Accelerated Abstract Lattices

Location:	LaBRI (Computer Science Research Laboratory of Bordeaux), University of Bordeaux, France
Team:	Formal Methods, Modeling and Verification Group
Contact:	Jérôme Leroux and Grégoire Sutre
Keywords:	Verification, Data-Flow Analysis, Infinite-State Systems, Symbolic Representations, Acceleration, Abstract Interpretation
Requirements:	Background in theoretical computer science, readiness to acquire basic knowledge on infinite-state systems and abstract interpretation.
Duration:	5 months
Stipend:	436 € per month

Summary

System verification often reduces to the effective computation of the reachability set, i.e, the set of all reachable configurations. In general, this set is infinite as the system's variables take values in an infinite domain (integers, clocks, queue channels, and so on). To represent and compute such infinite sets, one may use symbolic representations. For instance, linear constraints [1] and arithmetic automata [2] may be used for systems with counters.

There are two prominent families of verification methods based on symbolic computations : ones based on exact computations and others based on abstraction refinements. These two families are complementary. The first ones allow the (semi-)computation of the reachability set *RS* by an increasing sequence of sets contained in *RS*. The second ones are guided by the property to verify, and compute a precise over-approximation of *RS* by a decreasing sequence of sets containing *RS*.

Used separately, these techniques do not scale up to large, complex systems. The long-term objective of this proposal is to reduce the gap between these techniques, by limiting the loss of precision during approximated computations [3]. Our first results [4, 5] towards this goal address the exact computation of the least fix-point in an abstract lattice, or, put differently, the most precise inductive invariant that can be represented by an abstract value. Thus, the loss of precision is solely controlled by the choice of the abstract lattice (intervals, octagons [6], octahedra, and so on), and the resulting fix-point does not depend on the way that it is computed. This approach has provided efficient algorithms for interval analysis [4].

The objective of this proposal is to identify classes of systems and abstract lattices that support the exact computation of the least fix-point. As a starting point, the candidate will consider the class of Petri nets and the octagons abstract lattice. Next, extensions of the octagons will be considered: octahedra and templates.

References

1. P. Cousot and N. Halbwachs. *Automatic discovery of linear restraints among variables of a program*. In Proc. POPL'78, pages 84–96. ACM Press, 1978.
2. B. Boigelot and P. Wolper. *Representing Arithmetic Constraints with Automata: An Overview*. In Proc. ICLP'02, LNCS 2401, pages 1–19. Springer, 2002.
3. L. Gonnord and N. Halbwachs. *Combining widening and acceleration in linear relation analysis*. In Proc. SAS'06, LNCS 4134, pages 144–160. Springer, 2006.
4. J. Leroux, G. Sutre. *Accelerated Data-Flow Analysis*. In Proc. SAS'07, LNCS 4634, pages 184–199. Springer, 2007.
5. J. Leroux, G. Sutre. *Acceleration in Convex Data-Flow Analysis*. In Proc. FSTTCS'07, LNCS 4855, pages 520–531. Springer, 2007.
6. A. Miné. *A New Numerical Abstract Domain Based on Difference-Bound Matrices*. In Proc. PADO'01, LNCS 2053, pages 155–172. Springer, 2001.