Horn Clauses and Beyond for Relational and Temporal Program Verification

Hiroshi Unno
University of Tsukuba, Japan
uhiro@cs.tsukuba.ac.jp

In this talk, we present our recent and ongoing work on constraint solving for verification of higher-order functional programs, where we address two important classes of specifications: relational specifications [1] and dependent temporal specifications [2]. These classes impose a new challenge: validity checking of first-order formulas with least and greatest fixpoints respectively for inductive and coinductive predicates, which generalizes existing variants of constrained Horn clause (CHC) solving.

The former class of relational specifications includes functional equivalence, associativity, commutativity, distributivity, monotonicity, idempotency, and non-interference, whose verification often boils down to inferring mutual invariants among inputs and outputs of multiple function calls. To this end, we present a novel CHC solving method based on inductive theorem proving: the method reduces CHC solving to validity checking of first-order formulas with least fixpoints for inductive predicates, which are then checked by induction on the derivation of the predicates. The method thus enables relational verification by expressing and checking mutual invariants as induction hypotheses.

The latter class of dependent temporal specifications is used to constrain (possibly infinite) event sequences generated by the target program. We express temporal specifications as first-order formulas over finite and infinite strings that encode event sequences. The use of first-order formulas allows us to express temporal specifications that depend on program values, so that we can specify input-dependent temporal behavior of the target program. Furthermore, we use least and greatest fixpoints to respectively model finite and infinite event sequences generated by the target program. To solve such fixpoint constraints, we present a novel deductive system consisting of rules for soundly eliminating fixpoints via invariants and well-founded relations.

References

[1] Hiroshi Unno, Sho Torii, and Hiroki Sakamoto. Automating induction for solving Horn clauses. In *CAV '17*, pages 571–591. Springer, 2017.

[2] Yoji Nanjo, Hiroshi Unno, Eric Koskinen, and Tachio Terauchi. A fixpoint logic and dependent effects for temporal property verification. In *LICS '18*. ACM, 2018.