INFORMATION AND CONTROL 71, 231–243 (1986)

On Relativized Exponential and Probabilistic Complexity Classes

HANS HELLER

Technische Universität München, Munich, West Germany

An oracle X is constructed such that the exponential complexity class $\Delta_2^{\mathrm{EP},X}$ equals the probabilistic class $\mathrm{R}(\mathrm{R}(X))$. This shows that it will be difficult to prove that Δ_2^{EP} is different from $\mathrm{R}(\mathrm{R})$, although it seems very unlikely that these two classes are equal. The result subsumes several known results about relativized computations:

(i) the existence of relativized polynomial hierarchies extending two levels (Long, T., 1978, Dissertation, Purdue Univ., Lafayette, Ind.; Heller, H., 1984(a), *SIAM J. Comput.* **13**, 717–725; Heller, H., 1984(b), *Math. Systems Theory* **17**, 71–84);

(ii) the existence of an oracle X such that $\mathrm{BPP}(X) \not\subseteq \Delta_2^{P,X}$ (Stockmeyer, L., 1983, "Proc. 15th STOC" pp. 118–126),

(iii) the existence of an oracle X such that $\mathrm{NP}(X)$ is polynomially Turing reducible to a sparse set (Wilson, C., 1983, "Proc. 24th FOCS," pp. 329–334; Immerman, N., and Mahaney, S., 1983, "Conference on Computational Complexity Theory," Santa Barbara, March 21–25).

The result shows possible inclusion relations for nonrelativized complexity classes and points out that certain results about probabilistic complexity classes and about polynomial size circuits cannot be improved unless methods are applied which do not relativize.

2. INTRODUCTION

This paper investigates the relationship between polynomial and exponential time complexity classes relative to some oracle X under the additional constraint that $\mathrm{R}(X)$, the set of random-polynomial time computable sets, is equal to $\mathrm{NP}(X)$. By relativization of a result of Adleman (1978) we know that languages in $\mathrm{R}(X)$ are polynomial Turing reducible to a sparse set where the reduction is relativized. Therefore, if $\mathrm{NP}(X) = \mathrm{R}(X)$, then $\mathrm{NP}(X)$ is reducible to a sparse set and for the nonrelativized case this is equivalent to NP having polynomial size circuits. Therefore one direction of the investigation is the question of which complexity classes may have polynomial size circuits. This question was also raised by Wilson (1983) in a slightly different setting. He showed that it will be difficult to prove that Δ_2^{EP} does not have polynomial size circuits. On the

0019-9958/86 $3.00

other hand, if $\mathrm{NP}(X)=\mathrm{R}(X)$, then the polynomial hierarchy is equal to an appropriately defined probabilistic hierarchy, so that the other direction aims at the question of how much of the exponential hierarchy can be included in the probabilistic hierarchy. It turns out that Δ_2^{EP} may be equal to the probabilistic class Σ_2^{R} and this seems to be the strongest result possible. The result shown here stresses that several known facts about complexity classes are difficult to improve unless we apply techniques which do not relativize.

3. Basic Definitions

The notation used in the following is similar to that of Baker, Gill, and Solovay (1975). The underlying alphabet is $\Sigma=\{0,1\}$. The reader is assumed to be familiar with the following concepts not explained in detail: (non)deterministic Turing machines, oracle machines, time bounded computations, reducibility ($\leqslant_m^P$ denotes plynomial many-one reducibility, $\leqslant_T^P$ denotes polynomial Turing reducibility), and completeness with respect to a given reducibility. We also introduce a relativized version of Turing reducibility: a set A is polynomial Turing reducible relative to X to a set B ($A \leqslant_T^{P,X} B$) if $A \leqslant_T^P X \oplus B$, where $\oplus$ denotes the disjoint union. Let P_i (NP_i) be an enumeration of the polynomial deterministic (nondeterministic) oracle machines. P_i^X (NP_i^X) denotes machine P_i (NP_i) with oracle X. Without loss of generality, assume that the ith machine runs in time $p_i(n)=i+n^i$. Let EL_i (NEL_i) be an enumeration of the deterministic (nondeterministic) oracle machines running in exponential linear time (the ith machine runs in time 2^{i*n}) and EP_i (NEP_i) be an enumeration of the exponential polynomial machines running in time $2^{p_i(n)}$. By abuse of notation M_i^X denotes the machine M_i outfitted with oracle X as well as the language accepted by M_i with oracle X. For all oracle machines considered here the size of the queries is bounded only by the running time. $\exists kx[\mathrm{R}(x)]$ means that there exist k many x such that $\mathrm{R}(x)$ holds. There is a coding $\langle\cdot\rangle$ of finite sequences of words over Σ into Σ^* for which encoding and decoding can be done in polynomial time. The coding of oracle machines is such that

$$K(X)=\{\langle i, x, 0^d\rangle\colon \mathrm{NP}_i^X \text{ accepts } X \text{ in fewer than } d \text{ steps}\}$$

can be computed by a polynomial-time bounded nondeterministic oracle machine with oracle X.

$\mathrm{R}(X)$ is the set of randomly polynomial-time computable sets relative to X, i.e., A is in $\mathrm{R}(X)$ iff there is an $i\in N$ and a polynomial q such that for all x

$$x \in A \leftrightarrow \exists y [|y| = q(|x|) \vee \langle x, y\rangle \in P_i^X]$$
$$\text{and } \forall x\, \exists y\, [|y| = q(|x|) \wedge \langle x, y\rangle \in P_i^X] \text{ implies}$$
$$\exists 2^{q(|x|)-1} y\, [|y| = q(|x|) \wedge \langle x, y\rangle \in P_i^X].$$

BPP(X) is the class of languages acceptable in polynomial time relative to X with bounded error:

$A \in \mathrm{BPP}(X)$ iff there is an $i \in N$, a polynomial q, and a constant c, $0 < c < \frac{1}{2}$, such that for all x,

$$x \in A \leftrightarrow \exists c * 2^{q(|x|)} y [|y| = q(|x|) \wedge \langle x, y\rangle \in P_i^X]$$
$$\text{and } \forall x \exists c * 2^{q(|x|)} y [|y| = q(|x|) \wedge \langle x, y\rangle \in P_i^X]$$
$$\text{implies}$$
$$\exists (1-c) * 2^{q(|x|)} y [|y| = q(|x|) \wedge \langle x, y\rangle \in P_i^X].$$

For C a class of languages over Σ define the operators P, NP, R, EL, NEL, and NEP by

$$\mathrm{P}(C) = \{\mathrm{P}_i^X : i \in N, X \in C\},$$
$$\mathrm{NP}(C) = \{\mathrm{NP}_i^X : i \in N, X \in C\},$$
$$\mathrm{R}(C) = \{\mathrm{R}_i^X : i \in N, X \in C, \mathrm{R}_i^X \in \mathrm{R}(X)\},$$
$$\mathrm{EL}(C) = \{\mathrm{EL}_i^X : i \in N, X \in C\},$$
$$\mathrm{NEL}(C) = \{\mathrm{NEL}_i^X : i \in N, X \in C\},$$
$$\mathrm{EP}(C) = \{\mathrm{EP}_i^X : i \in N, X \in C\},$$

and

$$\mathrm{NEP}(C) = \{\mathrm{NEP}_i^X : i \in N, X \in C\}.$$

We write P(X) for P($\{X\}$) and do similarly for the other operators and co C denotes the class of complements of sets in C:

$$\mathrm{co}\, C = \{X : \bar{X} \in C\}.$$

Define the polynomial hierarchy relative to X by

$$\Sigma_0^{P,X} = \Pi_0^{P,X} = \Delta_0^{P,X} = \mathrm{P}(X)$$

and for $i \geqslant 0$,

$$\Sigma_{i+1}^{P,X} = \mathrm{NP}(\Sigma_i^{P,X}),$$
$$\Pi_{i+1}^{P,X} = \mathrm{co}\, \Sigma_{i+1}^{P,X},$$

and

$$\Delta_{i+1}^{P,X} = \mathrm{P}(\Sigma_i^{P,X}).$$

$\mathrm{PH}(X) = \{\Sigma_i^{P,X}, \Pi_i^{P,X}, \Delta_i^{P,X} : i \in N\}$ is the polynomial hierarchy relativized to X. Similar to the jump operation in recursion theory (see Rogers, 1967) we can consider $K(X)$ as a polynomial jump of X. $K^i(X) = K(K^{i-1}(X))$ is the ith jump of X. $K^i(X)$ is $\leqslant_m^P$-complete in $\Sigma_i^{\mathrm{P},X}$. We say $\mathrm{PH}(X)$ extends $i+1$ levels, for $i \geqslant 1$, if $\Sigma_i^{\mathrm{P},X} \subseteq \Sigma_{i+1}^{\mathrm{P},X} = \Pi_{i+1}^{\mathrm{P},X}$. The random hierarchy relative to X is given by

$$\Sigma_0^{\mathrm{R},X} = \Pi_0^{\mathrm{R},X} = \Delta_0^{\mathrm{R},X} = \mathrm{P}(X)$$

and for $i \geqslant 0$,

$$\Sigma_{i+1}^{\mathrm{R},X} = \mathrm{R}(\Sigma_i^{\mathrm{R},X}),$$

$$\Pi_{i+1}^{\mathrm{R},X} = \mathrm{co}\ \Sigma_{i+1}^{\mathrm{R},X},$$

and

$$\Delta_{i+1}^{\mathrm{R},X} = \mathrm{P}(\Sigma_i^{\mathrm{R},X}).$$

The exponential linear (resp. exponential polynomial) hierarchy is defined by

$$\Sigma_0^{\mathrm{EL},X} = \Pi_0^{\mathrm{EL},X} = \Delta_0^{\mathrm{EL},X} = \mathrm{EL}(X)$$

and for $i \geqslant 0$,

$$\Sigma_{i+1}^{\mathrm{EL},X} = \mathrm{NEL}(\Sigma_i^{\mathrm{P},X}),$$

$$\Pi_{i+1}^{\mathrm{EL},X} = \mathrm{co}\ \Sigma_{i+1}^{\mathrm{EL},X},$$

and

$$\Delta_{i+1}^{\mathrm{EL},X} = \mathrm{EL}(\Sigma_i^{\mathrm{P},X}).$$

(resp.

$$\Sigma_0^{\mathrm{EP},X} = \Pi_0^{\mathrm{EP},X} = \Delta_0^{\mathrm{EP},X} = \mathrm{EP}(X)$$

and for $i \geqslant 0$

$$\Sigma_{i+1}^{\mathrm{EP},X} = \mathrm{NEP}(\Sigma_i^{\mathrm{P},X}),$$

$$\Pi_{i+1}^{\mathrm{EP},X} = \mathrm{co}\ \Sigma_{i+1}^{\mathrm{EP},X},$$

and

$$\Delta_{i+1}^{\mathrm{EP},X} = \mathrm{EP}(\Sigma_i^{\mathrm{P},X})).$$

For similar definitions see also Hartmanis, Sewelson, and Immerman (1983). A set S is sparse if there is a polynomial p such that the number of strings up to length n in S is bounded by $p(n)$.

4. Main Result

The following technical theorem is the basis for the later considerations.

Theorem 1. *There is a recursive oracle X such that* $\mathrm{NP}(X) = \mathrm{R}(X)$ *and* $\Delta_2^{\mathrm{EL},X} \subseteq \Sigma_2^{\mathrm{P},X}$.

Proof. Let

$$D_2(X) = \{\langle i, x, d\rangle : \mathrm{EL}_i^{K(X)} \text{ accepts } x \text{ in } d \text{ steps}\}.$$

Note that $D_2(X)$ is $\leqslant_m^P$-complete in $\Delta_2^{\mathrm{EL},X}$ as well as in $\Delta_2^{\mathrm{EP},X}$ (for $\Delta_2^{\mathrm{EL},X}$ only linear time reductions are needed).

We guarantee that the following two requirements will be satisfied:

$$(1) \quad x \in D_2(X) \leftrightarrow \exists y\, \forall z\ [3\,|x| = |y| \wedge (|y| = |z| \rightarrow xyz0 \in X)]$$

and

$$(2) \quad x \in K(X) \leftrightarrow \exists 2^{3|x|-1} y\ [|y| = 3\,|x| \wedge xy1 \in X] \leftrightarrow \exists y\ [|y| = 3\,|x| \wedge xy1 \in X].$$

(1) implies that $D_2(X) \in \Sigma_2^{\mathrm{P},X}$ and thereby $\Delta_2^{\mathrm{EL},X} \subseteq \Sigma_2^{\mathrm{P},X}$.

(2) implies that $K(X) \in \mathrm{R}(X)$ from which we get $\mathrm{NP}(X) = \mathrm{R}(X)$.

X is constructed in stages. Each stage consists of two steps. The first serves to satisfy the first requirement, the second step to satisfy the second requirement. Initially, let $X = \varnothing$.

Stage m

Step 1. We say a string $y = \langle j, c, 0^k\rangle$ is m-forced into $K(X)$ if an accepting computation for $y \in K(X)$ can be obtained by adding strings s to X which satisfy the following three conditions:

(1) $|s| > m$,

(2) s is not reserved for $\bar{X}$,

(3) if s has rightmost symbol 1, then $s = uv1$, $|v| = 3\,|u|$, and $u \in K(X$ constructed so far) or u can be m-forced (and is m-forced) into $K(X)$.

Note that m-forcing y into $K(X)$ may lead to m-forcing strings u into $K(X)$ such that the length of u is less than $\frac{1}{3}|y|$. Therefore, the recursive process of m-forcing will stop after finite many steps.

For each string x of length m such that $x = \langle i, b, d\rangle$ (i.e., x is candidate for $D_2(X)$) consider the computation of $\mathrm{EL}_i^{K(X)}$ on string b for d steps. For each string y queried during this computation such that $y = \langle j, c, 0^k\rangle$ (i.e., y is candidate for $K(X)$) m-force y into $K(X)$ if this is possible. Do this in a consistent way, which means: whenever $y = \langle j, c, 0^k\rangle$ is m-forced into $K(X)$ then guarantee that y remains in $K(X)$:

Select an accepting computation of NP_j^X on c for k steps and reserve for $\bar{X}$ those string for which queries are made during this computation and which are not in X. Recursively for strings $s = uv1$ asked during this computation, such that $u \in K(X)$, guarantee that u remains in $K(X)$.

After this is done for all candidates y for $K(X)$ queried by $\mathrm{EL}_i^{K(X)}$ on b in the order they are asked about, test if $\mathrm{EL}_i^{K(X)}$ accepts b in d steps. If b is accepted then select a y_0 of length $3m$ such that no string xy_0z0, where z varies over strings of length $3m$, is reserved for $\bar{X}$. (It is shown below that such a y_0 exists.) Add all such xy_0z0 to X. Otherwise do nothing.

Step 2. For each string x of length m, if $x \in K(X)$ then select 2^{3m-1} strings y of length $3m$ such that no string $xy1$ is reserved for $\bar{X}$ and add all these $xy1$ to X.

Let us first determine for $x = \langle i, b, d\rangle$ with $|x| = m$ the maximal number of strings that are reserved for $\bar{X}$, when the strings y queried by $\mathrm{EL}_i^{K(X)}$ on b are m-forced into $K(X)$. Let $Y = \{y_1, ..., y_s\}$ be the strings that are asked in this computation. The sum of the length of the strings in Y is obviously bounded by $d < 2^m$. Let Y_- be the strings in Y that are not in $K(X)$ and cannot be m-forced into $K(X)$ and let Y_+ be the rest, i.e., $Y_+ = (Y - Y_-) = Y \cap K(X)$. The y's in Y_- do not cause the reservation of any string. For $y = \langle j, c, 0^k\rangle$ in Y_+ we must recursively consider an accepting computation of NP_j^X on c for k steps. Again, let $Z = \{z_1, ..., z_t\}$ be the strings z asked in this computation. Define Z_- and Z_+ by $Z_- = Z \cap \bar{X}$ and $Z_+ = Z \cap X$. The strings from Z_- are reserved for $\bar{X}$ and do not lead to more reservations. The strings from Z_+ are not reserved for $\bar{X}$ but need more consideration, if they are of the form $uv1$ where $|v| = 3|u|$ and $u \in K(X)$. The worst case happens when $|Z_-|$ is maximal, i.e., Z_+ is empty. In this case, the highest number of strings is reserved for $\bar{X}$, no computation step is lost for reproducing a string $uv1$ on the oracle tape where u encodes a further computation. Now, $|Z_-|$ is less than k, where k comes from $y = \langle j, c, 0^k\rangle \in Y_+$. The sum over the lengths of the y's in Y_+ is bounded by $d < 2^m$. This shows that for $x = \langle i, b, d\rangle$ not more than d strings are reserved for $\bar{X}$. Since there are 2^m strings of length m, less than 2^{2m} strings are reserved for $\bar{X}$ at stage m. At stages up to and including m, less than $\sum_{i=1}^{m} 2^{2i} \leqslant 2^{3m-1}$ strings are reserved for $\bar{X}$. Therefore at later stages we have enough strings available to do the encoding, i.e., to satisfy requirements (1) and (2). A similar calculation shows that at stages up to and including m, less than 2^{3m-1} strings with rightmost symbol 0 are added to X, when strings are forced into $K(X)$. Since encoding $x \in D_2(X)$ according to requirement (1) requires 2^{3m-1} strings, we get for no string $x_0 \notin D_2(X)$ that

$$\exists y, \forall z \; [3|x| = |y| = |z| \wedge x_0 yz0 \in X].$$

This shows that the construction is possible and that it satisfies the requirements. Q.E.D.

5. Implications of the Main Result

It will be shown that Theorem 1 has many implications and subsumes many results about relativized computations.

5.1. *The Polynomial and the Exponential Hierarchy*

We can derive some relations between the polynomial and the exponential time hierarchies relative to the oracle X constructed in Theorem 1.

Theorem 2. *There exists an oracle X such that* $\Delta_2^{\mathrm{P},X} \subsetneq \Sigma_2^{\mathrm{P},X} = \mathrm{PH}(X) = \mathrm{Pspace}(X) = \mathrm{EP}(X) = \mathrm{NEP}(X) = \Delta_2^{\mathrm{EP},X} \subsetneq \Sigma_2^{\mathrm{EP},X}$.

Proof. Let X be as in Theorem 1. Since $\Sigma_2^{\mathrm{P},X}$ is closed under $\leqslant_m^{\mathrm{P}}$-reducibility, $\Delta_2^{\mathrm{EL},X} \subseteq \Sigma_2^{\mathrm{P},X}$ implies $\Delta_2^{\mathrm{EP},X} \subseteq \Sigma_2^{\mathrm{P},X}$. The other inclusion $\Sigma_2^{\mathrm{P},X} \subseteq \Delta_2^{\mathrm{EP},X}$ is trivial. Polynomial time complexity classes are always properly contained in the corresponding exponential time classes, i.e., $\Delta_2^{\mathrm{P},X} \subsetneq \Delta_2^{\mathrm{EP},X}$ and $\Sigma_2^{\mathrm{P},X} \subsetneq \Sigma_2^{\mathrm{EP},X}$. From this we get $\Delta_2^{\mathrm{P},X} \subsetneq \Sigma_2^{\mathrm{P},X}$ and $\Delta_2^{\mathrm{EP},X} \subsetneq \Sigma_2^{\mathrm{EP},X}$. Q.E.D.

Theorem 2 shows that there exists a polynomial hierarchy extending two levels; i.e., a hierarchy which collapses at $\Sigma_2^{\mathrm{P},X}$ but not before $\Sigma_2^{\mathrm{P},X}$. Such hierarchies have also been constructed in Heller (1984(a), 1984(b)) and Long (1978). The relation $\Sigma_2^{\mathrm{P},X} = \mathrm{NEP}(X) = \Sigma_1^{\mathrm{EP},X}$ can be interpreted as two polynomial quantifiers having as much power as one exponential quantifier. This result is also known from Heller (1984a).

5.2. *$\leqslant_T^{\mathrm{P}}$-Reducibility to Sparse Sets*

In the following we will deal with a relativized version of $\leqslant_T^{\mathrm{P}}$-reducibility. Relativized reducibility means that the reduction procedure can ask queries to the oracle; i.e., $A \leqslant_T^{\mathrm{P},X} B$ iff there is a deterministic polynomial oracle machine M, which outfitted with oracle X and B accepts A. Karp and Lipton (1980) have proved tthe following result which is stated here in a relativized form.

PROPOSITION 1. *For all oracles X, if there is a sparse set S, such that* $\mathrm{NP}(X) \leqslant_T^{\mathrm{P},X} S$, *then* $\Sigma_2^{\mathrm{P},X} = \Pi_2^{\mathrm{P},X}$ *and* PH(X) is $\leqslant_T^{\mathrm{P},X}$*-reducible to a sparse set.*

THEOREM 3. *There is an oracle X and a sparse set S such that* $\Delta_2^{\mathrm{EP},X} \leqslant_T^{\mathrm{P},X} S$.

Proof. Let X be as in Theorem 1. Relativization of a result of Adleman (1978) shows that for all oracles Y there is a sparse set S such that $\mathrm{R}(Y) \leqslant_T^{\mathrm{P},Y} S$. Since $\mathrm{R}(X) = \mathrm{NP}(X)$, we get $\mathrm{NP}(X) \leqslant_T^{\mathrm{P},X} S$ for a sparse set S. Proposition 1 shows that PH(X) is $\leqslant_T^{\mathrm{P},X}$- reducible to a sparse set S. By Theorem 2, $\mathrm{PH}(X) = \Sigma_2^{\mathrm{P},X} = \Delta_2^{\mathrm{EP},X}$ and therefore $\Delta_2^{\mathrm{EP},X} \leqslant_T^{\mathrm{P},X} S$. Q.E.D.

Wilson (1983) proved a similar result in a slightly different setting. He defined relativized circuits and showed that there is an oracle X such that $\Delta_2^{\mathrm{EP},X}$ has relativized polynomial size circuits. Note that in the non-relativized case polynomial Turing reducibility to sparse sets is equivalent to having polynomial size circuits (see Bennet and Gill, 1981). Assuming that properties of relativized complexity classes may hold in the non-relativized case, then Theorem 3 shows also that Δ_2^{EP} may have polynomial size circuits, which, however, seems to be very unlikely.

5.3. *Sparse Sets in the Polynomial Hierarchy and the Exponential Hierarchy*

The following results of Hartmanis, Sewelson, and Immerman (1983) are of interest here:

PROPOSITION 2. *For all oracles Y there is a sparse set in* $\mathrm{NP}(Y) - \mathrm{P}(Y)$ *iff* $\mathrm{EL}(Y) \subsetneq \mathrm{NEL}(Y)$.

PROPOSITION 3. *There exists an oracle Z such that there is a sparse set in* co $\mathrm{NP}(Z) - \mathrm{P}(Z)$, *but there are no sparse sets in* $\mathrm{NP}(Z) - P(Z)$.

The following result is similar to Proposition 3:

THEOREM 4. *There is an oracle X such that there is a sparse set in* $\Sigma_2^{\mathrm{P},X} - \Delta_2^{\mathrm{P},X}$ *but no sparse set in* $\mathrm{NP}(X) - \mathrm{P}(X)$.

Proof. In Theorem 1 we actually proved that $D_2(X)$ is in EL(X): for a given x we can test whether $x \in D_2(x)$ by evaluating two linearly bounded quantifiers over a predicate computable in linear time relative to X. The evaluation can be done in deterministic exponential linear time. Therefore $\mathrm{EL}(X) = \mathrm{NEL}(X) = \Delta_2^{\mathrm{EL},X}$. This guarantees that there is no sparse set in $\mathrm{NP}(X) - \mathrm{P}(X)$. On the other hand $\Delta_2^{\mathrm{EL},X} \subsetneq \Sigma_2^{\mathrm{EL},X}$, because otherwise we would have $\Delta_2^{\mathrm{EP},X} = \Sigma_2^{\mathrm{EP},X}$, a contradiction to Theorem 2. Therefore

$\mathrm{EL}(K(X)) \subsetneq \mathrm{NEL}(K(X))$. This shows that there are sparse sets in $\mathrm{NP}(K(X)) - \mathrm{P}(K(X))$ which is $\Sigma_2^{\mathrm{P},X} - \Delta_2^{\mathrm{P},X}$. Q.E.D.

With the following two results we can strengthen Theorem 4.

Proposition 4 (Proved by S. Mahaney, 1982). *If* NP *is* $\leqslant_T^{\mathrm{P}}$*-reducible to a sparse set, then there is a sparse set in* Σ_2^{P} *such that* PH *is* $\leqslant_T^{\mathrm{P}}$*-reducible to* S.

Proposition 5 (Proved by Long, 1982). *If the polynomial hierarchy* PH *is* $\leqslant_T^{\mathrm{P}}$*-reducible to a sparse set in* Δ_2^{P}, *then* PH *collapses to* Δ_2^{P}.

Relativizations of Proposition 4 and 5 hold also. Using this we can conclude that there exists an oracle X such that $\Sigma_2^{\mathrm{P},X} = \mathrm{PH}(X) = \Delta_2^{\mathrm{EP},X}$ is $\leqslant_T^{\mathrm{P},X}$-reducible to a sparse set in $\Sigma_2^{\mathrm{P},X}$ (Proposition 4), which is not in $\Delta_2^{\mathrm{P},X}$ (by Proposition 5 and $\Delta_2^{\mathrm{P},X} \subsetneq \Sigma_2^{\mathrm{P},X}$) and there is no sparse set in $\mathrm{NP}(X) - \mathrm{P}(X)$. This shows that there exists an X such that there is no sparse set in $\mathrm{NP}(X) - \mathrm{P}(X)$, but there is a powerful sparse set S in $\Sigma_2^{\mathrm{P},X}$: $\mathrm{PH}(X)$ is $\leqslant_T^{\mathrm{P},X}$-reducible to S.

5.4. *Probabilistic Complexity Classes*

In this section we will see which inclusion relations we can get for probabilistic complexity classes from Theorem 1. First we prove a property of the operators NP and R.

Lemma 5. $\mathrm{NP}(\mathrm{R}(X)) \subseteq \mathrm{R}(\mathrm{NP}(X))$ *for all oracles* X.

Proof. Let $L \in \mathrm{NP}(\mathrm{R}(X))$; i.e., $L = \mathrm{NP}_i^{R_j^X}$, where

$$y \in R_j^X \leftrightarrow \exists z\, [|z| = p(|y|) \wedge P^X(y, z)]$$
$$\leftrightarrow \exists 2^{p(|y|)-1} z\, [|z| = p(|y|) \wedge P^X(y, z)]$$

for some polynomial time predicate P^X and some polynomial p. That means for all y in R_j^X there are many witnesses z, which testify $y \in R_j^X$. The witnesses are the accepting computation paths of the underlying nondeterministic polynomial machine. By an argument similar to that of Adleman (1978) proving that R has polynomial size circuits, it follows that there exists a set of witnesses $Z = \{z_1, ..., z_{p(|y|)}\}$ with $|z_i| \leqslant p(|y|)$, such that $y \in R_j^X \leftrightarrow \bigvee_{z \in Z} P^X(y, z)$. The following algorithm A tests for a given x, whether $x \in \mathrm{NP}_i^{R_j^X}$:

A:

Step 1: Guess a set of witnesses $Z = \{z_1, ..., z_{p(|y|)}\}$.

Step 2: Verify that $\forall y[(|y| < p_i(|x|) \wedge y \in R_j^X) \Rightarrow \bigvee_{z \in Z} P^X(y, z)]$. (Note that on x, only strings of length $< p_i(|x|)$ will be asked about in computations of NP_i. This step guarantees that Z contains sufficient information to check deterministically in polynomial time (with machine P^X) membership in R_j^X for strings of length $< p_i(|x|)$.)

Step 3. Verify that $x \in \mathrm{NP}_i^{R_j^X}$, by computing NP_i on x and answering queries y to the oracle by evaluating the predicate $\bigvee_{z \in Z} P^X(y, z)$.

For all y we have

$$y \in R_j^X \leftrightarrow \exists u\ [|u| = p(|y|) \wedge P^X(y, u)].$$

Therefore the formula in step 2 is equivalent to

$$\forall y[(|y| < p_i(|x|) \wedge \exists u\ [|u| = p(|y|) \wedge P^X(y, u)]) \Rightarrow \bigvee_{z \in Z} P^X(y, z)].$$

Further transformations yield

$$\forall y[|y| < p_i(|x|) \Rightarrow (\forall u[|u| = p(|y|) \Rightarrow \neg P^X(y, u)] \vee \bigvee_{z \in Z} P^X(y, z))]$$

and

$$\forall \langle y, u \rangle [(|y| < p_i(|x|) \wedge |u| = p(|y|) \Rightarrow (\neg P^X(y, u) \vee \bigvee_{z \in Z} P^X(y, z))].$$

This shows that in step 2 we have a $\Pi_1^{\mathrm{P},X}$ computation. Step 3 is a $\Sigma_1^{\mathrm{P},X}$ computation. A probabilistic argument shows that more than half of the sets Z satisfy step 2. This argument uses the fact that for languages in $R(X)$ we can assume an exponentially small error probability, i.e., the number of witnesses is large. Therefore using $\mathrm{R}(\mathrm{P}(\mathrm{NP}(X))) = \mathrm{R}(\mathrm{NP}(X))$, the whole algorithm A turns out to be a $\mathrm{R}(\mathrm{NP}(X))$ computation. Q.E.D.

THEOREM 6. *There exists a recursive set X such that $\Sigma_2^{\mathrm{R},X} = \Delta_2^{\mathrm{EP},X}$.*

Proof. Let X be as in Theorem 1. Since $\mathrm{R}(X) = \mathrm{NP}(X)$ and by Lemma 5 we get $\Sigma_2^{R,X} = \mathrm{R}(\mathrm{R}(X)) = \mathrm{R}(\mathrm{NP}(X)) \supseteq \mathrm{NP}(\mathrm{R}(X)) = \Sigma_2^{\mathrm{P},X}$. Therefore $\Sigma_2^{\mathrm{R},X} = \Sigma_2^{\mathrm{P},X}$. The claim follows from Theorem 2. Q.E.D.

Theorem 6 shows that for oracle X as in Theorem 1, the polynomial hierarchy and the probabilistic hierarchy are identical. Note that they extend two levels: $\Sigma_2^{\mathrm{P},X} = \Pi_2^{\mathrm{P},X} = \Sigma_2^{\mathrm{R},X} \supseteq \Delta_2^{\mathrm{P},X} = \Delta_2^{\mathrm{R},X}$.

Remark. Note that for a relativized version it is possible to encode nondeterministic exponential time into R: there exists a Y such that $\mathrm{R}(Y) = \mathrm{EP}(Y)$ (see Kurtz, 1983; Heller, 1983). In this case we get $\mathrm{P}(Y) \subsetneq \mathrm{R}(Y) = \mathrm{EP}(Y) \subsetneq \mathrm{NEP}(Y)$. The random hierarchy relative to Y is equal to the polynomial hierarchy $\mathrm{PH}(Y)$ and they both extend 1 level: $\mathrm{P}(Y) \subsetneq \Sigma_1^{\mathrm{P},Y} = \Pi_1^{\mathrm{P},Y} = \Sigma_1^{\mathrm{R},Y} = \Pi_1^{\mathrm{R},Y}$.

THEOREM 7. *There exists an X such that* $\mathrm{BPP}(X) = \Delta_2^{\mathrm{EP},X}$.

Proof. Since $\mathrm{RH}(X) \subseteq \mathrm{BPP}(X)$ (see also results of Zachos (1983) and Ko (1982)), the claim follows from Theorem 6. Q.E.D.

5.5. *Problems Shown to Be Difficult*

Inclusion relations shown for relativized complexity classes are often counterintuitive, but demonstrate that we cannot discard such relations for the corresponding nonrelativized complexity classes. These relations are consistent with any argumentation which relativizes. Disproving them would require methods, which do not relativize. But we know almost no such methods. Presumably such methods are more complicated or at least less understood. Therefore relativized results may show the borderline at which problems get difficult. Because of the relativized results shown here, it will be difficult to improve the following nonrelativized results:

(1) If $\mathrm{NP} \leqslant_T^{\mathrm{P}} S$ for some sparse set S, then $\Sigma_2^{\mathrm{P}} = \Pi_2^{\mathrm{P}}$ (see Karp and Lipton, 1980, see also Proposition 3).

(2) $\Sigma_2^{\mathrm{EL}} \cap \Pi_2^{\mathrm{EL}}$ is not $\leqslant_T^{\mathrm{P}}$-reducible to a sparse set (see Kannan, 1981).

(3) $\mathrm{BPP} \subseteq \Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}}$ (See Sipser, 1983 and Lautemann, 1983).

Let X be as in Theorem 1, 2, 3, 4, and 6.

Comment to (1). We have $\mathrm{NP}(X) \leqslant_T^{\mathrm{P},X} S$ for some sparse set S (Theorem 3) but $\Delta_2^{\mathrm{P},X} \subsetneq \Sigma_2^{\mathrm{P},X}$. Therefore it will not be easy to improve the result of Karp and Lipton, such that $\mathrm{NP} \leqslant_T^{\mathrm{P}} S$ for some sparse set S would imply $\Delta_2^{\mathrm{P}} = \Sigma_2^{\mathrm{P}}$. This has also been observed by Wilson (1983). A slightly weaker result can be found in Immerman and Mahaney (1983).

Comment to (2). We have $\Delta_2^{\mathrm{EP},X} \leqslant_T^{\mathrm{P},X} S$ for some sparse set S. It will therefore be difficult to show that Δ_2^{EP} or (Δ_2^{EL}) is not polynomial Turing reducible to a sparse set, respectively, does not have polynomially sized circuits. This has also been observed by Wilson (1983).

Comment to (3). We have seen that there exists an X such that $\Delta_2^{\mathrm{P},X} \subsetneq \Sigma_2^{\mathrm{P},X} = \mathrm{BPP}(X)$. Therefore showing that $\mathrm{BPP} \subseteq \Delta_2^{\mathrm{P}}$ seems to be a hard problem. A similar observation has been made by Stockmeyer (1983). On the other hand the following result, stated here in a relativized version, has been shown by Zachos (1983).

LEMMA 8. $\mathrm{R}(X) \subsetneq \mathrm{NP}(X)$ *iff* $K(X) \notin \mathrm{BPP}(X)$.

Sketch of a Proof. We show that $K(X) \in \mathrm{BPP}(X)$ implies $\mathrm{R}(X) = \mathrm{NP}(X)$. The other direction is trivial since $\mathrm{R}(X) \subseteq \mathrm{BPP}(X)$. Let $K(X) \in \mathrm{BPP}(X)$. Assume without loss of generality that nondeterministic Turing machines, when in nondeterministic states, have the choice between two different next states. Words over the alphabet $\{0, 1\}$ represent sequences of choices in a nondeterministic computation. Let $x = \langle i, b, 0^k \rangle$ be given. If $x \in K(X)$ then there is a string $c = c_1 \cdots c_m$ over $\{0, 1\}$, $m < k$, such that NP_i^X accepts a in $<k$ steps, if nondeterministic choices are made according to c. Since $K(X) \in \mathrm{BPP}(X)$ there is a BPP(X) machine M accepting $K(X)$. We can use M in a binary search to determine c. Therefore, with high probability we will find c which represents an accepting computation; i.e. we do not accept an x which is not in $K(X)$. Therefore $K(X) \in \mathrm{R}(X)$ and so $\mathrm{R}(X) = \mathrm{NP}(X)$. Q.E.D.

Therefore if $\mathrm{R}(X) \subsetneq \mathrm{NP}(X)$ then $K(X) \notin \mathrm{BPP}(X) \subseteq \Sigma_2^{\mathrm{P},X} \cap \Pi_2^{\mathrm{P},X}$. This indicates that under the hypothesis that $\mathrm{R} \neq \mathrm{NP}$, it might be possible to improve the result of Sipser (1983) and Lautemann (1983); there might be a characterization below $\Sigma_2^{\mathrm{P}} \cap \Pi_2^{\mathrm{P}}$ for BPP in this case.

6. Conclusion

The results shown in this paper are quite powerful. They subsume many results about relativized computations; see Wilson (1983), Long (1978, 1982), Heller (1984a, 1984b), Stockmeyer (1983), Immerman and Mahaney (1983). As it is often the case, the relativization done here shows that certain questions about complexity classes are likely to be difficult to answer. Equalities and inclusion relations between the relativized complexity classes shown here may as well hold in the nonrelativized case, though some of them seem to be very unlikely. It would be of great interest to find properties of the nonrelativized complexity classes, which would at least exclude such unbelievable relations as, for example, $\mathrm{BPP} = \Delta_2^{\mathrm{EP}}$ (see Theorem 7).

Received December 19, 1983; accepted March 31, 1986

References

Adleman, L. (1978), Two theorems on random polynomial time, *in* "Proc. 19th FOCS, pp. 75–83.

Baker, T., Gill, J., and Solovay, R. (1975). Relativizations of the P = NP? question, *SIAM J. Comput.* **4** (4), 431–442.

Bennet, C. H., and Gill, J. (1981), Relative to a random oracle A, $\mathrm{P}^A \neq \mathrm{NP}^A \neq \mathrm{co\ NP}^A$ with probability 1, *SIAM J. Comput.* **10**, 96–112.

Hartmanis, J., Sewelson, V., and Immerman, N., Sparse sets in NP-P: EXPTIME versus NEXPTIME, *in* "Proc. 15th STOC," pp. 382–391.

Heller, H. (1983), On relativized polynomial hierarchies extending two levels, *in* "Conference on Computational Complexity Theory, March 21–25, 1983, Santa Barbara Calif." pp. 109–114.

HELLER, H., (1984a), Relativized polynomial and exponential computations, *SIAM J. Comput.* **13** (4), 717–725.

HELLER, H. (1984b), Relativized polynomial hierarchies extending two levels, *Math. System Theory* **17**, 71–84.

IMMERMAN, N., AND MAHANEY, S. (1983), Oracles for which NP has polynomial size circuits, *in* "Conference on Computational Complexity Theory," March 21–25, Santa Barbara, Calif., pp. 89–93.

KANNAN, R. (1981), A circuit size lower bound, *in* "Proc. 22nd FOCS, pp. 304–309.

KARP, R., AND LIPTON, R. (1980), Some connections between nonuniform and uniform complexity classes, *in* "Proc. 12th STOC," pp. 302–309.

KO, K. (1982), Some observations on probabilistic algorithms and NP-hard problems, *Inform. Process. Lett.* **14**, 39–43.

KURTZ, S. (1983), The fine structure of NP: Relativizations, *in* "Conference on Computational Complexity Theory," Calif., pp. 42–50.

LAUTEMANN, C. (1983), "BPP and the Polynomial Hierarchy," Techn. Uni. Berlin, Informatik, Report 83–96; *Inform. Process. Lett.* **17**, 215–217.

LONG, T. (1978), "On Some Polynomial Time Reducibilities," Dissertation, Purdue Univ. Lafayette, Ind.

LONG, T. (1982), A note on sparse oracles for NP, *Comput. System Sci.* **24**, 224–332.

MAHANEY, S. (1982), Sparse complete sets for NP: Solution of a conjecture of Berman and Hartmanis, *J. Comput. System Sci.* **25**, 130–143.

ROGERS, H. (1967), "Theory of Recursive Functions and Effective Computability," McGraw–Hill, New York.

SIPSER, M. (1983), A complexity theoretic approach to randomness, *in* "Proc. 15th STOC," pp. 330–335.

STOCKMEYER, L. (1983), The complexity of approximate counting, *in* "Proc. 15th STOC," pp. 118–126.

WILSON, C. (1983), Relativized circuit complexity, *in* "Proc. 24th FOCS," pp. 329–334.

ZACHOS, S. (1983), Collapsing probabilistic polynomial hierarchies, *in* "Conference on Computational Complexity Theory, March 21–25," Santa Barbara, Calif., pp. 75–81.