Relationships between NP-sets, Co-NP-sets, and P-sets relative to random oracles

Nikolai K.Vereshchagin
The Institute of New Technologies
Kirovogradskaja 11, Moscow 113587, Russia
e-mail: amuchnik@globlab.msk.su

Abstract

In the present paper we prove that relative to random oracle A (with respect to the uniform measure) the following three assertions hold: (1) there is a pair of disjoint $\mathbf{NP}^A$-sets which are separable by no $\mathbf{P}^A$-set, (2) there is a pair of disjoint $\mathbf{Co\text{-}NP}^A$-sets which are separable by no $\mathbf{P}^A$-set and (3) there is an infinite $\mathbf{Co\text{-}NP}^A$-set having no infinite $\mathbf{NP}^A$-subset

1 Introduction

Many important problems in Complexity theory remain open. The most known one is whether the classes **P** and **NP** are equal. It is also unknown if the class **NP** coincides with the class **Co-NP** and if $\mathbf{NP} \cap \mathbf{Co\text{-}NP} = \mathbf{P}$.

In the paper [1] it was shown that all these problems have no relativizable solutions. More exactly, oracles A and B were constructed such that $\mathbf{P}^A = \mathbf{NP}^A$ (and, therefore, $\mathbf{P}^A = \mathbf{NP}^A = \mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$) and $\mathbf{NP}^B \neq \mathbf{Co\text{-}NP}^B$ (and, therefore, $\mathbf{P}^B \neq \mathbf{Co\text{-}NP}^B$). Using the same technique one can construct an oracle C for which $\mathbf{NP}^C \cap \mathbf{Co\text{-}NP}^C \neq \mathbf{P}^C$.

As the relationship between the classes $\mathbf{Co\text{-}NP}^A$, $\mathbf{NP}^A$ and $\mathbf{P}^A$ depends on the oracle A, it's natural to ask what happens for "typical" oracle A. A possible refinement of the notion of typicalness is randomness with respect to the uniform measure. In the present paper we just study the relationship between the classes $\mathbf{NP}^A$, $\mathbf{Co\text{-}NP}^A$ and $\mathbf{P}^A$ for oracle A random with respect to the uniform measure. More exactly, we say that the assertion $S(A)$ holds for random A, or for almost all A, if the uniform measure of the set $\{A \mid S(A)\}$ is equal to 1. All properties $S(A)$ of oracle A present in the introduction satisfy two following conditions: the set $\{A \mid S(A)\}$ is measurable and $S(A)$ is stable with respect to any changing the value of A on a finite set of arguments. Due to 0-1-law of A.N.Kolmogorov, for such properties $S(A)$ either $S(A)$ holds for random A, or $\neg S(A)$ holds for random A.

The study of Complexity theory relative to random oracle began in [2], where it was proved that $\mathbf{P}^A \neq \mathbf{NP}^A \neq \mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A$ for random A. In [2] it was proved also that for random A there is an infinite $\mathbf{NP}^A$-set having no infinite $\mathbf{P}^A$-subsets. Let us look at these results from the point of view of analogy between Recursion theory and Complexity theory. According to this analogy **P**-sets correspond to decidable sets, **NP**-sets correspond to recursively enumerable sets and **Co-NP**-sets correspond to complements of recursively enumerable sets. More exactly, we will consider the complexity theory relativized with a random oracle. Thus, in our case decidable sets correspond to $\mathbf{P}^A$-sets, recursively enumerable sets correspond to $\mathbf{NP}^A$-sets and complements of recursively enumerable sets correspond to $\mathbf{Co\text{-}NP}^A$-sets, where A is a random oracle. As we have said, in Complexity theory the analogue of the theorem on the existence of recursively enumerable undecidable set is true, the analogue of the theorem on the existence of recursively enumerable set whose complement is not recursively enumerable is true and the analogue of the theorem that every infinite recursively enumerable set has an infinite decidable subset is false.

In the present paper we consider the analogues of three other theorems of Recursion theory: the theorem on the existence of recursively enumerable inseparable sets, the theorem on separability of sets having recursively enumerable complements and the theorem on the existence of a simple set (recursively enumerable set whose complement is infinite but has no infinite recursively enumerable subset). Namely, we prove that the analogues of the first theorem and of the third theorem are true (theorems 1 and 3) and the analogue of the second theorem is false (theorem 2). Theorems 1 and 2 with a sketch of proof were published in author's paper [3]. It remains an open problem

at present whether the analogue of Post's theorem (if both a set and its complement are recursively enumerable, then the set is decidable) is true, i.e., it is unknown whether $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A = \mathbf{P}^A$ for random A. One can show that if $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A = \mathbf{P}^A$ for random A, then $\mathbf{AM} \cap \mathbf{Co\text{-}AM} = \mathbf{BPP}$, in particular, the problem of graph isomorphism is in $\mathbf{BPP}$. Thus, it cannot be hoped to prove that $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A = \mathbf{P}^A$ for random A. No absolute consequence of the assertion "$\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A \neq \mathbf{P}^A$ for random A" is known; so one may hope to prove that $\mathbf{NP}^A \cap \mathbf{Co\text{-}NP}^A \neq \mathbf{P}^A$ for random A.

2 Definitions

We will consider subsets of the set $\mathbf{B}^*$ of all the words over the binary alphabet $\mathbf{B} = \{0,1\}$. We will call them *languages*. An *oracle* is any function from the set $\mathbf{B}^*$ into the set $\mathbf{B}$.

Let A be an oracle. The class $\mathbf{P}^A$ consists of all languages L such that there is a deterministic polynomial-time oracle Turing machine M such that $x \in L \Leftrightarrow M^A(x) = 1$, where $M^A(x)$ stands for the output of M on input x with oracle A. The class $\mathbf{NP}^A$ consists of all languages L such that there are a deterministic polynomial-time oracle Turing machine M and a polynomial p such that

$$x \in L \Leftrightarrow \exists y \in \mathbf{B}^* \ \big(|y| = p(|x|) \ \&\ M^A(x,y) = 1\big),$$

where $|u|$ denotes the length of word u. The pair $N = \langle M, p\rangle$ will be called *nondeterministic* machine and we set

$$N^A(x) = \begin{cases} 1, & \text{if } \exists y \in \mathbf{B}^* \ (|y| = p(|x|) \\ & M^A(x,y) = 1); \\ 0, & \text{otherwise.} \end{cases}$$

Denote by L_{N^A} the language $\{x \in \mathbf{B}^* \mid N^A(x) = 1\}$.

Let L_1, L_2 and L be languages. Say that L *separates* L_1 from L_2 if $L_1 \subset L$ and $L_2 \subset \mathbf{B}^* \setminus L$. Let $\mathcal{C}$ and $\mathcal{C}'$ are two families of languages. Say that $\mathcal{C}$-languages are $\mathcal{C}'$-separable if for every two disjoint languages L_1 and L_2 from $\mathcal{C}$ there is a language L from $\mathcal{C}'$ which separates L_1 from L_2. Let $S(A)$ be a property of an oracle A. Say that $S(A)$ holds for random A if the uniform measure of the set $\{A \mid S(A)\}$ is equal to 1.

3 Results

Theorem 1. *$\mathbf{NP}^A$-languages are not $\mathbf{P}^A$-separable for random A.*

Proof. Define the sequence $\{t_i\}$ of integers by induction: $t_0 = 1$, $t_{i+1} = 2^{t_i}$. Let i be a natural number and let w be a binary word of length $2t_i - \log_2 t_i$. Consider the set

$$B_w = \{wv \mid v \in \mathbf{B}^*, |v| = \log_2 t_i\}.$$

Evidently, each B_w consists of t_i words (of length $2t_i$). Arrange B_w's according to the lexicographical order on w's.

Let us fix a sequence $\{s_i\}$ of natural numbers (the value of s_i will be defined later). Call the first $2s_i$ of B_w's the *i-blocks* (s_i will satisfy the inequality $2s_i \leq 2^{2t_i - \log_2 t_i}$). Call the first s_i i-blocks the *$i,0$-blocks* and call the remaining s_i blocks the *$i,1$-blocks*. Say that an oracle A is *identically zero in block B* if $\forall u \in B\ A(u) = 0$.

For every oracle A consider the $\mathbf{NP}^A$-languages

$$L_0^A = \{1^{t_i} \mid \ i \in \mathbf{N} \text{ and } A \text{ is identically zero, in some } i,0\text{−block}\}$$

$$L_1^A = \{1^{t_i} \mid \ i \in \mathbf{N} \text{ and } A \text{ is identically zero in some } i,1\text{−block}\}.$$

Now we will define the sequence $\{s_i\}$. We wish the probability of event "$1^{t_i} \in L_0^A$" to be equal to about $1/i$. Let us calculate this probability. For every i-block B the probability of event "A is identically zero in B" is equal to 2^{-t_i}. Therefore

$$\text{Prob}\left[1^{t_i} \in L_0^A\right] = \text{Prob}\left[1^{t_i} \in L_1^A\right] = 1 - (1 - 2^{-t_i})^{s_i}.$$

Set $s_i = [2^{t_i}/i]$. Evidently, $1 - (1 - 2^{-t_i})^{s_i} = 1 - e^{-2^{-t_i} s_i (1 + o(1))}$ when $i \to \infty$. We have $2^{-t_i} s_i = 2^{-t_i}[2^{t_i}/i] = \frac{1}{i}(1 + o(1))$. Therefore $1 - (1 - 2^{-t_i})^{s_i} = 1 - e^{-\frac{1}{i}(1+o(1))} = 1 - (1 - 1/i + o(1/i)) = 1/i + o(1/i)$. Let us prove that the set $L_0^A \cap L_1^A$ is finite with probability 1. The events $1^{t_i} \in L_0^A$ and $1^{t_i} \in L_1^A$ for $i \in \mathbf{N}$ are mutually independent, therefore, for all $i \in \mathbf{N}$

$$\text{Prob}\big[1^{t_i} \in L_0^A \cap L_1^A\big] = (1/i + o(1/i))^2 = 1/i^2 + o(1/i^2).$$

The series $\sum(1/i^2 + o(1/i^2))$ converges. Due to Borel–Cantelli lemma with probability 1 there are only finitely many i such that $1^{t_i} \in L_0^A \cap L_1^A$.

Set $C^A = L_1^A \setminus L_0^A$. With probability 1, $C^A \in \mathbf{NP}^A$ (as C^A differs from the language $L_1^A \in \mathbf{NP}^A$

only on finite number of words for almost all A). Besides that, C^A and L_0^A are disjoint for all A. Thus, all we have to prove is that C^A and L_0^A are not $\mathbf{P}^A$-separable for almost all A. To this end it is sufficient to prove that for every deterministic polynomial-time oracle machine M the probability of event

$$\exists x \in \mathbf{B}^* \ \big(M^A(x) = 1 \ \& \ x \in L_0^A \\ \text{or } M^A(x) = 0 \ \& \ x \in C^A\big)$$

is equal to 1. Let us fix a deterministic polynomial-time oracle machine M. It is sufficient to prove that for almost all A there are infinitely many i such that

$$M^A(1^{t_i}) = 1 \ \& \ 1^{t_i} \in L_0^A \text{ or } M^A(1^{t_i}) = 0 \ \& \ 1^{t_i} \in L_1^A.$$

Denote the displayed event by $P_i(A)$. Note that the events $P_i(A)$ for $i \in \mathbf{N}$ can be mutually dependent.

We claim that if for all $k \in \mathbf{N}$ the series

$$\sum_{i=k+1}^{\infty} \text{Prob}\,[P_i(A) \mid \neg P_{i-1}(A) \ \& \ \neg P_{i-2}(A) \ \& \ \cdots \\ \& \ \neg P_{k+1}(A) \neg P_k(A)] \quad (1)$$

diverges, then for almost all A there are infinitely many i such that $P_i(A)$ holds. Indeed, assume that for all k the series (1) diverges. Then for all $k \in \mathbf{N}$

$$\text{Prob}\,[\exists i \geq k \ P_i(A)] = 1 - \text{Prob}\,[\forall i \geq k \ \neg P_i(A)] = \\ 1 - \text{Prob}\,[\neg P_k(A)] \times \\ \times \prod_{i=k+1}^{\infty} \text{Prob}\,[\neg P_i(A) \mid \neg P_{i-1}(A) \& \cdots \& \neg P_k(A)] = \\ 1 - \text{Prob}\,[\neg P_k(A)] \times \\ \times \prod_{i=k+1}^{\infty} \big(1 - \text{Prob}\,[P_i(A) \mid \neg P_{i-1}(A) \& \cdots \& \neg P_k(A)]\big).$$

As (1) diverges, the last infinite product is equal to 0, therefore for all k, Prob $[\exists i \geq k \ P_i(A)] = 1$. Hence Prob $[\forall k \ \exists i \geq k \ P_i(A)] = 1$, as intersection of any countable family of sets of measure 1 has measure 1.

To prove that the series (1) diverges we will prove that for all sufficiently large i,

$$\text{Prob}\,[P_i(A) \mid \neg P_{i-1}(A) \& \cdots \& \neg P_k(A)] > 1/2i.$$

Denote by D_i the set of all binary words of length less than $2t_i$ and by F_i the set of all functions from D_i into $\mathbf{B}$. Denote by $f|S$ the restriction of function f on the set S.

We will use without reference the following simple lemma.

Lemma. *Let $\mathcal{A}$ and $\mathcal{B}$ be sets of oracles and let a family $\{\mathcal{B}_1, \ldots, \mathcal{B}_m\}$ of sets is a partition of $\mathcal{B}$, that is, $\mathcal{B}_1, \ldots, \mathcal{B}_m$ are pairwise disjoint and $\mathcal{B}_1 \cup \cdots \cup \mathcal{B}_m = \mathcal{B}$. Assume that* Prob $[A \in \mathcal{A} \mid A \in \mathcal{B}_i] > d$ *for all $i \leq m$. Then* Prob $[A \in \mathcal{A} \mid A \in \mathcal{B}] > d$.

Proof. Obviously.

Let us continue the proof of the theorem. For all j the event $P_j(A)$ depends only on the value of A on the words of length bounded by a polynomial of t_j (because M on input 1^{t_j} can put to the oracle questions of the length bounded by a polynomial of t_j and the event $1^{t_j} \in L_0^A$ depends only on the value of A on on words of length $2t_j$). As $t_i = 2^{t_{i-1}}$, for sufficiently large i the event $\neg P_{i-1}(A) \& \cdots \& \neg P_k(A)$ depends only on $A|D_i$. Therefore, it is sufficient to prove that for all $f \in F_i$ the conditional probability Prob $[P_i(A) \mid A|D_i = f]$ is greater than $1/2i$ for large enough i. Let us fix an $i \in \mathbf{N}$ and an $f \in F_i$. Let us restrict ourselves with oracles A such that $A|D_i = f$.

Let A be an oracle. Run M with oracle A on input 1^{t_i}. Let l queries be made in this computation, the k-th query being "$A(u_k) =?$", where $k \leq l$. Delete from the sequence $u_1, \ldots, u_l$ all the words of length less than $2t_i$. Denote the resulting sequence by $w_1, \ldots, w_j$. Let us call the sequence of pairs $\langle w_1, A(w_1)\rangle, \ldots, \langle w_j, A(w_j)\rangle$ the *computational protocol on A* and denote it by $C(A)$. Denote by Π the set of all the computational protocols, i.e.

$$\Pi = \{\text{computational protocol on } A \mid A|D_i = f\}. \quad (2)$$

Let $Z = (\langle w_1, b_1\rangle, \ldots, \langle w_j, b_j\rangle)$ be a protocol from Π (where $w_1, \ldots, w_j \in \mathbf{B}^*, b_1, \ldots, b_j \in \mathbf{B}$). Call an oracle A *consistent with* Z if $A(w_1) = b_1, \ldots, A(w_j) = b_j$. Obviously Z is computational protocol on A iff A is consistent with Z. Consequently, the family of sets $\big\{ \{A \mid A|D_i = f \text{ and } A \text{ is consistent with } Z\} \ \big| \ Z \in \Pi\big\}$ is a partition of the set $\{A \mid A|D_i = f\}$. Thus, it

is sufficient to prove that for every $Z \in \Pi$ the inequality

$$\text{Prob}\,[P_i(A) \mid A \text{ is consistent with } Z, \\ A|D_i = f] > 1/2i \qquad (3)$$

holds.

Let us fix a $Z \in \Pi$ and prove (3). Obviously, if A' and A'' are consistent with Z, then $M^{A'}(1^{t_i}) = M^{A''}(1^{t_i})$. Without loss of generality we may assume that $M^A(1^{t_i}) = 1$ if A is consistent with Z. Then

$$\text{Prob}\,[P_i(A) \mid A \text{ is consistent with } Z,\ A|D_i = f] = \\ \text{Prob}\left[1^{t_i} \in L_0^A \mid A \text{ is consistent with } Z,\ A|D_i = f\right] = \\ \text{Prob}\left[1^{t_i} \in L_0^A \mid A \text{ is consistent with } Z\right]$$

.

Let Z consist of j pairs. Then

$$\text{Prob}\left[1^{t_i} \in L_0^A \mid A \text{ is consistent with } Z\right] \geq \\ 1 - (1 - 2^{-t_i})^{s_i - j}.$$

(Recall that $1^{t_i} \in L_0^A$ means that A is identically zero in some $i,0$-block and that the number of $i,0$-blocks is s_i). As $j \leq \text{poly}(t_i)$ and $s_i = [2^{t_i}/i] \geq [2^{t_i}/t_i]$, we have

$$1 - (1 - 2^{-t_i})^{s_i - j} = \frac{1}{i}(1 + o(1)),$$

as $i \to \infty$. Thus for sufficiently large i we have

$$\text{Prob}\,[P_i(A) \mid A \text{ is consistent} \\ \text{with } Z,\ A|D_i = f] > 1/2i.$$

Theorem 2. **Co-NP**^{A}*-languages are not* $\mathbf{P}^A$*-separable for random* A

Proof. We will use the notions and notation from previous proof with the following changes. Now we set $s_i = [c2^{t_i}\log_2 i]$, where c is a rational constant being defined later. Set

$$L_0^A = \{1^{t_i} \mid i \in \mathbf{N} \text{ and } A \text{ is identically zero} \\ \text{in no } i,0-\text{block}\},$$
$$L_1^A = \{1^{t_i} \mid i \in \mathbf{N} \text{ and } A \text{ is identically zero} \\ \text{in no } i,1-\text{block}\}.$$

Evidently, s_i can be computed in time $\text{poly}(t_i)$, therefore $L_0^A \in \textbf{Co-NP}^A$ and $L_1^A \in \textbf{Co-NP}^A$. Clearly,

$$\text{Prob}\left[1^{t_i} \in L_0^A\right] = \text{Prob}\left[1^{t_i} \in L_1^A\right] = (1 - 2^{-t_i})^{s_i} = \\ e^{-2^{-t_i}s_i(1+o(1))} = e^{-c\log_2 i(1+o(1))} = i^{-c\log_2 e(1+o(1))}.$$

Take c such that $5/8 < c\log_2 e < 7/8$. Then

$$\text{Prob}\left[1^{t_i} \in L_0^A\right] = \text{Prob}\left[1^{t_i} \in L_1^A\right] < i^{-5/8}$$

for sufficiently large i. Therefore, $\text{Prob}\left[1^{t_i} \in L_0^A \cap L_1^A\right] < i^{-5/4}$ for sufficiently large i. As the series $\sum i^{-5/4}$ converges, the set $L_0^A \cap L_1^A$ is finite for almost all A.

Just as in the previous proof set $C^A = L_1^A \setminus L_0^A$. We have to prove that C^A and L_0^A are not $\mathbf{P}^A$-separable for almost all A. To this end it is sufficient to prove that for every deterministic polynomial-time oracle machine M the probability of event

$$\exists x \in \mathbf{B}^* \ \big(M^A(x) = 1 \ \&\ x \in L_0^A \text{ or} \\ M^A(x) = 0 \ \&\ x \in C^A\big)$$

is equal to 1. Let us fix a deterministic polynomial-time oracle machine M. It is sufficient to prove that for almost all A there are infinitely many i such that

$$M^A(1^{t_i}) = 1 \ \&\ 1^{t_i} \in L_0^A \text{ or } M^A(1^{t_i}) = 0 \ \&\ 1^{t_i} \in L_1^A.$$

Denote the displayed event by $P_i(A)$.

It suffices to prove that for all $k \in \mathbf{N}$ the series

$$\sum_{i=k+1}^{\infty} \text{Prob}\,[P_i(A) \mid \neg P_{i-1}(A) \ \&\ \neg P_{i-2}(A) \ \& \\ \cdots \ \&\ \neg P_{k+1}(A)\neg P_k(A)] \qquad (4)$$

diverges. To prove that the series (4) diverges we will prove that

$$\text{Prob}\,[P_i(A) \mid \neg P_{i-1}(A) \& \cdots \& \neg P_k(A)] > \\ i^{-7/8} - 2^{-t_i}\text{poly}(t_i).$$

Just as in the previous proof denote by D_i the set of all binary words of length less than $2t_i$ and by F_i the set of all functions from D_i into $\mathbf{B}$.

Just as earlier for sufficiently large i the event $\neg P_{i-1}(A) \& \cdots \& \neg P_k(A)$ depends only on $A|D_i$.

Therefore, it is sufficient to prove that for all $f \in F_i$ the conditional probability Prob $[P_i(A) \mid A|D_i = f]$ is greater than $i^{-7/8} - 2^{-t_i}\mathrm{poly}(t_i)$. Let us fix a $i \in \mathbf{N}$ and $f \in F_i$. Let us restrict ourselves with oracle A such that $A|D_i = f$.

We have to prove that

$$\mathrm{Prob}\,[P_i(A) \mid A|D_i = f] > i^{-7/8} - 2^{-t_i}\mathrm{poly}(t_i).$$

More exactly, we will prove the inequality

$$\mathrm{Prob}\,[\neg P_i(A) \mid A|D_i = f] < 1 - i^{-7/8} + 2^{-t_i}\mathrm{poly}(t_i).$$

Let A be an oracle. The event $\neg P_i(A)$ means that A is identically zero in an $i, (1 - M^A(1^{t_i}))$-block. Let $Z = (\langle w_1, b_1\rangle, \ldots, \langle w_j, b_j\rangle)$ be a computational protocol on A. Let us call an i-block B *A-free* (respectively, *A-occupied*) if B is an $i, (1 - M^A(1^{t_i}))$-block and B doesn't intersect with the set $\{w_1, \ldots, w_j\}$ (respectively, B intersects with the set $\{w_1, \ldots, w_j\}$). Evidently $P_i(A)$ is true iff A is identically zero in an A-free block or A is identically zero in an A-occupied block. Denote the event "A is identically zero in an A-free block" by $Q'(A)$ and the event "A is identically zero in an A-occupied block" by $Q''(A)$. We will prove that for sufficiently large i, (5) and (6) hold.

$$\mathrm{Prob}\left[Q'(A) \;\middle|\; A|D_i = f\right] < 1 - i^{-7/8}. \qquad (5)$$

$$\mathrm{Prob}\left[Q''(A) \;\middle|\; A|D_i = f\right] \leq 2^{-t_i}\mathrm{poly}(t_i). \qquad (6)$$

Let us prove first that the inequality (5) holds for large enough i. It suffices to prove that that for large enough i for every $Z \in \Pi$,

$$\mathrm{Prob}\,[Q'(A) \mid A \text{ is consistent with } Z,\ A|D_i = f] < 1 - i^{-7/8}.$$

We claim that for every $Z \in \Pi$,

$$\mathrm{Prob}\,[Q'(A) \mid A \text{ is consistent with } Z,\ A|D_i = f] \leq 1 - (1 - 2^{-t_i})^{s_i}.$$

Let us fix a protocol $Z = (\langle w_1, b_1\rangle, \ldots, \langle w_j, b_j\rangle)$ from Π. Recall that the set Π is defined by formula (2). Without loss of generality we may assume that $M^A(1^{t_i}) = 1$ for A consistent with Z. Then $Q'(A)$ means that A is identically zero in an $i, 0$-block disjoint with the set $\{w_1, \ldots, w_j\}$. Denote by k the number of $i, 0$-blocks disjoint with the set $\{w_1, \ldots, w_j\}$. Then $\mathrm{Prob}[Q'(A) \mid A \text{ is consistent with } Z] = 1 - (1 - 2^{-t_i})^k$. As $k \leq s_i$, the claim is proved.

The definition of s_i involves that $1 - (1 - 2^{-t_i})^{s_i} < 1 - i^{-7/8}$ for sufficiently large i.

Let us prove now inequality (6). (Recall that $Q''(A)$ means that A is identically zero in some occupied block.)

If a word u belongs to a i-block, then denote by $B(u)$ the i-block which u belongs to. Denote by $R(A)$ the event "there are a protocol $Z = (\langle w_1, b_1\rangle, \ldots, \langle w_j, b_j\rangle)$ from Π and an $m \leq j$ such that the following assertions (a), (b) and (c) hold:

(a) w_m belongs to some i-block and A is identically zero in $B(w_m)$;

(b) $\forall i < m\ w_i \notin B(w_m)$;

(c) $\forall i < m\ A(w_i) = b_i$".

It's clear that $Q''(A)$ implies $R(A)$. (Indeed, if $Q''(A)$ holds, then we can take as Z the computational protocol on A and as m the least m' such that A is identically zero in $B(w_{m'})$.) Let us prove that $\mathrm{Prob}\,[R(A) \mid A|D_i = f] \leq 2^{-t_i}\mathrm{poly}(t_i)$. Let us fix a protocol $Z = (\langle w_1, b_1\rangle, \ldots, \langle w_j, b_j\rangle)$ and an $m \leq j$ and prove that

$$\mathrm{Prob}\,[\text{(a) \& (b) \& (c)}] \leq 2^{-m+1}2^{-t_i}. \qquad (7)$$

The truth value of (b) depends only on m and Z. If (b) is false for fixed m and Z, then we are done, because the left hand side of (7) is equal to zero in this case. If w_m belongs to no i-block, then again we are done. Assume that (b) is true and that w_m belongs to some i-block. Then (a) and (c) are independent (we assume that $w_1, \ldots, w_j$ are distinct), therefore,

$$\mathrm{Prob}\,[\text{(a) \& (b) \& (c)}] = \mathrm{Prob}\,[\text{(a)}]\mathrm{Prob}\,[\text{(c)}] = 2^{-t_i}2^{-m+1}.$$

Let us fix an arbitrary m. Let us prove that the probability of event "there is a protocol $Z = (\langle w_1, b_1\rangle, \ldots, \langle w_j, b_j\rangle)$ such that $m \leq j$ and (a)&(b)&(c)" is at most 2^{-t_i}. Denote this event by $R_m(A)$. If $Z = (\langle w_1, b_1\rangle, \ldots, \langle w_j, b_j\rangle)$ is a protocol such that $j \geq m$, then call m-prefix of Z the sequence

$Z_m = (\langle w_1, b_1\rangle, \ldots, \langle w_{m-1}, b_{m-1}\rangle, w_m)$. Clearly, the cardinality of the set $\mathcal{Z}_m = \{Z_m \mid Z \in \Pi\}$ is at most 2^{m-1} (because Z_m is completely defined by the tuple $\langle b_1, \ldots, b_{m-1}\rangle$). The truth values of the assertions (a), (b), and (c) depend only on A and Z_m. Therefore,

$$\begin{gathered}\text{Prob}\,[R_m(A) \mid A|D_i = f] \leq \\ \sum_{Y \in \mathcal{Z}_m} \text{Prob}\,[\text{(a), (b), and (c) hold for } Y] \times \\ \times \text{Prob}\,[C(A)_m = Y \mid A|D_i = f] \leq \\ 2^{m-1}(2^{-t_i}2^{-m+1}) = 2^{-t_i}.\end{gathered}$$

Let k be the maximal length of protocol from Π. Evidently $k \leq \text{poly}(t_i)$. Then

$$\begin{gathered}\text{Prob}\,[R(A) \mid A|D_i = f] \leq \\ \sum_{m=1}^{k} \text{Prob}\,[R_m(A) \mid A|D_i = f] \leq \\ 2^{-t_i} k \leq 2^{-t_i}\text{poly}(t_i),\ \text{q.e.d.}\end{gathered}$$

Theorem 3. *For random A there is an infinite* **Co-NP**^{A}*-language having no infinite* **NP**^{A}*-subset*

Proof. We will use all notions and notation from the proof of theorem 1 with the following changes. Set $s_i = 2^{t_i}$. Now we will use only $i,0$-blocks and will call them simply i-blocks. Consider the following **Co-NP**^{A}-language

$$\begin{gathered}L^A = \{1^{t_i} \mid\ i \in \mathbf{N} \text{ and } A \text{ is identically zero} \\ \text{in no } i\text{−block}\}.\end{gathered}$$

The language L^A is infinite for almost all A, because

$$\text{Prob}\,[1^{t_i} \in L^A] = (1 - 2^{-t_i})^{2^{t_i}} \to e^{-1},$$

as $i \to \infty$.

Let us prove that L^A has no infinite **NP**^{A}-subset for almost all A. We claim that to this end it suffices to prove that for any nondeterministic polynomial-time oracle machine N the probability of event "L_{N^A} is infinite and $L_{N^A} \subset L^A$ " is less than 3/4. Indeed, assume that this assertion is true but the probability of event "L^A has an infinite **NP**^{A}-subset" is positive. Then there is nondeterministic polynomial-time oracle machine N such that the probability of event "L_{N^A} is infinite and $L_{N^A} \subset L^A$ " is positive. Call any set of oracles of the form

$$\{A \mid A(w_1) = b_1, \ldots, A(w_j) = b_j\} \tag{8}$$

where $w_1, \ldots, w_j \in \mathbf{B}^*, b_1, \ldots, b_j \in \mathbf{B}$ an *interval*. A simple fact of theory of measure is that if a set of oracles S has positive measure, then there is an interval Γ such that *measure* $(\Gamma \cap S)$ is greater than 3/4 *measure* (Γ), that is,

$$\text{Prob}\,[A \in \Gamma \cap S \mid A \in \Gamma] > 3/4.$$

Set

$$S = \{A \mid L_{N^A} \text{ is infinite and } L_{N^A} \subset L^A\}.$$

Thus, there is an interval Γ such that

$$\text{Prob}\,[A \in \Gamma \cap S \mid A \in \Gamma] > 3/4.$$

Let $w_1, \ldots, w_j \in \mathbf{B}^*, b_1, \ldots, b_j \in \mathbf{B}$ be such that $\Gamma = \{A \mid A(w_1) = b_1, \ldots, A(w_j) = b_j\}$. For any oracle A set

$$A'(u) = \begin{cases} b_l, & \text{if } u = w_l \text{ for some } l \in \{1, \ldots, j\}; \\ A(u), & \text{otherwise.}\end{cases}$$

We can easily see that

$$\text{Prob}\,[A' \in S] = \text{Prob}\,[A \in S \mid A \in \Gamma].$$

Denote $k = \max_{m \leq j} |w_m|$. We can easily construct a nondeterministic polynomial-time oracle machine N_1 such that

$$N_1^A(x) = \begin{cases} 0, & \text{if } |x| \leq 2k; \\ N^{A'}(x), & \text{otherwise.}\end{cases}$$

We claim that if $A' \in S$, then $L_{N_1^A}$ is infinite and $L_{N_1^A} \subset L^A$. Indeed, let $A' \in S$, that is, $L_{N^{A'}}$ is infinite and $L_{N^{A'}} \subset L^{A'}$. Then, evidently, $L_{N_1^A}$ is infinite. And $L_{N_1^A} \subset L^A$, as if $N_1^A(x) = 1$, then $|x| > 2k$ and $N^{A'}(x) = 1$, consequently, $x \in L^{A'}$, which implies that $x \in L^A$ (because $|x| > 2k$). Therefore,

$$\begin{gathered}\text{Prob}\,[L_{N_1^A} \text{ is infinite and } L_{N_1^A} \subset L^A] \geq \\ \text{Prob}\,[A' \in S] = \text{Prob}\,[A \in S \mid A \in \Gamma] > 3/4.\end{gathered}$$

So, let N be an arbitrary nondeterministic polynomial-time oracle machine. Let us prove that the probability of event "L_{N^A} is infinite and $L_{N^A} \subset L^A$" doesn't exceed 3/4. Evidently, if L_{N^A} is infinite and $L_{N^A} \subset L^A$, then for all $x \in \mathbf{B}^*$ if $N^A(x) = 1$, then x has the form 1^{t_i}, and, therefore, there are infinitely many i such that $N^A(1^{t_i}) = 1$. Thus, it suffices to prove that

$$\text{Prob}\left[\exists^\infty i \; N^A(1^{t_i}) = 1\right] \leq 3/4 \tag{9}$$

or

$$\text{Prob}\left[\forall i \; (N^A(1^{t_i}) = 1 \Rightarrow 1^{t_i} \in L^A)\right] \leq 3/4 \tag{10}$$

where $\exists^\infty i$ means "there are infinitely many i such that".

Assume that (9) is false, that is, $\text{Prob}\left[\exists^\infty i \; N^A(1^{t_i}) = 1\right] > 3/4$. Then for all $k \in \mathbf{N}$

$$\sum_{i=k}^{\infty} \text{Prob}\left[N^A(1^{t_i}) = 1 \right.$$
$$\left. \forall j \in \{k, \ldots, i-1\} \; N^A(1^{t_j}) = 0\right] > 3/4.$$

We claim that if k is sufficiently large, then for all $i \geq k$

$$\text{Prob}\left[1^{t_i} \notin L^A \mid N^A(1^{t_i}) = 1 \right.$$
$$\left. \forall j \in \{k, \ldots, i-1\} \; N^A(1^{t_j}) = 0\right] > 1/2 \tag{11}$$

If the claim is true, then for sufficiently large k we have

$$\sum_{i=k}^{\infty} \text{Prob}\left[1^{t_i} \notin L^A \; N^A(1^{t_i}) = 1 \right.$$
$$\left. \forall j \in \{k, \ldots, i-1\} \; N^A(1^{t_j}) = 0\right] > 3/8 \tag{12}$$

The events the probabilities of which are summed in (12) are pairwise disjoint and each of them is included in the event $\exists i \geq k \; (1^{t_i} \notin L^A \;\; N^A(1^{t_i}) = 1)$. Hence the probability of the event $\exists i \geq k \; (1^{t_i} \notin L^A \;\; N^A(1^{t_i}) = 1)$ is at least 3/8 and therefore (10) holds.

Thus, we have to prove that for large enough k for all $i \geq k$ the assertion (11) is true. Let us fix k and $i \geq k$. Just as in the previous proof denote by D_i the set of all binary words of length less than $2t_i$ and by F_i the set of all functions from D_i into $\mathbf{B}$.

For sufficiently large i the event $\forall j \in \{k, \ldots, i-1\} \; N^A(1^{t_j}) = 0$ depends only on $A|D_i$. Therefore, it is sufficient to prove that if i is large enough, then for all $f \in F_i$ the conditional probability $\text{Prob}\left[1^{t_i} \notin L^A \mid N^A(1^{t_i}) = 1, \; A|D_i = f\right]$ is greater than 1/2. Let us fix an $f \in F_i$. Let us prove that

$$\text{Prob}\left[1^{t_i} \notin L^A \mid N^A(1^{t_i}) = 1, A|D_i = f\right] > 1/2$$

if i is large enough. Let N be the pair $\langle M, p\rangle$, where p is a polynomial and M is a deterministic polynomial-time oracle machine. Recall that

$$N^A(x) = \begin{cases} 1, & \text{if } \exists y \in \mathbf{B}^* \; (|y| = p(|x|) \\ & \quad M^A(x, y) = 1); \\ 0, & \text{otherwise.} \end{cases}$$

Evidently, the number of queries made by M on any input of the form $\langle 1^{t_i}, y\rangle$, where $|y| = p(t_i)$ is bounded by a polynomial, say $q(t_i)$, of t_i. Denote $r = q(t_i)$. Call any set of oracles of the form

$$\{A \mid A|D_i = f, \; A|B_1 = f_1, \ldots,$$
$$A|B_j = f_j, \; A|E = g\}, \tag{13}$$

where $j \leq r$, $B_1, \ldots, B_j$ are i-blocks, $f_1, \ldots, f_j$ are functions from $B_1, \ldots, B_j$, respectively, into $\mathbf{B}$, E is a finite set disjoint with D_i and disjoint with all the i-blocks and g is a function from E into $\mathbf{B}$, a *circumstance*. The set $\{A \mid N^A(1^{t_i}) = 1, A|D_i = f\}$ can be represented as a finite union of circumstances, say $\Gamma_1 \cup \cdots \cup \Gamma_n$. Indeed, the set $\{A \mid N^A(1^{t_i}) = 1, A|D_i = f\}$ can be represented as finite union of intervals $\{A \mid A(w_1) = b_1, \ldots, A(w_j) = b_j\}$ such that $j \leq r$ and every such interval included in $\{A \mid A|D_i = f\}$ is a finite union of circumstances. Thus, we have to prove that $\text{Prob}\left[1^{t_i} \notin L^A \mid A \in \Gamma_1 \cup \cdots \cup \Gamma_n\right] > 1/2$. Call a circumstance (13) *bad* if f_l is identically zero for some $l \leq j$. Any oracle from a bad circumstance satisfies the assertion $1^{t_i} \notin L^A$, therefore, if we delete from the union $\Gamma_1 \cup \cdots \cup \Gamma_n$ all bad circumstances, then the probability

$$\text{Prob}\left[1^{t_i} \notin L^A \mid A \in \Gamma_1 \cup \cdots \cup \Gamma_n\right] \tag{14}$$

will not increase. Thus we will estimate the probability (14) from below assuming that all $\Gamma_1, \ldots, \Gamma_n$ are not bad. Let us represent the probability (14) as the sum

$$\sum_{m=1}^{n} \text{Prob}\,[A \text{ is identically zero in some } i\text{−block} \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1})] \times$$
$$\times \text{Prob}\,[A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1}) \mid A \in \Gamma_1 \cup \cdots \cup \Gamma_n].$$

Clearly, it suffices to prove that if i is sufficiently large, then for all $m \leq n$,

$$\text{Prob}\,[A \text{ is identically zero in some } i\text{−block} \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1})] > 1/2.$$

Let us fix an $m \leq n$. Let the circumstance Γ_m be equal to (13). Denote by $C_1, \ldots, C_{s_i - j}$ all the i-blocks that don't belong to the set $\{B_1, \ldots, B_j\}$. For any $l \leq s_i - j$ set

$$p_l = \text{Prob}\,[A \text{ is identically zero in } C_l \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1}) \text{ and } A \text{ isn't identically zero in all the blocks } C_1, \ldots, C_{l-1}].$$

Obviously, the probability (14) is equal to $1 - (1 - p_1)(1 - p_2) \cdots (1 - p_{s_i - j})$. Let us prove that for any $l \leq s_i - j$ the inequality $p_l \geq 2^{-t_i}$ holds.

Let us fix arbitrary $l \leq s_i - j$ and prove $p_l \geq 2^{-t_i}$. Define for any oracle A the new oracle

$$A'(u) = \begin{cases} 0, & \text{if } u \in C_l; \\ A(u), & \text{otherwise.} \end{cases}$$

We claim that the set

$$U = \{A \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1}) \text{ and } A \text{ isn't identically zero in all the blocks } C_1, \ldots, C_{l-1}\}$$

has the property "$A \in U \Rightarrow A' \in U$". Indeed, let $A \in U$. Let us prove that $A' \in U$. As C_l doesn't belong to the set $\{B_1, \ldots, B_j\}$, the oracle A' is in Γ_m. The oracle A' isn't in $\Gamma_1 \cup \cdots \cup \Gamma_{m-1}$ because A isn't in $\Gamma_1 \cup \cdots \cup \Gamma_{m-1}$ and all the circumstances Γ_1, ..., Γ_{m-1} are not bad. As A isn't identically zero in the blocks C_1, ..., C_{l-1}, the oracle A' is also such.

It's clear that any set U of positive measure having the property "$A \in U \Rightarrow A' \in U$" satisfies the inequality

$$\text{Prob}\,[A \text{ is identically zero in } C_l \mid A \in U] \geq 2^{-t_i}.$$

Thus, we have proved that

$$\text{Prob}\,[A \text{ is identically zero in some } i\text{−block} \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1})] > 1 - (1 - 2^{-t_i})^{s_i - j}.$$

It remains to note that if i is large enough, then $1 - (1 - 2^{-t_i})^{s_i - j} > 1/2$, as $j \leq r \leq \text{poly}(t_i)$.

References

[1] T.Baker, J.Gill, R.Solovay. "Relativization of P=?NP Question," *SIAM Journal on Computing*, Vol. 4, 1975, p.431-442.

[2] C.H.Bennett, J.Gill. "Relative to a random oracle $\mathbf{P}^A \neq \mathbf{NP}^A \neq \mathbf{Co\text{-}NP}^A$ with probability 1," *SIAM Journal on Computing*, Vol.10, p.96–113, 1981.

[3] N.K.Vereshchagin. "Relative to a random oracle there are P-inseparable NP-sets and Co-NP-sets," *Proc. of The second Math. Symp. in memory of M.Ya.Suslin*, p. 13, 1991.