

Precise Fixpoint Computation through Strategy Iteration and Optimization

Helmut Seidl
Technische Universität München, Germany

This tutorial summarizes joint work with Thomas Gawlitza.

Program analysis through abstract interpretation tries to infer invariants of the program behavior. One approach to abstract interpretation is to formulate the collecting semantics of the program by means of constraints. For every program point, the collecting semantics returns the set of all program states which are possibly attained at runtime when reaching this program point. This constraint system then is abstracted to a constraint system computing over a complete lattice of abstract states - each of which represents a property of concrete states. The goal of the analysis then technically consists in computing a solution of the given constraint system over the complete lattice. Since smaller values represent more precise invariants, the analysis thus can be cast as an optimization problem.

We explore this relationship for the specific case of numerical program invariants such interval analysis, analysis of variable differences or octagon analysis which tries to determine tight bounds for differences as well as sums of program variables. All these problems have in common that the required complete lattice has infinite ascending chains such that ordinary Kleene fixpoint iteration may not terminate. Here, we show how strategy iteration can be applied to reduce the complicated optimization problem to a sequence of simpler optimization problems where known optimization techniques, e.g., for network flow, linear programming or semi-definite programming can be applied.

The tutorial consists of two parts. The first part considers numerical properties of integer variables. Here we show how a generalization of the Bellman-Ford algorithm allows to construct a precise interval analysis. This base approach is then enhanced to a precise analysis of variable differences. For that purpose, Bellman-Ford algorithm must be enhanced with a solver for a variant of the transportation problem.

The second part considers numerical properties of variables holding fractional values. Again we start out with an interval analysis. Due to multiplications with fractional values, Bellman-Ford is no longer applicable. Still, we succeed in constructing a precise interval analysis by replacing that algorithm with techniques from linear programming. That approach then is enhanced to a precise analysis for arbitrary linear or even quadratic template constraints.

References

- [1] A. Costan, S. Gaubert, E. Goubault, M. Martel, S. Putot. *A Policy Iteration Algorithm for Computing Fixed Points in Static Analysis of Programs*. CAV'05, pp. 462-475, 2005.
- [2] T. Gawlitza, H. Seidl. *Precise Fixpoint Computation Through Strategy Iteration*. ESOP'07, pp. 300-315, 2007.

- [3] S. Gaubert, E. Goubault, A. Taly, S. Zennou. *Static Analysis by Policy Iteration on Relational Domains*. ESOP'07, pp. 237-252, 2007.
- [4] T. Gawlitza, H. Seidl. *Precise Relational Invariants Through Strategy Iteration*. CSL'07, pp. 23-40, 2007.
- [5] T. Gawlitza, H. Seidl. *Precise Interval Analysis vs. Parity Games*. FM'08, pp. 342-357, 2008.
- [6] T. Gawlitza, H. Seidl. *Games through Nested Fixpoints*. CAV'09, pp. 291-305, 2009.
- [7] A. Adjé, S. Gaubert, E. Goubault. *Coupling Policy Iteration with Semi-definite Relaxation to Compute Accurate Numerical Invariants in Static Analysis*. ESOP'10, pp. 23-42, 2010.
- [8] T. Gawlitza, H. Seidl. *Computing Relaxed Abstract Semantics w.r.t. Quadratic Zones Precisely*. SAS'10, pp. 271-286, 2010.