Конкурс «Молодая математика России»
отчет Д.М. Ицыксона за 2020 год

1 Публикации

Работы опубликованные в журналах:

[10] Dmitry Itsykson and Dmitry Sokolov. Resolution over linear equations modulo two. Ann. Pure Appl. Log., 171(1), 2020.

[3] Ludmila Glinskih and Dmitry Itsykson. On Tseitin formulas, read-once branching programs and treewidth. Theory Comput Syst, 2020. https://link.springer.com/article/10.1007/s00224-020-10007-8

[6] Dmitry Itsykson, Alexander Knop, Andrei Romashcenko, and Dmitry Sokolov. On OBDD-based algorithms and proof systems that dynamically change order of variables. The Journal of Symbolic Logic, pages 1–41, 2020. https://doi.org/10.1017/jsl.2019.53

Препринты :

[8] Dmitry Itsykson and Artur Riazanov. Proof complexity of natural formulas via communication arguments. Electron. Colloquium Comput. Complex., 27:184, 2020.

[7] Dmitry Itsykson, Alexander Okhotin, Vsevolod Oparin: Computational and proof complexity of partial string avoidability. Electron. Colloquium Comput. Complex. 27:67, 2020. Accepted to ACM Transactions on Computation Theory.

[2] Sam Buss, Dmitry Itsykson, Alexander Knop, Artur Riazanov, Dmitry Sokolov: Lower Bounds on OBDD Proofs with Several Orders. Electron. Colloquium Comput. Complex. 27:73, 2020.

2 Участие в конференциях

- Proof Complexity, Banff International Research Station, Banff, Canada, January 19-24, 2020. Доклад: On 1-BP complexity of satisfiable Tseitin formulas and how it relates to regular resolution,
- Conference on Computational Complexity, 28 - 30 июля 2020, online. Без доклада.

3 Педагогическая деятельность

В СПбГУ на факультете математики и компьютерных наук в весеннем семестре я прочитал курс лекций «Теория алгоритмов» студентам бакалавриата, в весеннем семестре я провел курс лекций и практических занятий «Дополнительные главы теории сложности». Также я прочитал курс лекций «Обзорный курс по теоретической информатике» в Computer Science клубе в Санкт-Петербурге.

В 2020 году под моим руководством защитил выпускную квалификационную работу студент магистратуры СПбГУ П.Ю. Смирнов, тема « Системы доказательств, основанные на диаграммах принятия решений».

В настоящее время я руковожу тремя аспирантами (А.А. Рязановым, С.И. Грязновым и П.Ю. Смирнов).

4 Полученные результаты

4.1 Коммуникационный подход для оценки сложности вывода естественных формул

Каноническая коммуникационная задача поиска $\mathrm{Search}(\varphi)$ определяется для каждой невыполнимой КНФ формулы φ: значения переменных формулы φ распределены среди участников коммуникационного протокола, им требуется найти дизъюнкт формулы φ, который опровергается этими значениями переменных. Известно, что нижние оценки на вероятностную коммуникационную сложнсоть задачи $\mathrm{Search}(\varphi)$ в моделе из k участников влекут нижние оценки на размер древовидных доказательств, на ранг обычных доказательств и утверждения о компромиссе между памятью и размером доказательства для формулы φ в семантической системе доказательств $\mathrm{T}^{\mathrm{cc}}(k, c)$. Система $\mathrm{T}^{\mathrm{cc}}(k, c)$ оперирует строками доказательств, которые можно вычислить с помощью вероятностного протокола из k участников, используя не более c битов коммуникации [4]. Все известные нижние оценки на коммуникационную сложность $\mathrm{Search}(\varphi)$ (например, [1, 4, 5]) доказываются на формулах, которые специально строились для этих доказательств. Нами предложен новый коммуникационный подход, который позволяет доказывать нижние оценки для естественных формул.

В работе [8] мы сначала демонстрируем этот подход для коммуникационных протоколов с двумя участниками и системе доказательств $\mathrm{Res}(\oplus)$, которая оперирует дизъюнкцяим линейных равенств над полем $\mathbb{F}_2$ [9]. Пусть формула PM_G кодирует в КНФ, что граф G содержит совершенное паросочетание. Известно, что если граф G имеют нечетное число вершин, то PM_G имеет древовидное $\mathrm{Res}(\oplus)$-опровержение полиномиального размера [9]. Верно ли это для графов с четным числом вершин не было известно. На этот вопрос не удается ответить ранее известными методами. Мы отвечаем на этот вопрос, используя наш коммуникационный подход.

Теорема 4.1. Размер любого древовидного $\mathrm{Res}(\oplus)$-опровержения формулы $\mathrm{PM}_{K_{n+2,n}}$ есть $2^{\Omega(n)}$, где $K_{n+2,n}$ обозначает полный двудольный граф с $n+2$ и n вершинами в долях.

В статье [8] мы также применяем наш подход к коммуникационным протоколам для k участников. Формула $\mathrm{BPHP}^M_{2^n}$ кодирует в КНФ бинарный принцип Дирихле, который гласит, что существует M различных n-битных строк.

Мы доказываем следующую теорему.

Теорема 4.2. Пусть $M = 2^n + 2^{n(1-1/k)}$, значения переменных формулы $\mathrm{BPHP}^M_{2^n}$ написаны на лбу у k участников коммуникационного протокола, у i-го участника

записаны переменные i-й части каждой из M строк. Вероятностная коммуникационная сложность задачи Search $\left(\mathrm{BPHP}_{2^n}^M\right)$ в модели с k участниками и «числами на лбу» не менее, чем $\Omega\left(\frac{1}{k}2^{n/2k-3k/2}\right)$.

В частности, из теоремы 4.2 следует, что формула $\mathrm{BPHP}_{2^n}^M$ требует экспоненциальных древовидных доказательств в семантической системе доказательств $\mathrm{Th}(k)$, которая оперирует полиномиальными неравествами степени не более k, где $k = \mathcal{O}(\log^{1-\epsilon} n)$ для некоторого $\epsilon > 0$.

Утверждение 4.1. При $m > 2^\ell$ существует древовидное $\mathrm{Th}(\ell)$-опровержение $\mathrm{BPHP}_{2^\ell}^m$ размера $\mathcal{O}(m^2 \cdot 2^\ell)$.

Из утверждения 4.1 следует, что $\mathrm{BPHP}_{2^n}^{2^n+1}$ суперполиномиально разделяет древовидную систему $\mathrm{Th}(\log^{1-\epsilon} m)$ от древовидной системы $\mathrm{Th}(\log m)$, где m — это число переменных в формуле.

4.2 Системы доказательств с правилом сдвига для PSPACE-полного языка

Пусть F — формула в КНФ которая использует конечное число переменные x_i, где i — натуральное число. Рассмотрим формулу $\mathrm{Shifts}(F)$, которая является конъюнкцией бесконечного числа дизъюнктов, каждый из которых получается из дизъюнкта формулы F добавлением одного и того же целого числа к индексам всех переменных. Таким образом, формула $\mathrm{Shifts}(F)$ использует все переменные $\{x_i \mid i \in \mathbb{Z}\}$. Множество формул $\mathrm{Shifts}(F)$ будем называть Shift-КНФ формулами.

На формулу $\mathrm{Shifts}(F)$ можно смотреть как на задачу избегаемости частичных слов. Каждый дизъюнкт формулы F задает запрещенное частичное бинарное слово (слово с пропусками), а формула $\mathrm{Shifts}(F)$ утверждает, что существует бесконечное в обе стороны слово, которое избегает все запрещенные частичные подслова.

Теорема 4.3. Язык Shift-UNSAT невыполнимых Shift-КНФ формул является PSPACE-полным.

Теорема 4.3 мотивирует изучение систем доказательств для языка Shift-UNSAT как подход к вопросу о неравенстве классов NP и PSPACE. Рассмотрим специфический класс систем доказательств для языка Shift-UNSAT, которые получаются из классических систем доказательств для языка невыполнимых КНФ формул UNSAT с помощью добавления правила сдвига. Правило сдвига позволяет из строки доказательств вывести другую строку, которая получается добавлением к индексам исходной строки одного и того же целого числа. Систему доказательств Π с добавленным правилом сдвига будем обозначать Shift-Π.

Мы показываем, что для изучения вопроса о равенстве классов NP и PSPACE можно ограничиться изучением только таких систем доказательств.

Теорема 4.4. Если для любой пропозициональной системы доказательств Π найдется невыполнимая Shift-КНФ формула, которая не имеет полиномиальных по размеру доказательств в системе Shift-Π, то PSPACE $\neq$ NP.

Пусть SC — это семантическая система доказательств, которая оперирует булевыми схемами и позволяет за шаг из двух схем вывести схему, которая из нее семантически следует. Все невыполнимые формулы из UNSAT имеют в этой семантической системе опровержения линейного размера. Однако, скорее всего язык Shift-UNSAT не имеет коротких опровержений в системе Shift-SC.

Утверждение 4.2. Если любая формула из Shift-UNSAT имеет полиномиальное по размеру опровержение в системе Shift-SC, то PSPACE $\subseteq \Sigma_2^{\mathrm{P}}$.

Оказывается, что доказательство суперполиномиальных нижних оценок на сложность вывода в системе Shift-SC влечет нижние оценки на схемную сложность.

Теорема 4.5. Если существует такое семейство CNF формул F_n, что Shifts(F_n) не имеет Shift-SC доказательств размера poly(n), то PSPACE $\not\subseteq$ P/poly.

Доказательства результатов этого раздела приведены в статье [7].

4.3 Нижние оценки в исчисление однопроходных ветвящихся программ с правилом проекции

Рассмотрим семантическую систему доказательств $1{-}\mathrm{NBP}(\wedge, \exists)$, в которой опровержение для невыполнимой КНФ формулы F представляется в виде последовательности булевых функций $D_1, D_2, \ldots, D_s$, представленных в виде $1{-}\mathrm{NBP}$ (однопроходных недетерминированных ветвящихся программ), где D_s — это тождественно ложная функция, а каждая D_i либо задает дизъюнкт формулы F, либо получается из предыдущих по одному из двух правил вывода:

- Правило конъюнкции ($\wedge$): $D_i = D_j \wedge D_k$, где $j, k < i$;
- Правило проекции ($\exists$): $D_i = \exists x D_j$, где $j < i$, а x — пропозициональная переменная.

$1{-}\mathrm{NBP}(\wedge, \exists)$ не является системой доказательств в классическом смысле, но моделирует систему доказательств OBDD($\wedge, \exists,$ reordering) [6].

В работе [2] мы рассматриваем подсистему $1{-}\mathrm{NBP}(\wedge, \exists_\ell)$ системы $1{-}\mathrm{NBP}(\wedge, \exists)$, в которой правило проекции разрешено применять не более, чем к ℓ переменным.

Теорема 4.6. Существует такая константа $\epsilon > 0$ и семейство цейтинских формул $T(G, f)$, основанных на графах G константной степени на n вершинах с функцией пометок f,что формулы $T(G, f)$ требуют $1{-}\mathrm{NBP}(\wedge, \exists_{\epsilon n})$ опровержений размера как минимум $2^{\Omega(n)}$.

Список литературы

[1] Paul Beame, Toniann Pitassi, and Nathan Segerlind. Lower bounds for lovász-schrijver systems and beyond follow from multiparty communication complexity. *SIAM J. Comput.*, 37(3):845–869, June 2007.

[2] Sam Buss, Dmitry Itsykson, Alexander Knop, Artur Riazanov, and Dmitry Sokolov. Lower bounds on OBDD proofs with several orders. *Electron. Colloquium Comput. Complex.*, 27(73), 2020.

[3] Ludmila Glinskih and Dmitry Itsykson. On Tseitin formulas, read-once branching programs and treewidth. *Theory Comput Syst*, 2020.

[4] Mika Göös and Toniann Pitassi. Communication lower bounds via critical block sensitivity. In *Proceedings of the Forty-Sixth Annual ACM Symposium on Theory of Computing*, STOC '14, page 847–856, New York, NY, USA, 2014. Association for Computing Machinery.

[5] Russell Impagliazzo, Toniann Pitassi, and Alasdair Urquhart. Upper and lower bounds for tree-like cutting planes proofs. In *Proceedings of the Ninth Annual Symposium on Logic in Computer Science (LICS '94), Paris, France, July 4-7, 1994*, pages 220–228. IEEE Computer Society, 1994.

[6] Dmitry Itsykson, Alexander Knop, Andrei Romashcenko, and Dmitry Sokolov. On OBDD-based algorithms and proof systems that dynamically change order of variables. *The Journal of Symbolic Logic*, pages 1–41, 2020.

[7] Dmitry Itsykson, Alexander Okhotin, and Vsevolod Oparin. Computational and proof complexity of partial string avoidability. *Electron. Colloquium Comput. Complex.*, 27(67), 2020.

[8] Dmitry Itsykson and Artur Riazanov. Proof complexity of natural formulas via communication arguments. *Electron. Colloquium Comput. Complex.*, 27(184), 2020.

[9] Dmitry Itsykson and Dmitry Sokolov. Lower bounds for splittings by linear combinations. In Erzsébet Csuhaj-Varjú, Martin Dietzfelbinger, and Zoltán Ésik, editors, *Mathematical Foundations of Computer Science 2014 - 39th International Symposium, MFCS 2014, Budapest, Hungary, August 25-29, 2014. Proceedings, Part II*, volume 8635 of *Lecture Notes in Computer Science*, pages 372–383. Springer, 2014.

[10] Dmitry Itsykson and Dmitry Sokolov. Resolution over linear equations modulo two. *Ann. Pure Appl. Log.*, 171(1), 2020.