УДК 510.52, 510.662
AMS MSC2020: 03F20, 03D15

Несколько слов о сложности доказательств

Соколов Д. О.

Санкт-Петербургский государственный университет;
Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН

Аннотация. Теория сложности доказательств изучает длины доказательств пропозициональных формул. За последние тридцать лет в данной области произошло ряд существенных прорывов, а также были открыты новые связи с другими разделами теории сложности вычислений. Мы рассмотрим, как основные задачи теории сложности доказательств, так и примеры применений.

Ключевые слова: теория сложности, системы доказательств, метод резолюций, булевы схемы.

Один из наиболее естественных вопросов математической логики: по заданному истинному утверждению оценить длину кратчайшего доказательства в какой-нибудь аксиоматической системе. Мы сосредоточимся на этом вопросе для пропозициональной логики, основном объекте теории сложности доказательств. Для удобства вместо истинных утверждений (тавтологий) мы перейдем ко всюду ложным утверждениям и будет рассматривать «доказательства» невыполнимости пропозициональных формул. Следуя терминологии теории сложности, мы будем изучать язык UNSAT невыполнимых пропозициональных формул в КНФ.

Начнем с основного определения, которое было сформулировано в работе [3].

Определение 1. *Системой доказательств для языка* UNSAT *будем называть такую полиномиально вычислимую функцию* $\Pi\colon \{0,1\}^* \times \{0,1\}^* \to \{0,1\}$, *что:*

- *если* $\varphi \in \mathsf{UNSAT}$, *то существует такое* $w \in \{0,1\}^*$, *что* $\Pi(\varphi, w) = 1$ *(будем говорить, что* w *— это доказательство для* φ*);*
- *если* $\varphi \notin \mathsf{UNSAT}$, *то для всех* $w \in \{0,1\}^*, \Pi(\varphi, w) = 0$.

Про системы доказательств можно думать в терминах игр. Рассмотрим двух игроков: Оптимист и Пессимист, которые получают формулу φ в КНФ от n переменных $x_1, \ldots, x_n$. Оптимист считает, что есть некоторый выполняющие набор для формулы φ, то есть такой набор значений $a_1, a_2, \ldots, a_n \in \{0, 1\}$, что $\varphi(a_1, a_2, \ldots, a_n) = 1$. А Пессимист считает что такого набора нет и пытается убедить в этом Оптимиста, предъявив некоторое доказательство w. При этом система доказательств определяется тем, какие доказательства Оптимист считает корректными.

Одним из классических примеров систем доказательств является резолюционная система. В данной системе доказательство π для формулы φ представляет собой такую упорядоченную последовательность дизъюнктов $\pi := D_1, \ldots, D_s$, что $D_s = \varnothing$ пустой дизъюнкт и для каждого $i \in [s]$ либо D_i это дизъюнкт φ, либо найдутся такие $j, k < i$, что D_i получен из D_j и D_k путем применения резолюционного правила

$$\frac{C \vee x \qquad D \vee \neg x}{C \vee D}$$

или правила ослабления

$$\frac{C}{D}\text{, где } [C \subseteq D].$$

В терминах нашего определения П — это алгоритм, который получает вместо формулу φ, и в качестве w он получает резолюционное доказательство, которое ему необходимо проверить.

Как мы уже замечали в начале, основной задачей сложности доказательств является оценка размера кратчайших доказательств невыполнимости формул в различных системах. И сложность доказательств — один из немногих разделов теории сложности, где удается получить безусловные нижние оценки. В частности: на резолюционную систему доказательств [5], на ряд систем алгебраического вывода [2, 6, 9]. Однако, для некоторых систем вопрос о нижних оценках по прежнему открыт, например для системы Фреге (Гильбертовская система).

Нижние и верхние оценки на сложность доказательств в различных системах часто удается переносить на другие модели вычислений.

1) Если бы нам удалось привести пример формул для которых кратчайшее доказательство имеет суперполиномиальный размер (от длины формулы) во всех системах, то это бы повлекло за собой неравенство классов $\mathsf{NP} \neq \mathsf{coNP}$ [3], и, в частности, классов $\mathsf{P} \neq \mathsf{NP}$, что является одной из «задач тысячелетия».
2) Даже если мы сосредоточимся на резолюционной системе доказательств, то нижние оценки размер доказательств в ней влекут нижние оценки на время работы популярных алгоритмов для решения задачи выполнимости булевых формул (что является NP-полной задачей) [1, 4].
3) Также, известных нижних оценок (на резолюционную систему, а также на ряд систем, основанных на алгебраическом выводе) хватает для получения сильных нижних оценок на монотонные модели вычисления, в частности на монотонные схемы и, так называемые, монотонные *span programs* [7, 8].

В докладе мы сосредоточимся на применения теории сложности, а также обсудим основные задачи и современные проблемы данной теории.

Список литературы

[1] *Alekhnovich, M.* Exponential Lower Bounds for the Running Time of DPLL Algorithms on Satisfiable Formulas / M. Alekhnovich, E. A. Hirsch, D. Itsykson // Journal of Automated Reasoning. — 2005. — Vol. 35. — P. 51–72.

[2] *Clegg, M.* Using the Groebner basis algorithm to find proofs of unsatisfiability / M. Clegg, J. Edmonds, R. Impagliazzo // Proceedings of the twenty-eighth annual ACM symposium on Theory of Computing (STOC '96). — New York : Association for Computing Machinery, 1996. — P. 174–183.

[3] *Cook, S. A.* The Relative Efficiency of Propositional Proof Systems / S. A. Cook, R. A. Reckhow // The Journal of Symbolic Logic. — 1979. — Vol. 44, iss. 1. — P. 36–50.

[4] *Davis, M.* A Computing Procedure for Quantification Theory / M. Davis, H. Putnam // Journal of the ACM. — 1960. — Vol. 7, iss. 3. — P. 201–215.

[5] *Haken, A.* The intractability of resolution // Theoretical Computer Science. — 1985. — Vol. 39. — P. 297–308.

[6] *Impagliazzo, R.* Lower Bounds for the Polynomial Calculus and the Gröbner Basis Algorithm / R. Impagliazzo, P. Pudlák, J. Sgall // Computational Complexity. — 1999. — Vol. 8. — P. 127–144.

[7] Monotone circuit lower bounds from resolution / A. Garg, M. Göös, P. Kamath, D. Sokolov // Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2018) / Eds. Ilias Diakonikolas, David Kempe, Monika Henzinger. — New York : Association for Computing Machinery, 2018. — P. 902–911.

[8] *Pitassi, T.* Lifting nullstellensatz to monotone span programs over any field. / T. Pitassi, R. Robere // Proceedings of the 50th Annual ACM SIGACT Symposium on Theory of Computing (STOC 2018) / Eds. Ilias Diakonikolas, David Kempe, Monika Henzinger. — New York : Association for Computing Machinery, 2018. — P. 1207–1219.

[9] Proof complexity in algebraic systems and bounded depth Frege systems with modular counting / S. Buss, R. Impagliazzo, J. Krajíček [et al.] // Computational Complexity. — 1997. — Vol. 6, iss. 3. — P. 256–298.

Библиографическая ссылка

Соколов, Д. О. Несколько слов о сложности доказательств // Всероссийская научная конференция «Математические основы информатики и информационно-коммуникационных систем». Сборник трудов. — Тверь : ТвГУ, 2021. — С. 69–72.
https://doi.org/10.26456/mfcsics-21-9

Сведения об авторах

Дмитрий Олегович Соколов
Санкт-Петербургский государственный университет;
Санкт-Петербургское отделение Математического института им. В. А. Стеклова РАН. Доцент; научный сотрудник

Санкт-Петербург, 14-я линия Васильевского острова 29
E-mail: sokolov.dmt@gmail.com