Complexity of Propositional Proofs
(Invited Talk)

Alexander Razborov[1,2]

[1] University of Chicago, Chicago IL 60637, USA
[2] Steklov Mathematical Institute, Moscow, 117966, Russia

The underlying question of propositional proof complexity is amazingly simple: when interesting propositional tautologies possess efficient (which usually means short) proofs in a given propositional proof system? This theory is extremely well connected to very different disciplines like computational complexity, theoretical cryptography, automated theorem proving, mathematical logic, algebra and geometry. And, given its mixed origins, methods and concepts employed in the area are also very diverse.

In this lecture we will try to accomplish as much of the following as possible; our choice of topics is highly biased and personal.

We will begin with a brief discussion of connections to the classical proof theory, notably bounded arithmetic. Essentially, for virtually all propositional proof systems of significance there exists a first-order logical theory such that *provability* in this theory can be almost equated with *efficient provability* in the original proof system. In a sense, both capture the philosophical concept of provability in the world in which all objects that can be used by the prover are of restricted computational complexity (and in particular are restricted in size).

We give a sample of concrete lower and upper bounds for weak proof systems. We definitely will mention the Feasible Interpolation Theorem, as well as more elaborate applications of the "locality" method.

It turns out that (apparently) all lower bounds for restricted models and explicit Boolean functions known in circuit complexity at the moment possess efficient propositional proofs [12, Appendix]. It is an extremely interesting open question whether the same systems can prove strong lower bounds for unrestricted circuits of formulas, i.e., if they can resolve major open problems in complexity theory like $NP \overset{?}{\subseteq} P/poly$ or $P \overset{?}{\subseteq} NC^1/poly$. While the prospect of giving an *unconditional* answer to these exciting questions does look slim at the moment, we will discuss the possibility of showing this under reasonable complexity assumptions [14, Introduction].

Somewhat surprisingly, it turned out [1] that certain techniques used in proof-complexity studies can give unexpected and strong applications in a very different area, (theoretical) machine learning. We will try to mention this application as well.

Another important by-product of propositional proof complexity consists in applications to studying so-called *integrality gaps* for a variety of linear or positive semi-definite relaxation procedures widely used by the algorithmic community.

F. Ablayev and E.W. Mayr (Eds.): CSR 2010, LNCS 6072, pp. 340–342, 2010.

From the side of propositional proof complexity, these procedures correspond to ordinary proof systems with a very distinct algebraic or geometric flavor (see [8] for a comprehensive catalogue), and we hope to spend a considerable time on these results.

All references in the list below not mentioned in the main text are to various books, surveys and other writings on proof complexity that serve various tastes and can be used for further reading on the subject.

References

1. Alekhnovich, M., Braverman, M., Feldman, V., Klivans, A.R., Pitassi, T.: Learnability and automatizability. In: Proceedings of the 45th IEEE Symposium on Foundations of Computer Science, pp. 621–630 (2004)
2. Beame, P.: Proof complexity. In: Computational Complexity Theory. IAS/Park City mathematics series, vol. 10, pp. 199–246. American Mathematical Society, Providence (2004)
3. Beame, P., Pitassi, T.: Propositional proof complexity: Past, present and future. In: Paun, G., Rozenberg, G., Salomaa, A. (eds.) Current Trends in Theoretical Computer Science: Entering the 21st Century, pp. 42–70. World Scientific Publishing, Singapore (2001)
4. Buss, S.R.: Bounded arithmetic and propositional proof complexity. In: Logic of Computation, pp. 67–122 (1997)
5. Buss, S.R.: Towards NP-P via proof complexity and search (2009), `http://math.ucsd.edu/~sbuss/ResearchWeb/lfcsSurvey`
6. Cook, S.A.: Feasibly constructive proofs and the propositional calculus. In: Proceedings of the 7th Annual ACM Symposium on the Theory of Computing, pp. 83–97 (1975)
7. Cook, S.A., Reckhow, A.R.: The relative efficiency of propositional proof systems. Journal of Symbolic Logic 44(1), 36–50 (1979)
8. Yu Grigoriev, D., Hirsch, E.A., Pasechnik, D.V.: Complexity of semi-algebraic proofs. In: Proceedings of the 19th Annual Symposium on Theoretical Aspects of Computer Science, pp. 419–430 (2002)
9. Krajíček, J.: Bounded arithmetic, propositional logic and complexity theory. Cambridge University Press, Cambridge (1995)
10. Pudlák, P.: The lengths of proofs. In: Buss, S. (ed.) Handbook of Proof Theory, pp. 547–637. Elsevier, Amsterdam (1998)
11. Pudlák, P.: Twelve problems in proof complexity. In: Hirsch, E.A., Razborov, A.A., Semenov, A., Slissenko, A. (eds.) CSR 2008. LNCS, vol. 5010, pp. 13–27. Springer, Heidelberg (2008)
12. Razborov, A.: Bounded Arithmetic and lower bounds in Boolean complexity. In: Clote, P., Remmel, J. (eds.) Feasible Mathematics II. Progress in Computer Science and Applied Logic, vol. 13, pp. 344–386. Birkhaüser, Basel (1995)
13. Razborov, A.: Lower bounds for propositional proofs and independence results in Bounded Arithmetic. In: Meyer auf der Heide, F., Monien, B. (eds.) ICALP 1996. LNCS, vol. 1099, pp. 48–62. Springer, Heidelberg (1996)
14. Razborov, A.: Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. Manuscript (2002), `http://www.genesis.mi.ras.ru/~razborov`

15. Razborov, A.: Propostional proof complexity. Lecture notes of a course taught at the University of Chicago (2009), `http://people.cs.uchicago.edu/~razborov/teaching/winter09/notes.pdf`
16. Segerlind, N.: The complexity of propositional proofs. Bulletin of Symbolic Logic 13(4), 417–481 (2007)
17. Urquhart, A.: The complexity of propositional proofs. Bulletin of Symbolic Logic 1, 425–467 (1995)