Combining Non-Stably Infinite Theories

Cesare Tinelli (tinelli@cs.uiowa.edu)
Department of Computer Science
The University of Iowa
14 MacLean Hall
Iowa City, IA 52242, USA

Calogero G. Zarba (zarba@loria.fr)
LORIA and INRIA-Lorraine
615 rue du Jardin Botanique, BP 101
54602 Villers-lès-Nancy Cedex, France

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 describe two extensions of the Nelson-Oppen method that address the problem of combining theories that are not stably infinite. In our extensions, the component decision procedures exchange not only equalities between shared variables, but also certain cardinality constraints.

Applications of our results include the combination of theories having only finite models, as well as the combination of non-stably infinite theories with the theory of equality, the theories of total and partial orders, and the theory of lattices with maximum and minimum.

Keywords: Combination of decision procedures, Nelson-Oppen method.

1. Introduction

In this paper we are concerned with the problem of how to modularly combine individual decision procedures for n first-order theories $T_1, \ldots, T_n$ into a decision procedure for their union.

The most successful and well-known method for combining decision procedures is due to Nelson and Oppen [15]. This method is at the heart of the verification systems CVC [20], EVES [5], SDVS [12], and SIMPLIFY [6], among others. Given n theories $T_1, \ldots, T_n$ over pairwise disjoint signatures, the Nelson-Oppen method allows one to decide the satisfiability of quantifier-free formulae in the union theory $T = T_1 \cup \cdots \cup T_n$, using as black boxes the decision procedures for the component theories $T_1, \ldots, T_n$. To be correct, the method requires that these component theories be pairwise signature disjoint and *stably infinite*.[1]

[1] A theory T is stably infinite if every quantifier-free formula satisfiable in a model of T is satisfiable in an infinite model of T.

The problem of combining signature disjoint theories has been addressed by Ghilardi [10], Tinelli [21], Tinelli and Ringeissen [23], and Zarba [28]. Here we present two extensions of the method that address the problem of combining theories that are not stably infinite. 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.

In the original Nelson-Oppen method, the component decision procedures are required to deduce equalities over the shared variables. In our extensions, the component decision procedures are also required to compute certain cardinality constraints. More in detail, when combining a theory T, the decision procedure for T is also required to compute the function $\mathit{mincard}_T$. This function takes as input a T-satisfiable conjunction Γ of literals, and returns the minimal cardinality k of any finite model of T that satisfies Γ.

In our **first extension**, we combine n signature-disjoint theories $T_1, \ldots, T_n$ that have a computable function *mincard*. We assume that all theories are stably *finite* (see later) and that one of them, T_1 say, has only finite models. Note that T_1 is not stably infinite, and therefore the original Nelson-Oppen method does not apply in this case.

Our first extension requires frequent computations of the function *mincard*. As we will see later, this function can be expensive to compute. To address this problem, we show a special case in which the number of calls to *mincard* can be drastically reduced. That happens whenever T_1 has only models of a fixed (and known) finite cardinality.

In our **second extension**, we combine n theories $T_1, \ldots, T_n$ such that T_1 is arbitrary, and $T_2, \ldots, T_n$ are *shiny*. We show that in this case it is enough to call *mincard* only $n-1$ times, once for each shiny theory T_i, with $i > 1$.

A shiny theory T is a theory with a computable *mincard* and such that (i) every T-satisfiable quantifier-free formula is satisfiable in a finite model of T, and (ii) every quantifier-free formula satifiable in a T-model of finite cardinality k is satisfiable in a T-model of cardinality k', for all $k' > k$. Examples of shiny theories include the theory of equality, the theory of partial orders, the theory of total orders, and the theory of lattices with maximum and minimum elements.

Shininess is a stronger property than stable infiniteness. Thus, the significance of our second extension is that, for instance, when we combine $n = 2$ theories, we can completely forego the stable infiniteness

requirement on one component theory if we can assume more (that is, shininess) about the other theory.

The shininess of the theory of equality leads to the following result, independently discovered also by Ganzinger [7]: if it is possible to decide the satisfiability in a Σ-theory T of quantifier-free Σ-formulae, then it is also possible to decide the satisfiability in T of quantifier-free formulae over any arbitrary signature $\Omega \supseteq \Sigma$.

1.1. Related work

The first description of the Nelson-Oppen method was published in a seminal paper by Nelson and Oppen [15]. This paper did not contain the stable infiniteness requirement. That notion was introduced later [14, 16] to correct a subtle problem in the original proof of correctness. Examples showing that stable infiniteness is indeed necessary for the method's correctness were given in [22] and [1]. The latter paper also shows that, while an equational theory need not be stably infinite, it is enough to add a *non-triviality* axioms $(\forall x)(\forall y)(x \not\approx y)$ to it to obtain a stably infinite theory. This result was later generalized first to Horn theories in [23] and then to *convex* theories in general in [2].

A model theoretic account on the significance of stable infiniteness for combination methods *a là* Nelson and Oppen can be found in [23]. In brief, and roughly speaking, the idea is that stable infiniteness is a sufficient condition for guaranteeing that all component theories in a combination have models of the same size. This intuition goes back to [19, 22] and was used in [1] (and later papers by the same authors) to prove the correctness of a combination method for the word problem in equational theories—with countable signatures.

In that work as well the correctness of the given combination method hinges on the existence of certain models of the same size for each component theories. There however the existence of these models is not provided by a stable infiniteness assumption on the theories but simply by a non-triviality assumption.[2] The reason this is enough in [1] is that the word problem for a non-trivial equational theory can be reduced to the word problem in the theory's free model with a countably infinite set of generators. And this model is countably infinite whenever the signature of the theory is countable.

The present paper has also connections with previous work by Zarba on the combination of integers with data structures such as lists [25], sets [27], and multisets [26]. In particular, in order to relax the stably infiniteness requirement, Zarba used a *mincard* function for the case

[2] A theory is non-trivial if it admits models of cardinality greater than one.

of lists and sets, whereas an ad hoc reduction to linear arithmetic was used for the case of multisets.

The work described in the present paper, which extends and revises results initially described in [24], is the first that focuses on relaxing the stable-infiniteness requirement in the general setting of the Nelson-Oppen method.

1.2. Organization of the paper

The paper is organized as follows. In Section 2 we introduce some preliminary notions that will be used in what follows. In Section 3 we describe a preprocessing phase that is common to both of our combination methods. In Section 4 we describe and prove correct our first combination method, which combines one or more stably finite theories with one having only finite models. In Section 5 we describe and prove correct our second method, which combines one or more shiny theories with an arbitrary one. In Section 6 we provide several applications of our methods. In Section 7 we conclude with directions for further research. Finally, in Appendix A we prove a technical theorem that is at the base of the correctness of our methods.

2. Preliminaries

The results in this paper are in the context of first-order logic *with equality*. We describe our version of the logic in the following.

2.1. Syntax

A *signature* is a countable set $\Sigma = \Sigma^{\mathrm{C}} \cup \Sigma^{\mathrm{F}} \cup \Sigma^{\mathrm{P}}$ where Σ^{C} is a set of constant symbols, Σ^{F} is a set of function symbols, and Σ^{P} is a set of predicate symbols.

A Σ-*atom* is an expression of the form $P(t_1, \ldots, t_n)$, where $P \in \Sigma^{\mathrm{P}}$ and $t_1, \ldots, t_n$ are Σ-terms, or an expression of the form $s \approx t$, where $\approx$ is the equality logical symbol and s, t are Σ-terms, or one of the symbols *true*, *false*. Σ-*formulae* are constructed by applying in the standard way the connectives $\neg$, $\wedge$, $\vee$, $\rightarrow$ and the quantifiers $\forall, \exists$ to Σ-atoms. Σ-*literals* are Σ-atoms or their negations. Σ-*sentences* are Σ-formulae with no free variables.

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

We identify a conjunction of formulae $\varphi_1 \wedge \cdots \wedge \varphi_n$ with the set $\{\varphi_1, \ldots, \varphi_n\}$. In addition, we abbreviate literals of the form $\neg(s \approx t)$ with $s \not\approx t$.

For every integer $n > 0$, we denote with δ_n a cardinality constraint that says that there must be at least n elements. More precisely, we use the notation $\Gamma \cup \delta_n$, for every conjunction Γ of literals, to denote a conjunction of literals obtained by using the following process:

1. generate n fresh variables $w_1, \ldots, w_n$ not occurring in Γ;
2. let $\delta_n = \{w_i \not\approx w_j \mid 1 \leq i < j \leq n\}$.

2.2. Semantics

DEFINITION 1. *Let Σ be a signature. A* Σ-interpretation *$\mathcal{A}$ with domain A over a set of variables V 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 $f^{\mathcal{A}} : A^n \to A$;*
- *each predicate symbol $P \in \Sigma^{\mathrm{P}}$ of arity n as a subset $P^{\mathcal{A}}$ of A^n.*

Unless otherwise specified, we use the convention that calligraphic letters $\mathcal{A}$, $\mathcal{B}$, ... denote interpretations, and that the corresponding Roman letters A, B, ... denote the domains of the interpretations.

Let $\mathcal{A}$ be a Σ-interpretation over a set of variables V. 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 *satisfied* by an interpretation $\mathcal{A}$ if it evaluates to true under $\mathcal{A}$. If φ is satisfied by $\mathcal{A}$, we say that $\mathcal{A}$ is a *model* of φ. A formula φ over a set V of variables is:

- *valid*, if it is satisfied by all interpretations over V;
- *satisfiable*, if it is satisfied by some interpretation over V;
- *unsatisfiable*, if it is not satisfiable.

The notion of validity, satisfiability, and unsatisfiability naturally extend to sets of formulae.

2.3. Theories

If Σ is a signature, 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 over a set V of variables is:

- T-*valid*, if it is satisfied by all T-models over V;
- T-*satisfiable*, if it is satisfied by some T-model over V;
- T-*unsatisfiable*, if it is not T-satisfiable.

The notion of T-validity, T-satisfiability, and T-unsatisfiability naturally extend to sets of formulae.

A theory T is *axiomatized* by a set S of sentences if S and T are logically equivalent, that is, if S and T have the same set of models.

Given a Σ-theory T and 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.

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

DEFINITION 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, the theory of integer arithmetic, the theory of rational arithmetic, the theory of acyclic lists, and the theory of arrays. (Note that since we regard $\approx$ as a logical symbol, for us the theory of equality and the empty theory are the same theory.)

Examples of stably finite theories include the theory of equality, all theories having only finite models, and all theories axiomatized by formulae in the Bernays-Schönfinkel-Ramsey class [3, 18].

A theory can be both stably finite and stably infinite. We will show that in Section 6 for a number of theories.

DEFINITION 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 $|B| = \kappa$.*

The following proposition is a direct consequence of Definition 3.

PROPOSITION 4. *Every smooth theory is stably infinite.*

The next proposition is useful when proving that a theory is smooth.

PROPOSITION 5. *Let T be a Σ-theory. Then the following are equivalent:*

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

Proof. $(1 \Rightarrow 2)$. Trivial.

$(2 \Rightarrow 1)$. Let φ be a quantifier-free formula, and let $\mathcal{A}$ be a model of φ.

By induction on $|A|$, one can see that if A is finite then φ has a model of any finite cardinality $\kappa > |A|$. By compactness, φ has a countably infinite model, and by the Upward Löwenheim-Skolem Theorem, φ has also a model of any infinite cardinality κ.

If instead A is infinite then, by the upward Löwenheim-Skolem Theorem again, it follows that φ has a model of any (infinite) cardinality $\kappa > |A|$. □

Given a Σ-theory T and a T-satisfiable set Γ of Σ-literals, we denote with $mincard_T(\Gamma)$ the smallest cardinality of a T-model satisfying Γ. When T is the theory of equality, we abbreviate $mincard_T$ with $mincard$ (without any subscript).

Note that if T is a stably finite theory then, for every T-satisfiable set of literals Γ, $mincard_T(\Gamma)$ is an integer.

DEFINITION 6. *A Σ-theory T is* SHINY *if:*

- *T is smooth;*
- *T is stably finite;*
- *$mincard_T$ is computable.*

Examples of shiny theories include the theory of equality, the theory of partial orders, the theory of total orders, and the theory of lattices with maximum and minimum elements.

3. Preprocessing

Let T_i be a Σ_i-theory, for $i = 1, \ldots, n$. Assume that all the signatures $\Sigma_1, \ldots, \Sigma_n$ are pairwise disjoint, and that all the quantifier-free satisfiability problems for $T_1, \ldots, T_n$ are decidable. Finally, let $T = T_1 \cup \cdots \cup T_n$ and $\Sigma = \Sigma_1 \cup \cdots \cup \Sigma_n$.

In this and the next two sections, we describe two combination methods that, under certain conditions, yield a decision procedure for the quantifier-free satisfiability problem of T.

Without loss of generality, we restrict ourselves to conjunctions of literals. Note that this can always be done because every formula φ can be effectively converted into an equisatisfiable formula in disjunctive normal form $\psi_1 \vee \cdots \vee \psi_n$, where each ψ_i is a conjunction of literals. Then φ is satisfiable if and only if at least one of the disjuncts ψ_i is satisfiable.

Our methods share a common nondeterministic *preprocessing phase*, and have separate *check phases*. We describe the preprocessing phase in this section, and we remind to Sections 4 and 5 for the check phases.

The preprocessing phase consists of a *variable abstraction step* and a nondeterministic *decomposition step*.

First step: variable abstraction
Let Γ be a conjunction of Σ-literals. The output of the variable abstraction step is a conjunction

$$\Gamma' = \Gamma_1 \cup \cdots \cup \Gamma_n$$

satisfying the following properties:

(a) each literal in Γ_i is a Σ_i-literal, for $i = 1, \ldots, n$;

(b) Γ' is T-satisfiable if and only if so is Γ.

Properties (a) and (b) can be effectively enforced with the help of fresh variables. For instance, the simplest way to enforce both properties is to use fresh variables in order to flatten the input, so that all literals in Γ' are of the form $x_0 \approx f(x_1, \ldots, x_n)$, $x_1 \approx x_2$, $x_1 \not\approx x_2$, $P(x_1, \ldots, x_n)$, or $\neg P(x_1, \ldots, x_n)$, where f is a function symbols, P is a predicate symbol, and the x_i are variables.

Second step: decomposition
Let $\Gamma_1 \cup \cdots \cup \Gamma_n$ be a conjunction of literals obtained in the variable abstraction step. Let V be the set of variables that occur in at least two of the conjunctions Γ_i, that is

$$V = \bigcup_{i \neq j} (vars(\Gamma_i) \cap vars(\Gamma_j)) \ .$$

In words, V is a set of the variables that are shared by at least two of the conjunctions $\Gamma_1, \ldots, \Gamma_n$.

In the decomposition step we nondeterministically guess an equivalence relation E over V. Intuitively, what we are guessing is, for each variable $x, y \in V$, whether or not we have $x = y$.

Then, we construct the *arrangement* of V induced by E, defined by

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

and we output the conjunction

$$\Gamma_1 \cup \cdots \cup \Gamma_n \cup arr(V, E). \tag{1}$$

We call (1) a conjunction in *arranged normal form.*

Note that a conjunction in arranged normal can also be thought as having the form

$$(\Gamma_1 \cup arr(V, E)) \cup \cdots \cup (\Gamma_n \cup arr(V, E)).$$

Then, if we let $V_i = vars(\Gamma_i \cup arr(V, E))$, we have the property that

$$\bigcup_{i \neq j} (V_i \cap V_j) = \bigcap_i V_i.$$

This is a crucial property for following technical result, which is at the core of our combination method's correctness, and whose proof can be found in the appendix.

THEOREM 7 (Generalized Combination for Disjoint Signatures). *Let $\Phi = \Phi_1 \cup \cdots \cup \Phi_n$, where Φ_i is a set of Σ_i-formulae, for $i = 1, \ldots, n$. Also, let $V_i = vars(\Phi_i)$ and $V = \bigcup_{i \neq j} (V_i \cap V_j)$. Assume that all the signatures $\Sigma_1, \ldots, \Sigma_n$ are pairwise disjoint, and that*

$$\bigcup_{i \neq j} (V_i \cap V_j) = \bigcap_i V_i.$$

Then Φ is satisfiable if and only if there exist interpretations $\mathcal{A}_1, \ldots, \mathcal{A}_n$ such that:

(i) $\mathcal{A}_i$ satisfies Φ_i, for $i = 1, \ldots, n$;

(ii) $|A_1| = |A_2| = \cdots = |A_n|$;

(iii) $x^{\mathcal{A}_i} = y^{\mathcal{A}_i}$ if and only if $x^{\mathcal{A}_j} = y^{\mathcal{A}_j}$, for all i, j and for every $x, y \in V$.

1: $N \leftarrow 1$
2: **while** *true* **do**
3: **if** $\exists i$ such that $\Gamma_i \cup arr(V,E) \cup \delta_N$ is T_i-unsatisfiable **then**
4: **return** `fail`
5: **else if** $\exists i$ such that $mincard_{T_i}(\Gamma_i \cup arr(V,E) \cup \delta_N) = m > N$ **then**
6: $N \leftarrow m$
7: **else**
8: **return** `succeed`

Figure 1. The check phase of the first combination method.

4. Theories having only finite models

In this section we describe and prove correct the check phase of our first combination method, which allows us to combine n theories with a computable *mincard*, provided that at least one of them has only finite models.

Thus, let T_i be a Σ_i-theory, for $i = 1, \ldots, n$. Assume that all the signatures $\Sigma_1, \ldots, \Sigma_n$ are pairwise disjoint, and that all the quantifier-free satisfiability problems for $T_1, \ldots, T_n$ are decidable. Also, let $T = T_1 \cup \cdots \cup T_n$ and $\Sigma = \Sigma_1 \cup \cdots \cup \Sigma_n$. Finally, assume that:

(i) T_i is stably finite, for $i = 1, \ldots, n$;

(ii) $mincard_{T_i}$ is computable, for $i = 1, \ldots, n$;

(iii) all T_1-interpretations are finite.

If $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_n \cup arr(V,E)$ is a conjunction of literals in arranged normal form obtained in the preprocessing phase, then we can check the T-satisfiability of Γ by running the procedure in Figure 1 on it.

4.1. An example

Example 8. Let T_1, T_2, T_3 be theories such that, for each interpretation $\mathcal{A}$ we have:

- $\mathcal{A}$ is a T_1-interpretation if and only if $|A| \leq 10$;
- $\mathcal{A}$ is a T_2-interpretation if and only if $|A|$ is not even;
- $\mathcal{A}$ is a T_3-interpretation if and only if $|A|$ is not odd.

Note that the union theory $T = T_1 \cup T_2 \cup T_3$ is inconsistent. This inconstency can be formally checked with our methods by verifying that the formula *true* is T-unsatisfiable.

Indeed, the formula *true* is already in arranged normal form, and therefore we can simply apply to it the procedure in Figure 1. Then, said procedure will return `fail` after 10 iterations of the **while** loop. □

4.2. Correctness

The following proposition shows that the procedure in Figure 1 is terminating.

PROPOSITION 9. *Let* $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_n \cup arr(V, E)$ *be a conjunction of literals in arranged normal form. Then the procedure in Figure 1 terminates on input* Γ.

Proof. By contradiction, assume that the procedure in Figure 1 does not terminate on input Γ. Then the set $T_1 \cup \Gamma_1 \cup arr(V, E) \cup \delta_N$ is satisfiable for increasing large N. By compactness, $T_1 \cup \Gamma_1 \cup arr(V, E)$ is satisfiable in an infinite interpretation, which contradicts the assumption that all T_1-interpretations are finite. □

The following two propositions show that the procedure in Figure 1 is also partially correct.[3]

PROPOSITION 10. *Let* $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_n \cup arr(V, E)$ *be a conjunction of literals in arranged normal form. If* Γ *is* T*-satisfiable then the procedure in Figure 1 outputs* `succeed` *on input* Γ.

Proof. Let $\mathcal{F}$ be a T-interpretation satisfying Γ, and let $\kappa = |F|$. Since $\mathcal{F}$ satisfies T_1, $\kappa \in \mathbb{N}^+$.

Recalling that the procedure is terminating, let $k_1, \ldots, k_q$ be all the values taken by N, in order, during the execution of the procedure on input Γ.

By induction, we show that $k_i \leq \kappa$, for all $i = 1, \ldots, q$. The base case is trivial because $k_1 = 1$. For the induction step, assume that $k_j \leq \kappa$. By construction, there exists an index i such that $k_{j+1} = mincard_{T_i}(\Gamma_i \cup arr(V, E) \cup \delta_{k_j})$. Note that $\mathcal{F}$ satisfies $\Gamma_i \cup arr(V, E) \cup \delta_{k_j}$. Thus, $k_{j+1} \leq \kappa$.

Since $k_q \leq \kappa$, the procedure cannot fail for $N = k_q$. Thus, since k_q is the last value held by N, the procedure must return `succeed`. □

PROPOSITION 11. *Let* $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_n \cup arr(V, E)$ *be a conjunction of literals in arranged normal form. If the procedure in Figure 1 outputs* `succeed` *on input* Γ *then* Γ *is* T*-satisfiable.*

[3] Recall that a procedure P is *partially correct* if it returns a correct answer each time it terminates.

1: $N \leftarrow k$
2: **if** $\Gamma_1 \cup arr(V,E) \cup \delta_N$ is T_1-unsatisfiable **then**
3: **return** `fail`
4: **else**
5: **for** $i \leftarrow 2$ **to** n **do**
6: **if** $\Gamma_i \cup arr(V,E) \cup \delta_N$ is T_i-unsatisfiable **then**
7: **return** `fail`
8: **else if** $mincard_{T_i}(\Gamma_i \cup arr(V,E) \cup \delta_N) > N$ **then**
9: **return** `fail`
10: **return** `succeed`

Figure 2. An optimization of the first combination method.

Proof. Let k be the last value held by the variable N. Then, for all indices i, we have that $\Gamma_i \cup arr(V,E) \cup \delta_k$ is T_i-satisfiable, and that $mincard_{T_i}(\Gamma_i \cup arr(V,E) \cup \delta_k) = k$. It follows that there exist interpretations $\mathcal{A}_1, \ldots, \mathcal{A}_n$ satisfying all requirements of Theorem 7. Hence, Γ is satisfiable. □

Combining Propositions 9, 10, and 11 with the observation that a conjunction of literals has only finitely many arranged normal forms, we obtain the following decidability result.

THEOREM 12. *Let $T = T_1 \cup \cdots \cup T_n$ be the union of pairwise signature-disjoint theories such that:*

(i) T_i is stably finite, for $i = 1, \ldots, n$;

(ii) $mincard_{T_i}$ is computable, for $i = 1, \ldots, n$;

(iii) all T_1-interpretations are finite.

If all the quantifier-free satisfiability problems of $T_1, \ldots, T_n$ are decidable, then the quantifier-free satisfiability problem of T is decidable.

4.3. An optimization

Our first combination method can be optimized when all T_1-models have a fixed, known cardinality k. In this case, in order to prove that a conjunction $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_n \cup arr(V,E)$ in arranged normal form is T-satisfiable, it suffices to run the more efficient procedure in Figure 2 to Γ.

The correctness of this optimization can be proved along the same lines as in Section 4.2.

Example 13. Let T_1 and T_2 be theories such that, for each interpretation $\mathcal{A}$ we have:

- $\mathcal{A}$ is a T_1-interpretation if and only if $|A| = 10$;
- $\mathcal{A}$ is a T_2-interpretation if and only if $|A|$ is not even.

Note that the union theory $T = T_1 \cup T_2$ is inconsistent. This inconstency can be formally checked with our methods by verifying that the formula *true* is T-unsatisfiable.

Indeed, the formula *true* is already in arranged normal form, and therefore we can simply apply to it the procedure in Figure 2, which will return `fail` at line 7 of the first (and unique) iteration of the **for** loop. □

5. Shiny theories

In this section we describe and prove correct the check phase of our second combination method, which allows us to combine several shiny theories with one arbitrary theory.

Thus, let T_i be a Σ_i-theory, for $i = 1, \ldots, n$. Assume that all the signatures $\Sigma_1, \ldots, \Sigma_n$ are pairwise disjoint, and that all the quantifier-free satisfiability problems for $T_1, \ldots, T_n$ are decidable. Also, let $T = T_1 \cup \cdots \cup T_n$ and $\Sigma = \Sigma_1 \cup \cdots \cup \Sigma_n$. Finally, assume that:

(i) T_1 is arbitrary;

(ii) $T_2, \ldots, T_n$ are shiny.

If $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_n \cup arr(V, E)$ is a conjunction of literals in arranged normal obtained in the preprocessing phase, then we can check the T-satisfiability of Γ by running the procedure in Figure 3 on it.

5.1. Examples

The next two examples illustrate the use of our second combination method. They are adapted from [22] and [1], respectively, where they were used to show that the Nelson-Oppen method is in fact incorrect on non-stably infinite theories.

Example 14. Let $\Sigma_1 = \{f\}$ and $\Sigma_2 = \{g\}$ be signatures, where f and g are distinct unary function symbols. Also, let T_1 be a Σ_1-theory such that all T_1-interpretations have cardinality at most two, and let T_2 be the theory of equality over the signature Σ_2.

```
1:  N ← 1
2:  for i ← 2 to n do
3:    if Γ_i ∪ arr(V, E) is T_i-unsatisfiable then
4:      return fail
5:    else
6:      N ← max(N, mincard_{T_i}(Γ_i ∪ arr(V, E)))
7:  if Γ_1 ∪ arr(V, E) ∪ δ_N is T_1-unsatisfiable then
8:    return fail
9:  else
10:   return succeed
```

Figure 3. The check phase of the second combination method.

Since T_1 is not stably infinite, we cannot use the Nelson-Oppen combination method in order to combine T_1 with T_2. However, in Section 6.2 we will show that the theory of equality is shiny, regardless of the associated signature. Thus, we can apply our second combination method to T_1 and T_2.[4]

As an example, let Γ be the following conjunction of literals:

$$\Gamma = \left\{ \begin{array}{l} f(x) \not\approx f(y)\,, \\ g(x) \not\approx g(z)\,, \\ g(y) \not\approx g(z) \end{array} \right\}.$$

This conjunction is $(T_1 \cup T_2)$-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. However, every $(T_1 \cup T_2)$-interpretation has at most two elements.

Let us apply our second combination method to Γ. In the variable abstraction phase we return the conjunctions

$$\Gamma_1 = \{\ f(x) \not\approx f(y)\ \}\,, \qquad \Gamma_2 = \left\{ \begin{array}{l} g(x) \not\approx g(z)\,, \\ g(y) \not\approx g(z) \end{array} \right\}.$$

Since $vars(\Gamma_1) \cap vars(\Gamma_2) = \{x, y\}$, in the decomposition phase only two equivalence relations can be guessed: either $(x, y) \in E$ or $(x, y) \notin E$.

If we guess $(x, y) \in E$ then we have that $\Gamma_1 \cup \{x \approx y\}$ is T_1-unsatisfiable and therefore the procedure in Figure 3 will output `fail` when reaching line 8.

If instead we guess $(x, y) \notin E$ then we have that $\Gamma_2 \cup \{x \not\approx y\}$ is T_2-satisfiable. In addition, we also have $mincard_{T_2}(\Gamma_2 \cup \{x \not\approx y\}) = 3$. To see this, first observe that $\Gamma_2 \cup \{x \not\approx y\}$ implies $x \not\approx y \wedge x \not\approx z \wedge y \not\approx z$,

[4] Note that if we knew that $mincard_{T_1}$ was computable, we could use the first combination method as well.

and therefore $mincard_{T_2}(\Gamma_2 \cup \{x \not\approx y\}) \geq 3$. Moreover, we can construct an interpretation $\mathcal{A}$ of cardinality 3 satisfying $\Gamma_2 \cup \{x \not\approx y\}$ 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 $a \in A$.[5] Since $\Gamma_1 \cup \{x \not\approx y\} \cup \delta_3$ is T_1-unsatisfiable, the procedure in Figure 3 will output `fail` when reaching line 8.

Summing up, the procedure in Figure 3 outputs `fail` for all possible arrangements, and therefore we can declare that Γ is $(T_1 \cup T_2)$-unsatisfiable. □

Example 15. Let $\Sigma_1 = \{f, g, h\}$ and $\Sigma_2 = \{k\}$ and be signatures, where k, f and g are distinct unary function symbols. Let T_1 be the equational theory

$$T_1 = \left\{ \begin{array}{l} (\forall x)(\forall y)(x \approx f(g(x), g(y))), \\ (\forall x)(\forall y)(f(g(x), h(y)) \approx y) \end{array} \right\},$$

and let T_2 be the theory of equality over the signature Σ.

As explained in [1], using simple term rewriting arguments it is possible to show that T_1 admits models of cardinality greater than one, and so admits models of infinite cardinality. (This is because the set of models of an equational theory is closed under direct products.) However, T_1 is not stably infinite.

In fact, consider the quantifier-free formula $g(z) \approx h(z)$. This formula is T_1-satisfiable because both the formula and T_1 admit a trivial model, that is, a model with just one element. Now let $\mathcal{A}$ be any T_1-model of $g(z) \approx h(z)$, let $a_0 = z^{\mathcal{A}}$, and let $a \in A$. Because of the axioms of T_1, 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_1, which entails that the theory T_1 is not stably infinite.

Now let Γ be the following conjunction of literals:

$$\Gamma = \left\{ \begin{array}{l} g(z) \approx h(z), \\ k(z) \not\approx z \end{array} \right\}.$$

This conjunction is $(T_1 \cup T_2)$-unsatisfiable, because $g(z) \approx h(z)$ is satisfiable only in trivial models of $T_1 \cup T_2$ (for being satisfiable only in trivial models of T_1, as seen above), while $k(z) \not\approx z$ is satisfiable only in non-trivial models of $T_1 \cup T_2$.

[5] We will see how to effectively compute $mincard_{T_1}$ in Section 6.1.

Let us apply our second combination method to Γ. In the variable abstraction phase we simply return the conjunctions

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

Since $vars(\Gamma_1) \cap vars(\Gamma_2) = \{z\}$, in the decomposition phase there is only one equivalence relation that can be guessed: $(z, z) \in E$.

Clearly, Γ_2 is T_2-satisfiable, and in models of cardinality at least 2. Therefore, we have that $mincard_{T_2}(\Gamma_1) = 2$. Moreover, for what we argued above, $\Gamma_1 \cup \delta_2$ is T_1-unsatisfiable, so that the procedure in Figure 3 will output `fail` when reaching line 8. □

5.2. Correctness

Clearly, the procedure in Figure 3 is terminating. The following two propositions show that the procedure is also partially correct.

PROPOSITION 16. *Let $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_n \cup arr(V, E)$ be a conjunction of literals in arranged normal form. If Γ is T-satisfiable then the procedure in Figure 3 outputs* `succeed` *on input Γ.*

Proof. Let $\mathcal{F}$ be a T-interpretation satisfying Γ. Clearly, $\mathcal{F}^{\Sigma_i, V}$ is a T_i-interpretation satisfying $\Gamma_i \cup arr(V, E)$, for $i = 2, \ldots, n$, and therefore the procedure can never reach line 4.

Let k be the final value held by the variable N. By definition of *mincard*, we have $k \leq |F|$, which implies that $\mathcal{F}^{\Sigma_1, V}$ is also a T_1-interpretation satisfying $\Gamma_1 \cup arr(V, E) \cup \delta_k$. Therefore, the procedure can never reach line 7 either, and it must terminate at line 9 outputting `succeed`. □

PROPOSITION 17. *Let $\Gamma = \Gamma_1 \cup \cdots \cup \Gamma_n \cup arr(V, E)$ be a conjunction of literals in arranged normal form. If the procedure in Figure 3 outputs* `succeed` *on input Γ then Γ is T-satisfiable.*

Proof. Let k be the final value held by the variable N. Then there exist interpretations $\mathcal{A}_1, \ldots, \mathcal{A}_n$ such that:

- $\mathcal{A}_1$ is a T_1-interpretation satisfying $\Gamma_1 \cup arr(V, E) \cup \delta_k$;
- $\mathcal{A}_i$ is a T_i-interpretation satisfying $\Gamma_i \cup arr(V, E)$, for $i = 2, \ldots, n$.

Moreover, $mincard(\Gamma_i \cup arr(V, E)) \leq k$, for $i = 2, \ldots, n$. Let $\kappa = |A_1|$. Clearly, $|A_1| \geq k$. By definition of *mincard* and the smoothness of $\mathcal{A}_2, \ldots, \mathcal{A}_n$, we can then assume without loss of generality that $|A_i| = \kappa$ as well, for $i = 2, \ldots, n$.

Thus, since all the $\mathcal{A}_i$ satisfy $arr(V, E)$, we can apply Theorem 7, obtaining that Γ is T-satisfiable. □

Combining Propositions 16 and 17 with the fact that the procedure in Figure 3 is terminating, we obtain the following decidability result.

THEOREM 18. *Let $T = T_1 \cup \cdots \cup T_n$ be the union of pairwise signature-disjoint theories such that:*

(i) T_1 is arbitrary;

(ii) $T_2, \ldots, T_n$ are shiny;

If all the quantifier-free satisfiability problems of $T_1, \ldots, T_n$ are decidable, then the quantifier-free satisfiability problem of T is decidable.

6. Applications

In this section, we present some examples of theories to which our combination results apply.

To prove our claims we will use the following definition and lemmas, adapted from basic notions and results in model theory (see, for instance, [11]).

DEFINITION 19. *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 $a_1, \ldots, a_n \in A$.*

We say that $\mathcal{A}$ IS EMBEDDED IN *$\mathcal{B}$ if there is an embedding of $\mathcal{A}$ into $\mathcal{B}$.*

LEMMA 20. *Let $\mathcal{A}, \mathcal{B}$ be two interpretations such that $\mathcal{A}$ is embedded in $\mathcal{B}$, and let φ be a quantifier-free formula. Then φ is satisfied by $\mathcal{B}$ whenever it is satisfied by $\mathcal{A}$.*

DEFINITION 21. *A formula is* UNIVERSAL *if it is of the form*

$$(\forall x_1) \cdots (\forall x_n) \psi \,,$$

where $n \geq 0$ and ψ is quantifier-free. A theory is UNIVERSAL *if it is axiomatized by a set of universal sentences.*

Input: a T-satisfiable set Γ of Σ-literals over the variables V
Output: $mincard_T(\Gamma)$
1: $k \leftarrow 0$
2: **while** *true* **do**
3: $\quad k \leftarrow k + 1$
4: $\quad$ **for** all Σ-interpretations $\mathcal{A}$ over V of cardinality k **do**
5: $\quad\quad$ **if** $\Gamma \cup diagram(\mathcal{A})$ is T-satisfiable **then**
6: $\quad\quad\quad$ **return** k

Figure 4. A procedure for computing $mincard_T$.

LEMMA 22. *Let T be a universal Σ-theory and let $\mathcal{A}$ be a Σ-interpretation. If $\mathcal{A}$ is embedded in a model of T, then $\mathcal{A}$ is also a model of T.*

Since both combination methods require at least one of the component theories to have a computable *mincard*, we start by providing a general sufficient condition for that, which will be useful later.

6.1. Computability of $mincard_T$

In this subsection we address the problem of computing $mincard_T$, for theories T that are stably finite and have a decidable quantifier-free satisfiability problem. We show that for any such theory T, $mincard_T$ is always computable, provided that Σ is finite and that T is universal.

Intuitively, we compute $mincard_T(\Gamma)$ by enumerating, modulo isomorphism, all Σ-interpretations $\mathcal{A}$ in increasing order of cardinality, and checking whether $T \cup \Gamma$ is satisfied by $\mathcal{A}$. This enumeration can be effectively done because we assume that Σ is finite. Termination is guaranteed by the stable finiteness of T, and partial correctness is guaranteed by the universality of T.

Figure 4 shows a procedure for computing $mincard_T$. There, the notation $diagram(\mathcal{A})$ in line 5 stands for a set of literals that can be intuitively seen as a finite specification of the interpretation $\mathcal{A}$. More in detail, $diagram(\mathcal{A})$ is effectively constructed from $\mathcal{A}$ using the following process:

1. For each element a in A, generate a fresh variable y_a. Also, initially let $\Delta = \emptyset$.
2. For each variable or constant symbol u in $V \cup \Sigma^{\mathrm{C}}$, if $u^{\mathcal{A}} = a$, add the literal $u \approx y_a$ to Δ.
3. For each function symbol f in Σ^{F} of arity n, if $a = f^{\mathcal{A}}(a_1, \ldots, a_n)$, add the literal $y_a \approx f(y_{a_1}, \ldots, y_{a_n})$ to Δ.

4. For each predicate symbol P in $\Sigma^{\mathrm{P}} \cup \{\approx\}$ of arity n, if $(a_1, \ldots, a_n) \in P^{\mathcal{A}}$, add the literal $P(y_{a_1}, \ldots, y_{a_n})$ to Δ; if instead $(a_1, \ldots, a_n) \notin P^{\mathcal{A}}$, add the literal $\neg P(y_{a_1}, \ldots, y_{a_n})$ to Δ.

We define $\mathit{diagram}(\mathcal{A})$ as the set Δ obtained at the end of this process. By construction, $\mathit{diagram}(\mathcal{A})$ is satisfied by the expansion $\mathcal{A}'$ of $\mathcal{A}$ to the new variables y_a (with $a \in A$) that interprets each y_a as a. For simplicity, we will identify $\mathcal{A}'$ with $\mathcal{A}$ in the following.

The following proposition proves that the procedure in Figure 4 effectively computes $\mathit{mincard}_T(\Gamma)$.

PROPOSITION 23. *Let T be a stably finite Σ-theory with a decidable quantifier-free satisfiability problem. If Σ is finite and T is universal, then $\mathit{mincard}_T$ is computable.*

Proof. Let Γ be a T-satisfiable set of Σ-literals over some set V of variables.

We first show that the procedure in Figure 4 must terminate on input Γ. In fact, since T is stable finite, there exists a T-interpretation $\mathcal{A}$ satisfying Γ such that $|A| = k$, for some positive integer k. By construction of $\mathit{diagram}(\mathcal{A})$, we have that $\mathcal{A}$ satisfies $\mathit{diagram}(\mathcal{A})$. Therefore, $\mathcal{A}$ satisfies $T \cup \Gamma \cup \mathit{diagram}(\mathcal{A})$, and the procedure stops no later than at iteration k.

Next, we show that the procedure is also partially correct. Thus, assume that the procedure stops at iteration k. Then there exists a T-interpretation $\mathcal{B}$ satisfying $\Gamma \cup \mathit{diagram}(\mathcal{A})$, where $|A| = k$. If we prove that there exists an embedding of $\mathcal{A}$ into $\mathcal{B}$, by Lemma 22 we obtain that $\mathcal{A}$ satisfies $T \cup \Gamma \cup \mathit{diagram}(\mathcal{A})$,[6] which implies that $\mathit{mincard}_T(\Gamma) \leq k$.

Indeed, an embedding of $\mathcal{A}$ into $\mathcal{B}$ is provided by the function $h : A \to B$ defined by

$$h(a) = y_a^{\mathcal{B}}\,, \qquad \text{for each } a \in A\,.$$

By construction, h in injective.

Let $u \in V \cup \Sigma^{\mathrm{C}}$, and let $a = u^{\mathcal{A}}$. Then the literal $u \approx y_a$ is in Γ. Thus $h(u^{\mathcal{A}}) = y_a^{\mathcal{B}} = u^{\mathcal{B}}$.

Let $f \in \Sigma_{\mathrm{F}}$ be a function symbol of arity n. Let $f^{\mathcal{A}}(a_1, \ldots, a_n) = a$. Then

$$\begin{aligned} h(f^{\mathcal{A}}(a_1, \ldots, a_n)) &= h(a) \\ &= y_a^{\mathcal{B}} \\ &= f^{\mathcal{B}}(y_{a_1}^{\mathcal{B}}, \ldots, y_{a_n}^{\mathcal{B}}) \\ &= f^{\mathcal{B}}(h(a_1), \ldots, h(a_n))\,. \end{aligned}$$

[6] This is because $T \cup \Gamma \cup \mathit{diagram}(\mathcal{A})$ can be seen as an universal theory if we consider the (free) variables of Γ and of $\mathit{diagram}(\mathcal{A})$ as constant symbols.

Let $P \in \Sigma^{\mathrm{F}}$ be a predicate symbol of arity n. Assume first that $(a_1, \ldots, a_n) \in P^{\mathcal{A}}$. Then $(y^{\mathcal{B}}_{a_1}, \ldots, y^{\mathcal{B}}_{a_n}) \in P^{\mathcal{B}}$. It follows that $(h(a_1), \ldots, h(a_n)) \in P^{\mathcal{B}}$. Vice versa, it can be shown that if $(h(a_1), \ldots, h(a_n)) \in P^{\mathcal{B}}$ then $(a_1, \ldots, a_n) \in P^{\mathcal{A}}$.

Since h is an embedding of $\mathcal{A}$ into $\mathcal{B}$, by Lemma 22 $\mathcal{A}$ satisfies $T \cup \Gamma \cup \mathit{diagram}(\mathcal{A})$, and therefore $\mathit{mincard}_T(\Gamma) \leq k$. All we need to show then is that $\mathit{mincard}_T(\Gamma) = k$. Assume by contradiction that $\mathit{mincard}_T(\Gamma) < k$. Then there exists a T-interpretation $\mathcal{A}$ of cardinality $n < k$ that satisfies Γ. But then, $\mathcal{A}$ also satisfies $T \cup \Gamma \cup \mathit{diagram}(\mathcal{A})$, and the procedure would have stopped at iteration n, not k. □

The procedure in Figure 4 has of course only theoretical interest because it has a prohibitive time complexity. To see that, first observe that for any set A of cardinality $n > 1$ there are at least 2^n possible functions from A into itself—all the possible binary functions on A. That means that if Σ has at least one function symbol, there are at least 2^n non-isomorphic Σ-interpretations of cardinality n. Consider then any satisfiable set Γ of literals containing the set δ_{n+1}. Since the smallest T-model satisfying δ_{n+1} has cardinality $n + 1$, the procedure will certainly construct all those 2^n interpretations of cardinality n before succeeding. It follows that for all formulae Γ like the above for which $n + 1$ is at least linear in the size of Γ,[7] the complexity of the procedure is at least exponential in the size of Γ.

One may wonder whether $\mathit{mincard}_T$ can be computed more efficiently using a better procedure. Unfortunately, this is not the case for many theories of interest. We show in the next subsection that for a large class of theories, including the theory of equality, the computation of *mincard* is actually $\mathcal{NP}$-hard.[8]

6.2. The Theory of Equality

For any signature Σ, the Σ-theory of equality—the theory axiomatized by an empty set of Σ-sentences—is stably infinite and has a decidable quantifier-free satisfiability problem [16]. The decidability results in [16] also show that a quantifier-free formula φ is satisfiable in the theory if and only if it is satisfiable in a model of the theory with cardinality bounded above by the size of φ. Given that the theory is trivially universal, we have the following specialization of Proposition 23.

PROPOSITION 24. *For every finite signature Σ, the Σ-theory of equality is stably finite and has a computable mincard.*

[7] Which is the case for instance if Γ coincides with δ_{n+1}.

[8] This amends an incorrect result in [24] where we claimed that the complexity of *mincard* for the theory of equality is polynomial.

We point out that, for satisfiability purposes, the limitation to finite signatures is really immaterial. In fact, if one is interested in the satisfiability of a formula φ in the theory of equality, it is enough to consider the theory of equality over the (finitely-many) symbols of φ.

We now show that the theory of equality is also shiny.

PROPOSITION 25. *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:

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

– 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 20 it follows that $\mathcal{B}$ also satisfies φ. □

Combining Propositions 5 and 25, we obtain smoothness.

PROPOSITION 26. *For every signature Σ, the Σ-theory of equality is smooth.*

The shininess of the theory of equality then follows from Propositions 24 and 26.

PROPOSITION 27. *For every finite signature Σ, the Σ-theory of equality is shiny.*

Proposition 27 is relevant because, together with our second combination method,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[9] in addition to the symbols in Σ. More formally, we have the following theorem.

THEOREM 28. *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.*

The result in Theorem 28 was also independently discovered by Ganzinger and reported (without proof) in [7]. A new proof of the result that does not explicitly rely on the shininess of the theory of equality was recently given by Ganzinger, Sofronie-Stokkermans, and Waldmann [8].

6.2.1. *Complexity of mincard*

Although *mincard* is computable for the theory of equality, its computation is $\mathcal{NP}$-hard. We show that below by reducing the k-coloring problem to it.[10]

The k-coloring problem is defined as follows: Given a finite undirected graph G with nodes V and a positive integer k, is there a way to map each node in V to an integer in $\{1, \ldots, k\}$ so that no two adjacent nodes are mapped to the same integer? This problem is $\mathcal{NP}$-complete [9].

Now consider the *k-cardinality problem*, which we define as follows: Given a satisfiable set Γ of literals over the empty signature[11], and a positive integer k, does Γ have a model of cardinality k?

We start by showing that the k-coloring problem is polynomially reducible to the k-cardinality problem. Let $G = (V, E)$ be an undirected graph with nodes $V = \{v_1, \ldots v_n\}$ and edges E, and let k be a positive integer. Consider $v_1, \ldots v_n$ as logical variables and let

$$\Gamma = \{u \not\approx v \mid u, v \in V \text{ and } (u, v) \in E\}\,.$$

Note that Γ is satisfiable—by an interpretation that interprets each variable in V as a different element—and that the construction of Γ takes polynomial time in the size of G.

PROPOSITION 29. *The set Γ is satisfied by an interpretation of cardinality k if and only if G is k-colorable.*

[9] Also referred to as "uninterpreted" symbols by some authors.

[10] That the k-coloring problem was already used in [17] to find models of the theory of equality of "small" cardinality.

[11] In other words, Γ is a set of equalities and disequalities between variables.

Proof. Since Γ contains only disequalities between variables of V, we can consider in the following only Σ-interpretations over V where Σ is the empty signature.

First, assume that Γ is satisfied by a Σ-interpretation $\mathcal{A}$ of cardinality k. Let $A = \{a_1, \ldots, a_k\}$. Then we can map each variable $v \in \Sigma$ to i if $v^{\mathcal{A}} = a_i$. This way, we map V into $\{1, ..., k\}$ so that for all $(u \not\approx v) \in \Gamma$, u and v are mapped to different values. But then this map is precisely a k-coloring of G.

Vice versa, let $h : V \to \{1, \ldots, k\}$ be a k-coloring of G. We can define a Σ-interpretation $\mathcal{A}$ as follows: $A = \{1, \ldots, k\}$ and $v^{\mathcal{A}} = h(v)$ for all $v \in \Sigma$. By construction, $\mathcal{A}$ satisfies Γ. □

The proposition above implies that the k-cardinality problem is $\mathcal{NP}$-hard. A consequence of this fact is that the computation of *mincard* for the theory of equality *over the empty signature* is itself $\mathcal{NP}$-hard, as it corresponds to the "optimization version" of the k-cardinality problem—given a satisfiable set Γ of literals over the empty signature, determine the size of the smallest model of Γ.

PROPOSITION 30. *The computation of mincard for the theory of equality over the empty signature is $\mathcal{NP}$-hard.*

Proof. The k-cardinality problem can be reduced polynomially to the computation of *mincard* for the given theory as follows.

To see if a set Γ of literals over the empty signature is satisfied by an interpretation of cardinality k, we can compute $m = \mathit{mincard}(\Gamma)$ and then compare it with k. If $m \leq k$, by the smoothness of the theory of equality we know that Γ has a model of cardinality k. If $m > k$, by definition of *mincard*—and the fact that the theory has an empty axiomatization—we know that Γ has no models of cardinality k. □

The result above has far-reaching implications as it can be extended to the Σ-theory of equality for any signature Σ, and more generally, to *any* Σ-theory T with computable $\mathit{mincard}_T$ that admits models of arbitrary finite cardinality. The reason is that if T is such a theory, we can use $\mathit{mincard}_T$ to implement *mincard* for the theory of equality over the empty signature.

To see that, let Γ be a satisfiable set of literals over the empty signature. Because of the stable finiteness of the theory of equality, we can assume that Γ is satisfied by a finite interpretation $\mathcal{A}$, again over the empty signature. Since T admits models of any finite cardinality and $\mathcal{A}$'s signature is empty, it is easy to see that $\mathcal{A}$ is the reduct of some model of T. It follows that Γ is T-satisfiable and so $\mathit{mincard}_T$ is defined for it. Let then $m = \mathit{mincard}_T(\Gamma)$. We claim that $m =$

mincard(Γ) as well. In fact, assume by contradiction that Γ has a model $\mathcal{B}$ of cardinality less than m. Then, by the same argument as above, $\mathcal{B}$ is the reduct of some T-model of Γ. But then *mincard*(Γ) cannot be m. By Proposition 30 it follows that the computation of $mincard_T$ is $\mathcal{NP}$-hard.

6.3. BSR-THEORIES

In this subsection we show that a large class of theories are stably finite and have a computable *mincard* function. Among these theories we single out a couple that are also smooth. We call these theories *BSR-theories* after Bernays, Schönfinkel, and Ramsey, who studied some of their properties.

DEFINITION 31 (BSR-theories). *A sentence φ is a* BSR-SENTENCE *if it is of the form $(\exists x_1)\cdots(\exists x_m)(\forall y_1)\cdots(\forall y_n)\psi$, where $m, n \geq 0$ and ψ is a quantifier-free formula that does not contain function symbols.*

A BSR-THEORY *is a finite set of BSR-sentences.*

The following proposition was proved by Bernays and Schönfinkel [3] for the case of first-order logic without equality, and by Ramsey [18] for the case of first-order logic with equality.

PROPOSITION 32. *Let Φ a conjunction of BSR-sentences. Then there exists an integer k, bounded above by the size of Φ, such that Φ is satisfiable if and only if it has a model of cardinality k.*

A consequence of Proposition 32 is that the satisfiability of finite sets Φ of BSR-sentences is decidable: one simply Skolemizes Φ into a set Φ' and checks the satisfiability of Φ' in Herbrand interpretations.[12] Now, it is easy to see that Φ' will contain no function symbols, therefore all Herbrand interpretations over the signature of Φ' are finite. It is enough then to construct all such interpretations up to cardinality n where n is the size of Φ, until one is found that satisfies Φ'.

Proposition 32 is interesting because it entails that the quantifier-free satisfiability problem of any BSR-theory T is decidable. The reason is simply that a quantifier-free formula φ is T-satisfiable exactly when the finite set $T \cup \varphi'$ of BSR-sentences is satisfiable, where φ' is the existential closure of φ. From this observation it is clear that the following proposition holds.

PROPOSITION 33. *Every BSR-theory T is stably finite. Moreover, the quantifier-free satisfiability problem of T is decidable and $mincard_T$ is computable.*

[12] By the Herbrand theorem, looking at Herbrand interpretations only is enough because Φ' is universal.

From Proposition 33, we can immediately obtain the following specialization of Theorem 12.

COROLLARY 34. *Let S be a stably finite theory admitting only finite models and let T be any BSR-theory signature-disjoint with S. If the quantifier-free satisfiability problem of S is decidable and $\mathit{mincard}_S$ is computable, then the quantifier-free satisfiability problem of $S \cup T$ is also decidable.*

In general BSR-theories are not smooth, and so not shiny either. For instance, the theory

$$T = \{\ (\forall x)(\forall y)(x \approx y)\ \}$$

is a BSR-theory, but it is obviously not smooth because it only admits models of cardinality 1. Smooth BSR-theories however do exist. We provide two examples of them in the following.

Partial and total orders
Two smooth—and so also shiny— BSR-theories are the theories of partial and of total orders. The theory PO of partial orders is defined by the following axioms:

$$\begin{array}{ll} (\forall x)\neg(x < x) & \text{(irreflexivity)} \\ (\forall x)(\forall y)(\forall z)(x < y \ \wedge\ y < z \ \rightarrow\ x < z) & \text{(transitivity)}\,. \end{array}$$

The theory TO of total orders extends the theory of partial orders, with the following axiom

$$(\forall x)(\forall y)(x < y \ \vee\ x = y \ \vee\ y < x) \qquad \text{(trichotomy)}\,.$$

We prove that both PO and TO are smooth.

PROPOSITION 35. *Let $\Sigma = \{<\}$, let φ be a quantifier-free Σ-formula, let $\mathcal{A}$ be a finite PO-model of φ, and let $k = |A|$ be an integer. Then there exists a PO-model $\mathcal{B}$ of φ of cardinality $k+1$.*

Proof. 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 let

$$u^{\mathcal{B}} = u^{\mathcal{A}}\,, \qquad \text{for variables}\,,$$

and

$$a_1 <^{\mathcal{B}} a_2 \quad \Longleftrightarrow \quad a_1 <^{\mathcal{A}} a_2 \text{ and } a_1, a_2 \in A\,.$$

We have $|B| = k + 1$. Since $<^{\mathcal{B}}$ is clearly irreflexive and transitive by construction, $\mathcal{B}$ is a model of PO. 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 20 it follows that $\mathcal{B}$ satisfies φ as well. □

Combining Proposition 5 and 35 we obtain the smoothness of the theory of partial orders.

PROPOSITION 36. *The theory PO of partial orders is smooth.*

PROPOSITION 37. *Let $\Sigma = \{<\}$, let φ be a quantifier-free Σ-formula, let $\mathcal{A}$ be a finite TO-model of φ, and let $k = |A|$ be an integer. Then there exists a TO-model $\mathcal{B}$ of φ of cardinality $k + 1$.*

Proof. 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 let

$$u^{\mathcal{B}} = u^{\mathcal{A}}\,, \qquad \text{for variables}\,,$$

and

$$a_1 <^{\mathcal{B}} a_2 \quad \Longleftrightarrow \quad \left[\begin{array}{c} a_1 <^{\mathcal{A}} a_2 \text{ and } a_1, a_2 \in A \\ \text{or} \\ a_1 \neq b \text{ and } a_2 = b \end{array}\right]$$

Intuitively, we defined $<^{\mathcal{B}}$ exactly as $<^{\mathcal{A}}$, with the difference that the new element b becomes the new maximum element. It is immediate that $<^{\mathcal{B}}$ is a total order and so that $\mathcal{B}$ is a model of TO. We have that $|B| = k + 1$. 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 20 it follows that $\mathcal{B}$ satisfies φ as well. □

Combining Proposition 5 and 37 we obtain the smoothness of the theory of total orders.

PROPOSITION 38. *The theory TO of total orders is smooth.*

In conclusion, we have the following result.

PROPOSITION 39. *The theory TO of total orders and the theory PO partial orders are shiny.*

Proof. By Propositions 33, 36 and 38. □

From Proposition 39, we now obtain the following specialization of Theorem 18.

COROLLARY 40. *Where O is either TO or PO, let T be any theory signature-disjoint with O. If the quantifier-free satisfiability problem of T is decidable, then the quantifier-free satisfiability problem of $O \cup T$ is also decidable.*

6.4. The Theory of Lattices with Top and Bottom

We conclude the section with one more example of a shiny theory, the theory of lattices with top and bottom elements. In contrast with the theories considered so far, this theory has both a non-empty axiomatization and a signature with function symbols. Furthermore, although the theory can be axiomatized as an extension of the theory PO of partial orders, its shininess does not follow from the shininess of PO. As a matter of fact, it appears that the basic theory of lattices, with no top and bottom elements (and with no distributivity axioms), is not shiny.[13]

The theory LTB of lattices with top and bottom elements is the theory defined by the following axioms:

$$
\begin{array}{ll}
(\forall x)(x + x = x) & (\text{ cancelation for } +) \\
(\forall x)(x \cdot x = x) & (\text{ cancelation for } \cdot) \\
(\forall x)(\forall y)(x + y = y + x) & (\text{ commutativity of } +) \\
(\forall x)(\forall y)(x \cdot y = y \cdot x) & (\text{ commutativity of } \cdot) \\
(\forall x)(\forall y)(\forall z)(x + (y + z) = (x + y) + z) & (\text{ associativity of } +) \\
(\forall x)(\forall y)(\forall z)(x \cdot (y \cdot z) = (x \cdot y) \cdot z) & (\text{ associativity of } \cdot) \\
(\forall x)(x + 1 = 1 \ \wedge \ x \cdot 1 = x) & (\text{ maximum element } 1) \\
(\forall x)(x + 0 = x \ \wedge \ x \cdot 0 = 0) & (\text{ minimum element } 0) .
\end{array}
$$

The quantifier-free satisfiability problem of LTB is decidable. This can be shown, for instance, by adapting the decidability results in [4] about a theory of complete lattices with monotone functions. More precisely, the decision procedure given in [4] can be readily adapted to provide a decision procedure for the quantifier-free satisfiability problem of LTB. For any LTB-satisfiable conjunction of literals Γ given as input, this procedure essentially contructs a LTB-model of Γ of cardinality polynomial in the size of Γ (see [4] for details). From the correctness of the procedure (and the basic fact that a quantifier-free formula is satisfied by an interpretation $\mathcal{A}$ if one disjunct of its conjunctive normal form is satisfied by $\mathcal{A}$) it follows that LTB is stably finite. These observations are summarized in the following proposition.

[13] More accurately, our attempts to prove it shiny have failed so far.

PROPOSITION 41. *LTB is a stably finite universal theory with a decidable quantifier-free satisfiability problem.*

We now show that *LTB* is smooth.

PROPOSITION 42. *Let $\Sigma = \{+, \cdot, 0, 1\}$, let φ be a quantifier-free Σ-formula, let $\mathcal{A}$ be a finite LTB-model of φ, and let $k = |A|$ be an integer. Then there exists an LTB-model $\mathcal{B}$ of φ of cardinality $k + 1$.*

Proof. 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 let

$$u^{\mathcal{B}} = u^{\mathcal{A}}\,, \qquad \text{for variables and constants}\,,$$

$$b_1 +^{\mathcal{B}} b_2 \quad = \quad \begin{cases} b_1 +^{\mathcal{A}} b_2 & \text{if } b_1, b_2 \in A \\ 1 & \text{if } b_1 \neq b_2 \text{ and } b \in \{b_1, b_2\} \\ b & \text{if } b_1 = b_2 = b \end{cases}$$

and

$$b_1 \cdot^{\mathcal{B}} b_2 \quad = \quad \begin{cases} b_1 \cdot^{\mathcal{A}} b_2 & \text{if } b_1, b_2 \in A \\ 0 & \text{if } b_1 \neq b_2 \text{ and } b \in \{b_1, b_2\} \\ b & \text{if } b_1 = b_2 = b \end{cases}$$

Intuitively, if we take the usual view of a lattices as partial order where $x < y$ if $x \neq y \wedge x + y = y$, the new element b is one that is incomparable with all the old ones except that it is smaller than 1 and greater than 0. It is not difficult to see that both $+^{\mathcal{B}}$ and $\cdot^{\mathcal{B}}$ are well-defined and satisfy the axioms of *LTB*, making $\mathcal{B}$ a model of *LTB*. Moreover, 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 20 it follows that $\mathcal{B}$ satisfies φ as well. □

Combining Proposition 5 and 42 we obtain the smoothness of *LTB*.

PROPOSITION 43. *The theory LTB is smooth.*

Finally, observing that *LTB* is universal we have the following result.

PROPOSITION 44. *The theory LTB of lattices with top and bottom element is shiny.*

Proof. By Propositions 23, 41 and 43. □

From Proposition 44, we now obtain the following specialization of Theorem 18.

COROLLARY 45. *Let T be any theory signature-disjoint with LTB. If the quantifier-free satisfiability problem of T is decidable, then also the quantifier-free satisfiability problem of $LTB \cup T$ is decidable.*

7. Conclusion

We have addressed the problem of extending the Nelson-Oppen combination method to theories that are not stably infinite.

We provided two new combination methods that are based on the Nelson-Oppen method, but that can combine theories that may not be stably infinite. Our methods work by propagating equality constraints between the component decision procedures, as well as minimal cardinality constraints.

Using the first method, we are able to combine n stably finite theories $T_1, \ldots, T_n$ with a computable *mincard* function, provided that T_1 has only finite models.

Using our second method we are able to combine one arbitrary theory with n theories that are shiny. Recall that shininess is a stronger property than stable infiniteness. The significance of this result then is that we can completely forego the stable infiniteness requirement on one component theory if we can assume more (i.e., shininess) about the other ones.

Both methods require the computability of the *mincard* function for some or all of the component theories. We showed that for theories T that satisfy the other combination requirements, $mincard_T$ is often computable because the additional requirement on T that make $mincard_T$ computable are not very strong: it is enough for T to have a finite signature and be universal. We also showed however that when $mincard_T$ is computable its complexity is in general $\mathcal{NP}$-hard. In fact, we showed this to be the case for all theories T that have models of arbitrary finite cardinality.

We gave some examples of shiny theories, namely the theory of equality, the theory of partial orders, the theory of total orders, and the theories of lattices with top and bottom.

We plan to continue our research on relaxing the stable infiniteness requirement by aiming at finding general sufficient conditions for shininess, and identifying additional specific examples of shiny theories. Moreover, due to the complexity of *mincard*, it would be natural to study how to avoid its computation.

Acknowledgments

We are grateful to the anonymous reviewers for their detailed and helpful comments. We are also grateful to David Dill and Kasturi Varadarajan who independently pointed out to us the relationship between the k-coloring and the k-cardinality problem.

References

1. Franz Baader and Cesare Tinelli. A new approach for combining decision procedure for the word problem, and its connection to the Nelson-Oppen combination method. In William McCune, editor, *Automated Deduction – CADE-14*, volume 1249 of *Lecture Notes in Computer Science*, pages 19–33. Springer, 1997.
2. Clark W. Barrett, David L. Dill, and Aaron Stump. A generalization of Shostak's method for combining decision procedures. In Alessandro Armando, editor, *Frontiers of Combining Systems*, volume 2309 of *Lecture Notes in Computer Science*, pages 132–146. Springer, 2002.
3. Paul Bernays and Moses Schönfinkel. Zum Entscheidungsproblem der mathematischen Logic. *Mathematische Annalen*, 99:342–372, 1928.
4. Domenico Cantone and Calogero G. Zarba. A decision procedure for monotone functions over lattices. In Francesco Buccafurri, editor, *Joint Conference on Declarative Programming APPIA-GULP-PRODE*, pages 1–12, 2003.
5. Dan Craigen, Sentot Kromodimoeljo, Irwin Meisels, Bill Pase, and Mark Saaltink. EVES: An overview. In Soren Prehen and Hans Toetenel, editors, *Formal Software Development Methods*, volume 552 of *Lecture Notes in Computer Science*, pages 389–405. Springer, 1991.
6. David Detlefs, Greg Nelson, and James B. Saxe. Simplify: A theorem prover for program checking. Technical Report HPL-2–3-148, HP Laboratories, Palo Alto, CA, 2003.
7. Harald Ganzinger. Shostak light. In Andrei Voronkov, editor, *Automated Deduction – CADE-18*, volume 2392 of *Lecture Notes in Computer Science*, pages 332–346. Springer, 2002.
8. Harald Ganzinger, Viorica Sofronie-Stokkermans, and Uwe Waldmann. Modular proof systems for partial functions with weak equality. In David Basin and Michaël Rusinowitch, editors, *Automated Reasoning*, volume 3097 of *Lecture Notes in Computer Science*, pages 168–182. Springer, 2004.
9. Michael R. Garey and David S. Johnson. *Computers and Intractability.* W. H. Freeman & Co., 1979.
10. Silvio Ghilardi. Quantifier elimination and provers integration. In Ingo Dahn and Laurent Vigneron, editors, *First Order Theorem Proving*, volume 86.1 of *Electronic Notes in Theoretical Computer Science*. Elsevier, 2003.
11. Wilfrid Hodges. *A Shorter Model Theory.* Cambridge University Press, 1997.
12. Beth Levy, Ivan Filippenko, Leo Marcus, and Telis Menas. Using the state delta verification system (SDVS) for hardware verification. In Tom F. Melham, V. Stavridou, and Raymond T. Boute, editors, *Theorem Prover in Circuit Design: Theory, Practice and Experience*, pages 337–360. Elsevier Science, 1992.

13. Zohar Manna and Calogero G. Zarba. Combining decision procedures. In *Formal Methods at the Cross Roads: From Panacea to Foundational Support*, volume 2757 of *Lecture Notes in Computer Science*, pages 381–422. Springer, 2003.
14. Greg Nelson. Techniques for program verification. Technical Report CSL-81-10, Xerox Palo Alto Research Center, 1981.
15. Greg Nelson and Derek C. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1(2):245–257, 1979.
16. Derek C. Oppen. Complexity, convexity and combination of theories. *Theoretical Computer Science*, 12:291–302, 1980.
17. Amir Pnueli, Yoav Rodeh, Ofer Strichman, and Michael Siegel. Deciding equality formulas by small domains instantiations. In Nicolas Halbwachs and Doron Peled, editors, *Computer Aided Verification*, volume 1633 of *Lecture Notes in Computer Science*, pages 455–469. Springer, 1999.
18. Frank P. Ramsey. On a problem in formal logic. *Proceedings of the London Mathematical Society*, 30:264–286, 1930.
19. Christophe Ringeissen. Cooperation of decision procedures for the satisfiability problem. In Franz Baader and Klaus U. Schulz, editors, *Frontiers of Combining Systems*, volume 3 of *Applied Logic Series*, pages 121–140. Kluwer Academic Publishers, 1996.
20. Aaron Stump, Clark W. Barret, and David L. Dill. CVC: A cooperating validity checker. In Ed Brinksma and Kim Guldstrand Larsen, editors, *Computer Aided Verification*, volume 2404 of *Lecture Notes in Computer Science*, pages 500–504, 2002.
21. Cesare Tinelli. Cooperation of background reasoners in theory reasoning by residue sharing. *Journal of Automated Reasoning*, 30(1):1–31, 2003.
22. Cesare Tinelli and Mehdi T. Harandi. A new correctness proof of the Nelson-Oppen combination procedure. In Franz Baader and Klaus U. Schulz, editors, *Frontiers of Combining Systems*, volume 3 of *Applied Logic Series*, pages 103–120. Kluwer Academic Publishers, 1996.
23. Cesare Tinelli and Christophe Ringeissen. Unions of non-disjoint theories and combinations of satisfiability procedures. *Theoretical Computer Science*, 290(1):291–353, 2003.
24. Cesare Tinelli and Calogero G. Zarba. Combining non-stably infinite theories. In Ingo Dahn and Laurent Vigneron, editors, *First Order Theorem Proving*, volume 86.1 of *Electronic Notes in Theoretical Computer Science*. Elsevier, 2003.
25. Calogero G. Zarba. Combining lists with integers. In Rajeev Goré, Alexander Leitsch, and Tobias Nipkow, editors, *Automated Reasoning: Short Papers*, Technical Report DII 11/01, pages 170–179. Università di Siena, Italy, 2001.
26. Calogero G. Zarba. Combining multisets with integers. In Andrei Voronkov, editor, *Automated Deduction – CADE-18*, volume 2392 of *Lecture Notes in Computer Science*, pages 363–376. Springer, 2002.
27. Calogero G. Zarba. Combining sets with integers. In Alessandro Armando, editor, *Frontiers of Combining Systems*, volume 2309 of *Lecture Notes in Computer Science*, pages 103–116. Springer, 2002.
28. Calogero G. Zarba. C-tableaux. Technical Report RR-5229, INRIA, 2004.
29. Calogero G. Zarba. *The Combination Problem in Automated Reasoning*. PhD thesis, Stanford University, 2004.

Appendix

A. The Combination Theorem

In this appendix, we prove the Generalized Combination Theorem for Disjoint Signatures (Theorem 7).

We will use the following Combination Theorem, a fundamental model-theoretic result originally due to Ringeissen [19] and Tinelli and Harandi [22] independently, and later refined by Tinelli and Ringeissen [23] and Manna and Zarba [13].

THEOREM 46 (Combination). *Let Σ_1 and Σ_2 be arbitrary signatures, let Φ_i be a set of arbitrary Σ_i-formulae, for $i = 1, 2$, and let $V_i = vars(\Phi_i)$. Then $\Phi_1 \cup \Phi_2$ is satisfiable if and only if there exists a Σ_1-interpretation $\mathcal{A}$ satisfying Φ_1 and a Σ_2-interpretation $\mathcal{B}$ satisfying Φ_2 such that*

$$\mathcal{A}^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2} \cong \mathcal{B}^{\Sigma_1 \cap \Sigma_2, V_1 \cap V_2}\,.$$

Proof. See either [13] or [29]. □

THEOREM 47 (Generalized Combination). *Let $\Sigma_1, \ldots, \Sigma_n$ be $n > 1$ arbitrary signatures and let $\Phi = \Phi_1 \cup \cdots \cup \Phi_n$, where Φ_i is a set of Σ_i-formulae, for $i = 1, \ldots, n$. Also, let $V_i = vars(\Phi_i)$, $V = \bigcup_{i \neq j}(V_i \cap V_j)$, and $\Sigma = \bigcup_{i \neq j}(\Sigma_i \cap \Sigma_j)$. Assume that*

$$\bigcup_{i \neq j} (\Sigma_i \cap \Sigma_j) = \bigcap_i \Sigma_i\,,$$

and

$$\bigcup_{i \neq j} (V_i \cap V_j) = \bigcap_i V_i\,.$$

Then Φ is satisfiable if and only if there exist interpretations $\mathcal{A}_1, \ldots, \mathcal{A}_n$ such that:

(i) $\mathcal{A}_i$ satisfies Φ_i, for $i = 1, \ldots, n$;

(ii) $\mathcal{A}_i^{\Sigma,V} \cong \mathcal{A}_j^{\Sigma,V}$, for each i, j.

Proof. Assume that Φ is satisfiable, and let $\mathcal{F}$ be any interpretation satisfying Φ. Then the only-if direction holds if we let $\mathcal{A}_i = \mathcal{F}^{\Sigma_i, V_i}$, for $i = 1, \ldots, n$.

Vice versa, suppose that there exist interpretations $\mathcal{A}_1, \ldots, \mathcal{A}_n$ such that (i) and (ii) hold. For $k = 2, \ldots, n$, let $\Omega_k = \Sigma_1 \cup \cdots \cup \Sigma_k$ and $U_k = V_1 \cup \cdots \cup V_k$. We claim that, for $k = 2, \ldots, n$, $\Phi_1 \cup \cdots \cup \Phi_k$ is satisfied by an Ω_k-interpretation $\mathcal{F}_k$ over U_k such that $\mathcal{F}_k^{\Sigma,V} = \mathcal{A}_1^{\Sigma,V}$.

We proceed by induction on k. The base case, $k = 2$, follows immediately by (the proof of) Theorem 46.

For the induction step, assume that $\Phi_1 \cup \cdots \cup \Phi_k$ is satisfied by an interpretation $\mathcal{F}_k$ such that $\mathcal{F}_k^{\Sigma,V} = \mathcal{A}_1^{\Sigma,V}$. Observing that $\Omega_k \cap \Sigma_{k+1} = \Sigma$, $U_k \cap V_{k+1} = V$, and $\mathcal{A}_1^{\Sigma,V} \cong \mathcal{A}_{k+1}^{\Sigma,V}$, we then have that $\mathcal{F}_k^{\Sigma_F \cap \Sigma_{k+1}} \cong \mathcal{A}_{k+1}^{\Sigma_F \cap \Sigma_{k+1}}$. Therefore, we can apply (the proof of) Theorem 46, and obtain an interpretation $\mathcal{F}_{k+1}$ satisfying $\Phi_1 \cup \cdots \cup \Phi_k \cup \Phi_{k+1}$ such that $\mathcal{F}_{k+1}^{\Sigma,V} \cong \mathcal{A}_1^{\Sigma,V}$. □

THEOREM 7 (Generalized Combination for Disjoint Signatures). *Let $\Phi = \Phi_1 \cup \cdots \cup \Phi_n$, where Φ_i is a set of Σ_i-formulae, for $i = 1, \ldots, n$. Also, let $V_i = vars(\Phi_i)$ and $V = \bigcup_{i \neq j} (V_i \cap V_j)$. Assume that all the signatures $\Sigma_1, \ldots, \Sigma_n$ are pairwise disjoint, and that*

$$\bigcup_{i \neq j} (V_i \cap V_j) = \bigcap_i V_i \,.$$

Then Φ is satisfiable if and only if there exist interpretations $\mathcal{A}_1, \ldots, \mathcal{A}_n$ such that:

(i) $\mathcal{A}_i$ satisfies Φ_i, for $i = 1, \ldots, n$;

(ii) $|A_1| = |A_2| = \cdots = |A_n|$;

(iii) $x^{\mathcal{A}_i} = y^{\mathcal{A}_i}$ if and only if $x^{\mathcal{A}_j} = y^{\mathcal{A}_j}$, for all i, j and for every $x, y \in V$.

Proof. Assume that Φ is satisfiable, and let $\mathcal{F}$ be any interpretation satisfying Φ. Then the only-if direction holds if we let $\mathcal{A}_i = \mathcal{F}^{\Sigma_i, V_i}$, for $i = 1, \ldots, n$.

Vice versa, suppose that there exist interpretations $\mathcal{A}_1, \ldots, \mathcal{A}_n$ such that (i) and (ii) hold. We can construct an isomorphism h of $\mathcal{A}_i^V$ into $\mathcal{A}_j^V$, for each i, j by using the following process.

First, let $h(x^{\mathcal{A}_i}) = x^{\mathcal{A}_j}$, for every $x \in V$. Note that this position is sound because property (ii) holds. Moreover, we have that h is bijective.

Since h is a bijective function, we have $|V^{\mathcal{A}_i}| = |V^{\mathcal{A}_j}|$, and since $|A_i| = |A_j|$, we also have that $|A_i \setminus V^{\mathcal{A}_i}| = |A_j \setminus V^{\mathcal{A}_j}|$. We can therefore extend h to a bijective function h' from A_i to A_j.

Clearly, by construction h' is an isomorphism of ${\mathcal{A}_i}^V$ into ${\mathcal{A}_j}^V$. Thus, we can apply Theorem 47, and obtain the existence of an interpretation $\mathcal{F}$ satisfying $\Phi_1 \cup \cdots \cup \Phi_n$. □