PROOF COMPLEXITY

ALEXANDER A. RAZBOROV

Proof complexity relates to the classical proof theory roughly in the same way computational complexity relates to the classical computability theory. Namely, instead of studying mere existence of proofs of certain formulas in a theory of interest, we are studying their *efficient* or *feasible* provability, where the exact meaning of this term depends on the context. It is worth noting immediately that the similarity between proof and computational complexities is much more than just an useful analogy; it appears rigorously in many different forms, tightly connects both areas and is very beneficial to each of them. We will see numerous examples throughout our course.

We will begin with a brief overview of Bounded arithmetic and equational theories. This was historically the first attempt to work out the principles of proof complexity entirely within the scope of classical proof theory. Namely, the central requirement of feasibility shifts from a proof itself (that is still a single finite object) to severely restricting the axioms of the underlying theory. Then "efficiency" comes in the form of the computational content one can *extract* from the proof via so-called witnessing theorems.

The rest of the course will be devoted to propositional proof complexity. In the computational world, it corresponds to non-uniform models, that is (mostly) Boolean circuits. Besides logic, this area is extremely well connected to many other directions, notably practical SAT solving, combinatorial optimization and operation research. While we will pay special attention to propositional proof systems underlying these connections: Resolution, Positivestellensatz (aka sum-of-squares proof system) and Cutting Planes, a significant amount of time will be also devoted to more logic-oriented systems like Frege, constant-depth Frege and Extended Frege.

We will primarily discuss, with or without proofs, several general methods for analyzing the complexity (measured by, say, their length or degree) of propositional proofs: restrictions, feasible interpolation,

size-width relation, pseudo-expectations. Time permitting, we can also do some or all of the following:

(1) Pseudo-random generators, feasible provability of the P vs. NP question [5].
(2) Space complexity.
(3) Lifting theorems.

Pre-requisites: some familiarity with the modern computational complexity (say, at the level of a few introductory chapters in [1]) might be useful, but I will also remind everything we need.

References

[1] S. Arora and B. Barak. *Computational Complexity: a Modern Approach*. Cambridge University Press, 2009.
[2] S. Cook and P. Nguyen. *Logical Foundations of Proof Complexity*. Cambridge University Press, 2014.
[3] A. Razborov. Proof complexity and beyond. *SIGACT News*, 47(2):66–86, 2016.
[4] J. Krajíček. *Proof Complexity (Encyclopedia of Mathematics and its Applications Book 170)*. Cambridge University Press, 2019.
[5] A. Razborov. Pseudorandom generators hard for k-DNF resolution and polynomial calculus resolution. *Annals of Mathematics*, 181(3):415–472, 2015.

University of Chicago, Chicago, USA and
Steklov Mathematical Institute, Moscow, Russia
E-mail address: razborov@math.uchicago.edu, razborov@mi-ras.ru