Constrained Horn Clauses for Program Verification and Synthesis

Arie Gurfinkel ✉ 🏠 ⓘ
University of Waterloo, ON, Canada

—— **Abstract** ——————————————————————————————

First Order Logic (FOL) is a powerful formalism that naturally captures many interesting decision and optimization problems. In recent years, there has been a tremendous progress in automated logic reasoning tools, such as Boolean SATisfiability Solvers and Satisfiability Modulo Theory solvers. This enabled the use of logic and logic solvers as a universal solution to many problems in Computer Science, in general, and in Program Analysis, in particular. Most new program analysis techniques formalize the desired analysis task in a fragment of FOL, and delegate the analysis to a SAT or an SMT solver.

In this talk, we focus on a fragment of FOL called Constrained Horn Clauses (CHC) and the CHC solver SPACER. CHCs arise in many applications of automated verification. They naturally capture such problems as discovery and verification of inductive invariants; Model Checking of safety properties of finite- and infinite-state systems; safety verification of push-down systems (and their extensions); modular verification of distributed and parameterized systems; type inference, and many others.

Using CHC separates the process of developing a proof methodology (also known as generation of Verification Condition (VC)) from the algorithmic details of deciding whether the VC is correct. Such a flexible design simplifies supporting multiple proof methodologies, multiple languages, and multiple verification tasks with a single framework, without sacrificing performance and scalability.