NP-sets are Co-NP-immune Relative to a Random Oracle

Nikolai K. Vereshchagin*
Department of Mathematical Logic
Moscow State University, Moscow 119899, Russia
E-mail: ver@math.math.msu.su

Abstract

We prove that the class NP *has* Co-NP*-immune sets relative to a random oracle. Moreover, we prove that, relative to a random oracle, there are* $L \in$ P *and* NP*-set* $L_1 \subseteq L$ *such that* L_1 *is* Co-NP*-immune and* $L \setminus L_1$ *is* NP*-immune. The second theorem implies the theorem in [4] that* Co-NP *has* NP*-immune sets relative to a random oracle.*

1 Introduction

Many important problems in Complexity theory remain open. The most known one is if the classes P and NP coincide. It is also unknown if NP = Co-NP and if NP $\cap$ Co-NP = 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 $\mathrm{P}^A = \mathrm{NP}^A$ (and, therefore, $\mathrm{P}^A = \mathrm{NP}^A \cap \text{Co-NP}^A$) and $\mathrm{NP}^B \neq \text{Co-NP}^B$ (and, therefore, $\mathrm{P}^B \neq \mathrm{NP}^B$). By using the same technique one can construct an oracle C for which $\mathrm{NP}^C \cap \text{Co-NP}^C \neq \mathrm{P}^C$.

As the relationships between the classes Co-NP^A, NP^A and P^A depend 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 relationships between the classes NP^A, Co-NP^A and P^A for oracle A being random with respect to the uniform

*This research was in part supported by a grant from the American Mathematical Society former Soviet Union Aid Fund, the grant MQT000 from the International Science Foundation, by a grant from "Cultural Initiative" foundation and by NSF grant CCR-8957604. Work done in part while visiting the University of Rochester.

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 $S(A)$ 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, either $S(A)$ holds for random A, or $\neg S(A)$ holds for random A.

The study of Complexity theory relative to a random oracle began in [2], where it was proved that $\mathrm{P}^A \neq \mathrm{NP}^A \neq \text{Co-NP}^A$ for random A. It was also proved in [2] that for random A there exists an infinite NP^A-set which is P^A-immune, that is, has no infinite P^A-subsets. In [4], it was proved that both NP-sets and Co-NP-sets are P-inseparable relative to a random oracle. It was proved also in that paper that Co-NP has an infinite NP-immune set relative to a random oracle.

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 P^A-sets, recursively enumerable sets correspond to NP^A-sets and complements of recursively enumerable sets correspond to Co-NP^A-sets, where A is a random oracle. As we have said, in Complexity theory the analogs of the following theorems are true: the theorem on the existence of recursively enumerable undecidable set, the theorem on the existence of recursively enumerable set whose complement is not recursively enumerable, the theorem on the existence of recursively enumerable inseparable sets, the theorem on the existence of a simple set (recursively enumerable set whose complement is infinite but has no infinite recursively enumerable subsets). The analogs of the following theorems are false: the theorem that every infinite recursively enumerable set has an infinite decidable subset and the theorem on separability of sets having recursively enumerable complements.

It remains an open problem at present if the analog of Post's theorem is true (if both a set and its complement are recursively enumerable, then the set is decidable), i.e., it is unknown if $\mathrm{NP}^A \cap \text{Co-NP}^A = \mathrm{P}^A$ for random A. As mentioned in [5], if $\mathrm{NP}^A \cap \text{Co-NP}^A = \mathrm{P}^A$ for random A, then $\mathrm{AM} \cap \text{Co-AM} = \mathrm{BPP}$, in particular, the problem of graph isomorphism is in BPP. Thus, it cannot be hoped to prove that $\mathrm{NP}^A \cap \text{Co-NP}^A = \mathrm{P}^A$ for random A. No absolute consequences of the assertion "$\mathrm{NP}^A \cap \text{Co-NP}^A \neq \mathrm{P}^A$ for random A" are known; so one may hope to prove that $\mathrm{NP}^A \cap \text{Co-NP}^A \neq \mathrm{P}^A$ for random A.

It remained an open problem if NP has a Co-NP-immune set relative to a random oracle. Some advance in solving this problem was achieved in [3] where it was proved that relative to a random oracle there exists an infinite NP-set whose Co-NP-subsets must be "thin" in a sense.

In the present paper we solve this problem: we prove that NP has Co-NP-

Table 1:

	Relative to random oracle	Relative to generic oracle	Recursion theory
P $\neq$ NP	+	+	+
NP $\neq$ Co-NP	+	+	+
NP-sets are P-inseparable	+	?	+
Co-NP-sets are P-inseparable	+	+	−
P = NP $\cap$ Co-NP	?	?	+
NP has P-immune sets	+	−	−
NP has Co-NP-immune sets	+	−	−
Co-NP has NP-immune sets	+	+	+

immune sets relative to a random oracle. Moreover, we prove that, relative to a random oracle, there are $L \in$ P and NP-set $L_1 \subseteq L$ such that L_1 is Co-NP-immune and $L \setminus L_1$ is NP-immune. The second theorem implies the theorem in [4] that Co-NP has NP-immune sets relative to a random oracle.

All the result citied above are presented in the Table 1. The analogous results on generic oracle are also shown there.

2 Definitions

We consider subsets of the set $\mathbf{B}^*$ of all the words over the binary alphabet $\mathbf{B} = \{0,1\}$. We 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 P^A consists of all languages L such that there exists 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 NP^A consists of all languages L such that there exist 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

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

A possible computation of machine N on input x is a computation of M on

any input of the form $\langle x, y\rangle$, where $|x| = p(|y|)$. 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. We say that L *separates* L_1 from L_2 if $L_1 \subseteq L$ and $L_2 \subseteq \mathbf{B}^* \setminus L$. Let $\mathcal{C}$ and $\mathcal{C}'$ be families of languages. Say that $\mathcal{C}$-languages are $\mathcal{C}'$-separable if for every two disjoint languages L_1 and L_2 in $\mathcal{C}$ there exists a language L in $\mathcal{C}'$ which separates L_1 from L_2. Let $S(A)$ be a property of an oracle A. We say that $S(A)$ holds for random A, or for almost all A, if the uniform measure of the set $\{A \mid S(A)\}$ is equal to 1.

3 The results

Theorem 1 *Relative to a random oracle, there are* $L \in$ P *and* NP*-set* $L_1 \subseteq L$ *such that both* L_1 *and* $L \setminus L_1$ *are infinite,* L_1 *has no infinite* Co-NP*-subsets and* $L \setminus L_1$ *has no infinite* NP*-subsets.*

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. An *i-blocks* is any set of the form

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

where w is a binary word of length t_i. Thus, each i-block consists of t_i words (of length $t_i + \log_2 t_i$).

Let

$$L = \{1^{t_i} \mid\ i \in \mathbf{N}\}.$$

We say that an oracle A is *identically zero in block* B if $\forall u \in B\ A(u) = 0$.

For any oracle A let

$$L_1^A = \{1^{t_i} \mid\ i \in \mathbf{N} \text{ and } A \text{ is identically zero in some } i\text{−block}\},$$
$$L_0^A = L \setminus L_1^A$$

Obviously, L is in P^A and L_1^A is in NP^A for any A.

Both languages L_0^A and L_1^A are infinite for almost all A, because

$$\begin{aligned}\mathrm{Prob}\,[1^{t_i} \in L_0^A] &= 1 - \mathrm{Prob}\,[1^{t_i} \in L_1^A] \\ &= (1 - 2^{-t_i})^{2^{t_i}} \to e^{-1},\end{aligned}$$

as $i \to \infty$.

Let us prove that

1) L_0^A has no infinite NP^A-subset for almost all A and

2) L_1^A has no infinite Co-NP^A-subset for almost all A.

We claim that instead of 1) it suffices to prove the following assertion

1′) there exists $c < 1$ such that for any nondeterministic polynomial-time oracle machine N the probability of event "L_{N^A} is infinite and $L_{N^A} \subseteq L_0^A$" is less than c,

and instead of 2) it suffices to prove the following assertion

2′) there exists $c < 1$ such that for any nondeterministic polynomial-time oracle machine N the probability of event "$\mathbf{B}^* \setminus L_{N^A}$ is infinite and $\mathbf{B}^* \setminus L_{N^A} \subseteq L_1^A$" is less than c.

Let us prove first the implication 1′) $\Rightarrow$ 1). Assume that 1′) is true but the probability of event "L_0^A has an infinite NP^A-subset" is positive. Then there exists a nondeterministic polynomial-time oracle machine N such that the probability of event "L_{N^A} is infinite and $L_{N^A} \subseteq L_0^A$ " is positive. Call any set of oracles of the form

$$\{A \mid A(w_1) = b_1, \ldots, A(w_j) = b_j\} \tag{1}$$

where $w_1, \ldots, w_j \in \mathbf{B}^*, b_1, \ldots, b_j \in \mathbf{B}$ an *interval*. A simple theorem in the measure theory states that if a set of oracles S has positive measure and $c < 1$, then there exists an interval Γ such that

$$\mathrm{Prob}\,[A \in S \mid A \in \Gamma] > c. \tag{2}$$

Let us apply that theorem to the set

$$S = \{A \mid L_{N^A} \text{ is infinite and } L_{N^A} \subseteq L_0^A\}.$$

Thus, there exists an interval Γ such that (2) is true. 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 let us define the new oracle A' as follows:

$$A'(u) = \begin{cases} b_l, & \text{if } u = w_l \text{ where } l \in \{1, \ldots, j\}; \\ A(u), & \text{if } u \notin \{w_1, \ldots, w_j\}. \end{cases}$$

It is easy to see that

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

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

$$N_1^A(x) = \begin{cases} 0, & \text{if } |x| + 2\log_2|x| \le k; \\ N^{A'}(x), & \text{otherwise.} \end{cases}$$

We claim that if $A' \in S$, then $L_{N_1^A}$ is infinite and $L_{N_1^A} \subseteq L_0^A$. Indeed, let A' be in S, that is, $L_{N^{A'}}$ is infinite and $L_{N^{A'}} \subseteq L_0^{A'}$. Then, obviously, $L_{N_1^A}$ is infinite.

And $L_{N_1^A} \subseteq L_0^A$, as if $N_1^A(x) = 1$, then $|x| + 2\log_2|x| > k$ and $N^{A'}(x) = 1$, consequently, $x \in L_0^{A'}$, which implies that $x \in L_0^A$ (because $|x| + 2\log_2|x| > k$). Therefore,

$$\begin{aligned}&\mathrm{Prob}\left[L_{N_1^A} \text{ is infinite and } L_{N_1^A} \subseteq L_0^A\right]\\ &\quad \geq \mathrm{Prob}\left[A' \in S\right] > c.\end{aligned}$$

The obtained contradiction proves the implication $1') \Rightarrow 1)$. The implication $2') \Rightarrow 2)$ can be proved in a similar way.

So, we have to prove $1')$ and $2')$. Let N be an arbitrary nondeterministic polynomial-time oracle machine. Let us prove that the probabilities of both events

$$\text{“}L_{N^A} \text{ is infinite and } L_{N^A} \subseteq L_0^A\text{”} \tag{3}$$

$$\text{“}\mathbf{B}^* \setminus L_{N^A} \text{ is infinite and } \mathbf{B}^* \setminus L_{N^A} \subseteq L_1^A\text{”} \tag{4}$$

do not exceed 0.9. Obviously, if L_{N^A} is infinite and $L_{N^A} \subseteq L_0^A$ then there exist infinitely many i such that $N^A(1^{t_i}) = 1$. Thus, to prove that $\mathrm{Prob}\left[(3)\right] \leq 0.9$ it suffices to prove the implication

$$\mathrm{Prob}\left[\exists^\infty i\ N^A(1^{t_i}) = 1\right] > 0.9 \Rightarrow \tag{5}$$

$$\mathrm{Prob}\left[\exists i\ (N^A(1^{t_i}) = 1\ \&\ 1^{t_i} \in L_1^A)\right] \geq 0.1 \tag{6}$$

where $\exists^\infty i$ means “there exist infinitely many i such that”. Likewise, to prove that $\mathrm{Prob}\left[(4)\right] \leq 0.9$ it suffices to prove the implication

$$\mathrm{Prob}\left[\exists^\infty i\ N^A(1^{t_i}) = 0\right] > 0.9 \Rightarrow \tag{7}$$

$$\mathrm{Prob}\left[\exists i\ (N^A(1^{t_i}) = 0\ \&\ 1^{t_i} \in L_0^A)\right] \geq 0.1. \tag{8}$$

We will prove these two implications in parallel. The combined implication is as follows: for any $\delta \in \{0, 1\}$

$$\mathrm{Prob}\left[\exists^\infty i\ N^A(1^{t_i}) = \delta\right] > 0.9 \Rightarrow \tag{9}$$

$$\mathrm{Prob}\left[\exists i\ (N^A(1^{t_i}) = \delta\ \&\ 1^{t_i} \in L_\delta^A)\right] \geq 0.1. \tag{10}$$

Let us fix a $\delta \in \{0, 1\}$. Assume that (9) is true. Let us prove (10). Assertion (9) implies that

$$\begin{aligned}\sum_{i=k}^{\infty} \mathrm{Prob}\big[&N^A(1^{t_i}) = \delta\ \&\ N^A(1^{t_{i-1}}) \neq \delta,\\ &N^A(1^{t_{i-2}}) \neq \delta, \ldots, N^A(1^{t_k}) \neq \delta\big] > 0.9\end{aligned} \tag{11}$$

for all $k \in \mathbf{N}$.

Denote the event

$$N^A(1^{t_{i-1}}) \neq \delta, N^A(1^{t_{i-2}}) \neq \delta, \ldots, N^A(1^{t_k}) \neq \delta$$

by $P_{ik\delta}(A)$.

Lemma 1 *If k is large enough, then for any $i \geq k$,*

$$\begin{aligned} &\mathrm{Prob}\left[1^{t_i} \in L_\delta^A \ \&\ N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A)\right] > \\ &\quad (1/3)\mathrm{Prob}\left[N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A)\right] - \varepsilon_i, \end{aligned} \tag{12}$$

where ε_i is a sequence having the convergent series $\sum_{i=1}^{\infty} \varepsilon_i$.

We will prove the lemma later. Let us continue now the proof of the theorem. By summing (12) over $i \geq k$ we get

$$\begin{aligned} &\sum_{i=k}^{\infty} \mathrm{Prob}\left[1^{t_i} \in L_\delta^A \ \&\ N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A))\right] > \\ &\quad (1/3)\sum_{i=k}^{\infty} \mathrm{Prob}\left[N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A)\right] - \sum_{i=k}^{\infty} \varepsilon_i. \end{aligned} \tag{13}$$

Combining (11) and (13) we get

$$\begin{aligned} &\textstyle\sum_{i=k}^{\infty} \mathrm{Prob}\left[1^{t_i} \in L_\delta^A \ \&\ \mathbf{N}^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A)\right] \\ &\qquad > 0.3 - \textstyle\sum_{i=k}^{\infty} \varepsilon_i. \end{aligned} \tag{14}$$

As the events whose probabilities are summed in the left hand side of (14) are pairwise disjoint and included in the event

$$\exists i \ (N^A(1^{t_i}) = \delta \ \&\ 1^{t_i} \in L_\delta^A), \tag{15}$$

we get that the probability of (15) is greater then $0.3 - \sum_{i=k}^{\infty} \varepsilon_i$. By taking k so large that $\sum_{i=k}^{\infty} \varepsilon_i < 0.2$ we get (10).

Thus the proof of the theorem is completed. However, it remains to prove Lemma 1. □

Proof of the Lemma 1. Let us fix a sufficiently large k (how large should be k we will see later). Let us fix an arbitrary $i \geq k$. Denote by D_i the set of all binary words of length less than $t_i + \log_2 t_i$ and by F_i the set of all functions from D_i into $\mathbf{B}$. Denote by $f|S$ the restriction of function f to the set S. For any j, the event $N^A(1^{t_j}) \neq \delta$ depends only on the value of A on the words of length bounded by a polynomial of t_j (because N on input 1^{t_j} can put to the oracle questions of the length bounded by a polynomial of t_j). As $t_i = 2^{t_{i-1}}$, if k is sufficiently large, then for any $i \geq k$, the event $P_{ik\delta}(A)$ depends only on $A|D_i$. Therefore, we may assume that this is the case.

We will prove that for all $f \in F_i$,

$$\begin{aligned} &\mathrm{Prob}\left[1^{t_i} \in L_\delta^A \ \&\ N^A(1^{t_i}) = \delta \mid A|D_i = f\right] > \\ &\quad (1/3)\mathrm{Prob}\left[N^A(1^{t_i}) = \delta \mid A|D_i = f\right] - \varepsilon_i, \end{aligned} \tag{16}$$

where $\{\varepsilon_i\}$ is a sequence such the series $\sum_{i=1}^{\infty}\varepsilon_i$ converges. Let us prove that this imply (12). Assume that (16) is true for any $f \in F_i$. Then by multiplying (16) by $\mathrm{Prob}\,[A|D_i = f]$ we get

$$\begin{gathered}\mathrm{Prob}\left[1^{t_i} \in L_\delta^A \ \&\ N^A(1^{t_i}) = \delta \ \&\ A|D_i = f\right] > \\ (1/3)\mathrm{Prob}\left[N^A(1^{t_i}) = \delta \ \&\ A|D_i = f\right] - \\ \varepsilon_i \mathrm{Prob}\left[A|D_i = f\right]. \end{gathered} \tag{17}$$

By summing (17) over all $f \in F_i$ such that $P_{ik\delta}(A)$ is true provided $A|D_i = f$, we get

$$\begin{gathered}\mathrm{Prob}\left[1^{t_i} \in L_\delta^A \ \&\ N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A)\right] > \\ (1/3)\mathrm{Prob}\left[N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A)\right] - \\ \varepsilon_i \mathrm{Prob}\left[P_{ik\delta}(A)\right] \geq \\ (1/3)\mathrm{Prob}\left[N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A)\right] - \varepsilon_i, \end{gathered}$$

that is, we get (12)

So we have to prove that (16) is true for all $f \in F_i$. Fix an arbitrary $f \in F_i$. Obviously, the number of queries made by M during possible computations on input 1^{t_i}, is bounded by a polynomial of t_i. Denote that polynomial by $q(t_i)$.

To proceed further we have to handle the cases $\delta = 0$ and $\delta = 1$ separately.

Lemma 2

$$\begin{gathered}\mathrm{Prob}\left[N^A(1^{t_i}) = 1 \ \&\ 1^{t_i} \in L_1^A \mid A|D_i = f\right] > \\ \left(1 - (1 - 2^{-t_i})^{2^{t_i} - q(t_i)}\right) \times \\ \times \mathrm{Prob}\left[N^A(1^{t_i}) = 1 \mid A|D_i = f\right]. \end{gathered} \tag{18}$$

Proof. Let $r = q(t_i)$. An *r-circumstance* is a set of oracles of the form

$$\begin{gathered}\{A \mid A|D_i = f,\ A|B_1 = f_1, A|B_2 = f_2, \ldots, \\ A|B_r = f_r,\ A|E = g\}, \end{gathered} \tag{19}$$

where $B_1, \ldots, B_r$ are i-blocks, $f_1, \ldots, f_r$ are functions from $B_1, \ldots, B_r$, 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 $\mathbf{B}$. Let

$$W = \{A \mid N^A(1^{t_i}) = 1, A|D_i = f\}.$$

Lemma 2.1 *The set W can be represented as a finite union of r-circumstances.*

Proof. Let us prove first that the set W can be represented as finite union of intervals of the form $\{A \mid A(w_1) = b_1, \ldots, A(w_r) = b_r,\ A|D_i = f\}$. Let A be

an oracle such that $A|D_i = f$. Assume that $N^A(1^{t_i}) = 1$. Fix an accepting computation of N^A on input 1^{t_i}. Let the oracle be queried about the value on the words $w_1, \ldots, w_r$. Then the set W contains the entire interval $\{A \mid A(w_1) = b_1, \ldots, A(w_r) = b_r,\ A|D_i = f\}$. Since the number of all the computations of N on input 1^{t_j} with all the oracles is finite, we are done.

Thus, the set W can be represented as a finite union of intervals of the form $\{A \mid A(w_1) = b_1, \ldots, A(w_r) = b_r,\ A|D_i = f\}$. Obviously any interval having this form is a finite union of r-circumstances.$\Box$

Denote by $\Gamma_1, \ldots, \Gamma_n$ the r-circumstances such that $W = \Gamma_1 \cup \cdots \cup \Gamma_n$. Thus, we have to prove that

$$\begin{aligned} &\text{Prob}\left[1^{t_i} \in L_1^A \mid A \in \Gamma_1 \cup \cdots \cup \Gamma_n\right] > \\ &\qquad 1 - (1 - 2^{-t_i})^{2^{t_i} - r}. \end{aligned} \tag{20}$$

Call r-circumstance (19) *bad* if f_l is identically zero for some $l \leq r$. Any oracle A in a bad r-circumstance satisfies the assertion $1^{t_i} \in L_1^A$. Therefore, if we remove from the union $\Gamma_1 \cup \cdots \cup \Gamma_n$ all bad r-circumstances, the probability

$$\text{Prob}\left[1^{t_i} \in L_1^A \mid A \in \Gamma_1 \cup \cdots \cup \Gamma_n\right]$$

will not increase. Thus it suffices to prove (20) in the case when all $\Gamma_1, \ldots, \Gamma_n$ are not bad. Clearly, it suffices to prove that for all $m \leq n$,

$$\begin{aligned} &\text{Prob}\,[A \text{ is identically zero in some } i\text{-block} \mid \\ &\quad A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1})] > \\ &\quad 1 - (1 - 2^{-t_i})^{2^{t_i} - r} \end{aligned} \tag{21}$$

provided $\Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1})$ is not empty.

Let us fix $m \leq n$. Let Γ_m be equal to (19). Denote by $C_1, \ldots, C_{2^{t_i} - r}$ all the i-blocks that do not belong to the set $\{B_1, \ldots, B_r\}$. For any $l \leq 2^{t_i} - r$ let

$$\begin{aligned} p_l = \text{Prob}\,[&A \text{ is identically zero in } C_l \mid \\ &A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1}) \text{ and } A \text{ is not identically zero} \\ &\text{in all the blocks } C_1, \ldots, C_{l-1}]. \end{aligned} \tag{22}$$

Of course, it may happen that some of p_l's is undefined because the set

$$\begin{aligned} &\{A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1}) \mid \\ &A \text{ is not identically zero in all the blocks } C_1, \ldots, C_{l-1}\} \end{aligned}$$

is empty. This means that any $A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1})$ is identically zero in some of the blocks $C_1, \ldots, C_{l-1}$. Thus in this case the probability (21) is equal to 1 so we are done.

Obviously, the probability (21) is equal to $1 - (1 - p_1)(1 - p_2) \cdots (1 - p_{2^{t_i} - r})$. Thus to prove Lemma 2 it suffices to prove the following

Lemma 2.2 *$p_l \geq 2^{-t_i}$ for any $l \leq 2^{t_i} - r$ such that p_l is defined.*

Proof. Let us fix arbitrary $l \leq 2^{t_i} - r$ such that p_l is defined and prove that $p_l \geq 2^{-t_i}$. Define for any oracle A the new oracle A' as follows:

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

Let us call a set of oracles U *monotone* if $A \in U$ implies $A' \in U$. We claim that the set

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

is monotone. Recall that

$$\Gamma_m = \{A \mid A|D_i = f,\ A|B_1 = f_1, \ldots, A|B_r = f_r,\ A|E = g\},$$

and C_l does not belong to the set $\{B_1, \ldots, B_r\}$. This implies that Γ_m is monotone.

Since $\Gamma_1, \ldots, \Gamma_{m-1}$ are not bad, the complement of the set $\Gamma_1 \cup \cdots \cup \Gamma_{m-1}$ is monotone, too. Obviously, the set $\{A \mid A$ is not identically zero in all the blocks $C_1, \ldots, C_{l-1}\}$ is monotone. Therefore, U is monotone as an intersection of monotone sets.

Thus Lemma 2.2 easily follows from the following

Sublemma 2.2.1 *Any monotone set V of positive measure satisfies the inequality*

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

Proof of Sublemma 2.2.1. Let V satisfy the assumptions of the Sublemma 2.2.1. Denote by H the set of all the functions from C_l into $\mathbf{B}$. Denote by $\mathbf{0}$ the identically zero function in H. Let h be an arbitrary function in H. We claim that there exists a measure preserving 1–1–function from the set

$$\mathcal{B} = \{A \in V \mid A|C_l = h\}$$

into the set

$$\mathcal{D} = \{A \in V \mid A|C_l = \mathbf{0}\}$$

Indeed, let π be a permutation of H such that $\pi(h) = \mathbf{0}$. Then the mapping $A \mapsto A''$, where

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

maps $\mathcal{B}$ into $\mathcal{D}$ because $A'' = A'$ if $A \in \mathcal{B}$ and V is monotone.

Thus for any h,

$$\mathrm{Prob}\,[A \in V \ \&\ A|C_l = h] \le \mathrm{Prob}\,[A \in V \ \&\ A|C_l = \mathbf{0}].$$

Therefore,

$$\begin{aligned}\mathrm{Prob}\,[A \in V] &= \sum_h \mathrm{Prob}\,[A \in V \ \&\ A|C_l = h] \\ &\le 2^{|C_l|}\mathrm{Prob}\,[A \in V \ \&\ A|C_l = \mathbf{0}].\Box\end{aligned}$$

Thus Lemma 2.2 and Lemma 2 are proved.$\Box$

It is easy to verify that $\lim_{i\to\infty}\left(1-(1-2^{-t_i})^{2^{t_i}-q(t_i)}\right) = 1-e^{-1} > 1/3$, therefore Lemma 2 implies the Lemma 1 in the case $\delta = 1$ (in this case we set $\varepsilon_i = 0$).

It remains to handle with the case $\delta = 0$. Let $a_i = (1-2^{-t_i})^{2^{t_i}} = \mathrm{Prob}\,[1^{t_i} \in L_0^A]$ and $\varepsilon_i = (1-2^{-t_i})^{2^{t_i}-q(t_i)} - a_i$. Obviously,

$$\varepsilon_i = O(q(t_i)2^{-t_i}).$$

Thus the series $\sum_{i=1}^{\infty}\varepsilon_i$ converges.

Lemma 1 for $\delta = 0$ immediately follows from the following

Lemma 3

$$\begin{aligned}&\mathrm{Prob}\left[1^{t_i} \in L_0^A \ \&\ N^A(1^{t_i}) = 0 \mid A|D_i = f\right] > \\ &\qquad a_i\mathrm{Prob}\left[N^A(1^{t_i}) = 0 \mid A|D_i = f\right] - \varepsilon_i. \end{aligned} \tag{23}$$

Proof. By Lemma 2,

$$\begin{aligned}&\mathrm{Prob}\left[1^{t_i} \in L_1^A,\ N^A(1^{t_i}) = 1 \mid A|D_i = f\right] \\ &\quad > (1-a_i-\varepsilon_i)\mathrm{Prob}\left[N^A(1^{t_i}) = 1 \mid A|D_i = f\right].\end{aligned} \tag{24}$$

In the next equations we shall omit the condition $A|D_i = f$ to make them readable. We have

$$\begin{aligned}&\mathrm{Prob}\,[1^{t_i} \in L_1^A,\ N^A(1^{t_i}) = 0] \\ &\quad = \mathrm{Prob}\,[1^{t_i} \in L_1^A] - \mathrm{Prob}\,[1^{t_i} \in L_1^A,\ N^A(1^{t_i}) = 1] \\ &\quad \le 1-a_i-(1-a_i-\varepsilon_i)\mathrm{Prob}\,[N^A(1^{t_i}) = 1] \\ &\quad = (1-a_i)\mathrm{Prob}\,[N^A(1^{t_i}) = 0] + \varepsilon_i\mathrm{Prob}\,[N^A(1^{t_i}) = 1] \\ &\quad \le (1-a_i)\mathrm{Prob}\,[N^A(1^{t_i}) = 0] + \varepsilon_i. \\ &\mathrm{Prob}\,[1^{t_i} \in L_0^A,\ N^A(1^{t_i}) = 0] \\ &\quad = \mathrm{Prob}\,[N^A(1^{t_i}) = 0] - \mathrm{Prob}\,[1^{t_i} \in L_1^A,\ N^A(1^{t_i}) = 0] \\ &\quad \ge \mathrm{Prob}\,[N^A(1^{t_i}) = 0] - (1-a_i)\mathrm{Prob}\,[N^A(1^{t_i}) = 0] - \varepsilon_i \\ &\quad = a_i\mathrm{Prob}\,[N^A(1^{t_i}) = 0] - \varepsilon_i.\end{aligned}$$

The Lemma 3 is proved.$\Box$

Corollary 2 [4] *For random A there exists an infinite* NP^A*-set having no infinite* $\mathrm{Co\text{-}NP}^A$*-subset.*

Corollary 3 *For random A there exists an infinite* $\mathrm{Co\text{-}NP}^A$*-set having no infinite* NP^A*-subset.*

References

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

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

[3] S. Kurtz, S. Mahaney, J. Royer. "Average Dependence and Random Oracle", *Proc. of 7th Annual Conference on Structure in Complexity Theory,* July 22-25, 1992, Boston MA, pp. 306–317.

[4] N. K. Vereshchagin. "Relationships between NP-sets, Co-NP-sets and P-sets relative to random oracles", *Izvestiya Vysshykh Uchebnykh Zavedenij. Seria Matematika*, 1993, No. 3, pp. 31–39 (in Russian). Conference version appeared in: *Proc. of 8th Annual IEEE Conference on Structure in Complexity Theory,* May 1993, San-Diego CA, pp. 132–138.

[5] M. Blum and R. Impagliazzo. "General Oracle and Oracle Classes", *Proc. 28th Annual IEEE Symposium on Foundations of Computer Science*, May 1987, pp. 118–126.