Decision procedures for variable-inactive theories and two polynomial $\mathcal{T}$-satisfiability procedures*

(Position paper)

Maria Paola Bonacina and Mnacho Echenim

Dipartimento di Informatica – Università degli Studi di Verona**
Strada Le Grazie 15, I-39134 Verona, Italy

Most reasoning-based verification systems rely on *$\mathcal{T}$-decision procedures* for the validity of ground formulæ modulo a background theory $\mathcal{T}$ (*$\mathcal{T}$-decision problems*). Since testing validity and testing satisfiability are dual, these problems are called *Satisfiability Modulo Theories (SMT) problems*. Theories of data structures, such as *lists*, *arrays* or *records*, and linear arithmetic, or fragments thereof, appear in verification of microprocessors, where arrays can be used to model registers, programs, to be proved correct or at least free of certain bugs, and hybrid or reactive systems, to be proved safe or deadlock-free. Since most problems involve multiple theories, the ability to *reason in combinations of theories* is crucial. Since practical $\mathcal{T}$-decision problems are huge and still represent only part of the verification task, $\mathcal{T}$-decision procedure ought to be *efficient* and *scalable*.

The importance of these challenges spurred a variety of approaches to design *SMT-solvers*. The *eager* approach (e.g., [7]) reduces the $\mathcal{T}$-decision problem to an instance of SAT and applies a SAT-solver, typically based on the DPLL procedure. The *lazy* or *hybrid* approaches (e.g., [4, 8, 2, 12]) integrate a SAT-solver, that handles the Boolean part of the formula, with a *$\mathcal{T}$-satisfiability procedure*, that decides sets of ground unit clauses. Combination of theories is achieved by the *Nelson-Oppen scheme* [11] for stably infinite theories, or its extensions (e.g., [10]). The *hierarchic* approach (e.g., [9]) conceives combination of theories as *extension* of theories, where functions coming from one theory are *partial* with respect to another. An inference system for first-order logic with equality (FOL+=) is modified to reason about partial functions, and integrated with $\mathcal{T}$-satisfiability procedures to handle arithmetic [13].

The *rewrite-based* approach to $\mathcal{T}$-satisfiability [3] applies directly an inference system for FOL+=. If a refutationally complete inference system $\mathcal{I}$ is guaranteed to *terminate* on $\mathcal{T}$-satisfiability problems, a fair $\mathcal{I}$-strategy *is* a $\mathcal{T}$-satisfiability procedure. Termination was shown for the rewrite-based inference system $\mathcal{SP}$ and several theories in [3, 1]. The approach is *uniform*, because the presentation of the theory is part of the input. It is *modular*, because if the $\mathcal{SP}$-strategy is a $\mathcal{T}_i$-satisfiability procedure for $\mathcal{T}_1, \ldots \mathcal{T}_n$, it is also a $\mathcal{T}$-satisfiability procedure for

* Summary of *On variable-inactivity and polynomial $\mathcal{T}$-satisfiability procedures*, where more references can be found, available at `http://profs.sci.univr.it/~bonacina/gendp.html`, and submitted for publication.

** Authors' e-mail addresses: *mariapaola.bonacina@univr.it* and *echenim@sci.univr.it*

$\mathcal{T} = \bigcup_i \mathcal{T}_i$, provided the $\mathcal{T}_i$'s are *variable-inactive* [1], a condition satisfied by all theories in [3, 1, 5]. Variable-inactivity implies stable-infiniteness [6].

Although the experiments in [1] suggested that a theorem prover's balance of *genericity*, *robustness* and *reliability*, on one hand, and *efficiency* and *scalability*, on the other, deserves to be pursued, almost all the rewrite-based $\mathcal{T}$-satisfiability procedures of [3, 1, 5] are exponential (for some theories, e.g., arrays, this is a lower bound). A first contribution of this paper is to show how to derive *polynomial* rewrite-based $\mathcal{T}$-satisfiability procedures for the theories of *integer offsets* and *records with extensionality*. The theory of integer offsets is especially difficult, because its axiomatization is *infinite*. We present a *reduction* that makes the problem *finite* and yields a procedure whose time complexity is polynomial. The polynomial $\mathcal{T}$-satisfiability procedure for records is based on analyzing possible $\mathcal{SP}$-inferences in a variable-inactive theory and using the $\mathcal{SP}$-strategy as a *pre-processor* for part of the problem. Since variable-inactivity is the only hypothesis, these elements may apply to any other variable-inactive theory. As far as we know, this is the first polynomial $\mathcal{T}$-satisfiability procedure for the theory of records with extensionality.

A second contribution of this paper is a *generalization* of the rewrite-based approach from $\mathcal{T}$-satisfiability to $\mathcal{T}$-decision procedures. A lazy approach with rewrite-based $\mathcal{T}$-satisfiability procedures was experienced with in *haRVey*[1]. A tight integration as in the hybrid approaches would be problematic, because DPLL-based SAT-solvers do case analysis by backtracking, whereas rewrite-based inference engines are *proof-confluent* and do not require backtracking. We give a general and simple approach shown in Fig. 1. Assume that $\mathcal{T}$ is variable-inactive and we already know that any fair $\mathcal{SP}$-strategy is a $\mathcal{T}$-satisfiability procedure. A set of ground clauses S is *flattened* into a set S_1 of ground unit clauses and a set S_2 of ground non-unit clauses made only of equalities and inequalities of constants, in such a way that $\mathcal{T} \cup S$ and $\mathcal{T} \cup S_1 \cup S_2$ are equisatisfiable. The strategy is applied to $\mathcal{T} \cup S_1$ and generates a limit S_∞, which is finite by the assumption that the strategy is a $\mathcal{T}$-satisfiability procedure. We prove that under variable-inactivity the strategy is guaranteed to halt also on $S_\infty \cup S_2$, so that we have altogether a rewrite-based $\mathcal{T}$-decision procedure.

References

1. A. Armando, M. P. Bonacina, S. Ranise, and S. Schulz. New results on rewrite-based satisfiability procedures. *ACM TOCL*, to appear. Available at `http://profs.sci.univr.it/~bonacina/rewsat.html`.
2. A. Armando, C. Castellini, E. Giunchiglia, and M. Maratea. A SAT-based decision procedure for the boolean combination of difference constraints. In *Online Proc. SAT-7*, 2004.
3. A. Armando, S. Ranise, and M. Rusinowitch. A rewriting approach to satisfiability procedures. *Inf. Comput.*, 183(2):140–164, 2003.

[1] http://www.loria.fr/equipes/cassis/softwares/haRVey

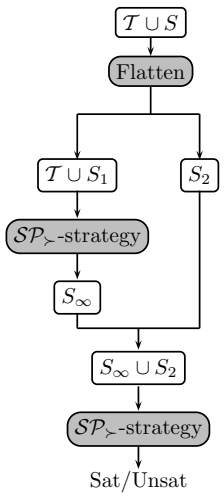

Fig. 1. Solving $\mathcal{T}$-decision problems by the rewrite-based approach.

4. C. W. Barrett, D. L. Dill, and A. Stump. Checking satisfiability of first-order formulas by incremental translation to SAT. In K. G. Larsen and E. Brinksma, editors, *Proc. CAV-14*, volume 2404 of *LNCS*, pages 236–249. Springer, 2002.
5. M. P. Bonacina and M. Echenim. Rewrite-based satisfiability procedures for recursive data structures. In B. Cook and R. Sebastiani, editors, *Proc. 4th PDPAR Workshop, FLoC 2006*, volume 174(8) of *ENTCS*, pages 55–70. Elsevier, 2007.
6. M. P. Bonacina, S. Ghilardi, E. Nicolini, S. Ranise, and D. Zucchelli. Decidability and undecidability results for Nelson-Oppen and rewrite-based decision procedures. In U. Furbach and N. Shankar, editors, *Proc. IJCAR-3*, volume 4130 of *LNAI*, pages 513–527. Springer, 2006.
7. R. E. Bryant and M. N. Velev. Processor verification using efficient reductions of the logic of uninterpreted functions to propositional logic. *ACM TOCL*, 2(1):93–134, 2001.
8. L. de Moura, H. Rueß, and M. Sorea. Lazy theorem proving for bounded model checking over infinite domains. In A. Voronkov, editor, *Proc. CADE-18*, volume 2392 of *LNAI*, pages 438–455. Springer, 2002.
9. H. Ganzinger, V. Sofronie, and U. Waldmann. Modular proof systems for partial functions with Evans equality. *Inf. Comput.*, 240(10):1453–1492, 2006.
10. S. Ghilardi, E. Nicolini, and D. Zucchelli. A comprehensive framework for combined decision procedures. In B. Gramlich, editor, *Proc. 5th FroCoS*, volume 3717 of *LNAI*, pages 1–30. Springer, 2005.
11. G. Nelson and D. C. Oppen. Simplification by cooperating decision procedures. *ACM TOPLAS*, 1(2):245–257, 1979.
12. R. Nieuwenhuis, A. Oliveras, and C. Tinelli. Solving SAT and SAT Modulo Theories: from an Abstract Davis-Putnam-Logemann-Loveland Procedure to DPLL(T). *J. ACM*, 53(6):937–977, Nov. 2006.
13. U. Waldmann and V. Prevosto. SPASS+T. In G. Sutcliffe, R. Schmidt, and S. Schulz, editors, *Proc. ESCoR, FLoc 2006*, volume 192 of *CEUR Workshop Proceedings*, pages 18–33, 2006.