From Non-Disjoint Combination to Satisfiability and Model-Checking of Infinite-State Systems

Silvio Ghilardi[1] and Enrica Nicolini[2]

[1] Dipartimento di Informatica, Università degli Studi di Milano (Italia)
[2] LORIA & INRIA-Lorraine, Nancy (France)

Abstract. (*Joint work also with S. Ranise and D. Zucchelli*).In the first part of our contribution, we review recent results on combined constraint satisfiability for first order theories in the non-disjoint signatures case: this is done mainly in view of the applications to temporal satisfiability and model-checking covered by the second part of our talk, but we also illustrate in more detail some case-study where non-disjoint combination arises. The first case deals with extensions of the theory of arrays where indexes are endowed with a Presburger arithmetic structure and a length expressing 'dimension' is added; the second case deals with the algebraic counterparts of fusion in modal logics. We then recall the basic features of the Nelson-Oppen method and investigate sufficient conditions for it to be complete and terminating in the non-disjoint signatures case: for completeness we rely on a model-theoretic T_0-compatibility condition (generalizing stable infiniteness) and for termination we impose a noetherianity requirement on positive constraints chains. We finally supply examples of theories matching these combinability hypotheses.

In the second part of our contribution, we develop a framework for integrating first-order logic (FOL) and discrete Linear time Temporal Logic (LTL). Manna and Pnueli [7] have extensively shown how a mixture of FOL and LTL is sufficient to precisely state verification problems for the class of reactive systems: theories in FOL model the (possibly infinite) data structures used by a reactive system while LTL specifies its (dynamic) behavior. Our framework for the integration is the following: we fix a theory T in a first-order signature Σ and consider as a temporal model a sequence $\mathcal{M}_1, \mathcal{M}_2, \ldots$ of standard (first-order) models of T and assume such models to share the same carrier (or, equivalently, the domain of the temporal model to be 'constant'). Following [8], we consider symbols from a subsignature Σ_r of Σ to be *rigid*, i.e. in a temporal model $\mathcal{M}_1, \mathcal{M}_2, \ldots$, the Σ_r-restrictions of the $\mathcal{M}_i$'s must coincide. The symbols in $\Sigma \setminus \Sigma_r$ are called 'flexible' and their interpretation is allowed to change over time (free variables are similarly divided into 'rigid' and 'flexible'). For model-checking, the *initial states* and the *transition relation* are represented by first-order formulae, whose role is that of (non-deterministically) restricting the temporal evolution of the model.

In the quantifier-free case, we obtain sufficient conditions for decidability for both satisfiability and model-checking of safety properties *by lifting combination methods* for *non-disjoint* theories in FOL: noetherianity and T_0-compatibility (where T_0 is the theory axiomatizing the rigid subtheory) gives decidability of

Dagstuhl Seminar Proceedings 07401
Deduction and Decision Procedures
http://drops.dagstuhl.de/opus/volltexte/2007/1247

satisfiability, whereas T_0-compatibility and local finiteness give safety model-checking decidability. The proofs of these decidability results suggest how decision procedures for the constraint satisfiability problem of theories in FOL and algorithms for checking the satisfiability of propositional LTL formulae can be integrated. This paves the way to employ efficient Satisfiability Modulo Theories solvers in the model-checking of infinite state systems. We illustrate our techniques on some examples and discuss further work in the area.

Results from the first part of our talk are published in [1],[2], [3],[4], whereas the recent results mentioned in the second part are published in [5], [6].

References (Part I)

1. S. Ghilardi. Model theoretic methods in combined constraint satisfiability. *Journal of Automated Reasoning*, 33(3-4), 2004.
2. S. Ghilardi, E. Nicolini, S. Ranise, and D. Zucchelli. Decision procedures for extensions of the theory of arrays. *Annals of Mathematics and Artificial Intelligence*, 50(3-4):231–254, 2007.
3. S. Ghilardi, E. Nicolini, and D. Zucchelli. A comprehensive framework for combined decision procedures. *ACM Transactions on Computational Logic*. To appear.
4. E. Nicolini. *Combined decision procedures for constraint satisfiability*. PhD thesis, Dipartimento di Matematica, Università degli Studi di Milano, 2007.

References (Part II)

5. S. Ghilardi, E. Nicolini, S. Ranise, and D. Zucchelli. Combination methods for satisfiability and model-checking of infinite-state systems. In *Proc. of CADE 2007*, LNAI, 2007.
6. S. Ghilardi, E. Nicolini, S. Ranise, and D. Zucchelli. Noetherianity and combination problems. In *Proc. of FroCoS 2007*, LNAI, 2007.
7. Z. Manna and A. Pnueli. *Temporal Verification of Reactive Systems: Safety*. Springer-Verlag, 1995.
8. D. A. Plaisted. A decision procedure for combination of propositional temporal logic and other specialized theories. *Journal of Automated Reasoning*, 2(2), 1986.