ICM 1998, Berlin, Aug. 18–27

Abstracts of Plenary and Invited Lectures

Section:

14. Mathematical Aspects of Computer Science

1991 MS Classification: 03F, 68Q, 68R05, 20C30, 14Q99
Pitassi, Toniann, University of Arizona, USA
Combinatorial and algebraic techniques in proof complexity

An very basic and fundamental question in logic is: How long does a proof of a propositional tautology have to be, as a function of the size of the tautology? This question is equivalent to whether or not NP equals coNP, and has many other connections with computer science and mathematics. In the last 20 years, significant advances have been made in this area, through the introduction of techniques from such areas as circuit complexity, combinatorics, and representation theory.

In this talk, we will survey some of the important advances that have been made recently. In an influential paper in the 70's, Cook and Reckhow began a systematic program of studying and classifying standard proof systems in terms of their relative complexity. (Some standard systems include: resolution, natural deduction, Frege systems, FOL and ZFC.) A key contribution of this work is the realization that the representation complexity of intermediate formulas in a proof (more specifically the complexity of the cut formulas in the proof) is the key property of proof system power. Thus, proof systems can be divided into groups and these groups correspond to well-known complexity classes.

This analogy/connection with complexity classes has led to several beautiful results in proof complexity lower bounds. Here we give a few examples. First, in breakthrough work by Ajtai, it was shown that the propositional pigeonhole principle does not have short bounded-depth Frege proofs. This result makes heavy use of ideas used to obtain lower bounds for bounded-depth circuits.

Secondly, Bonet, Pitassi and Raz, and independendently Razborov developed a new technique for proving lower bounds for various proof systems, including Cutting Planes and systems of bounded arithmetic. This technique, known as feasible interpolation, and first proposed by Krajicek, essentially shows that sometimes a proof system lower bound can be obtained directly from a corresponding circuit complexity lower bound. This technique has been extensively studied and generalized, and has been successfully used to prove many other proof system lower bounds (including work by Pudlak, Cook, and Haken.) Furthermore, feasible interpolation gives a precise tradeoff between proving power and proof search: If a proof system has feasible interpolation, then lower bounds for the proof system can be obtained (sometimes under assumptions). But on the other hand, if a proof system does not possess feasible interpolation, then it can be shown that proofs in the system cannot be searched for efficiently.

Most recently, algebraic proof systems have been studied, and techniques from the representation theory of the symmetric group have come into play in a very important way. This line of research, pioneered in a paper by Ajtai, has led to an important new lower bound for Frege systems with mod p counting gates, by Krajicek. One important aspect in this work is that uniformity of the underlying family of tautologies is exploited in a new and powerful way. We will survey the important developments highlighted above, and conclude by discussing some of the most important problems yet to be resolved.