IAS/PCMI Summer Session 2000
Clay Mathematics Undergraduate Program
Advanced Course on Computational Complexity

Lecture 12: Measuring the Complexity of Proofs (Part 2)

David Mix Barrington and Alexis Maciel
August 1, 2000

In the previous lecture, we motivated, through a couple of examples, the idea of a proof system based on axioms and inference rules. We then defined the Sequent Calculus and briefly explained why this proof system is both sound and complete. We ended by asking whether the Sequent Calculus has proofs of polynomial size for every tautology.

In this lecture, we will finish covering the material that was originally planned for Lecture 11. We will define precisely what a proof system is and show that there is a proof system in which every tautology has a polynomial-size proof if and only if NP is closed under complement. As will be explained, we can then work towards a proof that P $\neq$ NP by proving exponential lower bounds for increasingly more powerful proof systems.

The plan for the next three lectures is to investigate the power of some of these systems. The goal will not be to present the most definite results, but to highlight the strong and fruitful connections between proof complexity and computational complexity.

The tautology that has been used most frequently in establishing lower bounds for various proof systems is perhaps the pigeonhole principle. So our first result will be to show that the pigeonhole principle (that is, the propositional tautology expressing this principle) has polynomial-size Frege proofs. This will be established by exploiting the fact that input bits can be added and compared to a threshold k by NC^1 circuits.

Second, we will consider the Resolution proof system, which can be viewed as a version of the Sequent Calculus in which all formulas are variables and the only rule is the cut rule. We will show that a certain restriction of Resolution can not prove the pigeonhole principle by studying, in terms of decision trees, the computational complexity of a search problem associated with the tautology.

Third, we will present a general method for proving lower bounds on the complexity of proof systems called the interpolation method. The idea is to establish that small proofs of certain tautologies can be translated into small circuits of a related computational problem. We will illustrate how this method has been used to prove lower bounds for the Cutting Planes proof system. Lines in a Cutting Planes proof are linear inequalities of the form $a_1x_1 + \cdots + a_nx_n \geq A$. New lines can be inferred from previous ones by addition and by multiplication and division by positive integers. The goal is to obtain the contradiction $0 \geq 1$, which then refutes the initial set of inequalities. Cutting Planes are more powerful than Resolution and no more powerful than the Sequent Calculus and Frege systems.

Finally, if time permits, we will briefly survey results concerning some other proofs systems such as Frege systems in which all formulas are of constant-depth. Once again, techniques and ideas from computational complexity play a key role in establishing lower bounds for these systems.