Decidability and Undecidability Results for Nelson-Oppen and Rewrite-based Decision Procedures*

Maria Paola Bonacina[1], Silvio Ghilardi[2], Enrica Nicolini[3], Silvio Ranise[2,4], and Daniele Zucchelli[2,4]

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

Abstract. In the context of combinations of theories with disjoint signatures, we classify the component theories according to the decidability of constraint satisfiability problems in arbitrary and in infinite models, respectively. We exhibit a theory T_1 such that satisfiability is decidable, but satisfiability in infinite models is undecidable. It follows that satisfiability in $T_1 \cup T_2$ is undecidable, whenever T_2 has only infinite models, even if signatures are disjoint and satisfiability in T_2 is decidable.
In the second part of the paper we strengthen the Nelson-Oppen decidability transfer result, by showing that it applies to theories over disjoint signatures, whose satisfiability problem, in either arbitrary or infinite models, is decidable. We show that this result covers decision procedures based on rewriting, complementing recent work on combination of theories in the rewrite-based approach to satisfiability.

1 Introduction

In many applications of automated reasoning (for instance to software verification), it is important to decide the satisfiability of conjunctions of literals modulo a given background theory; quite often, it is also necessary to combine modularly such decision procedures to unions of background theories. If such theories have disjoint signatures and are stably infinite (which means that we can safely restrict to infinite models to decide satisfiability of literals), then the well-known Nelson-Oppen combination schema provides a combination transfer result. Recently, relaxing the stably infiniteness requirement has received a lot of attention in order to design combination schemas handling theories that are not stably-infinite. For instance,[1] Tinelli and Zarba [22] have shown how to combine

* The full version of this paper is available as a Technical Report RI DSI 308-06, Università degli Studi di Milano, at `http://homes.dsi.unimi.it/~zucchell/publications/techreport/BoGhiNiRaZu-RI308-06.pdf`

[1] For lack of space, we only discuss results that are closely related to ours (see, e.g., [19] for an overview on combination of decision procedures and references).

U. Furbach and N. Shankar (Eds.): IJCAR 2006, LNAI 4130, pp. 513-527, 2006.

an arbitrary theory with one satisfying requirements which are stronger than stable-infiniteness. Thus, contrary to the combination schema by Nelson-Oppen [14], such a schema is asymmetric in the sense that the requirements on the component theories are not the same.

In this paper, we consider combinations of theories whose signatures are disjoint and classify the component theories according to the decidability of their satisfiability problems in arbitrary and in infinite models. Assume that the satisfiability problem in a theory T_1 is decidable in arbitrary models but not in infinite models. Then, any combination of such a T_1 with a theory T_2 that does not have finite models yields an undecidable satisfiability problem. This holds even if T_1 and T_2 have disjoint signatures and even if satisfiability in T_2 is decidable in arbitrary models. As a consequence of this observation, we obtain the first (undecidability) result of the paper, by exhibiting a theory such that the satisfiability problem is decidable, whereas the satisfiability problem in infinite models is undecidable.

The second result of the paper is related to decision procedures based on rewriting. Armando et al [1] recently showed how to use a rewrite-based inference system to obtain decision procedures for (disjoint) unions of *variable-inactive* theories, when there exist rewrite-based decision procedures for the component theories. Here, we explain the relationship between variable-inactivity and stable-infiniteness. We show that if a theory is not stably infinite, then the inference system is guaranteed to generate clauses that constrain the cardinality of its models, so that the theory is not variable-inactive. This result has two applications: first, it complements the combination schema of [1] for (disjoint) unions of theories that have a rewrite-based satisfiability procedures. Second, it suggests a simple way to combine the rewrite-based approach with constraint-solving techniques that check satisfiability in finite models.

2 Preliminaries

A *signature* Σ is an (at most countable) set of functions and predicate symbols, each of them endowed with the corresponding arity. We assume the binary equality predicate symbol '=' to be always present in any signature Σ. The signature obtained from Σ by the addition of a set of new constants (that is, 0-ary function symbols) $\mathcal{K}$ is denoted by $\Sigma \cup \mathcal{K}$ or by $\Sigma^{\mathcal{K}}$; when the set of constants is finite, we use letters $\underline{a}, \underline{b}, \underline{c}$, etc. in place of $\mathcal{K}$. We have the usual notions of Σ-*term*, (full first order) -*formula*, -*atom*, -*literal*, -*clause*, -*positive clause*, etc.: e.g., an atom is an atomic formula, a literal is an atom or the negation of an atom, a clause is a multiset of literals, a positive clause is a multiset of atoms, etc. Abusing notation, we write a clause C either as the disjunction of its literals or as a sequent $\Delta_1 \Rightarrow \Delta_2$, meaning that Δ_1 (resp. Δ_2) contains the negative (resp. positive) literals of C. Terms, literals, clauses and formulæ are called *ground* whenever variables do not appear. Formulæ without free variables are called *sentences*. The universal (resp. existential) closure of a formula ϕ is the sentence obtained from ϕ by adding a prefix of universal (resp. existential) quantifiers binding all

variables occurring free in ϕ. A *Σ-theory* T is a set of sentences (called the axioms of T) in the signature Σ. If T is finite, the theory is said to be finitely axiomatized. A *universal* theory is a theory whose axioms are universal closures of quantifier-free formulae.

From the semantic side, we have the standard notion of a *Σ-structure* $\mathcal{A}$: this is a support set endowed with an arity-matching interpretation of the function and predicate symbols from Σ. We use $f^{\mathcal{A}}$ (resp. $P^{\mathcal{A}}$) to denote the interpretation of the function symbol f (resp. predicate symbol P) in the structure $\mathcal{A}$. The support set of a structure $\mathcal{A}$ is indicated by the notation $|\mathcal{A}|$. We say that $\mathcal{A}$ is *finite* when there exists an integer $N > 0$ such that the cardinality of $|\mathcal{A}|$ is less than N; if such an integer does not exist, we say that $\mathcal{A}$ is *infinite*. The *truth* of a Σ-formula in $\mathcal{A}$ is defined in the standard way (so that truth of a formula is equivalent to truth of its *universal* closure). A formula ϕ is *satisfiable* in $\mathcal{A}$ iff its *existential* closure is true in $\mathcal{A}$.

A Σ-structure $\mathcal{A}$ is a *model* of a Σ-theory T (in symbols $\mathcal{A} \models T$) iff all axioms of T are true in $\mathcal{A}$. For models of a Σ-theory T we shall use the letters $\mathcal{M}, \mathcal{N}, \ldots$ to distinguish them from arbitrary Σ-structures. If ϕ is a formula, $T \models \phi$ ('*ϕ is a logical consequence of T*') means that ϕ is true in any model of T. A Σ-theory T is *complete* iff for every Σ-sentence ϕ, either ϕ or $\neg\phi$ is a logical consequence of T; T is *consistent* iff it has a model.

A *Σ-constraint* in a signature Σ is a finite set of ground $\Sigma^{\underline{a}}$–literals (where $\underline{a}$ is a finite set of new free constants). The *constraint satisfiability problem* for a Σ-theory T is the problem of deciding whether a Σ-constraint is satisfiable in a model of T: if this problem is decidable, we say that the theory T is *$\exists$-decidable*. Notice that, equivalently, T is $\exists$-decidable iff it is decidable whether a universal Σ-formula is entailed by the axioms of T.

3 Satisfiability in Infinite Models

Let T_1 and T_2 be theories such that the signature Σ_1 of T_1 is disjoint from the signature Σ_2 of T_2, i.e., $\Sigma_1 \cap \Sigma_2$ contains only the equality symbol. We consider the decidability of the constraint satisfiability problem of the theory $T_1 \cup T_2$. We are especially interested in establishing the relationships between the decidability of the constraint satisfiability problems in the component theories T_1 and T_2, and the decidability of the constraint satisfiability problem in $T_1 \cup T_2$.

3.1 Undecidability Result

Let us recall two simple facts. First, combined word problems are decidable whenever the word problems for the component theories are decidable [18]. Second, it is commonly believed that combining word problems is more difficult than combining constraint satisfiability problems - the reason is that the algorithms to be combined are less powerful, as they can handle only constraints formed by a single negative literal. From these two observations, one may conjecture that the decidability of the constraint satisfiability problem in $T_1 \cup T_2$ always follows

from the decidability of the constraint satisfiability problem in T_1 and T_2. Contrary to expectation, all known combination results for the decidability of the constraint satisfiability problems in unions of theories (such as [14,22]) assume that the component theories satisfy certain requirements. The key observation is that such requirements are related to the satisfiability of constraints in infinite models of a component theory. For example, the Nelson-Oppen combination schema [14] requires the component theories to be stably-infinite. A Σ-theory T is *stably infinite* iff every Σ-constraint satisfiable in a model of T is satisfiable in an infinite model of T. Motivated by this observation, we introduce the following definition.

Definition 3.1. *Let T be a Σ-theory; we say that T is* $\exists_\infty$-decidable *iff it is $\exists$-decidable and moreover it is decidable whether any Σ-constraint Γ is satisfiable in some* infinite *model of T.*

From the definition, it is trivially seen that $\exists$-decidability is equivalent to $\exists_\infty$-decidability in the case of stably infinite theories. To illustrate the interest of studying the decidability of satisfiability in the infinite models of a theory, we state the following

Theorem 3.1. *Let T_i be a Σ_i-theory (for $i = 1, 2$) and let the signatures Σ_1, Σ_2 be disjoint. If T_1 is $\exists$-decidable but it is not $\exists_\infty$-decidable and if T_2 is consistent, $\exists$-decidable but does not admit finite models, then the constraint satisfiability for $T_1 \cup T_2$ is undecidable.*

Proof. We simply show that a Σ_1-constraint Γ is $T_1 \cup T_2$-satisfiable iff it is satisfiable in an infinite model of T_1. One side is obvious; for the other side, pick infinite models $\mathcal{M}_1$ of $T_1 \cup \Gamma$ and $\mathcal{M}_2$ of T_2 (the latter exists by consistency of T_2). By Löwhenheim-Skolem theorem, we can assume that both models are countable, i.e. that they have the same support (up to isomorphism). But then, we can simply put together the interpretations of functions and predicate symbols and get a model of $T_1 \cup T_2 \cup \Gamma$. □

We notice that there are many theories which are $\exists$-decidable and have only infinite models. One such theory is Presburger Arithmetic, another one is the theory of acyclic lists [17]. More interestingly, one could ask the following

QUESTION 1: Are there $\exists$-decidable theories that are not $\exists_\infty$-decidable?

If the answer is positive, then Theorem 3.1 implies that *there exist theories which are $\exists$-decidable and whose union is not $\exists$-decidable.* In Section 4, we exhibit some theories that are $\exists$-decidable but not $\exists_\infty$-decidable, thereby answering *QUESTION 1* positively.

3.2 Decidability Result

Notwithstanding the negative result implied by Theorem 3.1, we observe that when both T_1 and T_2 are $\exists_\infty$-decidable, we are close to get the decidability of constraint satisfiability in $T_1 \cup T_2$. To understand why, recall the following well-known fact.

Lemma 3.1. *Let Λ be a set of first-order sentences. If Λ does not admit infinite models, then there must exist an integer $N > 0$ such that, for each model $\mathcal{M}$ of Λ, the cardinality of the support set of $\mathcal{M}$ is bounded by N.*

For a proof, the interested reader is referred to any introductory textbook about model theory (see, e.g., [23]). The key idea is to apply compactness to infinitely many 'at-least-n-elements' constraints (these are the constraints expressed by the formulæ $\exists x_1, \ldots, x_n \bigwedge_{i \neq j} x_i \neq x_j$). It is interesting to notice that the above bound on the cardinality of finite models can be effectively computed for $\exists$-decidable theories:

Lemma 3.2. *Let T be an $\exists$-decidable Σ-theory; whenever it happens*[2] *that a given Σ-constraint Γ is not satisfiable in an infinite model, one can compute a natural number N such that all models of $T \cup \Gamma$ have cardinality at most N.*

Proof. For $h = 2, 3, \ldots$, add the following set $\delta_h := \{c_i \neq c_j \mid 1 \leq i < j \leq h\}$ of literals to $T \cup \Gamma$, where the constants $c_1, \ldots, c_h$ are fresh.[3] Clearly, if $T \cup \Gamma \cup \delta_h$ is unsatisfiable, then we get a bound for the cardinality of the models of $T \cup \Gamma$. Since, by Lemma 3.1, such a bound exists, the process eventually terminates. □

Definition 3.2. *An $\exists_\infty$-decidable Σ-theory T is said to be* strongly $\exists_\infty$*-decidable iff for any finite Σ-structure $\mathcal{A}$, it is decidable whether $\mathcal{A}$ is a model of T.*

It is not difficult to find strongly $\exists_\infty$-decidable theories. For example, any finitely axiomatizable $\exists_\infty$-decidable Σ-theory with a finite Σ is strongly $\exists_\infty$-decidable, since it is sufficient to check the truth of the axioms for finitely many valuations. Now, we are in the position to state and prove the following modularity property for $\exists_\infty$-decidable theories.

Theorem 3.2. *Let T_i be a strongly $\exists_\infty$-decidable Σ_i-theory (for $i = 1, 2$) such that Σ_1, Σ_2 are finite and disjoint. Then the combined theory $T_1 \cup T_2$ is $\exists$-decidable.*[4]

Proof. Let Γ be a finite set of ground $\Sigma_1 \cup \Sigma_2$-literals containing free constants. By well-known means (see, e.g., [5]), we can obtain an equisatisfiable set $\Gamma_1 \cup \Gamma_2$ such that Γ_i contains only $\Sigma_i^{\underline{a}}$-symbols, for $i = 1, 2$ and for some free constants $\underline{a}$. Let Γ_0 be an *arrangement* of the constants $\underline{a}$, i.e. a finite set of literals such that either $a_i = a_j \in \Gamma_0$ or $a_i \neq a_j \in \Gamma_0$, for $i \neq j$ and $a_i, a_j \in \underline{a}$. Clearly, $\Gamma_1 \cup \Gamma_2$ is satisfiable iff $\Gamma_1 \cup \Gamma_0 \cup \Gamma_2$ is satisfiable for some arrangement Γ_0 of the constants $\underline{a}$. From the fact that theories T_1, T_2 are both $\exists_\infty$-decidable, the following case analysis can be *effectively* performed:

[2] There is a subtle point here: Lemma 3.2 applies to all $\exists$-decidable theories, but it is really useful only for $\exists_\infty$-decidable theories, because only for these theories the hypothesis 'Γ in not satisfiable in an infinite model of T' can be effectively checked.

[3] Notice that the literals in δ_h are simply the Skolemization of the 'at-least-h-elements' constraint.

[4] This result can be easily generalized to the combination of $n > 2$ theories.

- If $\Gamma_0 \cup \Gamma_i$ is satisfiable in an infinite model of T_i (for both $i = 1, 2$), then $\Gamma_0 \cup \Gamma_1 \cup \Gamma_2$ is satisfiable in an infinite model of $T_1 \cup T_2$ by the standard argument underlying the correctness of the Nelson-Oppen combination schema (see, e.g., [21,12]).
- If $\Gamma_0 \cup \Gamma_i$ is unsatisfiable in any infinite model of T_i (for either $i = 1$ or $i = 2$), then (by Lemma 3.2) we can effectively compute an integer $N > 0$ such that each model $\mathcal{M}$ of $T \cup \Gamma_i \cup \Gamma_0$ has cardinality less than N. Hence, it is sufficient to exhaustively search through $\Sigma_1 \cup \Sigma_2 \cup \underline{a}$-structures up to cardinality N. The number of these structures is finite because Σ_1 and Σ_2 are finite and, by Definition 3.2, it is possible to effectively check whether each such a structure is a model of T_1 and T_2, and hence also of $T_1 \cup T_2 \cup \Gamma_0 \cup \Gamma_1 \cup \Gamma_2$. If a model is found, the procedure returns 'satisfiable', otherwise another arrangement Γ_0 (if any) is tried. □

Since a stably infinite theory is $\exists$-decidable if and only if it is $\exists_\infty$-decidable, it is clear that Theorem 3.2 substantially generalizes Nelson-Oppen result (the further requirement of Definition 3.2 being only a technical condition which is usually fulfilled). Theorem 3.2 raises the following

QUESTION 2: Is there a practical sufficient condition for a theory to be strongly $\exists_\infty$-decidable?

Clearly, stably infinite $\exists$-decidable theories are $\exists_\infty$-decidable. More interesting examples are given in Section 5, where we will show that, whenever a finitely axiomatized theory T admits a rewrite-based decision procedure for its constraint satisfiability problem [2,1], T is not only $\exists$-decidable but also strongly $\exists_\infty$-decidable.

4 Undecidability

In this section, we give an affirmative answer to *QUESTION 1* by defining some $\exists$-decidable theories that are not $\exists_\infty$-decidable. Let Σ_{TM_∞} be the signature containing (in addition to the equality predicate) the following (infinite) set of propositional letters $\{P_{(e,n)} \mid e, n \in \mathbb{N}\}$. Consider the propositional letter $P_{(e,n)}$: we regard e as the index (i.e. the code) of a Turing Machine and n as the input to the Turing machine identified by e (this coding is possible because of basic results about Turing machines, see, e.g., [16]). We indicate by $k : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \cup \{\infty\}$ the (non-computable) function associating to each pair (e, n) the number $k(e, n)$ of computation steps of the Turing Machine e on the input n. We write $k(e, n) = \infty$ when the computation does not halt. The axioms of the theory TM_∞ are the universal closures of the following formulæ:

$$P_{(e,n)} \rightarrow \bigvee_{i<j\leq m} x_i = x_j, \qquad \text{if } k(e, n) < m. \tag{1}$$

Two observations are in order. First, the property "being an axiom of TM_∞" is decidable, because the ternary predicate $k(e, n) < m$ is recursive. Indeed, it is

sufficient to run the Turing Machine e on input n and wait at most m computation steps to verify whether e halts. Second, the consequent of implication (1) is an *at-most cardinality constraint*, i.e. it is a formula of the form

$$\bigvee_{i \neq j} x_i = x_j \tag{2}$$

where x_i, x_j are (implicitly universally quantified) distinct variables for $i, j = 1, \ldots, n$, which constrain the domain of any model to contain at most n elements. Thus, axioms of the form (1) tells us that if $P_{(e,n)}$ holds and the Turing Machine e halts in at most m steps, then the cardinality of the domains of a model is bounded by m. These properties allow us to state and prove the following key result:

Proposition 4.1. *The theory TM_∞ is $\exists$-decidable but it is not $\exists_\infty$-decidable.*

Proof. To show that the theory is $\exists$-decidable, consider a constraint Γ over the signature $\Sigma^{\underline{a}}_{TM_\infty}$. First, guess an arrangement Γ_0 for the constants $\underline{a}$ and check the set of equations and inequations from $\Gamma \cup \Gamma_0$ for consistency in the pure theory of equality. Then, if the satisfiability check succeeds, Γ_0 explicitly gives the minimum cardinality m for $\Gamma \cup \Gamma_0$ to be satisfied. Clearly, $\Gamma \cup \Gamma_0$ is unsatisfiable if it contains both $P_{(e,n)}$ and $\neg P_{(e,n)}$. If this is not the case, we still have to consider the constraints represented by axiom (1), which states that if a literal of the kind $P_{(e,n)}$ is in a Σ_{TM_∞}-constraint, such a constraint can be only satisfied in a model whose cardinality is at most $k(e,n)$. Thus, if $P_{(e,n)} \in \Gamma \cup \Gamma_0$, we only need to check that $m \leq k(e,n)$, which can be effectively done since the ternary predicate $k(e,n) < m$ is recursive.

To see that TM_∞ is not $\exists_\infty$-decidable, notice that the constraint $\{P_{(e,n)}\}$ is TM_∞-satisfiable in an infinite structure iff $k(e,n) = \infty$. In turn, this is equivalent to check whether the computation of the Turing Machine e on the input n does not terminate, which is obviously undecidable, being the complement of the Halting problem. □

The theory TM_∞ is defined on an infinite signature. However, it is possible to introduce a universal theory $TM_{\forall\omega}$ over a finite signature, with the same characteristics as TM_∞ as far as decidability in finite and infinite models is concerned. Since the proof that such theory is $\exists$-decidable but not $\exists_\infty$-decidable is similar to that of Proposition 4.1, modulo some technical details, we report it in the full TR version of the present paper. Thus, we are ready to state our first main result:

Theorem 4.1. *There exist $\exists$-decidable universal theories over finite and disjoint signatures, whose union is not $\exists$-decidable.*

5 Decidability

The answer to *QUESTION 2* rests on showing that (under suitable assumptions) rewrite-based methods give practical sufficient conditions for a theory to be

strongly $\exists_\infty$-decidable. First, we need to introduce some technical definitions. In Section 5.1, we recall some basic notions underlying the superposition calculus [15] and we introduce superposition modules as suitable abstractions for the subsequent technical development. Then, in Section 5.2, we introduce the notion of invariant superposition modules and, in Section 5.3, we show that they can generate an "at most" cardinality constraint (cf. (2) in Section 4) whenever a theory does not admit infinite models. Last, in Section 5.4, we describe how to combine rewrite-based procedures [1,2] with Satisfiability Modulo Theory (SMT) tools, such as [9,3,10,11], in order to obtain automatic methods to solve constraint satisfiability problems involving theories admitting only finite models (e.g., enumerated data-types).

5.1 Superposition Calculi and Superposition Modules

From now on, we consider only universal, finitely axiomatized theories, whose signatures are finite. Without loss of generality, we may assume that signatures contain only function symbols (see, e.g., [15]). A fundamental assumption of superposition-based inference systems [15] is that the universe of terms is ordered by a *reduction ordering*. A reduction ordering on terms can be extended to literals and clauses by using standard techniques. The most commonly used orderings are the *Knuth-Bendix ordering (KBO)* and the *lexicographic path ordering (LPO)*. Definitions, results, and references on orderings can be found in, e.g., [4]. Since we have to deal with constraints involving finitely (but arbitrarily) many new constants, we consider a countable set[5] $\mathcal{K}$ disjoint from Σ to form the expanded signature $\Sigma^{\mathcal{K}}$. We collect all needed data in the following:

Definition 5.1 (Suitable Ordering Triple). *A* suitable ordering triple *is a triple* $(\Sigma, \mathcal{K}, \succ)$ *where:* (a) Σ *is a finite signature;* (b) $\mathcal{K} := \{c_1, c_2, c_3, \dots\}$ *is a countably infinite set of constant symbols such that* Σ *and* $\mathcal{K}$ *are disjoint;* (c) $\succ$ *is a reduction ordering over* $\Sigma^{\mathcal{K}}$*-terms satisfying the following conditions:*

(i) $\succ$ *is total on ground* $\Sigma^{\mathcal{K}}$*-terms;*
(ii) *for every ground* $\Sigma^{\mathcal{K}}$*-term* t *with root symbol* $f \in \Sigma$ *and for every* $c_i \in \mathcal{K}$*, we have* $t \succ c_i$*;*
(iii) *for* $c_i, c_j \in \mathcal{K}$*, we have* $c_i \succ c_j$ *iff* $i > j$*.*

The above conditions on the reduction ordering are similar to those adopted in [2,1] to build rewrite-based decision procedures for the constraint satisfiability problem in theories of data structures, fragments of integer arithmetic, and their combinations. It is indeed very easy and natural to produce suitable ordering triples: for instance, if an LPO is adopted, it is sufficient to take a total precedence $>_p$ satisfying the condition $f >_p c_i >_p c_j$, for $f \in \Sigma$, $c_i \in \mathcal{K}$, $c_j \in \mathcal{K}$ and $i > j$.

[5] Usual results on orderings can be extended to infinite signatures, see [13]; notice however that one can keep the signature $\Sigma^{\mathcal{K}}$ finite, by coding c_i as $s^i(0)$ (for new symbols $s, 0$), like e.g. in [8].

Another key characteristic of a rewrite-based inference system is the possibility of associating a model to the set of derived clauses, defined by building incrementally a convergent term rewriting system.

Let $(\Sigma, \mathcal{K}, \succ)$ be a suitable ordering triple and let S be a set of $\Sigma^{\mathcal{K}}$-clauses not containing the empty clause. The set $gr(S)$ contains all ground $\Sigma^{\mathcal{K}}$-clauses that are instances of clauses in S. By transfinite induction on $C \in gr(S)$, we simultaneously define $Gen(C)$ and the ground rewrite system R_C as follows:

(a) $R_C := \bigcup_{D \in gr(S), C \succ D} Gen(D)$;
(b) $Gen(C) := \{l \to r\}$ in case C is of the kind $\Delta_1 \Rightarrow l = r, \Delta_2$ and the following conditions are satisfied:
   1. $R_C \not\models \Delta_1 \Rightarrow \Delta_2$, i.e. (i) for each $l = r \in \Delta_1$, l and r have the same normal form with respect to R_C (in symbols, $l \downarrow_{R_C} r$) and (ii) for each $s = t \in \Delta_2$, $s \not\downarrow_{R_C} t$;
   2. $l \succ r$, $l \succ u$ (for all u occurring in Δ_1), $\{l, r\} \succ^{ms} \{u, v\}$, for every equation $u = v$ occurring in Δ_2, where $\succ^{ms}$ is the multi-set extension [4] of $\succ$;
   3. l is not reducible by R_C, and
   4. $R_C \not\models r = t'$, for every equation of the kind $l = t'$ occurring in Δ_2;
(c) $Gen(C) := \emptyset$, otherwise.

We say that C is *productive* if $Gen(C) \neq \emptyset$. Finally, let $R_S := \bigcup_{C \in gr(S)} Gen(C)$. Note that R_S is a convergent rewrite system, by conditions 2 and 3 above.

A set of clauses is *saturated* with respect to an inference system, if any clause that can be inferred from S is redundant in S (see, e.g., [7]). In a more abstract treatment, that makes saturation independent of the inference system and only requires a well-founded ordering on proofs, a set of formulæ is *saturated* if it contains all the premises of all normal-form proofs in the theory [6]. For the purposes of this paper, we are interested in a semantic notion of saturation based on model generation.

Definition 5.2. *A set S of $\Sigma^{\mathcal{K}}$-clauses is* model-saturated *iff the rewrite system R_S is a model of S (i.e. the quotient of the Herbrand universe of $\Sigma^{\mathcal{K}}$ modulo R_S-convergence is a model of the universal closures of the clauses in S).*

The following definition of reasoning module is precisely what we need to prove the main technical Lemma 5.2 below.

Definition 5.3 (Superposition Module). *Let $(\Sigma, \mathcal{K}, \succ)$ be a suitable ordering triple. A* superposition module $\mathcal{SP}(\Sigma, \mathcal{K}, \succ)$ *is a computable function which takes a finite set S_0 of $\Sigma^{\mathcal{K}}$-clauses as input and returns a (possibly infinite) sequence*

$$S_0, S_1, \ldots, S_n, \ldots \tag{3}$$

of finite sets of $\Sigma^{\mathcal{K}}$-clauses, called an S_0-derivation*, such that (*i*) if S_0 is unsatisfiable, then there exists $k \geq 0$ such that the empty clause is in S_k; (*ii*) if S_0 is satisfiable, then the set*

$$S_\infty := \bigcup_{j \geq 0} \bigcap_{i \geq j} S_i$$

of persistent clauses *is model-saturated, and (*iii*) the sets S_i and S_j are logically equivalent for $(0 \leq i, j \leq \infty)$. We say that $\mathcal{SP}(\Sigma, \mathcal{K}, \succ)$* terminates *on the set of $\Sigma^{\mathcal{K}}$-clauses S_0 iff the S_0-derivation* (3) *is finite.*

Superposition modules are *deterministic*, i.e. there exists just one S_0-derivation starting with a given finite set S_0 of clauses. Any implementation of the superposition calculus [15] together with a fair strategy satisfies Definition 5.3.

5.2 Superposition Modules and Rewrite-based Decision Procedures

For the proofs below, we need a class of superposition modules which are invariant (in a sense to be made precise) under certain renamings of finitely many constants. Formally, an *n-shifting* (where n is an integer such that $n > 0$) is the operation that applied to a $\Sigma^{\mathcal{K}}$-expression E returns the $\Sigma^{\mathcal{K}}$-expression E^{+n} obtained from E by simultaneously replacing each occurrence of the free constant $c_i \in \mathcal{K}$ by the free constant c_{i+n}, for $i > 0$ (where the word 'expression' may denote a term, a literal, a clause, or a set of clauses). In practice, an n-shifting rearranges the set of free constants occurring in the set of clauses by eliminating the constants $c_1, \ldots, c_n$ that are not in the range of the function $(\cdot)^{+n}$.

Example 5.1. Let us consider the set $S := \{f(c_1, c_4) = c_1, f(f(c_1, c_4), c_4) = c_2\}$ of ground $\Sigma^{\mathcal{K}}$-literals where $\Sigma := \{f\}$ and $\mathcal{K} := \{c_1, c_2, \ldots\}$. Then, we have that $S^{+5} := \{f(c_6, c_9) = c_6, f(f(c_6, c_9), c_9) = c_7\}$.

Definition 5.4 (Invariant Superposition Module). *Let $(\Sigma, \mathcal{K}, \succ)$ be a suitable ordering triple. A superposition module $\mathcal{SP}(\Sigma, \mathcal{K}, \succ)$ is* invariant *iff for every S_0-derivation $S_0, S_1, \ldots, S_j, \ldots$ (with S_0 being a set of $\Sigma^{\mathcal{K}}$-clauses), we have that $(S_0)^{+n}, (S_1)^{+n}, \ldots, (S_j)^{+n}, \ldots$ is an $(S_0)^{+n}$-derivation, for all $n \geq 0$.*

Most of the actual implementations of superposition are *stable under signature extensions* (this is so because they need to handle Skolem symbols) and hence, the behavior of a superposition prover is not affected by any proper extension of the signature and the ordering. The property of producing derivations being invariant under shifting is weaker than stability under signature extensions. As a consequence, any superposition prover can be turned into an invariant superposition module. However, not all possible implementations of the superposition calculus are invariant superposition modules, as we point out in the full TR version of the paper.

Example 5.2. Suppose that in the suitable ordering triple $(\Sigma, \mathcal{K}, \succ)$, the term ordering $\succ$ is an LPO whose precedence satisfies $f >_p c_i >_p c_j$ (for $f \in \Sigma, c_i \in \mathcal{K}, c_j \in \mathcal{K}, i > j$). Let us consider the superposition module given by the standard superposition calculus and let us take again the situation in Example 5.1. The (model-)saturated set output by $\mathcal{SP}(\Sigma, \mathcal{K}, \succ)$ when taking S as input is $S_s := \{f(c_1, c_4) = c_1, c_2 = c_1\}$. It is not difficult to see that the set $(S_s)^{+5} := \{f(c_6, c_9) = c_6, c_7 = c_6\}$ is exactly the set that we would obtain as output by the superposition module $\mathcal{SP}(\Sigma, \mathcal{K}, \succ)$ when taking as input the set $(S)^{+5}$ (see Example 5.1).

Definition 5.5. *Let $(\Sigma, \mathcal{K}, \succ)$ be a suitable ordering triple. A universal and finitely axiomatized Σ-theory T is* $\exists$-superposition-decidable *iff there exists an invariant superposition module $\mathcal{SP}(\Sigma, \mathcal{K}, \succ)$ that is guaranteed to terminate when taking as input $T \cup \Gamma$, where Γ is a $\Sigma^{\mathcal{K}}$-constraint.*

From the termination results for superposition given in [2,1], it follows that theories such as equality, (possibly cyclic) lists, arrays, and so on are $\exists$-decidable by superposition. According to Definition 5.5, any theory T which is $\exists$-superposition-decidable is $\exists$-decidable. In the following, we show that T is also $\exists_\infty$-decidable, which is the second main result of the paper.

5.3 Invariant Superposition Modules and Cardinality Constraints

A *variable clause* is a clause containing only equations between variables or their negations. The *antecedent-mgu* (a-mgu, for short) of a variable clause $\Delta_1 \Rightarrow \Delta_2$ is the most general unifier of the unification problem $\{x \stackrel{?}{=} y \mid x = y \in \Delta_1\}$. A *cardinality constraint clause* is a variable clause $\Delta_1 \Rightarrow \Delta_2$ such that $\Rightarrow \Delta_2\mu$ does not contain any trivial equation like $x = x$, where μ is the a-mgu of $\Delta_1 \Rightarrow \Delta_2$; the number of free variables of $\Delta_2\mu$ is called the *cardinal* of the cardinality constraint clause $\Delta_1 \Rightarrow \Delta_2$. For example, the clause $x = y \Rightarrow y = z_1, x = z_2$ is a cardinality constraint clause whose cardinal is 3 (notice that this clause is true only in the one-element model).

Lemma 5.1. *If a satisfiable set S of clauses contains a cardinality constraint clause $\Delta_1 \Rightarrow \Delta_2$, then S cannot have a model whose domain is larger than the cardinal of $\Delta_1 \Rightarrow \Delta_2$.*

Proof. Let μ be the a-mgu of $\Delta_1 \Rightarrow \Delta_2$. By definition of a cardinality constraint clause, the clause $\Rightarrow \Delta_2\mu$ does not contain trivial equations; if n is the number of distinct variables in $\Rightarrow \Delta_2\mu$, then there cannot be more than $n - 1$ distinct elements in any model of S. □

The next crucial lemma expresses the property that an invariant superposition module discovers a cardinality constraint clause whenever the input set of clauses does not admit infinite models.

Lemma 5.2. *Let $(\Sigma, \mathcal{K}, \succ)$ be a suitable ordering triple. Let $\mathcal{SP}(\Sigma, \mathcal{K}, \succ)$ be an invariant superposition module. If S_0 is a satisfiable finite set of clauses, then the following conditions are equivalent:*

(i) *the set S_∞ of persistent clauses in an S_0-derivation of $\mathcal{SP}(\Sigma, \mathcal{K}, \succ)$ contains a cardinality constraint clause;*
(ii) *S_0 does not admit infinite models.*

Proof. The implication (i) ⇒ (ii) is proved by Lemma 5.1. To show (ii) ⇒ (i), assume that the set S_0 does not have a model whose domain is infinite. By Lemma 3.1, there must exist a natural number N such that every model $\mathcal{M}$ of S_0 has a domain with at most N elements. Since a cardinality constraint clause

does not contain constants, it is in S_∞ iff it is in $(S_\infty)^{+N}$. Hence, by Definition 5.4 of an invariant superposition module (considering $(S_0)^{+N}$ rather than S_0, if needed) we are free to assume that the constants $\{c_1, \ldots, c_N\}$ do not occur in S_∞. Recall also that, according to the definition of a suitable ordering triple, the constants $\{c_1, \ldots, c_N\}$ are the smallest ground $\Sigma^{\mathcal{K}}$-terms.

According to the definition of superposition module (cf. Definition 5.3), since S_0 is assumed to be satisfiable, S_∞ is model-saturated, which means that the convergent rewrite system R_{S_∞} is a model of S_∞ (hence also of S_0, which is logically equivalent to S_∞). Now, since S_0 does not have a model whose domain is of cardinality N or greater, there is at least one constant among $c_1, \ldots, c_N$ which is not in normal form (with respect to R_{S_∞}). Assume that c_i is not in normal form (with respect to R_{S_∞}) and that each c_j (for $j < i$) is. By model generation (see section 5.1), to reduce c_i we need a rule $l \to r$ from a productive clause C of the kind $\Delta_1 \Rightarrow l = r, \Delta_2 \in gr(S_\infty)$; furthermore, c_i can be reduced only to c_j for $j < i$. The maximality condition 2 of model generation in Section 5.1 on l implies that l is c_i and that the remaining terms in C are of the kind c_j for $j \leq i$.[6] By condition 1 of model generation in Section 5.1, the fact that all terms c_j ($j < i$) are in R_{S_∞}-normal form, and the fact that R_{S_∞} is a convergent rewrite system extending R_C, it follows that each equation in Δ_1 is of the form $c_j = c_j$. Furthermore, again by condition 1 of model generation in Section 5.1, there is no (trivial) equality of the form $c_j = c_j$ in Δ_2. Since the constants $\{c_1, \ldots, c_N\}$ do not occur in S_∞, we are entitled to conclude that the productive clause $\Delta_1 \Rightarrow l = r, \Delta_2$ is the ground instance of a variable clause, i.e. there must exist a variable clause $\tilde{C}$ of the form $\tilde{\Delta}_1 \Rightarrow \tilde{l} = \tilde{r}, \tilde{\Delta}_2$ in S_∞ such that $\tilde{C}\theta \equiv C$ for some ground substitution θ. Since the antecedent of C consists of trivial equalities, θ is less general than μ, where μ is the a-mgu of $\tilde{C}$, i.e. we have that $\theta = \mu\theta'$ for some substitution θ'. Furthermore, since there are no positive trivial equalities in $C \equiv \tilde{C}\mu\theta'$, there are no positive trivial equalities in $\tilde{C}\mu$ either, which implies that $\tilde{C}$ is a cardinality constraint clause belonging to S_∞. □

The following result immediately follows from Lemma 5.2 above, because unsatisfiability in infinite models can be detected by looking for a cardinality constraint clause among the finitely many final clauses of a terminating derivation:

Theorem 5.1. *Let T be a finitely axiomatized universal Σ-theory where Σ is finite. If T is $\exists$-superposition-decidable, then T is strongly $\exists_\infty$-decidable.*

5.4 Combining Superposition Modules and SMT Procedures

Invariant superposition modules provide us with means to check whether a theory is strongly $\exists_\infty$-decidable (and this answers *QUESTION 2* in Section 3.2). However, the situation is not really clear in practice. By using available state-of-the-art implementations of the superposition calculus, such as SPASS [24] or E

[6] More precisely (this is important for the proof): terms occurring positively can only be c_j for $j \leq i$ and terms occurring negatively can only be c_j for $j < i$.

function *Grounding* (N : *integer*, T: *axioms*, Γ: *Ground literals*)
1 introduce fresh constants $c_1, \ldots, c_N$;
2 for every k-ary function symbol f in $\Gamma \cup T$ (with $k \geq 0$), generate the positive clauses

$$\bigvee_{i=1}^{N} f(a_1, \ldots, a_k) = c_i$$

for every $a_1, \ldots, a_k \in \{c_1, \ldots, c_N\}$ and let E be the resulting set of clauses;
3 for every clause $C \in T$, instantiate C in all possible ways by ground substitutions whose range is the set $\{c_1, \ldots, c_N\}$ and let T_g be the resulting set of clauses;
4 return the set $T_g \cup E \cup \Gamma$.
end

Fig. 1. Computing equisatisfiable sets of ground clauses for instances of the constraint satisfiability problem of theories with no infinite models

[20], with suitable ordering, we have run concrete invariant superposition modules for a theory $T^{\leq k}$, admitting only finite models with at most $k-1$ elements, axiomatized by an appropriate "at most" cardinality constraint, see (2). Indeed, according to Definition 5.4, the hard part is to prove termination for arbitrary input clauses of the form $T^{\leq k} \cup \Gamma$, where Γ is a set of ground literals. Our preliminary experiments were quite discouraging. In fact, both SPASS and E were able to handle only the trivial theory $T^{\leq 1}$ (axiomatized by $\Rightarrow x = y$). Already for $T^{\leq 2}$ (axiomatized by $\Rightarrow x = y, x = z, y = z$), the provers do not terminate in a reasonable amount of time although we experimented with various settings. For example, while SPASS is capable of finding a saturation for $T^{\leq 2} \cup \Gamma$ when $\Gamma := \emptyset$, it seems to diverge when $\Gamma := \{a \neq b\}$. This seems to dramatically reduce the scope of applicability of Theorem 5.1 and hence of Theorem 3.2.

Fortunately, this problem can be solved by the following two observations. First, although a superposition module may not terminate on instances of the constraint satisfiability problem of the form $T \cup \Gamma$, where Γ is a constraint and T does not admit infinite models (such as $T^{\leq k}$, above), Lemma 5.2 ensures that a cardinality constraint clause will eventually be derived in a finite amount of time: if a clause C is in the set S_∞ of persistent clauses of a derivation $S_0, S_1, \ldots$, then there must exists an integer $k \geq 0$ such that $C \in S_k$ (recall Definition 5.3). Second, when a cardinality constraint clause C is derived from $T \cup \Gamma$, a bound on the cardinality of the domains of any model can be immediately obtained by the cardinal associated to C. It is possible to use such a bound to build an equisatisfiable set of clauses (see Figure 1) and pass it to an SMT procedure for the pure theory of equality (e.g., those in [9,3,10,11]) or to a model builder. The observations above motivate the following relaxation of the notion of an $\exists$-superposition-decidable theory.

Definition 5.6. *Let $(\Sigma, \mathcal{K}, \succ)$ be a suitable ordering triple. A universal and finitely axiomatized Σ-theory T is* weakly-$\exists$-superposition-decidable *iff there exists an invariant superposition module $\mathcal{SP}(\Sigma, \mathcal{K}, \succ)$ such that for every $\Sigma^{\mathcal{K}}$-*

constraint Γ, any $T \cup \Gamma$-derivation either (i) *terminates or* (ii) *generates a cardinality constraint clause.*

We can easily adapt Theorem 5.1 to this new definition.

Theorem 5.2. *Let T be a universal and finitely axiomatized Σ-theory, where Σ is finite. If T is weakly-$\exists$-superposition-decidable, then T is strongly $\exists_\infty$-decidable.*

Proof. Decidability of Σ-constraints in T-models can be obtained by halting the invariant superposition module, as soon as a cardinality constraint clause is generated at some stage i, and applying an SMT procedure for the theory of equality or a model builder to the set of clauses produced by applying the function *Grounding* of Figure 1 to S_i. Satisfiability in infinite models is answered negatively if a cardinality constraint clause is generated; otherwise, we have termination of the invariant superposition module and if the empty clause is not produced, satisfiability is reported by Lemma 5.2. □

6 Conclusion and Future Work

By classifying the component theories according to the decidability of constraint satisfiability problems in arbitrary and in infinite models, respectively, we exhibited a theory T_1 such that T_1-satisfiability is decidable, but T_1-satisfiability in infinite models is undecidable. It follows that satisfiability in $T_1 \cup T_2$ is undecidable, whenever T_2 has only infinite models, even if signatures are disjoint and satisfiability in T_2 is decidable. In the second part of the paper we strengthened the Nelson-Oppen combination result, by showing that it applies to theories over disjoint signatures, whose satisfiability problem, in either arbitrary or infinite models, is decidable. We showed that this result covers decision procedures based on superposition, offering an alternative to the results in [1].

An interesting line of future work consists of finding *ad hoc* contraction rules which allow the superposition calculus to terminate on theories that do not admit infinite models such as the $T^{\leq k}$'s considered in Section 5.4.

References

1. A. Armando, M. P. Bonacina, S. Ranise, and S. Schulz. On a rewriting approach to satisfiability procedures: extension, combination of theories and an experimental appraisal. In *Proc. of FroCoS'05*, volume 3717 of *LNCS*, pages 65–80. Springer, 2005. Full version available as DI RR 36/2005, Università degli Studi di Verona, `http://www.sci.univr.it/~bonacina/verify.html`.
2. A. Armando, S. Ranise, and M. Rusinowitch. A rewriting approach to satisfiability procedures. *Information and Computation*, 183(2):140–164, 2003.
3. G. Audemard, P. Bertoli, A. Cimatti, A. Korniłowicz, and R. Sebastiani. A SAT based approach for solving formulas over boolean and linear mathematical propositions. In *Proc. of CADE-18*, volume 2392 of *LNCS*, pages 195–210. Springer, 2002.

4. F. Baader and T. Nipkow. *Term Rewriting and All That*. Cambridge University Press, United Kingdom, 1998.
5. F. Baader and C. Tinelli. Deciding the word problem in the union of equational theories. *Information and Computation*, 178(2):346–390, 2002.
6. M. P. Bonacina and N. Dershowitz. Abstract canonical inference. *ACM Transactions on Computational Logic*, (to appear), 2006.
7. M. P. Bonacina and J. Hsiang. Towards a foundation of completion procedures as semidecision procedures. *Theoretical Computer Science*, 146:199–242, July 1995.
8. H. Comon, P. Narendran, R. Nieuwenhuis, and M. Rusinowitch. Decision problems in ordered rewriting. In *Proc. of LICS'98*, pages 276–286. IEEE Computer Society Press, 1998.
9. D. Déharbe and S. Ranise. Light-weight theorem proving for debugging and verifying units of code. In *Proc. of SEFM'03*. IEEE Computer Society Press, 2003.
10. J.-C. Filliâtre, S. Owre, H. Rueß, and N. Shankar. ICS: Integrated canonizer and solver. In *Proc. of CAV'01*, LNCS, pages 246–249. Springer, 2001.
11. H. Ganzinger, G. Hagen, R. Nieuwenhuis, A. Oliveras, and C. Tinelli. DPLL(T): Fast decision procedures. In *Proc. of CAV'04*, volume 3114 of *LNCS*, pages 175–188. Springer, 2004.
12. S. Ghilardi. Model theoretic methods in combined constraint satisfiability. *Journal of Automated Reasoning*, 33(3-3):221–249, 2005.
13. A. Middeldorp and H. Zantema. Simple termination revisited. In *Proc. of CADE'94*, LNCS, pages 451–465. Springer, 1994.
14. G. Nelson and D. C. Oppen. Simplification by cooperating decision procedures. *ACM Trans. on Programming Languages and Systems*, 1(2):245–257, 1979.
15. R. Nieuwenhuis and A. Rubio. Paramodulation-based theorem proving. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*. Elsevier and MIT Press, 2001.
16. P. Odifreddi. *Classical recursion theory*, volume 125 of *Studies in Logic and the Foundations of Mathematics*. North-Holland, 1989.
17. D. C. Oppen. Complexity, convexity and combinations of theories. *Theoretical Computer Science*, 12:291–302, 1980.
18. D. Pigozzi. The join of equational theories. *Colloquium Mathematicum*, 30(1):15–25, 1974.
19. S. Ranise, C. Ringeissen, and D.-K. Tran. Nelson-Oppen, Shostak and the extended canonizer: A family picture with a newborn. In *Proc. of ICTAC 2004*, LNCS. Springer, 2004.
20. S. Schulz. E - a brainiac theorem prover. *AI Communications*, 15(2/3):111–126, 2002.
21. C. Tinelli and M. T. Harandi. A new correctness proof of the Nelson-Oppen combination procedure. In *Proc. of FroCoS'96*, pages 103–120. Kluwer Academic Publishers, 1996.
22. C. Tinelli and C. G. Zarba. Combining non-stably infinite theories. *Journal of Automated Reasoning*, 2006. (to appear).
23. D. van Dalen. *Logic and Structure*. Springer-Verlag, 1989. Second edition.
24. C. Weidenbach. Combining superposition, sorts and splitting. In A. Robinson and A. Voronkov, editors, *Handbook of Automated Reasoning*. Elsevier and MIT Press, 2001.