with $L(M, B)(x) = A(x)$. Therefore, $\Pr_{c \cdot \log|x|}[y : A(x) = D(\langle x, y\rangle)] > \frac{3}{4}$. Since $D \in \mathrm{P}$ and $\langle x, y\rangle \in D$ implies $|y| = c \cdot \log|x|$, there is a deterministic polynomial-time bounded machine M_0 that on input x can compute $\|\{y \mid \langle x, y\rangle \in D\}\| / c \cdot \log|x|$, and accept x if and only if this fraction is greater than $\frac{3}{4}$. Thus, M_0 witnesses A's membership in P. □

In the proof of Theorem 4.1, we constructed a language D in P with the property that more than $\frac{3}{4}$ of the y's with length $c \cdot \log|x|$ guarantee that $A(x)$ and $D(\langle x, y\rangle)$

agree. If we regard y as the nondeterministic choice in the computation on x, then $|y| = c \cdot \log|x|$ means that only O($\log n$) many nondeterministic steps are allowed. Kintala and Fischer [5] proved that allowing O($\log n$) many nondeterministic steps is equivalent to being deterministic when only polynomial running time is involved. Here we are using the idea that we can deterministically count the number of accepting paths for such a machine.

From Theorem 4.1, we have the following result.

Theorem 4.2. *For every set A, the following are equivalent*:

(a) $A \in \mathrm{P}$;

(b) *for almost every set B, $A \leqslant_{\mathrm{m}}^{\mathrm{P}} B$*;

(c) *for almost every set B, $A \leqslant_{\mathrm{btt}}^{\mathrm{P}} B$*;

(d) *for almost every set B, $A \leqslant_{(\log n)\text{-}\mathrm{T}}^{\mathrm{P}} B$.*

Now we consider reducibilities where the number of queries is bounded only by the polynomial running time. Recall the definition of the class BPP:

> $A \in \mathrm{BPP}$ if and only if there exists a nondeterministic Turing machine N_A such that for all x [$x \in A$ if and only if more than $\frac{3}{4}$ of N_A's computations on x are accepting, and $x \notin A$ if and only if less than $\frac{1}{4}$ of N_A's computations on x are accepting].

Bennett and Gill claimed that $A \in \mathrm{BPP}$ if and only if for almost every set B, $A \leqslant_{\mathrm{T}}^{\mathrm{P}} B$; later, Ambos-Spies gave a proof of this. We provide a small extension.

Theorem 4.3. *For every set A, the following are equivalent*:

(a) $A \in \mathrm{BPP}$;

(b) *for almost every set B, $A \leqslant_{\mathrm{tt}}^{\mathrm{P}} B$*;

(c) *for almost every set B, $A \leqslant_{\mathrm{T}}^{\mathrm{P}} B$.*

Proof. Tang and Watanabe showed that if $A \in \mathrm{BPP}$, then for almost every tally set T, $A \leqslant_{\mathrm{tt}}^{\mathrm{P}} T$. From Lemma 2.1, if for almost every tally set T, $A \leqslant_{\mathrm{tt}}^{\mathrm{P}} T$, then for almost every set B, $A \leqslant_{\mathrm{tt}}^{\mathrm{P}} B$. On the other hand, if for almost every set B, $A \leqslant_{\mathrm{tt}}^{\mathrm{P}} B$, then for almost every set B, $A \leqslant_{\mathrm{T}}^{\mathrm{P}} B$, so that $A \in \mathrm{BPP}$ by the result cited above. □

We apply these results as follows.

Theorem 4.4. *For every set A, the following hold*:

(a) *for almost every set B, $A \leqslant_{\mathrm{m}}^{\mathrm{P}} B$ if and only if $A \leqslant_{(\log n)\text{-}\mathrm{T}}^{\mathrm{P}} B$*;

(b) *for almost every set B, $A \leqslant_{\mathrm{tt}}^{\mathrm{P}} B$ if and only if $A \leqslant_{\mathrm{T}}^{\mathrm{P}} B$.*

Proof. Apply Theorem 4.2. If $A \in \mathrm{P}$, then for almost every set B, $A \leqslant_{\mathrm{m}}^{\mathrm{P}} B$ and $A \leqslant_{(\log n)\text{-}\mathrm{T}}^{\mathrm{P}} B$. If $A \notin \mathrm{P}$, then for almost every set B, $A \not\leqslant_{\mathrm{m}}^{\mathrm{P}} B$ (since $\nu(\{B \mid A \leqslant_{\mathrm{m}}^{\mathrm{P}} B\}) \neq 1$ if and only if $\nu(\{B \mid A \not\leqslant_{\mathrm{m}}^{\mathrm{P}} B\}) = 1$ if and only if for almost every set B, $A \not\leqslant_{\mathrm{m}}^{\mathrm{P}} B$). Similarly, if $A \notin \mathrm{P}$, then for almost every set B, $A \not\leqslant_{(\log n)\text{-}\mathrm{T}}^{\mathrm{P}} B$. Thus, (a) is proved. The proof of (b) is just the same only Theorem 4.3 is used. □

Thus, when considering upwards reduction to almost all oracle sets associated with an arbitrary set, there is no difference between the adaptive and the nonadaptive polynomial-time reducibilities and no difference between random oracle sets that are from the alphabet Σ and random tally oracle sets. The only parameter that plays a role is whether there is a bound of $O(\log n)$ or a polynomial bound on the number of oracle queries.

From Theorem 4.4(a) we see that for any set A, the collection of sets witnessing $\{B \mid A \leq_{\mathrm{m}}^{\mathrm{P}} B\} \neq \{B \mid A \leq_{\mathrm{btt}}^{\mathrm{P}} B\}$ has measure 0 so that such sets are very rare. The same thing is true for any other pair of different bounded truth-table reducibilities. From Theorem 4.4(b) we see that for any set A, the collection of sets witnessing $\{B \mid A \leq_{\mathrm{tt}}^{\mathrm{P}} B\} \neq \{B \mid A \leq_{\mathrm{T}}^{\mathrm{P}} B\}$ has measure 0 so that such sets are very rare.

Consider the collection of sets witnessing $\{B \mid A \leq_{\mathrm{m}}^{\mathrm{P}} B\} \neq \{B \mid A \leq_{\mathrm{T}}^{\mathrm{P}} B\}$. Since $A \in \mathrm{P}$ if and only if for almost every set B, $A \leq_{\mathrm{m}}^{\mathrm{P}} B$, and $A \in \mathrm{BPP}$ if and only if for almost every set B, $A \leq_{\mathrm{T}}^{\mathrm{P}} B$, we see that the collection of sets witnessing $\{B \mid A \leq_{\mathrm{m}}^{\mathrm{P}} B\} \neq \{B \mid A \leq_{\mathrm{T}}^{\mathrm{P}} B\}$ has measure 0 if $A \notin \mathrm{BPP}-\mathrm{P}$ and has measure 1 if $A \in \mathrm{BPP}-\mathrm{P}$ (provided $\mathrm{P} \neq \mathrm{BPP}$).

5. Conjunctive and disjunctive reducibilities

We have claimed that when considering upwards reductions to almost all oracle sets associated with an arbitrary set, there is no difference between the bounded and unbounded polynomial-time reducibilities. Here we present a result which on the surface appears to be a counterexample to that statement but whose proof shows that it is not.

Recall that set A is *conjunctive truth-table reducible* to set B *via* f in PF if for all x, $f(x)$ is a list of strings, say $y_1, \ldots, y_{k(x)}$, and $x \in A$ if and only if for each i, $1 \leq i \leq k(x)$, $y_i \in B$. Set A is *conjunctive truth-table reducible* to set B, $A \leq_{\mathrm{ctt}}^{\mathrm{P}} B$, if there exists f in PF such that A is conjunctive truth-table reducible to B via f.

Recall that set A is *disjunctive truth-table reducible* to set B *via* f in PF if for all x, $f(x)$ is a list of strings, say $y_1, \ldots, y_{k(x)}$, and $x \in A$ if and only if for some i, $1 \leq i \leq k(x)$, $y_i \in B$. Set A is *disjunctive truth-table reducible* to set B, $A \leq_{\mathrm{dtt}}^{\mathrm{P}} B$, if there exists an f in PF such that A is disjunctive truth-table reducible to B via f.

In both cases we are interested only in the case of polynomial-time reducibilities.

Theorem 5.1. *For every set A the following are equivalent*:

(a) $A \in \mathrm{P}$;

(b) *for almost every set B, $A \leq_{\mathrm{ctt}}^{\mathrm{P}} B$*;

(c) *for almost every set B, $A \leq_{\mathrm{dtt}}^{\mathrm{P}} B$.*

Proof. Since many-one reducibility is a special case of both conjunctive and disjunctive reducibility, the fact that (a) implies both (b) and (c) follows from Theorem 4.2.

Suppose that (b) is true. Then $\nu(\{B \mid A \leq^{\mathrm{P}}_{\mathrm{ctt}} B\}) = 1$ so that there exists a function $f \in \mathrm{PF}$ such that $\nu(\{B \mid A \leq^{\mathrm{P}}_{\mathrm{ctt}} B \text{ via } f\}) > 0$. If $f(x) = y_1{}^{\#} \ldots {}^{\#} y_{k(x)}$, then let set-$f(x) = \{y_1, \ldots, y_{k(x)}\}$. Let set-$f(A) = \bigcup \{\text{set-}f(x) \mid x \in A\}$.

From the definition notice that $A \leq^{\mathrm{P}}_{\mathrm{ctt}} B$ via f means that for all x, $x \in A$ if and only if set-$f(x) \subseteq B$, and, hence, implies that set-$f(A) \subseteq B$.

If set-$f(A)$ is finite, then set-$f(A)$ is in P so that $A \leq^{\mathrm{P}}_{\mathrm{ctt}}$ set-$f(A)$ via f implies that A is in P. Assume that set-$f(A)$ is infinite.

Notice that we have shown that $\{B \mid A \leq^{\mathrm{P}}_{\mathrm{ctt}} B \text{ via } f\} \subseteq \{B \mid \text{set-}f(A) \subseteq B\}$. By assumption, set-$f(A)$ is infinite so that $\nu(\{B \mid \text{set-}f(A) \subseteq B\}) = 0$; hence, $\nu(\{B \mid A \leq^{\mathrm{P}}_{\mathrm{ctt}} B \text{ via } f\}) = 0$, contradicting the choice of f. This means that set-$f(A)$ is finite.

Suppose that (c) is true. Notice that

(i) for almost every set B, $A \leq^{\mathrm{P}}_{\mathrm{dtt}} B$ if and only if,

(ii) for almost every set B, $\bar{A} \leq^{\mathrm{P}}_{\mathrm{ctt}} \bar{B}$ if and only if,

(iii) for almost every set B, $\bar{A} \leq^{\mathrm{P}}_{\mathrm{ctt}} B$ if and only if,

(iv) $\bar{A} \in \mathrm{P}$ (since (b) implies (a)) if and only if,

(v) $A \in \mathrm{P}$ (since P is closed under complementation). □

References

[1] K. Ambos-Spies, Randomness, relativizations and polynomial reducibilities, in: *Proc. 1st Conf. Structure in Complexity Theory*, Lecture Notes in Computer Science **223** (Springer, Berlin, 1986), 23-34.

[2] L. Babai and S. Moran, Arthur-Merlin games: a randomized proof system, and a hierarchy of complexity classes, *J. Comput. System. Sci.* **36** (1988) 254-276.

[3] D. 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 J. Comput.* **10** (1981) 96-113.

[4] R. Book and K. Ko, On sets truth-table reducible to sparse sets, *SIAM J. Comput.* **17** (1988) 903-919.

[5] C. Kintala and P. Fischer, Refining nondeterminism in relativized computation, *SIAM J. Comput.* **9** (1980) 46-53.

[6] R. Ladner, N. Lynch and A. Selman, A comparison of polynomial-time reducibilities, *Theoret. Comput. Sci.* **1** (1975) 103-123.

[7] U. Schöning, Probabilistic complexity classes and lowness, in: *Proc. 2nd IEEE Conf. Structure in Complexity Theory* (1987) 2-8.

[8] I. Simon and J. Gill, Polynomial reducibilities and upwards diagonalizations, in: *Proc. 9th ACM Symp. Theory of Computing* (1977) 186-194.

[9] S. Tang and O. Watanabe, On tally relativizations of BP-complexity classes, *SIAM J. Comput.* **18** (1989).