Отчет по гранту фонда «Династия» за 2017 год

Д. Соколов

3 декабря 2017 г.

1 Результаты за отчетный период

OBDD **системы доказательств.** OBDD [Bry85] — ветвящиеся программы, где на каждом пути от корня до листа переменные встречаются в заранее фиксированном порядке. Начиная с 1990 года подходы, основанные на OBDD, начинают активно применяться для решения задачи выполнимости булевых формул [US94, PV05].

Атсериасом, Колаитисом и Варди [AKV04] была рассмотрена система доказательств, основанная на OBDD. В работы в данной системе мы должны выбрать некоторый порядок π и закодировать клозы исходной формулы в виде OBDD$[\pi]$. Доказательством является последовательность π-OBDD, где в последняя OBDD кодирует тождественно нулевую функцию, а на каждом шаге мы применяем одно из следующих правил:

- **join или** $\wedge$ мы выводим конъюнкцию двух уже выведенных OBDD;
- **weakening** мы выводим OBDD, которая семантически следует из выведенной ранее OBDD.

Мы будем обозначать такие системы OBDD$(\wedge, \text{weakening})$. Крайчек [Kra08] доказал первые экспоненциальные нижние оценки на данную систему доказательств.

В работе [BIKS17] мы построили короткое доказательство формул Clique-Coloring в системе OBDD$(\wedge, \text{weakening})$, и как следствие, мы показали, что система CP не моделирует систему OBDD$(\wedge, \text{weakening})$ и более того, OBDD$(\wedge, \text{weakening})$ строго сильнее CP*. Существование короткого доказательства данной формулы влечет отсутствие свойства эффективной монотонной интерполяции, однако техника интерполяции все равно помогает доказать нижние оценки.

Интересной подсистемой OBDD$(\wedge, \text{weakening})$ является система, в которой можно пользоваться только правилом объединения. Тверетина и др. [TSZ09] доказали нижнюю оценку на размер доказательства $\texttt{PHP}n+1n$ в системе OBDD$(\wedge)$ и тот факт, что OBDD$(\wedge)$ не моделирует резолюционную систему. В нашей работе [BIKS17] мы доказали, что обратное моделирование также невозможно, более того CP не моделирует OBDD$(\wedge)$.

Ярвисало [Jär11] доказал, что система OBDD$(\wedge)$ не моделирует древесную резолюцию. Также, в работе [Jär11] отмечено, что существует такая формула, что любое древесное резолюционное доказательство имеет экспоненциальный размер, но существует OBDD$(\wedge)$ доказательство данной формулы полиномиального размера. К сожалению, аргументы в указанной работе содержат ошибку. В нашей работе [BIKS17]

мы исправили доказательство и доказали более сильный результат: существует такая формула, что в некотором порядке любое OBDD($\wedge$, weakening) доказательство имеет суперполиномиальный размер, но существует полиномиальное OBDD($\wedge$) доказательство в другом порядке.

В работе [BIKS17] мы также закрыли вопрос, поставленный нами ранее в работе [IKRS17] и показали, что система OBDD($\wedge$, weakening, reordering) строго сильнее системы доказательств OBDD($\wedge$, weakening).

Коммуникационные протоколы на графах. В 1990 году Карчмер и Вигдерсон [KW90] рассмотрели следующую коммуникационную задачу `Bit`: Алиса получает на вход точку u из множества $U \subseteq \{0,1\}^n$, а Боб точку v из множества $V \subseteq \{0,1\}^n$, причем $U \cap V = \emptyset$, их цель найти такой индекс i, что $u_i \neq v_i$. Также была рассмотрена монотонная версия данной задачи `MonBit`, где цель Алицы и Боба найти такой индекс i, что $u_i = 1$ и $v_i = 0$. В работе [KW90] Карчмер и Вигдерсон доказали следующую теорему: для любой (монотонной) функции f существует (монотонная) булева формула размера S тогда и только тогда, когда существует коммуникационный протокол размера S для задачи `Bit` (`MonBit`), где $U = f^{-1}(1)$ и $V = f^{-1}(0)$.

В работе [Sok17] мы рассмотрели обобщение понятия коммуникационный протоколов на случай графов (классический коммуникационный протокол может быть описан деревом, где в листьях находятся ответы, а внутренние вершины помечены игроком, который делает текущий ход). Определение данных протоколов тесно связано с PLS играми, описанными в работах [Raz95, Pud10]. Мы показали, что для любой коммуникационной задачи существует коммуникационный протокол на графах размера S тогда и только тогда, когда для этой задачи существует PLS игра размера $\Theta(S)$. Мы также предъявили простое доказательство усиления теоремы Карчмера–Вигдерсона на случай графовых коммуникационных протоколов и и булевых схем.

Второй важной коммуникационной задачей является каноническая задача поиска $\texttt{Search}_\varphi$ для некоторой невыполнимой КНФ формулы $\varphi(x, y)$: Алиса получает на вход значение переменных x, Боб получает на вход значение переменных y, их цель найти клоз формулы φ, который не выполнен их совместной подстановкой. Нижние оценки на данную коммуникационную задачу позволяют доказывать нижние оценки на древовидные версии различных систем доказательств [BPS07], при этом данная задача достаточно хорошо изучена и получены достаточно сильные нижние оценки на классические коммуникационные протоколы для нее [BPS07, HN12, GP14].

В работе [Sok17] мы рассмотрели обобщение коммуникационных протоколов на графах — вещественные коммуникационные протоколы на графах (аналог классических вещественных коммуникационных протоколов [Kra98]). Мы доказали аналог теоремы Крайчека: если существует короткое доказательство формулы φ в системе Cutting Planes, то существует короткий вещественный коммуникационный протокол для задачи $\texttt{Search}_\varphi$. Также мы применили технику *бутылочного горлышка* из работы [HC99] для доказательства нижних оценок на вещественные коммуникационные протоколы для задачи $\texttt{Search}_\varphi$, как следствие были получены новые нижние оценки на вещественные монотонные схемы. Также при помощи данной техники нами были доказаны нижние оценки на обобщение системы доказательств CP — так называемую систему random Cutting Planes.

В работе [GGKS17] нами были доказаны новые нижние оценки на вещественные коммуникационные игры на графах. Как следствие был получен следующий результат: пусть минимальная ширина резолюционного доказательства формулы φ равна w, тогда минимальный размер доказательства формулы $\varphi \circ \mathtt{Ind}_{n^{256}}$ в системе CP равен $n^{\Omega(w)}$. Данная техника является второй техникой для доказательства нижних оценок в системе Cutting Planes, при этом, в отличие от предыдущей техники [GGKS17], нам удалось доказать нижнюю оценку для очень большого класса формул, что частично или полностью дает ответ на вопрос из книги Юкны [Juk12].

Коммуникационная модель на графах легко обобщается на более сложные системы доказательств, однако, нижние оценки на модели пока не доказаны (например на коммуникационной модели, описывающей систему Res($\oplus$)).

Публикации

[BIKS17] Sam Buss, Dmitry Itsykson, Alexander Knop, and Dmitry Sokolov. Reordering rule makes OBDD proof systems stronger. 2017. In progress.

[GGKS17] Ankit Garg, Mika Göös, Pritish Kamath, and Dmitry Sokolov. Monotone circuit lower bounds from resolution. 2017. https://eccc.weizmann.ac.il/report/2017/175/.

[IKRS17] Dmitry Itsykson, Alexander Knop, Andrey Romashchenko, and Dmitry Sokolov. On OBDD-Based Algorithms and Proof Systems That Dynamically Change Order of Variables. In Heribert Vollmer and Brigitte Vallée, editors, *34th Symposium on Theoretical Aspects of Computer Science (STACS 2017)*, volume 66 of *Leibniz International Proceedings in Informatics (LIPIcs)*, pages 43:1–43:14, Dagstuhl, Germany, 2017. Schloss Dagstuhl–Leibniz-Zentrum fuer Informatik.

[Sok17] Dmitry Sokolov. Dag-like communication and its applications. In *Computer Science – Theory and Applications: 12th International Computer Science Symposium in Russia, CSR 2017, Kazan, Russia, June 8-12, 2017, Proceedings*, pages 294–307. Springer International Publishing, 2017.

2 Преподавательская деятельность

1. Лектор по дополнительным главам дискретной математике в Академическом Университете.

2. Преподаватель по практике к курсу основы дискретной математики и математической логики в Академическом Университете.

3. Лектор по курсу DAG-like communication в KTH Royal Institute of Technology в Стокгольме.

3 Участие в конференциях и школах

1. Workshop on Complexity of Computation, Communication, Descriptions and Proofs. Moscow, Russia 2017. Higher School of Economics. Докладчик.
2. Swedish Summer School in Computer Science 2017. Stockholm, Sweden 2017. KTH Royal Institute of Technology. Участник.
3. The 12th International Computer Science Symposium in Russia. Kazan, Russia 2017. Докладчик.
4. Workshop "Proof Complexity and Beyond". Oberwolfach, Germany 2017. Участник.

4 Сравнение с заявкой

Задачи, указанные в заявке.

1. Теорема о компромиссе между памятью и размером доказательства была успешно доказана для системы Res($\oplus$) (старое название Res$_{lin}$).
2. Оценки на память в системе доказательств Res($\oplus$) по прежнему являются открытым вопросом.

Результаты, полученные в совместных в соавторами работах, по темам смежным с темой заявки.

1. Описание коммуникационных протоколов на графах.
2. Доказательство нижних оценок на коммуникационные протоколы на графах методом «бутылочного горлышка».
3. Перенос нижних оценок с резолюционной системы доказательств на CP и монотонные булевы схемы.
4. Доказательство нижних оценок на OBDD($\wedge$) систему доказательств.
5. Разделение различных вариантов OBDD систем доказательств.
6. Доказательство нижних оценок на алгоритмы для решения задачи выполнимости, основанные на OBDD.
7. Доказательство нижних оценок на размер доказательств в резолюционной системе для формул, кодирующих существование совершенного паросочетания в двудольно графе.

Результаты, полученные в совместных в соавторами работах, по другим темам.

1. Усиление теорема Тода и описание *промис* иерархии (аналог полиномиальной иерархии).
2. Построение иерархии эвристических вычислений.
3. Построение иерархии распределений.

Список литературы

[AKV04] Albert Atserias, Phokion G. Pg. Kolaitis, and Moshe Y. Vardi. Constraint propagation as a proof system. In Mark Wallace, editor, *Principles and Practice of Constraint Programming - CP 2004*, volume 3258 of *Lecture Notes in Computer Science*, pages 77–91. Springer, 2004.

[BIKS17] Sam Buss, Dmitry Itsykson, Alexander Knop, and Dmitry Sokolov. Reordering rule makes OBDD proof systems stronger. 2017. In progress.

[BPS07] 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, 2007.

[Bry85] Randal E Bryant. Symbolic manipulation of Boolean functions using a graphical representation. In Hillel Ofek and Lawrence A O'Neill, editors, *Proceedings of the 22nd ACM/IEEE conference on Design automation, DAC 1985, Las Vegas, Nevada, USA, 1985.*, pages 688–694. ACM, 1985.

[GGKS17] Ankit Garg, Mika Göös, Pritish Kamath, and Dmitry Sokolov. Monotone circuit lower bounds from resolution. 2017. https://eccc.weizmann.ac.il/report/2017/175/.

[GP14] Mika Göös and Toniann Pitassi. Communication lower bounds via critical block sensitivity. In *Symposium on Theory of Computing, STOC 2014, New York, NY, USA, May 31 - June 03, 2014*, pages 847–856, 2014.

[HC99] Armin Haken and Stephen A. Cook. An exponential lower bound for the size of monotone real circuits. *Journal of Computer and System Sciences*, 58(2):326–335, 1999.

[HN12] Trinh Huynh and Jakob Nordström. On the virtue of succinct proofs: amplifying communication complexity hardness to time-space trade-offs in proof complexity. In *Proceedings of the 44th Symposium on Theory of Computing Conference, STOC 2012, New York, NY, USA, May 19 - 22, 2012*, pages 233–248, 2012.

[IKRS17] Dmitry Itsykson, Alexander Knop, Andrei Romashchenko, and Dmitry Sokolov. On OBDD-Based Algorithms and Proof Systems That Dynamically Change Order of Variables. In Heribert Vollmer and Brigitte Vallée, editors, *34th Symposium on Theoretical Aspects of Computer Science, STACS 2017, March 8-11, 2017, Hannover, Germany*, volume 66 of *LIPIcs*, pages 43:1–43:14. Schloss Dagstuhl - Leibniz-Zentrum fuer Informatik, 2017.

[Jär11] Matti Järvisalo. On the Relative Efficiency of DPLL and OBDDs with Axiom and Join. In Jimmy Ho-Man Lee, editor, *Principles and Practice of Constraint Programming - CP 2011 - 17th International Conference, CP 2011, Perugia, Italy, September 12-16, 2011. Proceedings*, volume 6876 of *Lecture Notes in Computer Science*, pages 429–437. Springer, 2011.

[Juk12] Stasys Jukna. *Boolean Function Complexity: Advances and Frontiers*, volume 27 of *Algorithms and Combinatorics*. Springer, 2012.

[Kra98] Jan Krajíček. Interpolation by a game. *Math. Log. Q.*, 44:450–458, 1998.

[Kra08] Jan Krajiček. An exponential lower bound for a constraint propagation proof system based on ordered binary decision diagrams. *Journal of Symbolic Logic*, 73(1):227–237, 2008.

[KW90] Mauricio Karchmer and Avi Wigderson. Monotone circuits for connectivity require super-logarithmic depth. *SIAM J. Discrete Math.*, 3(2):255–265, 1990.

[Pud10] Pavel Pudlák. On extracting computations from propositional proofs (a survey). In *IARCS Annual Conference on Foundations of Software Technology and Theoretical Computer Science, FSTTCS 2010, December 15-18, 2010, Chennai, India*, pages 30–41, 2010.

[PV05] Guoqiang Pan and Moshe Y. Vardi. Search vs. Symbolic Techniques in Satisfiability Solving. *7th International Conference on Theory and Applications of Satisfiability Testing, SAT 2004, Revised Selected Papers*, 3542:235–250, 2005.

[Raz95] A. A. Razborov. Unprovability of lower bounds on circuit size in certain fragments of bounded arithmetic. *Izvestiya RAN. Ser. Mat.*, pages 201–224, 1995.

[Sok17] Dmitry Sokolov. Dag-like communication and its applications. In *Computer Science – Theory and Applications: 12th International Computer Science Symposium in Russia, CSR 2017, Kazan, Russia, June 8-12, 2017, Proceedings*, pages 294–307. Springer International Publishing, 2017.

[TSZ09] Olga Tveretina, Carsten Sinz, and Hans Zantema. An Exponential Lower Bound on OBDD Refutations for Pigeonhole Formulas. *Proceedings Fourth Athens Colloquium on Algorithms and Complexity*, 4(Acac):13–21, 2009.

[US94] Tomás E. Uribe and Mark E. Stickel. Ordered Binary Decision Diagrams and the Davis-Putnam Procedure. In Jean-Pierre Jouannaud, editor, *Constraints in Computational Logics, First International Conference, CCL'94, Munich, Germant, September 7-9, 1994*, volume 845 of *Lecture Notes in Computer Science*, pages 34–49. Springer, 1994.