The Global Power of Additional Queries to Random Oracles

August 3, 1993

Ronald V. Book [*]
Department of Mathematics
University of California
Santa Barbara, CA ffD10G
U.S.A.

Jack H. Lutz[†]
Department of Computer Science
Iowa State University
Ames, IA F0011
U.S.A.

David M. Martin Jr. [†‡]
Department of Computer Science
Boston University
111 *Cummington Street*
Boston, MA 0 1F
U.S.A.

Abstract

It is shown that, for every $k \geq 0$ and every fixed algorithmically random language B, there is a language that is polynomial-time, truth-table reducible in $k+1$ queries to B but not truth-table reducible in k queries in *any* amount of time to *any* algorithmically random language C. In particular, this yields the separation $\mathrm{P}_{k\text{-}tt}(\mathrm{RAND}) \subsetneqq \mathrm{P}_{(k+1)\text{-}tt}(\mathrm{RAND})$, where RAND is the set of all algorithmically random languages.

This research was supported in part by National Science Foundation Grant CCR-8913584.

1 Introduction

*Will an algorithm have increased computational power when it is modified to be able to ask additional questions*ff ff*ne way of making this question precise is to consider it in the context of reducibilities computed by algorithms with bounds on their computational resources. In this paper, we investigate the phenomenon of increased access to oracle sets lending increased computational power for bounded truth-table reducibilities computed in polynomial time. We show that, in a strong global sense, if* ff*ust one more question can be asked of sets with* ff*maximum information content," then the class of problems that can be solved will indeed grow.*

ff*or each* $k \geq 1$ *and each language* A, *let* $P_{k-tt}(A)$ *denote the class of languages that are polynomial time truth-table reducible in* k *queries to* A. *It is well-known that there are languages* A *such that for every* $k \geq 1$, $P_{k-tt}(A)$ *is properly included in* $P_{(k+1)-tt}(A)$. *If the language* A *is restricted to the class of those having very low information content, say tally languages* (*languages over a one letter alphabet*), *or to the class of those having very high information content, say the* ff*algorithmically random" languages* (*in the sense of Martin-L*ff*f* ff11ff), *then this same phenomenon holds* (*see* ff1ff, *D*ff). (*The definition and some basic properties of algorithmic randomness are given in Section D.*)

The property of gaining more computational power by making additional queries can be extended from a ff*local" property of individual languages to a* ff*global" property of classes of languages.* ff*or each* $k \geq 1$ *and each class* $\mathcal{C}$ *of languages, let* $P_{k-tt}(\mathcal{C})$ *be the class of languages* B *such that for some* $A \in \mathcal{C}$, B *is polynomial-time truth-table reducible in* k *queries to* A. *In the case of languages with small information content,* ff*ook and* ff*o* ff ff *showed that for every* $k \geq 1$, $P_{k-tt}(SP\mathrm{ffff}S\mathrm{ff})$ *is properly included in* $P_{(k+1)-tt}(SP\mathrm{ffff}S\mathrm{ff})$, *where* $SP\mathrm{ffff}S\mathrm{ff}$ *denotes the class of all languages with some polynomial bound on the number of strings of each length. In the case of languages with high information content, the main result of the present paper shows the parallel result for the case of* $\mathrm{fff}N\mathrm{ff}$, *the class of algorithmically random languages* (*the class of languages with essentially maximum information content*)ff *for every* $k \geq 1$, $P_{k-tt}(\mathrm{fff}N\mathrm{ff})$ *is properly included in* $P_{(k+1)-tt}(\mathrm{fff}N\mathrm{ff})$. *The proof of the main result establishes an even stronger property*ff *for every* $k \geq 1$ *and every* $A \in \mathrm{fff}N\mathrm{ff}$, *there is a language* B *in* $P_{(k+1)-tt}(A)$ *with the property that* B *is not* k*-truth table reducible to any language in* $\mathrm{fff}N\mathrm{ff}$ *in any amount of time, that is,* $P_{(k+1)-tt}(A) \not\subseteq \mathrm{fffff}_{k-tt}(\mathrm{fff}N\mathrm{ff})$.

ff note of caution is in order. Languages in the class SPffffSff and also languages in the class ffffNff have the local property that increasing the number of queries to an individual language A in the class allows more computational power (i.e., $P_{k\text{-}tt}(A) \subsetneqq P_{(k+1)\text{-}tt}(A)$). In addition, the classes themselves have this property as a global property. This might suggest that for any class $\mathcal{C}$ of languages, if $\mathcal{C}$ has the local property, then $\mathcal{C}$ also has the corresponding global property. ffut this is known to be false. ffs noted above, the class of all tally languages, denoted TffLLff, has the local property, but it is known (see ff , 1ff) that TffLLff does not have the global propertyff for every k, $P_m(\mathrm{TffLLff})$ ff $P_{k-tt}(\mathrm{TffLLff})$ ff $P_{btt}(\mathrm{TffLLff})$.

It is important to note that while for each k, there is a recursive witness to the separation of $P_{(k+1)-tt}(\mathrm{SPffffSff})$ from $P_{k-tt}(\mathrm{SPffffSff})$ ff ff, the separation of $P_{(k+1)-tt}(\mathrm{ffffNff})$ from $P_{k-tt}(\mathrm{ffffNff})$ can have no recursive witness. This is because $P_{(k+1)-tt}(\mathrm{ffffNff}) \cap$ fffff ff P ffEff.

Section is devoted to preliminary definitions. In Section D, algorithmic randomness and the class ffffNff are considered and some useful properties are reviewed. The main result is presented in Section E.

2 Preliminaries

The Boolean value of a condition ψ is

$$\mathrm{ffff}\psi\mathrm{ffff}\ \mathrm{ff} \begin{cases} 1 & \text{if } \psi \\ 0 & \text{if not } \psi. \end{cases}$$

We write $\mathbf{N}$ for the set of nonnegative integers and $\mathbf{Z}^+$ for the set of positive integers.

We write $\{0,1\}^*$ for the set of all (finite, binary) strings and $\{0,1\}^\infty$ for the set of all (infinite, binary) sequences. The length of (number of bits in) a string $x \in \{0,1\}^*$ is denoted by $|x|$. The length of a sequence $x \in \{0,1\}^\infty$ is ∞. The empty string is the unique string λ of length 0 and, for $k \in \mathbf{N}$, $\{0,1\}^k$ ff $\{\, x \in \{0,1\}^* \mid |x|$ ff $k \,\}$. ffinally, $\{0,1\}^+$ ff $\{0,1\}^* - \{\lambda\}$.

If x is a string or sequence and $0 \le i \le j < |x|$, then $x$ff$i..j$ff is the string consisting of the i^{th} through j^{th} bits of x. In particular, if x is a string, then x ff $x$ff$0..|x|-1$ff. We write $x$ff$i$ff for $x$ff$i..i$ff, the i^{th} bit of a string or sequence x. ff prefix of a sequence $x \in \{0,1\}^\infty$ is a string of the form $x$ff$0..n-1$ff, where $n \in \mathbf{N}$. ffor $w \in \{0,1\}^*$ and $x \in \{0,1\}^\infty$, we write $w \sqsubseteq x$ to indicate that w is a prefix of x.

The standard enumeration of $\{0,1\}^*$ *is the sequence*

$$s_0 = \lambda, s_1 = 0, s_2 = 1, s_3 = 00, s_4 = 01, \cdots.$$

More generally, the standard enumeration of an infinite set $X \subseteq \{0,1\}^*$ *is the sequence* $x_0, x_1, \cdots$ *in which the elements of* X *appear first in order of length, then in lexicographic order.*

A language is a set $A \subseteq \{0,1\}^*$. *The characteristic sequence of a language* A *is the sequence* $\chi_A \in \{0,1\}^\infty$ *defined by* $\chi_A[n] = [\![s_n \in A]\!]$ *for all* $n \in \mathbf{N}$.

We fix a one-to-one pairing function $\langle , \rangle$ *from* $\{0,1\}^* \times \{0,1\}^*$ *onto* $\{0,1\}^*$ *that is computable in polynomial time. Then we extend this function to* k*-tuples for all* k *so that* $\langle , \rangle : (\{0,1\}^*)^k \to \{0,1\}^*$.

Given a number $k \in \mathbf{N}$, *a* k*-query function is a function* f *with domain* $\{0,1\}^*$ *such that, for all* $x \in \{0,1\}^*$,

$$f(x) = \langle f_0(x), ..., f_{k-1}(x) \rangle \in \{0,1\}^*.$$

Each $f_i(x)$ *is called a query of* f *on input* x, *and the* k*-tuple* $f(x)$ *is called a* k*-query list on input* x. *A* k*-truth table function is a function* g *with domain* $\{0,1\}^*$ *such that, for each* $x \in \{0,1\}^*$, $g(x)$ *is the encoding of a* k*-input,* 1*-output Boolean circuit. We write* $g(x)(w)$ *for the output of this circuit on input* $w \in \{0,1\}^k$. *A* $\leq^{\mathrm{P}}_{k-tt}$*-reduction is an ordered pair* (f,g) *such that* f *is a* k*-query function,* g *is a* k*-truth table function, and* f *and* g *are computable in polynomial time.*

Let $A, B \subseteq \{0,1\}^*$. *A* $\leq^{\mathrm{P}}_{k-tt}$*-reduction of* A *to* B *is a* $\leq^{\mathrm{P}}_{k-tt}$*-reduction* (f,g) *such that, for all* $x \in \{0,1\}^*$,

$$[\![x \in A]\!] = g(x)([\![f_1(x) \in B]\!] \cdots [\![f_k(x) \in B]\!]).$$

In this case we say that $A \leq^{\mathrm{P}}_{k-tt} B$ *via* (f,g). *We say that* A *is* $\leq^{\mathrm{P}}_{k-tt}$*-reducible to* B, *and write* $A \leq^{\mathrm{P}}_{k-tt} B$, *if there exists* (f,g) *such that* $A \leq^{\mathrm{P}}_{k-tt} B$ *via* (f,g). *For a language* $A \subseteq \{0,1\}^*$ *and a class of languages* $\mathcal{C} \subseteq \{0,1\}^\infty$,

$$P_{k\text{-}tt}(A) = \left\{ B \subseteq \{0,1\}^* \,\middle|\, B \leq^{\mathrm{P}}_{k-tt} A \right\}$$

and

$$P_{k\text{-}tt}(\mathcal{C}) = \bigcup_{A \in \mathcal{C}} P_{k\text{-}tt}(A).$$

We also use general k*-truth-table reductions, which only require the functions* f *and* g *to be computable. A* $\leq_{k-tt}$*-reduction is an ordered pair*

(f, g) *such that* f *is a* k*-query function,* g *is a* k*-truth table function, and* f *and* g *are computable. For a language* $A \subseteq \{0,1\}^*$ *and a class of languages* $\mathcal{C} \subseteq \{0,1\}^\infty$*, define*

$$\mathrm{fffff}_{k\text{-}tt}(A) = \{\, B \subseteq \{0,1\}^* \mid B \leq_{k-tt} A \,\}$$

and

$$\mathrm{fffff}_{k\text{-}tt}(\mathcal{C}) = \bigcup_{A \in \mathcal{C}} \mathrm{fffff}_{k\text{-}tt}(A).$$

Finally, let fffff *denote the class of all recursive (i.e., decidable) languages.*

3 Randomness, 1-Reductions, and Normality

In this section we review Martin-Löf's definition of algorithmic randomness, along with two well-known properties of random sequences that are used in this paper.

Recall that the characteristic sequence of a language $A \subseteq \{0,1\}^*$ *is the infinite binary sequence*

$$\chi_A = [\![s_0 \in A]\!][\![s_1 \in A]\!][\![s_2 \in A]\!]\cdots,$$

where $s_0, s_1, s_2, \cdots$ *is the standard enumeration of* $\{0,1\}^*$.

Definition. *The cylinder generated by a string* $w \in \{0,1\}^*$ *is*

$$\mathbf{C}_w = \{\, A \subseteq \{0,1\}^* \mid w \sqsubseteq \chi_A \,\}.$$

The cylinder generated by the special symbol $\top$ *is*

$$\mathbf{C}_\top = \emptyset.$$

Definition. *For* $w \in \{0,1\}^* \cup \{\top\}$*, the probability (or measure) of the cylinder* $\mathbf{C}_w$ *is*

$$Pr(\mathbf{C}_w) = \begin{cases} {}^{-|w|} & \text{if } w \in \{0,1\}^* \\ 0 & \text{if } w = \top. \end{cases}$$

Remark 3.1. *Note that* $Pr(\mathbf{C}_w)$ *is the probability that* $A \in \mathbf{C}_w$ *when a language* $A \subseteq \{0,1\}^*$ *is chosen probabilistically according to a random experiment in which an independent toss of a fair coin is used to decide whether* $x \in A$ *for each* $x \in \{0,1\}^*$.

Definition (*Martin-Löf* ff11ff). ff *constructive null cover of a set* Y *of languages is a computable function*

$$G \text{ ff } \mathbf{N}\times\mathbf{N}\to\{0,1\}^*\cup\{\top\}$$

such that, for each $k\in\mathbf{N}$,

(*i*) $Y\subseteq\bigcup_{l=0}^{\infty}\mathbf{C}_{G(k,l)}$ (*the covering condition*)ff *and*

(*ii*) $\sum_{l=0}^{\infty} Pr(\mathbf{C}_{G(k,l)})\leq\ ^{-k}$ (*the measure condition*).

ff *constructive null set is a set of languages that has a constructive null cover.*

Remark 3.2. ff*onditions* (*i*) *and* (*ii*) *of the above definition imply that the event* $A\in Y$ *occurs with probability at most* $\ ^{-k}$ *in the random experiment of* ff*emark D*.1. *Since this holds for all* k, *every constructive null set is a probability* 0 *event in this random experiment. The computability requirement on* G *then means that a constructive null set is a set of languages that* ff*has probability* 0 *in a constructively specifiable sense.*"

Intuitively, membership in a constructive null set is a very special (*unusual*) *property for a language to have, and random languages should not have such properties.*

Definition (*Martin-Löf* ff11ff). ff *language is algorithmically random* (*or, briefly, random*) *if it is not an element of any constructive null set. We write* fffNff *for the set of all algorithmically random languages.*

It is well known that the above definition is robust, in the sense that it is equivalent to subsequent definitions given by Levin ff10ff, *Schnorr* ff1*D*ff, ff*haitin* ff*F*ff, *Solovay* ff1*G*ff, *and Shen* ff1*E*, 1*F*ff.

Remark 3.3. ff*lgorithmically random languages exist. In fact, it is easy to see* ff11ff *that* fffNff *is a probability* 1 *event in the random experiment of* ff*emark D*.1.

Now we discuss an important closure property of fffNff *that we use in this paper.*

Definition (*Post* ff1 ff). ff *1-reduction is a function* h ff $\{0,1\}^* \rightarrow \{0,1\}^*$ *that is one-to-one and computable. If* A *and* B *are languages, then a 1-reduction of* A *to* B *is a* 1*-reduction* h *such that* ffff$x \in A$fff ff ffff$h(x) \in B$fff *for all* $x \in \{0,1\}^*$. *We write* $A \leq_1 B$ *via* h *to indicate that* h *is a* 1*-reduction of* A *to* B. *We say that* A *is 1-reducible to* B, *and write* $A \leq_1 B$, *if there exists* h *such that* $A \leq_1 B$ *via* h.

The following well-known fact follows directly from the definitions of algorithmic randomness and 1*-reducibility.*

Lemma 3.4. ffff$N$ff *is downward closed under* 1*-reductions. That is, if* $A \leq_1 B \in$ ffff$N$ff, *then* $A \in$ ffff$N$ff.

We also use the fact that random languages are normal. This notion, which is a minor variant of a property investigated by ff*orel, is developed in the following definitions.*

Definition. ff*or all* $x \in \{0,1\}^\infty$, $w \in \{0,1\}^+$, *and* $n \in \mathbf{Z}^+$, *define the* n^{th} *frequency of* w *in* x *by*

$$freq^{w,n}\, x \text{ ff } \frac{1}{n}\left|\{\, i \mid 0 \leq i < n \text{ and } x\text{ff}i|w|\,..\,(i+1)|w|-1\text{ff ff } w\,\}\right|,$$

where $|S|$ *denotes the cardinality of* S. *That is,* $freq^{w,n}\, x$ *is the frequency with which the string* w *occurs in the first* n *nonoverlapping blocks of length* $|w|$ *in* x.

Definition. ff*or* $x \in \{0,1\}^\infty$ *and* $w \in \{0,1\}^+$, *the limiting frequency of* w *in* x *is*

$$freq^{w}\, x \text{ ff } \lim_{n\rightarrow\infty} freq^{w,n}\, x,$$

provided that this limit exists.

Definition. *Let* $k \in \mathbf{Z}^+$. ff *language* $A \subseteq \{0,1\}^*$ *is k-normal, and we write* $A \in N$ffffM_k, *if for all* $w \in \{0,1\}^k$,

$$freq^{w}\, \chi_A \text{ ff } {}^{-k}.$$

ff *language* $A \subseteq \{0,1\}^*$ *is normal, and we write* $A \in N$ffff$M$, *if* A *is k-normal for all* $k \in \mathbf{Z}^+$. *That is,*

$$N\text{ffff}M \text{ ff } \bigcap_{k=1}^{\infty} N\text{ffff}M_k.$$

Remark 3.5. *Several properties similar to that defined above have been investigated under various terminologies over the years. ffnuth fffff surveys much of this work. The k-normality property defined above is the special case j ff 0 of ffnuth's ff(k,k)-distributivity."*

We use the following well-known fact.

Theorem 3.6. fffNff $\subseteq$ NffffM.

We do not know a single, direct reference for this fact, but it is well-known that every algorithmically random language is ffhurch-random fffff and that every ffhurch-random sequence is normal fffff.

In addition, the ffhampernowne sequence

$$x \text{ ff } 0\,1\,00\,01\,10\,11\,000\,001\,010\,011\,110\cdots,$$

formed by concatenating the elements of $\{0,1\}^*$ in standard order, is known to be normal fffff. Since x is clearly computable, it cannot be random, so fffNff *is a proper subset of* NffffM.

4 Main Result

In this section we prove our main result, namely, that for every $k \in \mathbf{N}$ and every language $A \in$ fffNff, there exists a language B with the following two properties.

(*i*) $B \le^{\mathrm{P}}_{(k+1)-tt} A$.

(*ii*) ff*or every language* $A' \in$ fffNff, $B \not\le\ _{k-tt} A'$.

That is, $B \in P_{(k+1)\text{-}tt}(A) -$ fffff $_{k\text{-}tt}$(fffNff).

ff*ur principal tool for proving this result is the notion of k-resolvability, which we now develop.*

Definition. *The limiting frequency of a language $A \subseteq \{0,1\}^*$ is*

$$freq\,A \text{ ff } freq^1\,\chi_A,$$

i.e., the limiting frequency of the string 1 *in the sequence* χ_A, *as defined in section D.*

Definition. *Let* $k \in \mathbf{N}$. ff *language* $A \subseteq \{0,1\}^*$ *is* k*-resolvable if there is a language* $B \leq_1 A$ *such that* $^k \cdot \mathit{freq}\, B \in \mathbf{N}$.

That is, A *is* k*-resolvable if there is a* 1*-reduction* h *such that the inverse image* B ff $h^{-1}(A)$ *has a limiting frequency that can be written as a rational number with denominator* ^{k}. *It is clear that if* A *is* k*-resolvable and* $k \leq k'$, *then* A *is also* k'*-resolvable. Intuitively, we regard a language that is* k*-resolvable as being* ff*coarse at level* k.*" The smaller the parameter* k *is, the coarser the* k*-resolvable language must be. (Similarly, D*0*-grit sandpaper is coarser than G*0*-grit sandpaper!)*

The following fact is obvious but useful.

Lemma 4.1. ff*or each* $k \in \mathbf{N}$, *the collection of* k*-resolvable languages is upward closed under* 1*-reductions. That is, if* $A \leq_1 B$ *and* A *is* k*-resolvable, then* B *is* k*-resolvable.*

The following two easy lemmas illustrate the notion of k*-resolvability.*

Lemma 4.2. ff*very recursive language is* 0*-resolvable.*

Proof. *Let* $A \in$ fffff. *Then* A *and its complement* A^c *are both r.e. languages, and at least one of these languages is infinite.*

- (i) *If* A *is infinite, then there is a* 1*-reduction* h *such that* A ff *range*(h). *In this case, we have* $\{0,1\}^* \leq_1 A$ *via* h *and freq*$\{0,1\}^*$ ff 1.
- (ii) *If* A^c *is infinite, then there is a* 1*-reduction* h' *such that* A^c ff *range*(h'). *In this case, we have* $\emptyset \leq_1 A$ *via* h' *and freq*$\,\emptyset$ ff 0.

ff*ither way,* A *is* 0*-resolvable.* □

Lemma 4.3. ff*very algorithmically random language is* 1*-resolvable, but not* 0*-resolvable.*

Proof. *Let* $A \in$ fff*N*ff. ff*y Theorem D.G,* A *is* 1*-normal, so freq* A ff $\frac{1}{2}$. *Since* $A \leq_1 A$, *it follows that* A *is* 1*-resolvable.*

To see that A *is not* 0*-resolvable, assume that* $B \leq_1 A$. *Then* $B \in$ fff*N*ff *by Lemma D.E, so* B *is* 1*-normal by Theorem D.G, so freq* B ff$\frac{1}{2} \notin \mathbf{N}$. *Thus* A *is not* 0*-resolvable.* □

The following terminology simplifies our discussion.

Definition. *For languages $B, X \subseteq \{0,1\}^*$ with X infinite, the X-selection of B is the language*

$$\sigma_X(B) = \{\, s_i \mid x_i \in B \,\},$$

where $s_0, s_1, \cdots$ is the standard enumeration of $\{0,1\}^*$ and $x_0, x_1, \cdots$ is the standard enumeration of X.

Observation 4.4. *Let $B, X \subseteq \{0,1\}^*$. If X is recursive and infinite, then $\sigma_X(B) \leq_1 B$ and $\sigma_X(B) \leq_1 B \cap X$.*

Now we move to the central part of our argument.

Lemma 4.5 (*Main Lemma*). *Let $k \in \mathbf{N}$ and $A, B \subseteq \{0,1\}^*$. If $A \in$ ffffNff and $B \leq_{k-tt} A$, then B is k-resolvable.*

Proof. *We proceed by induction on k.*

Basis *The case $k = 0$ follows immediately from Lemma E. .*

Induction Step *Assume that the statement holds for k, where $k \in \mathbf{N}$, that $A \in$ ffffNff, and that $B \leq_{(k+1)-tt} A$ via (f, g).*

For each $x \in \{0,1\}^*$, let

$$Q(x) = \{f_0(x), f_1(x), \cdots, f_k(x)\}$$

be the set of queries of f on input x. Define the sets

$$H = \left\{ x \in \{0,1\}^* \,\middle|\, |Q(x)| \leq k \right\}$$

and, for each $y \in \{0,1\}^*$,

$$V_y = \{\, x \in \{0,1\}^* \mid y \in Q(x) \,\}.$$

Thus H is the set of inputs on which f repeats a query and V_y is the set of inputs on which f queries y. Note that the sets H and V_y are all recursive.

It suffices to prove that B is $(k+1)$-resolvable in each of the following three cases.

Case 1. *H is infinite*

Case 2. *V_y is infinite for some $y \in \{0,1\}^*$.*

Case 3. *The sets H and V_y, for $y \in \{0,1\}^*$, are all finite.*

In Case 1, the reduction (f, g) can clearly be modified to make do with one fewer query on inputs in H, so $B \cap H \leq_{k-tt} A$. It follows by Observation

E.E that $\sigma_H(B) \leq_{k-tt} A$, whence $\sigma_H(B)$ is k-resolvable by the induction hypothesis. ffy ffbservation E.E and Lemma E.1, it follows that B is k-resolvable, hence certainly $(k+1)$-resolvable.

In ffase , fix $y \in \{0,1\}^*$ such that V_y is infinite. The answer to the query ffy $\in$ Aff" is constant, so the reduction (f, g) can be modified to make do with one fewer query on elements of V_y. Thus $B \cap V_y \leq_{k-tt} A$. It follows by ffbservation E.E that $\sigma_{V_y}(B) \leq_{k-tt} A$. ffy the induction hypothesis, this implies that $\sigma_{V_y}(B)$ is k-resolvable. Thus, by ffbservation E.E and Lemma E.1, B is k-resolvable, hence $(k+1)$-resolvable.

ffinally, assume that ffase D holds. Then for each finite set $S \subseteq \{0,1\}^*$, the set

$$\widetilde{S} \text{ ff } H \cup \left(\bigcup_{x \in S} \bigcup_{y \in Q(x)} V_y \right)$$

is finite. ffix a truth table τ ff $\{0,1\}^{k+1} \rightarrow \{0,1\}$ such that the set

$$T \text{ ff } \{\, x \in \{0,1\}^* \mid g(x) \text{ ff } \tau \,\}$$

is infinite. ffor each finite set $S \subseteq \{0,1\}^*$, let $u(S)$ be the first element of the infinite set $T - \widetilde{S}$ in the standard enumeration of $\{0,1\}^*$. ffefine a language U ff $\bigcup_{i=0}^{\infty} U_i$ by the recursion

$$U_0 \text{ ff } \emptyset, \qquad U_{i+1} \text{ ff } U_i \cup \{u(U_i)\}.$$

It is easy to check that U has the following properties.

(i) U is infinite and recursive.

(ii) $U \subseteq T$.

(iii) $U \cap H$ ff $\emptyset$.

(iv) ffor all $x, y \in U$, if $x \not{\text{ff}}\, y$, then $Q(x) \cap Q(y)$ ff $\emptyset$.

Let $u_0, u_1, \cdots$ be the standard enumeration of U. ffefine the language

$$D \text{ ff } \{\, s_n \mid f_r(u_q) \in A \,\},$$

where q and r are the quotient and remainder, respectively, when n is divided by $k+1$. That is, for $q \in \mathbf{N}$ and $0 \leq r \leq k$, $s_{q(k+1)+r}$ is an element of D if and only if the r^{th} query of f on input u_q is an element of A. Properties (i), (iii), and (iv) above ensure that the function $s_n \mapsto f_r(u_q)$ is one-to-one *and recursive, so* $D \leq_1 A$. *Since* $A \in \mathrm{RAND}$, *it follows by Lemma D.E and Theorem D.G that* $D \in \mathrm{RAND} \subseteq \mathrm{NORM}_{k+1}$. *Let* $W \subseteq \{0,1\}^{k+1}$ *be the support of the truth table* τ, *i.e.,*

$$W = \left\{ w \in \{0,1\}^{k+1} \,\middle|\, \tau(w) = 1 \right\}.$$

Intuitively, the membership (or nonmembership) of each string s_i *in* $\sigma_U(B)$ *is determined, via the truth table* τ, *by the membership (or nonmembership) in* D *of the elements of the* i^{th} *nonoverlapping block of* $k+1$ *consecutive strings in the standard enumeration of* $\{0,1\}^*$. *That is, for all* $i \in \mathbf{N}$, *property (ii) tells us that*

$$\begin{aligned} s_i \in \sigma_U(B) &\iff u_i \in B \\ &\iff \tau([\![f_0(u_i) \in A]\!] \cdots [\![f_k(u_i) \in A]\!]) = 1 \\ &\iff [\![f_0(u_i) \in A]\!] \cdots [\![f_k(u_i) \in A]\!] \in W \\ &\iff [\![s_{i(k+1)} \in D]\!] \cdots [\![s_{i(k+1)+k} \in D]\!] \in W \\ &\iff \chi_D[i(k+1)..i(k+1)+k] \in W. \end{aligned}$$

Recalling that D *is* $(k+1)$*-normal, it follows that*

$$\mathit{freq}\,\sigma_U(B) = \sum_{w \in W} \mathit{freq}^w \chi_D = |W| \cdot 2^{-(k+1)}.$$

It follows by property (i) above and Observation E.E that B *is* $(k+1)$*-resolvable.*

This completes the proof of the Main Lemma. □

Recall that our objective is to prove that, for every $k \in \mathbf{N}$ *and* $A \in \mathrm{RAND}$, *there is a language* $B \in \mathrm{P}_{(k+1)\text{-}tt}(A) - \mathrm{P}_{k\text{-}tt}(\mathrm{RAND})$. *By Lemma E.F, this can be achieved by exhibiting a language* $B \leq^{\mathrm{P}}_{(k+1)-tt} A$ *that is not* k*-resolvable. The following definition provides such a language.*

Definition. *For* $k \in \mathbf{N}$, *the* k*-fold conjunction of a language* $A \subseteq \{0,1\}^*$ *is the language*

$$\wedge^{(k)} A = \left\{ x \in \{0,1\}^* \,\middle|\, (\forall 0 \leq i < k)\, x10^i \in A \right\}.$$

(Note that, vacuously, $\wedge^{(0)} A = \{0,1\}^*$*.)*

We need just one more lemma.

Lemma 4.6. *Let $k \in \mathbf{N}$. If $A \in \mathrm{ffff}N\mathrm{ff}$ and $C \leq_1 \wedge^{(k)}A$, then $\mathit{freq}\,C \;\mathrm{ff}\; {}^{-k}$.*

Proof. *If $k \;\mathrm{ff}\; 0$, then $\wedge^{(k)}A \;\mathrm{ff}\; \{0,1\}^*$ and this is trivial, so assume that $k > 0$. Assume that $C \leq_1 \wedge^{(k)}A$ via h and define the language*

$$D \;\mathrm{ff}\; \{ s_n \in \{0,1\}^* \mid h(s_q)10^r \in A \},$$

where q and r are the quotient and remainder obtained when n is divided by k. Then $D \leq_1 A$, so D is k-normal by Lemma D.E and Theorem D.G. In particular, this implies that

$$\mathit{freq}^{1^k}\chi_D \;\mathrm{ff}\; {}^{-k}.$$

Also, for all $i \in \mathbf{N}$,

$$\begin{aligned} \mathrm{ffff}_i s \in C\,\mathrm{ffff} \;&\mathrm{ff}\; \mathrm{ffff}h_i()s \in \wedge^{(k)}A\,\mathrm{ffff} \\ &\mathrm{ff}\; \mathrm{ffff}(\forall 0 \leq r < k)\, h(s_i)10^r \in A\,\mathrm{ffff} \\ &\mathrm{ff}\; \mathrm{ffff}(\forall 0 \leq r < k)\, s_{ki+r} \in D\,\mathrm{ffff} \\ &\mathrm{ff}\; \mathrm{ffff}\chi_D\mathrm{ff}ki..k(i+1)-1\mathrm{ff}\;\mathrm{ff}\;1^k\mathrm{ffff}, \end{aligned}$$

so

$$\mathit{freq}\,C \;\mathrm{ff}\; \mathit{freq}^{1^k}\chi_D \;\mathrm{ff}\; {}^{-k}.$$

□

Now we have our main result.

Theorem 4.7 (*Main Theorem*). *For all $k \in \mathbf{N}$ and $A \in \mathrm{ffff}N\mathrm{ff}$,*

$$P_{(k+1)\text{-}tt}(A) \not\subseteq \mathrm{fffff}_{k\text{-}tt}(\mathrm{ffff}N\mathrm{ff}).$$

Thus, for all $k \in \mathbf{N}$,

$$P_{k\text{-}tt}(\mathrm{ffff}N\mathrm{ff}) \subsetneqq P_{(k+1)\text{-}tt}(\mathrm{ffff}N\mathrm{ff}).$$

Proof. *Let $k \in \mathbf{N}$ and $A \in \mathrm{ffff}N\mathrm{ff}$. Let $B \;\mathrm{ff}\; \wedge^{(k+1)}(A)$. It is clear that $B \in P_{(k+1)\text{-}tt}(A)$. On the other hand, Lemma E.G tells us that, for all $C \leq_1 B$, ${}^k \cdot \mathit{freq}\,C \;\mathrm{ff}\; {}^k \cdot {}^{-(k+1)} \;\mathrm{ff}\; 1/ \notin \mathbf{N}$, so B is not k-resolvable. It follows by the Main Lemma that $B \notin \mathrm{fffff}_{k\text{-}tt}(\mathrm{ffff}N\mathrm{ff})$. Thus $B \in P_{(k+1)\text{-}tt}(A) - \mathrm{fffff}_{k\text{-}tt}(\mathrm{ffff}N\mathrm{ff})$.* □

In the course of proving the above result, we have shown that, for $k \in \mathbf{N}$ and $A \in \mathrm{ffff}N\mathrm{ff}$, the language $\wedge^{(k+1)}A$ is $(k+1)$-resolvable but not k-resolvable. It is interesting to note that, when $k \;\mathrm{ff}\; 0$, this is precisely Lemma E.D.

Acknowledgments

We thank ff*harles* ff*ennett and Steve* ff*aut*ff *for helpful discussions.*

References

ff1ff *J. L.* ff*alcá*ff*ar, J.* ff*ía*ff*, and J.* ff*abarró, Structural Complexity I, Springer-*ff*erlag,* 1fffff.

ff ff ff. ff*ook and* ff.-*I* ff*o,* ff*n sets truth-table reducible to sparse sets, SIAM Journal on Computing* **17** (1fffff), *pp.* ff0*D*ffff1ff.

ff*D*ff ff. ff. ff*ook,* ff*dditional queries and algorithmically random languages, In* ff. ff*mbos-Spies, S.* ff*omer, and U. Sch*ff*ning, editors, Complexity Theory.* ff*ambridge University Press,* 1fff*D*, *to appear.*

ff*E*ff ff. ff. ff*ook, J.* ff. *Lut*ff*, and* ff. *Wagner,* ff*n observation on probability versus randomness with applications to complexity classes, Mathematical Systems Theory* (1fff*D*), *to appear.*

ff*F*ff ff. *J.* ff*haitin,* ff *theory of program si*ff*e formally identical to information theory, Journal of the Association for Computing Machinery* **22** (1fff*F*), *pp. D* fff*DE*0.

ff*G*ff ff. *J.* ff*haitin, Incompleteness theorems for random reals, Advances in Applied Mathematics* **8** (1fffff), *pp.* 11ffff1*EG*.

fffff ff. ff. ff*hampernowne,* ff*onstruction of decimals normal in the scale of ten, J. London Math. Soc.* **2** (1ff*DD*), *pp. FE*ff *G*0.

fffff ff*onald* ff. ff*nuth, The Art of Computer Programming, volume* , ff*ddison-Wesley,* 1ff*GG*.

fffff ff. *N.* ff*olmogorov and* ff. ff. *Uspenskii,* ff*lgorithms and randomness, translated in Theory of Probability and its Applications* **32** (1fffff), *pp. D*fffff*E*1 .

ff10ff *L.* ff. *Levin,* ff*n the notion of a random sequence, Soviet Mathematics Doklady* **14** (1fff*D*), *pp.* 1*E*1*D*ff1*E*1*G*.

ff11ff *P. Martin-L*ff*f,* ff*n the definition of random sequences, Information and Control* **9** (1ff*GG*), *pp. G*0 ff*G*1ff.

ff1 ff ff. L. Post, *Recursively enumerable sets of positive integers and their decision problems*, Bulletin of the American Mathematical Society **50** (1ffEE), pp. ffEffD1G.

ff1Dff ff. P. Schnorr, *Process complexity and effective random tests*, Journal of Computer and System Sciences **7** (1ffffD), pp. DffGffDffff.

ff1Eff ff. ffh. Sheh, *The frequency approach to the definition of a random sequence*, Semiotika i Informatika (1ffff), pp. 1EffE , in Russian.

ff1Fff ff. ffh. Sheh, *On relations between different algorithmic definitions of randomness*, Soviet Mathematics Doklady **38** (1fffff), pp. D1GffD1ff.

ff1Gff ff. M. Solovay, 1ffffF, reported in ffGff.

ff1ffff S. Tang and ff. Book, *Polynomial-time reducibilities and "almost-all" oracle sets*, Theoretical Computer Science **81** (1fff1), pp. DFffEff.