Solving Multiple Containment Tests for Linear Constraints over Integers

Dmitri Chubarov* and Andrei Voronkov

Department of Computer Science
The University of Manchester

ABSTRACT

We consider the containment problem for sets integral solutions of systems of linear inequalities

$$\left\{ x \in \mathbb{Z}^k \,\middle|\, Ax \leq b \right\}.$$

Given two such sets Φ and Ψ, the Containment Problem as a decision problem is to tell if $\Phi \subseteq \Psi$. Many algorithms for model-checking of infinite-state systems require solving multiple instances of the problem when the same set Φ is to be tested for containment in different sets $\Psi_1 \ldots \Psi_k$. This is a different problem. We describe a way to represent a set Φ based on the computation of a Hilbert basis, such that containment in a set Ψ, represented with a system of linear inequalities, can be tested in linear time in the size of the basis and inequalities.

The representation used in the model-checker BRAIN [RV02] can be described as follows. The set Φ of integral solutions for a system of linear inequalities $Ax \leq b$ can be decomposed into a cone of solutions of the homogeneous part $C = \left\{ x \in \mathbb{Z}^k \,\middle|\, Ax \leq 0 \right\}$ and a finite set of vectors B, such that $\Phi = C + B$. The cone C has a finite Hilbert basis H. Since H and B are computed, containment test for Φ and Ψ can be performed by testing if each vector of $H \cup B$ satisfies Ψ. However the number of vectors in $H \cup B$ can be exponential in the size of the system (A, b).

The usual alternative is to apply the methods of integer programming to check that Ψ is consistent with the negation of every inequality which defines Φ. Testing consistency of a system of linear inequalities over integers is an NP-complete problem.

Depending on the number of containment tests, the performance gain on solving containment becomes worth the effort spent in computing the Hilbert basis. We observed the implementation which uses Hilbert bases to perform better when applied to model-checking for a class of infinite-state transition systems.

The model-checking problem is defined by a temporal logic and a class of transition systems. It is the problem to decide if a given temporal formula holds

* supported by an Overseas Research Students Award

over the sequences of states of the given transition system visited during the evolution of the system.

We consider a particular class of transition systems with states represented by integral vectors. Even for EF formulas which specify safety properties, the model-checking problem is undecidable. However, there exists a semi-decision procedure which decides model-checking for some special classes of systems [EFM99]. The procedure is based on the *backward reachability* algorithm.

The algorithm computes fixed points of the inverse transition relation. The inverse transition relation is the relation between states and all their possible predecessors. Instead of operating on individual states the algorithm operates simultaneously on sets of states defined by systems of linear inequalities. This allows to apply model-checking techniques to infinite state spaces and evade the "state explosion". For example, computation of a least fixpoint of a binary relation is an iterative process which generates an increasing sequence of sets of states. Each set is represented as a finite set of systems of linear inequalities. Each time a new system is generated it is checked for containment with the systems generated before, which results in multiple checks with the same system.

This pattern of behaviour is exhibited by the backward reachability algorithm, when it was applied to models of uniform cache-coherency protocols and broadcast protocols.

We have compared an algorithm used in BRAIN which computes Hilbert bases with a Gauss-Jordan solver of CLP(Q) on problems where rational and integer containment tests produce the same result and observed better results from the implementation from BRAIN. In our experiments we follow the methodology of using sequences of problems extracted from practical application [HNRV]. Preliminary results show that representing solutions of linear inequalities with Hilbert bases gives a significant performance gain on many reachability problems.

References

[RV02] Rybina, T., Voronkov, A.: Using canonical representations of solutions to speed up infinite-state model checking. Submitted

[EFM99] Esparza, J., Finkel, A., Mayr, R., On the Verification of Broadcast Protocols. Proceedings of LICS'99, pp. 352–359

[HNRV] Nieuwenhuis, R., Hillenbrand, T., Riazanov, A., Voronkov, A., On the Evaluation of Indexing Techniques for Theorem Proving, IJCAR'01, LNAI 2083, pp. 257–271