От булевых схем к доказательству теорем

Боков Г. В.

Вопрос о сложности доказательств теорем в формальных системах возникает во многих областях. С точки зрения вычислительной сложности точные нижние оценки сложности доказательств служат средством отделения классов вычислительной сложности. В современных SAT- и SMT-решателях анализ лежащих в их основе систем доказательств позволяет оценить производительность и ограниченность решателей. Центральное место в вопросе сложности доказательств отводится доказательству теорем классического исчисления высказываний. Несмотря на то, что за последние десятилетия удалось разработать много разнообразных техник для доказательства верхних и нижних оценок в различных пропозициональных системах, успеха в получении нижних оценок для классических систем доказательств достичь так и не удалось. Тем не менее, среди специалистов в области сложности доказательств сложилась прочная уверенность в том, что существует тесная связь между прогрессом в получении нижних оценок сложности булевых схем и прогрессом в получении нижних оценок размера пропозициональных доказательств. В работе будет рассказано о связи между булевыми схемами и системами доказательств теорем, о том, как идеи и методы, применяемые для оценки сложности схем, применяются для оценки сложности доказательств теорем.

Ключевые слова: Системы пропозициональных доказательств, сложность доказательств, булевы схемы, сложность схем, классы сложности.

Одной из центральных проблем теории сложности вычислений является вопрос о существовании полиномиальной разрешающей процедуры для классического пропозиционального исчисления. Её важность обусловлена взаимосвязью с задачей о равенстве классов сложности **P** и **NP** [Coo71], решение которой позволит получить ответ о сложности многих комбинаторных проблем [Kar72]. Сама проблема тесно связана с изучением сложности минимального пропозиционального вывода классических тавтологий [CR74].

Отправной точкой в изучении сложности пропозиционального вывода является работа Кука и Рекхау 1979 года [CR79], в которой они формализовали систему пропозициональных доказательств, как полиномиально вычислимую функцию, область значений которой совпадает с множеством всех пропозициональных тавтологий. В этой работе Кук и Рекхау установили фундаментальную взаимосвязь между сложностью пропозиционального выводы и классами сложности вычислений: существование *полиномиальной системы доказательств* пропозициональных формул, в которой каждая истинная формула имеет доказательство, сложность которого не превосходит некоторого полинома $p(n)$ от длины формулы n, равносильно тому, что класс **NP** замкнут относительно дополнений, т.е. $\mathbf{NP} = \mathbf{coNP}$. Данная взаимосвязь послужила основой так называемой *программы Кука-Рекхау*: так как класс **P** замкнут относительно дополнений, то для того, чтобы отделить его от класса **NP**, достаточно доказать отсутствие полиномиальной системы доказательств для классических тавтологий. Этот подход связан с получением суперполиномиальных нижних оценок сложности вывода.

На сегодняшний день суперполиномиальные нижние оценки известны только для слабых систем пропозициональных доказательств [Urq95, Raz96, UF96, Pud98, BP98]. Первая из таких оценок была получена еще в конце 60-х годов Цейтиным [Tse68] для подсистем резолюции. Первым же значительным с точки зрения программы Кука-Рекхау результатом является суперполиномиальная нижняя оценка для резолюции, найденная в 1985 году Хэйкеном [Hak85]. Начиная с конца 90-х годов подобные оценки были получены и для многих других систем доказательств: системы Фреге ограниченной глубины [Ajt94, BIK$^+$92, BIP93, KPW95], исчисление полиномов [CEI96, Raz98], системы Nullstellensatz [BIK$^+$96], системы линейных уравнений [BPR97, Pud97]. Для всех этих систем были получены экспоненциальные нижние оценки на длину вывода для конкретных последовательностей тавтологий, представляющих собой естественную интерпретацию известных комбинаторных утверждений. Наиболее полный обзор последних результатов в этой области можно найти в [Seg07].

В то же время, для сильных систем доказательств, таких как системы Фреге и расширенные системы Фреге [Kra95a], известны лишь линейные нижние оценки для длины вывода и квадратичные нижние оценки для размера вывода [Bus95, BG98]. Вопрос о существовании суперполиномиальных нижних оценок для таких систем до сих пор остается открытым. В первую очередь это связано с тем, что все известные методы доказательства нижних оценок (мощностной принцип, метод подстано-

вок [Kra97a], интерполяционные теоремы [Kra97b], соотношения между длиной и шириной опровержений в методе резолюции [BSW01], псевдослучайные генераторы [ABR$^+$04, Kra01, Kra04] и др.), которые хорошо зарекомендовали себя для слабых систем доказательств, оказались непригодными для систем Фреге [KP98]. Например, принцип Дирихле, как и другие комбинаторные принципы, использующие мощностные соображения, не может иметь сложного доказательства в системах Фреге [Bus87], поэтому любые комбинаторные принципы, требующие суперполиномиальных доказательств, должны быть очень сложными [BBP95]. В некоторых случаях вопрос о существовании нижних оценок удалось свести к оценке числа раундов интерактивной игры, но получить при этом нетривиальные нижние оценки не удалось [PB95, Pud00, Kra15].

Важность изучения сложности пропозиционального вывода не ограничивается только применением в области сложности вычислений в качестве средства отделения классов сложности. Здесь можно отметить полезную взаимосвязь между длиной вывода в сильных системах пропозициональных доказательств, подобных системам Фреге и их расширениям, и выполнимостью формул в ограниченной арифметике [Kra95b]. Также понимание устройства оптимального пропозиционального вывода необходимо для создания эффективных SAT-решателей и систем автоматического доказательства теорем [PS10, Bus12].

Одна из неожиданных и вместе с тем удивительных взаимосвязей была обнаружена между сложностью доказательства теорем и сложность булевых схем. Известно, что системы Фреге не зависят от выбора аксиом и правил вывода. Все такие системы полиномиально эквивалентны [CR79]. Однако системы Фреге можно охарактеризовать по классам формул, участвующих в выводах. И в этом случае не все системы Фреге будут полиномиально эквивалентны друг другу. Например, системы формул в конъюнктивных нормальных формах вместе с методом резолюции являются системами Фреге над формулами глубины 2. Для таких систем Фреге доказана экспоненциальная нижняя оценка длины вывода [Hak85]. Рассмотрение стандартных классов булевых схем

$$\mathbf{AC} \subset \mathbf{AC}^0[p] \subset \mathbf{TC}^0 \subseteq \mathbf{NC}^1 \subseteq \mathbf{P}/\mathrm{poly}$$

привело к появлению соответствующей иерархии систем Фреге. В этой иерархии **AC**-системам Фреге соответствуют системы Фреге над формулами ограниченной глубины, $\mathbf{NC}^1$-системы Фреге — это обычные системы Фреге, а $\mathbf{P}/\mathrm{poly}$-системы Фреге — это расширенные системы Фреге и системы Фреге с подстановкой.

На сегодняшний день экспоненциальные нижние оценки сложности булевых схем для конкретных функций были получены только для класса $\mathbf{AC}^0[p]$ [Raz87, Smo87]. Для систем Фреге экспоненциальные нижние оценки сложности вывода найдены только для **AC**-систем Фреге [Ajt94, BIK$^+$92, BIP93, KPW95]. Все попытки применить метод Разборова и Смоленского для $\mathbf{AC}^0[p]$-схем к система Фреге до сих успехом не увенчались. Несмотря на это, среди специалистов по сложности доказательств сложилась твердая уверенность, что прогресс в получении нижних оценок сложности булевых схем послужит толчком к получению нижних оценок размера пропозициональных доказательств. Хотя данная связь между булевыми схемами и системами доказательств часто постулируется [BP98], формального обоснования она до сих пор так и не получила [BBC16]. В тоже время, данный подход послужил толчком к появлению новых, интересных и открытых до сих пор проблем [Pud08].

Список литературы

[Ajt94] *Ajtai M.* The complexity of the pigeonhole-principle // Combinatorica, vol. 14, no. 4, 1994, pp. 417–433.

[ABR$^+$04] *Alekhnovich M., Ben-Sasson E., Razborov A. A., and Wigderson A.* Pseudorandom generators in propositional proof complexity // SIAM Journal on Computing, vol. 34, no. 1, 2004, pp. 67–88.

[BIK$^+$92] *Beame P. W., Impagliazzo R., Krajíček J., Pitassi T., Pudlák P., and Woods A.* Exponential lower bounds for the pigeonhole principle // In Proc. 24th ACM Symposium on Theory of Computing, 1992, pp. 200–220.

[BIK$^+$96] *Beame P. W., Impagliazzo R., Krajíček J., Pitassi T., and Pudlák P.* Lower bounds on Hilbert's Nullstellensatz and propositional proofs // Proc. London Mathematical Society, vol. 73, no. 3, 1996, pp. 1–26.

[BIP93] *Beame P. W., Impagliazzo R., and Pitassi T.* Exponential lower bounds for the pigeonhole principle // Computational Complexity, vol. 3, no. 2, 1993, pp. 97–140.

[BP98] *Beame P., Pitassi T.* Propositional proof complexity: Past, present, and future // Bulletin of the European Association for Theoretical Computer Science, The Computational Complexity Column, vol. 65, 1998, pp. 66–89.

[BSW01] *Ben-Sasson E. and Wigderson A.* Short proofs are narrow — resolution made simple // Journal of the ACM, vol. 48, no. 2, 2001, pp. 149–169.

[BBC16] *Beyersdorff O., Bonacina I. and Chew L.* Lower Bounds: From Circuits to QBF Proof Systems // ITCS '16 Proceedings of the 2016 ACM Conference on Innovations in Theoretical Computer Science, 2016, pp. 249–260.

[BG98] *Bonet M. L., Galesi N.* Linear Lower Bounds and Simulations in Frege Systems with Substitutions // CLS, Lecture Notes in Computer Science, Selected Papers of 11-th Computer Science Logic, vol. 1414, 1998, pp. 115–128.

[BPR97] *Bonet M. L., Pitassi T., and Raz R.* Lower bounds for cutting planes proofs with small coefficients // The Journal of Symbolic Logic, vol. 62, no. 3, 1997, pp. 708–728.

[BBP95] *Bonet M. L., Buss S. R., Pitassi T.* Are there hard examples for Frege systems // Feasible Mathematics II, 1995, pp. 30–56.

[Bus87] *Buss S. R.* The propositional pigeonhole principle has polynomial size Frege proofs // J. Symbolic Logic, vol. 52, 1987, pp. 916–927.

[Bus95] *Buss S. R.* Some remarks on lengths of propositional proofs // Archive for Mathematical Logic, vol. 34, no. 6, 1995, pp. 377–394.

[Bus12] *Buss S. R.* Towards NP–P via proof complexity and search // Annals of Pure and Applied Logic, vol. 163, 2012, pp. 906—917.

[CEI96] *Clegg M., Edmonds J., and Impagliazzo R.* Using the Groebner basis algorithm to find proofs of unsatisfiability // In Proc. 28th ACM Symposium on Theory of Computing, 1996, pp. 174–183.

[Coo71] *Cook S. A.* The complexity of theorem-proving procedures // Proceedings of the third annual ACM symposium on Theory of computing, 1971, pp. 151–158.

[CR74] *Cook S. A., Reckhow R. A.* On the lengths of proofs in the propositional calculus // Proceedings of the sixth annual ACM symposium on Theory of computing, 1974, pp. 135–148.

[CR79] *Cook S. A., Reckhow R. A.* The relative efficiency of propositional proof systems // J. Symbolic Logic, vol. 44, 1979, pp. 36–50.

[Hak85] *Haken A.* The intractability of resolution // Theoretical Computer Science, v. 39, 1985, pp. 297–308.

[Kar72] *Karp R. M.* Reducibility among combinatorial problems // Complexity of Computer Computations, R.E. Miller and J.W. Thatcher, ed., New York (Plenum Press), 1972, pp. 85–103.

[Kra95a] *Krajíček J.* On Frege and Extended Frege Proof Systems // Feasible Mathematics II, Series "Progress in Computer Science and Applied Logic", vol. 13, 1995, pp. 284-319.

[Kra95b] *Krajíček J.* Bounded Arithmetic, Propositional Logic, and Complexity Theory // Vol. 60 of Encyclopedia of Mathematics and Its Applications, Cambridge University Press, Cambridge, 1995.

[Kra97a] *Krajíček J.* On methods for proving lower bounds in propositional logic // Logic and Scientific Methods: Proc. of the Tenth International Congress on Logic, Methodology and Philosophy of Science, vol. 259, 1997, pp. 69–83.

[Kra97b] *Krajíček J.* Interpolation theorems, lower bounds for proof systems and independence results for bounded arithmetic // The Journal of Symbolic Logic, vol. 62, no. 2, 1997, pp. 457–486.

[Kra01] *Krajíček J.* Tautologies from pseudo-random generators // Bulletin of Symbolic Logic, vol. 7, no. 2, 2001, pp. 197–212.

[Kra04] *Krajíček J.* Dual weak pigeonhole principle, pseudo-surjective functions, and provability of circuit lower bounds // The Journal of Symbolic Logic, vol. 69, no. 1, 2004, pp. 265–286.

[Kra15] *Krajíček J.* A reduction of proof complexity to computational complexity for $AC^0[p]$ frege systems // Proceedings of the American Mathematical Society, vol. 143, no. 11, 2015, pp. 4951–4965.

[KP98] *Krajíček J., Pudlák P.* Some Consequences of Cryptoproof diagramical Conjectures for S^1_2 and EF // Information and Computation, vol. 140, issue 1, 1998, pp. 82–94.

[KPW95] *Krajíček J., Pudlák P., and Woods A.* Exponential lower bounds to the size of bounded depth Frege proofs of the pigeonhole principle // Random Structures and Algorithms, vol. 7, no. 1, 1995, pp. 15–39.

[PS10] *Pitassi T. and Santhanam R.* Effectively polynomial simulations // In Proc. 1st Innovations in Computer Science, 2010.

[Pud97] *Pudlák P.* Lower bounds for resolution and cutting planes proofs and monotone computations // The Journal of Symbolic Logic, vol. 62, no. 3, 1997, pp. 981–998.

[Pud98] *Pudlák P.* The lengths of proofs // Chapter VIII in S. R. Buss (ed.): Handbook of Proof Theory, 1998, pp. 547–637.

[Pud00] *Pudlák P.* Proofs as Games // The American Mathematical Monthly, vol. 107, no. 6, 2000, pp. 541–550.

[Pud08] *Pudlák P.* Twelve Problems in Proof Complexity // Computer Science —- Theory and Applications, CSR 2008, Lecture Notes in Computer Science, vol 5010, 2008, pp. 13–27.

[PB95] *Pudlák P. and Buss S. R.* How to lie without being (easily) convicted and the lengths of proofs in propositional calculus // Computer Science Logic: 8th Workshop, CSL '94 Kazimierz, Poland, September 25–30, 1994 Selected Papers, 1995, pp. 151–162.

[Raz96] *Razborov A. A.* Lower bounds for propositional proofs and independence results in bounded arithmetic // Proceedings of the 23rd ICALP, Lecture Notes in Computer Science, vol. 1099, 1996, pp. 48–62.

[Raz87] *Razborov A. A.* Lower bounds for the size of circuits of bounded depth with basis $\{\&, \oplus\}$ // Math. Notes Acad. Sci. USSR, vol. 41, no. 4, 1987, pp. 333—338.

[Raz98] *Razborov A. A.* Lower bounds for the polynomial calculus // Computational Complexity, vol. 7, no. 4, 1998, pp. 291–324.

[Seg07] *Segerlind N.* The complexity of propositional proofs // The Bulletin of Symbolic Logic, vol. 13, no. 4, 2007, pp. 417–481.

[Smo87] *Smolensky R.* Algebraic methods in the theory of lower bounds for Boolean circuit complexity // In Proc. of 19th ACM STOC, 1987, pp. 77—82.

[Tse68] *Tseitin G. C.* On the complexity of derivations in propositional calculus // In A. O. Slisenko, editor, Studies in Mathematics and Mathematical Logic, Part II, 1968, pp. 115–125.

[Urq95] *Urquhart A.* The Complexity of Propositional Proofs // Bulletin of Symbolic Logic, vol. 1, 1995, pp. 425–467.

[UF96] *Urquhart A., Fu X.* Simplified lower bounds for propositional proofs // Notre Dame Journal of Formal Logic, vol. 73, no. 4, 1996, pp. 523–544.

From Boolean circuits to theorem proving

Bokov G. V.

The question how difficult it is to prove given theorems in given formal systems arises in many areas. In computational complexity, lower bounds to the size of proofs offer an approach towards the separation of complexity classes. Analysis of proof systems underlying recent SAT solvers provides the main theoretical framework towards understanding the power and limitations of solving. The main part of research in proof complexity has concentrated on proof systems for classical propositional logic. Despite the fact that propositional proof complexity has made enormous progress over the past three decades in showing tight lower and upper bounds for many proof systems, some of strong classical proof systems have resisted all attempts for lower bounds for decades. Nevertheless, a general and long-standing belief in the proof complexity community asserts that there is a close connection between progress in lower bounds for Boolean circuits and progress in proof size lower bounds for strong propositional proof systems. In the paper we show how relates Boolean circuits and proof systems with respect to complexity, i.e. how ideas and techniques from Boolean circuit complexity applies to propositional proof complexity.

Keywords: Propositional proof systems, proof complexity, Boolean circuits, circuit complexity, complexity classes.