Combining Theories Sharing Dense Orders*

Calogero G. Zarba, Zohar Manna, and Henny B. Sipma

Department of Computer Science, Stanford University
Gates Building, Stanford, CA 94305, USA
e-mail: {zarba, zm, sipma}@theory.stanford.edu

Abstract. The Nelson-Oppen combination method combines decision procedures for first-order theories satisfying certain conditions into a single decision procedure for the union theory. The Nelson-Oppen combination method can be applied only if the signatures of the combined theories are disjoint.
Combination tableaux (C-tableaux) are an extension of Smullyan tableaux for combining first-order theories whose signatures may not be disjoint. C-tableaux are sound and complete, but not terminating in general.
In this paper we show that, when we combine first-order theories that share the theory of dense order, C-tableaux can be made terminating without sacrificing completeness. Thus, C-tableaux provide a decision procedure for the combination of first-order theories sharing the theory of dense order.

1 Introduction

In 1979, Nelson and Oppen [7] invented what is still considered to be the state-of-the-art method for combining decision procedures. Given two theories T_1, T_2 satisfying certain conditions, the Nelson-Oppen method combines the available decision procedures for T_1 and T_2 into a decision procedure for the combined theory $T_1 \cup T_2$.

In order to be applicable, the Nelson-Oppen method requires that the signatures of the theories T_1 and T_2 are disjoint. This disjointness requirement has revealed very hard to lift, as witnessed by the fact that, more than two decades after Nelson and Oppen's seminal paper was published, non-disjoint combination research is still in its infancy.

Recently, Zarba [15, 16] invented a general method for combining theories over disjoint signatures. His method is based on *Combination tableaux* (C-tableaux), an extension of Smullyan tableaux that generalizes the Nelson-Oppen method to the combination of theories whose signatures may not be disjoint.

C-tableaux are sound and complete with respect to unsatisfiability in the combined theory. Soundness means that if there exists a C-tableau proof that a formula is unsatisfiable, then the formula is indeed unsatisfiable. Completeness

* This research was supported in part by NSF grants CCR-01-21403, CCR-02-20134 and CCR-02-09237, by ARO grant DAAD19-01-1-0723, and by ARPA/AF contracts F33615-00-C-1693 and F33615-99-C-3014.

means that if a formula is unsatisfiable, then there exists a C-tableau proof that demonstrates the unsatisfiability.

In general, C-tableaux are not terminating. In other words, a procedure based on C-tableaux may run forever if it receives as input a formula that is satisfiable in the combined theory.

In this paper we address the problem of making C-tableaux terminating. The idea is to find suitable restrictions to the tableau rules that enforce termination without sacrificing completeness. We show that this is possible when one combines theories that share the dense orders.

The theory of dense order models a predicate symbol $<$ as a linear order that is dense in the following sense: For every two elements x, y, if $x < y$ then there exists an element z between x and y, that is, $x < z$ and $z < y$. Examples of domains that are densely ordered include the set of rational numbers and the set of real numbers.

We show that if T_1 and T_2 are theories that properly extend the theory of dense order, and whose signatures share only the predicate symbol $<$, then C-tableaux can be made terminating, and therefore they provide a decision procedure for the combined theory $T_1 \cup T_2$.

Related work. Related results on non-disjoint combination exist in term rewriting for rewriting systems sharing constructors [3, 8], in unification for equational theories sharing either constant symbols [9] or constructors [1, 2], and in constraint satisfiability for theories sharing constructors [10, 14].

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 the Nelson-Oppen combination method, and in Section 4 we describe C-tableaux. In Section 5 we show how C-tableaux can be made terminating when combining theories sharing the dense orders. Finally, in Section 6 we draw conclusions from our work.

2 Preliminaries

2.1 Syntax

A *signature* Σ consists of a set Σ^{C} of constants, a set Σ^{F} of function symbols, and a set Σ^{P} of predicate symbols.

Given a set V of variables, we denote with $\mathit{Terms}(\Sigma, V)$ the set of terms built from the variables in V and the symbols in Σ. An element of $\mathit{Terms}(\Sigma, V)$ is a *Σ-term*. $\mathit{Terms}(\Sigma)$ stands for $\mathit{Terms}(\Sigma, \emptyset)$.

A *Σ-atom* is either 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 $s = t$, where $=$ 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 t is a term, $vars(t)$ denotes the set of variables occurring in t. If φ is a formula, $vars(\varphi)$ denotes the set of free variables occurring in φ. If Φ is a set of terms or a set of formulae, $vars(\Phi) = \bigcup_{\varphi \in \Phi} vars(\varphi)$.

For convenience, we identify conjunction of formulae $\varphi_1 \wedge \cdots \wedge \varphi_n$ with the set $\{\varphi_1, \ldots, \varphi_n\}$, and we abbreviate the literal $\neg(x = y)$ with $x \neq y$.

2.2 Semantics

Definition 1. Let Σ be a signature. A Σ-INTERPRETATION $\mathcal{A}$ with domain A over a set V of variables is a map which interprets each variable $x \in V$ 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 $f^{\mathcal{A}} : A^n \rightarrow A$, and 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 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 *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 Σ-formula φ over a set V of variables is:

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

Let Ω be a signature, and let $\mathcal{A}$ be an Ω-interpretation over some set U of variables. For a subset Σ of Ω and a subset V of U, we denote with $\mathcal{A}^{\Sigma,V}$ the Σ-interpretation obtained by restricting $\mathcal{A}$ to interpret only the symbols in Σ and the variables in V. In particular, $\mathcal{A}^{\Sigma}$ stands for $\mathcal{A}^{\Sigma,\emptyset}$.

Definition 2. Let Σ be a signature, and let $\mathcal{A}$ and $\mathcal{B}$ be Σ-interpretations over some set V of variables. A map $h : A \rightarrow B$ is an ISOMORPHISM of $\mathcal{A}$ into $\mathcal{B}$ if the following conditions hold:

- h is bijective;
- $h(u^{\mathcal{A}}) = u^{\mathcal{B}}$ 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 write $\mathcal{A} \cong \mathcal{B}$ to indicate that there exists an isomorphism of $\mathcal{A}$ into $\mathcal{B}$.

2.3 Theories

Definition 3. Let Σ be 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 Σ-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-models over V;
- *T-unsatisfiable*, if it is not T-satisfiable.

Given a Σ-theory T, the *satisfiability problem* of T is the problem of deciding, for each Σ-formula φ, whether or not φ is T-satisfiable. Similarly, the *quantifier-free satisfiability problem* of T is the problem of deciding, for each quantifier-free Σ-formula φ, whether or not φ is T-satisfiable.

Definition 4. A theory is UNIVERSAL if all its sentences are of the form $(\forall *)\varphi$, where φ is quantifier-free. □

Definition 5. A Σ-theory T is STABLY INFINITE if every quantifier-free Σ-formula φ is T-satisfiable if and only if it is satisfied by a T-model $\mathcal{A}$ whose domain A is infinite. □

Examples of stably infinite theories include the theory of equality,[1] the theory of integers, the theory of reals, the theory of lists, the theory of arrays, and the theory of sets.

2.4 Dense orders

Let $\Sigma_{\mathbb{O}}$ be the signature containing the binary predicate symbol $<$ (*less than*). The theory $T_{\mathbb{O}}$ of dense order (without endpoints) is defined by the following $\Sigma_{\mathbb{O}}$-sentences:

$(\forall x)\neg[x < x]$	(irreflexivity)
$(\forall x)(\forall y)(\forall z)[x < y \ \wedge \ y < z \ \rightarrow \ x < z]$	(transitivity)
$(\forall x)(\forall y)[x < y \ \vee \ x = y \ \vee \ y < x]$	(trichotomy)
$(\forall x)(\forall y)[x < y \ \rightarrow \ (\exists z)[x < z \ \wedge \ z < y]]$	(density)
$(\forall x)(\exists y)[y < x]$	(no first element)
$(\forall x)(\exists y)[x < y]$	(no last element).

The satisfiability problems of $T_{\mathbb{O}}$ is decidable, a result proved by Langford [6].

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

2.5 The theory $T_{\mathbb{R}}$ of reals

An example of a domain that satisfies the theory of dense order is the domain of real numbers. More precisely, let $\Sigma_{\mathbb{R}}$ be the signature containing a constant symbol c_r, for each rational number $r \in \mathbb{Q}$, a binary function symbol $+$ (*addition*), a unary function symbol $-$ (*minus*), a binary function symbol $\times$ (*multiplication*) and a binary predicate symbol $<$ (*less than*). The theory $T_{\mathbb{R}}$ of the reals is the set of all $\Sigma_{\mathbb{R}}$-sentences that are true in the standard interpretation $\mathcal{A}$ of the reals. This interpretation has domain $A = \mathbb{R}$, and interprets the symbols in $\Sigma_{\mathbb{R}}$ according to their standard meaning over $\mathbb{R}$.

Clearly, the theory of reals properly extends the theory of dense order, that is, $T_{\mathbb{Q}} \subset T_{\mathbb{R}}$. It follows that for every formula φ, if φ is $T_{\mathbb{Q}}$-valid then φ is also $T_{\mathbb{R}}$-valid.

The satisfiability problem of $T_{\mathbb{R}}$ is decidable, a result proved by Tarski [12].

3 Nelson-Oppen

Let Σ_1 and Σ_2 be signatures, and let T_i be a Σ_i-theory, for $i = 1, 2$. Assume that there exist decision procedures P_1 and P_2 such that, for $i = 1, 2$, P_i can decide the quantifier-free satisfiability problem of T_i. The Nelson-Oppen combination method uses P_1 and P_2 as black boxes in order to decide the $(T_1 \cup T_2)$-satisfiability of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae.

Provided that $\Sigma_1 \cap \Sigma_2 = \emptyset$, and that T_1 and T_2 are stably infinite, the Nelson-Oppen combination method provides a decision procedure for the quantifier-free satisfiability problem of $T_1 \cup T_2$.

We now describe the Nelson-Oppen combination method. Without loss of generality, we restrict ourselves to conjunctions of literals. Note that this can always be done because every quantifier-free 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.

Thus, let Γ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. The Nelson-Oppen method consists of two phases: *variable abstraction* and *check*.

In the variable abstraction phase we convert Γ into a conjunction $\Gamma_1 \cup \Gamma_2$ satisfying the following properties:

(a) each literal in Γ_i is a Σ_i-literal, for $i = 1, 2$;
(b) $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable if and only if so is Γ.

Note that all properties can be effectively enforced with the help of new auxiliary variables.

We call $\Gamma_1 \cup \Gamma_2$ a conjunction of literals in *separate* form. Moreover, we denote with $\mathit{shared}(\Gamma_1, \Gamma_2)$ the set of variables occurring in both Γ_1 and Γ_2, that is, $\mathit{shared}(\Gamma_1, \Gamma_2) = \mathit{vars}(\Gamma_1) \cap \mathit{vars}(\Gamma_2)$.

In order to describe the check phase, we introduce the notion of *arrangement*.

Definition 6. Let E be an equivalence relation over some set V of variables. The *arrangement* of V induced by E is defined as the conjunction:

$$\begin{aligned} arr(V,E) = \{x = y \mid x,y \in V \text{ and } (x,y) \in E\} \cup \\ \{x \neq y \mid x,y \in V \text{ and } (x,y) \notin E\}\,. \end{aligned}$$

□

Let $\Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form, and let $V = \mathit{shared}(\Gamma_1, \Gamma_2)$. In the check phase we perform the following two steps, for each equivalence relation E of V:

Step 1. If $\Gamma_1 \cup \mathit{arr}(V,E)$ is T_1-satisfiable go to the next step; otherwise output `fail`;

Step 2. If $\Gamma_2 \cup \mathit{arr}(V,E)$ is T_2-satisfiable output `succeed`; otherwise output `fail`.

If there exists an equivalence relation E of V for which we output `succeed` then we declare that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable. If instead we output `fail` for each equivalence relation E of V then we declare that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-unsatisfiable.

Provided that the signatures Σ_1 and Σ_2 are disjoint, and that the theories T_1 and T_2 are stably infinite, then the Nelson-Oppen method just described is correct. The following theorem summarizes this result.

Theorem 7. *Let T_i be a stably infinite Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \emptyset$. Also, assume that the quantifier-free T_i-satisfiability problem is decidable. Then the Nelson-Oppen combination method provides a decision procedure for the quantifier-free satisfiability problem of $T_1 \cup T_2$.* □

3.1 An example in which all goes well

Let $T_{\mathbb{R}}$ be the theory of reals, let $\Sigma_f = \{f\}$, where f is a unary function symbol, and let T_f be the theory of equality over the signature Σ_f.

Since $\Sigma_{\mathbb{R}} \cap \Sigma_f = \emptyset$, and since both $T_{\mathbb{R}}$ and T_f are stably infinite, Theorem 7 tells us that the Nelson-Oppen method is able to correctly combine $T_{\mathbb{R}}$ and T_f.

Consider the conjunction

$$\Gamma = \left\{ \begin{array}{l} x + y = z\,, \\ f(x) \neq f(y) \end{array} \right\}.$$

We have that Γ is $(T_{\mathbb{R}} \cup T_f)$-satisfiable: A $(T_{\mathbb{R}} \cup T_f)$-model $\mathcal{A}$ of Γ can be obtained by letting $A = \mathbb{R}$, $x^{\mathcal{A}} = 1$, $y^{\mathcal{A}} = 2$, $z^{\mathcal{A}} = 3$, and $f^{\mathcal{A}}(a) = a$, for each $a \in \mathbb{R}$.

Let us apply the Nelson-Oppen combination method to Γ. In the variable abstraction phase we do not need to introduce new variables, and we simply return the conjunctions

$$\Gamma_{\mathbb{R}} = \{x + y = z\}\,, \qquad \Gamma_f = \{f(x) \neq f(y)\}\,.$$

Since $\mathit{shared}(\Gamma_{\mathbb{R}}, \Gamma_f) = \{x, y\}$, there are only two equivalence relations to examine: either $(x,y) \in E$ or $(x,y) \notin E$. In the former case $\Gamma_f \cup \{x = y\}$ is

T_f-unsatisfiable. However, in the latter case we have that $\Gamma_{\mathbb{R}} \cup \{x \neq y\}$ is $T_{\mathbb{R}}$-satisfiable and that $\Gamma_f \cup \{x \neq y\}$ is T_f-satisfiable. Thus, we correctly conclude that Γ is $(T_{\mathbb{R}} \cup T_f)$-satisfiable.

3.2 An example in which something goes wrong

Let $T_{\mathbb{R}}$ be the theory of reals, let $\Sigma_{\mathbb{M}} = \{f, <\}$, and let $T_{\mathbb{M}}$ be the theory defined by

$$T_{\mathbb{M}} = T_{\mathbb{O}} \ \cup \ \{ \ (\forall x)(\forall y)[x < y \ \rightarrow \ f(x) < f(y)] \ \} \, ,$$

where $T_{\mathbb{O}}$ is the theory of dense order. Intuitively, $T_{\mathbb{M}}$ models f as a monotone increasing function with respect to the dense order $<$.

Since $\Sigma_{\mathbb{R}} \cap \Sigma_{\mathbb{M}} = \{<\}$, the Nelson-Oppen combination method cannot be applied in order to combine $T_{\mathbb{R}}$ in $T_{\mathbb{M}}$. As an example of what can go wrong, consider the conjunction

$$\Gamma = \left\{ \begin{array}{c} u < v \, , \\ u = x + 1 \, , \\ v = y + 1 \, , \\ \neg(f(x) < f(y)) \end{array} \right\} .$$

We have that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-unsatisfiable. In particular, the unsatisfiability is caused by the shared predicate symbol $<$. In fact, the first three literals imply $x < y$, whereas the last literal implies $\neg(x < y)$.

However, the Nelson-Oppen method is unable to detect the unsatisfiability. To see this, let us apply the method to Γ. In the variable abstraction phase, we obtain the conjunctions

$$\Gamma_{\mathbb{R}} = \left\{ \begin{array}{l} u < v \, , \\ u = x + 1 \, , \\ v = y + 1 \end{array} \right\} , \qquad \Gamma_{\mathbb{M}} = \left\{ \begin{array}{l} u < v \, , \\ \neg(f(x) < f(y)) \end{array} \right\} .$$

Let $V = \mathit{shared}(\Gamma_{\mathbb{R}}, \Gamma_{\mathbb{M}}) = \{x, y, u, v\}$. For the check phase, consider the equivalence relation E induced by the partition $\{\{x\}, \{y\}, \{u\}, \{v\}\}$. In other words, E models all variables in V as different. We have that both $\Gamma_{\mathbb{R}} \cup \mathit{arr}(V, E)$ is $T_{\mathbb{R}}$-satisfiable and that $\Gamma_{\mathbb{M}} \cup \mathit{arr}(V, E)$ is $T_{\mathbb{M}}$-satisfiable. Thus, the Nelson-Oppen method *incorrectly* concludes that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-satisfiable.

The Nelson-Oppen combination method is unable to detect the unsatisfiability because it does not take into account the shared predicate symbol $<$. We will see in the next section that, by using C-tableaux, we are able to detect the unsatisfiability.

4 Combination tableaux

In this section we describe *Combination tableaux* (C-tableaux), an extension of Smullyan tableaux for combining theories whose signatures may not be disjoint [15, 16].

Let Σ_1 and Σ_2 be arbitrary signatures (that is, not necessarily disjoint), and let T_i be a Σ_i-theory, for $i = 1, 2$. Also, assume that there exist decision procedures P_1 and P_2 such that, for $i = 1, 2$, P_i can decide the quantifier-free satisfiability problem of T_i. Using P_1 and P_2 as black boxes, C-tableaux provide a method for checking the $(T_1 \cup T_2)$-satisfiability of $(\Sigma_1 \cup \Sigma_2)$-formulae.

Zarba [16] proved that if the theories T_1 and T_2 are universal then C-tableaux are sound and complete for the $(T_1 \cup T_2)$-*un*satisfiability of any $(\Sigma_1 \cup \Sigma_2)$-formula φ.[2] Unfortunately, in this paper we are interested in the theory of dense order, which is not universal. Nevertheless, in Section 5 we will prove that C-tableaux remain sound and complete when combining theories sharing the dense orders.

Since in this paper we do not address quantifiers, we will describe a version of C-tableaux that deals only with quantifier-free formulae. Thus, we can conveniently restrict ourselves to conjunctions of literals. Moreover, by using the variable abstraction phase of the Nelson-Oppen combination method, we can further restrict ourselves to conjunctions of literals in separate form.

Definition 8 (C-tableaux). Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form. An INITIAL C-TABLEAU for Γ is a tree consisting of one branch whose nodes are labeled with the literals in Γ. A C-TABLEAU for Γ is either an initial C-tableau for Γ or is obtained by applying the rules in Figure 1 to an initial C-tableau for Γ. □

The intuition behind the rules in Figure 1 is as follows. The *closure rule* is used in order to detect inconsistencies. The *decomposition rule* is used to let the decision procedures for T_1 and T_2 "agree" on the truth-value of every atom.

The intuition behind the *abstraction rule* is more complex. Suppose that t is a Σ_1-term but not a Σ_2-term. Then the decision procedure for T_1 "knows" about t, but the decision procedure for T_2 does not. After an application of the abstraction rule, the decision procedure for T_2 is aware of the existence of t.

We now define when a C-tableau is closed.

Definition 9. Let B be a branch of a C-tableau T. We say that B is CLOSED if it contains the literal *false*. A branch which is not closed is OPEN. A C-tableau is CLOSED if so are all its branches; otherwise it is OPEN. □

C-tableaux are sound, as stated by the following theorem.

Theorem 10 (Soundness [16]). *Let Γ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. If there exists a closed C-tableau for φ then Γ is $(T_1 \cup T_2)$-unsatisfiable.* □

Under the assumption that T_1 and T_2 are universal, C-tableaux are also complete.

Theorem 11 (Completeness [16]). *Let T_1 and T_2 be universal theories, and let Γ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. If Γ is $(T_1 \cup T_2)$-unsatisfiable then Γ has a closed C-tableau.* □

[2] We need the hypothesis that T_1 and T_2 are universal because the completeness proof relies on the Herbrand Theorem.

Abstraction rule

$$\frac{}{t = w}$$

Where t is either a Σ_1-term or a Σ_2-term, and w is a newly generated variable.

Decomposition rules

$$\frac{}{x = y \mid x \neq y} \qquad \frac{}{P(x_1, \ldots, x_n) \mid \neg P(x_1, \ldots, x_n)}$$

Where $x, y, x_1, \ldots, x_n$ are variables already occurring in the branch and $P \in \Sigma_1^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}}$.

Closure rule

$$\frac{\begin{array}{c}\ell_1 \\ \vdots \\ \ell_n\end{array}}{\mathit{false}}$$

Provided that there exists an index $i \in \{1, 2\}$ such that $\ell_1, \ldots, \ell_n$ are Σ_i-literals and $\{\ell_1, \ldots, \ell_n\}$ is T_i-unsatisfiable.

Figure 1: C-tableau rules.

In general, C-tableaux are not terminating. Nontermination is caused by the abstraction rule, which requires that we add a literal of the form $t = w$, for each $(\Sigma_1 \cup \Sigma_2)$-term t. Clearly, when $\Sigma_1^{\mathrm{F}} \cup \Sigma_2^{\mathrm{F}} \neq \emptyset$, there is an infinite number of such terms.[3]

Although in general C-tableaux are not terminating, in Section 5 we will show that, when we combine theories sharing the dense orders, C-tableaux can be made terminating without sacrificing completeness.

4.1 An example

Let $T_{\mathbb{R}}$ be the theory of reals, let $\Sigma_{\mathbb{M}} = \{f, <\}$, and let $T_{\mathbb{M}}$ be the theory defined by

$$T_{\mathbb{M}} = T_{\mathbb{O}} \cup \{\ (\forall x)(\forall y)[x < y \ \rightarrow \ f(x) < f(y)]\ \},$$

where $T_{\mathbb{O}}$ is the theory of dense order.

In Section 3.2 we saw that the Nelson-Oppen combination method cannot be used in order to combine $T_{\mathbb{R}}$ and $T_{\mathbb{M}}$. In particular, we saw that the Nelson-Oppen

[3] Technically speaking, nontermination is due to more than the presence of infinitely many terms. The problem is that, in general, the abstraction rule cannot be safely restricted to a finite subset of $(\Sigma_1 \cup \Sigma_2)$-terms without sacrificing completeness.

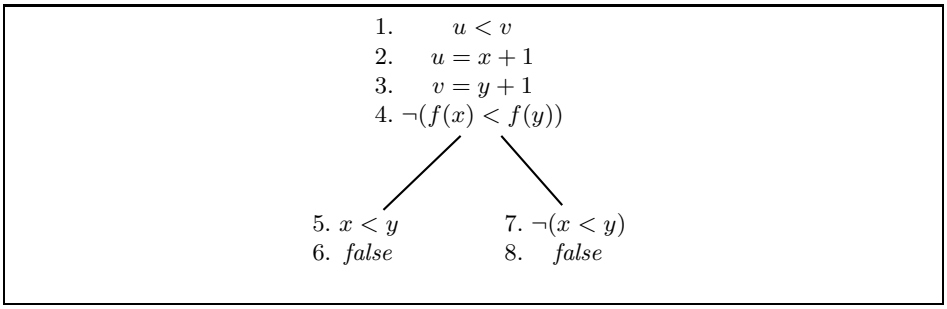

Figure 2: A closed C-tableau.

combination method *incorrectly* concludes that the conjunction

$$\Gamma = \left\{ \begin{array}{c} u < v\,, \\ u = x + 1\,, \\ v = y + 1\,, \\ \neg(f(x) < f(y)) \end{array} \right\}$$

is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-satisfiable, despite the fact that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-unsatisfiable.

Let us see what happens if, instead of the Nelson-Oppen combination method, we use C-tableaux.

Figure 2 shows a closed C-tableau for Γ. Denoting with ℓ_i the literal labeling node i, the inferences can be justified as follows:

- $\ell_1, \ell_2, \ell_3, \ell_4$ are the formulae occurring in Γ.
- ℓ_5 and ℓ_7 are obtained by means of an application of the second decomposition rule.
- ℓ_6 is obtained by using the closure rule, exploiting the fact that $\{\ell_4, \ell_5\}$ is $T_{\mathbb{M}}$-unsatisfiable.
- ℓ_8 is obtained by using the closure rule, exploiting the fact that $\{\ell_1, \ell_2, \ell_3, \ell_5\}$ is $T_{\mathbb{R}}$-unsatisfiable.

Since the C-tableau in Figure 2 is closed, we *correctly* conclude that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{M}})$-unsatisfiable.

5 Dense orders

C-tableaux can be made terminating when we combine theories that share the dense orders.

Let T_i be a Σ_i-theory extending the theory $T_{\mathbb{O}}$ of dense orderings, for $i = 1, 2$. In other words, we have

$$T_1 = T_{\mathbb{O}} \cup S_1\,,$$
$$T_2 = T_{\mathbb{O}} \cup S_2\,,$$

for some sets of sentences S_1, S_2. Assume that $\Sigma_1 \cap \Sigma_2 = \{<\}$. Assume that there exist decision procedures P_1 and P_2 such that, for $i = 1, 2$, P_i can decide the quantifier-free satisfiability problem of T_i.

We now describe how to use C-tableaux to obtain a decision procedure for the quantifier-free satisfiability problem of $T_1 \cup T_2$. As a corollory, we will also obtain a decision procedure for the quantifier-free satisfiability problem of $T_{\mathbb{R}} \cup T_{\mathbb{M}}$ considered in Sections 3.2 and 4.1.

Without loss of generality, let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form. In order to decide whether Γ is $(T_1 \cup T_2)$-satisfiable, we construct an initial C-tableau for Γ, and then we repeatedly apply the rules in Figure 1. However, when applying the rules, we impose the following restriction:

> **Restriction 1.** All rule applications must be *regular*, that is, an application of a rule R to a branch B is forbidden if it would add a literal already occurring in B.

> **Restriction 2.** An application of the abstraction rule to a branch B is allowed to add a literal $t = w$ only if:
> - t is not a variable;
> - t already occurs in B.

If during this process we obtain a closed C-tableau, then we declare that Γ is $(T_1 \cup T_2)$-unsatisfiable. If instead we obtain an open C-tableau for which no rule can be applied without violating the restrictions, then we declare that Γ is $(T_1 \cup T_2)$-satisfiable.

We now prove that, by using Restrictions 1 and 2, C-tableaux are sound, complete, and terminating. Therefore, they provide a decision procedure for the satisfiability problem of the union of theories sharing the dense orders.

Theorem 12 (Termination). *Using Restrictions 1 and 2, C-tableaux are terminating.* □

Proof. Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form, and let T be a C-tableau obtained by exhaustively applying the rules in Figure 1 to an initial C-tableau for Γ. We want to show that T is finite.

Since the decomposition and closure rules never add a new term to T, it follows that the number of new variables introduced by the abstraction rule is finite. Therefore, every rule can be applied only a finite number of times, which implies that all branches in T are finite. Thus, T must also be finite. ■

Since C-tableaux are already sound without Restrictions 1 and 2, they are also sound with the restrictions.

Theorem 13 (Soundness). *Let $\Gamma = \Gamma_1 \cup \Gamma_2$ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. If there exists a closed C-tableau for φ then Γ is $(T_1 \cup T_2)$-unsatisfiable.* □

The completeness proof relies on the following Combination Theorem, independently due to Ringeissen [10] and Tinelli and Harandi [13].

Theorem 14 (Combination Theorem). *Let Σ_1 and Σ_2 be signatures, let Φ_i be a set of Σ_i-formulae, for $i = 1, 2$, and let $V_i = vars(\Phi_i)$. Also, let $\Sigma = \Sigma_1 \cap \Sigma_2$ and $V = V_1 \cap V_2$.*

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

$$\mathcal{A}^{\Sigma,V} \cong \mathcal{B}^{\Sigma,V} .$$ □

We will also use the following lemma, which can be proved using a back-and-forth argument due to Hausdorff [4].[4]

Lemma 15. *Let $\mathcal{A}$ and $\mathcal{B}$ be two enumerable $T_{\mathbb{Q}}$-models. Then $\mathcal{A} \cong \mathcal{B}$.* □

Finally, we will use the following terminology. We say that a branch B is *saturated* if no rule can be applied to it without violating either one of Restrictions 1 and 2.

Lemma 16. *Let B be an open and saturated branch of a C-tableau T. Then B is $(T_1 \cup T_2)$-satisfiable.* □

Proof. Let $V = vars(\mathsf{B})$, and let θ_i be the set of Σ_i-literals occurring in B, for $i = 1, 2$. Since B is open, there exist a T_1-model $\mathcal{A}$ of θ_1 and a T_2-model $\mathcal{B}$ of θ_2. Without loss of generality, we can assume that A and B are enumerable, that is, $|A| = |B| = \aleph_0$.

Our goal is to merge the interpretations $\mathcal{A}$ and $\mathcal{B}$ into a $(T_1 \cup T_2)$-model of $\theta_1 \cup \theta_2$. This goal can be accomplished by an application of the Combination Theorem 14 if we can show that $\mathcal{A}^{\{<\},V} \cong \mathcal{B}^{\{<\},V}$.

Let us define a map $f : V^{\mathcal{A}} \to V^{\mathcal{B}}$ by letting

$$f(x^{\mathcal{A}}) = x^{\mathcal{B}} , \qquad \text{for each } x \in V .$$

By saturation with respect to the decomposition rules, f is a bijective function preserving the ordering $<$. In other words, $a <^{\mathcal{A}} b$ if and only if $f(a) <^{\mathcal{B}} f(b)$, for each $a, b \in V^{\mathcal{A}}$.

Let $a_1, a_2, \ldots, a_m$ be, in increasing order, the elements of $V^{\mathcal{A}}$. Likewise, let $b_1, b_2, \ldots, b_m$ be, in increasing order, the elements of $V^{\mathcal{B}}$. Then $f(a_i) = b_i$, for each $i = 1, \ldots, m$.

Consider the open intervals

$$(-\infty, a_1) = \{a \in A \mid a < a_1\}$$

and

$$(-\infty, b_1) = \{b \in B \mid b < b_1\} .$$

[4] In literature, Hausdorff's back and forth argument has customarily been attributed to Cantor. A recounting of this mis-attribution was written by Silver [11].

Since both intervals are $T_{\mathbb{O}}$-models, by Lemma 15 there exists a bijective map

$$g_{-\infty} : (-\infty, a_1) \to (-\infty, b_1)$$

such that $a <^{\mathcal{A}} b$ if and only if $h(a) <^{\mathcal{B}} h(b)$, for all $a, b \in (-\infty, a_1)$. Similarly, if we let

$$(a_m, +\infty) = \{a \in A \mid a_m < a\}$$

and

$$(b_m, +\infty) = \{b \in B \mid b_m < b\}$$

then there exists a bijective map

$$g_{+\infty} : (a_m, +\infty) \to (b_m, +\infty)$$

such that $a <^{\mathcal{A}} b$ if and only if $h(a) <^{\mathcal{B}} h(b)$, for all $a, b \in (a_m, +\infty)$. Finally, if we let

$$(a_i, a_{i+1}) = \{a \in A \mid a_i < a < a_{i+1}\}$$

and

$$(b_i, b_{i+1}) = \{b \in B \mid b_i < b < b_{i+1}\},$$

for each $i = 1, \ldots, m-1$, then there exist bijective maps

$$g_i : (a_i, a_{i+1}) \to (b_i, b_{i+1})$$

such that $a <^{\mathcal{A}} b$ if and only if $h(a) <^{\mathcal{B}} h(b)$, for all $a, b \in (a_i, a_{i+1})$.

Define a map $h : A \to B$ by letting

$$h(a) = \begin{cases} f(a), & \text{if } a = a_i, \text{for some } i \in \{1, \ldots, m\}, \\ g_{-\infty}(a) & \text{if } a < a_1, \\ g_{+\infty}(a) & \text{if } a_m < a, \\ g_i(a) & \text{if } a_i < a < a_{i+1}, \text{for some } i \in \{1, \ldots, m-1\}. \end{cases}$$

Then h is an isomorphism of $\mathcal{A}$ into $\mathcal{B}$. ∎

Theorem 17 (Completeness). *Let T_i be a Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \{<\}$. Assume that T_1 and T_2 are both extensions of the theory $T_{\mathbb{O}}$ of dense order. Finally, let Γ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. If Γ is $(T_1 \cup T_2)$-unsatisfiable then Γ has a closed C-tableau.* □

Proof. Assume, for a contradiction, that Γ has no closed C-tableau, and let T be the C-tableau obtained by applying exhaustively the rules in Figure 1 to an initial C-tableau for Γ.

Since Γ has no closed C-tableau, T must contain an open and saturated branch B. By Lemma 16, B is $(T_1 \cup T_2)$-satisfiable, which implies that Γ is also $(T_1 \cup T_2)$-satisfiable, a contradiction. ∎

Combining Theorems 12, 13, and 17 we obtain the following decidability result.

Theorem 18 (Decidability). *Let T_i be a Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \{<\}$. Assume that T_1 and T_2 are both extensions of the theory $T_{\mathbb{O}}$ of dense order. Finally, assume that the quantifier-free satisfiability problems of T_1 and T_2 are decidable. Then the quantifier-free satisfiability problem of $T_1 \cup T_2$ is decidable.* □

We conclude this section mentioning the following complexity result.

Theorem 19 (Complexity). *Let T_i be a Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \{<\}$. Assume that T_1 and T_2 are both extensions of the theory $T_{\mathbb{O}}$ of dense order. Finally, assume that the quantifier-free satisfiability problems of T_1 and T_2 are in $\mathcal{NP}$. Then the quantifier-free satisfiability problem of $T_1 \cup T_2$ is $\mathcal{NP}$-complete.* □

Proof. $\mathcal{NP}$-hardness follows by the $\mathcal{NP}$-hardness of the propositional calculus.

To show membership in $\mathcal{NP}$, note that we can check that a $(\Sigma_1 \cup \Sigma_2)$-formula φ is $(T_1 \cup T_2)$-satisfiable by (1) guessing a disjunct Γ of a disjunctive normal form of φ, (2) converting Γ into a $(T_1 \cup T_2)$-equisatisfiable separate form, (3) guessing a branch B of a C-tableau for Γ, and (4) verifying that B is open and saturated.

Since the size of Γ is polynomially bounded by the size of φ, to prove $\mathcal{NP}$-completeness we only need to show that the size of B is polynomially bounded by the size of Γ.

Let n be the number of terms occurring in Γ. Then the number of literals added by the abstraction, decomposition, and closure rules is bounded by $\mathcal{O}(n^2)$. It follows that the size of B is polynomially bounded by the size of Γ. ■

6 Conclusion

We proved that the combination of any two decidable theories sharing the theory of dense order (without endpoints) is decidable. Since these theories share the predicate symbol $<$, we could not use the Nelson-Oppen combination method, because this method does not apply to theories whose signatures are not disjoint. Instead, we used C-tableaux, an extension of Smullyan tableaux that can combine theories whose signatures are not disjoint.

C-tableaux are sound and complete, but not terminating in general. Nevertheless, we showed that, when we combine theories sharing the dense orders, C-tableaux can be made terminating without sacrificing completeness. Thus, C-tableaux provide a decision procedure for the combination of theories sharing dense orders.

We plan to continue our research on non-disjoint combination by investigating more cases of pairs of theories over non-disjoint signatures. In particular, we are interested in the combination of theories sharing the discrete orders or other $\aleph_0$-categorical theories, and in the combination of theories sharing only predicate symbols.

Acknowledgments

We thank the anonymous referees for useful comments.

References

1. Franz Baader and Cesare Tinelli. Combining decision procedures for positive theories sharing constructors. In Sophie Tison, editor, *Rewriting Techniques and Applications*, Lecture Notes in Computer Science. Springer, 2002.
2. Eric Domenjoud, Francis Klay, and Christophe Ringeissen. Combination techniques for non-disjoint equational theories. In Alan Bundy, editor, *Automated Deduction – CADE-12*, volume 814 of *Lecture Notes in Computer Science*, pages 267–281. Springer, 1994.
3. Bernhard Gramlich. On termination and confluence properties of disjoint and constructor-sharing conditional rewrite systems. *Theoretical Computer Science*, 165(1):97–131, 1996.
4. Felix Hausdorff. *Grundzuege der Mengenlehre*. 1914. Reprinted and translated in [5].
5. Felix Hausdorff. *Set Theory*. Chelsea Publishing Company, 5th edition, 2001.
6. C. H. Langford. Some theorems on deducibility. *Annals of Mathematics*, 28:16–40, 1927.
7. Greg Nelson and Derek C. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1(2):245–257, 1979.
8. Enno Ohlebusch. Modular properties of composable term rewriting systems. *Journal of Symbolic Computation*, 20(1):1–41, 1995.
9. Christophe Ringeissen. Unification in a combination of equational theories with shared constants and its application to primal algebras. In Andrei Vonronkov, editor, *Logic Programming and Automated Reasoning*, volume 624 of *Lecture Notes in Computer Science*, pages 261–272. Springer, 1992.
10. 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.
11. Charles L. Silver. Who invented Cantor's back-and-forth argument? *Modern Logic*, 4:74–78, 1994.
12. Alfred Tarski. *A Decision Method for Elementary Algebra and Geometry*. University of California Press, 1951.
13. 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.
14. Cesare Tinelli and Christophe Ringeissen. Unions of non-disjoint theories and combinations of satisfiability procedures. *Theoretical Computer Science*, 290(1):291–353, 2003.
15. Calogero G. Zarba. Combining non-disjoint theories. In Rajeev Gorè, Alexander Leitsch, and Tobias Nipkow, editors, *International Joint Conference on Automated Reasoning: Short Papers*, Technical Report DII 11/01, pages 180–189. Università di Siena, 2001.

16. Calogero G. Zarba. A tableau calculus for combining non-disjoint theories. In Uwe Egly and Christian G. Fermüller, editors, *Automated Reasoning with Analytic Tableaux and Related Methods*, volume 2381 of *Lecture Notes in Computer Science*, pages 315–329. Springer, 2002.