Н. К. Верещагин, Соотношение NP- и со-NP-множеств относительно случайного оракула, *Изв. вузов. Матем.*, 1993, номер 3, 31–39

ИЗВЕСТИЯ ВЫСШИХ УЧЕБНЫХ ЗАВЕДЕНИЙ

1993 МАТЕМАТИКА № 3 (370)

УДК 510.52

Н.К.ВЕРЕЩАГИН

СООТНОШЕНИЕ NP- И co-NP-МНОЖЕСТВ ОТНОСИТЕЛЬНО СЛУЧАЙНОГО ОРАКУЛА

В данной работе доказано, что для случайного оракула A выполнены следующие три утверждения:

(1) существуют непересекающиеся NP^A-языки, не отделимые никаким P^A-языком;

(2) существуют непересекающиеся co-NP^A-языки, не отделимые никаким P^A-языком;

(3) существует бесконечный co-NP^A-язык, не имеющий бесконечных подмножеств из NP^A.

§ 1. Введение

Многие важные проблемы теории сложности вычислений открыты. Наиболее известная из них – совпадают ли классы P и NP. Неизвестно также, совпадают ли классы NP и co-NP и верно ли, что $NP \cap$ co-$NP = P$.

В работе [1] доказано, что эти проблемы не имеют релятивизуемого решения. Точнее, построены такие оракулы A и B, что $P^A = NP^A$ (и, следовательно, $P^A = NP^A =$ co-$NP^A = NP^A \cap$ co-NP^A) и $NP^B \neq$ co-NP^B (и, следовательно, $P^B \neq NP^B$). Используя метод работы [1], нетрудно построить оракул C, для которого $NP^C \cap$ co-$NP^C \neq P^C$.

Поскольку для разных оракулов получаются разные соотношения классов P, NP, co-NP, возникает вопрос – что имеет место для "типичного" оракула. Одно из возможных уточнений понятия типичности – это случайность по равномерной мере. Данная работа посвящена соотношению классов P^A, NP^A, co-NP^A для оракула A, случайного по равномерной мере. Мы говорим, что для случайного оракула A верно некоторое утверждение $S(A)$, если вероятность по равномерной мере события $S(A)$ равна единице. Все утверждения $S(A)$, встречающиеся во введении, будут обладать двумя свойствами: множество $\{A \mid S(A)\}$ измеримо и $S(A)$ устойчиво относительно конечных изменений A. Для таких утверждений $S(A)$ по 0-1-закону А.Н.Колмогорова либо для случайного A выполнено $S(A)$, либо для случайного A выполнено $\neg S(A)$.

Исследование сложности вычислений относительно случайного оракула начато в работе [2], где доказано, что для случайного A выполнено $P^A \neq NP^A \neq$ co-NP^A. Там же доказано, что для случайного A существует бесконечный NP^A-язык, не имеющий бесконечного подмножества из P^A. Интересно провести аналогию между качественной теорией алгоритмов (теорией рекурсии) и количественной теорией алгоритмов (теорией сложности вычислений) относительно случайного оракула. При этой аналогии разрешимым множествам соответствуют P-языки, перечислимым множествам соответствуют NP-языки, а коперечислимым множествам (дополнениям перечислимых) соответствуют co-NP-языки. Тогда, как уже сказано, в теории сложности вычислений относительно случайного оракула верны аналоги теорем о существовании перечислимого неразрешимого множества и о существовании перечислимого множества с неперечислимым дополнением. А аналог теоремы о том, что любое бесконечное перечислимое множество имеет бесконечное разрешимое подмножество, неверен.

В данной работе рассматриваются аналоги еще трех хорошо известных теорем качественной теории алгоритмов: теоремы о существовании перечислимых неотделимых множеств, теоремы об отделимости коперечислимых множеств и теоремы о существовании простого множества (перечислимого множества, дополнение которого бесконечно, но не имеет бесконечного перечислимого подмножества). Именно, доказывается, что аналоги первой и третьей теорем верны (теоремы 1 и 3 в §3), а аналог второй теоремы неверен (теорема 2 в §3). Формулировки теорем 1 и 2 вместе с планом доказательства опубликованы также в работе автора [3].

Остается неизвестным, верен ли для случайного оракула аналог теоремы Поста, т.е. верно ли, что $NP^A \cap \text{co-}NP^A = P^A$ для случайного A. Нетрудно доказать, что из положительного решения этой проблемы следует некоторое абсолютное утверждение о сложностных классах, истинность или ложность которого неизвестна. Это утверждение — $AM \cap \text{co-}AM = BPP$, из него, в частности, следует существование полиномиального вероятностного алгоритма распознавания изоморфности графов. Таким образом, мало надежд на доказательство $NP^A \cap \text{co-}NP^A = P^A$ для случайного A. Абсолютных следствий из выполненности $NP^A \cap \text{co-}NP^A \neq P^A$ для случайного A неизвестно, так что остается надежда доказать, что $NP^A \cap \text{co-}NP^A \neq P^A$ для случайного A.

Таким образом, сравнение качественной теории алгоритмов и теории сложности вычислений относительно случайного оракула можно изобразить следующей таблицей.

Таблица

Теорема качественной теории алгоритмов	Существует перечислимое неразрешимое множество	Теорема Поста	Существует перечислимое, но не коперечислимое множество	Отделимость коперечислимых множеств	Неотделимость перечислимых множеств	Любое бесконечное перечислимое множество содержит бесконечное разрешимое подмножество	Существует простое множество
Верен ли аналог в теории сложности относительно случайного оракула	Да [2]	Неизвестно	Да [2]	Нет (данная работа)	Да (данная работа)	Нет [2]	Да (данная работа)

§ 2. Определения

Мы будем рассматривать подмножества множества $\mathbb{B}^*$ всех слов в бинарном алфавите $\mathbb{B} = \{0,1\}$ и называть их *языками*. *Оракулом* называется произвольная функция $A:\mathbb{B}^* \to \mathbb{B}$.

Пусть L – язык, а A – оракул. Говорят, что $L \in P^A$, если существует детерминированная полиномиальная машина Тьюринга M с оракулом такая, что $x \in L \leftrightarrow M^A(x) = 1$, где $M^A(x)$ обозначает результат, выданный M на входе x, если в качестве ответов оракула даются значения A. Говорят, что L принадлежит классу NP^A, если существуют полиномиальная (детерминированная) машина M с оракулом и полином p такие, что $x \in L \leftrightarrow \exists y \in \mathbb{B}^* \ (|y| = p(|x|) \& M^A(x,y) = 1)$, где $|u|$ обозначает длину слова u. Пару $N = (M,p)$ будем называть *недетерминированной* машиной и полагать

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

Через L_{N^A} обозначим язык $\{x \mid N^A(x)=1\}$.

Пусть L_1, L_2, L – языки. Говорят, что L *отделяет* L_1 и L_2, если $L_1 \subset L$ и $L_2 \subset \mathbb{B}^* \setminus L$. Пусть C и C' – два семейства языков. Будем говорить, что C–языки C'–*отделимы*, если для любых двух непересекающихся языков L_1 и L_2 из C существует язык L из C', отделяющий L_1 и L_2. В противном случае будем говорит, что C–языки C'–*неотделимы*. Пусть $S(A)$ – некоторое свойство оракула A. Мы говорим, что *для случайного* A *выполнено* $S(A)$, если с вероятностью 1 при равномерном распределении на оракулах выполнено свойство $S(A)$.

§ 3. Результаты

ТЕОРЕМА 1. *Для случайного оракула* A NP^A*–языки* P^A*–неотделимы.*

ДОКАЗАТЕЛЬСТВО. Введем некоторые технические понятия. Зафиксируем некоторую последовательность натуральных чисел s_i (какую именно, определим позднее). Обозначим через t_i i–этажную двойку, т.е. $t_0=1$ и $t_{i+1}=2^{t_i}$. Пусть $i \in \mathbb{N}$ и w – какое-то бинарное слово длины $2t_i-\log_2 t_i$. Рассмотрим множество

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

из t_i слов длины $2t_i$. Упорядочим лексикографически все слова длины $2t_i-\log_2 t_i$. Будем называть i–*блоками* множества вида B_w, где номер w в лексикографическом упорядочении не превосходит $2s_i$. Последовательность s_i будет удовлетворять неравенству $2s_i \leqslant 2^{2t_i-\log_2 t_i}$. Таким образом, мы будем иметь $2s_i$ i–блоков, каждый из t_i слов. Первые s_i i–блоков будем называть $i,0$–*блоками*, а остальные s_i i–блоков назовем $i,1$–*блоками*. Скажем, что оракул A *единичен в блоке* B, если $\forall u \in B\ A(u)=1$.

Сопоставим каждому оракулу A два NP^A–языка:

$L_0^A = \{1^{t_i} \mid i \in \mathbb{N}$ и A единичен в некотором $i,0$–блоке$\}$,

$L_1^A = \{1^{t_i} \mid i \in \mathbb{N}$ и A единичен в некотором $i,1$–блоке$\}$.

Подберем s_i таким, чтобы вероятность события $1^{t_i} \in L_0^A$ была равна примерно $1/i$. Вероятность того, что A не единичен в одном фиксированном i–блоке, равна $1-2^{-t_i}$. Поэтому

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

Положим $s_i=[2^{t_i}/i]$. Ясно, что $(1-2^{-t_i})^{s_i} = e^{-2^{-t_i}s_i(1+o(1))}$ при $i \to \infty$. Но

$$2^{-t_i}s_i = 2^{-t_i}[2^{t_i}/i] = \frac{1}{i}(1+o(1)).$$

Следовательно,

$$1-(1-2^{-t_i})^{s_i} = 1-e^{(-1/i)(1+o(1))} = 1-(1-\tfrac{1}{i}+o(\tfrac{1}{i})) = \tfrac{1}{i}+o(\tfrac{1}{i}).$$

Докажем, что с вероятностью 1 множество $L_0^A \cap L_1^A$ конечно. События $1^{t_i} \in L_0^A$ и $1^{t_i} \in L_1^A$ независимы, следовательно, для всех $i \in \mathbb{N}$

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

Ряд $\sum \frac{1}{i^2}$ сходится. Поэтому по лемме Бореля–Кантелли для случайного A существует лишь конечное множество таких i, что $1^{t_i} \in L_0^A \cap L_1^A$.

Положим $C^A=L_1^A\setminus L_0^A$. Тогда для случайного A язык C^A принадлежит NP^A (поскольку отличается от языка $L_1^A\in NP^A$ лишь на конечном множестве). Кроме того, C^A и L_0^A не пересекаются при всех A. Поэтому нам достаточно доказать, что для случайного A языки C^A и L_0^A не отделимы никаким языком из P^A. Нам достаточно доказать, что для любой полиномиальной детерминированной машины M вероятность события $\exists x\in\mathbb{B}^*\ (M^A(x)=1\&x\in L_0^A\vee M^A(x)=0\&x\in C^A)$ равна 1. Очевидно, для этого достаточно доказать, что для случайного A существует бесконечно много таких i, что

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

Обозначим для удобства выделенное событие через $P_i(A)$. Заметим, что события $P_i(A)$ могут быть зависимы.

Нам достаточно доказать, что для всех $k\in\mathbb{N}$ ряд

$$\sum_{i=k+1}^{\infty}\mathrm{Prob}[P_i(A)\,|\,\neg P_{i-1}(A)\&\ldots\&\neg P_{k+1}(A)\&\neg P_k(A)] \qquad (1)$$

расходится. Действительно, в этом случае для любого $k\in\mathbb{N}$

$$\mathrm{Prob}[\exists i\geqslant k\ P_i(A)] = 1-\mathrm{Prob}[\forall i\geqslant k\ \neg P_i(A)] =$$

$$= 1-\mathrm{Prob}[\neg P_k(A)]\prod_{i=k+1}^{\infty}\mathrm{Prob}[\neg P_i(A)\,|\,\neg P_{i-1}(A)\&\ldots\&\neg P_k(A)] =$$

$$= 1-\mathrm{Prob}[\neg P_k(A)]\prod_{i=k+1}^{\infty}(1-\mathrm{Prob}[P_i(A)\,|\,\neg P_{i-1}(A)\&\ldots\&\neg P_k(A)]).$$

Расходимость ряда (1) означает, что последнее бесконечное произведение равно нулю, следовательно, $\mathrm{Prob}[\exists i\geqslant k\ P_i(A)]=1$. Поэтому $\mathrm{Prob}[\forall k\ \exists i\geqslant k\ P_i(A)]=1$, т.к. пересечение счетного семейства множеств меры 1 имеет меру 1.

Чтобы доказать расходимость ряда (1), докажем, что при достаточно больших i

$$\mathrm{Prob}[P_i(A)\,|\,\neg P_{i-1}(A)\&\ldots\&\neg P_k(A)] > \frac{1}{2i}\ .$$

Обозначим через D_i множество всех слов длины $<2t_i$, а через F_i – множество всех функций из D_i в $\mathbb{B}$. Через $f\restriction M$ будем обозначать сужение функции f на множество M.

Событие $P_j(A)$ зависит только от значения A на словах длины, ограниченной некоторым полиномом от t_j (поскольку M на входе 1^{t_j} может задавать оракулу вопросы только полиномиальной от t_j длины, а событие $1^{t_j}\in L_0^A$ зависит только от значения A на словах длины $2t_j$). Поскольку $t_i=2^{t_{i-1}}$, при достаточно больших i событие $\neg P_{i-1}(A)\&\ldots\&\neg P_k(A)$ зависит только от $A\restriction D_i$. Поэтому нам достаточно доказать, что при всех $f\in F_i$ условная вероятность $\mathrm{Prob}[P_i(A)\,|\,A\restriction D_i=f]$ больше $\frac{1}{2i}$ при достаточно больших i. Зафиксируем некоторое $i\in\mathbb{N}$ и $f\in F_i$ и будем дальше рассматривать только такие A, что $A\restriction D_i=f$.

Запустим машину M с оракулом A на входе 1^{t_i} и будем записывать все слова длины $\geqslant 2t_i$, о которых M спрашивает оракул, и ответы оракула. Получим последовательность пар $\langle w_1,b_1\rangle,\ldots,\langle w_j,b_j\rangle$, где w_l – слова, а $b_l\in\mathbb{B}$. Будем называть эту последовательность *протоколом вычисления на* $1^{t_i},A$ и обозначать через Π_i множество всех возможных протоколов, т.е. $\Pi_i=\{\text{протокол } M \text{ на } 1^{t_i},A\,|\,A\restriction D_i=f\}$. Будем говорить, что оракул A согласован с протоколом $Z=(\langle w_1,b_1\rangle,\ldots,\langle w_j,b_j\rangle)$, если $A(w_1)=b_1,\ldots,A(w_j)=b_j$. Очевидно, A согласован с Z

тогда и только тогда, когда Z есть протокол вычисления на $1^{t_i}, A$. Достаточно доказать, что для достаточно больших i для любого протокола $Z \in \Pi_i$ выполнено

$$\mathrm{Prob}[P_i(A) \mid A \text{ согласован с } Z] > \frac{1}{2i} .$$

Зафиксируем некоторый протокол $Z \in \Pi_i$. Очевидно, протокол вычисления на $1^{t_i}, A$ полностью определяет $M^A(1^{t_i})$. Пусть, напр., $M^A(1^{t_i})=1$, если A согласован с Z. Тогда $\mathrm{Prob}[P_i(A) \mid A$ согласован с $Z] = \mathrm{Prob}[1^{t_i} \in L_0^A \mid A$ согласован с $Z]$. Пусть протокол Z состоит из j пар. Тогда последняя вероятность не меньше чем $1-(1-2^{-t_i})^{s_i-j}$. Поскольку j ограничено некоторым полиномом от t_i, а s_i сверхполиномиально растет с ростом t_i, имеем $1-(1-2^{-t_i})^{s_i-j} = \frac{1}{i}(1+o(1))$ при $i \to \infty$. Таким образом, при достаточно больших i $\mathrm{Prob}[P_i(A) \mid A$ согласован с $Z] > \frac{1}{2i}$, что и требовалось доказать. Теорема доказана.

ТЕОРЕМА 2. *Для случайного оракула A со-NP^A-языки P^A-неотделимы.*

ДОКАЗАТЕЛЬСТВО. Доказательство похоже на доказательство предыдущей теоремы, поэтому воспользуемся всеми понятиями и обозначениями предыдущего доказательства. Произведем следующие изменения. Положим $s_i = [c2^{t_i}\log_2 i]$, где c – рациональная константа, которую мы определим позднее (соответственно изменится и количество i-блоков). Положим

$L_0^A = \{1^{t_i} \mid i \in \mathbb{N}$ и A не единичен ни в каком $i,0$-блоке$\}$,

$L_1^A = \{1^{t_i} \mid i \in \mathbb{N}$ и A не единичен ни в каком $i,1$-блоке$\}$.

Нетрудно доказать, что s_i вычислимо за полиномиальное от t_i время, поэтому $L_0^A, L_1^A \in$ со-NP^A. Ясно, что

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

$$= e^{-2^{-t_i} s_i (1+o(1))} = e^{-c\log_2 i (1+o(1))} = i^{-c\log_2 e (1+o(1))} .$$

Число c возьмем таким, что $\frac{5}{8} < c\log_2 e < \frac{7}{8}$. Тогда $\mathrm{Prob}[1^{t_i} \in L_0^A] = \mathrm{Prob}[1^{t_i} \in L_1^A] < i^{-5/8}$ при достаточно больших i. Следовательно, $\mathrm{Prob}[1^{t_i} \in L_0^A \cap L_1^A] < i^{-5/4}$ при достаточно больших i, и поскольку ряд $\sum i^{-5/4}$ сходится, для случайного A множество $L_0^A \cap L_1^A$ конечно.

Далее рассуждаем в точности так же, как в предыдущем доказательстве до того места, где доказывается нижняя оценка условной вероятности $\mathrm{Prob}[P_i(A) \mid A \upharpoonright D_i = f]$. Напомним, нам нужно оценить эту вероятность снизу таким числом a_i, чтобы ряд $\sum a_i$ расходился. Теперь докажем, что при достаточно больших i выполнено

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

где $\mathrm{poly}(n)$ обозначает некоторый полином от n. Точнее, будем доказывать неравенство

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

Как и раньше, будем рассматривать далее только такие оракулы A, что $A \upharpoonright D_i = f$ (напомним, что f фиксировано).

Событие $\neg P_i(A)$ означает, что A единичен в некотором $i,(1-M^A(1^{t_i}))$-блоке. Пусть $Z = (\langle w_1, b_1\rangle, \ldots, \langle w_j, b_j\rangle)$ – протокол вычисления на $1^{t_i}, A$. Будем называть *A-свободными* бло-

ками все $i,(1-M^A(1^{t_i}))$-блоки, не пересекающиеся с $\{w_1,...,w_j\}$. Остальные $i,(1-M^A(1^{t_i}))$-блоки назовем *A-занятыми*. Представим событие $\neg P_i(A)$ как объединение двух событий:

$Q'(A)$ – "A единичен в некотором A-свободном блоке",

$Q''(A)$ – "A единичен в некотором A-занятом блоке".

Докажем сначала, что вероятность первого события не превосходит $1-(1-2^{-t_i})^{s_i}$. Как и раньше, достаточно доказать, что для любого протокола $Z\in\Pi_i$

$$\mathrm{Prob}[Q'(A)\,|\,A \text{ согласован с } Z] \leqslant 1-(1-2^{-t_i})^{s_i}.$$

Зафиксируем некоторый протокол $Z=(\langle w_1,b_1\rangle,...,\langle w_j,b_j\rangle)$. Пусть, напр., $M^A(1^{t_i})=1$, если A согласован с Z. Тогда если A согласован с Z, то событие $Q'(A)$ означает, что A единичен в некотором $i,0$-блоке, не пересекающемся с множеством $\{w_1,...,w_j\}$. Пусть количество $i,0$-блоков, не пересекающихся с $\{w_1,...,w_j\}$, равно k. Тогда $\mathrm{Prob}[Q'(A)\,|\,A$ согласован с $Z]=1-(1-2^{-t_i})^k$. Поскольку $k\leqslant s_i$, неравенство доказано. Из определения s_i следует, что при достаточно больших i выполнено $1-(1-2^{-t_i})^{s_i}<1-i^{-7/8}$.

Теперь докажем, что

$$\mathrm{Prob}[Q''(A)] \leqslant 2^{-t_i}\mathrm{poly}(t_i).$$

Если слово u принадлежит одному из i-блоков, то обозначим через $B(u)$ i-блок, содержащий u. Обозначим через $R(A)$ событие "найдутся такие m и протокол $Z=(\langle w_1,b_1\rangle,...,\langle w_j,b_j\rangle)$ с $j\geqslant m$, что выполнено (а)&(б)&(в)",где(а)-(в) – это следующие события:

(а) – "w_m принадлежит одному из i-блоков и A единичен в $B(w_m)$";

(б) – "$\forall i<m \quad w_i\notin B(w_m)$";

(в) – "$\forall i<m \quad A(w_i)=b_i$".

Очевидно, событие $Q''(A)$ включено в событие $R(A)$. Докажем, что $\mathrm{Prob}[R(A)]\leqslant 2^{-t_i}\mathrm{poly}(t_i)$. Сначала докажем, что при любых фиксированных $m\leqslant j$, $Z=(\langle w_1,b_1\rangle,...,\langle w_j,b_j\rangle)$ выполнено $\mathrm{Prob}[(а)\&(б)\&(в)]\leqslant 2^{-m+1}2^{-t_i}$. Зафиксируем m, j, Z. Истинность события (б) зависит только от m, Z. Если при зафиксированных m, Z событие (б) ложно, то неравенство очевидно, поскольку его левая часть равна нулю. Если (б) истинно, то события (а) и (в) независимы, поэтому $\mathrm{Prob}[(а)\&(б)\&(в)]=\mathrm{Prob}[(а)]\mathrm{Prob}[(в)]=2^{-t_i}2^{-m+1}$.

Зафиксируем некоторое m. Докажем, что вероятность события "найдется протокол $Z=(\langle w_1,b_1\rangle,...,\langle w_j,b_j\rangle)$ из Π_i с $j\geqslant m$, для которого выполнено (а)-(в)" не превосходит 2^{-t_i}. Назовем m-началом протокола $Z=(\langle w_1,b_1\rangle,...,\langle w_j,b_j\rangle)$ последовательность $\langle w_1,b_1\rangle,...,\langle w_{m-1},b_{m-1}\rangle,w_m$. Ясно, что количество различных m-начал протоколов из Π_i не превосходит 2^{-m+1}. Истинность (а)-(в) зависит только от A и m-начала Z. Поэтому вероятность указанного события не превосходит $2^{m-1}(2^{-t_i}2^{-m+1})=2^{-t_i}$. Пусть $k=\mathrm{poly}(t_i)$ – максимальная длина протокола из Π_i. Тогда $\mathrm{Prob}[R(A)]\leqslant 2^{-t_i}k$. Теорема доказана.

ТЕОРЕМА 3. *Для случайного оракула A существует бесконечный* co-NP^A*-язык, не имеющий бесконечных подмножеств из* NP^A.

ДОКАЗАТЕЛЬСТВО. Воспользуемся всеми обозначениями предыдущих доказательств, сделав следующие изменения. Положим $s_i=2^{t_i}$. Будем рассматривать только $i,0$-блоки, называя

их теперь просто i-блоками. Рассмотрим со-NP^A-язык $L^A=\{1^{t_i} \mid A$ не единичен ни в одном из i-блоков$\}$. Очевидно, для случайного A язык L^A бесконечен, поскольку $\mathrm{Prob}[1^{t_i} \in L^A] = (1-2^{-t_i})^{2^{t_i}} \longrightarrow e^{-1}$ при $i \longrightarrow \infty$.

Докажем, что для случайного A язык L^A не имеет бесконечных подмножеств из NP^A. Для этого достаточно доказать, что для любой недетерминированной машины N вероятность события "L_{N^A} бесконечен и $L_{N^A} \subset L^A$" меньше 3/4. Действительно, допустим, что вероятность события "L^A имеет бесконечное подмножество из NP^A" положительна. Тогда для некоторой недетерминированной машины N положительна вероятность события "L_{N^A} бесконечен и $L_{N^A} \subset L^A$". Назовем конусом любое множество оракулов вида $\{A \mid A(w_1)=b_1,\ldots,A(w_j)=b_j\}$, где $w_1,\ldots,w_j \in \mathbb{B}^*$, $b_1,\ldots,b_j \in \mathbb{B}$. Если мера множества оракулов S положительна, то существует конус Γ такой, что мера множества $S \cap \Gamma$ больше 3/4 меры Γ. Следовательно, существует конус Γ такой, что $\mathrm{Prob}[A \in \Gamma \cap S \mid A \in \Gamma] > 3/4$, где S – это множество оракулов, для которых $L_{N^A} \subset L^A$ и L_{N^A} бесконечен. Пусть $\Gamma=\{A \mid A(w_1)=b_1,\ldots,A(w_j)=b_j\}$. Определим новую недетерминированную машину N_1 следующим образом. Для любого оракула A обозначим через $\tilde{A}$ оракул

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

Пусть k – максимальная длина слова из множества $\{w_1,\ldots,w_j\}$. Нетрудно построить недетерминированную машину N_1 такую, что

$$N_1^A(x) = \begin{cases} 0, & \text{если } |x| \leqslant 2k; \\ N^{\tilde{A}}(x), & \text{если } |x| > 2k. \end{cases}$$

Очевидно, если $\tilde{A} \in S$, то $L_{N_1^A} \subset L^A$ и $L_{N_1^A}$ бесконечен. Поэтому $\mathrm{Prob}[L_{N_1^A} \subset L^A,\ L_{N_1^A}$ бесконечен$] \geqslant \mathrm{Prob}[\tilde{A} \in S] = \mathrm{Prob}[A \in S \mid A \in \Gamma] > 3/4$.

Итак, пусть N – произвольная недетерминированная машина. Докажем, что вероятность события "$L_{N^A} \subset L^A$ и L_{N^A} бесконечен" не превосходит 3/4. Ясно, что достаточно доказать

$$\mathrm{Prob}[\exists^\infty i\ N^A(1^{t_i})=1,\ \forall i(N^A(1^{t_i})=1 \longrightarrow 1^{t_i} \in L^A)] \leqslant 3/4. \qquad (2)$$

Допустим (2) ложно. Тогда $\mathrm{Prob}[\exists^\infty i\ N^A(1^{t_i})=1] > 3/4$, следовательно, для всех $k \in \mathbb{N}$ выполнено

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

Докажем, что если k достаточно велико, то при всех $i \geqslant k$

$$\mathrm{Prob}[1^{t_i} \notin L^A \mid N^A(1^{t_i})=1 \,\&\, \forall j \in \{k,\ldots,i-1\} N^A(1^{t_j})=0] > 1/2. \qquad (3)$$

Если это уже доказано, то при достаточно больших k получим

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

События, вероятности которых суммируются в последней формуле, не пересекаются, и каждое из них включено в событие $\exists i \geq k$ $(1^{t_i} \notin L^A \& N^A(1^{t_i})=1)$. Значит, вероятность последнего события не меньше 3/8, и мы получаем противоречие, т.к. по предположению вероятность этого события меньше 1/4.

Итак, докажем, что при достаточно больших k при всех $i \geq k$ выполнено (3). Зафиксируем k и $i \geq k$. Достаточно доказать, что при всех $f \in F_i$ выполнено неравенство

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

Пусть машина N есть пара (p,M), где p – полином, а M – детерминированная полиномиальная машина. Количество вопросов M к оракулу, задаваемых на входе вида $1^{t_i},y$, $|y| = p(t_i)$, ограничено некоторым полиномом от t_i. Обозначим через q этот полином и положим $r=q(t_i)$. Назовем окрестностью любое множество оракулов вида

$$\{A \,|\, A \restriction D_i = f,\ A \restriction B_1 = f_1, \ldots,\ A \restriction B_j = f_j,\ A \restriction E = g\}, \tag{4}$$

где $B_1,\ldots,B_j$ – некоторые i-блоки, $j \leq r$, $f_1,\ldots,f_j$ – соответственно функции из $B_1,\ldots,B_j$ в $\mathbb{B}$, E – конечное множество слов, не пересекающееся с D_i и ни с одним из i-блоков, а $g: E \to \mathbb{B}$. Тогда множество $\{A \,|\, N^A(1^{t_i})=1,\ A \restriction D_i = f\}$ можно представить как конечное объединение окрестностей, напр., $\Gamma_1 \cup \ldots \cup \Gamma_n$.

Итак, нам нужно доказать, что $\mathrm{Prob}\left[1^{t_i} \notin L^A \,\middle|\, A \in \Gamma_1 \cup \ldots \cup \Gamma_n\right] > 1/2$. Назовем окрестность вида (4) плохой, если f_l – тождественно единичная функция для некоторого $l \leq j$. Любой оракул A из плохой окрестности удовлетворяет свойству $1^{t_i} \notin L^A$, поэтому при удалении из объединения $\Gamma_1 \cup \ldots \cup \Gamma_n$ всех плохих окрестностей вероятность

$$\mathrm{Prob}\left[1^{t_i} \notin L^A \,\middle|\, A \in \Gamma_1 \cup \ldots \cup \Gamma_n\right] \tag{5}$$

может только уменьшиться. Будем поэтому считать, что среди $\Gamma_1,\ldots,\Gamma_n$ нет плохих окрестностей, и оценим в этом случае вероятность (5) снизу. Представим эту вероятность как сумму

$$\sum_{m=1}^{n} \mathrm{Prob}\left[A \text{ единичен в некотором } i\text{-блоке} \;\middle|\; A \in \Gamma_m \setminus (\Gamma_{m-1} \cup \ldots \cup \Gamma_1)\right] \times$$

$$\times\ \mathrm{Prob}\left[A \in \Gamma_m \setminus (\Gamma_{m-1} \cup \ldots \cup \Gamma_1) \,\middle|\, A \in \Gamma_1 \cup \ldots \cup \Gamma_n\right].$$

Очевидно, достаточно доказать, что для всех $m \leq n$ выполнено

$$\mathrm{Prob}\left[A \text{ единичен в некотором } i\text{-блоке} \;\middle|\; A \in \Gamma_m \setminus (\Gamma_{m-1} \cup \ldots \cup \Gamma_1)\right] \geq 1-(1-2^{-t_i})^{s_i-r}.$$

Зафиксируем некоторое $m \leq n$. Пусть Γ_m задается выражением (4). Пусть $C_1,\ldots,C_{s_i-j}$ – это все i-блоки, не входящие в множество $\{B_1,\ldots,B_j\}$. Обозначим для $l \leq s_i - j$ через p_l вероятность $\mathrm{Prob}[A$ единичен в $C_l \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \ldots \cup \Gamma_{m-1}),\ A$ не единичен в блоках $C_1,\ldots,C_{l-1}]$. Тогда вероятность (5) равна $1-(1-p_1)(1-p_2)\ldots(1-p_{s_i-j})$. Докажем, что для любого $l \leq s_i - j$ выполнено $p_l \geq 2^{-t_i}$. Зафиксируем произвольное $l \leq s_i - j$. Обозначим для произвольного оракула A через $\tilde{A}$ оракул

$$\tilde{A}(u) = \begin{cases} 1, & \text{если } u \in C_l; \\ A(u) & \text{иначе.} \end{cases}$$

Нетрудно проверить, что множество

$$U = \{A \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \ldots \cup \Gamma_{m-1}),\ A \text{ не единичен } C_1,\ldots,C_{t-1}\}$$

обладает свойством "$A \in U \longrightarrow \tilde{A} \in U$". Ясно, что для любого множества U положительной меры, обладающего этим свойством, выполнено $\mathrm{Prob}[A \text{ единичен в } C_t \mid A \in U] \geq 2^{-t_i}$. Осталось заметить, что если i достаточно велико, то $1-(1-2^{-t_i})^{s_i-r} > 1/2$. Теорема доказана.

ЛИТЕРАТУРА

1. Baker T., Gill J., Solovay R. *Relativizations of the P=?NP question* // SIAM J. Comput. – 1975. – V.4. – №4. – P.431–442.

2. Bennett C.H., Gill J. *Relative to a random oracle A*: $P^A \neq NP^A = \text{co-}NP^A$ *with probability* 1 // SIAM J. Comput. – 1981. – V.10. – №1. – P.96–113.

3. Верещагин Н.К. *Относительно случайного оракула существуют P–неотделимые NP–множества и co–NP–множества* // Тезисы докл. вторых математических чтений памяти М.Я.Суслина. Саратов, 1991. – С.13.

г.Москва

Поступила
07.10.1992