Feasible Interpolation: Power and Limitations (Invited Talk)

Amirhossein Akbar Tabatabai

Bernoulli Institute, University of Groningen, Groningen, Netherlands

Abstract

Feasible interpolation is a property of a proof system, a complexity-sensitive variant of Craig interpolation, which has become a powerful tool in proof complexity. It can be used to establish the existence of hard theorems, that is, short formulas that require exponentially long proofs in a given system. In this talk, we provide a gentle introduction to feasible interpolation and its applications. We show that it holds for weak proof systems such as resolution and the cut-free sequent calculus, yielding exponential lower bounds on proof length. We then turn to strong proof systems, such as the sequent calculus LK, and show that feasible interpolation fails for them, assuming widely believed cryptographic hardness assumptions, including the security of RSA and the Diffie–Hellman key-exchange protocol against polynomial-size circuits. Finally, we explain how this failure implies that these strong proof systems are not automatable in a precise formal sense.

CI-BD-SOQE 2026: Workshop on Craig Interpolation, Beth Definability, and Second-Order Quantifier Elimination, at FLoC 2026: The 9th Federated Logic Conference, July 24–25, 2026, Lisbon, Portugal

amir.akbar@gmail.com (A. A. Tabatabai)