Отчет по гранту фонда Династия за 2015-2016 годы

Д. Соколов

16 декабря 2016 г.

1 Результаты за отчетный период

1.1 Сложностные иерархии

Однозначные **иерархии.** Однозначные иерархии можно определить аналогично классической в теории вычислительной сложности полиномиальной иерархии; однако, в случае однозначных иерархий все подсказки для недетерминированных алгоритмов должны быть уникальными. Несколько типов таких иерархий определялись, начиная с 1993 года в работах Россманита и др. Отличия в типах иерархий проявляется при использовании алгоритмов в качестве оракулов. В работе [1] мы рассмотрели *свободную* однозначную иерархию $\mathrm{prUH}_\bullet$ с ослабленным набором требований в определении доступа к оракульной *промис* задаче. А именно, мы разрешили делать запросы к оракулу, которые не попадают в промис множество; однако, в такой ситуации ответ оракула может быть произвольным (похожее определение использовалось в работе Чакраварти и Роя, 2008).

Нам удалось доказать, что первая часть теоремы Тода $\mathrm{PH} \subseteq \mathrm{BP}\cdot\oplus\mathrm{P} \subseteq \mathrm{P}^{\mathrm{PP}}$ может быть усилена до следующего результата: $\mathrm{PH} = \mathrm{BP}\cdot\mathrm{prUH}_\bullet$, то есть замыкание иерархии, определенной в нашей работе, оператором Шонинга BP равняется классической полиномиальной иерархии. Можно также заметить, что $\mathrm{BP}\cdot\mathrm{prUH}_\bullet \subseteq \mathrm{BP}\cdot\oplus\mathrm{P}$.

Иерархии эвристических вычислений. В работе [2] мы представили новый метод доказательства теорем об иерархии для эвристических классов сложности. Основой данной метода является теорема об иерархии семплируемых распределений, доказанная Ватсоном в 2013 году. Класс $\mathrm{Heur}_\epsilon\mathrm{FBPP}$ состоит из пар: функция и распределение на входах данной функции, при этом существует вероятностный полиномиальный алгоритм, который считает данную функцию с ограниченной ошибкой по случайным битам на всех входах, кроме доли ϵ согласно распределению. Мы доказали, что для любых a, δ и целого k существует такая функция $F : \{0,1\}^* \to \{0,1,\ldots,k-1\}$, что $(F,U) \in \mathrm{Heur}_\epsilon\mathrm{FBPP}$ для всех $\epsilon > 0$ и для всех семейств распределений D_n, генерируемых за n^a шагов, $(F,D) \notin \mathrm{Heur}_{1-\frac{1}{k}-\delta}\mathrm{FBPTime}[n^a]$. Этот результат обобщает предыдущий результат, полученный Первышевым в 2007 году, на случай $k > 2$. Также нами было доказано, что если односторонние функции существуют, то $\mathrm{P} \not\subseteq \mathrm{Heur}_{\frac{1}{2}-\epsilon}\mathrm{BPTime}[n^k]$.

В той же работе нами было показано, что данная техника доказательства теорем об иерархиях обобщается и на ряд других эвристических классов.

Иерархии по распределениям. В работе [3] мы обратились к следующему вопросу теории сложности в среднем: существует ли такой язык L, что для всех простых распределений D распределенная задача (L, D) будет являться простой в среднем случае, однако, существует такое более сложное распределение D', что задача (L, D') является сложной в среднем? Мы рассмотрели два типа сложности распределений: сложность генерирования и сложность вычисления функции распределения.

В случае, когда под сложностью распределения понимается сложность генерирования, мы установили связь между описанным вопросом и теоремой Ватсона об иерархии распределений. Используя данную связь мы доказали следующий результат: для любых $0 < a < b$ существует язык L, семейство распределений D, генерируемое за $n^{\log^b n}$ шагов и такой линейный по времени алгоритм A, что для любого семейства распределений F, генерируемых за $n^{\log^a n}$ шагов, алгоритм A корректно решает L на всех входах $\{0,1\}^n$, кроме множества с бесконечно малой F-мерой, и для любого алгоритма B существует бесконечно много таких n, что множество элементов $\{0,1\}^n$, для которых B корректно решает L имеет бесконечно малую D-меру.

В случае, когда под сложность распределения понимается сложность вычисления функции распределения, мы доказали следующий результат: для любого $a > 0$ существует язык L, семейство полиномиально вычислимых распределений D и такой линейный по времени алгоритм A, что для любого вычислимого за n^a шагов семейства распределений F, A корректно решает L на всех входах из $\{0,1\}^n$, кроме доли с F-мерой не превосходящей $2^{-n/2}$, и для любого алгоритма B существует бесконечно много таких n, что множество элементов $\{0,1\}^n$, для которых B корректно решает L, имеет D-меру не более 2^{-n+1}.

1.2 Сложность доказательств и алгоритмы для задачи выполнимости

Совершенные паросочетания. Пусть формула ϕ_G кодирует существование совершенного паросочетания в графе G. Резолюционная сложность формул ϕ_G изучалась в работе Разборова в 2004 году, где была продемонстрирована техника доказательства нижних оценок для разреженых графов. В работе [4] мы построили такое семейство двудольных графов константной степени G_n, что резолюционная сложность формул ϕ_{G_n} равна $2^{\Omega(n)}$, где n — число вершин в графе G_n. Данная оценка является точной относительно умножения на полиномиальный множитель. Наш результат влечет нижнюю оценку $2^{\Omega(n)}$ для полного графа K_{2n+1} и полного двудольного графа $K_{n,O(n)}$, что усиливает результат из работы Разборова. Мы показали, что для любого графа G на n вершинах, в котором нет совершенного паросочетания, существует резолюционное доказательство для формулы ϕ_G размера $O(n^2 2^n)$. Таким образом нижняя оценка совпадает с верхней с точностью до умножения на полином. Наш результат также влечет хорошо известную нижнюю оценку на формулы, кодирующие принцип Дирихле.

Также в работе [4] мы доказали следующее следствие. Для любого натурального числа d, любого достаточно большого числа n и любой функции $h : \{1, 2, \ldots, n\} \to$

$\{1, 2, \ldots, d\}$, мы построили граф на n вершинах удовлетворяющий следующим свойствам:

- существует такая константа D, что степень всех вершины i в графе не менее $h(i)$ и не более D;
- невозможно сделать так, чтобы для всех $i \in [n]$ степень вершины i была равна $h(i)$ путем выкидывания ребер из графа;
- любое доказательство данного факта в резолюциях имеет размер не менее $2^{\Omega(n)}$.

Данный результат влечет хорошо известную экспоненциальную нижнюю оценку на Цейтинские формулы, а также новые результаты, например, аналогичное свойство для полного графа.

OBDD **алгоритмы.** В 2004 году Пан и Варди предложили подход для решения задачи выполнимости пропозициональной формулы, основанный на OBDDs (ordered binary decision diagram), мы будем обозначать алгоритмы, основанные на данном подходе, как OBDD($\wedge, \exists$)-алгоритмы. Такой алгоритм выбирает порядок на переменных π и создает OBDD D, которая изначально задает тождественно единичную функцию. Затем алгоритм по одному добавляет клозы исходной формулы к диаграмме D, также алгоритму разрешается применить операцию проекции по переменной x если все клозы, которые ее содержат, уже загружены в D, т.е. записать диаграмму, задающую функцию $\exists x D$ вместо D. В работе [5] мы расширили данные алгоритмы операцией смены порядка переменных, обозначим такие алгоритмы OBDD($\wedge, \exists,$ reordering). Мы заметили, что существует алгоритм OBDD($\wedge, \exists$), который решает задачу выполнимости для Цейтинских формул за полиномиальное время. С другой стороны мы показали, что существуют формулы, кодирующие системы линейных уравнений над полем $\mathbb{F}_2$, которые сложны для OBDD($\wedge, \exists,$ reordering) алгоритмов. Наши трудные примеры выполнимых формул задают систему линейных уравнений над полем $\mathbb{F}_2$, которая соответствует проверочной матрице кода исправляющего ошибки.

DPLL **алгоритмы с расщеплением по линейным функциям.** Классический DPLL алгоритм для задачи выполнимости булевой формулы делает расщепление исходной задачи на две меньших путем подстановки двух различных значений одной из переменных, и упрощая получившиеся формулы. В 2014 году мной совместно с соавторами было рассмотрено расширение парадигмы DPLL алгоритмов. Нашим алгоритмам разрешается проводить расщепление по значению произвольной линейной комбинации переменных по модулю 2. Эти алгоритмы быстро решают задачу выполнимости для формул, которые кодируют линейные системы уравнений по модулю 2, которые используются для доказательства экспоненциальной нижней оценки на классическую модель DPLL алгоритмов. Также нами было рассмотрено обобщение резолюционной системы доказательств, оперирующее с дизъюнкциями линейный уравнений над полем $\mathbb{F}_2$ — система доказательств Res_{lin}. Древовидные доказательства в данной системе соответствуют протоколам работы наших алгоритмов на невыполнимых формулах. В 2016 году нами была доказана теорема о компромиссе

между памятью, требуемой на реализацию доказательства, и его длиной. Если говорить более формально, то была предъявлена формула, для которой произведение числа клозов, которые нужно хранить в памяти для реализации доказательства в системе Res_{lin}, на логарифм размера доказательства хотя бы $\Omega(\frac{n}{\log(n)})$, где n — число переменных в формуле (данный результат на текущий момент не опубликован).

2 Работы

[1] Edward A. Hirsch and Dmitry Sokolov. On the probabilistic closure of the loose unambiguous hierarchy. *Inf. Process. Lett.*, 115(9):725–730, 2015.

[2] Dmitry Itsykson, Alexander Knop, and Dmitry Sokolov. Heuristic time hierarchies via hierarchies for sampling distributions. In Khaled Elbassioni and Kazuhisa Makino, editors, *Algorithms and Computation*, volume 9472 of *Lecture Notes in Computer Science*, pages 201 – 211. Springer Berlin Heidelberg, 2015.

[3] Dmitry Itsykson, Alexander Knop, and Dmitry Sokolov. Complexity of Distributions and Average-Case Hardness. In Seok-Hee Hong, editor, *27th International Symposium on Algorithms and Computation (ISAAC 2016)*, volume 64 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 38:1–38:12, Dagstuhl, Germany, 2016. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[4] Dmitry Itsykson, Vsevolod Oparin, Mikhail Slabodkin, and Dmitry Sokolov. Tight lower bounds on the resolution complexity of perfect matching principles. *Fundam. Inform.*, 145(3):229–242, 2016.

[5] Dmitry Itsykson, Alexander Knop, Andrey Romashchenko, and Dmitry Sokolov. On obdd based algorithms and proof systems that dynamically change order of variables. *Appear in proceedings of STACS 2017.*

[6] Dmitry Sokolov. Dag-like communication and its applications. *In progress.*

3 Доклады

1. Lower Bounds for Splittings by Linear Combinations. ELC mini-workshop, Tokyo, Japan, 2015.

2. Complexity of distributions and average-case hardness. Problems in Theoretical Computer Science, Moscow, Russia, 2015.

3. Tree-like diagonalization and its applications. Complexity Semester seminar, St. Petersburg, 2016.

4. Dag-like communication and its application. Problems in Theoretical Computer Science, Moscow, Russia, 2016.

4 Педагогическая деятельность

1. Преподаватель практических занятий по теории сложности в Санкт-Петербургском Академическом университете. 2015-2016.

2. Лектор и преподаватель практических занятий по анализу булевых функций в Санкт-Петербургском Академическом университете. 2016.

3. Преподаватель практических занятий по основам математической логики и дискретной математики в Санкт-Петербургском Академическом университете. 2015-2016.

4. Преподаватель практических занятий обзорного курса по computer scince в Computer Science Center. 2016.

5. Лектор мини-курса Basic constructions for Krajicek's interpolation в рамках семестра по сложности в СПБГУ.

5 Другое

В 2015 году году была подготовлена и защищена диссертация по теме "Сложность решения задачи выполнимости булевых формул алгоритмами, основанными на расщеплении" на соискание ученой степени кандидата физико-математических наук по специальностям: 01.01.06 — математическая логика, алгебра и теория чисел, 01.01.09 — дискретная математика и математическая кибернетика.