УДК 510.52

Оракульное отделение некоторых сложностных классов и нижние оценки сложности персептронов, решающих некоторые проблемы отделения *

Н.К. Верещагин

В первой части настоящей работы доказано, что относительно случайного оракула существуют бесконечные множества в NP, которые не имеют бесконечных Co-NP-подмножеств (Co-NP-иммунные NP-множества). Во второй части работы доказано, что любой персептрон, отделяющий булевы матрицы, в которых каждая строка содержит хотя бы одну единицу, от матриц, в которых многие строки (скажем, 99%) состоят из одних нулей, должен иметь большой порядок или большой общий вес. Этот результат развивает известную теорему «один в блоке» Минского и Пейперта, утверждающую, что никакой персептрон маленького порядка не может по булевской матрице выяснить, содержит ли каждая её строка хотя бы одну единицу. В качестве следствия мы доказываем, что $\mathrm{AM} \cap \text{Co-AM} \not\subseteq \mathrm{PP}$ относительно некоторого оракула.

Библиография: 21 наименование.

*Предварительные варианты частей настоящей работы были опубликован в сборнике докладов конференции *Third Israel Symposium on Theory of Computing and Systems (ISTCS'95)*.

[0]Работа выполнена при поддержке гранта Американского математического общества, гранта MQT000 Международного научного фонда, гранта фонда «Культурная инициатива» и NSF-гранта CCR-8957604. Работа выполнена частично во время пребывания в университете г. Рочестера.

§ 1. Введение

В настоящей работе изучаются вопросы оракульного отделения различных сложностных классов и связанные с этим комбинаторные проблемы.

Многие важные проблемы теории сложности вычислений остаются открытыми. Наиболее известная из них — совпадают ли классы P и NP. Неизвестно также, верно ли, что NP = Co-NP, и верно ли, что $\mathrm{NP} \cap \mathrm{Co\text{-}NP} = \mathrm{P}$.

В работе [2] было показано, что эти проблемы не имеют релятивизуемого решения. Иными словами, были построены такие оракулы A и B, что $\mathrm{P}^A = \mathrm{NP}^A$ (и, следовательно, $\mathrm{P}^A = \mathrm{NP}^A \cap \mathrm{Co\text{-}NP}^A$) и $\mathrm{NP}^B \neq \mathrm{Co\text{-}NP}^B$ (и, следовательно, $\mathrm{P}^B \neq \mathrm{NP}^B$). Используя ту же технику, можно построить оракул C, для которого $\mathrm{NP}^C \cap \mathrm{Co\text{-}NP}^C \neq \mathrm{P}^C$. Эти результаты имеют отрицательный характер: они показывают, что известная к тому времени техника неприменима к решению указанных проблем, поскольку эта техника релятивизуема.

Так как соотношение между классами $\mathrm{Co\text{-}NP}^A$, NP^A и P^A зависит от оракула A, естественно выяснить, что имеет место относительно «типичного» оракула? Этому вопросу посвящена первая часть настоящей работы.

Одним из возможных уточнений понятия типичности является понятие генеричности в бэровской топологии. Другим возможным уточнением понятия типичности является понятие случайности по равномерной мере. В настоящей работе мы выбираем в качестве такого уточнения случайность, т.е. мы изучаем соотношение классов NP^A, $\mathrm{Co\text{-}NP}^A$ и P^A для оракула A, случайного по равномерной мере. Точнее, мы говорим, что некоторое утверждение $S(A)$ выполнено для случайного A, или для почти всех A, если равномерная мера множества $\{A \mid S(A)\}$ равна 1. Все свойства $S(A)$ оракула, о которых идет речь в настоящем параграфе, обладают следующими двумя свойствами: множество $\{A \mid S(A)\}$ измеримо и $S(A)$ устойчиво относительно конечных изменений A. По 0-1-закону А.Н. Колмогорова для всех таких свойств, или $S(A)$ выполнено для случайного A, или $\neg S(A)$ выполнено для случайного A.

Изучение соотношений между рассматриваемыми классами относительно случайного оракула было начато в работе [5], где было доказано, что $\mathrm{P} \neq \mathrm{NP} \neq \mathrm{Co\text{-}NP}$ относительно случайного оракула. Там же было доказано, что относительно случайного оракула существуют P-

иммунные NP-множества, т.е. бесконечные NP-множества, не имеющие бесконечных P-подмножеств. В [18] было показано, что относительно случайного оракула существуют как P-неотделимые NP-множества, так и P-неотделимые Co-NP-множества. Там же доказано, что относительно случайного оракула класс Co-NP содержит NP-иммунные множества.

Посмотрим на эти результаты с точки зрения аналогии между качественной теорией алгоритмов и теорией сложности вычислений (количественной теорией алгоритмов). По этой аналогии множества из класса P соответствуют разрешимым множествам, множества из класса NP соответствуют перечислимым множествам, а множества из Co-NP соответствуют дополнениям перечислимых множеств, т.е. коперечислимым множествам. Точнее, мы рассматриваем аналогию между качественной теорией алгоритмов и теорией сложности вычислений, «релятивизованной случайным оракулом». В нашем случае разрешимым множествам соответствуют P^A-множества, перечислимым множествам соответствуют NP^A-множества и коперечислимым множествам соответствуют Co-NP^A-множества, где A — «случайный оракул». Таким образом, аналоги следующих теорем качественной теории алгоритмов верны в теории сложности вычислений относительно случайного оракула: аналог теоремы о существовании перечислимого неразрешимого множества, аналог теоремы о существовании коперечислимого неперечислимого множества, аналог теоремы о существовании перечислимых неотделимых множеств и аналог теоремы о существовании простого множества (перечислимого множества, дополнение которого бесконечно, но не имеет бесконечных перечислимых подмножеств). Аналоги следующих теорем ложны: аналог теоремы о том, что любое бесконечное перечислимое множество имеет бесконечное разрешимое подмножество и аналог теоремы об отделимости коперечислимых множеств.

Остаётся открытой проблема, верен ли аналог теоремы Поста о разрешимости всех перечислимых и одновременно коперечислимых множеств, т.е. неизвестно, верно ли, что $\mathrm{NP} \cap \text{Co-NP} = \mathrm{P}$ относительно случайного оракула. Как замечено в [6], если $\mathrm{NP} \cap \text{Co-NP} = \mathrm{P}$ относительно случайного оракула, то $\mathrm{AM} \cap \text{Co-AM} = \mathrm{BPP}$ (без оракулов), в частности, проблема изоморфизма графов принадлежит BPP. Таким образом, мало надежд на то, что $\mathrm{NP} \cap \text{Co-NP} = \mathrm{P}$ относительно случайного оракула. Никаких абсолютных следствий утверждения «$\mathrm{NP}^A \cap \text{Co-NP}^A \neq \mathrm{P}^A$ для случайного A» неизвестно, таким образом, остаётся надежда доказать,

что $\mathrm{NP} \cap \mathrm{Co\text{-}NP} \neq \mathrm{P}$ относительно случайного оракула.

До сих пор оставалось неизвестным, содержит ли класс NP Co-NP-иммунные множества относительно случайного оракула. Как уже было сказано, существование P-иммунных NP-множеств относительно случайного оракула доказано в [5]. Некоторый прогресс в решении этой проблемы был достигнут в работе [12], где было показано, что относительно случайного оракула существует бесконечное NP-множество, все Co-NP-подмножества которого в некотором смысле «тонки».

В настоящей работе мы решаем эту проблему: мы доказываем, что класс NP содержит Co-NP-иммунные множества относительно случайного оракула. Более того, мы доказываем, что относительно случайного оракула существуют язык $L \in \mathrm{P}$ и NP-язык $L_1 \subseteq L$ такие, что и L_1, и $L \setminus L_1$ бесконечны, но при этом L_1 не имеет бесконечных Co-NP-подмножеств, а $L \setminus L_1$ не имеет бесконечных NP-подмножеств. Отсюда, в частности, вытекает теорема из [18] о том, что относительно случайного оракула класс Co-NP содержит NP-иммунные множества.

Все результаты, о которых упоминалось выше, собраны в табл. 1. Для сравнения в ней приведены также результаты о генерическом оракуле.

Таблица 1.

	Относит. случайного оракула	Относит. генерич. оракула	Качеств. теория алг-мов
$\mathrm{P} \neq \mathrm{NP}$	+	+	+
$\mathrm{NP} \neq \mathrm{Co\text{-}NP}$	+	+	+
NP-множ-ва P-неотделимы	+	?	+
Co-NP-множ-ва P-неотделимы	+	+	−
$\mathrm{P} = \mathrm{NP} \cap \mathrm{Co\text{-}NP}$	?	?	+
NP имеет P-иммунные мн-ва	+	−	−
NP имеет Co-NP-имм. мн-ва	+	−	−
Co-NP имеет NP-имм. мн-ва	+	+	+

Во второй части работы мы доказываем, что относительно некоторого оракула класс AM не включён в класс PP и изучаем сложность

связанной с этим проблемы отделения для персептронов (определения будут даны ниже).

Персептроном называется схема глубины 2 с пороговой вершиной в корне (т.е., вершиной, помеченной некоторым целым числом, называемым её порогом) и с вершинами, помеченными конъюнкциями (И-вершинами), на втором уровне. Каждый вход пороговой вершины помечен целым числом (возможно, отрицательным), называемым его *весом*. Входами И-вершин являются булевские переменные и их отрицания. Персептрон выдаёт единицу, если сумма весов всех истинных входов корневой вершины больше её порога, и выдаёт 0 в противном случае.

Порядком персептрона называется максимальная входная степень его И-вершин. *Размер* персептрона — это количество его И-вершин. *Весом* персептрона называется максимум абсолютных величин весов, которыми помечены входы его пороговой вершины, а *общим весом* — сумма абсолютных величин его весов.

Персептроны изучались Минским и Пейпертом в монографии [19]. Среди результатов, полученных ими, нам хотелось бы выделить две теоремы о нижних оценках порядка персептронов, вычисляющих некоторые булевы функции. Первая теорема гласит о том, что персептрон, вычисляющий сумму n булевских переменных по модулю 2, должен иметь порядок по крайней мере n. Вторая теорема утверждает, что персептрон, распознающий, все ли ряды данной булевой матрицы размера $n \times 4n^2$ содержат по крайней мере одну единицу, имеет порядок не меньше n (теорема «один в блоке»). Бигел в работе [3] построил булеву функцию n переменных, вычислимую некоторым персептроном экспоненциального (от n) общего веса и порядка 1, но не вычислимую персептронами квазиполиномиального ($2^{\mathrm{poly}(\log_2(n))}$) общего веса и полилогарифмического ($\mathrm{poly}(\log_2(n))$) порядка. Точнее, он получил нижнюю оценку $d^2 \log_2 w = \Omega(n)$ на порядок d и общий вес w персептронов, вычисляющих эту функцию.

В настоящей работе мы развиваем теорему «один в блоке» Минского и Пейперта в следующем направлении. Пусть П обозначает следующую проблему отделения: отделить булевы матрицы, в которых каждый ряд содержит по крайней мере одну единицу от булевых матриц, в которых много рядов (скажем, 99%) содержат одни нули. Очевидно, любой персептрон, распознающий, содержит ли данная булева матрица 1 в каждом ряду, также решает проблему П. Основная теорема настоящей работы

утверждает, что проблему П невозможно решить, используя персептроны порядка $o(\sqrt{m})$ и одновременно общего веса $2^{o(n)}$, где n — количество рядов, а m это количество столбцов матрицы (теорема 5). Из этого следует, что персептроны полилогарифмического порядка и квазиполиномиального общего веса не могут решить проблемы П. Предварительный вариант работы опубликован в препринте [15] и в сборнике докладов [16]. Доказательство основной теоремы, приведенное здесь, существенно проще доказательства из [15]. В частности, оно не использует теоремы Рисса из функционального анализа, использованной в [15]. Вместо этого настоящее доказательство использует более простую теорему двойственности из теории линейного программирования. И сама нижняя оценка, доказываемая в настоящей работе, лучше аналогичной оценки из [15].

Необходимость доказательства того, что персептроны полилогарифмического порядка и квазиполиномиального общего веса не могут решать те или иные проблемы, часто возникает по следующей причине. При переходе от недетерминированных машин с оракулом к схемам из функциональных элементов в стиле Фёрста, Сэйкса и Сипсера [11] полиномиальные по времени машины соответствуют схемам глубины 2 квазиполиномиального размера, веса 1 и полилогарифмического порядка с вершиной, помеченной ИЛИ, в корне (булевскими переменными являются значения оракула на словах длины не более заданного числа). Недетерминированным полиномиальным оракульным машинам с каким-нибудь другим механизмом принятия входа соответствуют схемы глубины 2 квазиполиномиального размера, веса 1 и полилогарифмического порядка с соответствующей вершиной в корне. В частности, PP-машинам соответствуют персептроны полилогарифмического порядка, квазиполиномиального размера и веса 1. Поэтому, чтобы построить оракул, относительно которого некоторый сложностной класс не включен в класс PP, достаточно доказать, что персептроны указанной сложности не могут решить соответствующую этому классу проблему отделения. (Например, чтобы построить оракул, относительно которого класс AM не включен в PP, достаточно доказать, что персептроны указанной сложности не могут отделить булевские матрицы, в которых по крайней мере 2/3 строк содержат хоть одну единицу, от булевых матриц, в которых не более 1/3 строк содержат 1.) Если уж удаётся доказать, что персептроны указанной сложности не могут решить ту или иную проблему

отделения, то это удаётся сразу доказать и для персептронов полилогарифмического порядка и квазиполиномиального общего веса.

Таким образом, из теоремы Минского и Пейперта о порядке персептронов, вычисляющих функцию сложения по модулю 2, следует существование оракула, относительно которого $\oplus\mathrm{P} \not\subseteq \mathrm{PP}$. А из теоремы «один в блоке» следует, что $\mathrm{NP}^{\mathrm{NP}} \not\subseteq \mathrm{PP}$ относительно некоторого оракула [10]. Приведенный выше результат Бигела показывает, что $\mathrm{P}^{\mathrm{NP}} \not\subseteq \mathrm{PP}$ относительно некоторого оракула [3]. А наш результат о проблеме отделения П даёт оракул, относительно которого $\mathrm{AM} \not\subseteq \mathrm{PP}$. Небольшое усиление этого результата показывает, что существует оракул, относительно которого $\mathrm{AM} \cap \mathrm{Co\text{-}AM} \not\subseteq \mathrm{PP}$ [14].

Класс PP интересен по следующим трём причинам. Во-первых, этот класс имеет следующую интерпретацию. Случайный вход r вероятностной машины M, распознающей язык L из PP, можно рассматривать как избирателя, при этом результат $M(x, r)$, выдаваемый машиной M на входе x и случайном входе r, можно считать мнением избирателя r о том, входит ли x в L. С этой точки зрения, класс PP — это класс таких языков L, что принадлежность слова x к L может быть определена голосованием среди $2^{\mathrm{poly}(|x|)}$ избирателей, причём время определения мнения каждого избирателя равномерно ограничено некоторым полиномом.

Во-вторых, как показано в [13], класс PP оказался неожиданно богатым: все языки из полиномиальной иерархии PH сводятся по Тьюрингу к PP-полному языку.

В-третьих, класс PP замкнут относительно полиномиальной табличной сводимости (см. [4], [9]). Таким образом, класс PP имеет довольно регулярную структуру.

§ 2. Определения

Языком называется любое подмножество множества $\mathbf{B}^*$ всех слов в алфавите $\mathbf{B} = \{0, 1\}$. *Оракул* — это произвольная функция из $\mathbf{B}^*$ в $\mathbf{B}$.

Машиной Тьюринга с оракулом называется машина Тьюринга, имеющая дополнительную ленту, называемую оракульной, на которой имеется читающе-записывающая головка. Будем считать, что эта головка может записывать только 0 и 1. Если машина приходит в некоторое выделенное состояние, то содержимое оракульной ленты от первой ячейки

до той ячейки, где находится головка, воспринимается как вопрос к оракулу и на оракульной ленте за единицу времени появляется «ответ оракула» — 0 или 1 в той ячейке, где находится головка. Время записи вопроса входит в общее время. Пусть M машина с оракулом, а A — оракул. Обозначим через $M^A(x)$ результат работы M на x, если в качестве ответа оракула на вопрос z дается $A(z)$.

Пусть A — оракул. Класс P^A состоит из всех языков L таких, что существует детерминированная полиномиальная по времени машина Тьюринга[1] M такая, что $x \in L \Leftrightarrow M^A(x) = 1$. Класс NP^A состоит из языков L таких, что существуют детерминированная полиномиальная по времени машина Тьюринга M и полином p такие, что

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

где $|u|$ обозначает длину слова u. Пару $N = \langle M, p\rangle$ будем называть *полиномиальной недетерминированной* машиной и будем обозначать

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

Возможным вычислением машины N на входе x будем называть вычисление M на любом входе вида $\langle x, y\rangle$, где $|y| = p(|x|)$. Обозначим через L_{N^A} язык $\{x \in \mathbf{B}^* \mid N^A(x) = 1\}$.

О п р е д е л е н и е 1. $L \in \mathrm{AM}$ [$L \in \mathrm{AM}^A$], если существуют полином p и полиномиально вычислимый [относительно A] предикат $Q(x, r, s)$ такие, что

$$\begin{aligned} x \in L &\Rightarrow \mathrm{Prob}_r[\exists s \in \mathbf{B}^{p(|x|)} Q(x, r, s)] > 2/3, \\ x \notin L &\Rightarrow \mathrm{Prob}_r[\exists s \in \mathbf{B}^{p(|x|)} Q(x, r, s)] < 1/3, \end{aligned}$$

где вероятность берётся по равномерному распределению на $\mathbf{B}^{p(|x|)}$.

О п р е д е л е н и е 2. $L \in \mathrm{MA}$, если существуют полином p и полиномиально вычислимый предикат $Q(x, r, s)$ такие, что

$$\begin{aligned} x \in L &\Rightarrow \exists s \in \mathbf{B}^{p(|x|)} \ \mathrm{Prob}_r[Q(x, r, s)] > 2/3, \\ x \notin L &\Rightarrow \forall s \in \mathbf{B}^{p(|x|)} \ \mathrm{Prob}_r[Q(x, r, s)] < 1/3, \end{aligned}$$

[1] В настоящей работе мы рассматриваем только машины с оракулом.

где вероятность берётся по равномерному распределению на $\mathbf{B}^{p(|x|)}$.

О п р е д е л е н и е 3. Язык L принадлежит классу PP, если существует полиномиальная по времени вероятностная машина Тьюринга T такая, что $x \in L \Leftrightarrow \mathrm{Prob}[T(x) = 1] > 1/2$.

В работе [1] доказано, что MA $\subseteq$ AM. Доказательство релятивизуемо. В [14] доказано, что MA $\subseteq$ PP. Доказательство также релятивизуемо.

Пусть L_1, L_2 и L — языки. Мы говорим, что L *отделяет* L_1 от L_2, если $L_1 \subseteq L$ и $L_2 \subseteq \mathbf{B}^* \setminus L$. Пусть $\mathcal{C}$ и $\mathcal{C}'$ — семейства языков. Мы говорим, что $\mathcal{C}$-языки $\mathcal{C}'$-отделимы, если для любых непересекающихся языков L_1 и L_2 из $\mathcal{C}$ существует язык L из $\mathcal{C}'$, отделяющий L_1 от L_2. В противном случае мы говорим, что $\mathcal{C}$-языки $\mathcal{C}'$-неотделимы. Язык называется $\mathcal{C}$-иммунным, если он бесконечен, но не содержит бесконечных подмножеств, принадлежащих $\mathcal{C}$.

Пусть $S(A)$ — некоторое свойство оракулов. Мы говорим, что $S(A)$ выполнено для случайного A, или для почти всех A, если равномерная мера множества $\{A \mid S(A)\}$ равна 1.

§ 3. Результаты о случайном оракуле

ТЕОРЕМА 1. *Относительно случайного оракула существуют язык $L \in P$ и* NP*-язык $L_1 \subseteq L$ такие, что L_1 является* Co-NP*-иммунным, а $L \setminus L_1$ является* NP*-иммунным.*

Д о к а з а т е л ь с т в о. Определим последовательность натуральных чисел $\{t_i\}$ по индукции: $t_0 = 1$, $t_{i+1} = 2^{t_i}$. Пусть i — натуральное число. *i-блоком* называется любое множество вида

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

где w — двоичное слово длины t_i. Таким образом, каждый i-блок состоит из t_i слов длины $t_i + \log_2 t_i$.

Положим

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

Скажем, что оракул A является *нулевым в блоке* B, если $\forall u \in B \quad A(u) = 0$.

Для любого оракула A положим

$$\begin{aligned} L_1^A &= \{1^{t_i} \mid i \in \mathbf{N} \text{ и } A \text{ является нулевым в некотором } i\text{–блоке}\}, \\ L_0^A &= L \setminus L_1^A. \end{aligned}$$

Очевидно, что $L \in \mathrm{P}^A$ и $L_1^A \in \mathrm{NP}^A$ для всех A.

Оба языка L_0^A и L_1^A бесконечны для почти всех A, поскольку

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

при $i \to \infty$.

Докажем, что

1) L_0^A не содержит бесконечных NP^A-подмножеств для почти всех A и

2) L_1^A не содержит бесконечных $\mathrm{Co\text{-}NP}^A$-подмножеств для почти всех A.

Мы утверждаем, что вместо 1) достаточно доказать следующее утверждение

1′) существует такое $c < 1$, что для любой полиномиальной недетерминированной машины N вероятность события «язык L_{N^A} бесконечен и $L_{N^A} \subseteq L_0^A$» меньше c,

а вместо 2) достаточно доказать следующее утверждение

2′) существует $c < 1$ такое, что для каждой полиномиальной недетерминированной машины N вероятность события «язык $\mathbf{B}^* \setminus L_{N^A}$ бесконечен и $\mathbf{B}^* \setminus L_{N^A} \subseteq L_1^A$» меньше c.

Докажем импликацию 1′) $\Rightarrow$ 1). Допустим, что 1′) истинно, но вероятность события «язык L_0^A содержит бесконечное NP^A-подмножество» положительна. Тогда существует полиномиальная недетерминированная машина N такая, что вероятность события «язык L_{N^A} бесконечен и $L_{N^A} \subseteq L_0^A$» положительна. Назовём *интервалом* любое множество оракулов вида

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

где $w_1, \ldots, w_j \in \mathbf{B}^*, b_1, \ldots, b_j \in \mathbf{B}$. Известная теорема теории меры гласит, что если множество оракулов S имеет положительную меру и $c < 1$, то существует интервал Γ такой, что

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

Применим эту теорему к множеству

$$S = \{A \mid L_{N^A} \text{ бесконечен и } L_{N^A} \subseteq L_0^A\}.$$

Значит, существует интервал Γ такой, что выполнено (2). Пусть интервал Γ задаётся набором $w_1, \ldots, w_j \in \mathbf{B}^*, b_1, \ldots, b_j \in \mathbf{B}$, т.е. $\Gamma = \{A \mid A(w_1) = b_1, \ldots, A(w_j) = b_j\}$. Для любого оракула A определим новый оракул A' следующим образом:

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

Легко проверить, что

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

Положим $k = \max_{m \le j} |w_m|$. Легко построить полиномиальную недетерминированную машину N_1 такую, что

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

Мы утверждаем, что если $A' \in S$, то язык $L_{N_1^A}$ бесконечен и $L_{N_1^A} \subseteq L_0^A$. В самом деле, пусть A' принадлежит S, т.е. язык $L_{N^{A'}}$ бесконечен и $L_{N^{A'}} \subseteq L_0^{A'}$. Тогда, очевидно, что язык $L_{N_1^A}$ тоже бесконечен. Кроме того, $L_{N_1^A} \subseteq L_0^A$, поскольку если $N_1^A(x) = 1$, то $|x| + 2\log_2|x| > k$ и $N^{A'}(x) = 1$, следовательно, $x \in L_0^{A'}$, что влечёт $x \in L_0^A$ (потому что $|x| + 2\log_2|x| > k$). Следовательно,

$$\mathrm{Prob}[L_{N_1^A} \text{ бесконечен и } L_{N_1^A} \subseteq L_0^A] \ge \mathrm{Prob}[A' \in S] > c.$$

Полученное противоречие доказывает импликацию $1') \Rightarrow 1)$. Импликация $2') \Rightarrow 2)$ доказывается аналогичным образом.

Итак, нам достаточно доказать $1')$ и $2')$. Пусть N — произвольная полиномиальная недетерминированная машина. Докажем, что вероятность каждого из событий

$$\text{“}L_{N^A} \text{ бесконечен и } L_{N^A} \subseteq L_0^A\text{”}, \tag{3}$$

$$\text{“}\mathbf{B}^* \setminus L_{N^A} \text{ бесконечен и } \mathbf{B}^* \setminus L_{N^A} \subseteq L_1^A\text{”} \tag{4}$$

не превосходит 0,9. Очевидно, что если L_{N^A} бесконечен и $L_{N^A} \subseteq L_0^A$, то существует бесконечно много таких i, что $N^A(1^{t_i}) = 1$. Поэтому для того, чтобы доказать, что $\mathrm{Prob}[(3)] \leq 0,9$, достаточно показать, что

$$\mathrm{Prob}[\exists^\infty i\ N^A(1^{t_i}) = 1] > 0,9 \Rightarrow \tag{5}$$
$$\mathrm{Prob}[\exists i\ (N^A(1^{t_i}) = 1\ \&\ 1^{t_i} \in L_1^A)] \geq 0,1, \tag{6}$$

где $\exists^\infty i$ означает «существует бесконечно много таких i, что». Аналогично, чтобы доказать, что $\mathrm{Prob}[(4)] \leq 0,9$, достаточно показать, что

$$\mathrm{Prob}[\exists^\infty i\ N^A(1^{t_i}) = 0] > 0,9 \Rightarrow \tag{7}$$
$$\mathrm{Prob}[\exists i\ (N^A(1^{t_i}) = 0\ \&\ 1^{t_i} \in L_0^A)] \geq 0,1. \tag{8}$$

Мы будем доказывать эти две импликации одновременно. Объединённое утверждение имеет вид: для всех $\delta \in \{0,1\}$

$$\mathrm{Prob}[\exists^\infty i\ N^A(1^{t_i}) = \delta] > 0,9 \Rightarrow \tag{9}$$
$$\mathrm{Prob}[\exists i\ (N^A(1^{t_i}) = \delta\ \&\ 1^{t_i} \in L_\delta^A)] \geq 0,1. \tag{10}$$

Зафиксируем произвольное $\delta \in \{0,1\}$. Предположим, что (9) истинно. Докажем, что выполнено (10). Из утверждения (9) следует, что

$$\sum_{i=k}^{\infty} \mathrm{Prob}[N^A(1^{t_i}) = \delta\ \&\ N^A(1^{t_{i-1}}) \neq \delta, N^A(1^{t_{i-2}}) \neq \delta, \ldots, N^A(1^{t_k}) \neq \delta] > 0,9 \tag{11}$$

для всех $k \in \mathbf{N}$.

Обозначим событие

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

через $P_{ik\delta}(A)$.

ЛЕММА 1. *Для всех достаточно больших k, для всех $i \geq k$ выполнено*

$$\mathrm{Prob}[1^{t_i} \in L_\delta^A\ \&\ N^A(1^{t_i}) = \delta\ \&\ P_{ik\delta}(A)] > \\ > (1/3)\,\mathrm{Prob}[N^A(1^{t_i}) = \delta\ \&\ P_{ik\delta}(A)] - \epsilon_i, \tag{12}$$

где ϵ_i — некоторая последовательность со сходящимся рядом $\sum_{i=1}^{\infty} \epsilon_i$.

Мы докажем эту лемму позднее. А сейчас мы продолжим доказательство теоремы.

Суммируя (12) по всем $i \geq k$, мы получаем

$$\sum_{i=k}^{\infty} \mathrm{Prob}[1^{t_i} \in L_\delta^A \ \&\ N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A))] > \\ > (1/3) \sum_{i=k}^{\infty} \mathrm{Prob}[N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A)] - \sum_{i=k}^{\infty} \epsilon_i. \qquad (13)$$

Из (11) и (13) следует

$$\sum_{i=k}^{\infty} \mathrm{Prob}[1^{t_i} \in L_\delta^A \ \&\ N^A(1^{t_i}) = \delta \ \&\ P_{ik\delta}(A)] > 0,3 - \sum_{i=k}^{\infty} \epsilon_i. \qquad (14)$$

Поскольку события, вероятности которых суммируются в левой части (14), попарно дизъюнктны и включены в событие

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

мы можем заключить, что вероятность события (15) больше $0,3 - \sum_{i=k}^{\infty} \epsilon_i$. Взяв теперь k столь большим, что $\sum_{i=k}^{\infty} \epsilon_i < 0,2$, мы получим (10).

Таким образом, теорема доказана по модулю леммы 1.⊠

Доказательство леммы 1. Зафиксируем достаточно большее k (насколько большим должно быть k, мы увидим позднее). Зафиксируем произвольное $i \geq k$. Обозначим через D_i множество двоичных слов длины менее $t_i + \log_2 t_i$ и обозначим через F_i множество всех функций из D_i в $\mathbf{B}$. Обозначим через $f|S$ сужение функции f на множество S. Для любого j событие $N^A(1^{t_j}) \neq \delta$ зависит только от значения оракула A на словах длины, ограниченной некоторым полиномом от t_j (поскольку N на входе 1^{t_j} может спрашивать значение оракула только на словах длины, ограниченной некоторым полиномом от t_j). Так как $t_i = 2^{t_{i-1}}$, при достаточно большом k, при всех $i \geq k$ событие $P_{ik\delta}(A)$ зависит только от $A|D_i$. Следовательно, мы можем предполагать, что $P_{ik\delta}(A)$ зависит только от $A|D_i$.

Мы докажем, что для всех $f \in F_i$

$$\mathrm{Prob}[1^{t_i} \in L_\delta^A \ \&\ N^A(1^{t_i}) = \delta \mid A|D_i = f] > \\ > (1/3) \mathrm{Prob}[N^A(1^{t_i}) = \delta \mid A|D_i = f] - \epsilon_i, \qquad (16)$$

где $\{\epsilon_i\}$ — некоторая последовательность такая, что ряд $\sum_{i=1}^{\infty}\epsilon_i$ сходится. Докажем, что из этого следует (12). Допустим, что (16) выполнено для всех $f \in F_i$. Тогда, умножая (16) на $\mathrm{Prob}[A|D_i = f]$, получаем

$$\mathrm{Prob}[1^{t_i} \in L_\delta^A \ \&\ N^A(1^{t_i}) = \delta \ \&\ A|D_i = f] > \\ > (1/3)\,\mathrm{Prob}[N^A(1^{t_i}) = \delta \ \&\ A|D_i = f] - \epsilon_i\,\mathrm{Prob}[A|D_i = f]. \qquad (17)$$

Суммируя (17) по всем $f \in F_i$ таким, что $P_{ik\delta}(A)$ истинно, если $A|D_i = f$, мы получаем

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

т.е., мы получаем (12).

Итак, нам достаточно доказать, что для всех $f \in F_i$ выполнено (16). Выберем произвольное $f \in F_i$. Очевидно, что количество вопросов, задаваемых машиной M к оракулу в возможных вычислениях на входе 1^{t_i}, ограничено некоторым полиномом от t_i. Обозначим этот полином через $q(t_i)$.

Далее мы будем рассматривать случаи $\delta = 0$ и $\delta = 1$ отдельно.

ЛЕММА 2. *Имеет место неравенство*

$$\mathrm{Prob}[N^A(1^{t_i}) = 1 \ \&\ 1^{t_i} \in L_1^A \mid A|D_i = f] > \\ > (1 - (1 - 2^{-t_i})^{2^{t_i} - q(t_i)})\,\mathrm{Prob}[N^A(1^{t_i}) = 1 \mid A|D_i = f]. \qquad (18)$$

Д о к а з а т е л ь с т в о. Положим $r = q(t_i)$. Назовём *r-окрестностью* любое множество оракулов вида

$$\{A \mid A|D_i = f,\ A|B_1 = f_1, A|B_2 = f_2, \ldots, A|B_r = f_r,\ A|E = g\}, \qquad (19)$$

где $B_1, \ldots, B_r$ — некоторые i-блоки, $f_1, \ldots, f_r$ — некоторые функции из $B_1, \ldots, B_r$ соответственно в $\mathbf{B}$, E — некоторое конечное множество, непересекающееся с D_i и со всеми i-блоками, а g — некоторая функция из E в $\mathbf{B}$. Положим

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

ЛЕММА 3. *Множество W является конечным объединением r-окрестностей.*

Д о к а з а т е л ь с т в о. Сначала докажем, что множество W является конечным объединением интервалов вида $\{A \mid A(w_1) = b_1, \ldots, A(w_r) = b_r,\ A|D_i = f\}$. Пусть A — некоторый оракул такой, что $N^A(1^{t_i}) = 1$ и $A|D_i = f$. Зафиксируем любое допускающее вычисление машины N^A на входе 1^{t_i}. Пусть в этом вычислении было спрошено значение оракула на словах $w_1, \ldots, w_r$. Тогда множество W содержит целиком интервал $\{A \mid A(w_1) = b_1, \ldots, A(w_r) = b_r,\ A|D_i = f\}$. Поскольку количество всевозможных вычислений машины N на входе 1^{t_j} при всевозможных оракулах конечно, утверждение доказано.

Итак, множество W является конечным объединением интервалов вида $\{A \mid A(w_1) = b_1, \ldots, A(w_r) = b_r,\ A|D_i = f\}$. Ясно, что любой такой интервал является конечным объединением r-окрестностей.⊠

Обозначим через $\Gamma_1, \ldots, \Gamma_n$ те r-окрестности, для которых $W = \Gamma_1 \cup \cdots \cup \Gamma_n$. Итак, мы хотим доказать, что

$$\mathrm{Prob}[1^{t_i} \in L_1^A \mid A \in \Gamma_1 \cup \cdots \cup \Gamma_n] > 1 - (1 - 2^{-t_i})^{2^{t_i} - r}. \qquad (20)$$

Назовём r-окрестность (19) *плохой*, если f_l — тождественно нулевая функция для некоторого $l \leq r$. Любой оракул A из плохой r-окрестности удовлетворяет утверждению $1^{t_i} \in L_1^A$. Следовательно, если мы удалим из объединения $\Gamma_1 \cup \cdots \cup \Gamma_n$ все плохие r-окрестности, то вероятность

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

не увеличится. Поэтому достаточно доказать (20) в случае, когда все окрестности $\Gamma_1, \ldots, \Gamma_n$ не являются плохими. Для этого достаточно показать, что

$$\mathrm{Prob}[A \text{ является нулевым в некотором } i\text{—блоке} \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1})] > 1 - (1 - 2^{-t_i})^{2^{t_i} - r} \qquad (21)$$

для всех $m \leq n$ таких, что $\Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1})$ непусто.

Зафиксируем произвольное $m \leq n$. Пусть Γ_m задаётся выражением (19). Обозначим через $C_1, \ldots, C_{2^{t_i} - r}$ все i-блоки, не принадлежащие множеству $\{B_1, \ldots, B_r\}$. Для любого $l \leq 2^{t_i} - r$ положим

$$p_l = \mathrm{Prob}[A \text{ является нулевым в } C_l \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1}) \text{ и } A \text{ не является нулевым во всех блоках } C_1, \ldots, C_{l-1}]. \qquad (22)$$

Конечно, может оказаться, что некоторое p_l не определено из-за того, что множество

$$\{A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1}) \mid \\ A \text{ не является нулевым во всех блоках } C_1, \ldots, C_{l-1}\}$$

пусто. Пустота этого множества означает, что любой оракул $A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1})$ является нулевым хотя бы в одном из блоков $C_1, \ldots, C_{l-1}$. В этом случае вероятность (21) равна 1, значит, утверждение доказано. ⊠

Очевидно, что вероятность (21) равна $1-(1-p_1)(1-p_2)\cdots(1-p_{2^{t_i}-r})$. Поэтому, чтобы доказать лемму 2, достаточно доказать следующую лемму.

ЛЕММА 4. *$p_l \geq 2^{-t_i}$ для всех $l \leq 2^{t_i} - r$ таких, что p_l определено.*

Доказательство. Зафиксируем произвольное $l \leq 2^{t_i} - r$ такое, что p_l определено, и докажем, что $p_l \geq 2^{-t_i}$. Определим отображение, сопоставляющее каждому оракулу A новый оракул A' следующим образом:

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

Назовём множество оракулов U *монотонным*, если $A \in U$ влечёт $A' \in U$. Мы утверждаем, что множество

$$U = \{A \mid A \in \Gamma_m \setminus (\Gamma_1 \cup \cdots \cup \Gamma_{m-1}) \text{ и } A \text{ не} \\ \text{является нулевым во всех блоках } C_1, \ldots, C_{l-1}\}$$

монотонно. Напомним, что

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

и что блок C_l не принадлежит множеству $\{B_1, \ldots, B_r\}$. Из этого следует, что Γ_m монотонно.

Поскольку все множества $\Gamma_1, \ldots, \Gamma_{m-1}$ не плохи, дополнение до множества $\Gamma_1 \cup \cdots \cup \Gamma_{m-1}$ также монотонно. Очевидно, что множество $\{A \mid A$ не является нулевым во всех блоках $C_1, \ldots, C_{l-1}\}$ монотонно. Следовательно, U монотонно как пересечение монотонных множеств.

Поэтому лемма 4 сразу следует из следующей леммы.

ЛЕММА 5. *Любое монотонное множество V положительной меры удовлетворяет неравенству*

$$\mathrm{Prob}[A \text{ является нулевым в } C_l \mid A \in V] \geq 2^{-t_i}.$$

Д о к а з а т е л ь с т в о.. Пусть множество оракулов V удовлетворяет условиям леммы. Обозначим через H множество функций из C_l в $\mathbf{B}$. Обозначим через $\mathbf{0}$ тождественно нулевую функцию из H. Пусть h — произвольная функция из H. Мы утверждаем, что существует сохраняющая меру 1–1–функция из множества

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

в множество

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

Действительно, пусть π — это такая перестановка H, что $\pi(h) = \mathbf{0}$. Тогда отображение $A \mapsto A''$, где

$$A''(u) = \begin{cases} \pi(A|C_l)(u), & \text{если } u \in C_l, \\ A(u) & \text{иначе,} \end{cases}$$

отображает множество $\mathcal{B}$ в множество $\mathcal{D}$, поскольку $A'' = A'$ для всех $A \in \mathcal{B}$ и V монотонно.

Таким образом, для всех h

$$\mathrm{Prob}[A \in V \ \&\ A|C_l = h] \leq \mathrm{Prob}[A \in V \ \&\ A|C_l = \mathbf{0}];$$

следовательно,

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

Итак, лемма 4 и лемма 2 доказаны.$\boxtimes$

Легко проверить, что $\lim_{i\to\infty}(1 - (1 - 2^{-t_i})^{2^{t_i} - q(t_i)}) = 1 - e^{-1} > 1/3$, следовательно, из леммы 2 следует лемма 1 в случае $\delta = 1$ (при этом $\epsilon_i = 0$).

Осталось разобрать случай $\delta = 0$. Положим $a_i = (1 - 2^{-t_i})^{2^{t_i}} = \mathrm{Prob}[1^{t_i} \in L_0^A]$ и $\epsilon_i = (1 - 2^{-t_i})^{2^{t_i} - q(t_i)} - a_i$. Очевидно, что

$$\epsilon_i = O(q(t_i)2^{-t_i}),$$

поэтому ряд $\sum_{i=1}^{\infty} \epsilon_i$ сходится.

Лемма 1 для $\delta = 0$ следует из следующей леммы

ЛЕММА 6. *Имеет место неравенство*

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

Д о к а з а т е л ь с т в о. По лемме 2

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

В следующих неравенствах мы опускаем условие $A|D_i = f$, чтобы сделать их удобочитаемыми. Мы имеем

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

Тем самым, лемма 6 доказана.⊠

СЛЕДСТВИЕ 2. [18] *Относительно случайного оракула существует* NP*-язык, являющийся* Co-NP*-иммунным.*

СЛЕДСТВИЕ 3. *Относительно случайного оракула существует* Co-NP*-язык, являющийся* NP*-иммунным.*

Далее работа построена следующим образом. Следующий параграф содержит две известные теоремы, используемые как техническое средство. В § 5 излагается основная теорема о персептронах. В § 6 мы применяем эту теорему (а точнее, основную лемму, использованную в её доказательстве) для доказательства того, что класс AM ∩ Co-AM не включен в класс PP относительно некоторого оракула. Доказательство, приведённое в настоящей работе, проще доказательства этого же результата в [14] за счёт более простого доказательства комбинаторной части, заключённой в теореме 5.

§ 4. Вспомогательные теоремы

Мы будем использовать следующие хорошо известные результаты.

ТЕОРЕМА 4. (неравенство Чернова [7, 21]) *Пусть* $\xi_1, \ldots, \xi_n$ *— это независимые случайные величины, принимающие значения во множестве* $\{0, 1\}$ *и такие, что* $\mathrm{Prob}[\xi_i = 1] = p$ *для всех* i. *Тогда для любого* $\delta \in (0; p(1-p)]$

$$\mathrm{Prob}\left[\left|\frac{1}{n}\sum_{i=1}^{n}\xi_i - p\right| \geq \delta\right] \leq 2e^{-\frac{\delta^2 n}{2p(1-p)}}.$$

Следующая лемма называется *леммой Фаркаша*. Она является одним из вариантов теоремы двойственности в теории линейного программирования (см., например, [17]).

ЛЕММА 7. *Система линейных уравнений*

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1t}x_t &= b_1, \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2t}x_t &= b_2, \\ &\ldots \\ a_{s1}x_1 + a_{s2}x_2 + \ldots + a_{st}x_t &= b_s \end{aligned}$$

в неотрицательных действительных переменных $x_1, x_2, \ldots, x_t$ *имеет решение тогда и только тогда, когда* не *имеет решений система линейных неравенств*

$$a_{11}y_1 + a_{21}y_2 + \ldots + a_{s1}y_s \geq 0,$$

$$\begin{aligned} a_{12}y_1 + a_{22}y_2 + \ldots + a_{s2}y_s &\geq 0, \\ &\ldots \\ a_{1t}y_1 + a_{2t}y_2 + \ldots + a_{st}y_s &\geq 0, \\ b_1y_1 + b_2y_2 + \ldots + b_sy_s &< 0 \end{aligned}$$

в действительных переменных (не обязательно неотрицательных) $y_1, y_2, \ldots, y_s$.

§ 5. Обобщение теоремы «один в блоке»

О п р е д е л е н и е 4. *Персептроном* называется схема глубины 2 с пороговой вершиной в корне и с вершинами, помеченными конъюнкциями (И-вершинами), на втором уровне. Каждый вход пороговой вершины помечен целым числом (возможно, отрицательным), называемым его *весом*. Входами И-вершин являются булевские переменные и их отрицания. *Порядком* персептрона называется максимальная входная степень его И-вершин. *Общим весом* персептрона называется сумма абсолютных величин его весов.

Пусть P — персептрон, а φ — присваивание булевских значений его переменным. *Весом* φ, обозначаемым $W_P(\varphi)$, называется сумма весов всех входов пороговой вершины, истинных при присваивании φ. Персептрон выдает 1 на входе φ, если $W_P(\varphi)$ больше чем порог его корневой вершины, и выдает 0 в противном случае. Значение, выданное персептроном на входе φ, обозначается $P(\varphi)$.

Пусть M — булева матрица, имеющая n рядов и m столбцов. Любая такая матрица может быть естественным образом задана посредством mn булевских значений. Мы говорим, что персептрон P получает такую матрицу M в качестве входа, если он имеет mn переменных и им присвоены эти булевские значения. В этом случае мы обозначаем выданное персептроном значение через $P(M)$.

Назовём булевскую матрицу *хорошей,* если каждый её ряд содержит хоть одну единицу. В противном случае назовём матрицу *плохой.* Пусть q — действительное число из отрезка [0;1]. Матрица называется *q-плохой*, если доля её рядов, не содержащих единиц, не меньше q (например, 1-плохие матрицы — это матрицы, состоящие из одних нулей).

Теорема «один в блоке» Минского и Пейперта утверждает, что любой

персептрон, распознающий, является ли данная булева матрица размера $n \times 4n^2$ хорошей, имеет порядок не меньше n.

Мы говорим, что персептрон P отделяет хорошие матрицы от q-плохих матриц размера $n \times m$, если $P(M) = 1$ для любой хорошей матрицы размера $n \times m$ и $P(M) = 0$ для любой q-плохой матрицы размера $n \times m$. Отметим, что для всех m, n существует персептрон порядка m и общего веса m, отделяющий хорошие матрицы от 1-плохих матриц размера $n \times m$ (для этого достаточно выяснить, содержит ли первый ряд матрицы хоть одну единицу).

ТЕОРЕМА 5. *Пусть $0 < \varepsilon \leq 1/2$. Если существует персептрон порядка d и общего веса w, отделяющий хорошие матрицы от $(1-\varepsilon)$-плохих матриц порядка $n \times m$, то*

$$d \geq \sqrt{(3/8)\varepsilon m}$$

или

$$w \geq 0,5e^{(2/15)\varepsilon n}.$$

Доказательство. Пусть m, n — натуральные числа. Обозначим множество булевых матриц, имеющих n рядов и m столбцов, через $\mathcal{M}$. Обозначим через M_{ij} элемент матрицы M, стоящий в i-м ряду и j-м столбце. Пусть μ — распределение вероятности на множестве $\mathcal{M}$. Если S — некоторое свойство матриц из $\mathcal{M}$, то через $\mathrm{Prob}_{\mu(M)}[S(M)]$ мы обозначаем вероятность события $S(M)$ по распределению μ. Пусть d — натуральное число. Два распределения вероятности μ и ν на множестве $\mathcal{M}$ называются *d-неразличимыми,* если

$$\mathrm{Prob}_{\mu(M)}[M_{i_1 j_1} = b_1, \ldots, M_{i_u j_u} = b_u] = \mathrm{Prob}_{\nu(M)}[M_{i_1 j_1} = b_1, \ldots, M_{i_u j_u} = b_u]$$

для любого $u \leq d$ и любой последовательности пар индексов $\langle i_1, j_1\rangle, \ldots, \langle i_u, j_u\rangle$ и любой последовательности битов $b_1, \ldots, b_u$.

Доказательство теоремы легко выводится из следующих двух лемм.

ЛЕММА 8. *Если существуют d-неразличимые распределения вероятности μ и ν на множестве $\mathcal{M}$ такие, что по распределению μ случайная матрица является хорошей с вероятностью 1, а по распределению ν случайная матрица является q-плохой с вероятностью не менее $1-\alpha$, то любой персептрон порядка d, отделяющий хорошие матрицы от q-плохих, имеет общий вес не менее α^{-1}.*

ЛЕММА 9. *Если* $d < \sqrt{(3/8)\varepsilon m}$ *и* $0 < \varepsilon \leq 1/2$, *то существуют такие* d*-неразличимые распределения вероятности* μ *и* ν *на множестве* $\mathcal{M}$, *что по распределению* μ *случайная матрица является хорошей с вероятностью* 1, *а по распределению* ν *случайная матрица является* $(1-\varepsilon)$*-плохой с вероятностью не менее* $1 - 2e^{-(2/15)\varepsilon n}$.

Доказательство леммы 8. Пусть d, μ, ν, q, α удовлетворяют условиям леммы 8. Пусть P — персептрон порядка d и общего веса w, отделяющий хорошие матрицы из $\mathcal{M}$ от q-плохих матриц из $\mathcal{M}$. Обозначим через E_μ и E_ν соответственно средние значения по распределениям μ и ν. Мы утверждаем, что

$$\mathrm{E}_\mu W_P(M) = \mathrm{E}_\nu W_P(M). \tag{25}$$

Докажем это. Пусть $C(M)$ обозначает булеву функцию, вычисляемую некоторой И-вершиной C из P. Обозначим через l общее количество И-вершин в P и обозначим через C_i i-ю И-вершину в P, а через w_i — её вес. Тогда

$$\mathrm{E}_\mu W_P(M) = \sum_{i=1}^{l} w_i \mathrm{E}_\mu C_i(M) = \sum_{i=1}^{l} w_i \,\mathrm{Prob}_{\mu(M)}[C_i(M) = 1].$$

Поэтому достаточно доказать, что $\mathrm{Prob}_{\mu(M)}[C(M) = 1] = \mathrm{Prob}_{\nu(M)}[C(M) = 1]$ для любой И-вершины C из P. Пусть C — какая-то И-вершина из P, $C = \bigwedge_{s=1}^{u}(M_{i_s j_s} = b_s)$, где $b_s = 0, 1$. Тогда

$$\mathrm{Prob}_{\mu(M)}[C(M) = 1] = \mathrm{Prob}_{\mu(M)}[M_{i_1 j_1} = b_1, \ldots, M_{i_u j_u} = b_u].$$

Поэтому d-неразличимость μ и ν влечёт (25).

Обозначим через t порог корневой вершины персептрона P. По распределению μ матрица с вероятностью 1 хороша, а на любой хорошей матрице M персептрон P выдаёт 1, т.е. $W_P(M) \geq t{+}1$. Поэтому $\mathrm{E}_\mu W_P(M) \geq t + 1$. С другой стороны, по распределению ν матрица q-плоха с вероятностью не менее $1 - \alpha$, а на любой q-плохой матрице M персептрон P выдаёт 0, т.е. $W_P(M) \leq t$. Следовательно, $\mathrm{E}_\nu W_P(M) \leq (1-\alpha)t + \alpha w$. Из этих двух неравенств получаем $t{+}1 \leq (1{-}\alpha)t{+}\alpha w$. Значит, $t{+}1 \leq t{+}\alpha w$ что влечёт $1 \leq \alpha w$.⊠

Доказательство леммы 9. Пусть d, ε, m, n удовлетворяют условию леммы 9. Распределение μ будет получено из некоторого распределения вероятности σ на множестве $\{1, 2, \ldots, m\}$ (которое мы определим позднее) следующим образом. Пользуясь распределением σ, выберем случайные и независимые числа $k_1, k_2, \ldots, k_n$ из множества $\{1, 2, \ldots, m\}$. Затем для каждого $i \leq n$ возьмём в качестве i-го ряда матрицы случайную строчку длины m, равномерно распределенную среди всех строк, содержащих ровно k_i единиц.

Распределение ν будет получено точно таким же образом, с тем отличием, что вместо σ будет использовано некоторое другое распределение τ, но уже на множестве $\{0, 1, 2, \ldots, m\}$.

Распределение τ в свою очередь будет получено из некоторого третьего распределения ρ опять на множестве $\{1, 2, \ldots, m\}$ посредством следующего преобразования:

$$\mathrm{Prob}_{\tau(k)}[k = a] = \begin{cases} 0,6\varepsilon \, \mathrm{Prob}_{\rho(k)}[k = a], & \text{если } a \in \{1, 2, \ldots, m\}, \\ 1 - 0,6\varepsilon, & \text{если } a = 0. \end{cases}$$

Заметим, что если распределение ν получено этим преобразованием из некоторого распределения ρ на множестве $\{1, 2, \ldots, m\}$, то по распределению ν случайная матрица $(1 - \varepsilon)$-плоха с вероятностью не менее $1 - 2e^{-(2/15)\varepsilon n}$. Это непосредственно следует из неравенства Чернова, приведенного в предыдущем параграфе. В самом деле, по распределению ν любой ряд не содержит ни одной единицы с вероятностью не менее $p = 1 - 0,6\varepsilon$. Возьмём $\delta = 0,4\varepsilon$. Поскольку мы предполагаем, что $\varepsilon \leq 1/2$, то δ и p удовлетворяют условиям теоремы 4. Применяя теорему, мы получаем, что матрица имеет меньше чем $(1 - \varepsilon)n$ нулевых рядов с вероятностью не более

$$2e^{-\frac{\delta^2 n}{2p(1-p)}} = 2e^{-\frac{(0,4\varepsilon)^2 n}{2 \cdot 0,6\varepsilon(1-0,6\varepsilon)}} = 2e^{-\frac{0,16\varepsilon n}{1,2(1-0,6\varepsilon)}} \leq 2e^{-\frac{0,16\varepsilon n}{1,2}} = 2e^{-2/15\varepsilon n}.$$

Итак, нам нужно определить распределения вероятности σ и ρ на множестве $\{1, 2, \ldots, m\}$ так, чтобы полученные из них распределения μ и ν были d-неразличимы. Для этого мы определим σ и ρ так, чтобы σ и τ имели d одинаковых первых моментов, т.е. чтобы

$$\mathrm{E}_{\sigma(k)} k^i = \mathrm{E}_{\tau(k)} k^i \tag{26}$$

для всех $1 \le i \le d$. Докажем, что из равенства d первых моментов распределений σ и τ следует d-неразличимость μ и ν.

В самом деле, мы утверждаем, что для любого $u \le d$, для любых $b_1, \ldots, b_u$ и любых $i_1, j_1, \ldots, i_u, j_u$ величина

$$\mathrm{Prob}_{\mu(M)}[M_{i_1 j_1} = b_1, \ldots, M_{i_u j_u} = b_u]$$

является полиномом от величин $\mathrm{E}_{\sigma(k)}k$, $\mathrm{E}_{\sigma(k)}k^2$, ..., $\mathrm{E}_{\sigma(k)}k^d$. Докажем это.

Пусть выбрано не более d мест $i_1, j_1, \ldots, i_u, j_u$ в матрице и значения $b_1, \ldots, b_u$, которые должны быть в этих местах. Тогда вероятность по распределению μ того, что в этих местах будут нужные значения, равна

$$\prod_{i=1}^{n} \mathrm{E}_{\sigma(k)} \frac{k(k-1)\cdots(k-c_i+1)(m-k)(m-k-1)\cdots(m-k-e_i+1)}{m(m-1)\cdots(m-c_i-e_i+1)},$$

где c_i обозначает количество мест в i-м ряду, значения в которых должны быть равны 1, а e_i обозначает количество мест в i-м ряду, значения в которых должны быть равны 0. Очевидно, что для всех i величина

$$\mathrm{E}_{\sigma(k)} \frac{k(k-1)\cdots(k-c_i+1)(m-k)(m-k-1)\cdots(m-k-e_i+1)}{m(m-1)\cdots(m-c_i-e_i+1)}$$

есть линейная комбинация величин $\mathrm{E}_{\sigma(k)}k^r$, $r = 0, 1, \ldots, c_i + e_i$. Поскольку $c_i + e_i \le d$, утверждение доказано. $\boxtimes$

Напомним, что ν получается из τ таким же образом, каким μ получается из σ. Поэтому из (26) следует d-неразличимость μ и ν.

Легко видеть, что

$$\mathrm{E}_{\tau(k)}k^i = 0,6\varepsilon\mathrm{E}_{\rho(k)}k^i$$

для всех $i \ge 1$. Поэтому, достаточно доказать существование распределений σ и ρ на множестве $\{1, 2, \ldots, m\}$, удовлетворяющих равенствам

$$\mathrm{E}_{\sigma(k)}k^i = 0,6\varepsilon\mathrm{E}_{\rho(k)}k^i \quad \text{для} \quad i = 1, 2, \ldots, d.$$

Мы сделаем это неконструктивно, применив лемму Фаркаша, поскольку двойственная проблема проще, чем исходная.

ЛЕММА 10. *Пусть $\beta \in (0, 1]$ и $d \in \mathbf{N}$. Следующие условия эквивалентны:*

1) *существуют распределения вероятности* σ *и* ρ *на отрезке* $\{1, 2, \ldots, m\}$ *такие, что*

$$E_{\sigma(k)} k^i = \beta E_{\rho(k)} k^i \quad \textit{для} \quad i = 1, 2, \ldots, d;$$

2) *не существует многочлена* $p(x)$ *степени не более* d *такого, что*

$$-p(0)\frac{1-\beta}{\beta} < p(j) \leq 0 \quad \textit{для} \quad j = 1, 2, \ldots, m.$$

Д о к а з а т е л ь с т в о. Условие 1) означает существование неотрицательных действительных решений системы

$$\begin{aligned}
\beta(1^1 x_1 + 2^1 x_2 + \ldots + m^1 x_m) - (1^1 x_{m+1} + 2^1 x_{m+2} + \ldots + m^1 x_{2m}) &= 0,\\
\beta(1^2 x_1 + 2^2 x_2 + \ldots + m^2 x_m) - (1^2 x_{m+1} + 2^2 x_{m+2} + \ldots + m^2 x_{2m}) &= 0,\\
&\ldots\\
\beta(1^d x_1 + 2^d x_2 + \ldots + m^d x_m) - (1^d x_{m+1} + 2^d x_{m+2} + \ldots + m^d x_{2m}) &= 0,\\
x_1 + x_2 + \ldots + x_m &= 1,\\
x_{m+1} + x_{m+2} + \ldots + x_{2m} &= 1.
\end{aligned}$$

По лемме Фаркаша это эквивалентно тому, что не существует таких действительных чисел $p_1, p_2, \ldots, p_d, y, z$, что

$$\beta \sum_{i=1}^{d} p_i j^i + y \geq 0 \quad \text{для} \quad j = 1, 2, \ldots, m, \tag{27}$$

$$-\sum_{i=1}^{d} p_i j^i + z \geq 0 \quad \text{для} \quad j = 1, 2, \ldots, m, \tag{28}$$

$$y + z < 0. \tag{29}$$

Будем интерпретировать числа $-z, p_1, p_2, \ldots, p_d$ как коэффициенты многочлена $p(u) = -z + p_1 u + \cdots + p_d u^d$. Тогда неравенства (28) означают, что $p(j) \leq 0$ для всех $j = 1, 2, \ldots, m$.

Кроме того, заменим y на новую переменную v, связанную с y соотношением $v = y + z$. Тогда неравенства (27) и (29) перепишутся в виде

$$\begin{aligned}
\beta(p(j) - p(0)) + p(0) + v &\geq 0 \quad \text{для} \quad j = 1, 2, \ldots, m,\\
v &< 0.
\end{aligned}$$

Ясно, что существование v, для которого выполнены эти неравенства, означает, что $\beta(p(j)-p(0))+p(0)>0$ для всех $j=1,2,\ldots,m$. Последнее неравенство можно переписать как $-p(0)\frac{1-\beta}{\beta} < p(j)$, что показывает эквивалентность условий 1) и 2).⊠

Итак, нам осталось доказать, что не существует многочлена $p(x)$ степени не более d такого, что $-p(0)\frac{1-0,6\varepsilon}{0,6\varepsilon} < p(j) \le 0$ для всех $j=1,2,\ldots,m$. Мы используем следующую теорему А.А. Маркова. Обозначим через $\|P\|$ максимальное абсолютное значение многочлена $P(x)$ на отрезке $[-1;1]$. Теорема Маркова утверждает (см., например, [20]), что $\|P'\| \le d^2\|P\|$ для любого многочлена $P(x)$ степени d.

Мы также будем использовать следующий упрощенный вариант известной леммы Элиха и Целлера [8], который легко следует из теоремы Маркова. Положим

$$Y=\{-1,-1+2/m,-1+4/m,\ldots,1-2/m,1\},$$

и пусть $\|P_Y\|$ обозначает наибольшее абсолютное значение многочлена $P(x)$ на множестве Y. Тогда

$$\|P\|\left(1-\frac{2d^2}{m}\right) \le \|P_Y\|. \tag{30}$$

Действительно, по теореме Лагранжа и по теореме Маркова мы имеем

$$\|P\|-\|P_Y\| \le \|P'\|\frac{2}{m} \le \|P\|\frac{2d^2}{m}.$$

Из этого сразу следует (30).

Итак, пусть $p(x)$ — такой многочлен степени d, что $-p(0)\frac{1-0,6\varepsilon}{0,6\varepsilon} < p(j) \le 0$ для всех $j=1,2,\ldots,m$. Докажем, что $d \ge \sqrt{(3/8)\varepsilon m}$.

Заметим, что $p(0)$ положительно. Обозначим число $\frac{1-0,6\varepsilon}{0,6\varepsilon}$ через α. Положим $P(x)=p(\frac{1}{2}m(x+1))+\frac{\alpha-1}{2}p(0)$. Легко видеть, что $\|P_Y\| = \frac{\alpha+1}{2}p(0)$, поэтому

$$(1-\frac{2d^2}{m})\|P\| \le \frac{\alpha+1}{2}p(0). \tag{31}$$

С другой стороны, поскольку $|P(-1+2/m)-P(-1)| = |p(1)-p(0)| \ge p(0)$, по теореме Лагранжа мы можем заключить, что $\|P'\| \ge p(0)m/2$.

Следовательно, по теореме Маркова

$$\|P\| \geq p(0)\frac{m}{2d^2}. \tag{32}$$

Из неравенств (31) и (32) мы получаем

$$\left(1 - \frac{2d^2}{m}\right) p(0)\frac{m}{2d^2} \leq \frac{\alpha+1}{2}p(0).$$

Поэтому

$$\frac{d^2}{m} \geq \frac{1}{\alpha+3} = \frac{0,6\varepsilon}{1+1,2\varepsilon} \geq \frac{0,6\varepsilon}{1,6} = \frac{3}{8}\varepsilon.\boxtimes$$

§ 6. Применение нижних оценок для персептронов для построения оракула, относительно которого AM∩Co-AM не включено в PP

Теоремы 5 достаточно для построения оракула, для которого AM $\not\subseteq$ PP. Чтобы построить оракул, для которого AM $\cap$ Co-AM $\not\subseteq$ PP, нам нужна теорема об отсутствии персептронов полилогарифмического веса и квазиполиномиального размера, решающих чуть более сильную проблему отделения, чем проблема, рассмотренная в теореме 5. Определим эту проблему.

Обозначим через $\mathcal{M}_n$ множество булевых матриц размера $n \times n$. Пусть $D = \langle M_0, M_1\rangle$ — пара матриц из $\mathcal{M}_n$. Скажем, что D имеет тип 0, если все ряды в M_0 содержат хоть одну единицу и по крайней мере $2/3$ рядов в M_1 состоят из одних нулей. Аналогично, D имеет тип 1, если все ряды в M_1 содержат хоть одну единицу и по крайней мере $2/3$ рядов в M_0 состоят из одних нулей. Обозначим $\mathcal{M}_n \times \mathcal{M}_n$ через $\mathcal{N}_n$.

ТЕОРЕМА 6. *Для некоторого $\delta > 0$, для всех достаточно больших n выполнено следующее. Если персептрон порядка d и общего веса w отделяет элементы $\mathcal{N}_n$ типа 0 от элементов типа 1, то $d \geq \delta n^{1/2}$ или $w \geq 2^{\delta n}$.*

Д о к а з а т е л ь с т в о. Пусть n — натуральное число. Пусть P — персептрон порядка d и общего веса w, отделяющий пары из $\mathcal{N}_n$ типа 0 от пар типа 1. Положим $\varepsilon = 1/3$, $\delta = 0.01$ и $m = n$. Предположим, что $d \leq \delta n^{1/2}$. Тогда выполнены условия леммы 9. По лемме 9 существуют распределения вероятности μ и ν на множестве $\mathcal{M}_n$ такие, что выполнено следующее:

1) матрица, случайная относительно μ, хороша с вероятностью 1;

2) матрица, случайная относительно ν, не является 2/3-плохой с вероятностью не более $2e^{-(2/15)(1/3)n}$;

3) μ и ν d-неразличимы.

Обозначим $2e^{-(2/15)(1/3)n}$ через p. Определим два распределения вероятности κ и λ на множестве $\mathcal{N}_n$ следующим образом. Чтобы получить случайную пару матриц $\langle M_0, M_1\rangle$ относительно κ, возьмём M_0 случайно относительно μ, а M_1 — случайно относительно ν. Чтобы получить случайную пару матриц $\langle M_0, M_1\rangle$ относительно λ, наоборот, возьмём M_0 случайно относительно ν, а M_1 — случайно относительно μ. Тогда мы получим

$$\mathrm{Prob}_{\kappa(D)}[D \text{ имеет тип } 0\ ] \geq 1 - 2p,$$
$$\mathrm{Prob}_{\lambda(D)}[D \text{ имеет тип } 1\ ] \geq 1 - 2p.$$

Как мы видели выше, из условия 3) вытекает, что

$$\mathrm{E}_\kappa W_P(D) = \mathrm{E}_\lambda W_P(D).$$

Обозначим порог корневой вершины P через t. Тогда $\mathrm{E}_\kappa W_P(D) \geq (1-2p)(t+1)-2pw$ и $\mathrm{E}_\lambda W_P(D) \leq (1-2p)t+2pw$. Следовательно, $(1-2p)(t+1) - 2pw \leq (1-2p)t + 2pw$, поэтому $w \geq 1/(6p) = (1/12)e^{(2/15)(1/3)n} \geq e^{\delta n}$ для достаточно больших n.⊠

ТЕОРЕМА 7. [14] *Существует такой оракул A, что $AM^A \cap Co\text{-}AM^A \not\subseteq PP^A$.*

Д о к а з а т е л ь с т в о. Пусть A — оракул и пусть $j \in \mathbf{N}$. Мы будем интерпретировать значение A на словах длины $2j+1$ как пару булевых матриц размера $2^j \times 2^j$. Обозначим эту пару через A_j. Будем говорить, что пара A_j *корректна,* если A_j имеет тип 1 или тип 0. Сопоставим каждому оракулу A язык $L(A) = \{1^j \mid A_j \text{ имеет тип } 0\}$.

Мы построим такой оракул A, что пара A_j корректна для всех $j \in \mathbf{N}$ и при этом $L(A) \notin \mathrm{PP}^A$. Из первого условия легко следует что язык $L(A)$ принадлежит $\mathrm{AM}^A \cap \mathrm{Co\text{-}AM}^A$.

Для того, чтобы выполнить требование $L(A) \notin \mathrm{PP}^A$, пронумеруем все полиномиальные вероятностные машины и обозначим i-ю машину через PP_i. Определим сначала A любым таким образом, чтобы пара A_j была корректна для всех $j \in \mathbf{N}$. Затем по шагам будем менять значение оракула, обеспечивая на i-м шаге отличие языка $L(A)$ от языка, распознаваемого машиной PP_i^A. С этой целью на i-м шаге мы изменим значение A на конечном множестве слов так, чтобы для некоторого $j \in \mathbf{N}$ было выполнено

$$1^j \in L(A) \not\Leftrightarrow \mathrm{Prob}[\mathrm{PP}_i^A(1^j) = 1] > 1/2. \tag{33}$$

После изменения мы зафиксируем все значения A, от которых зависит истинностное значение утверждения (33), и все изменённые на этом шаге значения. Это означает, что на более поздних шагах эти значения оракула не будут меняться.

Опишем i-й шаг. Выберем любое достаточно большое j такое, что ни одно значение оракула на словах длины $2j+1$ не зафиксировано (насколько большим должно быть j, мы увидим позднее). Положим $n = 2^j$. Обозначим через A оракул, построенный на $(i-1)$-м шаге. Для любого $D \in \mathcal{N}_n$ обозначим через $A[D]$ оракул, полученный из A заменой A_j на D. Докажем, что существует корректная пара $D \in \mathcal{N}_n$ такая, что условие (33) станет истинным, если заменить A на $A[D]$.

Пусть d — максимальное количество вопросов к оракулу, задаваемое машиной PP_i в вычислениях на входе 1^j. Обозначим через l количество случайных битов, используемых PP_i в вычислениях на входе 1^j. Положим $q = 2^l$. Очевидно, $d \le \mathrm{poly}(j) = \mathrm{poly}(\log_2 n)$ и $q \le 2^{\mathrm{poly}(j)} = 2^{\mathrm{poly}(\log_2 n)}$. Построим персептрон P порядка d и общего веса $w = 2^d q$ от 2^{2j+1} переменных такой, что

$$P(D) = 1 \Leftrightarrow \mathrm{Prob}[\mathrm{PP}_i^{A[D]}(1^j) = 1] > 1/2. \tag{34}$$

Пусть r — некоторая двоичная последовательность длины l. Пусть $v = v(1)v(2)\cdots v(d)$ — какая-нибудь двоичная последовательность длины d такая, что машина PP_i допускает вход 1^j, если в качестве случайных битов ей давать биты из r, а на вопросы к оракулу отвечать по-

следовательно $v(1), \ldots, v(d)$. Сопоставим каждой такой паре $\langle v, r \rangle$ следующую И-вершину C. Обозначим через $u_1, \ldots, u_d$ те слова, значение оракула на которых спрашивается в вычислении PP_i на входе 1^j, если в качестве случайных битов ей давать биты из r, а на вопросы к оракулу отвечать последовательно $v(1), \ldots, v(d)$. Тогда при присваивании переменным персептрона значений, соответствующих паре матриц $D \in \mathcal{N}_n$, вершина C выдаёт 1, если $A[D](u_k) = v(k)$ для всех $k \in \{1, 2, \ldots, d\}$. Все веса положим равными 1. Положим порог корневой вершины равным $q/2$. Легко проверить, что

$$W_P(D) = q \cdot \mathrm{Prob}[\mathrm{PP}_i^{A[D]}(1^j) = 1],$$

что влечёт (34).

Поскольку порядок P равен $d = \mathrm{poly}(j) = \mathrm{poly}(\log_2 n)$, а общий вес есть $2^d q = 2^{\mathrm{poly}(j)} = 2^{\mathrm{poly}(\log_2 n)}$, по теореме 6 для достаточно больших j персептрон P не может отделить пары типа 0 от пар типа 1 из $\mathcal{N}_n$. Значит, существует корректная пара $D \in \mathcal{N}_n$ такая, что

$$D \text{ имеет тип } 0 \;\Leftrightarrow\; \mathrm{Prob}[\mathrm{PP}_i^{A[D]}(1^j) = 1] > 1/2,$$

что доказывает теорему.⊠

§ 7. Заключение

Теорема 5 утверждает, что персептроны малого порядка и малого общего веса не могут отделить хорошие матрицы от q-плохих матриц (при $q < 1$). Она не противоречит возможности того, что персептроны малого порядка и большого веса могут отделять хорошие матрицы от q-плохих (для некоторого $q < 1$). Поскольку теорема «один в блоке» содержит ограничения только на порядок персептрона, хотелось бы усилить теорему 5, исключив из неё ограничение веса. Недавно Бигел (личное сообщение) получил такое усиление, хотя и с худшей оценкой порядка персептрона. Он доказал, что персептроны, отделяющие хорошие матрицы размера $n \times n$ от q-плохих, должны иметь сверхполилогарифмический от n порядок (для любого фиксированного $q < 1$). Остаётся открытой проблема, могут ли персептроны порядка $n^{o(1)}$ и произвольного общего веса решить эту задачу. Заметим, что оценка Бигела достаточна для

того, чтобы построить оракул, относительно которого AM не включено в PP. Поскольку его доказательство достаточно просто, оно даёт альтернативное упрощение отделения AM от PP с помощью оракулов. ⊠

Автор благодарен К.Ю. Горбунову за внимательное прочтение рукописи и А.А. Разборову за идею использования теоремы двойственности вместо теоремы Рисса.

Список литературы

1. Babai L. Trading group theory for randomness: 17th Annual ACM Symposium on Theory of Computing. 1985. P. 421–429.

2. Baker T., Gill J., and Solovay R. Relativization of P=?NP question// SIAM Journal on Computing. 1975. V. 4. № 4. P. 431–442.

3. Beigel R. Perceptrons, PP, and the polynomial time hierarchy: Seventh Annual Conference on Structure in Complexity Theory. Boston, MA, July 1992. P. 14–19.

4. Beigel R., Reingold N., and Spielman D. PP is closed under intersection: 23th Annual ACM Symposium on Theory of Computing. 1991. P. 1–9.

5. Bennet C. H. and Gill J. Relative to a random oracle P≠NP≠coNP with probability 1// SIAM Journal on Computing. 1981. V. 10. P. 96–113.

6. Blum M. and Impagliazzo R. General oracle and oracle classes: 28th Annual IEEE Symposium on Foundation of Computer Science. New York, May 1987. P. 118–126.

7. Chernoff H. A measure of assymptotic efficiency for tests of a hypothesis based on the sum of observations// Annals of Mathematical Statistics. 1952. V. 23. P. 493–509.

8. Ehlich H. and Zeller K. Schwankung von Polynomen zwischen Gitterpunkten// Mathematische Zeitschrift. 1964. V. 86. P. 41–44.

9. Fortnow L. and Reingold N. PP is closed under truth table reductions: Sixth Annual Conference on Structure in Complexity Theory. 1991. P. 13–15.

10. Fu B. Separating PH from PP by relativisation. Preprint, 1990.

11. Furst N. Saxe J. and Sipser M. Parity, circuits and the polynomial time hierarchy// Mathematical Systems Theory. 1984. V. 17. P. 13–27.

12. Kurtz S., Mahaney S. and Royer J. Average dependence and random oracle: Seventh Annual Conference on Structure in Complexity Theory. Boston, MA, July 1992. P. 306–317.

13. Toda S. On the computational power of PP and $\oplus$P: 30th Annual IEEE Symposium on Foundation of Computer Science. 1989. P. 514–519. PP is as hard as the polynomial time hierarchy// SIAM Journal on Computing. 1991. V. 20. P. 865–877.

14. Vereshchagin N. K. On the power of PP: 7th Conference on Structure in Complexity Theory. 1992. P. 138–143.

15. Vereshchagin N. K. Lower bounds for perceptrons solving some separation problems and oracle separation of AM from PP: Technical Report 498, Computer Science Department, University of Rochester, 1994.

16. Vereshchagin N. K. Lower bounds for perceptrons solving some separation problems and oracle separation of AM from PP: In Third Israel Symposium on Theory of Computing and Systems. 1995.

17. Ашманов С. А. Линейное программирование. М.: Наука, 1981.

18. Верещагин Н. К. “Соотношение NP- и Co-NP-множеств относительно случайного оракула” // Известия ВУЗов. Серия Математика. 1993. № 3. С. 31–39. Proc. of 8th Annual IEEE Conference on Structure in Complexity Theory, May 1993, San-Diego CA. P. 132–138.

19. Минский М., Пейперт С. Персептроны. М.: Мир, 1973.

20. Полиа Г., Сегё Г. Задачи и теоремы из анализа. Т. 2. М.: Наука, 1978.

21. Розенкрафт Дж. М., Рейфен А. Последовательное декодирование. М.: ИЛ, 1963.

МГУ им. М.В. Ломоносова
E-mail: ver@mech.math.msu.su

Поступило в редакцию
28.XI.94