На правах рукописи

Кноп Александр Анатольевич

Сложность эвристических вычислений и интерактивных протоколов

01.01.06 — математическая логика, алгебра и теория чисел

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Санкт-Петербург — 2016

Работа выполнена в лаборатории математической логики ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук

Научный руководитель:
Гирш Эдуард Алексеевич
доктор физико-математических наук, доцент, ведущий научный сотрудник лаборатории математической логики ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук

Официальные оппоненты:
Верещагин Николай Константинович
доктор физико-математических наук,
профессор ФГОУ ВПО "Московский Государственный Университет им. М.В. Ломоносова"
Охотин Александр Сергеевич
кандидат физико-математических наук,
профессор ФГОУ ВПО "Санкт-Петербургский Государственный Университет"
Ведущая организация: ФГБУН Институт проблем передачи информации им. А.А. Харкевича Российской академии наук

Защита состоится «15» марта 2017 г. в 17:00 на заседании диссертационного совета Д002.202.02 в ФГБУН Санкт-Петербургском отделении Математического института им. В. А. Стеклова Российской академии наук по адресу: 191023, Санкт-Петербург, наб. р. Фонтанки, 27, к. 311.

С диссертацией можно ознакомиться в библиотеке и на сайте ФГБУН Санкт-Петербургского отделения Математического института им. В. А. Стеклова Российской академии наук, http://www.pdmi.ras.ru/

Автореферат разослан «____» _____ 2017 г.

Ученый секретарь
диссертационного совета, д. ф.-м. н. А. В. Малютин

Общая характеристика работы

Актуальность темы

В классической теории сложности рассматривается время работы алгоритма (интерактивного протокола) в наихудшем случае. Однако для приложений, как правило, интереснее среднее время работы. В связи с этим в 1986 году Левин начал исследования в на тот момент новом разделе теории сложности — теории сложности в среднем.

По аналогии с классической теорией сложности (или теорией сложности в наихудшем случае), в теории сложности в среднем наибольший интерес представляет связь между различными вычислительными ресурсами. В данной работе нас будут более всего интересовать следующие вопросы:

1) насколько ресурс «время работы» существенен, правда ли, что за большее время можно решить большее число задач, и если да, то насколько;

2) насколько использование подсказки, зависящей от длины входа, увеличивает вычислительные возможности.

В терминах структурной сложности эти вопросы можно сформулировать следующим образом:

1) для каких моделей вычислений $\mathfrak{C}$ верно, что для любого k выполняется условие $\mathfrak{C}\mathbf{P} \not\subseteq \mathfrak{C}\mathbf{Time}[n^k]$, то есть полиномиальные по времени вычисления не моделируются за время n^k;

2) для каких моделей вычислений $\mathfrak{C}$ верно, что для любого k выполняется условие $\mathfrak{C}\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$, то есть полиномиальные по времени вычисления не моделируются вычислениями при помощи булевых схем размера n^k.

В классическом случае оба этих вопроса решены не полностью. Исследование первого из них началось в 1967 году с работы Хартманиса и Стернса в

которой они доказали, что $\mathbf{P} \not\subseteq \mathbf{DTime}[n^k]$ для любого k. Для доказательства этого результата ими была использована техника диагонализации. Однако этот метод невозможно перенести на классы, не замкнутые относительно отрицания, такие как **NP**. Для этих классов вопрос о существовании иерархии оставался открытым, пока в 1973 году Кук не доказал, что $\mathbf{NP} \not\subseteq \mathbf{NTime}[n^k]$ для всех k. Его доказательство базировалось на существовании **NP**-полной задачи и на иерархии для детерминированных вычислений. К сожалению, доказательство было сложным и не переносилось на другие классы. Десять лет спустя, в 1983 году, Зак предложил новое, более простое, доказательство, основанное на отложенной диагонализации. Это доказательство позволило доказать иерархию для всех синтаксических моделей вычислений, но для семантических же моделей, таких как **BPP**, вопрос до сих пор открыт. В 2004 году Фортноу и Сантанам совершили прорыв и доказали иерархию по времени для *эвристических* вероятностных алгоритмов с ограниченной ошибкой (они доказали, что $\mathrm{Heur}_\delta\mathbf{BPP} \not\subseteq \mathrm{Heur}_\delta\mathbf{BPTime}[n^k]$), для доказательства этого факта они воспользовались существованием оптимального алгоритма для **PSpace**-полного языка, их доказательство было технически сложным и не переносилось на другие модели вычислений. В 2007 году Первышев улучшил этот результат, доказав, что $\mathrm{Heur}_\delta\mathbf{BPP} \not\subseteq \mathrm{Heur}_{\frac{1}{2}-\delta}\mathbf{BPTime}[n^k]$ для всех k, и разработав технику, позволяющую доказать теоремы об иерархии для других семантических моделей вычислений (таких как интерактивные протоколы). В то же время вопрос об увеличении параметра ошибки выше $\frac{1}{2} - \delta$ все еще открыт.

Исследования второго вопроса начались в 1982 году с работы Каннана, в которой он доказал, что $\Sigma_2\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$ для всех k. Доказательство базировалось на теореме Карпа–Липтона. В 2001 Кай заметил, что теорему Карпа–Липтона можно усилить и тем самым доказать, что $\mathbf{S}_2\mathbf{P} \not\subseteq \mathbf{Size}[n^k]$ для любого k. К сожалению, успехи в классическом случае на этом закончи-

лись. Однако в 2009 Сантанам доказал, что $\mathbf{MA}/1 \not\subseteq \mathbf{Size}[n^k]$, тем самым улучшив предыдущие результаты.

Во всех вышеупомянутых результатах среднее время работы считалось по равномерному распределению, но естественно было бы рассматривать и другие распределения. Однако, если не ограничивать никак класс распределений, то становятся верны несколько парадоксальные утверждения: так, в 1992 году Ли и Витани доказали, что существует такое распределение D, что $(L, D) \in \mathrm{Heur}_{\frac{1}{n^3}}\mathbf{P}$ тогда и только тогда, когда $L \in \mathbf{P}$. В связи с этим, как правило, рассматривают распределения из какого-нибудь естественного класса. Своеобразным аналогом вопроса об иерархии по времени является следующий вопрос: может ли усложнение распределения увеличить сложность языка и, наоборот, можно ли уменьшить сложность языка, увеличив сложность распределения. В 1987 году Гуревич и Шелах доказали, что существует алгоритм, который проверяет граф на гамильтоновость за линейное время в среднем на равномерном распределении, что косвенно указывает на возможность положительного ответа на этот вопрос.

В следующих секциях мы детально рассмотрим каждый из трех вопросов.

Степень разработанности темы

Нижние оценки на схемную сложность. Широко известно доказательство подсчетом того, что существуют булевы функции суперполиномиальной схемной сложности. Однако все попытки доказать суперполиномиальную нижнюю оценку для явной функции (функции из класса **NP**) до сих пор не увенчались успехом...

Существует три основных направления, с которых пытаются подступиться к решению данной проблемы. Самый очевидный подход заключается в попытках доказать какие-нибудь оценки на функции из **NP**, но на данный

момент лучшим результатом в этой области является $3.01n - o(n)$ (оценку можно улучшить до $5n - o(n)$, если рассматривать схемы в базисе де Моргана). Другим вариантом является исследование ограниченных классов схем. Это направление оказывается более успешным, известна экспоненциальная нижняя оценка на монотонную схемную сложность, а также на схемы с ограниченной глубиной. Однако и это направление не привело к успехам в общем случае.

Последнее направление — это попытки доказать нижние оценки для функций из все меньших и меньших классов. Экспоненциальная нижняя оценка, полученная подсчетом, требует дважды экспоненциального времени. Бурман и другие показали, что данную оценку можно усилить и найти функцию экспоненциальной сложности в классе $\mathbf{MA_{Exp}}$. Менее амбициозной целью является доказательство нижних оценок вида n^k (для всех k). Это направление исследований было начато Кананом, который показал, что для каждого k существует язык из $\Sigma_2\mathbf{P} \cap \Pi_2\mathbf{P}$, не имеющий схем размера n^k. Данный результат был усилен до языков из класса $\mathbf{S}_2\mathbf{P}$. При этом попытки доказать существование такого языка в классе $\mathbf{MA}$ не привели ни к чему лучше задач из $Promise\mathbf{MA}$ и языков из $\mathbf{MA}/1$ (утверждение было доказано при помощи техники, разработанной в работах Барака, Фортноу и Сантанама).

Препятствие на пути доказательства нижних оценок на языки из $\mathbf{MA}$ типично для результатов структурной теории сложности (таких как иерархии по времени, существование полной задачи) для семантических классов. В конструкции Сантанама протокол не на всех входах имеет ограниченную вероятность ошибки, требующуюся в определении класса $\mathbf{MA}$. Аналогичную проблему решил Первышев для теоремы об иерархии по времени в классе эвристических вероятностных алгоритмов с ограниченной ошибкой; ее же решил Ицыксон при построении Avg$\mathbf{BPP}$-полной задачи (вопрос существо-

вания Avg**MA**-полной задачи все еще открыт). Они решили эту проблему, сопоставив каждому входу вероятность, начиная с которой мы примем данный вход.

Вопрос 1. Можно ли доказать нижнюю оценку на эвристическую схемную сложность задачи из эвристического аналога класса **MA**?

Теоремы об иерархиях по времени. Теорема об иерархии по времени для некоторой модели вычислений утверждает, что в данной модели вычислений за большее время можно решить строго большее множество задач. Для детерминированных машин Тьюринга подобная теорема была доказана Хартманисом и Стернсом при помощи диагонализации. Для того чтобы показать, что существует язык, разрешимый за $O(n^3)$ шагов, но не разрешимый за n^2 шагов, можно рассмотреть язык, содержащий строку x тогда и только тогда, когда машина Тьюринга M_x отвергает x за n^2 шагов. Иерархии по времени известны для всех синтаксических моделей вычислений. При этом стандартная диагонализация не работает, если класс не замкнут относительно дополнения (как, например, **NP**). Однако отложенная диагонализация, предложенная Заком, работает для всех синтаксических моделей.

Вычислительная модель называется семантической, если невозможно эффективно перечислить все корректные машины. Например, **BPTime**, **RTime** и **ZPTime** являются семантическими. На текущий момент неизвестно никаких точных теорем об иерархии по времени для семантических моделей вычислений. Например, лучший результат об иерархии по времени для вероятностных вычислений с ограниченной ошибкой имеет суперполиномиальный зазор: $\mathbf{BPTime}[n^{\log n}] \subsetneq \mathbf{BPTime}[2^{n^\epsilon}]$.

Первым продвижением в данной теме была теорема об иерархии по времени для вероятностных вычислений с несколькими битами неравномерной подсказки, позже была доказана иерархия для всех семантических классов с

одним битом подсказки: **BPTime**/1, **ZPTime**/1, **MATime**/1 и т.д.

Фортноу и Сантанам также доказали иерархию по времени для эвристических вероятностных алгоритмов с ограниченной ошибкой (такие алгоритмы могут на «малой» доле входов выдавать неправильный ответ или выдавать ответ с неправильной вероятностью). Точнее, они показали, что существует язык L, такой, что (L, U) принадлежит $\mathrm{Heur}_{\frac{1}{n^c}}\mathbf{BPP}$, но (L, U) не принадлежит $\mathrm{Heur}_{\frac{1}{n^c}}\mathbf{BPTime}[n^a]$. Доказательство этого факта также базируется на существовании оптимального алгоритма для **PSpace**-полного языка. Первышев упростил и усилил данную теорему об иерархии для эвристической версии **BPTime**, он доказал, что существует язык L, такой, что $(L, U) \in \mathrm{Heur}_{\epsilon}\mathbf{BPP}$, но $(L, U) \notin \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathbf{BPTime}[n^a]$. Первышев использовал отложенную диагонализацию против всех вероятностных машин. Отложенная диагонализация требует возможности промоделировать машину на входах с длиной, большей на единицу. Проблема заключается в том, что вероятностная машина может принять вход с произвольной вероятностью, поэтому промоделировать такую машину невозможно при помощи машин с ограниченной ошибкой. Пусть M — это вероятностная машина Тьюринга, которая не соблюдает условие ограниченной ошибки, но нам необходимо промоделировать ее на входе x. Первышев придумал метод, как промоделировать машину эвристически: для каждого входа x мы рассматриваем множество строк $\{y_1, y_2, \ldots, y_N\}$, где N достаточно большое. Для каждой строки y_i запускаем $M(x)$ много раз и вычисляем долю единиц μ_i среди ответов $M(x)$. Алгоритм принимает y_i, если μ_i больше θ_{y_i}, где $\theta_{y_i} = \frac{2}{5} + \frac{i}{5N}$. Заметим, что если $M(x)$ выполняет условие ограниченной ошибки, то с высокой вероятностью ответы для всех y_i будет одинаковыми. А если $M(x)$ не соблюдает условие ограниченной ошибки, то наш алгоритм не соблюдает его только на малой доле строк y_i, точнее, на таких y_i, что θ_{y_i} очень близка к $\Pr[M(x) = 1]$.

Вопрос 2. Можно ли доказать иерархию по времени для эвристических вы-

числений с параметром ошибки $1 - \epsilon$ вместо $\frac{1}{2} - \epsilon$?

Несложно заметить, что данное доказательство можно переделать в доказательство того, что существует такое полиномиально сэмплируемое распределение, что любое распределение, сэмплируемое за время n^a, имеет статистическое расстояние с ним не меньше $\frac{1}{2} - \epsilon$. В 2013 году Ватсон улучшил этот результат и доказал, что для любых констант a и k существует такое $D \in \mathbf{PSamp}$, что носитель D лежит в $[k]$, и для любого $R \in \mathbf{DSamp}[n^a]$ для бесконечно многих n статистическое расстояние между D_n и R_n не меньше $1 - \frac{1}{k} - \epsilon$.

Вопрос 3. Можно ли формализовать связь между теоремой Ватсона и иерархиями по времени для эвристических распределений?

Иерархии относительно сложности распределений. Как уже было сказано ранее, в теории сложности в среднем рассматриваются задачи в паре с распределением на входах. Задача называется простой в среднем, если она может быть эффективно решена на большой относительно этого распределения доле входов.

Соответственно, вопрос о том, как связана сложность проблемы с распределением на входах, естественен. Известно, что многие трудные задачи можно решить за полиномиальное в среднем время на равномерном распределении на входах: такое доказано для проверки графа на гамильтоновость (заметим, что в классическом случае данная задача **NP**-полна), проверки графов на изоморфизм (в тоже время существуют распределения, для которых неизвестно полиномиального алгоритма).

Также в работе Ли и Витани было построено распределение, такое, что любой язык прост в среднем на этом распределении тогда и только тогда, когда он прост в наихудшем случае. Из-за этого в теории сложности вычислений, как правило, рассматривают распределения из каких-то естественных

классов распределений, а не произвольные.

Двумя наиболее распространенными такими классами являются класс полиномиально сэмплируемых распределений (распределения являющиеся распределениями результата выполнения какого-то полиномиального вероятностного алгоритма) и класс полиномиально вычислимых распределений (распределений, чья функция распределения вычислима за полиномиальное время). Известно, что первый класс содержит второй, но неизвестно, равны они или нет. При этом доказано, что если существует односторонняя функция, то они не равны.

Вопрос 4. Верно ли, что любой «не очень сложный» язык можно упростить «не слишком сильно», усложнив распределение?

Вопрос 5. Верно ли, что существует «не слишком сложное» распределение, которое «сильно» усложняет язык?

Цели, полученные результаты и структура диссертации

Цели работы.

1) Доказать нижние оценки на эвристическую схемную сложность эвристической версии класса **MA**.

2) Найти более простое доказательство эвристической иерархии для вероятностных вычислений с ограниченной ошибкой.

3) Найти более простое доказательство эвристической иерархии для недетерминированных вычислений.

4) Усилить известные условные теоремы об иерархии для вероятностных вычислений с ограниченной ошибкой.

5) Исследовать возможность улучшения параметра ошибки в теоремах об иерархии по времени для эвристических вычислений.

6) Доказать теорему об иерархии для эвристических вероятностных вычислений с ограниченной ошибкой на всех «простых» распределениях.

7) Построить такой язык, что он решается на «простом» распределении за полиномиальное время, но ни на каком «не очень сложном» распределении он не решается «быстрее».

8) Построить такое «не очень сложное» распределение и язык, что этот язык не решается за полиномиальное время на этом распределении, но решается на «простых» распределениях.

Научная новизна. Все результаты диссертации являются новыми.

Теоретическая и практическая ценность. Работа носит теоретический характер. Ее результаты могут быть использованы в классической структурной теории сложности и теории сложности в среднем.

Методы исследований. В работе используются методы теории сложности вычислений.

Положения, выносимые на защиту.

1) Доказана нижняя оценка на эвристическую схемную сложность эвристических полиномиальных протоколов Мерлин–Артур: доказано, что для любого k выполняется $\mathrm{Heur}\mathbf{MA} \not\subseteq \mathrm{Heur}_{1-\delta}\mathbf{Size}[n^k]$.

2) Получено новое, более простое, доказательство того, что $\mathrm{Heur}_{\delta}\mathbf{BPP} \not\subseteq \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathbf{BPTime}[n^k]$.

3) Получено новое, более простое, доказательство того, что $\mathbf{NP} \not\subseteq \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathbf{NTime}[n^k]$.

4) Доказано, что если существует односторонняя функция, то $\mathbf{P} \not\subseteq \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathbf{BPTime}[n^k]$.

5) Доказано, что для любых a, k, δ и ϵ существует $f : \{0,1\}^* \to [a]$, такая, что $(f, U) \in \mathrm{Heur}_{\delta}\mathbf{FBPP}$, но $(f, U) \notin \mathrm{Heur}_{1-\frac{1}{a}-\epsilon}\mathbf{FBPTime}[n^k]$.

6) Доказано, что для любых a, δ и ϵ существует язык L, такой, что $(L, U) \in \mathrm{Heur}_{\delta}\mathbf{BPP}$, но $(L, R) \notin \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathbf{BPTime}[n^k]$ для любого $R \in \mathbf{DSamp}[n^k]$.

7) Доказано, что для любых $\epsilon > 0$ и $c > 0$ существуют такой язык L и распределение $D \in \mathbf{DSamp}[n^{\log^{\epsilon}(n)}]$, что $(L, D) \notin \mathrm{Heur}_{1-\frac{1}{2^{(\log\log\log n)^c}}}\mathbf{P}$ и для любого $R \in \mathbf{PSamp}$ верно, что $(L, R) \in \mathrm{Heur}_{\frac{1}{2^{(\log\log\log n)^c}}}\mathbf{DTime}[n]$.

8) Доказано, что для любого $a > 0$ существуют такой язык L и распределение $D \in \mathbf{PSamp}$, что $(L, D) \notin \mathrm{Heur}_{\frac{1}{n^a}}\mathbf{P}$ и для любого $R \in \mathbf{DSamp}[n^a]$ верно, что $(L, R) \in \mathrm{Heur}_{O(\frac{1}{n^a})}\mathbf{DTime}[n]$.

Апробация работы. Результаты диссертационной работы были изложены на следующих конференциях и семинарах.

1) Международная конференция “Eighth International Conference on Computability, Complexity and Randomness” (Москва, CCR 2013).

2) Международная конференция “The 10th International Computer Science Symposium in Russia” (Иркутск, CSR 2015).

3) Семинар лаборатории “Exploring limits of computations” (Токио, 2015).

4) Международная конференция “The 26th International Symposium on Algorithms and Computation” (Нагоя, ISAAC 2015).

5) Международная конференция “Problems in Theoretical Computer Science” (Москва, 2015).

6) Международный семинар “Special Semester Program on Complexity Theory” (Санкт-Петербург, 2016).

7) Международная конференция “The 27th International Symposium on Algorithms and Computation” (Сидней, ISAAC 2016).

Публикации. Основные результаты диссертации опубликованы в рецензируемых научных изданиях [1],[2],[3], входящих в список рекомендованных ВАК.

Работы [2] и [3] написаны в соавторстве. В работе [3] идея применения теоремы об иерархии по времени моделирования распределения для доказательства теорем об иерархии для эвристических вычислений была придумана в неразделимом соавторстве с Д.М. Ицыксоном. При этом техническая реализации всех доказательств теорем об иерархии для эвристических вычислений в классах **BPP**, **NP** и **FBPP** принадлежит диссертанту. Условная теорема об иерархии по времени для вероятностных вычислений при условии существования односторонних функций была доказана в неразделимом соавторстве с Д.М. Ицыксоном и Д.О. Соколовым. В работе [3] диссертанту принадлежит доказательство иерархии для слабого варианта трудности задачи в среднем и и доказательство теоремы об иерархии по времени моделирования распределения для бесконечно малых статистических расстояний, при этом постановка задачи принадлежит Д.М. Ицыксону. Неупомянутые результаты работ принадлежат соавторам.

Структура и объем работы. Диссертация состоит из введения, четырех глав и списка литературы. Общий объем диссертации 66 страниц. Список литературы включает 40 наименований на 5 страницах.

В главе 1 вводятся основные обозначения и определяются основные понятия.

В главе 2 доказывается нижняя оценка на схемную сложность эвристического класса Мерлин–Артур.

В главе 3 доказывается связь иерархии по времени для задачи сэмплирования и иерархии по времени для эвристических вероятностных вычислений с ограниченной ошибкой; связь иерархии по времени для задачи недетерминированного сэмплирования и иерархии по времени для эвристических недетерминированного вычислений; доказывается иерархия по времени для вероятностных вычислений с ограниченной ошибкой при условии существования односторонней функции; доказывается иерархия по времени вычисления функций для эвристических вероятностных вычислений с ограниченной ошибкой.

В главе 4 доказывается иерархия по времени сэмплирования распределения для строгой сложности для квазиполиномиально сэмплируемых распределений; доказывается слабая иерархия по времени сэмплирования распределения для слабой сложности для полиномиально сэмплируемых распределений; доказывается иерархия по времени вычисления распределений для полиномиально сэмплируемых распределений.

Содержание работы

Во **введении** описывается состояние области на сегодняшний день, рассматриваются задачи диссертации, ставятся цели, формулируются основные результаты и описывается структура диссертации.

Первая глава посвящена базовым понятиям, используемым в диссертации. Вводятся основные обозначения, упоминаемые классы языков, классы распределений и классы распределенных задач, используемые в работе.

Вторая глава посвящена нижним оценкам на эвристическую схемную сложность эвристического класса Мерлин–Артур.

Эвристические протоколы Мерлин-Артур определяются следующим образом

Определение 1. Распределенная задача (L, D) имеет эвристический протокол Мерлин-Артур (будем обозначать это как $(L, D) \in \mathrm{Heur}\mathbf{MA}$) тогда и только тогда, когда существует вероятностный алгоритм $A(x, y, \delta)$ (здесь x — вход, y — доказательство Мерлина и δ — параметр уверенности), а также семейство множеств $\{S_{n,\delta} \subseteq \{0,1\}^n\}_{\delta \in \mathbb{Q}_+, n \in \mathbb{N}}$ (большие множества, где протокол работает корректно) такие, что для всех n и δ

- $D_n(S_{n,\delta}) \geq 1 - \delta$,
- $A(x, y, \delta)$ работает время $\mathrm{poly}(\frac{n}{\delta})$ и
- для любого x из $S_{n,\delta}$:

$$x \in L \Rightarrow \exists y \ \Pr[A(x, y, \delta) = 1] > \frac{2}{3},$$
$$x \notin L \Rightarrow \forall y \ \Pr[A(x, y, \delta) = 0] > \frac{2}{3}.$$

Распределенная задача (L, D) имеет полиномиальный в среднем протокол Мерлин-Артур (будем обозначать это как $(L, D) \in \mathrm{Avg}\mathbf{MA}$), если в дополнение к предыдущим требованиям выполняется условие, что для всех x протокол возвращает «отказ» с высокой вероятностью или верный ответ:

$$x \in L \Rightarrow \exists y \ \Pr[A(x, y, \delta) = 1] > \frac{2}{3} \vee \Pr[A(x, y, \delta) = \perp] > \frac{1}{8},$$
$$x \notin L \Rightarrow \forall y \ \Pr[A(x, y, \delta) = 0] > \frac{2}{3} \vee \Pr[A(x, y, \delta) = \perp] > \frac{1}{8}.$$

Определим эвристическую схемную сложность:

Определение 2. 1) Будем называть булевой схемой от переменных x_1, $\ldots$, x_n помеченный ориентированный ациклический граф с входящей степенью 0 или 2, в листах которого стоят переменные $x_1, \ldots, x_n$, а каждая внутренняя вершина помечена бинарной булевой функцией. Значение булевой схемы на подстановке значений $v_1, \ldots, v_n$, переменным x_1,

$\ldots, x_n$ — это строка значений в вершинах степени 0, где значение в вершине — это v_i, если вершина — это лист помеченный x_i, и, если вершина является внутренней, то это значение, функции которой она помечена от значения в детях. Размером схемы будем называть размер графа.

2) Язык L принадлежит классу $\mathbf{Size}[f(n)]$ тогда и только тогда, когда существует семейство булевых схем C_n, такое, что $|C_n| < f(n)$ и для любого $x \in \{0,1\}^*$ выполняется равенство $C_{|x|}(x) = L(x)$.

3) Распределенная задача (L, D) принадлежит $\mathrm{Heur}_{\delta(n)}\mathbf{Size}[f(n)]$ тогда и только тогда, когда существует семейство булевых схем C_n, такое, что $|C_n| < f(n)$ и $\Pr\limits_{x \leftarrow D_n}[C_{|x|}(x) = L(x)] \geq 1 - \delta(n)$.

В данной главе доказывается следующая нижняя оценка.

Теорема 1. Существует константа $a > 0$, такая, что для любого $k \in \mathbb{Q}_+$, выполняется

$$\mathrm{Avg}\mathbf{MA} \not\subseteq \mathrm{Heur}_{1-\frac{1}{n^a}}\mathbf{Size}[n^k].$$

Третья глава посвящена эвристическим иерархиям по времени. В данной главе описывается метод получения эвристических иерархий по времени на основе иерархий по времени сэмплирования распределений.

В разделе 3.2 доказывается иерархия для класса $\mathrm{Heur}\mathbf{BPP}$, определенного следующим образом.

Определение 3. Класс $\mathrm{Heur}_{\delta(n)}\mathbf{BPTime}[f(n)]$ состоит из распределенных задач (L, D), таких, что существует вероятностный алгоритм $A(x)$, работающий $O(f(n))$ шагов, и для любого n верно, что $\Pr\limits_{x \leftarrow D_n}[\Pr[A(x) = L(x)] \geq \frac{3}{4}] \geq 1 - \delta(n)$. Также определим $\mathrm{Heur}_{\delta(n)}\mathbf{BPP} = \bigcup\limits_{k \geq 0} \mathrm{Heur}_{\delta(n)}\mathbf{BPTime}[n^k]$.

В этом разделе доказывается следующая теорема.

Теорема 2. Для любого $b > 0$ и $\delta\frac{1}{\mathrm{poly}(n)} > 0$ существует такой язык L, что $L \notin \mathrm{Heur}_{\frac{1}{2}-\delta}\mathbf{BPTime}[n^b]$ и для всех $\tau = \frac{1}{\mathrm{poly}(n)}$, $L \in \mathrm{Heur}_\tau\mathbf{BPP}$.

В разделе 3.3 Доказываются условные иерархии для класса **BPP** равного $\mathrm{Heur}_0\mathbf{BPP}$.

В разделе доказывается иерархия для класса **BPP** при условии существования односторонней функции.

Теорема 3. Предположим, что существует односторонняя функция. Тогда для любого $\epsilon > 0$ и $a > 0$ существует такой язык $L \in \mathbf{P}$, что $L \notin \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathbf{BPTime}[n^a]$.

А также доказывается, что если класс **BPP** содержит класс **NP**, то для класса **BPP** есть иерархия.

Теорема 4. Если $\mathbf{NP} \subseteq \mathbf{BPP}$, то $\mathbf{BPTime}[n^k] \subsetneq \mathbf{BPP}$ для всех $k > 0$.

В разделе 3.4 рассматривается обобщение теорем об иерархии по времени с языков на функции.

Докзывается, что если определить класс $\mathrm{Heur}_{\delta(n)}\mathbf{FBPTime}[f(n)]$ состоящий из таких пар (F, D), что

1) $F : \{0,1\}^* \to \{0,1\}^*$ — это функция,

2) D — это ансамбль распределений, таких и

3) существует вероятностный алгоритм A, работающий $O(f(n))$ шагов и для любого n выполняется неравенство $\Pr\limits_{x \leftarrow D_n}[\Pr[A(x) = F(x)] \geq \frac{3}{4}] \geq 1 - \delta(n)$, где внутренняя вероятность берется по случайным битам алгоритма A.

И определить класс $\mathrm{Heur}_{\delta(n)}\mathbf{FBPP} = \bigcup\limits_{k \geq 0} \mathrm{Heur}_{\delta(n)}\mathbf{FBPTime}[n^k]$.

Тогда выполянется теорема об иерархии по времени для этого класса.

Теорема 5. Для любого $b > 0$, $k > 0$ и $\delta = \frac{1}{\mathrm{poly}(n)} > 0$ существует такая функция $F\colon \{0,1\} \to \{0,1,\ldots,k-1\}$, что $F \notin \mathrm{Heur}_{1-\frac{1}{k}-\delta}\mathbf{FBPTime}[n^b]$ и $F \in \mathrm{Heur}_{\tau}\mathbf{FBPP}$ для любого $\tau = \frac{1}{\mathrm{poly}(n)} > 0$

В разделе 3.5 обобщается теорема об эвристической иерархии для вероятностных вычислений с ограниченной ошибкой, доказывается следующая теорема.

Теорема 6. Для любого $b > 0$, $k > 0$ и $\delta = \frac{1}{\mathrm{poly}(n)} > 0$ существует функция $H\colon \{0,1\}^* \to \{0,1,\ldots,k-1\}$ такая, что для любого $D \in \mathbf{DSamp}[n^b]$ $(H, D) \notin \mathrm{Heur}_{1-\frac{1}{k}-\delta}\mathbf{FBPTime}[n^b]$ и для любого $\tau = \frac{1}{\mathrm{poly}(n)}$ выполнено $H \in \mathrm{Heur}_{\tau}\mathbf{FBPP}$.

Наконец, в разделе 3.6 показывается как связаны иерархия по времени для недетерменированых вычислений и иерархия по времени для недетерминированого сэмплирования. Как результат доказывается следующая теорема.

Теорема 7. Для любого $b > 0$ и $\delta > 0$ существует такой язык L, что $L \notin \mathrm{Heur}_{\frac{1}{2}-\delta}\mathbf{NTime}[n^b]$ и $L \in \mathbf{NP}$.

В **четвертой главе** доказывается иерархия по времени сэмплирования распределения для строгой сложности для квазиполиномиально сэмплируемых распределений; доказывается слабая иерархия по времени сэмплирования распределения для «слабой сложности» для полиномиально сэмплируемых распределений; доказывается иерархия по времени вычисления распределений для полиномиально сэмплируемых распределений.

В разделе 4.2 определяются понятия свойства иерархии сэмплируемых распределений и иерархии распределенных задач (в сильном и слабом смысле).

Определение 4. Будем говорить, что две конструируемые функции f и g удовлетворяют *свойству иерархии сэмплируемых распределений* с параметром $\lambda(n)$, если существует ансамбль распределений $D \in \mathbf{DSamp}[f(n)]$, такой, что для любого ансамбля распределений $F \in \mathbf{DSamp}[g(n)]$, существует бесконечно много таких n, что статистическое расстояние между D_n и F_n как минимум $1 - \lambda(n)$.

Определение 5. Будем говорить, что две конструируемые функции f и g удовлетворяют *свойству иерархии распределенных задач* с параметрами $\alpha(n) > 0$ и $\beta(n) > 0$, если существуют такой язык L и такой ансамбль распределений $D \in \mathbf{DSamp}[f(n)]$, что

- $(L, F) \in \mathrm{Heur}_{\alpha(n)}\mathbf{P}$ для всех $F \in \mathbf{DSamp}[g(n)]$;
- $(L, D) \notin \mathrm{Heur}_{1-\beta(n)}\mathbf{P}$.

Также мы будем говорить, что f и g удовлетворяют *строгому* свойству иерархии распределенных задач, если

- Существует такой алгоритм A работающий линейное время, что для всех $F \in \mathbf{DSamp}[g(n)]$ и всех достаточно больших n выполняется неравенство $\Pr\limits_{x \leftarrow F_n}[A(x) = L(x)] \geq 1 - \alpha(n)$
- $(L, D) \notin \mathrm{Heur}_{1-\beta(n)}\mathbf{R}$.

Также доказывается, что они почти эквивалентны.

Лемма 1. Для всех конструируемых по времени функций $f(n)$, $h(n)$ и $g(n) \geq n$, если f и h удовлетворяют свойству иерархии сэмплируемых распределений с параметром $\lambda(n)$ и $g(n) \log g(n) = o(h(n))$, то f и g удовлетворяют свойству иерархии распределенных задач с параметрами $\alpha(n)$ и $\lambda(n)$, где $\alpha(n) = \omega(\lambda(n))$.

Лемма 2. Если f и g удовлетворяют свойству иерархии распределенных задач с параметрами $\alpha(n)$ и $\beta(n)$, то f и g удовлетворяют свойству иерархии сэмплируемых распределений с параметром $\alpha + \beta$.

В разделе 4.2.1 доказывается, что функции $n^{\log^b n}$ и $n^{\log^a n}$ удовлетворяют свойству иерархии сэмплируемых распределений.

Теорема 8. Для любых a, b, c, таких, что $0 < a < b$ и $c > 0$, функции $f(n) = n^{\log^b n}$ и $g(n) = n^{\log^a n}$ удовлетворяют свойству иерархии сэмплируемых распределений с параметром $\lambda(n) = \frac{1}{2^{(\log\log\log n)^c}}$.

И тем самым получаются следующий факт.

Следствие 1. Для любого $\epsilon > 0$ и $c > 0$ существует язык L и линейный по времени алгоритм A, такой, что для любого полиномиально сэмплируемого ансамбля распределений F и любого натурального n, $\Pr\limits_{x \leftarrow F_n}[A(x) = L(x)] \geq 1 - \frac{1}{2^{(\log\log\log n)^c}}$ и существует такой ансамбль $D \in \mathbf{DSamp}[n^{\log^\epsilon n}]$, что для любого алгоритма B и для бесконечно многих n, $\Pr\limits_{x \leftarrow D_n}[B(x) = L(x)] \leq \frac{1}{2^{(\log\log\log n)^c}}$.

В разделе 4.2.2 рассматривается слабая сложность и доказывается следующая иерархия.

Теорема 9. Для всех целых $a > 0$ и $b > 0$ существует ансамбль распределений $D \in \mathbf{PSamp}$, последовательность целых чисел l_n и последовательность множеств $S_n \subseteq \{0,1\}^{l_n}$, что следующие условия выполнены:

- $D(S_n) > \frac{1}{l_n^b}$ для всех n;
- Для любого $F \in \mathbf{DSamp}[n^a]$ следующее неравенство выполнено $F(S_n) \leq \frac{1}{l_n^b}$ для бесконечно многих n.

Вкачестве следствия получается следующее утверждение.

Следствие 2. Для любого $a > 0$ и $b > 0$ существуют такие ансамбль распределений $D \in \mathbf{PSamp}$, язык L и линейный по времени алгоритм A, что следующие условия выполнены:

- $\Pr_{x \leftarrow F_n}[A(x) \neq L(x)] = O(\frac{1}{n^b})$ для всех $F \in \mathbf{DSamp}[n^a]$;
- $(L, D) \notin \mathrm{Heur}_{\frac{1}{n^b}}\mathbf{R}$.

И наконец в разделе 4.3 рассматриваются такие же иерархии, но с вычислимыми распределениями.

Теорема 10. Для любого $a > 0$ существуют такие язык L и ансамбль распределений $D \in \mathbf{PComp}$, что

- $(L, F) \in \mathrm{Heur}_{O(\frac{1}{2^n})}\mathbf{DTime}[n]$ для всех $F \in \mathbf{Comp}[n^a]$;
- $(L, D) \notin \mathrm{Heur}_{1-\frac{1}{2^{n-1}}}\mathbf{R}$.

Публикации автора по теме диссертации в рецензируемых научных изданиях:

1. Knop Alexander. Circuit Lower Bounds for Average-Case MA // Lecture Notes in Computer Science. T. 9139. 2015. C. 283–295.
2. Itsykson Dmitry, Knop Alexander, Sokolov Dmitry. Heuristic Time Hierarchies via Hierarchies for Sampling Distributions // Lecture Notes in Computer Science. T. 9472. 2015. C. 201–211.
3. Itsykson Dmitry, Knop Alexander, Sokolov Dmitry. Complexity of distributions and average-case hardness // Leibniz International Proceedings in Informatics. T. 64. 2016. C. 38:1–38:12.

Другие публикации автора по теме диссертации:

4. Knop Alexander. Circuit Lower Bounds for Heuristic MA // Electronic Colloquium on Computational Complexity (ECCC). 2013. T. 20. C. 37. URL: http://eccc.hpi-web.de/report/2013/037.
5. Itsykson Dmitry, Knop Alexander, Sokolov Dmitry. Complexity of distributions and average-case hardness // Electronic Colloquium on

Computational Complexity (ECCC). 2015. T. 22. C. 174. URL: http://eccc.hpi-web.de/report/2015/174.

6. Itsykson Dmitry, Knop Alexander, Sokolov Dmitry. Heuristic time hierarchies via hierarchies for sampling distributions // Electronic Colloquium on Computational Complexity (ECCC). 2014. T. 21. C. 178. URL: http://eccc.hpi-web.de/report/2014/178.