Combining Non-Stably Infinite Theories

Cesare Tinelli [1]

Department of Computer Science
University of Iowa
Iowa City, IA 52242

Calogero G. Zarba [2]

Computer Science Department
Stanford University
Stanford, CA 94305, USA

Abstract

The Nelson-Oppen combination method combines decision procedures for first-order theories over disjoint signatures into a single decision procedure for the union theory. To be correct, the method requires that the component theories be stably infinite. This restriction makes the method inapplicable to many interesting theories such as, for instance, theories having only finite models.

In this paper we provide a new combination method that can combine any theory that is not stably infinite with another theory, provided that the latter is what we call a *shiny* theory. Examples of shiny theories include the theory of equality, the theory of partial orders, and the theory of total orders.

An interesting consequence of our results is that any decision procedure for the satisfiability of quantifier-free Σ-formulae in a Σ-theory T can always be extended to accept inputs over an arbitrary signature $\Omega \supseteq \Sigma$.

1 Introduction

An important research problem in automated reasoning asks how we can modularly combine decision procedures for theories T_1 and T_2 into a decision procedure for a combination of T_1 and T_2.

The most successful and well-known method for combining decision procedures was invented in 1979 by Nelson and Oppen [8]. This method is at

[1] Email: tinelli@cs.uiowa.edu.

[2] Email: zarba@theory.stanford.edu.

This is a preliminary version. The final version will be published in
Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

the heart of the verification systems CVC [12], ESC [3], EVES [2], and SDVS [6], among others.

The Nelson-Oppen method allows us to decide the satisfiability of quantifier-free formulae in a combination T of a theory T_1 and a theory T_2, by using as black boxes the decision procedures for the satisfiability of quantifier-free formulae in T_1 and in T_2. To be correct, the Nelson-Oppen method requires that the theories T, T_1, and T_2 satisfy the following restrictions:

- T is logically equivalent to $T_1 \cup T_2$;
- the signatures of T_1 and T_2 are disjoint;
- T_1 and T_2 are both stably infinite. [3]

There are several interesting combination problems that do not satisfy all these restrictions.

In this paper we concentrate on the issue of relaxing the stable infiniteness restriction. This is an important research problem at the theoretical level because it allows us to better understand the foundations of combination problems, and to prove more decidability results by combination techniques. But it is also interesting at a practical level because (i) proving that a given theory is stably infinite is not always easy, and (ii) many interesting theories, such as those admitting only finite models, are not stably infinite.

We show that when one component theory satisfies a stronger property than stable infiniteness, which we call *shininess*, [4] then the other component theory does not need to be stably infinite for their decision procedures to be combinable. We do that by providing and proving correct an extension of the Nelson-Oppen method that, in addition to propagating equality constraints between the component decision procedures, also propagates certain cardinality constraints.

Examples of shiny theories include the theory of equality, the theory of partial orders, and the theory of total orders. In particular, the fact that the theory of equality is shiny leads to a notable side result:

> **Result 1.** *If the satisfiability in a Σ-theory T of quantifier-free Σ-formulae is decidable, then the satisfiability in T of quantifier-free formulae over any arbitrary signature $\Omega \supseteq \Sigma$ is also decidable.*

Result 1 was proven by Policriti and Schwartz [11] for theories T that are universal. It was also known for theories T that are stably infinite, since in this case one can use the Nelson-Oppen method to combine the decision procedure for T with one for the theory of equality over the symbols in $\Omega \setminus \Sigma$. In this paper we prove that Result 1 holds regardless of whether T is universal or not, and regardless of whether T is stably infinite or not.

[3] See Definition 2.2.

[4] See Definition 2.5.

1.1 Related work.

Several researchers have worked on relaxing the requirements of the Nelson-Oppen combination method. The disjointness problem was addressed by Ghilardi [4], Tinelli [13], Tinelli and Ringeissen [15] and Zarba [20]. The stably infiniteness requirement was addressed by Baader and Tinelli [1] for combinations problems concerning the word problem, and by Zarba [17,18,19] for combinations of integers with lists, sets, and multisets. (The latter works by Zarba consider combination problems other than simple set-theoretic union.)

1.2 Organization of the paper

The paper is organized as follows. In Section 2 we introduce some preliminary notions, including the notion of a shiny theory. In Section 3 we describe our combination method. In Section 4 we provide two examples showing our method in action. In Section 5 we prove that our method is correct. In Section 6 we prove that the theory of equality is shiny. We conclude in Section 7 with directions for further research.

In order to focus on the main results, we omit here the proofs that the theories of partial and total orders are shiny. They can be found in the long version of this paper [16].

2 Preliminaries

A *signature* Σ is composed by a set Σ^{C} of constants, a set Σ^{F} of function symbols, and a set Σ^{P} of predicate symbols. We use the standard notions of (Σ-)term, atom, literal, formula, and sentence. We use $\approx$ to denote the equality logical symbol. We abbreviate with $s \not\approx t$ the negation of a literal $s \approx t$, and we identify a conjunction of formulae $\varphi_1 \wedge \cdots \wedge \varphi_n$ with the set $\{\varphi_1, \ldots, \varphi_n\}$.

If φ is a term or a formula, $\mathit{vars}(\varphi)$ denotes the set of variables occurring in φ. Similarly, if Φ is a set of terms or a set of formulae, $\mathit{vars}(\Phi)$ denotes the set of variables occurring in Φ.

For a signature Σ, a Σ-*interpretation* $\mathcal{A}$ with domain A over a set V of variables is a map which interprets each variable x as an element $x^{\mathcal{A}} \in A$, each constant $c \in \Sigma^{\mathrm{C}}$ as an element $c^{\mathcal{A}} \in A$, each function symbol $f \in \Sigma^{\mathrm{F}}$ of arity n as a function $f^{\mathcal{A}} : A^n \to A$, and each predicate symbol $P \in \Sigma^{\mathrm{P}}$ of arity n as a subset $P^{\mathcal{A}}$ of A^n. We adopt the convention that calligraphic letters $\mathcal{A}$, $\mathcal{B}$, ... denote interpretations, while the corresponding Roman letters A, B, ... denote the domains of the interpretations.

Let $\mathcal{A}$ be a Σ-interpretation over a set V of variables. For a Σ-term t over V, we denote with $t^{\mathcal{A}}$ the evaluation of t under the interpretation $\mathcal{A}$. Likewise, for a Σ-formula φ over V, we denote with $\varphi^{\mathcal{A}}$ the truth-value of φ under the interpretation $\mathcal{A}$. If T is a set of Σ-terms over V, we denote with $T^{\mathcal{A}}$ the set $\{t^{\mathcal{A}} \mid t \in T\}$.

A formula φ is *satisfiable*, if it is true under some interpretation, and *unsatisfiable* otherwise.

We use the standard model-theoretic notions of *embedding* and of *isomorphism* between interpretations [5].

Definition 2.1 Let Σ be a signature, and let $\mathcal{A}$ and $\mathcal{B}$ be Σ-interpretations over some set V of variables. A map $h : A \to B$ is an EMBEDDING of $\mathcal{A}$ into $\mathcal{B}$ if the following conditions hold:

- h is injective;
- $h(u^{\mathcal{A}}) = u^{\mathcal{B}}$ for each variable or constant $u \in V \cup \Sigma^{\mathrm{C}}$;
- $h(f^{\mathcal{A}}(a_1, \ldots, a_n)) = f^{\mathcal{B}}(h(a_1), \ldots, h(a_n))$, for each n-ary function symbol $f \in \Sigma^{\mathrm{F}}$ and $a_1, \ldots, a_n \in A$;
- $(a_1, \ldots, a_n) \in P^{\mathcal{A}}$ if and only if $(h(a_1), \ldots h(a_n)) \in P^{\mathcal{B}}$, for each n-ary predicate symbol $P \in \Sigma^{\mathrm{P}}$ and $a_1, \ldots, a_n \in A$.

An ISOMORPHISM of $\mathcal{A}$ into $\mathcal{B}$ is a surjective (and therefore bijective) embedding of $\mathcal{A}$ into $\mathcal{B}$.

A Σ-*theory* is any set of Σ-sentences. Given a Σ-theory T, a T-*model* is a Σ-interpretation that satisfies all sentences in T. A formula φ is T-*satisfiable* if it is satisfied by some T-model, and it is T-*unsatisfiable* otherwise. Given a set L of formulae, the *satisfiability problem* of T with respect to L is the problem of deciding, for each formula φ in L, whether or not φ is T-satisfiable. When we do not specify L, it is implicitly assumed that L is the set of all Σ-formulae. However, when we say "quantifier-free satisfiability problem", without specifying L, then we implicitly assume that L is the set of all quantifier-free Σ-formulae.

We use the usual notion of stable infiniteness for a theory, together with its "dual" one, which we call stable finiteness.

Definition 2.2 A Σ-theory T is STABLY INFINITE (respectively, STABLY FINITE) if every quantifier-free Σ-formula φ is T-satisfiable if and only if it is satisfied by a T-interpretation $\mathcal{A}$ whose domain A is infinite (respectively, finite).

Examples of stably infinite theories include the theory of equality, [5] the theory of integer arithmetic, the theory of rational arithmetic, the theory of lists, and the theory of arrays. Examples of stably finite theories include the theory of equality, all theories satisfied only by finite interpretations, and all theories finitely axiomatized by formulae in the Bernays-Schönfinkel-Ramsey class.

Note that a theory can be both stably finite and stably infinite. We will show that in Section 6 for the theory of equality.

[5] Since we regard $\approx$ as a logical symbol, for us the theory of equality and the empty theory are the same theory.

Definition 2.3 A Σ-theory T is smooth if for every quantifier-free Σ-formula φ, for every T-model $\mathcal{A}$ satisfying φ, and for every cardinal number $\kappa > |A|$ there exists a T-model $\mathcal{B}$ satisfying φ such that $|B| = \kappa$.

A direct consequence of Definition 2.3 is that every smooth theory is stably infinite. The following proposition is useful when proving that a theory is smooth.

Proposition 2.4 *A Σ-theory T is smooth if and only if for every quantifier-free Σ-formula φ and every finite T-model $\mathcal{A}$ of φ, there exists a T-model $\mathcal{B}$ of φ such that $|B| = |A| + 1$.*

Given a theory T and a T-satisfiable quantifier-free formula φ, we denote with $\mathit{mincard}_T(\varphi)$ the smallest cardinality of a T-model satisfying φ. Note that if T is a stably finite theory then, for every T-satisfiable formula φ, $\mathit{mincard}_T(\varphi)$ is a natural number.

Definition 2.5 A Σ-theory T is shiny if it is both smooth and stably finite, and such that $\mathit{mincard}_T$ is computable.

3 The combination method

Let S be a shiny Σ-theory and let T be an Ω-theory such that $\Sigma \cap \Omega = \emptyset$ and the quantifier-free satisfiability problems of S and of T are decidable. We now describe a method for combining decision procedures for the quantifier-free satisfiability problems of S and T into a single decision procedure for the quantifier-free satisfiability problem of $S \cup T$.

Since every quantifier free formula is logically equivalent to its disjunctive normal form, without loss of generality we restrict ourselves to conjunctions of literals. In addition, we consider only conjunctions of the form $\Gamma_1 \cup \Gamma_2$, which we call a *separate form*, where Γ_1 contains only Σ-literals and Γ_2 contains only Ω-literals. The latter restriction is also without loss of generality, as every conjunction Γ of $(\Sigma \cup \Omega)$-literals can be effectively converted into an equisatisfiable separate form $\Gamma_1 \cup \Gamma_2$ with the help of new auxiliary variables.

Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form. The combination method consists of two phases, described below.

Decomposition phase. Nondeterministically guess an equivalence relation E over the set $V = \mathit{vars}(\Gamma_1) \cap \mathit{vars}(\Gamma_2)$ of variables shared by Γ_1 and Γ_2.

Check phase. Where E is the guessed equivalence relation over V, perform the following steps:

1. Construct the *arrangement* of V induced by E, defined by

$$\begin{aligned} \mathit{arr}(V,E) = {} & \{x \approx y \mid x, y \in V, x \text{ and } y \text{ are distinct, and } (x,y) \in E\} \cup \\ & \{x \not\approx y \mid x, y \in V \text{ and } (x,y) \notin E\}\,. \end{aligned}$$

2. If $\Gamma_1 \cup \mathit{arr}(V, E)$ is S-satisfiable go to the next step; otherwise output `fail`.
3. Compute $n = \mathit{mincard}_S(\Gamma_1 \cup \mathit{arr}(V, E))$.
4. Construct a set δ_n of literals whose purpose is to force models with cardinality at least n. More precisely, let $\delta_n = \{w_i \not\approx w_j \mid 1 \leq i < j \leq n\}$, where $w_1, \ldots, w_n$ are new variables not occurring in $\Gamma_1 \cup \Gamma_2$.
5. If $\Gamma_2 \cup \mathit{arr}(V, E) \cup \delta_n$ is T-satisfiable output `succeed`; otherwise output `fail`.

In Section 5 we will prove that (i) if the check phase outputs `succeed` for some equivalence relation E over V, then Γ is $(S \cup T)$-satisfiable, and (ii) if the check phase outputs `fails` for each equivalence relation E over V, then Γ is $(S \cup T)$-unsatisfiable.

Our combination method differs from the Nelson-Oppen method as follows. In the check phase, the Nelson-Oppen method omits steps 3 and 4, and in step 5 it checks the T-satisfiability of $\Gamma_2 \cup \mathit{arr}(V, E)$ only. Note that this is enough in the Nelson-Oppen method because there T is assumed to be stably infinite, and therefore the constraint δ_n is guaranteed to hold.

Note that our method applies just as well in case T is stably-infinite. [6] However, if one knows that T is stably infinite, resorting to the original Nelson-Oppen method is more appropriate, as it lets one avoid the cost of computing $\mathit{mincard}_S$.

4 Examples

In this section we discuss two examples of theories that are not combinable with the Nelson-Oppen method but are combinable with ours. In both examples we combine the theory S of equality over a signature Σ with a non-stably infinite theory T over a signature Ω disjoint from Σ. In the first case, T is not stably infinite because it only admits finite models. In the second case, T is not stably infinite even if it has infinite models. The examples are adapted from [14] and [1], respectively, where they are used to show that the Nelson-Oppen method is in fact incorrect on non-stably infinite theories.

Example 4.1 Let $\Sigma = \{f\}$ and $\Omega = \{g\}$ be signatures, where f and g are distinct unary function symbols. Let S be the theory of equality over the signature Σ, and let T be an Ω-theory such that all T-interpretations have cardinality at most two. Since T is not stably infinite, we cannot use the Nelson-Oppen combination method. But since S is shiny, we can use our method.

Let $\Gamma = \Gamma_1 \cup \Gamma_2$, where

$$\Gamma_1 = \{f(x) \not\approx f(y)\,,\ f(x) \not\approx f(z)\} \quad \text{and} \quad \Gamma_2 = \{g(y) \not\approx g(z)\}\,.$$

[6] Recall that S is already stably infinite, since it is shiny.

Note that Γ is $(S \cup T)$-unsatisfiable. In fact, Γ implies $x \not\approx y \wedge x \not\approx z \wedge y \not\approx z$, and therefore every interpretation satisfying Γ must have cardinality at least three. Since every $(S \cup T)$-interpretation has at most two elements, it follows that Γ is $(S \cup T)$-unsatisfiable.

Let us apply our combination method to Γ. Since $\mathit{vars}(\Gamma_1) \cap \mathit{vars}(\Gamma_2) = \{y, z\}$, there are only two equivalence relations available for guessing: either $(y, z) \in E$ or $(y, z) \notin E$.

If $(y, z) \in E$ we have that $\Gamma_1 \cup \{y \approx z\}$ is S-satisfiable and that $\Gamma_2 \cup \{y \approx z\}$ is T-unsatisfiable. Thus, we will output `fail` when reaching step 4 of the check phase.

If instead $(y, z) \notin E$ then $\Gamma_1 \cup \{y \not\approx z\}$ is S-satisfiable. In addition, we have $\mathit{mincard}_S(\Gamma_1 \cup \{y \not\approx z\}) = 3$. To see this, first observe that $\Gamma_1 \cup \{y \not\approx z\}$ implies $x \not\approx y \wedge x \not\approx z \wedge y \not\approx z$, and therefore $\mathit{mincard}_S(\Gamma_1 \cup \{y \not\approx z\}) \geq 3$. In addition, we can construct an interpretation $\mathcal{A}$ of cardinality 3 satisfying $\Gamma_1 \cup \{y \not\approx z\}$ by letting $A = \{a_1, a_2, a_3\}$, $x^{\mathcal{A}} = a_1$, $y^{\mathcal{A}} = a_2$, $z^{\mathcal{A}} = a_3$, and $f^{\mathcal{A}}(a) = a$, for each $a \in A$.[7] In the third step of the check phase we introduce three new variables w_1, w_2, w_3, and construct δ_3 as the set $\{w_1 \not\approx w_2, w_1 \not\approx w_3, w_2 \not\approx w_3\}$. Since $\Gamma_2 \cup \{y \not\approx z\} \cup \delta_3$ is T-unsatisfiable, in the fourth step we output `fail`. We can therefore declare that Γ is $(S \cup T)$-unsatisfiable.

Example 4.2 Let $\Sigma = \{k\}$ and $\Omega = \{f, g, h\}$ be signatures, where k, f and g are distinct unary function symbols. Let S be again the theory of equality over the signature Σ, and let T be the following equational theory:

$$T = \left\{ \begin{array}{l} (\forall x)(\forall y)(x \approx f(g(x), g(y))), \\ (\forall x)(\forall y)(f(g(x), h(y)) \approx y) \end{array} \right\} .$$

Using simple term rewriting arguments, it is possible to show that T admits models of cardinality greater than one, and so admits models of infinite cardinality.[8] However, T is not stably infinite.

In fact, consider the set quantifier-free formula $g(z) \approx h(z)$. This formula is T-satisfiable because both the formula and T admit a trivial model, that is, a model with just one element. Now let $\mathcal{A}$ be any T-model of $g(z) \approx h(z)$, let $a_0 = z^{\mathcal{A}}$, and let $a \in A$. Because of T's axioms, we have that

$$a = f^{\mathcal{A}}(g^{\mathcal{A}}(a), g^{\mathcal{A}}(a_0)) = f^{\mathcal{A}}(g^{\mathcal{A}}(a), h^{\mathcal{A}}(a_0)) = a_0 .$$

Given that a is arbitrary, this entails that $|A| = 1$. Thus, $g(z) \approx h(z)$ is only satisfiable in trivial models of T, and therefore the theory T is not stably infinite.

For an application of our combination method to S and T, let $\Gamma = \Gamma_1 \cup \Gamma_2$,

[7] We will see how to effectively compute $\mathit{mincard}_S$ in Section 6.

[8] This is because the set of models of an equational theory is closed under direct products.

where

$$\Gamma_1 = \{g(z) \approx h(z)\} \quad \text{and} \quad \Gamma_2 = \{k(z) \not\approx z\}\,.$$

The conjunction Γ is $(S \cup T)$-unsatisfiable, because $g(z) \approx h(z)$ is satisfiable only in trivial models of $S \cup T$ (for being satisfiable only in trivial models of T, as seen above), while $k(z) \not\approx z$ is clearly satisfiable only in non-trivial models of $S \cup T$.

Let us apply our combination method to Γ. Since $\mathit{vars}(\Gamma_1) \cap \mathit{vars}(\Gamma_2) = \{z\}$, in the check phase there are no equivalence relations to examine, therefore we generate the empty arrangement. Clearly, Γ_1 is S-satisfiable, and in models of cardinality at least 2. Therefore, we have that $\mathit{mincard}_S(\Gamma_1) = 2$.

In the third step of the check phase, we then compute δ_2 as the set $\{w_1 \not\approx w_2\}$ for some fresh variables w_1, w_2. For what we argued above, $\Gamma_2 \cup \delta_2$ is T-unsatisfiable, so in the fourth step we output `fail`, as needed.

5 Correctness

In this section we prove that our combination method is correct.

Clearly, our combination method is terminating. This follows from the fact that, since there is only a finite number of equivalence relations over a finite set V of variables, the nondeterministic decomposition phase is finitary. Thus, we only need to prove that our method is also partially correct.

We will use the following theorem which is a special case of a more general combination result given in [15] for theories with possibly non-disjoint signatures. A direct proof of this theorem can be found in [7].

Theorem 5.1 (Combination Theorem for Disjoint Signatures) *Let Φ_i be a set of Σ_i-formulae, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \emptyset$.*

Then $\Phi_1 \cup \Phi_2$ is satisfiable if and only if there exists an interpretation $\mathcal{A}$ satisfying Φ_1 and an interpretation $\mathcal{B}$ satisfying Φ_2 such that:

(i) $|A| = |B|$,

(ii) $x^{\mathcal{A}} = y^{\mathcal{A}}$ if and only if $x^{\mathcal{B}} = y^{\mathcal{B}}$, for every $x, y \in \mathit{vars}(\Phi_1) \cap \mathit{vars}(\Phi_2)$.

The following proposition proves that our method is partially correct.

Proposition 5.2 *Let S be a shiny Σ-theory and let T be an Ω-theory such that $\Sigma \cap \Omega = \emptyset$. Let Γ_1 be a conjunction of Σ-literals and Γ_2 a conjunction of Ω-literals. Where $V = \mathit{vars}(\Gamma_1) \cap \mathit{vars}(\Gamma_2)$, the following are equivalent:*

(i) *$\Gamma_1 \cup \Gamma_2$ is $(S \cup T)$-satisfiable.*

(ii) *There exists an equivalence relation E over V such that $\Gamma_1 \cup \mathit{arr}(V, E)$ is S-satisfiable and $\Gamma_2 \cup \mathit{arr}(V, E) \cup \delta_n$ is T-satisfiable, with $n = \mathit{mincard}_S(\Gamma_1 \cup \mathit{arr}(V, E))$.*

Proof. $(1 \Rightarrow 2)$. Assume that $\Gamma_1 \cup \Gamma_2$ is $(S \cup T)$-satisfiable, and let $\mathcal{F}$ be one of its $(S \cup T)$-models. Let $E = \{(x, y) \mid x, y \in V \text{ and } x^{\mathcal{F}} = y^{\mathcal{F}}\}$.

Clearly, $\mathcal{F}$ is an $(S \cup T)$-model of $\Gamma_1 \cup \Gamma_2 \cup \mathit{arr}(E, V)$. It follows that $\mathcal{F}$ is also an S-model of $\Gamma_1 \cup \mathit{arr}(E, V)$. In addition, $\mathcal{F}$ is a T-model of $\Gamma_2 \cup \mathit{arr}(E, V)$. Let $\kappa = |F|$, and let $n = \mathit{mincard}_S(\Gamma_1 \cup \mathit{arr}(V, E))$. By definition of $\mathit{mincard}_S$, we have $n \leq \kappa$, which implies that $\mathcal{F}$ is also a T-model of $\Gamma_2 \cup \mathit{arr}(E, V) \cup \delta_n$.

$(2 \Rightarrow 1)$. Let $V_1 = \mathit{vars}(\Gamma_1)$ and $V_2 = \mathit{vars}(\Gamma_2 \cup \delta_n)$, and observe that $V_1 \cap V_2 = V$. Assume there is an equivalence relation E of V such that $\Gamma_1 \cup \mathit{arr}(V, E)$ is S-satisfiable and $\Gamma_2 \cup \mathit{arr}(V, E) \cup \delta_n$ is T-satisfiable, where $n = \mathit{mincard}_S(\Gamma_1 \cup \mathit{arr}(V, E))$. Then there exist an S-model $\mathcal{A}$ of $\Gamma_1 \cup \mathit{arr}(V, E)$ and a T-model $\mathcal{B}$ of $\Gamma_2 \cup \mathit{arr}(V, E) \cup \delta_n$.

Since $\mathcal{B}$ satisfies δ_n, we have $|B| \geq n$. Thus, by the smoothness of S, we can assume without loss of generality that $|A| = |B|$. In addition, because both $\mathcal{A}$ and $\mathcal{B}$ satisfy $\mathit{arr}(V, E)$, we have that $x^{\mathcal{A}} = y^{\mathcal{A}}$ if and only if $x^{\mathcal{B}} = y^{\mathcal{B}}$, for all $x, y \in V$. By Theorem 5.1, $S \cup T \cup \Gamma_1 \cup \Gamma_2 \cup \mathit{arr}(V, E) \cup \delta_n$ is satisfiable. Thus, $\Gamma_1 \cup \Gamma_2$ is $(S \cup T)$-satisfiable. □

Combining Proposition 5.2 with the fact that our combination method is terminating, we obtain the following decidability result.

Theorem 5.3 *Let S be a shiny Σ-theory and let be T an Ω-theory such that $\Sigma \cap \Omega = \emptyset$. If the quantifier-free satisfiability problems of S and of T are decidable, then the quantifier-free satisfiability problem of $S \cup T$ is also decidable.*

6 The theory of equality

It is known that the theory of equality (over an arbitrary signature) is stably infinite and has a decidable quantifier-free satisfiability problem [10]. We show here that it is also shiny.

We will use the following basic lemma of model theory [5].

Lemma 6.1 *Let $\mathcal{A}, \mathcal{B}$ be two interpretations such that there is an embedding of $\mathcal{A}$ into $\mathcal{B}$, and let φ be a quantifier-free formula. Then φ is satisfied by $\mathcal{A}$ if and only if it is satisfied by $\mathcal{B}$.*

Proposition 6.2 *Let φ be a quantifier-free formula, and let $\mathcal{A}$ be a finite model of φ. Then there exists a model $\mathcal{B}$ of φ such that $|B| = |A| + 1$.*

Proof. Let $k = |A|$. We construct a Σ-model $\mathcal{B}$ of φ such that $|B| = k + 1$ as follows. Let $B = A \cup \{b\}$, where $b \notin A$. Then, fix an arbitrary element $a_0 \in B$, and let

- for variables and constants: $u^{\mathcal{B}} = u^{\mathcal{A}}$,
- for function symbols of arity n:

$$f^{\mathcal{B}}(a_1, \dots, a_n) = \begin{cases} f^{\mathcal{A}}(a_1, \dots, a_n)\,, & \text{if } a_1, \dots, a_n \in A\,, \\ a_0\,, & \text{otherwise,} \end{cases}$$

```
Input: An $S$-satisfiable conjunction $\Gamma$ of $\Sigma$-literals
Output: $mincard_S(\Gamma)$
 1: if $\Gamma$ is empty then
 2:    return 1
 3: else
 4:    $U \leftarrow$ TERMS($\Gamma$)
 5:    $\Gamma' \leftarrow \Gamma$
 6:    for $s, t \in U$ do
 7:       if $\Gamma' \cup \{s \approx t\}$ is $S$-satisfiable then
 8:          $\Gamma' \leftarrow \Gamma' \cup \{s \approx t\}$
 9:       end if
10:    end for
11:    $E \leftarrow \{(s, t) \mid s \approx t \in \Gamma'\}$
12:    $C \leftarrow$ CONG-CLOSURE($E$)
13:    return CARD($U/_C$)
14: end if
```

Fig. 1: A procedure for *mincard*$_S$.

- for predicate symbols of arity n:

$$(a_1, \ldots, a_n) \in P^{\mathcal{B}} \iff a_1, \ldots, a_n \in A \text{ and } (a_1, \ldots, a_n) \in P^{\mathcal{A}} .$$

We have $|B| = k+1$. In addition, the map $h : A \to B$ defined by $h(a) = a$, for each $a \in A$, is an embedding of $\mathcal{A}$ into $\mathcal{B}$. Since $\mathcal{A}$ satisfies φ, by Lemma 6.1 it follows that $\mathcal{B}$ also satisfies φ. □

Combining Propositions 2.4 and 6.2, we obtain the smoothness of the theory of equality.

Proposition 6.3 *For every signature Σ, the Σ-theory of equality is smooth.*

Next, we show that $mincard_S(\varphi)$ is computable when S is the theory of equality. A procedure that computes $mincard_S$ is given in Figure 1.

In the procedure, the function TERMS returns the set of all terms and subterms occurring in its input Γ. For instance, if $\Gamma = \{f(g(x)) \approx g(f(y))\}$ then TERMS(Γ) returns the set $\{x, g(x), f(g(x)), y, f(y), g(f(y))\}$. The function CONG-CLOSURE computes the congruence closure of the binary relation E over the signature of Γ.[9] $U/_C$ denotes the quotient of U with respect to the congruence relation C.

Both C and $U/_C$ can be computed using any standard congruence closure algorithm [9]. The complexity of such algorithms is (no more than) $\mathcal{O}(n^2)$, where n is the cardinality of U. The test in line 7 can be performed by the same congruence closure algorithm used for computing C. Since the procedure in Figure 1 is clearly terminating, it then follows that its complexity is $\mathcal{O}(n^4)$.

We show below that the procedure is also partially correct.

[9] Given a binary relation E, the congruence closure of E is the smallest congruence C containing E.

Proposition 6.4 *For every input* Γ*, the procedure shown in Figure 1 returns* $\mathit{mincard}_S(\Gamma)$*.*

Proof. If Γ is empty then Γ is satisfied by every interpretation. Thus, in this case the procedure returns the correct value $\mathit{mincard}_S(\Gamma) = 1$.

Let us consider the case in which Γ is not empty. Let U, Γ', E, and C be as computed by the procedure. Moreover, let k be the value returned in line 13. Note that Γ' is S-satisfiable, and that $\Gamma \subseteq \Gamma'$. Thus, every model of Γ' is also a model of Γ. Finally, since Γ is not empty, then U is also not empty. It follows that the quotient $U/_C$ is not empty, hence $k \geq 1$.

Let $\mathcal{A}$ be any model of Γ', and consider the set $B = \{t^{\mathcal{A}} \mid t \in U\}$.

We claim that $|B| = k$. To see this, suppose, for a contradiction, that $|B| \neq k$. Assume first that $|B| < k$. Since k is equal to the number of equivalence classes of C, there exist two terms $s, t \in U$ such that $(s,t) \notin C$ and $s^{\mathcal{A}} = t^{\mathcal{A}}$. But then $\Gamma' \cup \{s \approx t\}$ is satisfied by $\mathcal{A}$, which implies that $s \approx t \in \Gamma'$. It follows that $(s,t) \in E$, and therefore $(s,t) \in C$, a contradiction.

Next, suppose that $|B| > k$. Then there exist distinct terms $t_1, \ldots, t_n$, with $n > k$, such that $t_i^{\mathcal{A}} \neq t_j^{\mathcal{A}}$, for $i < j$. Since C is the congruence closure of E, it follows that, for every term s, t, if $(s,t) \in C$ then $s^{\mathcal{A}} = t^{\mathcal{A}}$. But then, for every term s, t, if $s^{\mathcal{A}} \neq t^{\mathcal{A}}$ then $(s,t) \notin C$. Thus, $(t_i, t_j) \notin C$, for $i < j$. It follows that C has more than k equivalence classes, a contradiction.

Since $|B| = k$, by the generality of $\mathcal{A}$, we can conclude that every model of Γ has at least k elements.

We now construct a model $\mathcal{B}$ of Γ with domain B. The proposition's claim will then follow from the fact that $|B| = k$.

Let b be some element of B. We define

- for variables and constants:

$$u^{\mathcal{B}} = \begin{cases} u^{\mathcal{A}}\,, & \text{if } u^{\mathcal{A}} \in B\,, \\ b\,, & \text{otherwise}\,, \end{cases}$$

- for function symbols of arity n:

$$f^{\mathcal{B}}(b_1, \ldots, b_n) = \begin{cases} f^{\mathcal{A}}(b_1, \ldots, b_n)\,, & \text{if } f^{\mathcal{A}}(b_1, \ldots, b_n) \in B\,, \\ b\,, & \text{otherwise,} \end{cases}$$

- for predicate symbols of arity n:

$$(b_1, \ldots, b_n) \in P^{\mathcal{B}} \quad \Longleftrightarrow \quad (b_1, \ldots, b_n) \in P^{\mathcal{A}}\,.$$

By structural induction, one can show that $t^{\mathcal{B}} = t^{\mathcal{A}}$ for all terms $t \in U$, and that $\ell^{\mathcal{B}} = \ell^{\mathcal{A}}$ for all literals $\ell \in \Gamma'$. It follows that $\mathcal{B}$ satisfies Γ'. Since $\Gamma \subseteq \Gamma'$, $\mathcal{B}$ also satisfies Γ. □

As an immediate corollary of Proposition 6.4, we obtain the following result.

Proposition 6.5 *For every signature Σ, the Σ-theory of equality is stably finite.*

Putting together Propositions 2.4, 6.4, and 6.5, we obtain the shininess of the theory of equality.

Proposition 6.6 *For every signature Σ, the Σ-theory of equality is shiny.*

Proposition 6.6 is relevant because, together with our combination method in Section 3, it tells us that any procedure that decides the quantifier-free satisfiability problem for a Σ-theory T can be extended to accept inputs Γ containing arbitrary free symbols in addition to the symbols in Σ.

This fact was already known for theories T that are universal [11]. It was also known for theories T that are stably-infinite, since in this case one can use the Nelson-Oppen method to combine the decision procedure for T with one for the theory of equality over the symbols of Γ that are not in Σ. Thanks to Proposition 6.6 and our combination method, we are able to lift the universal and/or stable-infiniteness requirement for T altogether.

More formally, we have the following theorem.

Theorem 6.7 *Let T be a Σ-theory such that the quantifier-free satisfiability problem of T is decidable. Then, for every signature $\Omega \supseteq \Sigma$, the quantifier-free satisfiability problem of T with respect to Ω-formulae is decidable.*

7 Conclusion

We have addressed the problem of extending the Nelson-Oppen combination method to pairs of theories that are not stably infinite. We provided a modification of the Nelson-Oppen method in which it is possible to lift the stable infiniteness requirement from one theory, provided that the other one satisfies a stronger condition, which we called shininess.

Examples of shiny theories include the theory of equality, the theory of partial orders, and the theory of total orders.

In particular, the shininess of the theory of equality yields an interesting useful result: Any decision procedure for the quantifier-free satisfiability problem of a theory T can be extended to accept input formulae over an arbitrary signature. The usefulness of this result stems from the fact that, in practice, satisfiability problems in a theory T often contain free function symbols in addition to the original symbols of T. These function symbols are typically introduced by skolemization or abstraction processes. Our result says that these symbols can be always dealt with properly, no matter what T is.

The Nelson-Oppen method is applicable to an arbitrary number of stably infinite and pairwise signature-disjoint theories. Similarly, our method can be extended to the combination of one arbitrary theory and $n > 1$ shiny theories, all pairwise signature-disjoint. In is unlikely that our method can be extended to allow more than one arbitrary theory. In fact, if this were the case, we would be able to combine two arbitrary theories.

The correctness proof of both the Nelson-Oppen method and our method relies on the Combination Theorem for Disjoint Theories (Theorem 5.1). That theorem requires that the two parts of a separate form of an input formula be satisfied in models of the respective theories having the same cardinality. This requirement is impossible to check in general [15]. Considering only stably infinite theories, as done in the original method, allows one to completely forgo the check, because stably infinite theories always satisfy it. Our method deals with the cardinality requirement by assuming enough on one theory, the shiny one, so that a simpler cardinality check, the one represented by δ_n, can be performed on the other.

We plan to continue our research on relaxing the stable infiniteness requirement by aiming at finding general sufficient conditions for shininess, and at identifying additional specific examples of shiny theories.

References

[1] Baader, F. and C. Tinelli, *A new approach for combining decision procedures for the word problem, and its connection to the Nelson-Oppen combination method*, in: W. McCune, editor, *Automated Deduction – CADE-14*, Lecture Notes in Computer Science **1249** (1997), pp. 19–33.

[2] Craigen, D., S. Kromodimoeljo, I. Meisels, B. Pase and M. Saaltink, *EVES: An overview*, in: S. Prehen and H. Toetenel, editors, *Formal Software Development Methods*, Lecture Notes in Computer Science **552** (1991), pp. 389–405.

[3] Detlefs, D. L., K. R. M. Leino, G. Nelson and J. B. Saxe, *Extended static checking*, Technical Report 159, Compaq System Research Center (1998).

[4] Ghilardi, S., *Quantifier elimination and provers integration*, Electronic Notes in Theoretical Computer Science **86** (2003).

[5] Hodges, W., "A Shorter Model Theory," Cambridge University Press, 1997.

[6] Levy, B., I. Filippenko, L. Marcus and T. Menas, *Using the state delta verification system (SDVS) for hardware verification*, in: T. F. Melham, V. Stavridou and R. T. Boute, editors, *Theorem Prover in Circuit Design: Theory, Practice and Experience* (1992), pp. 337–360.

[7] Manna, Z. and C. G. Zarba, *Combining decision procedures*, in: *Formal Methods at the Cross Roads: From Panacea to Foundational Support*, Lecture Notes in Computer Science (2003), to appear.

[8] Nelson, G. and D. C. Oppen, *Simplification by cooperating decision procedures*, ACM Transactions on Programming Languages and Systems **1** (1979), pp. 245–257.

[9] Nelson, G. and D. C. Oppen, *Fast decision procedures based on congruence closure*, Journal of the ACM **27** (1980), pp. 356–364.

[10] Oppen, D. C., *Complexity, convexity and combination of theories*, Theoretical Computer Science **12** (1980), pp. 291–302.

[11] Policriti, A. and J. T. Schwartz, *T-theorem proving I*, Journal of Symbolic Computation **20** (1995), pp. 315–342.

[12] Stump, A., C. W. Barret and D. L. Dill, *CVC: A cooperating validity checker*, in: E. Brinksma and K. G. Larsen, editors, *Computer Aided Verification*, Lecture Notes in Computer Science **2404**, 2002, pp. 500–504.

[13] Tinelli, C., *Cooperation of background reasoners in theory reasoning by residue sharing*, Journal of Automated Reasoning **30** (2003), pp. 1–31.

[14] Tinelli, C. and M. T. Harandi, *A new correctness proof of the Nelson-Oppen combination procedure*, in: F. Baader and K. U. Schulz, editors, *Frontiers of Combining Systems*, Applied Logic Series **3** (1996), pp. 103–120.

[15] Tinelli, C. and C. Ringeissen, *Unions of non-disjoint theories and combinations of satisfiability procedures*, Theoretical Computer Science **290** (2003), pp. 291–353.

[16] Tinelli, C. and C. G. Zarba, *Combining non-stably infinite theories*, Technical report, University of Iowa (2003), electronically available at `ftp://ftp.cs.uiowa.edu/pub/tinelli/papers/TinZar-RR-03.pdf`.

[17] Zarba, C. G., *Combining lists with integers*, in: R. Goré, A. Leitsch and T. Nipkow, editors, *International Joint Conference on Automated Reasoning: Short Papers*, Technical Report DII 11/01, Università di Siena, 2001, pp. 170–179.

[18] Zarba, C. G., *Combining multisets with integers*, in: A. Voronkov, editor, *Automated Deduction – CADE-18*, Lecture Notes in Computer Science **2392** (2002), pp. 363–376.

[19] Zarba, C. G., *Combining sets with integers*, in: A. Armando, editor, *Frontiers of Combining Systems*, Lecture Notes in Computer Science **2309** (2002), pp. 103–116.

[20] Zarba, C. G., *A tableau calculus for combining non-disjoint theories*, in: U. Egly and C. G. Fermüller, editors, *Automated Reasoning with Analytical Tableaux and Related Methods*, Lecture Notes in Computer Science **2381** (2002), pp. 315–329.