Mathematics Department

ON HONEST POLYNOMIAL REDUCTIONS, RELATIVIZATIONS, AND P=NP.

R. Downey, W. Gasarch, S. Homer, & M. Moses

Research Report 89-37 March 1989

Victoria University of Wellington

P.O. BOX 600, WELLINGTON, NEW ZEALAND

to appear proceeding
"Structure in Complexity, 1989

On Honest Polynomial Reductions, Relativizations, and P=NP

by

Rod Downey
Department of Math
Victoria Univ. of Wellington
P.O. Box 600
Wellington, New Zealand

William I. Gasarch
Department of Comp. Sci.
Inst. for Adv. Comp. Studies
University of Maryland
College Park, MD 20742

Steven Homer
Department of Comp. Sci.
Boston University
Boston, MA, 02215

Michael Moses
Department of Comp. Sci.
Victoria Univ. of Wellington
P.O. Box 600
Wellington, New Zealand

ABSTRACT

We prove a number of structural theorems about the honest polynomial m-degrees, contingent on the assumption P = NP(or a unary alphabet). The ultimate goal would be to prove a contradiction from P = NP. We show that several types of sets cannot be minimal with respect to honest polynomial reduction, in particular, low sets and index sets cannot be minimal. We show that some theorems about honest polynomial reductions do not relativize, hence techniques in this area may be able to resolve the P=NP question (more humbly, they are not automatically ruled out from doing so). Lastly, we examine an alternative definition of honest m-reduction under which recursive minimal sets can be constructed.

1) Introduction

Homer [11] has shown connections between the P=NP question and the existence of sets that are minimal with respect to honest Turing reductions (henceforth "hT-minimal"). Informally, these reductions are polynomial Turing reductions where the strings queried cannot be "short" compared to the input length. Homer proved that if P=NP then there exist such minimal sets. Homer and Long [10,18] have simplified the original construction, showed that the P=NP assumption can be omitted if $|\Sigma| = 1$, and have proven partial converses by showing that several classes of sets cannot be minimal. Ambos-Spies [2] later simplified and extended their work. Homer, Long, and Ambos-Spies have also shown that there exists a set that is minimal with respect to honest m-reductions.

There are several motivations guiding work in this area. One motivation is that by deriving consequences from P=NP we may learn more about the P = NP? problem (ultimately we would like to derive a contradiction, though this seems unlikely). A second motivation is that there may be a converse to the statement "if P=NP then there exists a minimal set" (or some variation of the statement) that yields a statement about honest degrees that is equivalent to P = NP.

Throughout this paper, all results that can be obtained with P=NP as a hypothesis are also true in the context of tally sets (i.e. if $|\Sigma| = 1$). The proofs in the $|\Sigma| = 1$ case are similar to those in the P=NP case and are omitted. The reader should keep in mind that even though a theorem needs P=NP as a hypothesis, there is an analogous result with $|\Sigma| = 1$ that is absolute.

In this paper we pursue four goals.

- We push the P=NP hypothesis: Assuming P=NP we prove many structural theorems about the honest polynomial m-degrees. The proofs use techniques from the theory of the m-degrees in recursion theory [12,13,21].
- We exhibit several classes of sets that cannot be minimal. Ambos-Spies [2] showed that every high r.e. Turing degree (i.e., a degree a such that $a' \equiv_T 0''$) contains an r.e. hT-minimal set; and asked if non-high degrees can contain such. We give a partial negative answer by showing that low sets (i.e. sets A such that $A' \equiv_T \emptyset'$) are nonminimal. (The proof actually shows that semilow sets are nonminimal.)
  Our proof is an interesting extension of Ladner's proof that there are no recursive hm-minimal sets. It is best described as a finite injury delayed diagonalization. Our techniques can be used to prove other results as well. In addition, we show that index sets are nonminimal.
- Most results in structural complexity theory directly relativize, that is, if a theorem is proved, its proof holds for computations relative to an arbitrary oracle set. Since there exists sets A and B such that $P^A = NP^A$ and $P^B \neq NP^B$ [3], techniques that relativize will not suffice to resolve P = NP?. Techniques that do not relativize are of interest since they may be useful in resolving P = NP? We show that theorems about honest reductions need not relativize. In particular, we exhibit two statements that involve honest reductions, which are true relative to the empty oracle, but false relative to an oracle which we construct.
- We clarify the distinction between honest m-reductions and total honest m-reductions. An m-reduction from A to B is a function $f \in$P such that $x \in A$ iff $f(x) \in B$. A natural definition of an honest m-reduction would appear to be to require f is honest; however, Ambos-Spies has defined honest m-reduction such that f is allowed to map a string into $\{YES, NO\}$. We call the former definition a *total honest m-reduction* (and denote it $\leq_m^{h\text{-}to}$) and the latter just an *honest m-reduction* (and denote it $\leq_m^h$). We show that these two reductions differ in an interesting way. Ladner showed [14] that there are no recursive sets that are hm-minimal. We show, by contrast, that there are recursive sets that are $hmto$-minimal. Hence Ladner's theorem does not hold for total honest m-reductions. This is also of interest because all minimal degrees

constructed so far have been (necessarily) nonrecursive. The recursive *hmto*-minimal set is actually *superminimal*, i.e. for *all* B such that $B \leq_m^{h\text{-}to} A$, $B \equiv_m^{h\text{-}to} A$. The existence of superminimal sets is evidence that Ambos-Spies' definition of honest m-reduction actually is natural.

In Section 2 we review motivation, definitions, and notation that will be used throughout this paper. In Sections 3 through 7 we examine the four topics in detail.

2) Motivations, Definitions, and Notation

Many concepts and techniques of complexity theory are based on similar notions in recursion theory. Often these concepts are later seen to be of interest for reasons independent of their original motivation (e.g. Schoning's definition of high and low sets in NP [24]). The definition of an honest reduction is partially motivated by an attempt to examine an analog of minimal degrees; though it is of independent interest in complexity theory because of the connections to P=NP, discovered by Homer [11]. We review the recursion-theoretic motivation.

A nonrecursive set is $\leq_T$-minimal if for any set B such that $B \leq_T A$, either $B \equiv_T A$ or B is recursive. Spector [27] constructed a $\leq_T$-minimal set recursive in $\emptyset''$; later Sacks [23] constructed one recursive in $\emptyset'$. Here is a naive first attempt to define a minimal set in the context of complexity theory.

Attempted Definition: A set A is $\leq_T^p$-minimal if for any set B such that $B \leq_T^p A$, either $B \equiv_T^p A$ or $B \in$P.

There is one big problem with this definition: there are no $\leq_T^p$-minimal sets. If A is recursive and $A \notin$P then, by Ladner [14], there exists a set $B \notin$P such that $B <_T^p A$. If A is nonrecursive, then Homer [11] has shown that the set

$$B = \{z0^{2^{|z|}} \ : \ z \in A\}$$

is not in P (in fact, it is nonrecursive) and $B <_T^p A$. The set B is contrived as the 0's are there only for padding. Note that in the $B <_T A$ reduction, on input x we ask a question of A that is very short compared to $|x|$. This motivates us to study reductions where the questions asked are not allowed to be too short. We will need two preliminary definitions before defining a useful notion of minimal.

Definition : For a nondecreasing function q, a polynomial oracle Turing machine M is called *q-honest* if for all sets S and all x, if $M^S(x)$ queries oracle S about y, then $q(|y|) \geq |x|$.

Definition : Let A and B be sets. The set B is ***honest Turing reducible to*** A (written $B \leq_T^h A$) if there is a polynomial q and a q-honest oracle Turing machine $M^{()}$ such that $B \leq_T^p A$ via $M^{()}$. The set B is ***honest Turing equivalent to*** A (written $B \equiv_T^h A$) if $B \leq_T^h A$ and $A \leq_T^h B$. Note that $\equiv_T^h$ is an equivalence relation, and the equivalence classes are called honest Turing degrees (hT-degrees).

Note: Similar concepts have been studied by Machtey [19], Meyer and Ritchie [20], and Young [28].

Definition : A set $A \notin$P is ***hT-minimal*** if for any set B such that $B \leq_T^h A$, either $B \equiv_T^h A$ or $B \in$P.

In Ladner's proof, the reduction of B to A is honest, while in Homer's proof it is not. Hence there cannot be a recursive set that is hT-minimal. As mentioned in the introduction, if either P=NP or $|\Sigma| = 1$ then there is a (necessarily nonrecursive) hT-minimal set [11,18].

In both Ladner's and Homer's reductions of B to A, on every input at most one query to A is made. In the cases when no query is made, the machine just says YES or NO. This motivates the next definition.

Definition : Let A and B be sets. The set B is *honest m-reducible to A* (written $B \leq_m^h A$) if there exists a polynomial q and a function $f \in$P, $f : \Sigma^* \rightarrow \Sigma^* \cup \{YES, NO\}$, such that for all x :

1) if $f(x) = YES$ then $x \in A$,
2) if $f(x) = NO$ then $x \notin A$,
3) if $f(x) \in \Sigma^*$ then ($x \in B$ iff $f(x) \in A$),
4) if $f(x) \in \Sigma^*$ then $q(|f(x)|) \geq |x|$.

Definition : The definitions of $\equiv_m^h$, hm-degree, and hm-minimal are analogous to the definitions of $\equiv_T^h$, hT-degree, and hT-minimal, respectively.

This definition of honest m-reduction is not a direct analog of either m-reductions in recursion theory [22] or polynomial m-reductions [15]. This definition is used by Ambos-Spies [2] because by allowing YES and NO as outputs all sets in P are $\leq_m^h$-equivalent. We present a definition that appears more natural, but will turn out not to be.

Definition: Let A and B be two sets. The set B is *honest total m-reducible to A* (written $B \leq_m^{h\text{-}to} A$) if $B \leq_m^h A$ via a reduction f that cannot map to an element of $\{YES, NO\}$. The definitions of $\equiv_m^{h\text{-}to}$, *hmto*-degree, and *hmto*-minimal are similar to those of $\equiv_T^h$, hT-degree, and hT-minimal respectively. A set A is *hmto-superminimal* if for all sets B such that $B \leq_m^{h\text{-}to} A$, $B \equiv_m^{h\text{-}to} A$.

Note: In section 5 we will see that there exist superminimal sets $A \notin$P. This is somewhat unnatural since even for sets $B \in$P, have $B \not\leq_m^{h\text{-}to}$A.

We need a way to effectively represent the set of all $\leq_m^h$ reductions.

Notation: Let $M_1, M_2, M_3, \ldots$ be a list of all Turing machines, modified such that M_e runs in time $p_e(n) = n^e + e$; and on an input of length n either outputs a string of length m where $q_e(m) \geq n$, or outputs an element of $\{YES, NO\}$. For every e, let f_e be the function computed by M_e, and let V_e =range(f_e). If $A \subseteq \Sigma^*$ then Φ_e^A is the set that is $\leq_m^h$-reduced to A by M_e, namely

$$x \in \Phi_e^A \Leftrightarrow (f_e(x) \in A \text{ or } f_e(x) = YES).$$

For all e, M_e represents an $\leq_m^h$ reduction; and every $\leq_m^h$ reduction is represented by some M_e.

Notation: Let $P_1^{()}, P_2^{()}, P_3^{()}, \ldots$ be an effective enumeration of clocked oracle Turing machines, where $n^e + e$ bounds the runtime of $P_e^{()}$. If no oracle is written then the empty set is assumed to be the oracle. If we restrict some P_e to be 0-1 valued then $L(P_e)$ represents the set recognized by P_e.

Notation: Let $\varphi_1, \varphi_2, \varphi_3, \ldots$ be an acceptable programming system (e.g. an effective enumeration of Turing machines). Let W_e be the domain of φ_e, and $W_{e,s}$ be the enumeration of the first s elements of W_e (some may be repeated).

Convention: The term 'least string' means the least string in the lexicographic ordering on strings.

3) Honest Polynomial Partitions

In this section we define honest polynomial partitions and prove several lemmas about them. These lemmas will be the key to obtaining initial segments of the honest polynomial m-degrees.

Notation: If Π is a partition then $\Pi(x)$ is the set of elements in the same part as x, and $\mu\Pi(x)$ is the least element of $\Pi(x)$.

Definition: Let $B \subseteq \Sigma^*$ be a set in P. Π is an *honest polynomial partition of* B (henceforth '*hp* partition') if

a) there exists a polynomial p such that for all $x \in B$ the elements of $\Pi(x)$ can be determined in time $p(|x|)$.

b) there exists a polynomial q such that for all $x \in B$, $q(|\mu\Pi(x)|) \geq |x|$ (this is the polynomial honesty).

Note: p and q are called *the polynomials associated with* Π.

Definition: If Π is a partition of B and A is a set, then A *respects* Π if for every $x \in B$ either $\Pi(x) \subseteq A$ or $\Pi(x) \subseteq \Sigma^* - A$.

Lemma 1: (P = NP) Let $\Sigma^* = B \cup C \cup D$ be a partition of Σ^* such that B,C, and D are in P. Let A be a set such that $C \subseteq A$ and $D \subseteq \Sigma^* - A$. Let $e \in N$. If there exists an *hp* partition Π of B that A respects such that, for every $x \in B$, $\Pi(x) \cap W_e \neq \emptyset$, then $A \equiv_m^h \Phi_e^A$.

Proof:

Let Π be the partition and let p and q be the polynomials associated to Π. By definition f_e runs in p_e steps and is q_e-honest.

The following algorithm computes an $\leq_m^{h\text{-}to}$ reduction g of A to Φ_e^A.

ALGORITHM

1) Input(x).
2) If $x \in C$, then output(YES) and halt. If $x \in D$, then output(NO) and halt.
3) Compute $\Pi(x)$.
4) Using P=NP find a string y such that $f_e(y) \in \Pi(x)$. (We later show that y with $|y| \leq q_e(p(|x|))$ exists, so P=NP can be used.)
5) Output(y).

END OF ALGORITHM

Since Π respects A, for all $x \in B$

$$x \in A \Leftrightarrow f_e(y) \in A.$$

Since $\Phi_e^A \leq_m^h A$ via f_e

$$y \in \Phi_e^A \Leftrightarrow f_e(y) \in A.$$

Combining these two facts yields

$$x \in A \Leftrightarrow y \in \Phi_e^A.$$

Hence g reduces A to Φ_e^A. It remains to show that g is an $\leq_m^h$ reduction.

The only step in the algorithm for g that is not obviously polynomial time is step $\bar{3}$. Since $\Pi(x) \cap W_e \neq \emptyset$, y exists; but we have to show that $|y|$ is bounded by a polynomial. We show that $|y| \leq q_e(p(|x|)$ by showing that if not, then $f_e(y)$ is too large to be in $\Pi(x)$. Assume

$$q_e(p(|x|)) < |y|.$$

Since f_e is q_e honest,

$$q_e(|f_e(y)|) \geq |y|.$$

Combining these two inequalities yields

$$q_e(|f_e(y)|) > q_e(p(|x|)).$$

Since q_e is a strictly increasing function,

$$|f_e(y)| > p(|x|).$$

Since $f_e(y) \in \Pi(x)$, the string $f_e(y)$ has to be of length $\leq p(|x|)$, or else it could not be produced in time $p(|x|)$. Hence

$$|f_e(y)| \leq p(|x|).$$

This contradicts the previous inequality, hence $|y| \leq q_e(p(|x|))$. Lastly we show that g is honest. Let $x \in B$ and $g(x) = y \in \Sigma^*$. Since $f_e(y) \in \Pi(x)$,

$$q(|f_e(y)|) \geq |x|.$$

Since p_e bounds the complexity of f_e, $p_e(|y|) \geq |f_e(y)|$, hence

$$q(p_e(|y|)) \geq q(|f_e(y)|).$$

Combining these inequalities yields

$$q(p_e(|y|)) \geq |x|.$$

Hence g is $(q \circ p_e)$-honest. ⊠

Lemma 2: (P = NP): Let $\Sigma^* = B \cup C \cup D$ be a partition of Σ^* into three parts which are in P. Let S be some set in P. Let A be a set such that $C \subseteq A$ and $D \subseteq \Sigma^* - A$. Let $e \in N$. If there exists an *hp* partition Π of B that A respects such that

a) for every $x \in \Sigma^*$ if $f_e(x) \in B$ then $\Pi(f_e(x)) \cap S \neq \emptyset$, *b*) for every $y \in B \cap S$, $\Pi(y) \cap W_e \neq \emptyset$,

then $A \cap S \equiv_m^h \Phi_e^A$.

Proof:

$A \cap S \leq_m^h \Phi_e^A$ by a modification of the algorithm in Lemma 1. During step 4, instead of looking for y such that $f_e(y) \in \Pi(x)$, look for y such that $f_e(y) \in \Pi(x) \cap S$.

$\Phi_e^A \leq_m^h A \cap S$ by the following algorithm

ALGORITHM

1) Input(x).
2) If $f_e(x) = YES$, then output(YES). If $f_e(x) = NO$, then output(NO).
3) Compute $\Pi(f_e(x))$.
4) Find $y \in \Pi(f_e(x)) \cap S$.
5) Output(y).

END OF ALGORITHM

☒

4) The Structure of $\mathbf{H_m}$

We sketch a number of theorems about the structure of the *hm*-degrees, contingent on P = NP. Full proofs are in [7].

Notation: The partial order which has the *hm*-degrees as its underlying set, and $\leq_m^h$ as its ordering, is denoted by $\mathbf{H_m}$. The subordering consisting of *hm*-degrees that contain an r.e. set (and hence only r.e. sets) is denoted by $\mathbf{H_m} \cap \mathbf{RE}$.

Note: The partial orders $\mathbf{H_m}$ and $\mathbf{H_m} \cap \mathbf{RE}$ are distributive upper semilattices. The proof of this fact is similar to the proof that the (classical) *m*-degrees form a distributive upper semilattice [21].

Definition : A partial order $\langle X, \leq \rangle$ is an *initial segment of* $\mathbf{H_m}$ if there exists a 1-1 map $\rho : X \to \mathbf{H_m}$ such that range(ρ) is closed downward under $\leq_m^h$ and

$$x \leq y \Leftrightarrow \rho(x) \leq_m^h \rho(y).$$

The existence of an *hm*-minimal set (assuming P=NP) can be restated as "if P=NP then the two element chain is an initial segment of $\mathbf{H_m}$." We have obtained extensions along these lines: If P=NP then

- the topped finite initial segments of $\mathbf{H_m}$ are exactly the finite distributive lattices,
- the topped initial segments of $\mathbf{H_m}$ are exactly the direct limits of ascending sequences of finite distributive lattices,
- all recursively presentable distributive lattices are initial segments of $\mathbf{H_m} \cap \mathbf{RE}$.

All results also hold if Σ is unary, with proofs modified as in [18].

We show, in detail, that if P=NP then the three element chain is an initial segment of $\mathbf{H_m}$. Then we sketch the proofs of the three results stated above. The proofs can be found in detail in [7]. Using techniques of [18] the proofs of all three theorems can easily be adapted to the $|\Sigma| = 1$ case, omitting the P=NP assumption. We then examine whether or not $\mathbf{H_m}$ ($\mathbf{H_m} \cap \mathbf{RE}$) is elementarily equivalent to the m-degrees (r.e. m-degrees). We show that $\mathbf{H_m} \cap \mathbf{RE}$ is not elementarily equivalent to the r.e. m-degrees, though the problem for $\mathbf{H_m}$ versus the m-degrees is open.

We use a modification of exptally sets. These sets have been used for constructing minimal honest degrees by Homer, Long, and Ambos-Spies [2,18].

Definition : Let $g(0) = 1$ and for all $m \geq 0$, $g(m+1) = 2^{g(m)}$. A set A is *exptally* i $A \subseteq \{0^{g(m)} \mid m \in N\}$. Let p be a fixed polynomial. Define

$$E^p = \{0^{g(m)+j} \mid m \in N,\ 0 \leq j \leq p(m) - 1\}.$$

Sets of the form E^p are called *poly-exptally*. For any fixed m the finite set

$$B^m = \{0^{g(m)+j} \mid 0 \leq j \leq p(m) - 1\}$$

is called *the* m^{th} *block of* E^p.

Note: We will later be partitioning E^p by partitioning every block of it. The sets tha form the partition are called *boxes*. Each block will consist of a finite number of boxes.

Convention: Modify the machines $P_1, P_2, P_3, \ldots$ so that they are 0-1 valued. Let $L(P_e)$ denote the language recognized by P_e.

Theorem 3: (P = NP): The three element chain is a finite initial segment of $\mathbf{H_m}$.

Proof:

Let p be a fixed polynomial. Let

$$S_1 = \{0^{g(m)+j} \mid m \in N,\ 0 \leq j \leq p(m) - 1,\ j \text{ odd}\}$$
$$S_2 = \{0^{g(m)+j} \mid m \in N,\ 0 \leq j \leq p(m) - 1,\ j \text{ even}\}$$

We construct A such that the degrees of $\emptyset$, $A \cap S_2$, and A, form a 3-element chain $\mathbf{H_m}$. More precisely we construct $A \subseteq E^p$ in stages to satisfy the following requirement

$R_e^1 : A \cap S_2 \neq L(P_e)$
$R_e^2 : f_e$ is not a reduction of A to $A \cap S_2$
$R_e^3 : \Phi_e^A \in P$ or $\Phi_e^A \equiv_m^h A \cap S_2$ or $\Phi_e^A \equiv_m^h A$

At the end of each stage s we will have the following.

a) $A_s \in P$, the strings committed to A. $A \subseteq E^p$.
b) $\overline{A}_s$, the strings committed to $\Sigma^* - A$. (Note that $\overline{A}_s$ is not the complement of A_s.
c) for every m, B_s^m, the set of strings in B^m that are not committed to A or Σ^* –
Let $B_s = \cup_{m=1}^{\infty} B_s^m$.
d) Π_s, an hp partition of E^p such that
i) A will respect Π_s,
ii) if x and y are in different blocks, then $\Pi_s(x) \neq \Pi_s(y)$ (this makes Π_s p-honest
iii) as m increases, the number of boxes of Π_s in B_s^m that are wholly contained S_1 increases without bound. (Such boxes are needed to satisfy R_e^2 and are call *pure boxes*.)

During the construction we show inductively that $A_s \in \mathrm{P}$, $\overline{A}_s \in \mathrm{P}$, and that Π_s is an *hp* partition. The partitions get coarser and coarser; however if $x \in A_s$ or $x \in \overline{A}_s$ then for all $t \geq s$, $\Pi_t(x) = \Pi_s(x)$. For every $x \in E^p$ there is a stage s such that either $x \in A_s$ or $x \in \overline{A}_s$. The set A is defined as the set of all x that are placed in some A_s. The set A will respect all partitions Π_s.

If at stage $s+1$, A_s ($\overline{A}_s$, Π_s) is not mentioned, then $A_{s+1} := A_s$ ($\overline{A}_{s+1} := \overline{A}_s, \Pi_{s+1} := \Pi_s$).

CONSTRUCTION

Stage 0: $A_0 := \emptyset$. $\overline{A}_0 := \Sigma^* - E^p$. For all x, $\Pi_0(x) = \{x\}$.

Stage $s+1 = 3e+1$ (Satisfy R_e^1): Let x be the shortest element of E^p such that $x \notin A_s \cup \overline{A}_s$. If $P_e(x) = 1$ then $\overline{A}_{s+1} := \overline{A}_s \cup \Pi_s(x)$, else $A_{s+1} := A_s \cup \Pi_s(x)$.

Stage $s+1 = 3e+2$ (Satisfy R_e^2): Let x be the shortest element of E^p such that $x \notin A_s \cup \overline{A}_s$ and $\Pi(x) \cap S_2 = \emptyset$. (Such an x exists inductively). There are four cases

1) $f_e(x) \in A_s$. Let $\overline{A}_{s+1} := \overline{A}_s \cup \Pi_s(x)$.
2) $f_e(x) \in \overline{A}_s$. Let $A_{s+1} := A_s \cup \Pi_s(x)$.
3) $f_e(x) \notin A_s \cup \overline{A}_s$ and $f_e(x) \in \Pi_s(x)$. Let $A_{s+1} := A_s \cup \Pi_s(x)$.
4) $f_e(x) \notin (A_s \cup \overline{A}_s \cup \Pi_s(x))$. Let $A_{s+1} := A_s \cup \Pi_s(x)$ and $\overline{A}_{s+1} := \overline{A}_s \cup \Pi_s(f_e(x))$.
   (Note that in case 3, $x \in A$ but $f_e(x) \notin S_2$, so $f_e(x) \notin A \cap S_2$).

Stage $s+1 = 3e+3$ (Satisfy R_e^3): There are three cases.

1) There exists a constant c such that for all m, the number of boxes in B_s^m that intersect V_e is less than c. Set

$$A_{s+1} := A_s \cup \bigcup_{x \in V_e \cap B_s} \Pi_s(x).$$

Since we are assuming $\mathrm{P} = \mathrm{NP}$, $V_e \in$P. Inductively, Π_s is an honest partition, $B_s \in$P, and $A_s \in$P. Since $V_e \subseteq A_{s+1} \subseteq A$, $\Phi_e^A \in$P.

2) There exists a constant c such that for all m the number of pure boxes in B_s^m that intersect V_e is less than c. (Recall that a box b is pure if $b \subseteq S_1$.) Since we are not in case 1), the number of impure boxes in B_s^m that intersect V_e is unbounded.

We intend to set A_{s+1}, $\overline{A}_{s+1}$, and Π_{s+1} such that the following hold.

a) For every $x \in \Sigma^*$ if $f_e(x) \in B_{s+1}$ then $f_e(x)$ is in the same box as some $y \in S_2$.
b) For every $y \in B_{s+1} \cap S_2$, $\Pi_{s+1} \cap V_e \neq \emptyset$.

By Lemma 2 these two conditions make $A \cap S_2 \equiv_m^h \Phi_e^A$.

We set A_{s+1}, $\overline{A}_{s+1}$, and Π_{s+1} as follows. For every m, let $\langle b_1, \ldots, b_k \rangle$ be all the boxes induced by Π_s that contain elements of B_s^m (and therefore only elements of B_s^m). For $1 \leq i \leq k$ do the following. If b_i is a pure box that intersects V_e then place all the elements of b_i into A_{s+1}. If $b_i \cap V_e \cap S_2 \neq \emptyset$ then let b_i be the j^{th} such box and let b be the j^{th} box (if it exists) such that $b \cap V_e = \emptyset$ and $b \cap S_2 \neq \emptyset$. Merge b and b_i. If after the k^{th} box has been processed there are boxes b such that $b \cap V_e = \emptyset$ and $b \cap S_2 \neq \emptyset$, then place all the elements of all such boxes into A_{s+1}.

Using $A_s \in \mathrm{P}$, $\overline{A}_s \in \mathrm{P}$, Π_s polynomial honest, and $\mathrm{P} = \mathrm{NP}$, one can show that $A_{s+1} \in$P, $\overline{A}_{s+1} \in$P, and Π_{s+1} is polynomial honest. Since the number of pure boxes of B_s

is unbounded and the construction only affects at most c per block, the number of pure boxes in B_{s+1} is unbounded.

Every box b in B_{s+1} is either a pure box ($b \subseteq S_1$) such that $b \cap V_e = \emptyset$, or is such that $b \cap V_e \cap S_2 \neq \emptyset$. Hence both a) and b) are satisfied.

3) The number of boxes of B_s^m that intersect V_e is unbounded. We intend to set A_{s+1}, $\overline{A}_{s+1}$, and Π_{s+1} such that for all $x \in B_{s+1}$ there exists a $y \in \Pi_{s+1}(f_e(x))$. By Lemma 1 this implies $A \equiv_m^h B$.

We set $A_{s+1}, \overline{A}_{s+1}$, and Π_{s+1} as follows. For every m let $b_{11}, b_{12}, \ldots, b_{1k_1}, b_{21}, b_{22}, \ldots, b_{2k_2}$ be all the boxes induced by Π_s that contain elements of B_s^m (and therefore only elements of B_s^m); where $b_{11}, b_{12}, \ldots, b_{1k_1}$ are all the pure boxes that intersect V_e, and $b_{21}, b_{22}, \ldots, b_{2k_2}$ are the rest of the boxes. Let $k_3 = \max(\frac{k_1}{2}, k_2)$. For all $i < k_3$ merge b_{1i} and b_{2i}. For all $i \geq k_3$ place the elements of b_{2i} into A_{s+1}.

Using $A_s \in \mathrm{P}, \overline{A}_s \in \mathrm{P}, \Pi_s$ honest, and P=NP one can show that $A_{s+1} \in \mathrm{P}, \overline{A}_{s+1} \in \mathrm{P}$, and Π_{s+1} is a hp partition. Since the number of pure boxes in B_s is unbounded and the construction affects less than half of the pure boxes in each block, the number of pure boxes in B_{s+1} is unbounded.

It is easy to see that for every box b in B_{s+1}, $b \cap V_e \neq \emptyset$. Hence for all $x \in B_{s+1}$ there exists $y \in \Pi_{s+1}(f_e(x))$. ☒

Theorem 4: The topped finite initial segments of $\mathbf{H_m}$ are exactly the finite distributive lattices.

Proof sketch:

The proof that any topped finite initial segment of $\mathbf{H_m}$ is a finite distributive lattice is like the proof for a similar theorem about the m-degrees in recursion theory [21].

We show that if $\mathcal{D}$ is any topped finite distributive lattice, then $\mathcal{D}$ is an initial segment of $\mathbf{H_m}$. Let $\{a_1, \ldots, a_k\}$ be the join-irreducible elements of $\mathcal{D}$ (not including the bottom element) and let $\leq_{\mathcal{D}}$ be the natural partial ordering on $\mathcal{D}$. Note that every element x of $\mathcal{D}$ is the join of all elements less than x. Let p be a fixed polynomial. For $1 \leq i \leq k$ let

$$S_i = \{0^{e(m)+j} \mid m \in N,\ \ 0 \leq j \leq p(m) - 1,\ \ j \equiv i \ (\bmod k)\}.$$

We construct A such that the sets A_x (indexed by $x \in \mathcal{D}$) defined by

$$A_x = A \cap (\bigcup_{a_i \leq_{\mathcal{D}} x} S_i)$$

form an initial segment isomorphic to $\mathcal{D}$ in $\mathbf{H_m}$. More precisely we can construct $A \subseteq E^P$ in stages to satisfy the following requirements. The parameters e ranges over N while the parameters x and y range over $\mathcal{D}$.

$R_{\langle 1,e,i \rangle}$: $A_{a_i} \neq L(P_e)$.
$R_{\langle 2,e,x,y \rangle}$: If $x \not\leq_{\mathcal{D}} y$, then f_e is not a reduction of A_x to A_y.
R_e^3 : There exists an $x \in \mathcal{D}$ such that $\Phi_e^A \equiv_m^h A_x$.
In the last requirement note that if x is the bottom element of the lattice then $\Phi_e^A \in$P.

The rest of the proof is similar to that of Theorem 3. Various notions of pure boxes are needed to satisfy the second type of requirement and the fact that $\mathcal{D}$ is a distributive lattice is used to prove that all requirements fit together. ☒

Theorem 5: The topped initial segments of $\mathbf{H_m}$ are exactly the direct limits of ascending sequences of finite distributive lattices.

Proof sketch:

Combine the techniques of the last theorem with the techniques in [21] or [12] to prove the analogous theorem for the m-degrees. Details are in [7]. ☒

Having characterized exactly which finite and countable lattices are initial segments of $\mathbf{H_m}$, our next goal is to examine uncountable structures. It is here that the similarity of $\mathbf{H_m}$ and the m-degrees may fail.

Definition : Let $\langle X, \leq \rangle$ be any partial order. An element $x \in X$ has a *strong* $\leq$*-minimal cover* if there exists $y \in X$ such that $x < y$ and

$$(\forall z \in X)[z < y \Rightarrow z \leq x].$$

The first step towards characterizing the uncountable structures that are initial segments of the (classical) m-degrees is showing that every m-degree has a strong $\leq$-minimal cover. An analogous theorem in $\mathbf{H_m}$ is not known. Moreover, the question of whether or not $\mathbf{H_m}$ is elementarily equivalent to the m-degrees is open.

The r.e. m-degrees and $\mathbf{H_m} \cap \mathbf{RE}$ resemble each other in the same way the m-degrees and $\mathbf{H_m}$ do; however they are *not* elementarily equivalent. We first prove a theorem about the resemblance, and then about the difference.

Theorem 6: The topped finite initial segments of $\mathbf{H_m} \cap \mathbf{RE}$ are exactly the finite distributive lattices.

Proof sketch:

Combine the techniques of Theorems 5 with the e-state construction of a maximal r.e. set (see [26] for an e-state construction in recursion theory, and [2] for a modification used in complexity theory). The proof resembles a similar theorem proven for the (classical) m-degrees [13]. ☒

Lachlan showed that every incomplete r.e. m-degrees has an r.e. strong minimal $\leq_m$-cover. We show that the analogous theorem for $\mathbf{H_m} \cap \mathbf{RE}$ does not hold, which shows that the r.e. m-degrees are not elementarily equivalent to $\mathbf{H_m} \cap \mathbf{RE}$.

Theorem 7: There exists an incomplete r.e. set A that has no strong $\leq_m^h$-minimal cover.

Proof sketch

We construct r.e. sets $A, B, Q_1, Q_2, \ldots$ to satisfy the following requirements:

$$P_i : B \neq \Phi_i^A$$
$$N_e : A <_m^h W_e \Rightarrow (Q_e <_m^h W_e \text{ and } Q_e \not\leq_m^h A)$$

The P_i requirements ensures that A is incomplete, while the N_e requirements ensures that A has no strong $\leq_m^h$-minimal cover.

We break N_e into two subrequirements some of which may entail an infinite number of requirements.

Requirement $R_e^1 : A <_m^h W_e \Rightarrow Q_e <_m^h W_e$.

The condition $Q_e \leq_m^h W_e$ will hold since Q_e will be constructed by a Ladner-style "looking back techniques," [1,14,16] so Q_e will be "W_e with holes in it." To satisfy R_e^1 we satisfy the following requirements

$$N_{\langle e,i\rangle} : \neg(A \leq_m^h Q_e \text{ via } M_i).$$

It is easy to see that if $A <_m^h W_e$ and all the $N_{\langle e,i\rangle}$ are satisfied, then $Q_e <_m^h W_e$.

Requirement $R_e^2 : A <_m^h W_e \Rightarrow Q_e \not\leq_m^h A$

To satisfy R_e^2 we satisfy the following set of requirements:

$$\hat{N}_{\langle e,i\rangle} : (W_e \leq_m^h A) \vee \neg(Q_e \leq_m^h A \text{ via } M_i).$$

The sets Q_e are defined by a Ladner-style looking back construction. In particular, a 0-1 valued polynomial time function $f(-,-)$ with domain $N \times N$ in unary form will be constructed, and the sets $\{Q_e\}_{e=1}^{\infty}$ will be defined by

$$\sigma \in Q_e \Leftrightarrow (f(e,|\sigma|) = 1 \text{ and } \sigma \in W_e).$$

We informally describe how to satisfy each requirement.

Meeting $N_{\langle e,i\rangle}$: We use strings of the form $\langle 0,1^t\rangle$ to satisfy $N_{\langle e,i\rangle}$. At some stage s such that no member of $\{\langle 0,1^t\rangle \mid t \geq s\}$ has either entered or been restrained from entering A, we begin an attack on $N_{\langle e,i\rangle}$. Set $f(e,t) = 0$ for $t = s, s+1, s+2, \ldots$ until t is found such that either

a) $M_e(\langle 0,1^t\rangle) = YES$, in which case we restrain $\langle 0,1^t\rangle$ from entering A, or

b) $M_e(\langle 0,1^t\rangle) = NO$, in which case we put $\langle 0,1^t\rangle$ into A, or

c) $|M_e(\langle 0,1^t\rangle)| \geq s$, in which case we make sure that $f(e, |M_e(\langle 0,1^t\rangle)|)$ has been set to 0, and we put $\langle 0,1^t\rangle$ into A.

By honesty, one of these three conditions must occur.

Meeting $\hat{N}_{\langle e,i\rangle}$ *while meeting* $N_{\langle k,j\rangle}$: While $N_{\langle k,j\rangle}$ is being attacked we set $f(e,s) = 1$ for all $e \neq k$, hoping that if $W_e \not\leq_m^h A$ then making Q_e look like W_e will force $\neg(Q_e \leq_m^h A$ via $M_i)$. (We do not try to find a witness for this requirement). If $e = k$ then this course of action is not open to us, so instead we try to code W_e into A. For as long as $f(e,|\sigma|) = 0$, if τ enters W_e then put $\langle 1^e, \tau\rangle$ into A.

We show that these actions satisfy each requirement $\hat{N}_{\langle e,i\rangle}$. If $Q_e \leq_m^h A$ then we obtain $W_e \leq_m^h A$ as follows: Given σ, compute $f(e,|\sigma|)$. If $f(e,|\sigma|) = 1$ then $(\sigma \in Q_e$ iff $\sigma \in W_e)$. Hence $\sigma \in W_e$ iff $M_i(\sigma) \in A$. If $f(e,|\sigma|) = 0$ then $(\sigma \in W_e$ iff $\langle e,\sigma\rangle \in A)$.

Meeting P_i: P_i is satisfied in a manner similar to how $N_{\langle e,i\rangle}$ is satisfied. In particular, we keep elements out of A until an opportunity arises to diagonalize. By honesty, such an opportunity will arise. ☒

5) Low Sets Are Not hT-minimal

The hT-minimal sets constructed by Homer and Long [11] are recursive in $\emptyset''$. Ambos-Spies [2] (and independently Downey) constructed r.e. sets that are hT-minimal. Furthermore, Ambos-Spies showed that every high r.e. degree contains an hT-minimal set.

Definition : A set A is *low* if $A' \equiv_T \emptyset'$. A set A is *high* if $A' \equiv_T \emptyset''$. A Turing degree a is *low* (*high*) if it contains a low (high) set.

Note: Low sets resemble recursive sets, while high sets resemble K (the halting set). Examples of this resemblance can be found in [17,25]. The main theorem of this section indicates another way that low sets resemble recursive sets.

Ambos-Spies's construction seems to work only for high r.e. degrees. He raised the natural question of whether any nonhigh set can be hT-minimal. We give a partial negative answer by showing that low sets cannot be hT-minimal. Our proof also works for semilow sets which we define later. This result appears, in greater detail, in [6].

Convention: For this section we assume that all M_e are 0-1 valued. Let $L(M_e)$ be the language accepted by M_e.

Definition : Let A be any set. The *half jump of A* is

$$H_A = \{i \mid W_i \cap A \neq \emptyset\}.$$

Note that $H_A \leq_T A'$, and $H_{\overline{A}} \leq_T A'$.

Theorem 8: Let A be a set such that $A \leq_T \emptyset'$, $A \notin$P, and A is low. Then A is not hT-minimal.

Proof:

The proof resembles the delayed diagonalization arguments of Ladner [14], but the requirements may be injured. We sketch the proof assuming familiarity with Ladner's proof that no recursive set is hT-minimal.

We construct $B \leq_T^h A$ to satisfy the following requirements:

$$R_{2e} \ : \ B \neq L(M_e)$$
$$R_{2e+1} \ : \ L(P_e^B) \neq A$$

We construct a function $f \in$P, $f : 0^* \to \{0,1\}$, and define B via

$$x \in B \Leftrightarrow (f(0^{|x|}) = 1 \text{ and } x \in A).$$

The set B will alternate between looking like A and looking empty. The basic idea is that to satisfy R_{2e} we make B look like A until we spot a disagreement between B and $L(M_e)$ (which must happen since $A \notin P$); and to satisfy R_{2e+1} we make B look empty until we spot a disagreement (which must happen since $A \notin P$).

In the classical Ladner argument the set A is recursive so disagreements are easily spotted by looking back. In the present construction A is nonrecursive, so it is hard to spot a disagreement. We will use the lowness of A to get around this obstacle. (This sort of argument has a long history in recursion theory and is know there as the "Robinson trick".)

Since $A \leq_T \emptyset'$, by the Shoenfield limit lemma (see [26] Chapter III, Theorem 3.3) there is a recursive function $h : \Sigma^* \times N \rightarrow \{0,1\}$ such that $A(x) = \lim_{t\rightarrow\infty} h(x,t)$. By slowing down the construction of h we can take h as polynomial time computable in $|x|$ and t. Let A_s and B_s be

$$A_s = \{x \mid h(x,s) = 1 \text{ and } 0 \leq |x| \leq \log|s|\}$$
$$B_s = \{x \mid x \in A_s \text{ and } f(0^{|x|}) = 1\}$$

Note that A_s can be generated in time polynomial in $|s|$.

Since A is low

$$H_A \leq_T A' \leq_T \emptyset',$$
$$H_{\overline{A}} \leq_T A' \leq_T \emptyset'.$$

Hence by the Shoenfield limit lemma there exists recursive functions $g(i,s)$ and $\overline{g}(i,s)$ such that $g(i,t) \in \{0,1\}$, $\overline{g}(i,t) \in \{0,1\}$, $H_A(i) = \lim_{t\rightarrow\infty} g(i,t)$, and $H_{\overline{A}}(i) = \lim_{t\rightarrow\infty} g(i,t)$. We use g, $\overline{g}$, and the recursion theorem to help spot disagreements.

We describe how to spot an alleged disagreement of $L(M_e)$ and B at stage s. The key point will be that we may be wrong about the disagreement but this happens only finitely often, and eventually we are right. Keep in mind that while trying to spot a disagreement we make B look like A.

While trying to spot disagreement we may spot a z such that $M_e(z) \neq B_s(z)$. Since A may change and thus $B_s(z)$ might not equal $B(z)$, this disagreement may be deceptive. We need more evidence that $M_e(z) \neq B(z)$. By the recursion theorem we may assume that there are recursive functions i and j such that

$$W_{i(e)} = \{z \mid (\exists s) M_e(z) \neq B_s(z) = 0\},$$
$$W_{j(e)} = \{z \mid (\exists s) M_e(z) \neq B_s(z) = 1\}.$$

If $M_e(z) \neq B_s(z) = B(z)$ and $B(z) = 0$ ($B(z) = 1$) then $z \in A \cap W_{i(e)}$ ($z \in A \cap W_{j(e)}$), so $\lim_{t\rightarrow\infty} \overline{g}(i(e),t) = 1$ ($\lim_{t\rightarrow\infty} g(j(e),t) = 1$). We use this to supply further evidence that a disagreement has been spotted.

Formally R_{2e} *appears to be satisfied at stage* s if during the computation of $f(0^s)$ a z is found such that $M_e(z) \neq B_{s-1}(z)$ and either

1) $B_{s-1}(z) = 0$, $z \in W_{i(e),s}$, $g(i(e),s) = 1$, or
2) $B_{s-1}(z) = 1$, $z \in W_{j(e),s}$, $g(j(e),s) = 1$.

A definition of R_{2e+1} appearing satisfied at stage s can be formulated similarly.

We describe the computation of $f(0^s)$ informally. For s steps try to spot which requirements (in order) appear to be satisfied. Let a be the least number such that R_a does not appear satisfied. If a is even the let $f(0^s) = 1$, else let $f(0^s) = 0$. We say that requirement a has *received attention*. If a had appeared to be satisfied earlier, but has just been disovered to not be satisfied, then R_a is said to have been *injured*.

We need to see why this works. If the same requirement receives attention cofinitely often then $A \in$P by the usual arguments. Since g and $\overline{g}$ only change their mind finitely often on any argument, no requirement can be injured infinitely often. An induction proof shows that all requirements are eventually satisfied.

In the above proof we used the lowness of A only once, when we needed that H_A and $H_{\overline{A}}$ were recursive in $\emptyset'$.

Definition : A set A is *semilow* if $H_A \leq_T \emptyset'$.

From the proof of the above theorem we easily have

Theorem 9: Let A be a set such that $A \leq_T \emptyset'$, $A \notin$P, A is semilow, and $\overline{A}$ is semilow. Then A is not hT-minimal.

If A is r.e., then the set B constructed in the proof is r.e. also. Hence we can obtain the following theorems with minor modifications.

Theorem 10: The hT-degrees of low r.e. sets are dense. The pT-degrees of low r.e. sets are dense.

The results above are related to the machine independent theory of computational complexity of Blum [4] and Blum-Marques [5]. The following definition is due to Blum and Marques [5].

Definition : Let $\Phi_1, \Phi_2, \Phi_3, \ldots$ be a Blum complexity measure associated to the acceptable programming system $\phi_1, \phi_2, \phi_3, \ldots$ (e.g. step counting). An r.e. set A is *non-speedable* if there exists a recursive function h such that A has a fastest program modulo h. Formally There is an index i, $W_i = A$, such that

$$(\forall j)(W_j = A \Rightarrow (\text{ for almost all } x)[x \in A \Rightarrow \Phi_i(x) \leq h(x, \Phi_j(x))]).$$

In [25] Soare showed that an r.e. set A is non-speedable iff $\overline{A}$ is semilow. We thus have as a corollary

Corollary 11: If A is an r.e. non-speedable set then A is not hT-minimal.

6) Index Sets are not hT-minimal

We show index sets are nonminimal. Do do this, we need a convention about our programming system.

Convention: Let $\varphi_1, \varphi_2, \varphi_3, \ldots$ denote an acceptable programming system such that the s-m-n functions [22] are computable in polynomial time. This is reasonable if the machine model is similar to real programs, in which case the s-m-n functions merely replace a read statement with an assignment statement.

Definition : A set A is an *index set* if whenever $\varphi_i \equiv \varphi_j$ (as functions) then either $i, j \in A$ or $i, j \notin A$. The proof of the following theorem resembles the proof of Rice's Theorem [22].

Theorem 12: If A is a nontrivial index set (i.e. $A \neq \emptyset$, $A \neq \Sigma^*$), then A is not hT-minimal.

Proof:

Let $a \in A$ and $b \notin A$. Let C be a recursive set such that $C \notin$P and φ_i be a recursive function that computes the characteristic function of C. Let z be such that

$$\varphi_z(x, y) = \begin{cases} \varphi_a(y) & \text{if } x \in C \\ \varphi_b(y) & \text{if } x \notin C \end{cases}$$

Since we assume the s-m-n functions are polynomial time computable, we have a function $f \in$P such that $\varphi_z(x, y) = \varphi_{f(z,x)}(y)$.

$x \in C \Rightarrow \varphi_{f(z,x)} \equiv \varphi_a \Rightarrow f(z,x) \in A$
$x \notin C \Rightarrow \varphi_{f(z,x)} \equiv \varphi_b \Rightarrow f(z,x) \notin A$

The function f is polynomial time computable and honest, hence $C \leq_m^h A$. Since C is recursive and A is not recursive, it is not the case that $A \leq_T C$. Hence $C <_m^h A$ and thus A is not an hT-minimal set. ☒

7) Nonrelativizations and Double Jumps of Minimal Degrees

Virtually all the constructions in the honest minimal degree literature, including the ones in this paper, use recursion-theoretic techniques. Hence the question arises, "Do the theorems (and techniques) relativize?" If the techniques relativize, then they will not suffice to solve the P=?NP problem [3].

In this section we exhibit two theorems about honest reductions that do not relativize. The theorems are not contrived in that they arose while studying the jumps of minimal degrees. After presenting these results we will discuss this aspect.

Recall that P_e^A is $q(z)$-honest if for all x, for all queries y made in the computation of $P_e^A(x)$, $q(|y|) \geq |x|$. Hence P_e^A is z-honest if for all x, for all queries y made in the computation of $P_e^A(x)$, $|y| \geq |x|$.

For any set A, define

$$R^A = \{e \mid P_e^A \text{ is } z\text{-honest}\}.$$
$$Q^A = \{e \mid (\exists k)[P_e^A \text{ is } (z+k)\text{-honest}]\}$$

Note that honesty is a property of the computation rather than of the set computed. Even for recursive A, Q^A and R^A are not index sets in the usual sense (see Rogers [22]). The following theorem extends a result of Hajek [9].

Theorem 13: For every recursive set A, R^A is Π_1^A-complete.

Proof:

For recursive A, $\Pi_1^A = \Pi_1^\emptyset$, so giving this proof for $A = \emptyset$ would suffice. However the proof is given relative to an arbitrary recursive A to stress the dependence of the set on the particular oracle queries and to point up the difficulties of relativizing this construction to a general nonrecursive A.

R^A is Π_1^A as it can easily be expressed by a Π_1^A statement:

$$e \in R^A \Leftrightarrow (\forall x)[P_e^A(x) \text{ only queries } y \text{ such that } |y| \geq |x|]$$

(This is true for all A.)

To prove that R^A is Π_1^A-complete we will show that $\overline{K^A} \leq_m R^A$ where,

$$K^A = \{e | \varphi_e^A(e) \text{ halts}\}.$$

This suffices since $\overline{K^A}$ is a Π_1^A-complete set [22].

Given e, define the index $\rho(e)$ as follows. $P_{\rho(e)}^A$ is a linear time machine which on input x simulates φ_e^A on input e for $|x|$ steps. These $|x|$ steps include the simulation of a fixed algorithm for the recursive set A whenever a query of the oracle for A occurs in the computation. There are two cases.

1) If $\varphi_e^A(e)$ halts in less than $|x|$ steps of the above simulation, then $P^A_{\rho(e)}(x)$ queries if $1 \in A$ and halts.
2) Otherwise, $P^A_{\rho(e)}(x)$ halts immediately.

If $e \in K^A$, then for all but finitely many x, $P^A_{\rho(e)}(x)$ will query if $1 \in A$, and so $P^A_{\rho(e)}$ is not z-honest. If $e \notin K^A$, then 1) holds for only finitely many x, hence A is only queried for finitely many values of x so $P^A_{\rho(e)}$ is z-honest. These two statments show that ρ is the required reduction. ☒

Theorem 14: For every recursive set A, Q^A is Σ_2^A-complete.

Proof:

This proof is similar to the one above.

Q^A is Σ_2^A as it can easily be expressed by a Σ_2^A statement:

$$e \in Q^A \Leftrightarrow (\exists k)(\forall x)[P_e^A(x) \text{ is } (z+k)\text{-honest}].$$

To prove that Q^A is Σ_2^A-complete we will show that $FIN^A \leq_m Q^A$, where

$$FIN^A = \{e \mid \text{domain}(\varphi_e^A) \text{ is finite } \}.$$

This suffices since FIN^A is a Σ_2^A-complete set [22].

Given e, define the index $\rho(e)$ as follows. $P^A_{\rho(e)}$ is a linear time machine which on input $x10^k$ simulates φ_e^A on input x for k steps. These k steps include the simulation of a fixed algorithm for the recursive set A whenever a query of the oracle for A occurs in the computation. There are two cases.

1) If $\varphi_e^A(x)$ halts in exactly k steps of the above simulation, then $P^A_{\rho(e)}(x10^k)$ queries if $1 \in A$ and halts.
2) Otherwise, $P^A_{\rho(e)}(x10^k)$ halts immediately.

On any input not of the form $x10^k$, $P^A_{\rho(e)}$ halts immediately after checking this fact.

If domain(φ_e^A) is infinite, then for infinitely many x and any k, $P^A_{\rho(e)}(x10^k)$ will query if $1 \in A$, and so $P^A_{\rho(e)}$ is not $(z+k)$-honest for any k.

If domain(φ_e^A) is finite then the condition of 1) holds for only finitely many x and k, and A is queried only finitely often. Then, by 2), $P^A_{\rho(e)}$ is $(z+k)$-honest for some k.

So $e \in FIN^A$ iff $\rho(e) \in Q^A$. ☒

We show that neither of the above proofs relativize to arbitrary nonrecursive A. This is surprising, as most similar proofs in recursion theory and complexity theory easily relativize. The obstacle to relativization is the honesty condition in the definitions of sets P^A and Q^A. The failure to relativize points up the contention (see Homer [11]) that constructions which depend on honesty do not in general relativize.

Theorem 15: There exists a set B with $R^B \leq_T B$ (hence R^B is not Π_1^B-complete).

Proof:

Since R^B is Π_1^B for all B, we need only construct B such that R^B is Σ_1^B. Then $R^B \in \Sigma_1^B \cap \Pi_1^B$ so $R^B \leq_T B$.

Let $C_1, C_2, C_3, \ldots$ be a recursive partition of Σ^* such that each C_i is infinite. We construct B in stages. At the end of stage s we will have completely determined $B \cap C_s$, and also whether P_s^B is z-honest. The answer to the "$s \in R^B$?" question will be coded into C_s in a Σ_1^B way. We may also place (restrain) other elements into (out of) B.

CONSTRUCTION

Stage 0: Set $B_0 = \emptyset$.

Stage $e > 0$: Let B_{e-1} = the set of elements put into B through stage $e-1$. There are two cases.

CASE 1: There is a finite set D consistent with B_{e-1} such that $(\exists x)[P_e^D(x)$ not z-honest$]$. By D being consistent with B_{e-1} we mean that D agrees with any elements put into B_{e-1} or kept out of B_{e-1} at a previous stage.

In this case let D and x be the least such strings and let $D^+ = D - \{y : |y| \leq |x|\}$. Note that the $P_e^{B \cup D^+}(x)$ computation is dishonest since it is identical to the P_e^D computation up to and including the first dishonest query, i.e., the first query to a string of length less than $|x|$.

Set $B_e = B_{e-1} \cup D^+$.

For any C_i such that D^+ adds some element of C_i to B we fix all elements of $B \cap C_i$ up to length $|x|^e + e$. (Recall that $|x|^e + e$ bounds the running time of $P_e^{()}(x)$.) That is, at any subsequent stage we never put into B or take out of B any other elements of C_i which have length $\leq |x|^e + e$. Let $z \in C_i$ be the least element of C_i whose membership in B has not yet been decided and put $z \in \overline{B}$. Putting this z into $\overline{B}$ will make it impossible for case 1 of the construction to result in C_i having a long sequences of adjacent elements all in B.

CASE 2: For all finite sets D consistent with B_{e-1}, we have

$$(\forall x)[P_e^D(x) \text{ is } z\text{-honest}].$$

Find the least $x \in C_e$ with $2^{|x|} > |x|^e + e$ and whose membership in B has not yet been decided. There exists such an x since only finitely much of $C_e \cap B$ has been decided. Starting at x put the next $2^{|x|}$ many elements of C_e into B.

In either case 1 or 2 we now fix $B \cap C_e$ by putting all elements of C_e not yet decided into $\overline{B}$.

END OF CONSTRUCTION.

Intuitively, the only way a long sequence of elements from B can be in any C_e is if we put it there on purpose in Case 2. This is the key to our coding.

Claim 1: If P_e^B is z-honest, then at stage e of the construction, we put $2^{|x|}$ consecutive elements from C_e into B.

Proof of Claim 1:

Since P_e^B is z-honest at stage e of the construction we must have followed Case 2. Otherwise we would have put elements into B to guarantee that P_e^B is dishonest. But

then, in Case 2 of stage e, we put elements into B which satisfy the claim.
☒(end of proof of Claim 1)

Claim 2: For any e, $e \in R^B$ if and only if there exists an x such that $x \in C_e$, $2^{|x|} > |x|^e + e$, and $2^{|x|}$ consecutive elements of C_e starting with x are all in B.

Proof of Claim 2:

If e is in R^B, then P_e^B is z-honest. Thus, by Claim 1, there is $x \in C_e$ which satisfies this claim.

If e is not in R^B, P_e^B is not z-honest. Hence at stage e the construction follows Case 1 and we have, $(\exists D$ consistent with $B_{e-1})(\exists x)[P_e^D(x)$ is not z-honest$]$. Otherwise every extension consistent with B_{e-1} results in z-honesty and so P_e^B is z-honest. So at stage e we add D^+ (defined in the construction) to B and we fix all elements of C_e in or out of B at this stage.

Now note that $C_e \cap B$ cannot contain $2^{|x|}$ many consecutive elements of C_e starting at some $x \in C_e$ with $2^{|x|} > |x|^e + e$. To see this consider a stage $e' \leq e$. If we add elements of C_e to B at stage e' we do this for some computation $P_{e'}^{B_{e'-1}}(x)$. For this computation we only add elements y to B with $|y| > |x|$ and we add at most $|x|^{e'} + e' < 2^{|x|}$ such elements to C_e. When this occurs in Case 1 of e', we fix all elements of $C_e \cap B$ up to length $|x|^{e'} + e'$ and put the next element of C_e into $\overline{B}$. ☒(end of proof of claim 2)

Now, to finish the proof, note that Claim 2 gives a Σ_1^B definition of R^B. So we have R^B in $\Pi_1^B \cap \Sigma_1^B$ which gives $R^B \leq_T B$. ☒

Note: The set B constructed is recursive in the halting set.

Theorem 16: There exists a set B with $Q^B \leq_T B'$ (hence Q^B is not Σ_2^B-complete).

Proof:

We show that if $R^B \leq_T B$ then $Q^B \leq_m B'$. Since we constructed such B in the last theorem, this will complete the proof.

We need the following auxiliary function τ. If $e, k \in N$ then $\tau(e,k)$ is the polynomial oracle machine that, on input x, deletes the first k bits of x and runs $P_e^{()}$ on the remainder. Note that $e \in Q^B \Leftrightarrow (\exists k)[\tau(e,k) \in R^B]$. Since $R^B \leq_T B$ the predicate $\tau(e,k) \in R^B$ is equivalent to a predicate recursive in B. When that substitution is made we have a Σ_1^B definition of Q^B. Hence $Q^B \leq_m B$. ☒

In recursion theory the following two theorems about Turing-minimal degrees are known (see Lerman [17]).

Theorem 17: There exists a Turing-minimal set A such that $A' \equiv_T \emptyset'$.

Theorem 18: There exists a Turing-minimal set A such that $A'' \equiv_T \emptyset''$.

The construction in Theorem 12 (13) interleaves making the set A Turing-minimal and making $I^A \leq_T \emptyset'$ ($I^A \leq_T \emptyset''$) where I^A is some index set such that for every A, I^A is Π_1^A-complete (Σ_2^A-complete). The interleaving is difficult.

We attempt a similar construction with respect to $\leq_T^h$ reductions. The index sets we use are R^A and Q^A because they seem like a natural analogue to the sets I^A used in the recursion theoretic results. We show that interleaving the constructions can be carried out. Unfortunately, since Q^A is not always Σ_2^A-complete we do not obtain the analog we seek. It is of some interest that the 'easy' part- having a construction relativize- does not carry over, but the hard part- interleaving two constructions- does carry over.

Theorem 19: (P=NP) There is an hT-minimal set A such that $Q^A \leq_T \emptyset''$.

Proof sketch:

The construction is carried out in infinitely many stages. At each stage i a partial function f_i is constructed. Each f_i is an extension of f_{i-1}. The set A is the unique set which is consistent with every f_i. At even stages we do the Homer-Long construction of an hT-minimal set, and at the odd stages we help to make $Q^A \leq_T \emptyset''$. A key point is that at the end of every stage there is still an infinite number of values where the set is not determined. This enables the Homer-Long construction to be carried out on the even stages without any difficulty. (Full details are in [8].) ☒

8) A Recursive Superminimal Set

The sets constructed in section 4, and in all of the honest minimal degree literature, are nonrecursive. This is necessary since Ladner's Theorem says that recursive sets cannot be hm-minimal. However, Ladner's Theorem does not say anything about $hmto$-minimal sets. Total honest m-reductions differ from honest m-reductions in a significant way. In the cases where an honest m-reduction maps a string to either YES or NO, the honesty condition does not come into play. By contrast, in the case of total honest m-reductions, the honesty condition always comes into play. Thus, intuitively, these reductions are different from each other. We prove this by showing that that there exists a recursive set A, $A \notin P$, that is $hmto$-minimal, and in fact is superminimal (i.e. for any $B \leq_m^{h\text{-}to} A$, $B \equiv_m^{h\text{-}to} A$.)

Definition : Let g be as defined in section 4 (second definition of that section). Let $B^m = \{x \,:\, g(m) \leq |x| < g(m+1)\}$. A set A is *blocktype* if it is the union of sets of the form B^m. Note that for all m, if any element of B^m is in A, then all elements of B^m are in A (hence if some element of B^m is not in A, then no element of B^m is in A).

Lemma 20: If A is blocktype and $C \leq_m^{h\text{-}to} A$, then $A \leq_m^{h\text{-}to} C$.

Proof:

Let $C \leq_m^{h\text{-}to} A$ via a total honest f. Let p and q be polynomials such that p bounds the runtime of f, and f is q-honest.

The reduction $A \leq_m^{h\text{-}to} C$ is as follows: on input y find m such that $y \in B^m$, and then output $0^{q(g(m))}$.

We show

$$y \in A \Leftrightarrow f(0^{q(g(m))}) \in A \Leftrightarrow 0^{q(g(m))} \in C.$$

The second equivalence holds because f is a reduction of C to A. The first equivalence will follow if we show that $f(0^{q(g(m))}) \in B^m$, since A is blocktype.

Since f is computable in time p

$$|f(0^{q(g(m))})| \leq p(q(g(m))) < 2^{g(m)} = g(m+1).$$

Since f is q-honest

$$q(|f(0^{q(g(m))})|) \geq q(g(m)), \text{ so}$$
$$|f(0^{q(g(m))}|) \geq g(m).$$

Hence

$$g(m) \leq |f(0^{q(g(m))})| < g(m+1)$$

so $f(0^{q(g(m))}) \in B^m$. ⊠

Theorem 21: Given any recursive function T, there exists a recursive set A such that $A \notin$DTIME$(T(n))$ and A is *hmto*-minimal.

Proof:

It is easy to construct a blocktype set that is not in DTIME$(T(n))$. By the above Lemma, that set is *hmto*-minimal. ⊠

The techniques in this section can also be used to show that Ladner's proof cannot be extended to finite-to-1 reductions (honesty is not needed).

9) Acknowledgements

We would like to thank Tim Long for extensive discussions. We would also like to thank Amihood Amir, Valentina Harizanov, David Kamishlian, and Clyde Kruskal, for proofreading and discussion. The first author was partially supported by a United States-New Zealand Cooperative Foundation grant. The second author was partially supported by NSF grants MCS 80-05386, MCS 82-00269, and MCS 80-10707, the third author by NSF grant 83-18282.

to
:or
əs-
ed
by

REFERENCES

1. Ambos-Spies, K. Sublattices of the Polynomial Time Degrees. *Information and Control 65* (1985), 63-84.
2. Ambos-Spies, K. *Honest Polynomial Reducibilities, Recursively Enumerable Sets, and the P=?NP Problem.* Second Annual Structure in Complexity Theory Conference. An extended version is in Forschungsbericht Nr. 236, 1987, from Abteilung Informatik, Universitat Dortmund.
3. Baker, T., Gill, J., and Solovay, R. Relativizations of the P=?NP Question. *SIAM Journal of Computer Science 1* (1975), 305-322.
4. Blum, M. A Machine Independent Theory of the Complexity of Recursive Functions. *J. Assoc. Comput. Mach. 18* (1967), 322-336.
5. Blum, M. and Marques, I. On Complexity Properties of Recursively Enumerable Sets. *J. Symb. Logic 38* (1973), 579-593.
6. Downey, R. On Computational Complexity and Honest Polynomial Degrees. *Theoretical Computer Science* (1989). (to appear).
7. Downey, R. and Moses, M. *On the Structure of Honest Poly-m-degrees.* Manuscript.
8. Gasarch, W.I. and Homer, S. *Recursion Theoretic Properties of Minimal Honest Polynomial Degrees.* University of Maryland Computer Science Dept., TR 1803. Also Boston University TR 87-005.
9. Hajek, P. Arithmetical Hierarchy and Complexity of Computation. *Theoretical Computer Science 8* (1979), 227-237.
10. Homer, S. Minimal Polynomial Degrees of Nonrecursive Sets. *Lecture Notes in Mathematics No. 1141 (Recursion Theory Week)* (1985), 193-202.
11. Homer, S. Minimal Degrees for Polynomial Reducibilites. *Journal of the Association of Computing Machinery 34* (1987), 480-491.
12. Lachlan, A. Initial Segments of many-one degrees. *Canadian Journal of Math 22*(1987), 75-85.
13. Lachlan, A.H. Initial segments of the r.e. m-1 degrees. *Algebra and Logic 11* (1972), 156-172.
14. Ladner, R.E. On the Structure of Polynomial Time Reducibility. *Journal of the Assoc. for Computing Mach. 22, No. 1* (January 1975), 155-171.
15. Ladner, R.E., Lynch, N.A., and Selman, A.L. A Comparison of Polynomial Time Reducibilities. *Theoretical Computer Science 1* (1975), 103-123.
16. Landweber, L.H., Lipton, R.J., and Robertson, E.L. On the Structure of Sets in NP and Other Complexity Classes. *Theoretical Computer Science 15* (1981), 181-200.
17. Lerman, M. *Degrees of Unsolvability.* Springer Verlag, 1983.
18. Long, T.J. and Homer, S. Honest Polynomial Degrees and P =? NP. *Theoretical Computer Science 51* (1987), 265-280..
19. Machtey, M. On the Density of Honest Subrecursive Classes. *Journal of Computer and System Science 10* (1975), 183-199.

20. MEYER, A. AND RITCHIE, D. A Classification of the Recursive Functions. *Z. Math Logik Grundlagen Math. 18* (1972), 71-82.

21. ODIFREDDI, P. The Structure of the m-degrees. *Lecture Notes in Mathematics No. 1141 (Recursion Theory Week)* (1985), 315-332.

22. ROGERS, H. JR. *Theory of Recursive Functions and Effective Computability.* McGraw Hill, New York, 1967.

23. SACKS, G.E. A minimal degree less than 0'. *Bull. Amer. Math. Soc. 67* (1961), 416-419.

24. SCHONING, U. A Low and a High Hierarchy within NP. *Journal of Computer and System Sciences 27* (1983), 14-28.

25. SOARE, R.I. Computational Complexity of Recursively Enumberable Sets. *Information and Control 52* (1982).

26. SOARE, R.I. *Recursively Enumerable Sets and Degrees.* Springer Verlag (Omega Series), Berlin and New York, 1987.

27. SPECTOR, C. On Degrees of Recursive Unsolvability. *Annals of Mathematics 64* (1956), 581-592.

28. YOUNG, P. Some Structural Properties of Polynomial Reducibilities and Sets in NP. *Proceedings of the 15th annual STOC* (1983), 382-401.