A General Method to Construct Oracles Realizing Given Relationships between Complexity Classes

(Technical Report 500 of University of Rochester)

Andrei A. Muchnik*†
amuchnik@int.glas.apc.org

Nikolai K. Vereshchagin §‡
ver@math.math.msu.su

Abstract

We present a method to prove oracle results of the following type. Let $K_1, \ldots, K_{2n}$, and $L_1, \ldots, L_{2m}$ be complexity classes. Our method provides a general framework for constructing an oracle A such that $K_{2i-1}^A \neq K_{2i}^A$ for $i = 1, \ldots, n$ and $L_{2j-1}^A = L_{2j}^A$ for $j = 1, \ldots, m$. Using that method we prove several results of this kind. The hardest of them is the existence of an oracle A such that $\mathbf{P}^A \neq \mathbf{NP}^A$, $\mathbf{P}^A = \mathbf{BPP}^A$, and both $\mathbf{Co\text{-}NP}^A$-sets and $\mathbf{NP}^A$-sets are $\mathbf{P}^A$-separable. We exhibit also two theorems that cannot be proved by that method.

1 Introduction

When people realized that $\mathbf{P} \neq \mathbf{NP}$ is likely true but hard to prove (and impossible to prove by relativizable arguments [BGS 75]), they began to prove interesting theorems under $\mathbf{P} \neq \mathbf{NP}$ hypothesis. Interesting problems of this kind arise in cryptography, where the reliability of all known protocols is based on complexity assumptions even stronger than $\mathbf{P} \neq \mathbf{NP}$. A very challenging problem is to construct cryptographical protocols which are

*This research was in part supported by the grant from the American Mathematical Society former Soviet Union Aid Fund, by the Soros grant from the International Science Foundation, an NAS/NRC COBASE grant, and NSF grant CCR-8957604. Work done in part while visiting the University of Rochester.

†Institute of New Technologies, 11 Kirovogradskaja Street, Moscow, 113587 Russia

‡Dept. of Mathematical Logic, Moscow State University, Moscow 119899, Russia

§All the results in this paper are joint results by both authors. The text was written by the second author.

provably secure if $\mathbf{P} \neq \mathbf{NP}$. In the present paper we ascertain that many complexity assertions cannot be proved by relativizable arguments even under the $\mathbf{P} \neq \mathbf{NP}$ assumption or even under stronger assumptions. In other words, we construct oracles relative to which certain Boolean combinations of the $\mathbf{P} \neq \mathbf{NP}$ assumption and stronger ones are true. Moreover, we investigate a general powerful method to prove such theorems and in the last section we present some theorems which cannot be proved by that method.

Many results of this sort (when an oracle is constructed under which some boolean combination of complexity assertions is true) have appeared in literature. The following results among them deal with the classes considered in the present paper. Rackoff in [R 78] constructed oracles A and B such that $\mathbf{P}^A = \mathbf{R}^A \neq \mathbf{NP}^A$ and $\mathbf{P}^B \neq \mathbf{R}^B = \mathbf{NP}^B$. In [BGS 75], it was proved that $\mathbf{P} = \mathbf{NP} \cap \mathbf{Co\text{-}NP} \neq \mathbf{NP}$ under some oracle.

In the present paper we prove, for example, that there exists an oracle under which $\mathbf{P} \neq \mathbf{NP}$ and **NP**-sets are separable, thus we solve the problem left open in [GS 88]. This implies that reliability of all the cryptographical schemes based on the existence of one-way functions cannot be derived from $\mathbf{P} \neq \mathbf{NP}$ by relativizable arguments (since one-way functions do not exist if **NP**-sets are separable). Moreover, we show that one cannot prove using relativizable arguments that **NP**-sets are inseparable even under hypothesis that both **Co-NP**-sets are inseparable and $\mathbf{P} \neq \mathbf{R}$. The strongest result of our paper states that there exists an oracle under which $\mathbf{P} \neq \mathbf{NP}$ and **NP**-sets are separable and **Co-NP**-sets are separable and $\mathbf{P} = \mathbf{BPP}$. In other words, it is impossible to prove by relativizable arguments even the disjunction "**NP**-sets are inseparable or **Co-NP**-sets are inseparable or $\mathbf{P} \neq \mathbf{BPP}$" under $\mathbf{P} \neq \mathbf{NP}$ hypothesis.

The method to solve such problems goes back to [BGS 75]. We call it "the universum method". In a sense the method may be viewed as the forcing method in a general form (see subsection 3.2.1). In the present paper we refine that method and apply it to prove the existence of oracles relative to which certain boolean combinations of the assertions $\mathbf{P} = \mathbf{NP}$, $\mathbf{P} = \mathbf{R}$, $\mathbf{P} = \mathbf{BPP}$, $\mathbf{P} = \mathbf{NP} \cap \mathbf{Co\text{-}NP}$, $\mathbf{P} = \mathbf{R} \cap \mathbf{Co\text{-}R}$, "**NP**-sets are **P**-separable", and "**Co-NP**-sets are **P**-separable" hold (we are successful to construct oracles for 13 of 17 possible combinations, thus 4 problems of this kind remain unsolved).

Roughly speaking, the method works as follows. Suppose we want to prove that there exists an oracle A such that $\mathbf{P}^A \neq \mathbf{BPP}^A$ and $\mathbf{P}^A = \mathbf{R}^A$. First, we define a subset V (called *the universum*) of the set of all oracles. Second, we choose a sufficiently powerful oracle H (in all known applications

we can take any **PSPACE**-complete set as H). Third, we consider machines having two oracles: the oracle H and a varying oracle B ranging over V. (Thus, every machine of this type accepts a subset of $\mathbf{B}^* \times V$, where $\mathbf{B} = \{0,1\}$ is the input alphabet.) Finally, we prove that there exists a BPP-machine of this type which recognizes a subset of $\mathbf{B}^* \times V$ recognizable by no P-machine of this type and to prove that for any R-machine of this type there exists a P-machine of this type recognizing the same subset of $\mathbf{B}^* \times V$.

In the next section we introduce some notation and prove a sample theorem to exhibit all main ideas of the method in the simplest situation. In Section 3 we prove three general theorems on the universum method, which will considerably simplify all its further applications. In Section 4 we obtain specific results applying our method. In particular, we give a simple proof of the result by [HI 86] that there exists an oracle relative to which $\mathbf{P} \neq \mathbf{NP} \cap \mathbf{Co\text{-}NP} \neq \mathbf{NP}$ and $\mathbf{NP} \cap \mathbf{Co\text{-}NP}$ has a complete problem. In Section 5 we prove that the method fails to prove some true assertions.

2 Preliminaries

2.1 Notations

We restrict ourselves to binary alphabet $\mathbf{B} = \{0,1\}$. The set of all binary words is denoted by $\mathbf{B}^*$. The set of all functions from $\mathbf{B}^*$ into $\mathbf{B}$ is denoted by Ω. A language $L \subset \mathbf{B}^*$ is identified with its characteristic function. We say that a language L *separates* two disjoint languages L_0 and L_1 if $L_0(x) = 1 \Rightarrow L(x) = 0$ and $L_1(x) = 1 \Rightarrow L(x) = 1$ for any $x \in \mathbf{B}^*$. Call any language from a class C of languages a *C-set*. An *oracle* is an element of Ω.

We say that $\mathbf{NP}^A$*-sets* ($\mathbf{Co\text{-}NP}^A$*-sets*) are *separable* if any two disjoint $\mathbf{NP}^A$-sets ($\mathbf{Co\text{-}NP}^A$-sets) are separable by a $\mathbf{P}^A$-set. If this is not the case, then we say that $\mathbf{NP}^A$-sets ($\mathbf{Co\text{-}NP}^A$-sets) are *inseparable*.

Denote by $\mathbf{B}^n$ the set of all binary words of length n. Denote by $\mathbf{B}^{\leq n}$ ($\mathbf{B}^{\geq n}$) the set of all binary words of length at most n (at least n, respectively).

Denote by $f|D$ the restriction of function f to set D.

Let us define the binary operation $\oplus$ on languages as follows: $B \oplus C = \{0u \mid u \in B\} \cup \{1v \mid v \in C\}$ (we denote by xy the concatenation of words x and y).

An *interval* is a set of oracles having the form

$$\Gamma(\varphi) = \{A \in \Omega \mid \forall y \in \mathrm{Dom}(\varphi)\ A(y) = \varphi(y)\},$$

where φ is a function from a finite subset of $\mathbf{B}^*$ into $\mathbf{B}$, and $\mathrm{Dom}(\varphi)$ denotes the domain of φ.

For a function ψ from a subset of $\mathbf{B}^*$ into $\mathbf{B}$ denote by $\hat{\psi}$ the oracle

$$\hat{\psi}(y) = \begin{cases} \psi(y), & \text{if } y \in \mathrm{Dom}(\psi), \\ 0, & \text{if } y \in \mathbf{B}^* \setminus \mathrm{Dom}(\psi). \end{cases}$$

Denote by $|y|$ the length of word y. For a finite set $M \subset \mathbf{B}^*$ denote by $\mathit{maxlength}\,(M)$ the $\max_{y \in M} |y|$, denote by $|M|$ the number of elements of M and by $\mathit{size}\,(M)$ the $\max\{|M|, \mathit{maxlength}\,(M)\}$.

When we speak about an oracle machine we consider oracle as its extra input. In particular, when we say "the work of M on input $\langle x, A\rangle$" we mean the work of M with oracle A on input x, and so on.

For oracle machine P, oracle A and $x \in \mathbf{B}^*$, denote by $\mathit{Query}_P(x, A)$ the set of all $y \in \mathbf{B}^*$ such that P asks '$A(y) =?$' during the computation on input $\langle x, A\rangle$. Let B be another oracle. Denote by $\mathit{Query}_P^A(x, A \oplus B)$ the set of all $y \in \mathbf{B}^*$ such that P asks '$A(y) =?$' during the computation on input $\langle x, A \oplus B\rangle$. (To be more precise, $\mathit{Query}_P^A(x, A \oplus B) = \{y \mid 0y \in \mathit{Query}_P(x, A \oplus B)\}$.) Let N be a nondeterministic oracle machine and c be one of its computations with oracle A on some input. Denote by $\mathit{Query}_N(c, A)$ the set of all $y \in \mathbf{B}^*$ such that N asks '$A(y) =?$' during the computation c. We consider probabilistic machines as those having an extra "random" input. Let M be a probabilistic machine, x be its input and r be its random input. Denote by $\mathit{Query}_M(r, x, A)$ the set of all $y \in \mathbf{B}^*$ such that M asks '$A(y) =?$' during the computation on input $\langle x, r, A\rangle$. In the similar way the notations $\mathit{Query}_N^A(c, A \oplus B)$ and $\mathit{Query}_M^A(r, x, A \oplus B)$ are defined.

For a function ψ defined on a finite set D denote by $\#_1\psi$ the number of $y \in D$ such that $\psi(y) = 1$ (we use also the notation $\#_0\psi$ defined in the similar way).

Let x be a binary word of length n. Denote by $\bar{x}$ the word $x(1)x(1)x(2)x(2) \ldots x(n)x(n)01$ (for example, $\overline{010} = 00110001$). We use $\bar{x}y$ as the code of the pair $\langle x, y\rangle$.

2.2 A sample application of the universum method

Theorem 2.1 *There exists an oracle A such that $\mathbf{NP}^A$-sets are separable and $\mathbf{Co\text{-}NP}^A$-sets are inseparable.*

Proof. The proof of this theorem is very close to the proof of the theorem

from [BGS 75] stating that $\mathbf{P}^A = \mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A \neq \mathbf{NP}^A$ for some oracle A.

Consider the following set of oracles:

$$V = \{B \in \Omega \mid \text{ for all } n \in \mathbf{N} \text{ there exists at most one } y \in \mathbf{B}^n \text{ such that } B(y) = 1\}.$$

Let us fix a **PSPACE**-complete language H. The oracle A will have the form $B \oplus H$, where B is in V. Thus, we have to define the oracle B.

We construct B in such a way that the sets

$$L_0^B = \{1^n \mid \text{there exists } y \in \mathbf{B}^n \text{ such that } B(0y) = 1\},$$
$$L_1^B = \{1^n \mid \text{there exists } y \in \mathbf{B}^n \text{ such that } B(1y) = 1\}$$

are $\mathbf{P}^A$-inseparable. Obviously, both L_0^B and L_1^B belong to $\mathbf{NP}^{B\oplus H}$ and are disjoint if $B \in V$.

So we have to construct an oracle $B \in V$ such that

1) L_0^B and L_1^B are separable by no $\mathbf{P}^{B\oplus H}$-set, and

2) any two disjoint $\mathbf{Co\text{-}NP}^{B\oplus H}$-sets are separable by some $\mathbf{P}^{B\oplus H}$-set.

Let M be a deterministic or nondeterministic machine. Write $M^A(x) = 1$ if M accepts $\langle x, A\rangle$ and write $M^A(x) = 0$ otherwise. Say that a pair $\langle N_0, N_1\rangle$ of nondeterministic oracle machines is *correct on* A if the languages $\{x \mid N_0^A(x) = 0\}$ and $\{x \mid N_1^A(x) = 0\}$ are disjoint. The assertion 1) means that for any polynomial-time oracle machine P the language $\{x \mid P^{B\oplus H}(x) = 1\}$ does not separate L_0^B from L_1^B. The assertion 2) means that for any pair $\langle N_0, N_1\rangle$ of polynomial-time nondeterministic oracle machines being correct on $B \oplus H$ there exists a $\mathbf{P}^{B\oplus H}$-set separating the set $\{x \mid N_0^{B\oplus H}(x) = 0\}$ from the set $\{x \mid N_1^{B\oplus H}(x) = 0\}$. Let P_0, P_1, ..., P_i, ... be an enumeration of deterministic polynomial-time oracle machines and $\langle N_{00}, N_{01}\rangle$, $\langle N_{10}, N_{11}\rangle$, ..., $\langle N_{j0}, N_{j1}\rangle$, ... be an enumeration of pairs of nondeterministic polynomial-time oracle machines.

In the step i, we construct an interval Γ_i intersecting with V in such a way that $\Gamma_1 \supset \Gamma_2 \supset \Gamma_3 \supset \ldots$ and the following holds:

if $i = 2k + 1$, then the language $\{x \mid P_k^{B\oplus H}(x) = 1\}$ does not separate L_0^B from L_1^B for any $B \in \Gamma_i \cap V$ and

if $i = 2k+2$, then either the pair $\langle N_{k0}, N_{k1}\rangle$ is not correct on $B \oplus H$ for any $B \in \Gamma_i \cap V$, or the languages $\{x \mid N_{k0}^{B\oplus H}(x) = 0\}$ and $\{x \mid N_{k1}^{B\oplus H}(x) = 0\}$ are separable by a $\mathbf{P}^{B\oplus H}$-set for all $B \in \Gamma_i \cap V$.

Obviously, for any oracle B from the set $V \cap \bigcap_{i=1}^{\infty} \Gamma_i$ the assertions 1) and 2) will hold.

We start with $\Gamma_0 = \Omega$. Let us explain what to do on each step. Let Γ_{i-1} be the interval constructed during $(i-1)$th step. On ith step we make the following. Consider two cases.

First case: $i = 2k+1$. Let

$$\Gamma_{i-1} = \Gamma(\varphi) = \{B \in \Omega \mid B|\mathrm{Dom}(\varphi) = \varphi\}.$$

We want to construct an interval $\Gamma \subset \Gamma_{i-1}$ such that the language $\{x \mid P_k^{B\oplus H}(x) = 1\}$ does not separate L_0^B from L_1^B for any $B \in \Gamma \cap V$.

Pick $n \in \mathbf{N}$ greater than $maxlength\,\mathrm{Dom}(\varphi)$ and so large that P_k on input $\langle 1^n, A\rangle$ makes less than 2^n queries to oracle. Without loss of generality we may assume that $P_k^{\hat{\varphi}\oplus H}(1^n) = 0$ (other case is entirely similar). We know that $|Query_{P_k}^{\hat{\varphi}}(1^n, \hat{\varphi}\oplus H)|$ is less than the number of words of length n. Pick a word u of the form $1z$ in the set $\mathbf{B}^{n+1} \setminus Query_{P_k}^{\hat{\varphi}}(1^n, \hat{\varphi}\oplus H)$. Let

$$\psi(y) = \begin{cases} \varphi(y), & \text{if } y \in \mathrm{Dom}(\varphi); \\ 1, & \text{if } y = u; \end{cases}$$

(note that u is not in $\mathrm{Dom}(\varphi)$ since $n > maxlength\,(\mathrm{Dom}(\varphi))$). Then we have $P_k^{\hat{\psi}\oplus H}(1^n) = 0$ and $1^n \in L_1^{\hat{\psi}}$. Let

$$\Gamma_i = \Gamma_{i-1} \cap \{B \in \Omega \mid B(y) = \hat{\psi}(y) \text{ for all } y \in \mathrm{Dom}(\psi) \cup Query_{P_k}^{\hat{\psi}}(1^n, \hat{\psi}\oplus H)\}.$$

The set $\Gamma_i \cap V$ is nonempty because $\hat{\psi} \in \Gamma_i \cap V$.

Second case: $i = 2k+2$. Consider two subcases.

First subcase: there exists an oracle $C \in \Gamma_{i-1} \cap V$ such that the pair $\langle N_{k0}, N_{k1}\rangle$ is not correct on $C \oplus H$. Then pick $x \in \mathbf{B}^*$ such that $N_{k0}^{C\oplus H}(x) = N_{k1}^{C\oplus H}(x) = 0$. Let

$$\Gamma_i = \{B \in \Omega \mid B(y) = C(y) \text{ for all } y \in \bigcup_c (Query_{N_{k0}}^{C}(c, C\oplus H) \cup Query_{N_{k1}}^{C}(c, C\oplus H))\}.$$

Second subcase: for any $C \in \Gamma_{i-1} \cap V$, the pair $\langle N_{k0}, N_{k1}\rangle$ is correct on $C \oplus H$. Then let $\Gamma_i = \Gamma_{i-1}$. We claim that for any $B \in \Gamma_i \cap V$, the sets $\{x \mid N_{k0}^{B\oplus H}(x) = 0\}$ and $\{x \mid N_{k1}^{B\oplus H}(x) = 0\}$ are separable by a $\mathbf{P}^{B\oplus H}$-set. In other words, there exists a polynomial-time oracle machine M that on input $\langle x, B\oplus H\rangle$ outputs $j \in \{0,1\}$ such that $N_{kj}^{B\oplus H}(x) = 1$. We construct

M in two steps. First, we define a polynomial-space oracle machine P satisfying the following two conditions:

1) $P^B(x)$ is equal to some j such that $N_{kj}^{B\oplus H}(x) = 1$ (for all $x \in \mathbf{B}^*$ and all $B \in V$);

2) $|Query_P(x, B)| \leq \mathrm{poly}(|x|)$ (this means that there exists a polynomial $p(n)$ such that $|Query_P(x, B)| \leq p(|x|)$) for all $x \in \mathbf{B}^*$, $B \in \Omega$).

Second, we construct a polynomial-time oracle machine M such that $P^B(x) = M^{B\oplus H}(x)$ for all $x \in \mathbf{B}^*$ and all $B \in \Omega$.

Machine P on input $\langle x, B\rangle$ works as follows. Let $\Gamma_i = \Gamma(\varphi)$. We know that $\Gamma_i \cap V \neq \emptyset$. Therefore, $\hat{\varphi} \in \Gamma_i \cap V$, consequently, $N_{k0}^{\hat{\varphi}\oplus H}(x) = 1$ or $N_{k1}^{\hat{\varphi}\oplus H}(x) = 1$. Find first an $l \in \{0, 1\}$ such that $N_{kl}^{\hat{\varphi}\oplus H}(x) = 1$ and find an accepting computation c of N_{kl} on $\langle x, \hat{\varphi} \oplus H\rangle$. This can be done within polynomial space by checking all the computations of N_{k0} and N_{k1} on input $\langle x, \hat{\varphi} \oplus H\rangle$. All the queries made to H in those computations can be answered within polynomial space because their lengths are bounded by $\mathrm{poly}(|x|)$ and $H \in \mathbf{PSPACE}$. Let $D_1 = Query_{N_{kl}}^{\hat{\varphi}}(c, \hat{\varphi} \oplus H)$. Then query '$B(y) =?$' for all $y \in D_1 \setminus \mathrm{Dom}(\varphi)$. If $B(y) = 0$ for all $y \in D_1 \setminus \mathrm{Dom}(\varphi)$, then $N_{kl}^{B\oplus H}(x) = 1$ provided $B \in \Gamma(\varphi)$; in this case output l. If there exists $y \in D_1 \setminus \mathrm{Dom}(\varphi)$ such that $B(y) = 1$, then set

$$\varphi_1(y) = \begin{cases} \varphi(y), & \text{if } y \in \mathrm{Dom}(\varphi); \\ B(y), & \text{if } y \in D_1 \setminus \mathrm{Dom}(\varphi); \end{cases}$$

(thus, $\mathrm{Dom}(\varphi_1) = \mathrm{Dom}(\varphi) \cup D_1$).

Note that $\#_1\varphi_1 > \#_1\varphi$.

Check if $\hat{\varphi}_1 \in V$. If this is not the case, then $B \notin V$ and we output 0. Otherwise repeat the whole process for φ_1 instead of φ, i.e., find an $l \in \{0, 1\}$ such that $N_{kl}^{\hat{\varphi}_1\oplus H}(x) = 1$ and so on. We will output a correct result or define a function φ_2 such that $\hat{\varphi}_2 \in V$ and $\#_1\varphi_2 > \#_1\varphi_1$. In the latter case repeat the whole process for φ_2 instead of φ. And so on until we output a result.

We claim that we make $\mathrm{poly}(|x|)$ loops. Indeed, assume that k loops were done, i.e., we have constructed φ_1, φ_2, ..., φ_k. Note that $\#_1\varphi < \#_1\varphi_1 < \#_1\varphi_2 < \ldots < \#_1\varphi_k$, therefore $\#_1\varphi_i \geq i$, in particular, $\#_1\varphi_{k-1} \geq k - 1$. On the other hand, $maxlength\,(\mathrm{Dom}(\varphi_{k-1})) \leq m(x)$, where

$$m(x) = \max\{maxlength\,(Query_{N_{kl}}^{B}(c, B \oplus H)) \mid \\ l = 0, 1,\ c \text{ is a computation of } N_{kl} \text{ on } x\}.$$

Since $\hat{\varphi}_{k-1} \in V$ we can conclude that $\#_1\varphi_{k-1} \leq m(x) + 1$.

Thus, $k \leq m(x) + 2$. Obviously, $m(x) \leq \text{poly}(|x|)$. We have made $\text{poly}(|x|)$ queries to B during each iteration of the loop. Therefore, the defined machine P satisfies the requirement 2), i.e., it makes $\text{poly}(|x|)$ queries.

Thus, it remains to prove the following

Lemma 2.1 *Let P be a polynomial-space oracle machine that on input x makes only* $\text{poly}(|x|)$ *queries. Then there is a polynomial-time oracle machine M such that $P^B(x) = M^{B \oplus H}(x)$ for all $x \in \mathbf{B}^*$, $B \in \Omega$ (recall that H is a* **PSPACE***-complete set).*

Proof. Define the functions $question\,(x, w)$ and $result\,(x, w)$ as follows. Let w be a binary word of length n. For any $i \leq n$ denote by $w(i)$ the ith symbol of w. Run the machine P on input x and give the answer $w(1)$ to the first query, the answer $w(2)$ to the second query and so on. There are three possibilities:

1) P makes exactly n queries and then produces a result say r; in this case set

$$question\,(x, w) = \$,\ \ result\,(x, w) = r;$$

2) P makes n queries and then makes $(n + 1)$st query, say '$B(y) =?$'; in this case set

$$question\,(x, w) = y,\ \ result\,(x, w) = \$;$$

3) P makes less than n queries; in this case set

$$question\,(x, w) = result\,(x, w) = \$.$$

So *question* is a function from $\mathbf{B}^* \times \mathbf{B}^*$ into $\mathbf{B}^* \cup \{\$\}$ and *result* is a function from $\mathbf{B}^* \times \mathbf{B}^*$ into $\{0, 1, \$\}$. Obviously, both functions *question* and *result* are computable within polynomial space. Therefore, they can be computed by a polynomial-time machine with oracle H. Let machine M work according the program shown on Figure 1.

Thus, the lemma and the theorem are proved.□

We are going to present a formal exposition of the universum method, which simplifies all its applications and allows to prove that in some cases it fails.

Figure 1: Program 1

begin
  $w := \Lambda$ (the empty word);
  while $result(x, w) = \$$
      commentary: $result(x, w)$ is computed
      in time poly$(|x|, |w|)$ by querying H;
    do $y := question(x, w)$;
        commentary: $question(x, w)$ is computed in
        time poly$(|x|, |w|)$ by querying H;
        $b := B(y)$;
        $w := wb$;
    od
  output $result(x, w)$
end

3 General theorems

3.1 Basic definitions

We deal with decision problems as well as with separation problems. It is convenient to consider a decision problem as a particular case of a separation problem.

Definition 3.1 *A separation problem is a function P from $\mathbf{B}^*$ into $\{0, 1, *\}$ (the meaning of this definition is as follows: we have to separate the set $\{x \mid P(x) = 0\}$ from the set $\{x \mid P(x) = 1\}$). A language is a separation problem L such that $L(x) \neq *$ for all $x \in \mathbf{B}^*$. A language L is identified with the set $\{x \mid L(x) = 1\}$.*

We deal with classes of machines in which not every machine defines a language (for example, not every polynomial-time probabilistic machine (BPP-machine) defines a language in **BPP**). Likewise not every pair of NP-machines $\langle N_0, N_1 \rangle$ defines a problem of separation of **NP**-sets; it defines a problem only if L_{N_0} and L_{N_1} are disjoint. It may also happen that for some oracle A, a probabilistic polynomial-time oracle machine M^A defines a language in $\mathbf{BPP}^A$ and for another oracle A machine M^A defines no

language in $\mathbf{BPP}^A$. We say that M is correct on A in the former case and we say that M is incorrect on A in the latter case.

Consider for every probabilistic polynomial-time oracle machine M the mapping

$$M(x,A) = \begin{cases} 1, & \text{if } M^A \text{ accepts } x \text{ with probability} \\ & \text{being greater than } 2/3; \\ 0, & \text{if } M^A \text{ rejects } x \text{ with probability} \\ & \text{being greater than } 2/3; \\ \#, & \text{otherwise.} \end{cases} \tag{1}$$

In the sequel we do not distinguish the machine M and the mapping $\langle x, A\rangle \mapsto M(x,A)$. Call any mapping from $\mathbf{B}^* \times \Omega$ into $\{0,1,\#\}$ an *oracle machine.*

Likewise, consider for every pair $N = \langle N_0, N_1\rangle$ of polynomial-time nondeterministic machines the mapping

$$N(x,A) = \begin{cases} 1, & \text{if } N_1^A(x) = 1,\ N_0^A(x) = 0; \\ 0, & \text{if } N_1^A(x) = 0,\ N_0^A(x) = 1; \\ *, & \text{if } N_0^A(x) = N_1^A(x) = 0; \\ \#, & \text{if } N_0^A(x) = N_1^A(x) = 1. \end{cases} \tag{2}$$

Definition 3.2 *A description is a mapping from the set* $\mathbf{B}^* \times \Omega$ *into the set* $\{0,1,\#,*\}$. *A description* D *is called correct on an oracle* A *if* $D(x,A) \neq \#$ *for all* $x \in \mathbf{B}^*$.

For example, (1) and (2) are descriptions, and (1) is an oracle machine.

Definition 3.3 *For a description* D *and for an oracle* A *denote by* D^A *the mapping* $x \mapsto D(x,A)$. *Given a class* $\mathcal{D}$ *of descriptions and an oracle* A *denote by* $\mathcal{D}^A$ *the set* $\{D^A \mid D \in \mathcal{D}$ and D is correct on $A\}$.

Obviously, if M is an oracle machine being correct on A, then M^A is a language.

Denote by BPP the set of all descriptions having the form (1), where M is a probabilistic polynomial-time oracle machine. (We use bold face letters for classes of languages, e.g., **BPP**, and roman letters for classes of descriptions, thus, BPP $\neq$ **BPP**, however $\mathrm{BPP}^A = \mathbf{BPP}^A$ for any A).

Denote by NP-separation the class of all descriptions of the form (2), where N_0 and N_1 are polynomial-time nondeterministic oracle machines. Likewise one can define Co-NP-separation, as well as classes of descriptions P, NP, R, R $\cap$ Co-R, NP $\cap$ Co-NP, PSPACE.

Say that a separation problem P_1 is *easier* than a separation problem P_2 ($P_1 \leq P_2$ in symbols) if $P_1(x) \neq *$ implies $P_2(x) = P_1(x)$. In other words, the $P_1(x) \leq P_2(x)$ for all $x \in \mathbf{B}^*$, where $\leq$ denotes the partial ordering on the set $\{0, 1, *\}$ defined by inequalities $* \leq 0$, $* \leq 1$. Given classes K_1 and K_2 of separation problems we write $K_1 \leq K_2$ if for any $P_1 \in K_1$ there exists $P_2 \in K_2$ such that $P_1 \leq P_2$. Obviously, if K_1 is a class of languages, then $K_1 \leq K_2$ means the same as $K_1 \subset K_2$. For example, $\mathrm{BPP}^A \leq \mathrm{P}^A$ means the same as $\mathbf{BPP}^A = \mathbf{P}^A$ and $(\text{NP-separation})^A \leq \mathrm{P}^A$ means that $\mathbf{NP}^A$-sets are separable.

3.2 The most general scheme of the universum method

The universum method can be applied for proving theorems of the following form. Let

$$\mathcal{K}_1, \ldots, \mathcal{K}_n,\ \mathcal{L}_1, \ldots, \mathcal{L}_n,\ \mathcal{M}_1, \ldots, \mathcal{M}_m,\ \mathcal{N}_1, \ldots, \mathcal{N}_m$$

be classes of descriptions. We wish to prove that there exists an oracle A such that

$$\mathcal{K}_i^A \not\leq \mathcal{L}_i^A \text{ for } i = 1, \ldots, n \text{ and}$$
$$\mathcal{M}_j^A \leq \mathcal{N}_j^A \text{ for } j = 1, \ldots, m.$$

Let us describe how this can be done. Consider for simplicity of notation the case $m = n = 1$.

Let us call a *universum* any nonempty subset V of Ω.

Definition 3.4 *A superuniversum is any countable family $\mathcal{V}$ of universums having a largest universum up to inclusion and such that the following two assertions hold:*

1. *For any $V \in \mathcal{V}$ and for any interval Γ intersecting with V there exists $V' \in \mathcal{V}$ such that $V' \subset V \cap \Gamma$.*

2. *For any infinite chain $V_1 \supset V_2 \supset V_3 \supset \ldots$ of elements of $\mathcal{V}$ the intersection $\bigcap_{i=1}^{\infty} V_i$ is non-empty.*

In all the applications presented in this paper, the elements of $\mathcal{V}$ are closed in Cantor's topology. This implies 2 because Ω is compact in Cantor's topology. Recall that Cantor's topology is the topology the base of which is the set of intervals.

For example, if V is closed in Cantor's topology, then the family

$$\mathcal{V}(V) = \{V \cap \Gamma \mid \Gamma \text{ is an interval intersecting with } V\}$$

is a superuniversum. We call superuniversums of the form $\mathcal{V}(V)$ *principal* superuniversums. In all the applications of the universum method but one we use only principal superuniversums. The largest universum in $\mathcal{V}$ is denoted by largest($\mathcal{V}$).

Thus, we wish to prove that there exists an oracle A for which

$$\mathcal{K}^A \not\leq \mathcal{L}^A,$$
$$\mathcal{M}^A \leq \mathcal{N}^A,$$

where $\mathcal{K}$, $\mathcal{L}$, $\mathcal{M}$, $\mathcal{N}$ are classes of descriptions. The method can be applied only if $\mathcal{K}$, $\mathcal{L}$, $\mathcal{M}$, and $\mathcal{N}$ are countable and consist of the so called polynomial-local descriptions.

Definition 3.5 *A description D is called polynomial-local if there exists a polynomial $p(n)$ such that for all $x \in \mathbf{B}^*$ and all $A, B \in \Omega$ if $A|\mathbf{B}^{\leq p(|x|)} = B|\mathbf{B}^{\leq p(|x|)}$, then $D(x, A) = D(x, B)$.*

The first general theorem holds for any countable classes of polynomial-local descriptions. The second and the third general theorems require some extra restrictions being formulated later. We will apply the method to the following classes:

$$\begin{gathered} \text{P, NP, R, BPP, NP-separation,} \\ \text{Co-NP-separation, NP} \cap \text{Co-NP,} \\ \text{R} \cap \text{Co-R, PSPACE} \end{gathered} \tag{3}$$

Obviously, all the classes in the list (3) consists of polynomial-local descriptions.

Let H be an oracle and D be a description.

Notation 3.1 *For a class of descriptions $\mathcal{D}$ denote by $\mathcal{D}(H)$ the class of descriptions $\{\langle x, A\rangle \mapsto D(x, A \oplus H) \mid D \in \mathcal{D}\}$.*

For example, BPP(H) is the class of descriptions of the form (1), where M is a polynomial-time probabilistic oracle machine having an extra oracle H. And generally, if $\mathcal{K}$ is a class of machines of certain type, then $\mathcal{K}(H)$ is the class of machines of that type having the extra oracle H.

Notation 3.2 *Write* $D_1^V \leq D_2^V$ *if* $D_1(x, A) \leq D_2(x, A)$ *for all* $x \in \mathbf{B}^*$ *and all* $A \in V$.

Definition 3.6 *A description* D *is correct on a universum* V *if* D *is correct on each element of* V. *Let* $\mathcal{D}$ *be a class of descriptions. A description* D *is* $\mathcal{D}$-solvable *on a universum* V *if there exists a description* E *in* $\mathcal{D}$ *such that* $D^V \leq E^V$. *If this does not hold* D *is called* $\mathcal{D}$-unsolvable.

Assume that for a superuniversum $\mathcal{V}$ and for an oracle H the following two assertions are true:

(a) There is a description in $\mathcal{K}(H)$ that is correct on largest($\mathcal{V}$) and which is $\mathcal{L}(H)$-unsolvable on any V in $\mathcal{V}$;

(b) for any $V \in \mathcal{V}$, any description M in $\mathcal{M}(H)$ being correct on V is $\mathcal{N}(H)$-solvable on some universum $V' \subset V$, $V' \in \mathcal{V}$, that is, there exist $V' \subset V$, $V' \in \mathcal{V}$ and $N \in \mathcal{N}(H)$ such that $M^{V'} \leq N^{V'}$.

We claim that in this case there exists an oracle A such that $\mathcal{K}^A \not\leq \mathcal{L}^A$ and $\mathcal{M}^A \leq \mathcal{N}^A$.

Theorem 3.1 *Let* $\mathcal{K}, \mathcal{L}, \mathcal{M}$, *and* $\mathcal{N}$ *be countable classes of polynomial-local descriptions,* H *be an oracle and* $\mathcal{V}$ *be a superuniversum such that* (a) *and* (b) *are true. Then there exists an oracle* A *such that* $\mathcal{K}^A \not\leq \mathcal{L}^A$ *and* $\mathcal{M}^A \leq \mathcal{N}^A$.

Proof. Let $\mathcal{K}$, $\mathcal{L}$, $\mathcal{M}$, $\mathcal{N}$, H, and $\mathcal{V}$ satisfy the conditions of the theorem. Let K be a description in $\mathcal{K}(H)$ which is correct on largest($\mathcal{V}$) and $\mathcal{N}(H)$-unsolvable on any $V \in \mathcal{V}$. We shall construct an oracle $B \in$ largest($\mathcal{V}$) such that the separation problem K^B is not easier than any problem in $\mathcal{L}(H)^B$ and such that $\mathcal{M}(H)^B \leq \mathcal{N}(H)^B$. Then for the oracle $A = B \oplus H$ the assertions $\mathcal{K}^A \not\leq \mathcal{L}^A$ and $\mathcal{M}^A \leq \mathcal{N}^A$ will be true.

Let M_0, M_1, ..., M_i, ... be an enumeration of $\mathcal{M}(H)$ and let L_0, L_1, ..., L_j, ... be an enumeration of $\mathcal{L}(H)$. We have to satisfy countably many requirements of two types: for each $i \in \mathbf{N}$ we have to satisfy the requirement

$$K^B \not\leq L_i^B$$

and for each $i \in \mathbf{N}$ we have to satisfy the requirement

$(*)$ M_i is incorrect on B or $M_i^B \leq N^B$ for some $N \in \mathcal{N}(H)$

We make ω steps enumerated by numbers $1, 2, 3, \ldots$. On a step j we define a universum V_j in such a way that $V_1 \supset V_2 \supset V_3 \supset \ldots$. More exactly, on a step $j = 2i + 1$ we construct a universum V_j such that $K^B \not\leq L_i^B$ for any $B \in V_j$. On a step $j = 2i + 2$ we ensure the ith condition of the form $(*)$, that is, we construct a universum V_j such that M_i is incorrect on B or $M_i^B \leq N^B$ for some $N \in \mathcal{N}(H)$ for all $B \in V_j$.

As B we take any oracle from the set $\bigcap_{i=1}^{\infty} V_i$. Thus it remains to describe what to do on each step.

Set $V_0 = \text{largest}(\mathcal{V})$. Let j be the number of the current step. Consider two cases.

First case: $j = 2i + 1$. Since K is $\mathcal{L}(H)$-unsolvable on $V_{j-1,}$ there exist $x \in \mathbf{B}^*$ and $C \in V_{j-1}$ such that $K(x, C) \not\leq L_i(x, C)$. Pick x and C satisfying this inequality. As both K and L_i are local there exists an interval Γ including C such that $K(x, B) = K(x, C)$ and $L_i(x, B) = L_i(x, C)$ for all $B \in \Gamma$ and, therefore, $K(x, B) \not\leq L_i(x, B)$ for all $B \in \Gamma$. By Condition 1 in definition of superuniversum, there exists a universum $V \in \mathcal{V}$ such that $V \subset V_{j-1} \cap \Gamma$. Set $V_j = V$. Obviously, $K^B \not\leq L_i^B$ for all $B \in V_j$.

Second case: $j = 2i + 2$. Assume first that M_i is correct on V_{j-1}. By Condition (b) there exist a description $N \in \mathcal{N}(H)$ and a universum $V' \subset V_{j-1}$,$V' \in \mathcal{V}$ such that $M_i(x, B) \leq N(x, B)$ for all $x \in \mathbf{B}^*$ and all $B \in V'$. Then we can set $V_j = V'$. Obviously, for all $B \in V_j$ the assertion $(*)$ holds. Otherwise (when M_i is incorrect on V_{j-1}) we can reason as in the first case because incorrectness is a local property.$\square$

3.2.1 A generalization of Theorem 3.1

A natural question is if the above theorem can be generalized to involve other assertions on relativized classes, for example, "$\mathcal{K}^A$ has a complete problem". The answer is affirmative.

The general approach is as follows. Suppose we wish to prove that there exists an oracle A such that an assertion $\varphi(A)$ on complexity classes is true. Suppose that the assertion $\varphi(Y)$ can be expressed by a closed formula in a first order language having atomic formulae of the form $P(x_1, \ldots, x_n, Y)$, where each variable x_i ranges over a countable set (possibly, different for different variables). (When we say that a formula is closed we do not consider Y as a variable.) For example, the assertion $\mathcal{K}^Y \not\leq \mathcal{L}^Y \& \mathcal{M}^Y \leq \mathcal{N}^Y$ can be expressed by the following closed formula:

$$\exists K \in \mathcal{K}(\forall x \in \mathbf{B}^* K(x, Y) \neq \# \ \& \ \neg\exists L \in \mathcal{L} \forall x \in \mathbf{B}^* K(x, Y) \leq L(x, Y))$$

$$\& \neg\exists M \in \mathcal{M}(\forall x \in \mathbf{B}^* M(x,Y) \neq \# \ \& \ \neg\exists N \in \mathcal{N} \forall x \in \mathbf{B}^* M(x,Y) \leq N(x,Y))$$

having atomic formulae "$K(x,Y) = \#$", $K \in \mathcal{K}$, "$M(x,Y) = \#$", $M \in \mathcal{M}$, "$K(x,Y) \leq L(x,Y)$", $K \in \mathcal{K}$, $L \in \mathcal{L}$, "$M(x,Y) \leq N(x,Y)$", $M \in \mathcal{M}$, $N \in \mathcal{N}$.

Let $\mathcal{V}$ be a family of non-empty subsets of Ω, satisfying the Condition 2 in the definition of superuniversum. Call a set $W \subset \Omega$ *pseudo open* if for any V in $\mathcal{V}$ intersecting with W there exists V' in $\mathcal{V}$ such that $V' \subset V \cap W$. (Note that we do not require $\mathcal{V}$ to be a base of a topology.) Let us enrich our language by constants attached to all the elements from the domains of all the variables. Assume that the following condition is true:

($**$) for any atomic formula $P(x_1, \ldots, x_n, Y)$ for any values $a_1, \ldots, a_n$ of $x_1, \ldots, x_n$ the set $\{A \in \Omega \mid P(a_1, \ldots, a_n, A)\}$ is pseudo open.

Note that Condition 1 in the definition of superuniversum implies that all the sets $\{A \in \Omega \mid P(x,A) = \#\}$, $\{A \in \Omega \mid P(x,A) \neq \#\}$, $\{A \in \Omega \mid P(x,A) \leq Q(x,A)\}$, and $\{A \in \Omega \mid \neg P(x,A) \leq Q(x,A)\}$ are pseudo open for any $x \in \mathbf{B}^*$ and any polynomial-local descriptions P and Q.

Let us define the forcing relation $V \vdash \varphi(Y)$, where $\varphi(Y)$ is a closed formula of the enriched language, as follows. We use induction on the number of symbols in $\varphi(Y)$. Assume that only connectivities $\&$, $\vee$, and $\neg$ and only the quantifier $\exists$ are used in formulae (the quantifier $\forall x$ is expressed as $\neg\exists x\neg$).

1. If $\varphi(Y)$ is atomic, then $V \vdash \varphi(Y)$ if $\varphi(A)$ is true for all $A \in V$.
2. $V \vdash \varphi(Y)\&\psi(Y)$ if $V \vdash \varphi(Y)$ and $V \vdash \psi(Y)$.
3. $V \vdash \varphi(Y) \vee \psi(Y)$ if $V \vdash \varphi(Y)$ or $V \vdash \psi(Y)$.
4. $V \vdash \exists z \in Z \varphi(Y,z)$ if there exists $b \in Z$ such that $V \vdash \varphi(Y,b)$.
5. $V \vdash \neg\varphi(Y)$ if $V' \nvdash \varphi(Y)$ for all $V' \subset V$.

Obviously, the forcing relation is monotone, that is, if $V \vdash \varphi(Y)$ and $V' \subset V$, then $V' \vdash \varphi(Y)$.

Lemma 3.1 *For any closed atomic formula $\varphi(Y)$, $V \vdash \neg\varphi(Y)$ iff the formula $\neg\varphi(A)$ is true for all $A \in V$.*

*Proof.*Proof This easily follows from $(**)$.

We claim that if $\mathcal{V}$ satisfies the Condition 1 in the definition of superuniversum, then the assertion (a) means that $\text{largest}(\mathcal{V}) \vdash \mathcal{K}^Y \not\leq \mathcal{L}^Y$ and the assertion (b) means that $\text{largest}(\mathcal{V}) \vdash \mathcal{M}^Y \leq \mathcal{N}^Y$, thus (a)&(b) means that $\text{largest}(\mathcal{V}) \vdash (\mathcal{K}^Y \not\leq \mathcal{L}^Y \ \& \ \mathcal{M}^Y \leq \mathcal{N}^Y)$. Indeed, by above lemma, Condition 1 implies that for all polynomial-local descriptions P and Q, for all $x \in \mathbf{B}^*$, both sets $\{A \in \Omega \mid P(x,A) \neq \#\}$ and $\{A \in \Omega \mid \neg P(x,A) \leq Q(x,A)\}$ are pseudo open and therefore $V \vdash \forall x \in \mathbf{B}^* \ P(x,Y) \neq \#$ iff P is correct on V and $V \vdash \forall x \in \mathbf{B}^* P(x,Y) \leq Q(x,Y)$ iff $P^V \leq Q^V$. Therefore, $\text{largest}(V) \vdash \mathcal{K}^Y \not\leq \mathcal{L}^Y$ means that there exists $K \in \mathcal{K}$ correct on $\text{largest}(\mathcal{V})$ such that there exist no V and $L \in \mathcal{L}$ such that $K^V \leq L^V$ and the assertion $\text{largest}(V) \vdash \mathcal{M}^Y \leq \mathcal{N}^Y$ means that for all $M \in \mathcal{M}$ and all V, M is incorrect on V or there exist $V' \subset V$ and $N \in \mathcal{N}$ such that $M^{V'} \leq N^{V'}$.

The following theorem generalizes the Theorem 3.1.

Theorem 3.2 *Let $\eta(Y)$ be an assertion such that $V_0 \vdash \eta(Y)$ for some V_0 in $\mathcal{V}$. Then there exists A such that $\eta(A)$ is true.*

*Proof.*Proof Let $\varphi_1(Y)$, $\varphi_2(Y)$, $\varphi_3(Y)$, ... be an enumeration of closed formulae in the enriched language. We use a diagonal construction. On ith step we construct a universum V_i as follows. If $V_{i-1} \vdash \neg\varphi_i(Y)$, then let $V_i = V_{i-1}$. Otherwise pick $V' \subset V_{i-1}$ such that $V' \vdash \varphi_i(Y)$ and let $V_i = V'$.

Let A be any oracle from the intersection $\bigcap_{i=1}^{\infty} V_i$. Let us prove by induction that for every closed formula $\varphi(Y)$ of enriched language

$$(\exists i \ V_i \vdash \varphi(Y)) \iff \varphi(A) \text{ is true.}$$

1. $\varphi(Y)$ is atomic. If $V_i \vdash \varphi(Y)$ for some i, then by definition of forcing relation, $\varphi(B)$ is true for all $B \in V_i$, in particular, $\varphi(A)$ is true. If $\forall i \ V_i \nvdash \varphi(Y)$, then, by construction, $V_i \vdash \neg\varphi(Y)$ for some i. Take such i. By the Lemma 3.1, $\neg\varphi(B)$ is true for any $B \in V_i$, consequently, $\neg\varphi(A)$ is true.

2. If $\exists i \ V_i \vdash \neg\varphi(Y)$, then there exists no j such that $V_j \vdash \varphi(Y)$. By induction hypothesis, $\varphi(A)$ is false. If $\forall i \ V_i \nvdash \neg\varphi(Y)$, then, by construction, there exists j such that $V_j \vdash \varphi(Y)$, therefore $\varphi(A)$ is true by induction hypothesis.

3. If $\exists i \ V_i \vdash \varphi(Y)\&\psi(Y)$, then $\exists i \ V_i \vdash \varphi(Y)$ and $\exists i \ V_i \vdash \psi(Y)$, therefore both $\varphi(A)$ and $\psi(A)$ are true by induction hypothesis. If $\varphi(A)\&\psi(A)$

is true, then by induction hypothesis there exist i and j such that $V_i \vdash \varphi(Y)$ and $V_j \vdash \psi(Y)$. Therefore $V_{\max\{i,j\}} \vdash \varphi(Y)\&\psi(Y)$.

4. The remaining cases can be done similarly.

Since $V_0 \vdash \eta(Y)$, we are done. $\square$

Thus, if we want to prove that there exists an oracle A such that $\mathcal{K}^A \not\leq \mathcal{L}^A$ and $\mathcal{M}^A \leq \mathcal{N}^A$, then we have to find a superuniversum $\mathcal{V}$ and an oracle H such that (a) and (b) are true. In this form the method is universal. Indeed, if there exists an oracle A such that $\mathcal{K}^A \not\leq \mathcal{L}^A$ and $\mathcal{M}^A \leq \mathcal{N}^A$ then both (a) and (b) hold for $\mathcal{V} = \{\{A\}\}$, $H = \emptyset$ or for $\mathcal{V} = \{\{\emptyset\}\}$, $H = A$.

Now we describe the very universum method. It does not use any notion of computability. It is not universal as we will see in Section 5.

3.3 Non-uniformity

Given a class $\mathcal{D}$ of descriptions define the nonuniform counterpart of the class $\mathcal{D}$ as follows.

Definition 3.7 *The nonuniform counterpart of a class $\mathcal{D}$ of descriptions is the class*

$$\text{n.u.}\mathcal{D} = \bigcup_{C \in \Omega} \mathcal{D}(C).$$

For particular classes of descriptions we can give equivalent definitions using no notion of computability. Let us do this for the classes from the list (3). To do this we have to define the notion of a boolean decision tree and the notion of a branching program. More exactly, we define families of decision trees and families of branching programs; for the seak of breviety we omit the word "family".

A *boolean decision tree* (or simply decision tree) is a pair $T = \langle question\,, result \rangle$, where *question* is a function from $\mathbf{B}^* \times \mathbf{B}^*$ into $\mathbf{B}^* \cup \{\$\}$, *result* is a function from $\mathbf{B}^* \times \mathbf{B}^*$ into $\{0, 1, \$\}$. The decision tree T computes the description $\langle x, A \rangle \mapsto T(x, A)$ defined as follows: $T(x, A)$ is equal to the result produced by the program shown on Figure 2.

We assume that this program always halt. Call a decision tree *polynomial* if
1) there exists a polynomial p such that $|\,question\,(x, w)\,| \leq p(|x|, |w|)$ for any $x, w \in \mathbf{B}^*$ and any $A \in \Omega$ and

Figure 2: Program 2

```
begin
   w := Λ;
   while result(x, w) = $
      do
         y := question(x, w);
         b := A(y);
         w := wb;
      od
   output result(x, w);
end.
```

2) the Program 2 halts after executing poly($|x|$) loops; it is important that in this case the program makes only poly($|x|$) queries to A.

It must be stressed that we do not require any computability of functions *question* and *result*. Obviously, if both functions *question* and *result* are polynomial-time computable, then the description $T(x, A)$ can be computed by a polynomial-time oracle machine.

We claim that a description D is in n.u.P iff D can be computed by a polynomial decision tree. This is quite obvious: let D be in n.u.P, say $D(x, A) = M(x, A \oplus C)$, where M is a polynomial-time oracle machine and C is an oracle. Then let $question(x, w)$ be the question to oracle A made by M after getting answers $w(1)$, $w(2)$, ..., $w(|w|)$ to previous questions made to A and let $result(x, w)$ be the value output by M after getting answers $w(1)$, $w(2)$, ..., $w(|w|)$ to questions made to A (if the specified values are undefined, then we consider them to be equal to \$). Obviously, the defined decision tree $T = \langle question, result \rangle$ is polynomial and $T(x, A) = M(x, A \oplus C) = D(x, A)$ for all x, A. Conversely, let a description D be in n.u.P, say $D(x, A) = T(x, A)$, where $T = \langle question, result \rangle$ is a polynomial decision tree. Then take as C the oracle relative to which both functions *question* and *result* are computable in polynomial time. Program 2 defines then a P(C)-machine computing $D(x, A)$.

Figure 3: Program 3

```
begin
  s := initial_state(x);
  while result(s) = $
    do
      y := question(s);
      b := A(y);
      s := next_state(s, b);
    od
  output result(s)
end.
```

It is easy to prove that a description D belongs to n.u.NP iff there exists a polynomial $p(n)$ and a description $D' \in$ n.u.P such that

$$D(x, A) = 1 \Longleftrightarrow \exists y \in \mathbf{B}^{p(|x|)} D'(\bar{x}y, A) = 1.$$

In the similar way the classes n.u.BPP, n.u.R, n.u.(NP $\cap$ Co-NP) = n.u.NP$\cap$n.u.Co-NP, n.u.(R$\cap$Co-R) = n.u.R$\cap$n.u.Co-R can be characterized. For example, a description D is in n.u.BPP if there exist a polynomial $p(n)$ and a description $D' \in$ n.u.P such that

$$D(x, A) = \begin{cases} 1, & \text{if } \mathrm{Prob}_{r \in \mathbf{B}^{p(|x|)}}[D'(\bar{r}x, A) = 1] > 2/3; \\ 0, & \text{if } \mathrm{Prob}_{r \in \mathbf{B}^{p(|x|)}}[D'(\bar{r}x, A) = 0] > 2/3; \\ \#, & \text{otherwise.} \end{cases}$$

The nonuniform counterpart n.u.PSPACE of the class PSPACE can be also defined in the similar way: call a quadruple

$$P = \langle \mathit{initial\_state}, \mathit{next\_state}, \mathit{question}, \mathit{result} \rangle,$$

where $\mathit{initial\_state}: \mathbf{B}^* \to \mathbf{B}^*$, $\mathit{next\_state}: \mathbf{B}^* \times \mathbf{B} \to \mathbf{B}^*$, $\mathit{question}: \mathbf{B}^* \to \mathbf{B}^* \cup \{\$\}$, $\mathit{result}: \mathbf{B}^* \to \{0, 1, \$\}$, a *branching program*. The value $P(x, A)$ produced by the branching program P on input $\langle x, A \rangle$ is computed by the program shown on Figure 3. Call a branching program *polynomial-space* if there exists a polynomial p such that the length of word s does not exceed $p(|x|)$ in all the steps of execution of that program. It is easy to prove that

$D \in$ n.u.PSPACE $\Leftrightarrow$ there exists a polynomial-space branching program P computing D.

Now we are able to present the second general theorem which is the essence of the universum method. This theorem simplifies all further applications of the method.

Suppose there exists a superuniversum $\mathcal{V}$ such that the following two assertions hold:

(a′) there exists $K \in$ n.u.$\mathcal{K}$ which is correct on largest($\mathcal{V}$) and n.u.$\mathcal{L}$-unsolvable on any $V \in \mathcal{V}$;

(b′) for any V, every description $M \in$ n.u.$\mathcal{M}$ being correct on V is n.u.$\mathcal{N}$-solvable on some $V' \subset V$, $V' \in \mathcal{V}$.

Note that (a′) and (b′) are obtained from (a) and (b), respectively, by replacing uniform classes relativized by H by the corresponding nonuniform classes. The following theorem states that in this case there exists an oracle H for which (a) and (b) are true, and hence there exists an oracle A such that $\mathcal{K}^A \not\leq \mathcal{L}^A$ and $\mathcal{M}^A \leq \mathcal{N}^A$.

To prove that theorem we need some extra restrictions on classes $\mathcal{K}$, $\mathcal{L}$, $\mathcal{M}$, and $\mathcal{N}$. Let us formulate those restrictions. We would mention that they are rather combersome and therefore possibly it is better to skip them and to read the following theorem assuming that the classes $\mathcal{K}$, $\mathcal{L}$, $\mathcal{M}$, and $\mathcal{N}$ belong to the list (3).

Call a class $\mathcal{D}$ of descriptions *a polynomial complexity class* if

1. $\mathcal{D}$ consists of polynomial-local descriptions,
2. $\mathcal{D}$ includes the class P, and
3. there exist a larger class $\mathcal{D}'$ of descriptions, an enumeration D_0, D_1, D_2, ... of that class, and a function $c : \mathbf{N} \times \mathbf{B}^* \times \Omega \to \mathbf{N}$ (called complexity function) such that the following two conditions hold:
   (a) $\mathcal{D} = \{D_i \in \mathcal{D}' \mid c(i, x, A) \leq p(|x|)$ for some polynomial p an all $x, A\}$, and
   (b) for all polynomial-time oracle machines Q, R and S outputting an integer, a binary word and a bit, respectively, there exists m

such that

$$D_m(x,A) = D_{Q(x,A)}(R(x,A), S_x^A) \\ \text{and } c(m,x) \leq \text{poly}\,(Q(x,A)+ \\ |x| + c(Q(x,A), R(x,A), S_x^A)\Big), \tag{4}$$

where S_x^A stands for the oracle $\{y \in \mathbf{B}^* \mid S(x,y,A) = 1\}$. In particular, if D_i is in $\mathcal{D}$, then the description $\langle x, A\rangle \mapsto D_i(R(x,A), S_x^A)$ is in $\mathcal{D}$, too.

We can see that the Condition 3b is both a complexity version of the s-m-n-theorem in the Recursion theory and the property of closeness under polynomial-time reductions. It is easy to verify that all the classes in the list (3) are polynomial complexity classes. In the following general theorems we assume the classes $\mathcal{K}$, $\mathcal{L}$, $\mathcal{M}$, and $\mathcal{N}$ to be polynomial complexity classes and we sometimes use the conditions involved the definition of a polynomial complexity class without reference.

Theorem 3.3 *If a superuniversum $\mathcal{V}$ satisfies* (a′) *and* (b′) *then $\mathcal{V}$ satisfies* (a) *and* (b) *for some oracle H. Moreover, there exists an oracle E such that for all oracles G being polynomial-time Turing reducible to E, the conditions* (a) *and* (b) *are true for H being equal to any* EXP^G*-complete set, where* $\text{EXP} = \text{Time}(2^{\text{poly}(n)})$.

Proof. Let $\mathcal{V}$ be a superuniversum such that assertions (a′) and (b′) are true. Then there exists a description $K \in \text{n.u.}\mathcal{K}$ which is correct on largest($\mathcal{V}$) and n.u.$\mathcal{L}$-unsolvable on any $V \in \mathcal{V}$. Let D be the oracle such that $K \in \mathcal{K}(D)$. Then for all oracles H which D is polynomial-time Turing reducible to the assertion (a) holds. Thus, it suffices to construct an oracle H such that (b) is true and which D is reducible to.

Let $\mathcal{M} = \{M_0, M_1, M_2, \ldots\}$. Let $\mathcal{V} = \{V_0, V_1, V_2, \ldots\}$. Let $\mathcal{N}' = \{N_0, N_1, N_2, \ldots\}$ be the class of descriptions and c be a function for which the assertions 3a and 3b in the definition of complexity class are true for $\mathcal{D} = \mathcal{N}$.

Notation 3.3 *Given an $n \in \mathbf{N}$ and an oracle F, denote by F^n the binary word of length $2^{n+1} - 1$ encoding the value of F on all the words of length $\leq n$.*

The description M_j is polynomial-local for any j in $\mathbf{N}$, i.e., there exists a polynomial p_j such that $M_j(x,F)$ depends only on x and $F|\mathbf{B}^{\leq p_j(|x|)}$. Let j,l be in $\mathbf{N}$, x be in $\mathbf{B}^*$ and F be in Ω. Consider the set $U = U(j,l,x,F^{p_j(|x|)})$ consisting of all the pairs $\langle k,B\rangle$, $k \in \mathbf{N}$, $B \in \Omega$, such that

$$M_j(x, A \oplus F) \leq N_k(x, A \oplus B)$$

for all $x \in \mathbf{B}^*$ and all $A \in V_l$. Take a pair $\langle k,B\rangle$ from U having the minimal sum $k+|x|+c(k,x,B)$. Denote that pair by $\langle k(j,l,x,F^{p_j(|x|)}), B(j,l,x,F^{p_j(|x|)})\rangle$. Let C be any oracle such that

$$C(0\bar{j}\bar{l}\bar{x}\overline{F^{p_j(|x|)}}0^s) = \begin{cases} 1, & \text{if } s \leq k(j,l,x,F^{p_j(|x|)}), \\ 0, & \text{otherwise.} \end{cases}$$

$$C(1\bar{j}\bar{l}\bar{x}\overline{F^{p_j(|x|)}}y) = B(j,l,x,F^{p_j(|x|)})(y).$$

Let $E = C \oplus D$. Let us prove that if G is polynomial Turing reducible to E, then for any EXP^G-complete oracle H, the assertions (a$'$) and (b$'$) are true.

Let E be polynomial-time Turing reducible to G and let H be an EXP^G-complete oracle. The assertion (a$'$) is true because D is polynomial-time Turing reducible to H. Let us prove (b$'$). Let V_i be a universum in $\mathcal{V}$ and let $M_j(x, A \oplus H)$ be a description in $\mathcal{M}(H)$ correct on V_i. We have to prove that there exist a universum $V_l \subset V_i$ and a description N_m in $\mathcal{N}$ such that $M_j(x, A \oplus H) \leq N_m(x, A \oplus H)$ for all A in V_l and all x.

Lemma 3.2 *Both functions*

$$x \mapsto k(j,l,x,H^{p_j(|x|)}) \text{ and} \tag{5}$$

$$\bar{x}y \mapsto B(j,l,x,H^{p_j(|x|)})(y) \tag{6}$$

are polynomial-time computable relative to H.

Proof. By (b$'$) there exist k', l, and an oracle B' such that $N_{k'} \in \mathcal{N}$, $V_l \subset V_i$ and

$$M_j(x, A \oplus H) \leq N_{k'}(x, A \oplus B')$$

for all $A \in V_l$ and all x. Let us fix such k', such l, and such B'.

Since $\langle k', B'\rangle$ belong to $U(j,l,x,F^{p_j(|x|)})$ and

$$k' + |x| + c(k', x, A \oplus B') \leq \mathrm{poly}(|x|),$$

we can conclude that

$$k(j,l,x,H^{p_j(|x|)}) + |x| + \\ c(k(j,l,x,H^{p_j(|x|)}), x, A \oplus B(j,l,x,H^{p_j(|x|)})) \\ \leq \mathrm{poly}(|x|). \qquad (7)$$

Let us prove first the polynomial-time computability of the function (5) (denote it by f). By (7), $f(x) \leq \mathrm{poly}(|x|)$, therefore it suffices to prove that $f(x)$ can be computed in time $2^{\mathrm{poly}(|x|)}$ relative to G. (Recall that H is a EXP^G-complete oracle.) This can be done as follows. Let x be the input word. Find first $H^{p_j(|x|)}$. To this end compute $H(z)$ for all z such that $|z| \leq p_j(|x|)$ using an exponential machine with oracle G recognizing H. (As $|z| \leq p_j(|x|)$, each $H(z)$ can be computed in time $2^{\mathrm{poly}(|x|)}$.) Then ask '$C(0\bar{j}\bar{l}\bar{x}\overline{H^{p_j(|x|)}}0^s) =?$' for $s = 1, 2, 3, \ldots$ until we find an s such that $C(0\bar{j}\bar{l}\bar{x}\overline{H^{p_j(|x|)}}0^s) = 0$. Since C is polynomial-time reducible to G, all those questions to C can be answered in time $2^{\mathrm{poly}(|x|)}$ using the oracle G.

The polynomial-time computability of function (6) can be proved similarly.□

Thus, we have

$$M_j(x, A \oplus H) \leq \\ N_{k(j,l,x,H^{p_j(|x|)})}(x, A \oplus B(j,l,x,H^{p_j(|x|)}))$$

for all $A \in V_l$ and all x. By the above lemma and by property 3b in the definition of complexity class there exists m such that

$$N_m(x, A \oplus H) = \\ N_{k(j,l,x,H^{p_j(|x|)})}(x, A \oplus B(j,l,x,H^{p_j(|x|)}))$$

for all x and A and

$$c(m, x, A \oplus H) \leq \\ \mathrm{poly}\Big(k(j,l,x,H^{p_j(|x|)}) + |x| + \\ c(k(j,l,x,H^{p_j(|x|)}), x, A \oplus B(j,l,x,H^{p_j(|x|)}))\Big) \leq \\ \mathrm{poly}(|x|).$$

(The first inequality is true by (4) and the last inequality is true by (7).) Hence N_m is in $\mathcal{N}$ and we are done.□

Let us see how the proof of Theorem 2.1 can be simplified by using Theorems 3.6 and 3.3. Besides that general theorems we use one more tool due to [BGS 75].

New proof of Theorem 2.1. Consider the universum defined as follows. Define the sequence of integers $n(i)$ by induction $n(0) = 1$, $n(i+1) = 2^{2^{n(i)}}$. Set $\mathbf{S} = \{n(i) \mid i \in \mathbf{N}\}$. Let

$$V_0 = \{B \in \Omega \mid \forall n \in \mathbf{S}\ \#_1(A|\mathbf{B}^n) \leq 1 \text{ and } \forall n \notin \mathbf{S}\ \#_1(A|\mathbf{B}^n) = 0\}.$$

We claim that both (a′) and (b′) hold for the superuniversum $\mathcal{V}(V_0)$ and $\mathcal{K}$=NP-separation, $\mathcal{L} = \mathcal{N} = \mathrm{P}$ and $\mathcal{M}$=Co-NP-separation.

The assertion (a′) can be proved just as it was done in the old proof of Theorem 2.1.

Let us prove (b′). Let M belong to n.u.Co-NP-separation and is correct on $V \in \mathcal{V}(V_0)$. We have to construct a universum $V' \in \mathcal{V}(V_0)$, $V' \subset V$ and a polynomial decision tree N such that $M^{V'} \leq N^{V'}$.

Let $V' = V$. Let M be defined by the pair $\langle M_0, M_1\rangle$ of machines from n.u.NP. Then $M_0(x,B) = 1$ or $M_1(x,B) = 1$ for all $x \in \mathbf{B}^*$, $B \in V$. Procedure N on input $\langle x, B\rangle$, where $B \in V$, has to output a $j \in \{0,1\}$ such that $M_j(x,B) = 1$.

Procedure N on input $\langle x, B\rangle$ works as follows. Find first the number $n(i) \in \mathbf{S}$ such that $2^{n(i-1)} = \log_2 n(i) \leq |x| < 2^{n(i)}$. Then query the value of B on all the words of length $\leq n(i-1)$. The number of such queries is less than $2^{n(i-1)+1} \leq 2|x|$.

Let k be so large that $M_j(x,B)$ does not depend on $B|\mathbf{B}^{\geq n(i+1)}$ for $j = 0,1$ for all $|x| \geq k$, (such k does exist, as $n(i+1) = 2^{2^{n(i)}} \geq 2^{|x|}$). If $|x| < k$ then compute $M_0(x,B)$ directly and output 0 if $M_0(x,B) = 1$ and 1 else. Let $|x| \geq k$. Let $V = \Gamma(\varphi) \cap V_0$.

Define the function ψ as follows:

$$\psi(y) = \begin{cases} B(y), & \text{if } |y| \leq n(i-1); \\ \varphi(y), & \text{if } y \in \mathrm{Dom}(\varphi) \text{ and } |y| > n(i-1); \\ \text{undefined}, & \text{otherwise.} \end{cases}$$

Check if $\hat{\psi} \in V$. If this is not the case, then $B \notin V$ and we output 0. Otherwise $M_0(x,\hat{\psi}) = 1$ or $M_1(x,\hat{\psi}) = 1$. Find a $j \in \{0,1\}$ such that $M_j(x,\hat{\psi}) = 1$ and an accepting computation c of M_j on input $\langle x, \hat{\psi}\rangle$. Then query '$B(y) =?$' for all $y \in \mathit{Query}_{M_j}(c,\hat{\psi}) \setminus \mathrm{Dom}(\psi)$. If $B(y) = 0$ for all $y \in \mathit{Query}_{M_j}(c,\hat{\psi}) \setminus \mathrm{Dom}(\psi)$, then $M_j(x,B) = 1$ and we output j.

If there are at least two different y_1, y_2 in $Query_{M_j}(c, \hat{\psi}) \setminus \mathrm{Dom}(\psi)$ such that $B(y_1) = B(y_2) = 1$, then $B \notin V$ because $n(i-1) < |y_1|, |y_2| < n(i+1)$; in this case output 0. Therefore we can assume that there exists unique $y \in Query_{M_j}(c, \hat{\psi}) \setminus \mathrm{Dom}(\psi)$ such that $B(y) = 1$. Then define

$$\eta(z) = \begin{cases} 1, & \text{if } z = y; \\ \psi(z), & \text{if } z \in \mathrm{Dom}(\psi); \\ \text{undefined}, & \text{otherwise.} \end{cases}$$

Then $\hat{\eta}$ is in V. Find $j \in \{0, 1\}$ such that $M_j(x, \hat{\eta}) = 1$ and then output that j. We know, that if $B \in V$ then $B|\mathbf{B}^{<n(i+1)} = \hat{\eta}|\mathbf{B}^{<n(i+1)}$ and $M_j(x, B)$ does not depend on $B|\mathbf{B}^{\geq n(i+1)}$, thus we have output a correct answer. Obviously, $size\,(Query_N(x, B)) \leq \mathrm{poly}(|x|).\Box$

The new tool is the use of universums consisting only of oracles B such that $B|\mathbf{B}^n = \mathbf{0}_n$, where $\mathbf{0}_n$ is identically zero function defined on $\mathbf{B}^n$. We call such universums *scanty* and will prove a general theorem concerning such universums.

3.4 Cylindric scanty universums

Given an $n \in \mathbf{N}$, denote by $\mathbf{F}_n$ the set of all functions from $\mathbf{B}^n$ into $\mathbf{B}$; denote $\mathbf{F} = \bigcup_{n \in \mathbf{S}} \mathbf{F}_n$. For $\alpha \in \mathbf{F}$ call the n such that $\alpha \in \mathbf{F}_n$ the *norm of* α and denote it by $\|\alpha\|$. Call any subset Z of $\mathbf{F}$ a *base*. Given an $n \in \mathbf{N}$, denote by Z_n the set $Z \cap \mathbf{F}_n$. For a base Z define

$$V(Z) = \{A \in \Omega \mid \forall n \in \mathbf{S}\ A|\mathbf{B}^n \in Z,\ \forall n \notin \mathbf{S}\ A|\mathbf{B}^n = \mathbf{0}_n\}.$$

Call an oracle A *scanty* if $A|\mathbf{B}^n = \mathbf{0}_n$ for all $n \notin \mathbf{S}$. We call the universums of the form $V(Z)$ *cylindric scanty* universums. It is easy to verify that $V(Z)$ is closed in Cantor's topology. The set Z is called the *base of* $V(Z)$. Call any family $\mathcal{Z}$ of bases having the largest base up to inclusion a *superbase*. Denote the largest base in $\mathcal{Z}$ by largest($\mathcal{Z}$). For a superbase $\mathcal{Z}$ define the superuniversum

$$\mathcal{V}(\mathcal{Z}) = \{\Gamma \cap V(Z) \mid Z \in \mathcal{Z} \text{ and } \Gamma \text{ is an interval intersecting with } V(Z)\}.$$

Our aim is to formulate simpler conditions which are equivalent to conditions (a′) and (b′) in the case when $\mathcal{V}$ has the form $\mathcal{V}(\mathcal{Z})$.

To this end we want to define what means that a machine has a finite oracle $\alpha \in \mathbf{F}$ as input. Given a description D, $\alpha \in \mathbf{F}_n$, and $x \in \mathbf{B}^*$, denote

$$D[\alpha] = D(1^n, \hat{\alpha}),\ D[x, \alpha] = D(\bar{x}1^n, \hat{\alpha}).$$

Say that a description D is *correct* on a base Z if $D[x, \alpha] \neq \#$ for all $x \in \mathbf{B}^*$, $\alpha \in Z$. Say that a description is *good* on a base Z if $D[\alpha] \neq \#$ for all $\alpha \in Z$. If M is a machine then the words "M works on input $[x, \alpha]$ (on input $[\alpha]$, respectively)" mean that M works on input $\langle \bar{x}1^n, \hat{\alpha} \rangle$ (on input $\langle 1^n, \hat{\alpha} \rangle$, respectively).

Write $K^Z \leq L^Z$ if $K[x, \alpha] \leq L[x, \alpha]$ for all $x \in \mathbf{B}^*$, $\alpha \in Z$. Write $K^Z \preceq L^Z$ if $K[\alpha] \leq L[\alpha]$ for all $a \in Z$. The notation $Query_M[x, \alpha]$ means $Query_M(\bar{x}1^{\|\alpha\|}, \hat{\alpha})$. Other query notations are expanded in the similar way.

In the proof of the next theorem we use the following consequence from the property 3 of polynomial complexity classes: if $\mathcal{D}$ is a polynomial complexity class, D_0 and D_1 are in $\mathcal{D}$ and D is in P, then the description

$$D'(x, A) = \begin{cases} D_0(x, A), & \text{if } D(x, A) = 0; \\ D_1(x, A), & \text{if } D(x, A) = 1; \end{cases}$$

is in $\mathcal{D}$. Obviously, this is true for the nonuniform version of $\mathcal{D}$, too.

Theorem 3.4 *Let $\mathcal{Z}$ be a superbase such that the following two assertions are true:*

(a$''$) there exists a description $K \in$ n.u.$\mathcal{K}$ which is good on largest($\mathcal{Z}$) and such that there exist no base $Z \in \mathcal{Z}$ and $L \in$ n.u.$\mathcal{L}$ for which $K^Z \preceq L^Z$;

(b$''$) for all $Z \in \mathcal{Z}$ and all $M \in$ n.u.$\mathcal{M}$ being correct on Z there exist a base $Z' \subset Z$, $Z' \in \mathcal{Z}$ and a description $N \in$ n.u.$\mathcal{N}$ such that $M^{Z'} \leq N^{Z'}$.

Then for the superuniversum $\mathcal{V} = \mathcal{V}(\mathcal{Z})$ the assertions (a$'$) *and* (b$'$) *are true (and, therefore, there exists an oracle A such that $\mathcal{K}^A \not\leq \mathcal{L}^A$ and $\mathcal{M}^A \leq \mathcal{N}^A$).*

Proof. Let (a$''$) be true. We have to prove (a$'$). Let $K \in$ n.u.$\mathcal{K}$ be a description being good on largest($\mathcal{Z}$) and such that there exist no $Z \in \mathcal{Z}$ and $L \in$ n.u.$\mathcal{L}$ for which $K[\alpha] \leq L[\alpha]$ for all $\alpha \in Z$. Obviously, the largest universum in $\mathcal{V}$ is V(largest($\mathcal{Z}$)). Define the description

$$K'(x, A) = \begin{cases} K[A|\mathbf{B}^n], & \text{if } x = 1^n, \text{ where } n \in \mathbf{S}; \\ 0, & \text{otherwise.} \end{cases}$$

The description K' is correct on $V(\text{largest}(\mathcal{Z}))$ and belongs to n.u.$\mathcal{K}$. Let us prove that there exist no universum $V \in \mathcal{V}$ and description $L' \in$ n.u.$\mathcal{L}$ such that $K'(x,A) \le L'(x,A)$ for all $x \in \mathbf{B}^*$, $A \in V$. Assume the contrary: such V and L' exist. Denote by $\Gamma(\varphi)$ and by Z the interval and the base, respectively, such that $V = \Gamma(\varphi) \cap V(Z)$. Denote by k the $maxlength\,\mathrm{Dom}(\varphi)$. To obtain a contradiction let us construct a description $L \in$ n.u.$\mathcal{L}$ such that $K[\alpha] \le L[\alpha]$ for all $\alpha \in Z$.

For all $i \in \mathbf{S}$ let us fix a function $\psi_i \in Z_i$ being consistent with φ (i.e. $\varphi(y) = \psi_i(y)$ for all $y \in \mathrm{Dom}(\varphi) \cap \mathrm{Dom}(\psi_i)$). For any function $\alpha \in \mathbf{F}$ define the oracle $\tilde{\alpha}$ as follows: for any $i \in \mathbf{N}$, $y \in \mathbf{B}^i$,

$$\tilde{\alpha}(y) = \begin{cases} 0, & \text{if } i \notin \mathbf{S}; \\ \alpha(y), & \text{if } i = \|\alpha\|; \\ \psi_i(y), & \text{otherwise.} \end{cases}$$

Note that if α is in Z and $\|\alpha\| > k$, then $\tilde{\alpha} \in V$. Therefore, if $\alpha \in Z$ and $\|\alpha\| > k$, then $K'(x,\tilde{\alpha}) \le L'(x,\tilde{\alpha})$ for all $x \in \mathbf{B}^*$. In particular,

$$K[\alpha] = K'(1^{\|\alpha\|},\tilde{\alpha}) \le L'(1^{\|\alpha\|},\tilde{\alpha})$$

if $\alpha \in Z$ and $\|\alpha\| > k$. Obviously, there exists a description $L \in$ n.u.$\mathcal{L}$ such that

$$L[\alpha] = \begin{cases} L'(1^{\|\alpha\|},\tilde{\alpha}), & \text{if } \|\alpha\| > k; \\ K[\alpha], & \text{otherwise.} \end{cases}$$

Then $K[\alpha] \le L[\alpha]$ for all $\alpha \in Z$, because if $\|\alpha\| > k$, then $K[\alpha] = K'(1^{\|\alpha\|},\tilde{\alpha}) \le L'(1^{\|\alpha\|},\tilde{\alpha}) = L[\alpha]$, and if $\|\alpha\| \le k$ then $K[\alpha] = L[\alpha]$ by definition.

Let us prove that (b$''$)$\Rightarrow$(b$'$). Let (b$''$) be true. We have to prove (b$'$). Let $V = V(Z) \cap \Gamma(\varphi)$ be a universum in $\mathcal{V}$ and M be a description in n.u.$\mathcal{M}$ being correct on V. We have to prove that there exist a universum $V' \subset V$, $V' \in \mathcal{V}$ and a description $N \in$ n.u.$\mathcal{N}$ such that $M(x,B) \le N(x,B)$ for all $B \in V'$, $x \in \mathbf{B}^*$.

Given a $C \in \Omega$ and an $n \in \mathbf{N}$, denote by C^n the binary word of length $2^{n+1}-1$ encoding the value of C on all the words of length $\le n$. Denote for $x \in \mathbf{B}^*$ by $i(x)$ the number i such that $\log_2 n(i) \le |x| < 2^{n(i)}$. Recall that $n(i)$ is defined by induction: $n(0) = 1$, $n(i+1) = 2^{2^{n(i)}}$.

Fix an integer n_0 such that if $|x| > n_0$, then $M(x,B)$ does not depend on $B|\mathbf{B}^{\ge n(i(x)+1)}$ and $n(i(x)) > maxlength\,\mathrm{Dom}(\varphi)$ (such an n_0 does exist

because $n(i(x)+1) \geq 2^{|x|}$). Let us construct a description $M' \in$ n.u.$\mathcal{M}$ being correct on Z such that

$$M(x,B) = M'[\bar{x}B^{n(i(x)-1)}, B|\mathbf{B}^{n(i(x))}] \tag{8}$$

for all $B \in V$ and all $x \in \mathbf{B}^{>n_0}$.

The description M' on input $[u,\alpha]$, works as follows. Check first whether u has the form $\bar{x}C^{n(i(x)-1)}$ for some $C \in V$. If this is not the case, then output 0. Otherwise find x and $C \in V$ such that $u = \bar{x}C^{n(i(x)-1)}$. If $|x| \leq n_0$ or $\|\alpha\| \neq n(i(x))$, then output 0. Otherwise output $M(x,\tilde{\alpha})$, where

$$\tilde{\alpha}(y) = \begin{cases} C(y), & \text{if } |y| \neq n(i(x)); \\ \alpha(y), & \text{if } |y| = n(i(x)). \end{cases}$$

Obviously, (8) is true for all $B \in V$ and all $x \in \mathbf{B}^{>n_0}$. Let us prove that M' is correct on Z. Assume that α is in Z. If u has the form $\bar{x}C^{n(i(x)-1)}$, where $C \in V$, $|x| > n_0$ and $n(i(x)) = \|\alpha\|$, then $\tilde{\alpha}$ is in V (by definition of V and the choice of n_0); in this case $M'[u,\alpha] = M(x,\tilde{\alpha}) \neq \#$ (since M is correct on V). Otherwise $M'[u,\alpha] = 0$.

The assertion (b$''$) implies that there exist a base $Z' \in \mathcal{Z}$ and a description $N' \in$ n.u.$\mathcal{N}$ such that $Z' \subset Z$ and $M'[u,\alpha] \leq N'[u,\alpha]$ for all $u \in \mathbf{B}^*$, $\alpha \in Z'$. Set $V' = \Gamma(\varphi) \cap V(Z')$. If $B \in V'$, then $B|\mathbf{B}^{n(i(x))} \in Z'$, therefore,

$$M'\left[\bar{x}B^{n(i(x)-1)}, B|\mathbf{B}^{n(i(x))}\right] \leq N'\left[\bar{x}B^{n(i(x)-1)}, B|\mathbf{B}^{n(i(x))}\right]. \tag{9}$$

There exists a description $N \in$ n.u.$\mathcal{N}$ such that

$$N(x,B) = \begin{cases} N'[\bar{x}B^{n(i(x)-1)}, B|\mathbf{B}^{n(i(x))}], \\ \qquad\qquad \text{if } |x| > n_0; \\ M(x,B), \quad \text{if } |x| \leq n_0. \end{cases} \tag{10}$$

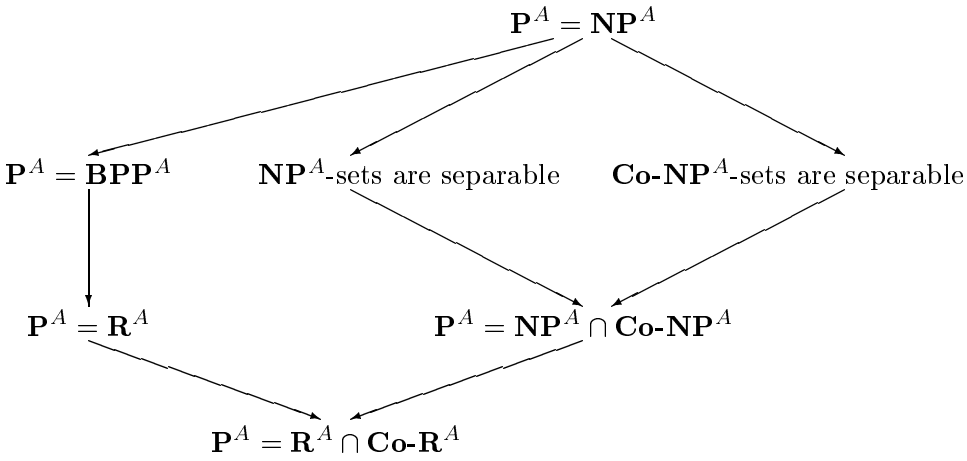
Combining (8), (9) and (10) we obtain that $M(x,B) \leq N(x,B)$ for all $x \in \mathbf{B}^*$ and all $B \in V'$.$\square$

In all the applications but one we will use only superbases consisting of a single base.

4 The applications of the universum method

The assertions on complexity classes to which the method will be applied are shown on the Figure 4. The edges of the drawn directed graph represent

Figure 4:



relativizable implications (i.e., implications that are true under any oracle). For example, the implication $\mathbf{P}^A = \mathbf{NP}^A \Rightarrow \mathbf{P}^A = \mathbf{BPP}^A$ is true by the well known Sipser's result $\mathbf{BPP}^A \subset \Sigma_4^A$ (P.Gács improved that result to $\mathbf{BPP}^A \subset \Sigma_2^A$ [S 83]). We apply the universum method to prove the existence of oracles under which one or another combination of assertions that label the nodes of the graph holds. There are 17 possible combinations of those assertions. They are listed in the Table 1. The signs "+" and "$\oplus$" put in a line of that table indicate that the corresponding assertion is true. The signs "$-$" and "$\ominus$" indicate that the corresponding assertion is false. The difference between the signs "+" and "$\oplus$" is that the truth of assertions labeled by "+" follows from the truth of assertions labeled by "$\oplus$" but the truth of any assertion labeled by "$\oplus$" does not follow from the truth of other assertions. The same difference is between the signs "$-$" and "$\ominus$". The commentary ending each line includes information about where the combination present in the line is proved or some information about how it can be proved.

We prove the existence of oracles for which the combinations of all the lines but the lines number 3, 4, 8, and 9 are true. The problem whether there exist oracles for which the combinations in lines 3, 4, 9 and 10 are

Table 1:

	$\mathbf{P = NP}$	**NP**-sets are separable	**Co-NP**-sets are separable	$\mathbf{P = NP \cap Co\text{-}NP}$	$\mathbf{P = BPP}$	$\mathbf{P = R}$	$\mathbf{P = R \cap Co\text{-}R}$	Commentary
1	$\oplus$	$+$	$+$	$+$	$+$	$+$	$+$	[BGS 75]
2	$\ominus$	$\oplus$	$\oplus$	$+$	$\oplus$	$+$	$+$	Theorem 4.12
3	$-$	$\oplus$	$\oplus$	$+$	$\ominus$	$\oplus$	$+$	Unknown
4	$-$	$\oplus$	$\oplus$	$+$	$-$	$\ominus$	$+$	Unknown
5	$-$	$\oplus$	$\ominus$	$+$	$\oplus$	$+$	$+$	Theorem 4.4
6	$-$	$\oplus$	$\ominus$	$+$	$\ominus$	$\oplus$	$+$	Theorem 4.7
7	$-$	$\oplus$	$\ominus$	$+$	$-$	$\ominus$	$+$	Theorem 4.6
8	$-$	$\ominus$	$\oplus$	$+$	$\oplus$	$+$	$+$	Theorem 4.2
9	$-$	$\ominus$	$\oplus$	$+$	$\ominus$	$\oplus$	$+$	Unknown
10	$-$	$\ominus$	$\oplus$	$+$	$-$	$\ominus$	$+$	Unknown
11	$-$	$\ominus$	$\ominus$	$\oplus$	$\oplus$	$+$	$+$	Theorem 4.5
12	$-$	$\ominus$	$\ominus$	$\oplus$	$\ominus$	$\oplus$	$+$	Theorem 4.8
13	$-$	$\ominus$	$\ominus$	$\oplus$	$+$	$\ominus$	$+$	Theorem 4.9
14	$-$	$-$	$-$	$\ominus$	$\oplus$	$+$	$+$	Theorem 4.3
15	$-$	$-$	$-$	$\ominus$	$\ominus$	$\oplus$	$+$	Theorem 4.10
16	$-$	$-$	$-$	$\ominus$	$-$	$\ominus$	$\oplus$	Theorem 4.11
17	$-$	$-$	$-$	$-$	$-$	$-$	$\ominus$	Theorem 4.1

true, remains open. Moreover, the following question remains unresolved.

Question 4.1 *Is there an oracle A under which* **Co-NP***-sets are separable and* $\mathbf{P}^A \neq \mathbf{BPP}^A$.

When constructing oracles we shall use following six standard bases:

- $Z(\leq 1) = \{\alpha \in \mathbf{F} \mid \#_1\alpha \leq 1\}$; this base was already used in the proof of Theorem 2.1
- $Z(=1) = \{\alpha \in \mathbf{F} \mid \#_1\alpha = 1\}$
- $Z(\geq 1) = \{\alpha \in \mathbf{F} \mid \#_1\alpha \geq 1\}$
- $Z(\mathbf{BPP}) = \bigcup_{n\in\mathbf{S}}\{\alpha \in \mathbf{F}_n \mid \#_1\alpha/2^n \notin [1/3; 2/3]\}$
- $Z(\mathbf{R}) = \bigcup_{n\in\mathbf{S}}\{\alpha \in \mathbf{F}_n \mid \#_1\alpha/2^n \notin (0; 1/2]\}$
- Let for $\alpha, \beta \in \mathbf{F}_n$ $\alpha \oplus \beta$ denote the function in $\mathbf{F}_{n+1}$ whose value on word $0u$ is equal to $\alpha(u)$ and on word $1u$ to $\beta(u)$. Let $Z(\mathbf{R}\cap\mathbf{Co\text{-}R}) = \bigcup_{n\in\mathbf{S}}\{\alpha\oplus\beta \mid \alpha, \beta \in \mathbf{F}_{n-1},\ (\#_1\alpha/2^{n-1} > 1/2, \#_1\beta = 0 \text{ or } \#_1\beta/2^{n-1} > 1/2, \#_1\alpha = 0)\}$

Other bases being used in proofs are built from these standard bases by the following operation $+$ on bases: $Z' + Z'' = \{\alpha \in \mathbf{F}_{n_i} \mid i \text{ is even and } \alpha \in Z'\} \cup \{\alpha \in \mathbf{F}_{n_i} \mid i \text{ is odd and } \alpha \in Z''\}$. In the similar way (by using residues modulo 3) $Z' + Z'' + Z'''$ is defined.

The universum $V(Z(\leq 1))$ fits for constructing an oracle under which NP-sets are inseparable (with L_0^B and L_1^B defined above being inseparable sets). The universum $V(Z(\geq 1))$ fits for constructing an oracle under which Co-NP-sets are inseparable (with $\{1^n \mid n \in \mathbf{S}\} \setminus L_0^B$ and $\{1^n \mid n \in \mathbf{S}\} \setminus L_1^B$ being unseparable sets). The universum $V(Z(=1))$ fits for constructing an oracle under which $\mathbf{NP} \cap \mathbf{Co\text{-}NP} \neq \mathbf{P}$ (with L_0^B being a language in $\mathbf{NP} \cap \mathbf{Co\text{-}NP} \setminus \mathbf{P}$). The universums $V(Z(\mathbf{BPP}))$, $V(Z(\mathbf{R}))$ and $V(Z(\mathbf{R}\cap\mathbf{Co\text{-}R}))$ respectively fit for constructing an oracle under which $\mathbf{BPP} \neq \mathbf{P}$, $\mathbf{R} \neq \mathbf{P}$ and $\mathbf{R}\cap\mathbf{Co\text{-}R} \neq \mathbf{P}$. It is easy to verify that assertion (a$''$) is true in all listed cases (i.e., it holds, for example, for $\mathcal{K} = \mathrm{BPP}$ and $\mathcal{L} = \mathrm{P}$ and $Z = Z(\mathbf{BPP})$. Moreover, in the listed cases, assertion (a$''$) is robust under addition of bases. This means, for example, that assertion (a$''$) is true for $\mathcal{K} = \mathrm{BPP}$ and $\mathcal{L} = \mathrm{P}$ and $Z = Z(\mathbf{BPP})+Z'$ for any Z'. In other words the following lemma holds.

Lemma 4.1 *Assertion* (a$''$) *holds for the following combinations of* $\mathcal{Z}, \mathcal{K}, \mathcal{L}$*:*

- $\mathcal{Z} = \{Z(\leq 1) + Z'\}$, $\mathcal{K} =$ NP-separation, $\mathcal{L} =$ P;
- $\mathcal{Z} = \{Z(=1) + Z'\}$, $\mathcal{K} =$ NP $\cap$ Co-NP, $\mathcal{L} =$ P;
- $\mathcal{Z} = \{Z(\geq 1) + Z'\}$, $\mathcal{K} =$ Co-NP-separation, $\mathcal{L} =$ P;
- $\mathcal{Z} = \{Z(\mathbf{BPP}) + Z'\}$, $\mathcal{K} =$ BPP, $\mathcal{L} =$ P;
- $\mathcal{Z} = \{Z(\mathbf{R}) + Z'\}$, $\mathcal{K} =$ R, $\mathcal{L} =$ P;
- $\mathcal{Z} = \{Z(\mathbf{R} \cap \mathbf{Co\text{-}R}) + Z'\}$, $\mathcal{K} =$ R $\cap$ Co-R, $\mathcal{L} =$ P.

*Proof.*Proof Obviously.□

We need also some facts about the cases in which the assertion (b$''$) is true. These facts are stated in the following five crucial lemmas.

Lemma 4.2 *The assertion* (b$''$) *is true for* $\mathcal{K} =$ Co-NP-separation, $\mathcal{L} =$ P *and* $\mathcal{Z} = \{Z(\leq 1)\}$.

Proof. This is already proved, in fact, in the second proof of Theorem 2.1.□

Lemma 4.3 *The assertion* (b$''$) *is true for* $\mathcal{K} =$ BPP, $\mathcal{L} =$ P *and* $\mathcal{Z} = \{Z(\leq 1)\}$ *or* $\mathcal{Z} = \{Z(=1)\}$.

Proof. Let M be a machine in n.u.BPP being correct on $Z(=1)$. As $Z(=1) \subset Z(\leq 1)$ it suffices to construct a polynomial decision tree N such that $M[x, \alpha] = N[x, \alpha]$ for all $x \in \mathbf{B}^*$, $\alpha \in Z(\leq 1)$. The decision tree N on input $[x, \alpha]$ works as follows. Denote by n the norm of α. Let k be the length of random strings used by M on input $[x, \alpha]$ (we may assume that k depends only on $|x|$ and $\|\alpha\|$). Find first the probability p of the event "M accepts $[x, \mathbf{0}_n]$", i.e., $\mathrm{Prob}_{r \in \mathbf{B}^k}\{M[x, \alpha, r] = 1\}$, where $M[x, \alpha, r]$ denotes the result output by M on input $[x, \alpha]$ and random string r, and $\mathrm{Prob}_{r \in \mathbf{B}^k}$ means the probability over $\mathbf{B}^k$ with respect to the uniform probability distribution. Without loss of generality we may assume that $p \geq 1/2$ (the case $p \leq 1/2$ is entirely similar). Given $y \in \mathbf{B}^n$ and $\beta \in \mathbf{F}_n$ denote

$$w_\beta(y) = \mathrm{Prob}_{r \in \mathbf{B}^k}\{y \in \mathit{Query}_M[x, \beta, r]\},$$

i.e., the probability of the event "M on input $[x, \beta]$ queries '$\beta(y) =?$'". It is easy to see that

$$\sum_{y \in \mathbf{B}^n} w_\beta(y) = \frac{1}{2^k} \sum_{r \in \mathbf{B}^k} |\mathit{Query}_M[x, \beta, r]| \leq \mathrm{poly}(|x|, n).$$

Denote by W the set of all $y \in \mathbf{B}^n$ such that $w_{\mathbf{0}_n}(y) \geq 1/6$. Obviously, $|W| \leq \mathrm{poly}(|x|, n)$.

Find W and query '$\alpha(y) =?$' for all $y \in W$. These are all the queries made by the decision tree N. There are two possibilities: 1) $\forall y \in W\ \alpha(y) = 0$ and 2) $\exists y \in W\ \alpha(y) = 1$. Consider the cases separately.

1) If $\forall y \in W\ \alpha(y) = 0$, then $M[x, \alpha] \neq 0$ provided $\alpha \in Z(\leq 1)$. Indeed, assume that $\alpha \in Z(\leq 1)$ and the probability q of the event "M accepts α" is less than $1/3$. Then $\alpha \neq \mathbf{0}_n$ because M accepts $\mathbf{0}_n$ with probability $p \geq 1/2$. Denote by y the word such that $\alpha(y) = 1$. Then $w_{\mathbf{0}_n}(y) < 1/6$ because $y \notin W$. Make use of the following

Lemma 4.4 *For any $\beta, \gamma \in \mathbf{F}_n$,*

$$\Big|\mathrm{Prob}_r\{M[x, \gamma, r] = 1\} - \mathrm{Prob}_r\{M[x, \beta, r] = 1\}\Big| \leq \textstyle\sum_{z \in \mathbf{B}^n : \gamma(z) \neq \beta(z)} w_\beta(z).$$

Proof. Obviously.

By the above lemma, $|\mathrm{Prob}_r\{M[x, \alpha, r] = 1\} - \mathrm{Prob}_r\{M[x, \mathbf{0}_n, r] = 1\}| \leq w_{\mathbf{0}_n}(y) < 1/6$, therefore, $\mathrm{Prob}_r\{M[x, \alpha, r] = 1\} > 1/2 - 1/6 = 1/3$. The obtained contradiction shows that $M[x, \alpha] \neq 1$ if α is in $Z(\leq 1)$. Output 1 in the first case.

2) $\exists y \in W\ \alpha(y) = 1$. If there exist at least two $y \in W$ such that $\alpha(y) = 1$, then output 0, as in this case $\alpha \notin Z(\leq 1)$. Assume that there exists the unique $y \in W$ such that $\alpha(y) = 1$. Define

$$\beta(z) = \begin{cases} 1, & \text{if } z = y; \\ 0, & \text{if } z \in \mathbf{B}^n \setminus \{y\}. \end{cases}$$

Note that $\beta = \alpha$ if $\alpha \in Z(\leq 1)$. Find the probability q of the event "M accepts $[x, \beta]$" and output 1 if $q > 2/3$ and 0 else.$\square$

Lemma 4.5 *The assertion* (b$''$) *is true for $\mathcal{K} =$* NP-separation, *$\mathcal{L} =$* P *and $\mathcal{Z} = \{Z\}$, where Z is any base of the following ones: $\mathbf{F}$, $Z(\geq 1)$, $Z(\mathbf{BPP})$, $Z(\mathbf{R})$.*

Proof. Let Z be a base from the above list. Let M be a description in n.u.NP-separation being correct on Z. It suffices to construct a polynomial decision tree N such that $M_i[x, \alpha] \leq N[x, \alpha]$ for all $x \in \mathbf{B}^*$, $\alpha \in \mathbf{F}$.

Let M be the pair $\langle M_0, M_1 \rangle$ of machines from n.u.NP. The correctness of M on Z means that for all $x \in \mathbf{B}^*, \alpha \in Z$ there exists $i \in \{0, 1\}$ such that

$M_i[x,\alpha] = 0$. We have to construct a polynomial decision tree N that on inputs $x \in \mathbf{B}^*$, $\alpha \in \mathbf{F}$ finds an $i \in \{0,1\}$ such that $M_i[x,\alpha] = 0$.

Let $x \in \mathbf{B}^*$ and $\alpha \in \mathbf{F}$ are inputs of N. Let α be in $\mathbf{F}_n$. Call any function having the form

$$\beta | \mathit{Query}_{M_i}[c,\beta] \cap \mathbf{B}^n$$

where $\beta \in \mathbf{F}_n$, $M_i[x,\beta] = 1$ and c is an accepting computation of M_i on input $[x,\beta]$, an *i-certificate*. Note that if γ is an i-certificate and α continues γ, then $M_i[x,\alpha] = 1$. Obviously, the cardinality of domain of any i-certificate ($i \in \{0,1\}$) is bounded by a polynomial of $|x|$ and n, say $p(|x|,n)$. We claim that if $2^n > 8p(|x|,n)$, then any 0-certificate φ is inconsistent with any 1-certificate ψ (that is, $\varphi(y) \neq \psi(y)$ for some $y \in \mathrm{Dom}(\varphi) \cap \mathrm{Dom}(\psi)$). Indeed, assume that φ and ψ are consistent. Then there exists a function $\beta \in \mathbf{F}_n$ that continues both φ and ψ. As $|\mathrm{Dom}(\varphi)| + |\mathrm{Dom}(\psi)| \leq 2p(|x|,n) < 2^{n-2}$ we may assume that $\beta \in Z$. We have $M_0[x,\beta] = M_1[x,\beta] = 1$ because β continues both φ and ψ. Therefore, M is incorrect on Z. The contradiction shows that any 0-certificate is inconsistent with any 1-certificate.

So N on input $[x,\alpha]$ works as follows. Consider two cases.

First case: $2^n \leq 8p(|x|,n)$. Then query '$\alpha(y) =?$' for all $y \in \mathbf{B}^n$ and then find $M_0[x,\alpha]$ and $M_1[x,\alpha]$ by checking all computations of M_0 and M_1 on $[x,\alpha]$. The number of queries made to α is at most $8p(|x|,n)$.

Second case: $2^n > 8p(|x|,n)$. Then any 0-certificate is inconsistent with any 1-certificate. Execute the program shown on the Figure 5. Obviously, that program makes $\mathrm{poly}(|x|,n)$ queries to α. It remains to prove that if $\alpha \in Z$, then the program outputs an $i \in \{0,1\}$ such $M_i[x,\alpha] = 0$.

Assume that $\alpha \in Z$. Let $m = p(|x|,n)$. Obviously, it suffices to prove that for some $i \leq m+1$ there exists no 1-certificate consistent with $\alpha|U_i$ or there exists no 0-certificate consistent with $\alpha|U_i$. Assume that this is not the case. Pick a 1-certificate ψ consistent with $\alpha|U_{m+1}$. Then $\mathrm{Dom}(\psi)$ intersects with $U_{i+1} \setminus U_i = \mathrm{Dom}(\varphi_i) \setminus U_i$ (for all $i \leq m+1$) because ψ and φ_i are inconsistent and have the same value (equal to $\alpha(y)$) on any $y \in U_i$. Therefore, $\mathrm{Dom}(\psi)$ intersects with each of pairwise disjoint sets U_1, $U_2 \setminus U_1$, $U_3 \setminus U_2$, ..., $U_{m+1} \setminus U_m$. Consequently $|\mathrm{Dom}(\psi)| \geq m+1$. Contradiction.

Lemma 4.6 *The assertion* (b'') *is true for* $\mathcal{K} = \mathrm{BPP}$, $\mathcal{L} = \mathrm{P}$ *and* $\mathcal{Z} = \{Z\}$, *where* $Z = \mathbf{F}$ *or* $Z = Z(\geq 1)$.

Proof. Consider only the case $Z = Z(\geq 1)$ (the case $Z = \mathbf{F}$ can be done even simpler). Let M be a machine from n.u.BPP that is correct on Z.

Figure 5:

```
begin
  U_0 := ∅;
  for i = 1 to p(|x|, n) + 1
    do
      if there exists no 0-certificate
        being consistent with α|U_i
        then output 0 and halt;
        elseif there exists no 1-certificate
          being consistent with α|U_i
        then output 1 and halt;
        else pick a 0-certificate φ_i
          being consistent with α|U_i;
          query 'α(y) =?' for all y ∈ Dom(φ_i);
          U_{i+1} := U_i ∪ Dom(φ_i);
      fi;
    od;
  output 0;
end
```

We have to find a machine N in n.u.P such that $M[x,\alpha] = N[x,\alpha]$ for all $x \in \mathbf{B}^*, \alpha \in Z$. Let us make use of Lemma 4.5. By that lemma it suffices to construct a description K in n.u.NP-separation such that $M[x,\alpha] = K[x,\alpha]$ for all $x \in \mathbf{B}^*, \alpha \in Z$ (as M is correct on Z this implies that K is correct on Z, too). In other words, we have to construct two machines N_0, N_1 in n.u.NP such that $N_1[x,\alpha] = M[x,\alpha]$, $N_0[x,\alpha] = 1 - M[x,\alpha]$ for all $x \in \mathbf{B}^*, \alpha \in Z$. We construct machine N_1 (and machine N_0 can be constructed in the similar way).

Machine N_1 on input $[x,\alpha]$ works as follows. Let $n = \|\alpha\|$ and let $k = \mathrm{poly}(|x|, n)$ be the maximal number of queries that M can make on inputs of the form $[x,\beta]$, $\beta \in \mathbf{F}_n$. Guess a set $W \subset \mathbf{B}^n$ of cardinality $\leq 9k^2 + 3k$ and then query '$\alpha(y) =?$' for all $y \in W$. Check if $M[x,\beta] = 1$ for any $\beta \in Z_n$ such that $\beta|W = \alpha|W$. If this is the case, then accept. Otherwise reject.

Obviously, if N_1 accepts $[x,\alpha]$, then $M[x,\alpha] = 1$. Thus, we have to prove the converse: if $M[x,\alpha] = 1$ then there exists a set $W \subset \mathbf{B}^n$ of cardinality $\leq 9k^2 + 3k$ such that

$$\forall \beta \in Z_n \ (\beta|W = \alpha|W \Rightarrow M[x,\beta] = 1). \tag{11}$$

Assume, that $M[x,\alpha] = 1$. For $y \in \mathbf{B}^n$ denote by $w_\alpha(y)$ the probability of the event "M on input $[x,\alpha]$ queries '$\alpha(y) =?$'". Let

$$W = \{y \in \mathbf{B}^n \mid w_\alpha(y) \geq \frac{1}{9k+3}\}.$$

As $\sum_{y \in \mathbf{B}^n} w_\alpha(y) \leq k$, we have $|W| \leq (9k+3)k$. We claim that assertion (11) is true. Assume that there exists $\beta \in Z_n$ such that $\beta|W = \alpha|W$ and $M[x,\beta] = 0$. Choose a $\beta \in Z_n$ satisfying these conditions and differing from α on the least number of arguments. Denote

$$U = \{y \in \mathbf{B}^n \mid \alpha(y) \neq \beta(y)\}.$$

For any $y \in \mathbf{B}^n$ denote by β_y the function

$$\beta_y(z) = \begin{cases} \beta(z), & \text{if } z \neq y, \\ \alpha(z), & \text{if } z = y. \end{cases}$$

We claim that $w_\beta(y) > 1/3$ for any y in U possibly but one (where $w_\beta(y)$ is the probability of the event "M on input $[x,\beta]$ queries '$\beta(y) =?$' "). Indeed, let y be an element of U. Then $\beta_y|W = \alpha|W$ and β_y differs from α on

less arguments than β does. Therefore $M[x, \beta_y] = 1$ or $\beta_y \notin Z_n$ (that is, $\#_1\beta_y = 0$). Consider two cases.

First case: $\beta_y \in Z_n$. Then $M[x, \beta_y] = 1$. Therefore, by Sublemma 4.4, $w_\beta(y) \geq \mathrm{Prob}_r\{M[x, \beta_y, r] = 1\} - \mathrm{Prob}_r\{M[x, \beta, r] = 1\} > 2/3 - 1/3 = 1/3$.

Second case: $\beta_y \notin Z_n$. Then $\#_1\beta_y = 0$. This may happen only if $\#_1\beta = 1$ and therefore this case can occur for the single y.

As $\sum_{y \in \mathbf{B}^n} w_\beta(y) \leq k$, we have $|U| < 3k + 1$. Since $U \cap W = \emptyset$, we have $w_\alpha(y) < \frac{1}{9k+3}$ for any $y \in U$. Hence $\sum_{y \in U} w_\alpha(y) < \frac{1}{(9k+3)}(3k + 1) = \frac{1}{3}$. On the other hand, by Sublemma 4.4

$$\begin{gathered}\sum_{y \in U} w_\alpha(y) \\ \geq \mathrm{Prob}_r\{M[x, \alpha, r] = 1\} - \mathrm{Prob}_r\{M[x, \beta, r] = 1\} \\ > 2/3 - 1/3 = 1/3.\end{gathered}$$

The contradiction proves the lemma.□

Lemma 4.7 *The assertion* (b″) *is true for* $\mathcal{K} = \mathrm{R}$, $\mathcal{L} = \mathrm{P}$ *and* $\mathcal{Z} = \{Z(\mathbf{BPP})\}$.

Proof. Let M be a machine in n.u.R being correct on Z. By Lemma 4.5 it sufices to construct a machine P in n.u.(NP ∩ Co-NP) such that

$$M[x, \beta] = P[x, \beta] \text{ for any } x \in \mathbf{B}^*, \beta \in Z_n.$$

It follows immediately from the definition of the class R that there exists an n.u.NP-machine P_1 such that $M[x, \beta] = P_1[x, \beta]$ for all x, β.

Thus, we have to construct an n.u.NP-machine P_0 such that $P_0[x, \beta] = 1 - M[x, \beta]$ for all $x \in \mathbf{B}^*, \beta \in Z_n$. Machine P_0 on input $[x, \beta]$, $\beta \in \mathbf{F}_n$, works as follows. Let $k = \mathrm{poly}(|x|, n)$ be the maximal number of queries to β which machine M can make during the work on input $[x, \beta]$, $\beta \in \mathbf{F}_n$. Let us prove that if $M[x, \beta] = 0$ and $\beta \in Z_n$, then there exists a set $W \subset \mathbf{B}^n$ of cardinality less than $4k^2$ such that $M[x, \gamma] = 0$ for all $\gamma \in \mathbf{F}_n$ such that $\gamma|W = \beta|W$. Denote by $w_\beta(y)$ the probability of the event "M on input $[x, \beta]$ queries '$\beta(y) =?$' ". Let

$$W = \{y \in \mathbf{B}^n \mid w_\beta(y) > 1/4k\}.$$

Note that $|W| < 4k^2$. Let us prove that $M[x, \gamma] = 0$ for all $\gamma \in \mathbf{F}_n$ such that $\gamma|W = \beta|W$. Assume the contrary: there exists $\gamma \in \mathbf{F}_n$ such that

$M[x,\gamma] \neq 0$ and $\gamma|W = \beta|W$. Then for at least one random input, M accepts $[x,\gamma]$. Let us fix such a random input and denote by U the set of all the $y \in \mathbf{B}^n$ such that the query '$\gamma(y) =?$' is made during the computation of M on $[x,\gamma]$ for that random input. Obviously, $|U| \leq k$. Let

$$\delta(y) = \begin{cases} \gamma(y), & \text{if } y \in U; \\ \beta(y), & \text{if } y \in \mathbf{B}^n \setminus U. \end{cases}$$

If δ belonged to Z_n we would obtain a contradiction: the probability of the event "M accepts $[x,\delta]$" is positive, hence, this probability is greater than $1/2$. Therefore, by Sublemma 4.4,

$$\sum_{\delta(y)\neq\beta(y)} w_\beta(y) > 1/2.$$

On the other hand, $\{y \mid \delta(y) \neq \beta(y)\} \subset U \setminus W$, consequently,

$$\sum_{\delta(y)\neq\beta(y)} w_\beta(y) \leq |U|\frac{1}{4k} \leq \frac{k}{4k} = \frac{1}{4}.$$

Now we have to explain what to do if $\delta \notin Z_n$, that is, $\#_1\delta \in [(1/3)2^n, (2/3)2^n]$. We have $\beta \in Z_n$, that is, $\#_1\beta \notin [(1/3)2^n, (2/3)2^n]$. Without loss of generality we may assume that $\#_1\beta > (2/3)2^n$. Then $\#_1\delta > (2/3)2^n - |U|$. We have $|U| \leq k = \mathrm{poly}(|x|, n)$. Therefore, we may assume that $2|U| + |W| \leq (1/3)2^n$ (if this is not the case, then $2^n \leq \mathrm{poly}(|x|, n)$ and we can query '$\beta(y) =?$' for all $y \in \mathbf{B}^n$ to get know β and then can simulate the work of M on $[x,\beta]$ for all random inputs). As $2|U| + |W| \leq (1/3)2^n \leq \#_0\delta$, there exists a set $V \subset \mathbf{B}^n$ of cardinality $|U|$ such that $V \cap (U \cup W) = \emptyset$ and such that $\delta(y) = 0$ for all $y \in V$. Pick such a V and change the value of δ on all the y in V. Now we have $\#_1\delta > (2/3)2^n$, therefore $\delta \in Z_n$. As $\delta(y) = \gamma(y)$ for any $y \in U$, we have $\mathrm{Prob}\{M \text{ accepts } [x,\delta]\} > 0$. Therefore, $\mathrm{Prob}\{M \text{ accepts } [x,\delta]\} > 1/2$. Recall that $M[x,\beta] = 0$, that is, $\mathrm{Prob}\{M \text{ accepts } [x,\beta]\} = 0$. Hence, by Lemma 4.4,

$$\sum_{\delta(y)\neq\beta(y)} w_\beta(y) > 1/2.$$

On the other hand,

$$\sum_{\delta(y)\neq\beta(y)} w_\beta(y) \leq (|U| + |V|)\frac{1}{4k} \leq \frac{2k}{4k} = \frac{1}{2}.$$

Table 2:

	NP-separation	Co-NP-separation	NP ∩ Co-NP	BPP	R	R ∩ Co-R
$Z(\leq 1)$	–	+	+	+	+	+
$Z(=1)$	–	–	–	+	+	+
$Z(\geq 1)$	+	–	+	+	+	+
$Z(\mathbf{F})$	+	– (o)	+	+	+	+
$Z(\mathbf{BPP})$	+	– (o)	+	–	+	+
$Z(\mathbf{R})$	+	– (o)	+	–	–	+
$Z(\mathbf{R}\cap\mathbf{Co\text{-}R})$	–	–	–	–	–	–

The contradiction shows that $M[x,\gamma]=0$ for all $\gamma\in\mathbf{F}_n$ such that $\gamma|W=\beta|W$.

Thus, machine P_0 on input $[x,\beta]$ accepts if there exists a set $W\subset\mathbf{B}^n$ of cardinality $<4k^2$ such that $M[x,\gamma]=0$ for any $\gamma\in Z_n$ such that $\beta|W=\gamma|W$.□

The above proven facts on bases are shown on the Table 2. The sign "+" in a line of Table 2 indicates that the assertion (b$''$) is true for the corresponding principal superbase, the corresponding class $\mathcal{M}$ and for $\mathcal{N}=$ P. The sign "–" in a line of the table indicates that the assertion (a$''$) is true for the corresponding principal superbase, the corresponding class $\mathcal{K}$ and for $\mathcal{L}=$ P. The letter "o" means that the proof was ommited (because we do not need the corresponding assertion).

As simple consequences from the above lemmas we get the following four theorems. The next theorem has been known for a long time.

Theorem 4.1 *There exists an oracle A for which $\mathbf{R}^A\cap\mathbf{Co\text{-}R}^A\neq\mathbf{P}^A$ (17th line in the Table 1).*

Proof. Take the base $Z(\mathbf{R}\cap\mathbf{Co\text{-}R})$.□

Theorem 4.2 *There exists an oracle A such that $\mathbf{NP}^A$-sets are inseparable, $\mathbf{Co\text{-}NP}^A$-sets are separable and $\mathbf{P}^A=\mathbf{BPP}^A$ (8th line in the Table 1).*

Proof. Take the base $Z=Z(\leq 1)$.□

Theorem 4.3 *There exists an oracle A such that* $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A \neq \mathbf{P}^A$ *and* $\mathbf{BPP}^A = \mathbf{P}^A$ *(14th line in the Table 1).*

Proof. Take the base $Z = Z(=1)$.□

Theorem 4.4 *There exists an oracle A such that* $\mathbf{NP}^A$*-sets are separable,* $\mathbf{Co\text{-}NP}^A$*-sets are inseparable and* $\mathbf{BPP}^A = \mathbf{P}^A$ *(5th line in the Table 1).*

Proof. Take the base $Z = Z(\geq 1)$.□

To obtain further consequences from the lemmas we need the following simple

Lemma 4.8 *If the assertion (b″) is true for the classes $\mathcal{M}$ and $\mathcal{N}$ and for both superbases $\{Z'\}$ and $\{Z''\}$, then it holds also for $\mathcal{M}$ and $\mathcal{N}$ and for superbase $\{Z' + Z''\}$.*

Proof. Obviously.□

Theorem 4.5 *There exists an oracle A such that* $\mathbf{NP}^A$*-sets and* $\mathbf{Co\text{-}NP}^A$*-sets are inseparable,* $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A = \mathbf{P}^A$ *and* $\mathbf{BPP}^A = \mathbf{P}^A$ *(11th line in the Table 1).*

Proof. Take the base $Z = Z(\leq 1) + Z(\geq 1)$.□

Theorem 4.6 *There exists an oracle A such that* $\mathbf{NP}^A$*-sets are separable,* $\mathbf{Co\text{-}NP}^A$*-sets are inseparable and* $\mathbf{P}^A \neq \mathbf{R}^A$ *(7th line in the Table 1).*

Proof. Take the base $Z = Z(\mathbf{R}) + Z(\geq 1)$.□

Theorem 4.7 *There exists an oracle A such that* $\mathbf{NP}^A$*-sets are separable,* $\mathbf{Co\text{-}NP}^A$*-sets are inseparable,* $\mathbf{BPP}^A \neq \mathbf{P}^A$, $\mathbf{R}^A = \mathbf{P}^A$ *(6th line in the Table 1).*

Proof. Take the base $Z = Z(\mathbf{BPP}) + Z(\geq 1)$.□

Theorem 4.8 *There exists an oracle A such that* $\mathbf{NP}^A$*-sets are inseparable,* $\mathbf{Co\text{-}NP}^A$*-sets are inseparable,* $\mathbf{BPP}^A \neq \mathbf{P}^A$, $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A = \mathbf{P}^A$ *and* $\mathbf{R}^A = \mathbf{P}^A$ *(12th line in the Table 1).*

Proof. Take the base $Z = Z(\leq 1) + Z(\geq 1) + Z(\mathbf{BPP})$.□

Theorem 4.9 *There exists an oracle A such that $\mathbf{NP}^A$-sets are inseparable, $\mathbf{Co\text{-}NP}^A$-sets are inseparable, $\mathbf{R}^A \neq \mathbf{P}^A$ and $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A = \mathbf{P}^A$ (13th line in the Table 1).*

Proof. Take the base $Z = Z(\leq 1) + Z(\geq 1) + Z(\mathbf{R})$.□

Theorem 4.10 *There exists an oracle A such that $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A \neq \mathbf{P}^A$, $\mathbf{BPP}^A \neq \mathbf{P}^A$ and $\mathbf{R}^A = \mathbf{P}^A$ (15th line in the Table 1).*

Proof. Take the base $Z = Z(=1) + Z(\mathbf{BPP})$.□

Theorem 4.11 *There exists an oracle A such that $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A \neq \mathbf{P}^A$, $\mathbf{R}^A \neq \mathbf{P}^A$ and $\mathbf{R}^A \cap \mathbf{Co\text{-}R}^A = \mathbf{P}^A$ (16th line in the Table 1).*

Proof. Take the base $Z = Z(=1) + Z(\mathbf{BPP})$.□

Theorem 4.12 *There exists an oracle A such that $\mathbf{P}^A \neq \mathbf{NP}^A$, $\mathbf{NP}^A$-sets are separable, $\mathbf{Co\text{-}NP}^A$-sets are separable and $\mathbf{BPP}^A = \mathbf{P}^A$ (second line in the Table 1).*

Proof. This is the only case in which the superbase consists of more than one base. For any $j \in \mathbf{N}$, $j \geq 1$ consider the base Z^j defined as follows:

$$\alpha \in Z^j_n \Leftrightarrow \#_1\alpha \leq n/j.$$

Take the superbase $\mathcal{Z} = \{Z^j \mid j \geq 1\}$.

To prove (a$''$) for $\mathcal{K} = \mathrm{NP}$, $\mathcal{L} = \mathrm{P}$ take the description

$$K[\alpha] = \begin{cases} 1, & \text{if } \#_1\alpha \geq 1 \\ 0, & \text{otherwise.} \end{cases}$$

Let us prove (b$''$) for $\mathcal{M} = \text{NP-separation}, \mathcal{N} = \mathrm{P}$. Let $M = \langle M_0, M_1 \rangle$ be a pair of machines in n.u.NP and let Z^j be a base in $\mathcal{Z}$ such that $M_0[x, \alpha] = 0$ or $M_1[x, \alpha] = 0$ for all $x \in \mathbf{B}^*, \alpha \in Z^j$. We have to construct a machine $N \in$ n.u.P and a base $Z^{j'} \subset Z^j$ such that $M[x, \alpha] \leq N[x, \alpha]$ for all $x \in \mathbf{B}^*$, $\alpha \in Z^{j'}$. Let $j' = 2j$. We have to construct a polynomial decision tree that for given $x \in \mathbf{B}^*$ and $\alpha \in Z^{j'}$ finds an $i \in \{0, 1\}$ such that $M_i[x, \alpha] = 0$.

Let us be given $x \in \mathbf{B}^*$ and $\alpha \in Z^{j'}$. Let $n = \|\alpha\|$. Call any function having the form

$$\beta | \mathit{Query}_{M_i}[c, \beta],$$

where $\beta \in Z_n^{j'}$, $M_i[x,\beta] = 1$ and c is an accepting computation of M_i on input $[x,\beta]$ an *i-certificate* ($i = 0, 1$). Let us prove that any 0-certificate is inconsistent with any 1-certificate. Assume that a 0-certificate φ is consistent with a 1-certificate ψ. Then $\#_1\varphi \le \frac{n}{2j}$ and $\#_1\psi \le \frac{n}{2j}$. Set

$$\beta(y) = \begin{cases} \varphi(y), & \text{if } y \in \mathrm{Dom}(\varphi); \\ \psi(y), & \text{if } y \in \mathrm{Dom}(\psi); \\ 0, & \text{if } y \in \mathbf{B}^n \setminus (\mathrm{Dom}(\varphi) \cup \mathrm{Dom}(\psi)). \end{cases}$$

Then $\#_1\beta \le \frac{n}{2j} + \frac{n}{2j} = \frac{n}{j}$, that is, $\beta \in Z^j$ and $M_0[x,\beta] = M_1[x,\beta] = 1$. The contradiction shows that any 0-certificate is iconsistent with any 1-certificate.

Further we can reason just as in the proof of Lemma 4.5.

Let us prove (b$''$) for $\mathcal{M}$ = Co-NP-separation, $\mathcal{N}$ = P. Let $M = \langle M_0, M_1\rangle$ be a description in n.u.Co-NP-separation and Z^j be a base such that M is correct on Z^j, i.e., $M_0[x,\alpha] = 1$ or $M_1[x,\alpha] = 1$ for all $x \in \mathbf{B}^*$, $\alpha \in Z^j$. We have to find a base $Z^{j'} \subset Z^j$ and a polynomial decision tree N that for given $x \in \mathbf{B}^*$ and $\alpha \in Z^{j'}$, finds an $i \in \{0,1\}$ such that $M_i[x,\alpha] = 1$. Let $j' = j$.

The decision tree N on input $[x,\alpha]$ works as follows. Let $n = \|\alpha\|$. Obviously, $\mathbf{0}_n \in Z^j$, therefore, $M_0[x,\mathbf{0}_n] = 1$ or $M_1[x,\mathbf{0}_n] = 1$. Find first an $i \in \{0,1\}$ such that $M_i[x,\mathbf{0}_n] = 1$ and an accepting computation c of M_i on $[x,\mathbf{0}_n]$. Set $W_0 = Query_{M_i}[c,\mathbf{0}_n]$. Ask '$\alpha(y) =?$' for all $y \in W_0$. If $\alpha(y) = 0$ for all $y \in W_0$, then $M_i[x,\alpha] = 1$. In this case output i and halt. If $\alpha(y) = 1$ for some $y \in W_0$ then let

$$\beta_1(y) = \begin{cases} \alpha(y), & \text{if } y \in W_0; \\ 0, & \text{if } y \in \mathbf{B}^n \setminus W_0. \end{cases}$$

If $\beta_1 \notin Z^j$, then output 0 and halt (in this case $\alpha \notin Z^j$). Otherwise find an $i \in \{0,1\}$ such that $M_i[x,\beta_1] = 1$ and repeat all done before, i.e., find W_1, ask '$\alpha(y) =?$' for all $y \in W_1$ and so on.

After at most $k = [n/j] + 1$ loops we will halt. Indeed, if we have done k loops and have not halt, then we have defined β_1, β_2, ..., β_k such that

$$0 < \#_1\beta_1 < \#_1\beta_2 < \ldots < \#_1\beta_k$$

(hence $\#_1\beta_k \ge k$) and $\beta_k \in Z^j$ (hence $\#_1\beta_k < k$).

The assertion (b$''$) for $\mathcal{M}$ = BPP, $\mathcal{N}$ = P can be proved in the similar way using the technique from the proof of Lemma 4.3.□

Let us present one more application of the universum method consisting in the new proof of a known theorem.

Theorem 4.13 (Hartmanis and Immerman [HI 86]). *There exists an oracle A such that $\mathbf{P}^A \neq \mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A \neq \mathbf{NP}^A$ and the class $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$ has an m-complete language.*

Proof. It is sufficient to construct an oracle A such that $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A \neq \mathbf{P}^A$, $\mathbf{NP}^A \not\subset \mathbf{Co\text{-}NP}^A$ and the class $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$ has an m-complete language. The oracle A will have the form $B \oplus H$, where H is a **PSPACE**-complete set. Thus, we have to construct the oracle B.

As Theorem 3.1 does not work in our case, we present the whole construction of B. Take the universum

$$V = \{A \in \Omega \mid \#_1(A|\mathbf{B}^n) = 1 \text{ for any even } n \text{ and } \#_1(A|\mathbf{B}^n) \leq 1 \text{ for any odd } n\}.$$

The language in $\mathbf{NP}^A \setminus \mathbf{Co\text{-}NP}^A$ will be

$$L_1^B = \{1^n \mid n \text{ is odd and } \exists u \in \mathbf{B}^n \ B(u) = 1\}.$$

The language in $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A \setminus \mathbf{P}^A$ will be

$$L_2^B = \{1^n \mid n \text{ is even and } \exists u \in \mathbf{B}^{n-1} B(1u) = 1\}.$$

Obviously, $L_1^B \in \mathbf{NP}^A$ and $L_2^B \in \mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$ for any $B \in V$ (recall that $A = B \oplus H$). Thus, we have to construct an oracle $B \in V$ such that

1. $L_1^B \notin \mathbf{Co\text{-}NP}^A$;
2. $L_2^B \notin \mathbf{P}^A$;
3. $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$ has a complete language.

To this end let us enumerate all the polynomial-time deterministic and nondeterministic oracle machines and all the pairs of nondeterministic polynomial-time oracle machines. In usual way we can construct a chain

$$\Gamma_0 \supset \Gamma_1 \supset \Gamma_2 \supset \Gamma_3 \supset \ldots$$

of intervals such that any Γ_i intersects with V and the following holds. If $i = 3k$, then kth nondeterministic machine does not accept the language $\{0,1\}^* \setminus L_1^B$ for all $B \in \Gamma_i \cap V$; if $i = 3k+1$, then kth deterministic machine does not recognise the set L_2^B for all $B \in \Gamma_i \cap V$; and if $i = 3k+2$, then either the languages accepted by the nondeterministic machines in

kth pair are complementary for all $B \in \Gamma_i \cap V$ or those languages are not complementary for all $B \in \Gamma_i \cap V$.

Pick any oracle B in $\bigcap_{i=1}^{\infty} \Gamma_i \cap V$. The assertions 1 and 2 are true. It remains to prove that $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$ has a complete language. Denote by N_j the jth nondeterministic polynomial-time Turing machine and by $p_j(|x|)$ a polynomial restricting its running time.

Recall that for $C \in \Omega$, C^n denotes the word of length $2^{n+1} - 1$ encoding C's value on words of length at most n.

Let us note that a pair $\langle N_j, N_k \rangle$ of NP-machines defines a language in $\mathbf{NP}^{B \oplus H} \cap \mathbf{Co\text{-}NP}^{B \oplus H}$ iff $N_j(x, B \oplus H) + N_k(x, B \oplus H) = 1$ for all x. As complete language we take the following language:

$$\begin{aligned} L^B = \{ & 1^j 0 1^k 0 \overline{B^n} \bar{x} 0^{p_j(|x|)+p_k(|x|)} \mid N_j(x, B \oplus H) = 1 \\ & \text{and } N_j(x, C \oplus H) + N_k(x, C \oplus H) = 1 \\ & \text{for all } C \in V \cap \Gamma(B \mid \mathbf{B}^{\leq n}) \}. \end{aligned}$$

Let us prove that L^B is in $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$. To this end let us prove that L^B is in $\mathbf{NP}^A$ (the remaining part $L^B \in \mathbf{Co\text{-}NP}^A$ can be proved entirely similar).

Let us prove that for given oracle B and word w by making polynomial number of queries we can nondeterministically, within polynomial space, accept w iff $w \in L^B$.

Let w be an input word. Decide first whether w has the form $1^j 0 1^k 0 \overline{D^n} \bar{x} 0^{p_j(|x|)+p_k(|x|)}$, for some $D \in V$. Then decide whether $B^n = D^n$ and whether $N_j(x, C \oplus H) + N_k(x, C \oplus H) = 1$ for all $C \in V$ such that $C^n = D^n$, (this can be done within polynomial space since both values $N_j(x, C \oplus H)$ and $N_k(x, C \oplus H)$ depend only on the value of C on words of length at most $p_j(|x|) + p_k(|x|)$, therefore all the necessary information about C can be written within polynomial space). If this is not the case, then reject. Otherwise run $N_j(x, B \oplus H)$ and accept if $N_j(x, B \oplus H) = 1$.

In usual way we can convert our nondeterministic polynomial-space machine into nondeterministic polynomial-time machine with oracle H.

Thus, it remains to prove that L^B is complete in $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$. Let (N_j, N_k) be a pair of nondeterministic polynomial-time oracle machines such that $N_j(x, B \oplus H) + N_k(x, B \oplus H) = 1$ for all x. The construction of the oracle ensures that there exists n such that $N_j(x, C \oplus H) + N_k(x, C \oplus H) = 1$ for all $C \in V \cap \Gamma(B \mid \mathbf{B}^{\leq n})$. Let us fix such an n. The mapping $x \mapsto 1^j 0 1^k 0 \overline{B^n} \bar{x} 0^{p_j(|x|)+p_k(|x|)}$ reduces $L_{N_j^A}$ to L^B. $\square$

Remark 4.1 *In the similar way we could prove all the previous theorems in a stronger form: we could add the assertion that all the involved classes have complete problems.*

5 When the universum method cannot be used

We say that the universum method can be applied to prove that there exists an oracle A such that $\mathcal{K}^A \not\leq \mathcal{L}^A$ and $\mathcal{M}^A \leq \mathcal{N}^A$ if there exists a superuniversum $\mathcal{V}$ such that (a$'$) and (b$'$) are true. In this section we present two theorems that cannot be proven by the universum method.

Theorem 5.1 [Ko 89] *There exists an oracle A such that* $\mathbf{P}^A = \mathbf{NP}^A \neq \mathbf{PSPACE}^A$.

Theorem 5.2 *There exists an oracle A such that* $\mathbf{P}^A \neq \mathbf{R}^A = \mathbf{PSPACE}^A$.

In fact, we prove that the following corollaries of Theorems 5.1 and 5.2 cannot be proven by the universum method.

Corollary 5.3 *There exists an oracle A such that* $\mathbf{NP}^A = \mathbf{Co\text{-}NP}^A \neq \mathbf{PSPACE}^A$

Corollary 5.4 *There exists an oracle A such that* $\mathbf{P}^A \neq \mathbf{PSPACE}^A$ *and* $\mathbf{Co\text{-}NP}^A \subset \mathbf{R}^A$.

Both Theorems 5.1 and 5.2 can be proven by a method that may be called "coding method" because, in those proofs, some difficult-to-compute information is encoded via oracle values, to ensure the truth of positive assertion ($\mathcal{M}^A \leq \mathcal{N}^A$). To prove Theorem 5.1, one needs a lower bound by [H 86, Y 85] on complexity of computation of PARITY function by means of AND,OR-circuits of bounded depth, which has a rather complicated proof. Theorem 5.2 was proved in the paper [R 78] (in fact a less strong asertion that $\mathbf{P} \neq \mathbf{R} = \mathbf{NP}$ under some oracle was proved there but the proof is good also for our case).

Theorem 5.5 *The universum method cannot be applied to prove Corollary* 5.3, *i.e., there exists no superuniversum $\mathcal{V}$ such that* (a$'$) *and* (b$'$) *are true for* $\mathcal{K} = \text{PSPACE}$, $\mathcal{L} = \text{NP}$, *and* $\mathcal{M} = \text{Co-NP}$, $\mathcal{N} = \text{NP}$.

Proof. Let V be a universum. Say that an interval Γ *n-isolates an oracle A in V* if $A \in \Gamma$ and $A|\mathbf{B}^n = B|\mathbf{B}^n$ for any $B \in V \cap \Gamma$. A set $W \subset \mathbf{B}^*$ *n-isolates an oracle A in V* if the interval $\Gamma(A|W)$ n-isolates A in V. Define the size of an interval $\Gamma = \Gamma(\varphi)$ to be the size of $\mathrm{Dom}(\varphi)$. Say that V is *thin* if there exists a polynomial $p(n)$ such that for all $A \in V$ and all $n \in \mathbf{N}$, there exists a set $W \subset \mathbf{B}^*$ of size $p(n)$ that n-isolates A in V. Consider two cases.

First case: there exists a universum V in $\mathcal{V}$ that is thin. Let $p(n)$ be the corresponding polynomial. Let us prove that (a$'$) is false in this case. Indeed, let K be a n.u.PSPACE-machine. Let us construct a n.u.NP-machine L such that $K^V = L^V$. Machine L on input $\langle x, A\rangle$ works as follows. Let the length of queries of K on input x be bounded by the polynomial $q(|x|)$. For every $i \le q(|x|)$ guess a set $W_i \subset \mathbf{B}^*$ such that $\mathit{size}\,(W_i) \le p(i)$. Ask '$A(y) =?$' for all y in W_i. If there exists no $B \in V$ such that the interval $\Gamma(A|W_i)$ i-isolates B in V for all $i \le q(|x|)$, then reject. Otherwise, pick such B. Note that if A is in V, then $A|\mathbf{B}^{\le q(|x|)} = B|\mathbf{B}^{\le q(|x|)}$, and therefore $K(x, A) = K(x, B)$. Then compute $K(x, B)$ and accept if $K(x, B) = 1$.

The total number of queries made to A is $\sum_{i=0}^{q(|x|)} p(i) = \mathrm{poly}(|x|)$. The maximal length of query is $\max_{i \le q(|x|)} p(i) = \mathrm{poly}(|x|)$. Thus, $L \in$ n.u.NP.

Second case: all the universums in $\mathcal{V}$ are not thin. We claim that in this case (b$'$) is false for $\mathcal{M} =$ Co-NP, $\mathcal{N} =$ NP. Let V_0, V_1, V_2, ..., V_i, ... be an enumeration of universums in $\mathcal{V}$. Given an oracle A, denote by $m^i_A(n)$ the minimal size of set n-isolating A in V_i. For all $i \in \mathbf{N}$, fix a sequence $\{B^{in}\}$, $n \in \mathbf{N}$ of oracles such that $B^{in} \in V_i$ and such that for any fixed i, the function $m^i_{B^{in}}(n)$ grows superpolynomially, i. e., for any polynomial p there exists an n such that $m^i_{B^{in}}(n) > p(n)$. Obviously, the set of natural numbers can be partitioned into subsets Q_0, Q_1, Q_2, ..., Q_i, ... such for any fixed $i \in \mathbf{N}$, the function $m^i_{B^{in}}(n)$ grows superpolynomially when n ranges Q_i. Obviously there exists a description $M \in$ n.u.Co-NP such that

$$M(1^n, A) = \begin{cases} 1, & \text{if } \forall y \in \mathbf{B}^n A(y) = B^{in}(y), \text{ where } i \\ & \text{is the number such that } n \in Q_i; \\ 0, & \text{otherwise.} \end{cases}$$

Let us prove that there exist no $N \in$ n.u.NP and no $i \in \mathbf{N}$ such that $M^{V_i} = N^{V_i}$. Suppose the contrary: such N and such i exist. Denote by $p(n)$ the polynomial bounding the size of $\mathit{Query}_N(1^n, A)$. Take an $n \in Q_i$ such that $m^i_{B^{in}}(n) > p(n)$. Then for all $A \in V_i$,

$$A|\mathbf{B}^n = B^{in}|\mathbf{B}^n \Leftrightarrow M(1^n, A) = 1 \Leftrightarrow N(1^n, A) = 1.$$

In particular, $N(1^n, B^{in}) = 1$. Pick an accepting computation c of N on input $\langle 1^n, B^{in}\rangle$ and denote $W = Query_N(c, B^{in})$. Then $size\,(W) \leq p(n)$ and $N(1^n, A) = 1$ for all $A \in \Gamma(B^{in}|W)$. Therefore, $A|\mathbf{B}^n = B^{in}|\mathbf{B}^n$ for all $A \in V_i \cap \Gamma(B^{in}|W)$ that is, W n-isolates B^{in} in V^i. The obtained contradiction proves the theorem.□

Theorem 5.6 *Corollary* 5.4 *cannot be proven by the universum method, that is, there exists no superuniversum* $\mathcal{V}$ *such that* (a′) *and* (b′) *hold for* $\mathcal{K} = \mathrm{PSPACE}$, $\mathcal{L} = \mathrm{P}$ *and* $\mathcal{M} = \text{Co-NP}$, $\mathcal{N} = \mathrm{R}$.

Proof. Say that a universum V is *identifiable* if there exists a polynomial decision tree P such that the set $Query_P(1^n, A)$ n-isolates A in V for all $n \in \mathbf{N}$ and all $A \in V$. Say that a universum V is *randomly identifiable* if there exists a polynomial decision tree P and a polynomial q such that

$$\mathrm{Prob}_{r\in\mathbf{B}^{q(n)}}\,[Query_P(\bar{r}1^n, A)\ n\text{-isolates } A \text{ in } V] > \frac{1}{2};$$

for all $n \in \mathbf{N}$, $A \in V$ (the probability is with respect to the uniform distribution over $r \in \mathbf{B}^{q(n)}$). Obviously

$$\begin{aligned}(V \text{ is identifiable}) &\Rightarrow (V \text{ is randomly identifiable})\\ &\Rightarrow (V \text{ is thin}).\end{aligned}$$

Lemma 5.1 *Any randomly identifiable universum is identifiable.*

Proof. Let V be randomly identifiable. For $n \in \mathbf{N}$ denote by Z_n the set $\{B|\mathbf{B}^{\leq n} \mid B \in V\}$. Let us prove that $|Z_n| \leq 2^{\mathrm{poly}(n)}$. As V is thin, there exists a polynomial $p(n)$ such that for all $n \in \mathbf{N}$ and all $B \in V$ there exists a set $W \subset \mathbf{B}^*$ of size $p(n)$ such that $C|\mathbf{B}^{\leq n} = B|\mathbf{B}^{\leq n}$ for any $C \in V \cap \Gamma(B|W)$. Thus, $|Z_n|$ is not greater than the cardinality of the set

$$\{B|W \mid W \subset \mathbf{B}^*,\ size\,(W) \leq p(n),\ B \in \Omega\}.$$

Evidently the number of sets of size at most $p(n)$ does not exceed $(2^{p(n)+1})^{p(n)}$. Thus, $|Z_n| \leq (2^{p(n)+1})^{p(n)} 2^{p(n)} = 2^{\mathrm{poly}(n)}$.

Let P be the polynomial decision tree and q be the polynomial such that

$$\begin{aligned}&\mathrm{Prob}_{r\in\mathbf{B}^{q(n)}}\,[Query_P(\bar{r}1^n, A)\ n\text{-isolates } A \text{ in } V]\\ &\qquad > \tfrac{1}{2}\end{aligned} \tag{12}$$

for all $n \in \mathbf{N}$, $A \in V$. Denote by $s(n)$ the polynomial such that size $Query_P(\bar{r}1^n, A) \leq s(n)$ for all $r \in \mathbf{B}^{q(n)}$. Obviously, for all n and all $r \in \mathbf{B}^{q(n)}$, $Query_P(\bar{r}1^n, A)$ depends only on $A|\mathbf{B}^{\leq s(n)}$. Let $t(n)$ be a polynomial such that $|Z_{s(n)}| \leq 2^{t(n)}$. Let us prove that for any n there exist $r_1, \ldots, r_{t(n)} \in \mathbf{B}^{q(n)}$ such that for all $A \in V$ at least one of the sets $Query_P(\bar{r}_j 1^n, A)$, $j = 1, 2, \ldots, t(n)$, n-isolates A in V.

Recall that for any partial function $\alpha\colon \mathbf{B}^* \to \mathbf{B}$, $\hat{\alpha}$ denotes the oracle

$$\hat{\alpha}(z) = \begin{cases} \alpha(z), & \text{if } z \in \mathrm{Dom}(\alpha); \\ 0, & \text{if } z \in \mathbf{B}^* \setminus \mathrm{Dom}(\alpha). \end{cases}$$

Obviously, for any A, n and $r \in \mathbf{B}^{q(n)}$,

$$\begin{gathered} Query_P(\bar{r}1^n, A) \text{ } n\text{-isolates } A \text{ in } V \Leftrightarrow \\ Query_P(\bar{r}1^n, A\widehat{|B^{s(n)}}) \text{ } n\text{-isolates } A\widehat{|B^{s(n)}} \text{ in } V. \end{gathered} \tag{13}$$

Therefore the assertion (12) implies that

$$\mathrm{Prob}_{r \in \mathbf{B}^{q(n)}} [Query_P(\bar{r}1^n, \hat{\alpha}) \text{ } n\text{-isolates } \hat{\alpha} \text{ in } V] > 1/2$$

for any $\alpha \in Z_{s(n)}$. Take random uniformly distributed $\alpha \in Z_{s(n)}$. Then

$$\begin{gathered} \mathrm{Prob}_{r \in \mathbf{B}^{q(n)}, \alpha \in Z_{s(n)}} [Query_P(\bar{r}1^n, \hat{\alpha}) \text{ } n\text{-isolates } \hat{\alpha} \text{ in } V] \\ > 1/2. \end{gathered}$$

Therefore, there exists $r_1 \in \mathbf{B}^{q(n)}$ such that

$$\mathrm{Prob}_{\alpha \in Z_{s(n)}} [Query_P(\bar{r}_1 1^n, \hat{\alpha}) \text{ } n\text{-isolates } \hat{\alpha} \text{ in } V] > 1/2.$$

Let

$$\begin{gathered} Z' = \{\alpha \in Z_{s(n)} \mid Query_P(\bar{r}_1 1^n, \hat{\alpha}) \\ \text{does not } n\text{-isolate } \hat{\alpha} \text{ in } V\}. \end{gathered}$$

Reasoning in similar way we can prove that there exists $r_2 \in \mathbf{B}^{q(n)}$ such that

$$\mathrm{Prob}_{\alpha \in Z'} [Query_P(\bar{r}_2 1^n, \hat{\alpha}) \text{ } n\text{-isolates } \hat{\alpha} \text{ in } V] > 1/2.$$

Let

$$\begin{gathered} Z'' = \{\alpha \in Z' \mid Query_P(\bar{r}_2 1^n, \hat{\alpha}) \\ \text{does not } n\text{-isolate } \hat{\alpha} \text{ in } V\} \end{gathered}$$

and so on. So we define the words r_1, r_2, ..., r_i, ... and the sets Z', Z'', ..., $Z^{(i)}$, ... Evidently,

$$|Z^{(i+1)}| < (1/2)|Z^{(i)}|$$

for all i, therefore for $i = t(n)$ we get $Z^{(i+1)} = \emptyset$. Thus for any $\alpha \in Z_{s(n)}$ there exists an $i \leq t(n)$ such that $W_P(\bar{r}_i 1^n, \hat{\alpha})$ n-isolates $\hat{\alpha}$ in V. By (14), this means that for any $A \in V$ there exists $i \leq t(n)$ such that $W_P(\bar{r}_i 1^n, A)$ n-isolates A in V.

The decision tree that for given $\langle 1^n, A\rangle$ ($A \in V$) n-isolates A in V works as follows. It simply executes P on inputs $\langle \bar{r}_1 1^n, A\rangle$, $\langle \bar{r}_2 1^n, A\rangle$, ..., $\langle \bar{r}_{t(n)} 1^n, A\rangle$.□

Let us continue the proof of the theorem. Consider two cases.

First case: there exists a randomly identifiable universum $V \in \mathcal{V}$. Then by above lemma the universum V is identifiable. Therefore, for any $K \in$ n.u.PSPACE there exists a polynomial decision tree L such that $K^V = L^V$ (first identify oracle A and then find $K(x, A)$). Therefore, (a′) is false for $\mathcal{K} =$ PSPACE, $\mathcal{L} =$ P.

Second case: all universums $V \in \mathcal{V}$ are not randomly identifiable. Let us prove that (b′) is false for $\mathcal{M} =$ Co-NP, $\mathcal{N} =$ R.

Let V_0, V_1, ..., V_i, ... be an enumeration of universums in $\mathcal{V}$. Denote by $m^i_B(n)$ the least $s \in \mathbf{N}$ such that there exists a decision tree P such that $\mathrm{Prob}_{r\in\mathbf{B}^s}[Query_P(\bar{r}1^n, B)$ n-isolates B in $V_i] > 1/2$, and $size\ Query_P(\bar{r}1^n, B) \leq s$ for all $r \in \mathbf{B}^s$.

Then we know that for any i there exists a sequence $\{B^{in}\}$, $n \in \mathbf{N}$, of oracles in V_i such that the function $n \mapsto m^i_{B^{in}}(n)$ grows superpolynomially. Obviously, the set $\mathbf{N}$ can partitioned into subsets Q_0, Q_1, ..., Q_i, ... such that for each $i \in \mathbf{N}$ the function $m^i_{B^{in}}(n)$ grows superpolynomially when n ranges Q_i. Obviously, there exists a n.u.Co-NP-description M such that

$$M(1^n, A) = 1 \Leftrightarrow A|\mathbf{B}^n = B^{in}|\mathbf{B}^n.$$

for any $i \in \mathbf{N}$ and any $n \in Q_i$. Suppose that there exist a description N in n.u.R and $i \in \mathbf{N}$ such that $M^{V_i} = N^{V_i}$.

Let $q(n)$ be the length of random strings used by N on inputs of the form $\langle 1^n, A\rangle$ ($A \in \Omega$). For $r \in \mathbf{B}^{q(n)}$ denote by $N(1^n, r, A)$ the output of N on input $\langle 1^n, A\rangle$ and random input r, and denote by $Query_N(1^n, r, A)$ the set of queries to A made by N during the work on the input $\langle 1^n, A\rangle$ and the random input r. Then

$$M(1^n, A) = 0 \Rightarrow$$
$$\mathrm{Prob}_{r\in\mathbf{B}^{q(n)}}[N(1^n, r, A) = 1] = 0, \qquad (14)$$

$$M(1^n, A) = 1 \Rightarrow \mathrm{Prob}_{r \in \mathbf{B}^{q(n)}} [N(1^n, r, A) = 1] > 1/2$$

for any $A \in V_i$. In particular,

$$\mathrm{Prob}_{r \in \mathbf{B}^{q(n)}} \left[N(1^n, r, B^{ni}) = 1 \right] > 1/2$$

for all $n \in Q_i$. Assertion (14) implies that if $A \in V_i$ and $A|\mathbf{B}^n \neq B^{ni}|\mathbf{B}^n$, then $N(1^n, r, A) = 0$ for all $r \in \mathbf{B}^{q(n)}$.

Thus, the set $Query_N(1^n, r, B^{ni})$ n-isolates B^{ni} in V_i for any $r \in \mathbf{B}^{q(n)}$ such that $N(1^n, r, B^{ni}) = 1$. Therefore $m^i_{B^{in}}(n)$ grows polynomially when n ranges Q_i. The obtained contradiction finishes the proof.□

References

[BGS 75] T. Baker, J. Gill and R. Solovay. "Relativization of P=?NP Question", *SIAM Journal on Computing*, 1975, pp. 431–442.

[GS 88] J. Grollman, A. L. Selman. "Complexity measures for public-key cryptosystems", *SIAM J. on Computing,* 1988, Vol. 17, No. 2, pp. 309–335.

[H 86] J. Hastad. "Almost optimal lower bounds for small depth circuits", in: S. Micali, ed., *Advances in Computer Research,* Vol. 5: Randomness and Computation (JAI Press, Greenwich, CT); see also *Computational Limitations for Small Depth Circuits* (MIT Press, Cambridge, MA, 1986).

[HI 86] J. Hartmanis, N. Immerman. "On complete problems for **NP** ∩ **Co-NP**", *Proc. of Intern. Colloq. on Automata, Languages and Programming* 1985, pp. 250–259. Springer-Verlag *Lecture Notes in Computer Science,* Vol. 194, 1985.

[Ko 89] Ker-I Ko. "Relativized polynomial-time hierarchies having exactly k levels", *SIAM Journal on Comput.*, 1989, Vol. 18, No. 2, pp. 392–408.

[R 78] C. Rackoff. "Relativized Questions Involving Probabilistic Algorithms", *Proc. of 10th Annual ACM Symp. on Theory of Comp.,* 1978, pp. 338–342. *Journal of ACM* **29** (1982), 261–268.

[S 83] M. Sipser. "A complexity Theoretic Approach for Randomness", *15th Annual ACM Symp. on Theory of Computing*, 1983, pp. 330–335.

[Y 85] A. C. Yao. "Separating the polynomial time hierarchy by oracles", *Proc. 26th Ann. IEEE Symp. on Foundations of Computer Science*, 1985, pp. 1–10.