Theoretical Computer Science 24 (1983) 279–289
North-Holland

ORACLE-DEPENDENT PROPERTIES OF THE LATTICE OF NP SETS

Steven HOMER
Department of Mathematics, Boston University, Boston, MA 02215, U.S.A.

Wolfgang MAASS*
Department of Mathematics, University of California, Berkeley, CA 94720, U.S.A.

Communicated by R. Karp
Received February 1982
Revised September 1982

Abstract. We consider under the assumption $P \neq NP$ questions concerning the structure of the lattice of NP sets together with the sublattice P. We show that two questions which are slightly more complex than the known splitting properties of this lattice cannot be settled by arguments which relativize. The two questions which we consider are whether every infinite NP set contains an infinite P subset and whether there exists an NP-simple set. We construct several oracles, all of which make $P \neq NP$, and which in addition make the above-mentioned statements either true or false. In particular we give a positive answer to the question, raised by Bennett and Gill (1981), whether an oracle B exists making $P^B \neq NP^B$ and such that every infinite set in NP^B has an infinite subset in P^B. The constructions of the oracles are finite injury priority arguments.

1. Introduction

Very few properties of the collection of NP sets are known. The central problems of complexity theory having to do with NP, e.g., whether $P = NP$ or $NP = co\text{-}P$, have yet to be solved. One approach which has yielded a number of interesting results has been to study the structure of NP under the assumption that $P \neq NP$. Such results are of interest not only because it is widely believed that $P \neq NP$ but as well because one might hope to shed some light on the central problems themselves by seeing what these assumptions entail.

In this paper we consider questions about the lattice of NP sets (where set-theoretic union and intersection are the lattice operations), together with the sublattice P, under the assumption $P \neq NP$. One aspect of this lattice which has been studied are its splitting properties (see Ladner [6]). Probably the strongest results here is that of Breitbart [4]. He shows that for every recursive infinite, coinfinite set A there is a set B recognizable in real time and log space which splits

* During the preparation of the paper this author was supported by the Heisenberg Programm der Deutschen Forschungsgemeinschaft, Fed. Rep. Germany.

A (i.e., each of $A \cap B, A \cap \bar{B}, \bar{A} \cap B, \bar{A} \cap \bar{B}$ is infinite). This implies that every infinite set in NP or co-NP can be split into two infinite sets of the same class. Thus there are for example no maximal elements in the lattice of NP sets mod finite sets.

We consider here two further properties of NP sets; whether there are any simple sets in NP and whether every infinite set contains an infinite subset in P. An NP-simple set is a coinfinite set in NP whose complement contains no infinite NP sets. As is the case with maximal sets, simple sets are the ones whose complements are in some sense small. Hence, once the question of maximal sets is settled, it is natural to look for NP-simple sets. We show that any answer to this question does not relativize. That is, we construct oracles relative to which $P \neq NP$ and for which the statement that NP-simple set exist is true respectively false.

A P-immune set is an infinite set which contains no infinite subset in P. The problem of whether there exists a P-immune set in NP is of some practical interest as it is useful to have a practically computable approximation to a set in NP. In [3] Bennett and Gill show that, with probability one, for an oracle A there is an infinite set in NP^A which has no infinite subset in P^A. Further they ask whether an oracle B exists such that $P^B \neq NP^B$ and every infinite set in NP^B contains an infinite subset in P^B. We answer this question affirmatively. Hence, any argument which solves under the assumption $P \neq NP$ the problem of whether any infinite NP set contains an infinite subset in P does not relativize.

These considerations are somewhat analogous to the study of the lattices of recursively enumerable and recursive sets. This study has led to the discovery of significant new constructions in recursion theory. The questions concerning the lattice of r.e. sets corresponding to those which we ask about NP sets are easily answered. It almost immediately follows from the definitions that every infinite recursively enumerable set contains an infinite recursive subset. Constructions of various types of simple sets are ubiquitous in recursion theory (see Soare [7]).

The methods of constructing oracles in this paper are in general more complex than those which have previously been used for this purpose (see [1] or [2]). The constructions are (with the exception of Theorem 3.1) finite injury priority arguments. The oracles that are constructed in Theorems 3.1, 4.1 and 4.5 are recursive sets; the oracle in Theorem 3.2 is recursively enumerable.

We expect that with further, more sophisticated constructions of oracles along the lines of this paper one will be able to show as well that even under the assumption $P \neq NP$ some immediate questions about P-degrees of sets in NP cannot be answered by using arguments that relativize (e.g. recursion theoretic arguments).

In the next section we present the main definitions and notations. Section 3 contains the construction of an A s.t. $NP^A = \text{co-}NP^A$ and some infinite set in NP^A contains no infinite subset in P^A and of an oracle A such that an NP^A-simple set exists. Section 4 contains the construction of an oracle B such that $P^B \neq NP^B$ and every infinite set in NP^B contains an infinite subset in P^B. Finally, this same method is used to construct a B with $P^B \neq NP^B$ such that no NP^B-simple set exists. In Section 5 we indicate that the previous arguments can also be used to show that

the existence of P-universal sets in NP is independent from the assumption $P \neq NP$ (in the same sense as above).

2. Definitions

We consider computations on oracle Turing machines. Without loss of generality we assume that the tape alphabet of our machines is $\Sigma = \{0, 1\}$. Our languages will be subsets of $\Sigma^* = \{\text{finite strings from alphabet } \Sigma\}$.

We fix enumerations $\{P_i\}_{i\in\mathbb{N}}$ and $\{N_i\}_{i\in\mathbb{N}}$ ($\mathbb{N}$ denotes the natural numbers) of polynomial-time bounded deterministic respectively non-deterministic oracle Turing machines. We may assume that $p_i(n) = i + n^i$ is a strict upper bound on the length of any computation by P_i or N_i with any oracle X on inputs of length n. P_i^X and N_i^X denote oracle Turing machines using oracle X. We also write P_i^X for the set $\{\alpha \in \Sigma^* | \text{machine } P_i^X \text{ accepts } \alpha \text{ (i.e., machine } P_i^X \text{ gives output 0 on input } \alpha)\}$. Similarly we write N_i^X for the set $\{\alpha \in \Sigma^* | N_i^X \text{ accepts } \alpha\}$. P^X is the collection of all the sets P_i^X, $i \in \mathbb{N}$. NP^X is the collection of all sets N_i^X, $i \in \mathbb{N}$. For a more complete account of these definitions see [5].

For any string s, s^n is s concatenated with itself n times. We use the notation $|\cdot|$ to denote both the length of a string and the cardinality of a set, depending on the context. Finally, we will make use of a recursive paring function $\langle \cdot, \cdot \rangle$ on the integers. We require that the pairing function be one–one and, for a fixed first argument, be strictly monotonic in its second argument.

3. Oracles relative to which P-immune and NP-simple sets exist

Bennett and Gill [3] have already shown that, with probability one, for a random oracle A there is an infinite set in NP^A which has no infinite subset in P^A and $NP^A \neq \text{co-}NP^A$.

We show here that one can as well directly construct a recursive oracle A s.t. some set in NP^A has no infinite subset in P^A. The corresponding requirements R_i make it necessary to restrain many elements from A (in general infinitely many for one R_i). Therefore the construction is most interesting if one combines these with other requirements that make $NP^A = \text{co-}NP^A$, which require an enumeration of a great number of elements into A. There occur no injuries of requirements in this construction.

Theorem 3.1. *There is a recursive oracle A s.t. some infinite set in NP^A has no infinite subset in P^A and s.t. $NP^A = \text{co-}NP^A$.*

Proof. In order to construct A s.t. some set in NP^A has no infinite subset in P^A it

is enough to make

$$M = \{0^k \mid k \in \mathbb{N} \text{ and } \exists\, \alpha \in \Sigma^* \ (|\alpha| = k \wedge \alpha \in A)\}$$

infinite and to satisfy for every $i \in \mathbb{N}$ the requirement

$$R_i : P_i^A \cap \{0^k \mid k \in \mathbb{N}\} \text{ infinite} \rightarrow P_i^A \not\subseteq M$$

(it is obvious that $M \in \mathrm{NP}^A$).

According to Baker, Gill and Solovay [1] it is sufficient to make sure that the complement of

$$K(A) = \{\langle i, \alpha, 0^n\rangle \mid \text{some computation of } N_i^A \text{ accepts } \alpha \text{ in fewer than } n \text{ steps}\}$$

is an NP^A in order to make $\mathrm{NP}^A = \text{co-}\mathrm{NP}^A$ ($K(A)$ is polynomial complete in NP^A).

Construction

Stage k. Let A_k be the set of elements that are already in A at the beginning of stage k.

For every $i \leq \frac{1}{8}k$ s.t. $p_i(k) < 2^{k/8}$ we restrain all strings of length $\geq k$ from A that are not in A_k and that are queried in the computation of $P_i^{A_k}$ on input 0^k. Further, if for one of these i, R_i has not yet received attention and $P_i^{A_k}$ accepts 0^k, we restrain all strings of length k from A (and thus make $0^k \notin M$). We then say that R_i receives attention at stage k.

Finally for every string $\alpha \notin K(A_k)$ s.t. there is a string β of length k s.t. β continues the string α, β is not restrained from A, $2|\alpha| < |\beta| \leq 4|\alpha|$ and β has a 1 in position $|\alpha|+1$ and 0 at positions $|\alpha|+2, \ldots, 2|\alpha|$, we enumerate β in A. (Then we can recover α from the code β by taking the first half of string β and stripping off the 1 and all 0's at the end of the first half.)

We first note that there is some k_0 s.t. for all $k \geq k_0$ at most $2^{k/4}$ strings of length k are restrained from A via the first clause. The effect of this first restraint clause is, that if some P_i^A accepts infinitely many 0^k, then there are infinitely many k s.t. $P_i^{A_k}$ accepts 0^k. Therefore R_i receives attention at some stage and thus we have $P_i^A \not\subseteq M$.

Further an easy calculation shows that for all strings α we have $\alpha \notin K(A)$ iff there is some β in A with a relation to α as in the construction. We use here that at no more than $\frac{1}{8}k$ many of the first k stages all strings of length k are restrained via the second clause. Therefore $\Sigma^* - K(A) \in \mathrm{NP}^A$.

Note that in this construction we cannot always place for $\alpha \notin K(A)$ a code β of length $2|\alpha|$ in A as in [1] because of the strong restraint of the requirements R_i.

Theorem 3.2. *There is an oracle A such that there exists an* NP^A*-simple set.*

Proof. For any oracle A the set

$$M = \{0^l \mid l \in \mathbb{N} \text{ and } \exists\, \alpha \in \Sigma^* \ (|\alpha| = l \wedge \alpha \in A)\}$$

is obviously in NP^A.

We construct A in such a way that for every $i \in \mathbb{N}$ the requirement

$$R_i : N_i^A \cap \{0^l \mid l \in \mathbb{N}\} \text{ infinite} \rightarrow N_i^A \cap M \neq \emptyset$$

and for every $n \in \mathbb{N}$ the requirement

$$S_n : |\{l' \mid A \text{ contains no string of length } l'\}| \geq n$$

is satisfied. This will immediately imply that

$$S = M \cup \{\alpha \in \Sigma^* \mid \alpha \text{ is not of the form } 0^l,\ l \in \mathbb{N}\}$$

is a simple set in NP^A.

There are obvious conflicts between the requirements R_i, which want to add elements to the set A, and the requirements S_n, which want to keep elements out of A. These conflicts are settled by assigning priorities to all requirements. We only allow that action for the sake of R_i injures S_n (by changing the set of the first n lengths l' s.t. no string of length l' is in A) if $i < n$, i.e., if R_i has higher priority than S_n.

Construction. We say that requirement R_i is satisfied at the beginning of stage k if there is a stage $k' < k$ s.t. R_i received attention at stage k' and no string that was restrained from A for R_i at stage k' has so far been enumerated into A.

We write A_k for the set of elements that have been enumerated into A by the beginning of stage k.

Stage k. Check whether some $i \leq k$ exists s.t. R_i is not satisfied and there are $l \leq k$, $\alpha \in \Sigma^*$ with $|\alpha| = l$ and an accepting computation of $N_i^{A_k}$ on input 0^l so that string α is not queried in this computation and such that α has not been restrained from A for some $R_{i'}$ with $i' < i$ and

$$|\{l' < l \mid A_k \text{ contains no string of length } l'\}| \geq i.$$

If such i, l, α exist, we choose i minimal and $\langle l, \alpha \rangle$ minimal for this i. We then say that R_i receives attention at stage k. We enumerate α in A and restrain from A for R_i all strings in $\Sigma^* - A_k$ which are queried in one canonically chosen accepting computation of $N_i^{A_k}$ on input 0^l in which α is not queried.

A trivial induction on i shows that every requirement R_i receives attention at only finitely many stages (note that R_i can only receive attention at stages k_1 and k_2 with $k_1 < k_2$ if there exists some $i' < i$ s.t. $R_{i'}$ receives attention at some stage k' with $k_1 < k' < k_2$). This already implies that every requirement S_n is satisfied because S_n can only be injured at a stage k if some R_i with $i < n$ receives attention at stage k. Thus $\{0^l \mid l \in N\} - M$ is infinite.

Lemma 3.3. *For every* $i \in \mathbb{N}$

$$N_i^A \cap \{0^l \mid l \in \mathbb{N}\} \text{ infinite} \rightarrow N_i^A \cap M \neq \emptyset.$$

Proof. Assume that $N_i^A \cap \{0^l \mid l \in \mathbb{N}\}$ is infinite. Choose $0^l \in N_i^A$ s.t.

$$|\{l' < l \mid A \text{ contains no string of length } l'\}| \geq i,$$

no string of length l is ever restrained from A for an $R_{i'}$ with $i' < i$ and some accepting computation of N_i^A on input 0^l does not query every string of length l (the latter holds as soon as $p_i(l) < 2^l$).

Choose k_0 s.t. no $R_{i'}$ with $i' \leq i$ receives attention at a stage $\geq k_0$. Then requirement R_i is permanently satisfied from stage k_0 on because otherwise the existence of l with the properties above guarantees that R_i receives attention after stage k_0. Thus $N_i^A \cap M \neq \emptyset$.

4. Oracles relative to which no P-immune or NP-simple sets exist

Theorem 4.1. *There is an oracle* B *s.t.* $\mathrm{P}^B \neq \mathrm{NP}^B$ *and s.t. every infinite set in* NP^B *has an infinite subset in* P^B.

Proof. We construct an oracle B and for every $i \in \mathbb{N}$ a deterministic oracle Turing machine Q_i such that

$$Q_i^B \subseteq N_i^B \quad \text{and} \quad N_i^B \text{ infinite} \rightarrow Q_i^B \text{ infinite}.$$

We define

$$Q_i^B = \{\alpha \in \Sigma^* \mid t_{i,\alpha} \in B\}$$

where $t_{i,\alpha} \in \Sigma^*$ is a 'test string' which is associated with α defined by $t_{i,\alpha} = \alpha 10^i 10^n$, where $n = |\alpha| + i + 2 + p_i(|\alpha|)$ (p_i is the polynomial which bounds the running time of N_i).

Obviously for every $i \in \mathbb{N}$ there is a deterministic Turing machine which runs in polynomial time and which produces for input α the output $t_{i,\alpha}$. Therefore $Q_i^B \in \mathrm{P}^B$ for every $B \subseteq \Sigma^*$.

The test strings $t_{i,\alpha}$ are chosen in such a way that the nondeterminsitic machine N_i cannot query the oracle about string $t_{i,\alpha}$ during a computation on input α (because $|t_{i,\alpha}| > p_i(|\alpha|)$). Further the function

$$\langle \alpha, i \rangle \rightarrow t_{i,\alpha}$$

is one–one. Finally we observe that for every $l \in \mathbb{N}$ the set

$$F_l = \{\beta \in \Sigma^* \mid |\beta| = l \text{ and the last } \lceil \tfrac{1}{2} l \rceil \text{ elements of the string } \beta \text{ are not all 0's}\}$$

does not contain any string of the form $t_{i,\alpha}$. Further F_l has at least $(2^{\lceil l/2 \rceil} - 1)$ many elements and thus the function

$$l \to |F_l|$$

majorizes every polynomial after a while.

We define a set $M \in \mathrm{NP}^B$ by

$$M = \{0^l \mid l \in \mathbb{N} \text{ and } F_l \cap B \neq \emptyset\}.$$

For every $j \in \mathbb{N}$ we have a requirement

$$S_j : M \neq P_j^B.$$

If all the requirements S_j are satisfied we have $M \notin \mathrm{P}^B$.

We have to satisfy in addition for all $i \geq 0$, $n > 0$ the requirements

$$R_{i,n} : N_i^B \text{ infinite} \to |Q_i^B| \geq n.$$

We assign priority $\langle j, 0 \rangle$ to requirement S_j and priority $\langle i, n \rangle$ to requirement $R_{i,n}$. Following the usual convention we say that requirement T' has higher priority than requirement T if (priority of T') $<$ (priority of T).

In the following construction of oracle B we sometimes try to satify S_j at a certain stage of the construction and later we see that we have to sacrifice this attempt in order to satisfy a requirement of higher priority than S_j. Nevertheless we will be able to satisfy every requirement S_j because it can be injured only finitely often (at most once by every requirement $R_{i,n}$ of higher priority than S_j). Thus we just have to be persistent enough in our attempts to satisfy S_j.

It will be obvious that the constructed oracle B is recursive because we enumerate the strings in B in the order of their length.

Construction. We say that requirement S_j is satisfied at the beginning of stage k ($k \in \mathbb{N}$) if there is a stage $k' < k$ where S_j received attention and s.t. no string that was restrained from B at stage k' for S_j has so far been enumerated into B.

We say that requirement $R_{i,n}$ is satisfied at the beginning of stage k if there is a stage $k' < k$ where $R_{i,n}$ received attention.

Stage k. Let B_k be the set of elements that are already in B at the beginning of stage k. Define

$$l_k = \max[\{k\} \cup \{\text{lengths of all strings that are in } B_k \text{ or that have been restrained from } B \text{ at previous stages}\}] + 1.$$

Choose j minimal s.t. S_j is not satisfied and $p_j(l) < |F_{l_k}|$.

Case 1. There is a requirement $R_{i,n}$ of higher priority than S_j which is not satisfied and there is a string α s.t. $\alpha \in N_i^{B_k}$, $|t_{i,\alpha}| \leq l_k$, $t_{i,\alpha}$ has not been restrained from B for a requirement of higher priority than $R_{i,n}$, and

$$|t_{i,\alpha}| > \max\{|\beta| \mid \beta \in B_k\}.$$

We choose $R_{i,n}$ and α with these properties s.t. $R_{i,n}$ has the highest possible priority and enumerate $t_{i,\alpha}$ in B. We say that $R_{i,n}$ receives attention at stage k.

Case 2. Otherwise.

In this case S_j receives attention at stage k. We restrain for requirement S_j all strings from B about which the oracle is queried during the compuation of $P_j^{B_k}$ on input 0^{l_k}. Further, if $P_j^{B_k}$ does not accept 0^{l_k}, we enumerate the alphabetically first string $\beta \in F_{l_k}$ into B s.t. β is not restrained from B for requirement S_j. If $P_j^{B_k}$ accepts 0^{l_k}, we restrain all strings in F_{l_k} from B for S_j.

Lemma 4.2. $M = \{0^l \mid l \in \mathbb{N} \text{ and } F_l \cap B \neq \emptyset\} \notin \mathrm{P}^B$.

Proof. We first note that every requirement $R_{i,n}$ receives attention at most once during the construction. Further, a requirement S_j can only receive attention at stages k_1, k_2 with $k_1 < k_2$ if some $R_{i,n}$ with $\langle i, n\rangle < \langle j, 0\rangle$ receives attention at some stage k' with $k_1 < k' < k_2$. Therefore, every requirement S_j only finitely often receives attention during the construction.

Fix some $j \in \mathbb{N}$. In order to prove that $M \neq P_j^B$ we consider a large enough stage k s.t. no requirement of priority $\leqslant \langle j, 0\rangle$ receives attention at any stage $\geqslant k$ and such that $p_j(l_k) < |F_{l_k}|$. Then S_j is satisfied at the beginning of stage k because otherwise some requirement of priority $\leqslant \langle j, 0\rangle$ would receive attention at stage k. Therefore, there is a stage $k' < k$ where S_j received attention and s.t. no string that was restrained from B at stage k' for S_j has been enumerated into B by the beginning of stage k. By the choice of k none of these restrained strings is enumerated into B at any stage $\tilde{k} \geqslant k$ (because no $R_{i,n}$ of higher priority than S_j receives attention at any stage $\tilde{k} \geqslant k$). This implies that P_j^B accepts $0^{l_{k'}}$ iff $P_j^{B_{k'}}$ accepts $0^{l_{k'}}$ iff $0^{l_{k'}} \notin M$.

Lemma 4.3. *For every* $i \in \mathbb{N}$, $Q_i^B \subseteq N_i^B$ *and*

$$N_i^B \text{ infinite} \rightarrow Q_i^B \text{ infinite}.$$

Proof. We place a string $t_{i,\alpha}$ in B at stage k only if some requirement $R_{i,n}$ receives attention at stage k. In this case we have $\alpha \in N_i^{B_k}$ and therefore as well $\alpha \in N_i^B$ because only strings of length $\geqslant |t_{i,\alpha}| > p_i(|\alpha|)$ are enumerated into B at stages $\geqslant$k and the machine N_i cannot query its oracle about such long strings during a computation on input α. Thus $Q_i^B \subseteq N_i^B$.

Assume that N_i^B is infinite. We show that, for every $n \in \mathbb{N}$, requirement $R_{i,n}$ receives attention at some stage. This implies that Q_i^B is infinite because at every stage where some requirement $R_{i,n}$ receives attention we create a new element in Q_i^B. Thus we fix some $n \in \mathbb{N}$. We choose some $\alpha \in N_i^B$ s.t. only strings of length less than $|t_{i,\alpha}|$ are restrained from B for requirements of priority $\leqslant \langle i, n\rangle$ during the construction and s.t. at the first stage k where a string of length $\geqslant |t_{i,\alpha}|$ is enumerated into B, a requirement of priority $\geqslant \langle i, n\rangle$ receives attention. Since for this k only

elements of length $\geq |t_{i,\alpha}| > p_i(|\alpha|)$ are enumerated into B at stages $\geq k$, we have $\alpha \in N_i^{B_k}$. Further, since a string of length $\geq |t_{i,\alpha}|$ is enumerated into B at stage k, we have $|t_{i,\alpha}| \leq l_k$. Therefore, $R_{i,n}$ receives attention at this stage k unless it has already received attention at some previous stage.

Corollary 4.4. *Arguments that remain valid under relativization are not sufficient to prove that*

$$\mathrm{P} \neq \mathrm{NP} \rightarrow \textit{every infinite set in } \mathrm{NP} \textit{ contains an infinite subset in } \mathrm{P}$$

or

$$\mathrm{P} \neq \mathrm{NP} \rightarrow \textit{not every infinite set in } \mathrm{NP} \textit{ contains an infinite subset in } \mathrm{P}.$$

Proof. For the first statement, consider the oracle of Theorem 3.1.

For the second statement, consider the oracle of Theorem 4.1.

Theorem 4.5. *There is an oracle B s.t. $\mathrm{NP}^B \neq \mathrm{co\text{-}NP}^B$ and every infinite set in $\mathrm{NP}^B \cup \mathrm{co\text{-}NP}^B$ has an infinite subset in P^B.*

Proof. The construction of the desired oracle is an inessential extension of the construction in the proof of Theorem 4.1.

We now have to make sure that

$$M = \{0^l \mid l \in \mathbb{N} \text{ and } F_l \cap B \neq \emptyset\}$$

is not in $\mathrm{co\text{-}NP}^B$. Thus, if requirement S_j receives attention at stage k, we make $F_{l_k} \cap B \neq \emptyset$ iff $0^{l_k} \in N_j^{B_k}$. If $0^{l_k} \in N_j^{B_k}$, restrain for S_j all strings from B which are queried in the least accepting computation of $N_j^{B_k}$ on input 0^{l_k}. On the other hand, if $0^{l_k} \notin N_j^{B_k}$, restrain from B all strings queried by any computation of N_j^B on input 0^{l_k}.

Besides the sets $Q_i^B \subseteq N_i^B$ one builds infinite subsets $\tilde{Q}_i^B$ in P^B for every infinite set $(\Sigma^* - N_i^B)$ in $\mathrm{co\text{-}NP}^B$. We take 'test strings' $\tilde{t}_{i,\alpha}$ that are different from the $t_{i',\alpha'}$ and we define

$$\tilde{Q}_i^B = \{\alpha \mid \tilde{t}_{i,\alpha} \in B\}.$$

If requirement

$$\tilde{R}_{i,n} : \Sigma^* - N_i^B \text{ infinite} \rightarrow |\tilde{Q}_i^B| \geq n$$

receives attention at stage k, we place some $\tilde{t}_{i,\alpha}$ in B with $\alpha \notin N_i^{B_k}$. As before we then have $\alpha \notin N_i^B$ because only strings of length $\geq |\tilde{t}_{i,\alpha}| > p_i(|\alpha|)$ are enumerated in B at stages $\geq k$.

Corollary 4.6. *Arguments that remain valid under relativization are not sufficient to prove that*

$$\mathrm{P} \neq \mathrm{NP} \rightarrow \textit{there exists an } \mathrm{NP}\textit{-simple set in the lattice of sets in } \mathrm{NP}$$

or

$$P \neq NP \rightarrow \textit{there exists no } NP\textit{-simple set in the lattice of sets in } NP.$$

Proof. For the first statement consider the oracle of Theorem 4.5.

For the second statement consider the oracle of Theorem 3.2.

5. P-universal sets in NP

The methods of the previous sections can be applied to other questions. Call a set U P^A-universal if

$$P^A = \{\{\alpha \in \Sigma^* \mid \langle \gamma, \alpha \rangle \in U\} \mid \gamma \in \Sigma^*\}.$$

The question of whether there exists a set U in NP which is P-universal is open. The existence of such a set would imply that the use of nondeterminism in polynomial time computations allows one to compute all sets in P with the fixed polynomial time bound of the set U in NP. The analogy with recursion theory suggests the existence of P-universal sets in NP. Many computer scientists believe the opposite is true.

The method of Theorem 3.1 can be used to show the following theorem.

Theorem 5.1. *There is a recursive oracle A such that $P^A \neq NP^A$ and there is a P^A-universal set in NP^A.*

On the other hand, we have the following theorem.

Theorem 5.2. *There is a recursive oracle B such that $P^B \neq NP^B$ and there is no P^B-universal set in NP^B.*

Proof. The construction is similar to that of the proof of Theorem 4.1. Besides the usual set M, which witnesses that $NP^B \neq P^B$, for every set N_i^B in NP^B a set Q_i^B in P^B is constructed such that $\forall \gamma \, \exists \alpha \;\; (\langle \gamma, \alpha \rangle \in N_i^B \leftrightarrow \alpha \notin Q_i^B)$.

References

[1] T. Baker, J. Gill and R. Solovay, Relativizations of the $P \stackrel{?}{=} NP$ question, *SIAM J. Comput.* **4** (4) (1975) 431–442.

[2] T. Baker and A. Selman, A second step toward the polynomial hierarchy, *Proc. 17th IEEE Symp. on the Foundations of Computer Science* (1976) 71–75.

[3] C.H. Bennett and J. Gill, Relative to a random oracle A, $P^A \neq NP^A \neq$ co-NP^A with probability one, *SIAM J. Comput.* **10** (1) (1981) 96–113.

[4] S. Breidbart, On splitting recursive sets, *J. CSS* **17** (1978) 56–64.

[5] J. Hopcroft and A. Ullman, *Introduction to Automata Theory, Languages and Computation* (Addison-Wesley, Reading, MA, 1979).

[6] R. Ladner, On the structure of polynomial time reducibility, *J. Assoc. Comput. Mach.* **22** (1975) 155–171.

[7] R.I. Soare, Recursively enumerable sets and degrees, *Bull. Amer. Math. Soc.* **84** (1978) 1149–1181.