Proofs, Interpolants, and Relevance Heuristics

(HVC 2008 Award Winner)

Ken McMillan

Cadence Berkeley Labs

Abstract. The technique of Craig interpolation provides a means of extracting from a proof about a bounded execution of a system the necessary information to construct a proof about unbounded executions. This allows us to exploit the relevance heuristics that are built into modern SAT solvers and SAT-based decision procedures to scale model checking to larger systems.

This talk will cover applications of Craig interpolation in various domains, including hardware verification using propositional logic, and software verification using first-order logic.