Combining Decision Procedures

Zohar Manna and Calogero G. Zarba

Stanford University
{zm,zarba}@theory.stanford.edu

Abstract. We give a detailed survey of the current state-of-the-art methods for combining decision procedures. We review the Nelson-Oppen combination method, Shostak method, and some very recent results on the combination of theories over non-disjoint signatures.

1 Introduction

Decision procedures are algorithms that can reason about the validity or satisfiability of classes of formulae in a given decidable theory, and always terminate with a positive or negative answer.

Decision procedures are at the heart of virtually every modern program analysis and program verification system. Decision procedures improve the overall efficiency of the verification system and relieve the user from plenty of boring and tedious interaction. In addition, decision procedures are available for many practical domains such as integers [44] and reals [54], as well as for many data structures frequently appearing in programs such as lists [41], arrays [52], sets [8], and multisets [60].

The major advantage of domain-specific decision procedures is efficiency. Fast and efficient decision procedures can be obtained by cleverly exploiting the structure of the domain itself. However, this efficiency comes at the price of specialization. Most verification conditions arising in program analysis and program verification typically involve a complex combination of multiple domains, which means that a decision procedure for a specific domain can be applied only if it is possible to combine it with the decision procedures for the other domains.

The field of combining decision procedures was initiated more than 20 years ago by Nelson and Oppen [35–37, 40] and Shostak [49, 50].

In 1979, Nelson and Oppen [37] proposed a very general approach for combining decision procedures. Given n theories $T_1, \ldots, T_n$ satisfying certain conditions, their method combines the available decision procedures for $T_1, \ldots, T_n$ into a single decision procedure for the satisfiability of quantifier-free formulae in the union theory $T_1 \cup \cdots \cup T_n$. The Nelson-Oppen combination method is at the base of the verification systems CVC [51], ESC [16], EVES [12], SDVS [31], and the Stanford Pascal Verifier [32]. A rigorous analysis of the Nelson-Oppen combination method can be found in [2, 45, 56].

In 1984, Shostak [50] proposed a more restricted method based on congruence closure for combining the quantifier-free theory of equality with theories that are what Shostak called *canonizable* and *solvable*. Shostak's method is at the base

B.K. Aichernig and T. Maibaum (Eds.): Formal Methods ..., LNCS 2757, pp. 381–422, 2003.

of the verification systems ICS [21], PVS [42], SVC [3], and STeP [7]. Shostak method is very popular, as witnessed by the impressive amount of research on it [4, 6, 13, 23, 24, 30, 46, 47, 58]. However, Shostak's original paper suffers from the lack of a rigorous correctness proof. Recently, it was discovered that a correct version of Shostak method can be obtained by recasting it as an instance of the more general Nelson-Oppen combination method [4, 47].

Both Shostak and Nelson-Oppen methods are restricted to the combination of theories over disjoint signatures, that is, theories whose signatures do not have any function or predicate symbol in common.

Combining theories over non-disjoint signatures is a much harder problem, as witnessed by the fact that, more than 20 years after its publication, the Nelson-Oppen combination method is still considered state-of-the-art.

Although it seems that it is not possible to obtain general decidability results in the non-disjoint case, recent research [45, 55, 57, 61] shows that it is always possible to combine decision procedures for theories whose signatures need not be disjoint into a semi-decision procedure for the unsatisfiability of formulae in the union theory.

This paper is organized as follow. In Section 2 we give some preliminary concepts and notations, and we briefly introduce some theories of interest in program verification. In Sections 3 and 4 we describe the Nelson-Oppen combination method, and in Section 5 we describe Shostak's method. In Section 6 we address the problem of combining theories over non-disjoint signatures, and in Section 7 we draw final conclusions.

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.

A *Σ-term* is a first-order term constructed using variables and the symbols in Σ. A *Σ-atom* is either an expression of the form $P(t_1, \dots, t_n)$, where $P \in \Sigma^{\mathrm{P}}$ and $t_1, \dots, t_n$ are Σ-terms, or an expression of the form $s = t$, where $=$ is the logical equality symbol and s, t are Σ-terms. *Σ-literals* are Σ-atoms or expressions of the form $\neg A$, where A is a Σ-atom. *Σ-formulae* are constructed by applying in the standard way the binary logical connectives $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ and the quantifiers $\forall, \exists$ to Σ-literals. *Σ-sentences* are Σ-formulae with no free variables.

When Σ is irrelevant or clear from the context, we will simply write atom, literal, formula, and sentence in place of Σ-atom, Σ-literal, Σ-formula, and Σ-sentence.

If t is a term, we denote with $hd(t)$ the top symbol of t, that is, $hd(t) = f$ if t is of the form $f(t_1, \dots, t_n)$, and $hd(t) = t$ if t is either a constant or a variable. If φ is either a term or a formula, we denote with $vars(\varphi)$ the set of variables occurring free in φ.

A *substitution* is a finite set $\{x_1 \leftarrow t_1, \dots, x_n \leftarrow t_n\}$ of replacement pairs $x_i \leftarrow t_i$, where the x_i are variables, the t_i are terms, and each x_i is distinct from the corresponding expression t_i and from all the other variables x_j. The empty substitution $\{\ \}$ is denoted with ϵ. If σ is a substitution and t is a term, $t\sigma$ denotes the term obtained by applying the substitution σ to the term t. If σ and τ are substitutions, $\sigma \circ \tau$ denotes their *composition*, that is, $t(\sigma \circ \tau) = (t\sigma)\tau$, for each term t.

In the rest of this paper, we will often identify a finite sets of formulae $\{\varphi_1, \ldots, \varphi_n\}$ with the conjunction $\varphi_1 \wedge \cdots \wedge \varphi_n$.

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 $x \in V$ 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 $f^{\mathcal{A}} : A^n \to A$;
- each predicate symbol $P \in \Sigma^{\mathrm{P}}$ of arity n as a subset $P^{\mathcal{A}}$ of A^n. □

In the rest of the paper we will use the convention that the calligraphic letters $\mathcal{A}$, $\mathcal{B}$, ... denote interpretations, and the corresponding Roman letters A, B, ... denote the domains of the interpretations.

For a term t, we denote with $t^{\mathcal{A}}$ the evaluation of t under the interpretation $\mathcal{A}$. Likewise, for a formula φ, we denote with $\varphi^{\mathcal{A}}$ the truth-value of φ under the interpretation $\mathcal{A}$.

Definition 2. A formula φ is

- *valid*, if it evaluates to true under all interpretations;
- *satisfiable*, if it evaluates to true under some interpretation;
- *unsatisfiable*, if it evaluates to false under all interpretations.

A set $\{\varphi_1, \ldots, \varphi_n\}$ of formulae is *valid*, *satisfiable*, *unsatisfiable* if so is the conjunction $\varphi_1 \wedge \cdots \wedge \varphi_n$. □

We say that two formulae φ and ψ are

- *equivalent*, if φ and ψ have the same truth-value under all interpretations;
- *equisatisfiable*, if φ is satisfiable if and only if so is ψ.

If φ is a formula and S is a set of formulae, the notation $S \models \varphi$ means that φ evaluates to true under every interpretation satisfying S.

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 3. 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 *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 First-Order Theories

Definition 4. Let Σ be a signature. A *Σ-theory* is any set of Σ-sentences.

Given a Σ-theory T, a *T-interpretation* is a Σ-interpretation $\mathcal{A}$ such that all Σ-sentences in T evaluate to true under $\mathcal{A}$. □

We will write theory instead of Σ-theory when Σ is irrelevant or clear from the context.

Definition 5. Given a Σ-theory T, a Σ-formula φ is

– *T-valid*, if φ evaluates to true under all T-interpretations;
– *T-satisfiable*, if φ evaluates to true under some T-interpretation;
– *T-unsatisfiable*, if φ evaluates to false under all T-interpretations.

A set $\{\varphi_1, \ldots, \varphi_n\}$ of formulae is *T-valid*, *T-satisfiable*, *T-unsatisfiable* if so is the conjunction $\varphi_1 \wedge \cdots \wedge \varphi_n$. □

For a Σ-theory T, we say that two Σ-formulae φ and ψ are

– *T-equivalent*, if φ and ψ have the same truth-value under all T-interpretations;
– *T-equisatisfiable*, if φ is T-satisfiable if and only if so is ψ.

Given a Σ-theory T, we can define several types of *decision problems*. More precisely, if T is a Σ-theory then

– the *validity problem* for T is the problem of deciding, for each Σ-formula φ, whether or not φ is T-valid;
– the *satisfiability problem* for T is the problem of deciding, for each Σ-formula φ, whether or not φ is T-satisfiable;

Similarly, one can define the *quantifier-free validity problem* and the *quantifier-free satisfiability problem* for a Σ-theory T by restricting the formula φ to be tested for the desired property to be a quantifier-free Σ-formula.

We say that a decision problem is *decidable* if there exists a decision procedure for it. For instance, the validity problem for a Σ-theory T is decidable if there exists a decision procedure for the T-validity of every Σ-formula φ.

Sometimes it is convenient to reduce the (quantifier-free) validity problem for a theory T to the (quantifier-free) satisfiability problem for T. Note that this is always possible because every formula φ is T-valid if and only if $\neg\varphi$ is T-unsatisfiable. Thus, in order to test φ for T-validity, one only needs to test $\neg\varphi$ for T-unsatisfiability.

2.4 Special Theories

In this section we briefly introduce some theories of interest in program verification.

2.4.1 The Theory $T_{\mathbb{E}}$ of Equality

The theory $T_{\mathbb{E}}$ of equality is the empty theory with no axioms, that is, $T_{\mathbb{E}} = \emptyset$.

Due to the undecidability of first-order logic [9, 59], the validity problem for $T_{\mathbb{E}}$ is undecidable.

However, the quantifier-free validity problem for $T_{\mathbb{E}}$ is decidable, a result proved by Ackerman [1]. Efficient decision procedures based on congruence closure are due to Kozen [26], Shostak [48], Downey, Sethi and Tarjan [18], and Nelson and Oppen [38].

2.4.2 The Theory $T_{\mathbb{Z}}$ of Integers

Let $\Sigma_{\mathbb{Z}}$ be the signature containing a constant symbol c_n, for each integer n, a binary function symbol $+$, a unary function symbol $-$, and a binary predicate symbol $\leq$. The theory $T_{\mathbb{Z}}$ of integers is defined as the set of $\Sigma_{\mathbb{Z}}$-sentences that are true in the interpretation $\mathcal{A}$ whose domain A is the set $\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\}$ of integers, and interpreting the symbols in $\Sigma_{\mathbb{Z}}$ according to their standard meaning over $\mathbb{Z}$.

The validity problem for $T_{\mathbb{Z}}$ is decidable, a result proved in 1929 by Presburger [44] using a technique called quantifier elimination. According to this technique, a $\Sigma_{\mathbb{Z}}$-sentence φ is converted into a $T_{\mathbb{Z}}$-equivalent $\Sigma_{\mathbb{Z}}$-sentence ψ without quantifiers. Since ψ is a boolean combination of ground $\Sigma_{\mathbb{Z}}$-atoms, its truth value can be effectively computed.

Other quantifier elimination algorithms for $T_{\mathbb{Z}}$ are described in classic textbooks [19, 27]. The best known quantifier elimination algorithm for $T_{\mathbb{Z}}$ is due to Cooper [11], and has a triple exponential complexity upper bound $2^{2^{2^n}}$, where n is the size of the input formula [39]. Fischer and Rabin [22] proved that *any* quantifier elimination algorithm for $T_{\mathbb{Z}}$ has a nondeterministic doubly exponential lower bound 2^{2^n}.

Better complexity results can be obtained in the quantifier-free case. In fact, the quantifier-free validity problem for $T_{\mathbb{Z}}$ is $\mathcal{NP}$-complete [43].

If we add the multiplication symbol $\times$ to $\Sigma_{\mathbb{Z}}$, and we interpret it as the standard multiplication over $\mathbb{Z}$, then the resulting theory $T_{\mathbb{Z}}^{\times}$ has an undecidable validity problem [9]. In addition, Matiyasevich [33] proved that even the quantifier-free validity problem for $T_{\mathbb{Z}}^{\times}$ is undecidable.

2.4.3 The Theory $T_{\mathbb{R}}$ of Reals

Let $\Sigma_{\mathbb{R}}$ be the signature containing all the symbols in $\Sigma_{\mathbb{Z}}$, plus a constant c_r, for each rational number $r \in \mathbb{Q}$. The theory $T_{\mathbb{R}}$ of real numbers is the set of $\Sigma_{\mathbb{R}}$-sentences that are true in the interpretation $\mathcal{A}$ whose domain A is the set $\mathbb{R}$ of real numbers, and interpreting the symbols in $\Sigma_{\mathbb{R}}$ according to their standard meaning over $\mathbb{R}$.

The validity problem for $T_{\mathbb{R}}$ can be proved to be decidable using quantifier elimination [27]. The best known quantifier elimination algorithm for $T_{\mathbb{R}}$ is due to Ferrante and Rackoff [20], and has a double exponential complexity upper bound 2^{2^n}, where n is the size of the input formula. Fischer and Rabin [22] proved that *any* quantifier elimination algorithm for $T_{\mathbb{R}}$ has a nondeterministic exponential lower bound 2^n.

The problem of deciding the $T_{\mathbb{R}}$-satisfiability of conjunctions of quantifier-free $\Sigma_{\mathbb{R}}$-formulae is solvable in polynomial time [25]. Exponential methods like Simplex [35] and Fourier-Motzkin [29] also also commonly used.

In sharp contrast with the theory of integers, if we add the multiplication symbol $\times$ to $\Sigma_{\mathbb{R}}$, then the validity problem for the resulting theory $T_{\mathbb{R}}^{\times}$ is decidable. This result was proved by Tarski [54] using quantifier elimination. Tarski's method is impractical even for very simple formulae, and a more efficient method based on cylindrical algebraic decomposition is due to Collins [10]. The complexity of the quantifier elimination problem for $T_{\mathbb{R}}^{\times}$ is doubly exponential [14].

2.4.4 The Theory $T_{\mathbb{L}}$ of Lists

Let $\Sigma_{\mathbb{L}}$ be the signature containing a binary function symbol *cons* and two unary function symbols *car* and *cdr*. The theory $T_{\mathbb{L}}$ of lists is defined by the following axioms:

1. a construction axiom

$$(\forall x)[\mathit{cons}(\mathit{car}(x), \mathit{cdr}(x)) = x]$$

2. two selection axioms

$$(\forall x)(\forall y)[\mathit{car}(\mathit{cons}(x, y)) = x]$$
$$(\forall x)(\forall y)[\mathit{cdr}(\mathit{cons}(x, y)) = y]$$

3. an infinite number of acyclicity axioms

$$(\forall x)[\mathit{car}(x) \neq x]$$
$$(\forall x)[\mathit{cdr}(x) \neq x]$$
$$(\forall x)[\mathit{car}(\mathit{car}(x)) \neq x]$$
$$(\forall x)[\mathit{car}(\mathit{cdr}(x)) \neq x]$$
$$\vdots$$

Oppen [41] showed that the validity problem for $T_{\mathbb{L}}$ is decidable but not elementary recursive. In other words, for any positive integer k, there is no decision procedure for the $T_{\mathbb{L}}$-validity of $\Sigma_{\mathbb{L}}$-formulae that always stops in time $2^{2^{\cdot^{\cdot^{2^n}}}}$, where the height of the stack of 2's is k.

More reasonable complexity results hold for the quantifier-free case. The problem of deciding the $T_{\mathbb{L}}$-satisfiability of conjunctions of $\Sigma_{\mathbb{L}}$-literals is solvable in linear time [41].

2.4.5 The Theory $T_{\mathbb{A}}$ of Arrays

The theory $T_{\mathbb{A}}$ of arrays has signature $\Sigma_{\mathbb{A}} = \{\mathit{read}, \mathit{write}\}$. The intended meaning of the function symbols *read* and *write* is as follows:

- given an array a and an index i, $\mathit{read}(a, i)$ is the result of reading the array a at location i;
- given an array a, an index i, and an element e, $\mathit{write}(a, i, e)$ is a new array b which is the same as a, except that $\mathit{read}(b, i) = e$.

Formally, the theory $T_{\mathbb{A}}$ is defined by McCarthy's *read* and *write* axioms [34]:

$$(\forall a)(\forall i)(\forall e)[\mathit{read}(\mathit{write}(a, i, e), i) = e]\,,$$
$$(\forall a)(\forall i)(\forall j)(\forall e)[i \neq j \;\rightarrow\; \mathit{read}(\mathit{write}(a, i, e), j) = \mathit{read}(a, j)]\,,$$

and the following extensionality axiom

$$(\forall a)(\forall b)\,[((\forall i)(\mathit{read}(a, i) = \mathit{read}(b, i))) \;\rightarrow\; a = b]\;.$$

The validity problem for $T_{\mathbb{A}}$ is undecidable [53], whereas the quantifier-free validity problem for $T_{\mathbb{A}}$ is decidable [17, 52].

3 Nelson-Oppen (Nondeterministic)

The Nelson-Oppen combination method combines decision procedures for first-order theories satisfying certain conditions into a single decision procedure for the union theory.

More formally, assume that we are given n signatures $\Sigma_1, \ldots, \Sigma_n$, and let T_i be a Σ_i-theory, for $i = 1, \ldots, n$. Also, assume that there exist decision procedures $P_1, \ldots, P_n$ such that, for $i = 1, \ldots, n$, P_i can decide the T_i-satisfiability of any quantifier-free Σ_i-formula. Using as black boxes the decision procedures P_i, the Nelson-Oppen combination method provides a way of deciding the $(T_1 \cup \cdots \cup T_n)$-satisfiability of $(\Sigma_1 \cup \cdots \cup \Sigma_n)$-formulae.

Three basic assumptions are needed for the Nelson-Oppen method to be applicable:

1. the formula φ to be tested for satisfiability must be *quantifier-free*;
2. the signatures $\Sigma_1, \ldots, \Sigma_n$ must be *disjoint*, that is $\Sigma_i \cap \Sigma_j = \emptyset$, for $i \neq j$;
3. the theories $T_1, \ldots, T_n$ must be *stably infinite* (see Section 3.1).

There are two versions of the Nelson-Oppen combination method: a nondeterministic one and a deterministic one. In this section we describe the nondeterministic version, since it is simpler to explain and easier to understand. We will describe the deterministic version in Section 4.

3.1 Stably Infinite Theories

Definition 6. A Σ-theory T is *stably infinite* if for every T-satisfiable quantifier-free Σ-formula φ there exists a T-interpretation $\mathcal{A}$ satisfying φ whose domain A is infinite. □

Example 1. Let $\Sigma = \{a, b\}$, where a and b are constants. The Σ-theory

$$T = \{(\forall x)(x = a \vee x = b)\}$$

is not stably infinite. In fact, for every quantifier-free formula φ, there cannot exist an infinite T-interpretation satisfying φ, since every T-interpretation must have cardinality no greater than 2. □

All the theories $T_{\mathbb{E}}$, $T_{\mathbb{Z}}$, $T_{\mathbb{R}}$, $T_{\mathbb{L}}$, $T_{\mathbb{A}}$ from Section 2.3 are stably infinite. As an example, we show that the theory $T_{\mathbb{E}}$ of equality is stably infinite.

Theorem 1. *The theory $T_{\mathbb{E}}$ of equality is stably infinite.* □

PROOF. Let φ be a $T_{\mathbb{E}}$-satisfiable quantifier-free formula, and let $\mathcal{A}$ be a $T_{\mathbb{E}}$-interpretation satisfying φ.

We define a $T_{\mathbb{E}}$-interpretation $\mathcal{B}$ as follows. Fix an infinite set A' disjoint from A, and fix an arbitrary element $a_0 \in A \cup A'$. Then, we let

$$B = A \cup A'$$

and

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

Clearly, $\mathcal{B}$ is an infinite $T_{\mathbb{E}}$-interpretation satisfying φ. ■

3.2 The Procedure

In this section we decribe the nondeterministic version of the Nelson-Oppen combination method.

To simplify the presentation, we restrict ourselves to the satisfiability of conjunctions of literals. Note that this does not cause any loss of generality since every quantifier-free formula φ can be effectively converted into an equisatisfiable formula in disjunctive normal form $\varphi_1 \vee \cdots \vee \varphi_n$, where each φ_i is a conjunction of literals. Then φ is satisfiable if and only if at least one of the disjuncts φ_i is satisfiable.

In addition, without loss of generality we can restrict ourselves to the combination of just two theories. In fact, once we know how to combine two theories, we can combine n theories, for each $n \geq 2$. For instance, suppose that we want to combine decision procedures P_1, P_2, P_3 for three theories T_1, T_2, T_3. Then we can first combine P_1 and P_2 into a decision procedure $P_{1\&2}$ for $T_1 \cup T_2$, and then we combine $P_{1\&2}$ and P_3 into a decision procedure $P_{1\&2\&3}$ for the theory $T_1 \cup T_2 \cup T_3$.

Thus, let T_i be a stably infinite Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \emptyset$. Also, let Γ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals.

The nondeterministic version of the Nelson-Oppen combination method consists of two phases: *Variable Abstraction* and *Check*.

3.2.1 First Phase: Variable Abstraction

Let Γ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. In the first phase of the Nelson-Oppen combination method 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.

This can be done by repeatedly applying the following transformations, until nothing more can be done[1].

– Replace each term of the form

$$f(t_1, \ldots, t, \ldots, t_n)$$

in Γ, where $f \in \Sigma_i$ and $hd(t) \in \Sigma_{3-i}$, for some $i \in \{1, 2\}$, with the term

$$f(t_1, \ldots, w, \ldots, t_n)\,,$$

where w is a newly introduced variable, and add the equality

$$w = t$$

to Γ.

– Replace each literal of the form

$$P(t_1, \ldots, t, \ldots, t_n)$$

in Γ, where $P \in \Sigma_i$ and $hd(t) \in \Sigma_{3-i}$, for some $i \in \{1, 2\}$, with the literal

$$P(t_1, \ldots, w, \ldots, t_n)\,,$$

where w is a newly introduced variable, and add the equation

$$w = t$$

to Γ. Literals of the form $\neg P(t_1, \ldots, t, \ldots, t_n)$ are treated similarly.

[1] In the following, note that when $i \in \{1, 2\}$, then $3 - i$ is the "complement" of i.

– Replace each equality of the form

$$s = t$$

in Γ, where $hd(s) \in \Sigma_i$ and $hd(t) \in \Sigma_{3-i}$, with the equalities

$$w = s\,,\ w = t\,,$$

where w is a newly introduced variable.

– Replace each literal of the form

$$s \neq t$$

in Γ, where $hd(s) \in \Sigma_i$ and $hd(t) \in \Sigma_{3-i}$, with the literals

$$w_1 \neq w_2\,,\ w_1 = s\,,\ w_2 = t\,,$$

where w_1 and w_2 are newly introduced variables.

Clearly, the above process must eventually terminate. In addition, the resulting conjunction can be written as $\Gamma_1 \cup \Gamma_2$ where Γ_i contains only Σ_i-literals and $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable if and only if so is Γ[2].

Example 2. Let $\Sigma_1 = \{f\}$ and let $\Sigma_2 = \{g\}$, where f, g are unary function symbols. Let us apply the Variable Abstraction phase to the conjunction of literals

$$\Gamma = \{f(g(x)) \neq g(f(x))\}\,.$$

First, we "purify" the term $f(g(x))$, by introducing a new variable w_1, and obtaining the new conjunction

$$\left\{ \begin{array}{l} w_1 = g(x)\,, \\ f(w_1) \neq g(f(x)) \end{array} \right\}\,.$$

We then purify the term $g(f(x))$, obtaining

$$\left\{ \begin{array}{l} w_1 = g(x)\,, \\ w_2 = f(x)\,, \\ f(w_1) \neq g(w_2) \end{array} \right\}\,.$$

Finally, we purify the disequality, obtaining

$$\left\{ \begin{array}{l} w_1 = g(x)\,, \\ w_2 = f(x)\,, \\ w_3 = f(w_1)\,, \\ w_4 = g(w_2)\,, \\ w_3 \neq w_4 \end{array} \right\}\,.$$

[2] If x, y are variables, a literal of the form $x = y$ or $x \neq y$ is both a Σ_1-literal and a Σ_2-literal. Therefore, such a literal can be arbitrarily placed in either Γ_1 or Γ_2, or both.

We conclude the Variable Abstraction phase by partitioning the literals, obtaining

$$\Gamma_1 = \left\{ \begin{array}{l} w_2 = f(x)\,, \\ w_3 = f(w_1) \end{array} \right\}, \qquad \Gamma_2 = \left\{ \begin{array}{l} w_1 = g(x)\,, \\ w_4 = g(w_2)\,, \\ w_3 \neq w_4 \end{array} \right\}$$

Note that we chose to place the literal $w_3 \neq w_4$ in Γ_2, but it would have been equally correct to place it in Γ_1, as well as to place it in both Γ_1 and Γ_2. □

We call $\Gamma_1 \cup \Gamma_2$ a conjunction of literals in $\langle \Sigma_1, \Sigma_2 \rangle$-*separate* form. We also denote with $\mathit{shared}(\Gamma_1, \Gamma_2)$ the set of variables occurring in both Γ_1 and Γ_2, that is, $\mathit{shared}(\Gamma_1, \Gamma_2) = \mathit{vars}(\Gamma_1) \cap \mathit{vars}(\Gamma_2)$.

3.2.2 Second Phase: Check

Let $\Gamma_1 \cup \Gamma_2$ be a conjunction of literals in $\langle \Sigma_1, \Sigma_2 \rangle$-separate form generated in the Variable Abstraction phase.

Definition 7. Let E be an equivalence relation over some set V of variables. The *arrangement* of V induced by E is defined as the conjunction:

$$\begin{aligned} \alpha(V, E) = \{x = y : x, y \in V \text{ and } xEy\} \cup \\ \{x \neq y : x, y \in V \text{ and not } xEy\} \end{aligned}$$

□

In the second phase of the Nelson-Oppen combination method we perform the following two checks, for every equivalence relation E of $\mathit{shared}(\Gamma_1, \Gamma_2)$.

1. Check whether $\Gamma_1 \cup \alpha(\mathit{shared}(\Gamma_1, \Gamma_2), E)$ is T_1-satisfiable.
2. Check whether $\Gamma_2 \cup \alpha(\mathit{shared}(\Gamma_1, \Gamma_2), E)$ is T_2-satisfiable.

If there exists an equivalence relation E of $\mathit{shared}(\Gamma_1, \Gamma_2)$ for which both check 1 and check 2 succeed, then we declare that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable. Otherwise, we declare $\Gamma_1 \cup \Gamma_2$ to be $(T_1 \cup T_2)$-unsatisfiable.

We will show the correctness of the method in Section 3.4.

3.3 Examples

To illustrate how the Nelson-Oppen combination method works, let us consider some examples.

Example 3. Let us consider the combination of the theory $T_{\mathbb{Z}}$ of integers with the theory $T_{\mathbb{E}}$ of equality, and note that the conjunction

$$\Gamma = \left\{ \begin{array}{l} 1 \leq x\,, \\ x \leq 2\,, \\ f(x) \neq f(1)\,, \\ f(x) \neq f(2) \end{array} \right\}$$

is $(T_{\mathbb{Z}} \cup T_{\mathbb{E}})$-unsatisfiable. In fact, the first two literals imply $x = 1 \vee x = 2$. But then $f(x) = f(1) \vee f(x) = f(2)$, which contradicts the last two literals.

We want to show that Γ is $(T_{\mathbb{Z}} \cup T_{\mathbb{E}})$-unsatisfiable using the Nelson-Oppen combination method. In the Variable Abstraction phase we introduce two new variables w_1, w_2, and we obtain the conjunctions

$$\Gamma_{\mathbb{Z}} = \left\{ \begin{array}{l} 1 \leq x\,, \\ x \leq 2\,, \\ w_1 = 1\,, \\ w_2 = 2 \end{array} \right\}, \qquad \Gamma_{\mathbb{E}} = \left\{ \begin{array}{l} f(x) \neq f(w_1)\,, \\ f(x) \neq f(w_2) \end{array} \right\}.$$

Let $V = \mathit{shared}(\Gamma_{\mathbb{Z}}, \Gamma_{\mathbb{E}}) = \{x, w_1, w_2\}$. There are 5 possible equivalence relations E to examine.

Case 1: xEw_1**,** xEw_2**,** w_1Ew_2**.**
Since $T_{\mathbb{E}} \cup \Gamma_{\mathbb{E}}$ implies $x \neq w_1$, it follows that $\Gamma_{\mathbb{E}} \cup \{x = w_1, x = w_2, w_1 = w_2\}$ is $T_{\mathbb{E}}$-unsatisfiable.

Case 2: xEw_1**,** not xEw_2**,** not w_1Ew_2**.**
Since $T_{\mathbb{E}} \cup \Gamma_{\mathbb{E}}$ implies $x \neq w_1$, it follows that $\Gamma_{\mathbb{E}} \cup \{x = w_1, x \neq w_2, w_1 \neq w_2\}$ is $T_{\mathbb{E}}$-unsatisfiable.

Case 3: not xEw_1**,** xEw_2**,** not w_1Ew_2**.**
Since $T_{\mathbb{E}} \cup \Gamma_{\mathbb{E}}$ implies $x \neq w_2$, it follows that $\Gamma_{\mathbb{E}} \cup \{x \neq w_1, x = w_2, w_1 \neq w_2\}$ is $T_{\mathbb{E}}$-unsatisfiable.

Case 4: not xEw_1**,** not xEw_2**,** w_1Ew_2**.**
Since $T_{\mathbb{Z}} \cup \Gamma_{\mathbb{Z}}$ implies $w_1 \neq w_2$, it follows that $\Gamma_{\mathbb{Z}} \cup \{x \neq w_1, x \neq w_2, w_1 = w_2\}$ is $T_{\mathbb{Z}}$-unsatisfiable.

Case 5: not xEw_1**,** not xEw_2**,** not w_1Ew_2**.**
Since $T_{\mathbb{Z}} \cup \Gamma_{\mathbb{Z}}$ implies the disjunction $x = w_1 \vee x = w_2$, it follows that $\Gamma_{\mathbb{Z}} \cup \{x \neq w_1, x \neq w_2, w_1 \neq w_2\}$ is $T_{\mathbb{Z}}$-unsatisfiable.

Thus, for every equivalence relation E of V we have that either $\Gamma_{\mathbb{Z}} \cup \alpha(V, E)$ is $T_{\mathbb{Z}}$-unsatisfiable or $\Gamma_{\mathbb{E}} \cup \alpha(V, E)$ is $T_{\mathbb{E}}$-unsatisfiable. We can therefore conclude that Γ is $(T_{\mathbb{Z}} \cup T_{\mathbb{E}})$-unsatisfiable. □

In the next example we consider a formula that is satisfiable in the union of two stably infinite theories.

Example 4. Let us consider again the theory $T_{\mathbb{Z}}$ of integers and the theory $T_{\mathbb{E}}$ of equality, and note that the conjunction

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

is $(T_{\mathbb{Z}} \cup T_{\mathbb{E}})$-satisfiable. For instance, a satisfying $(T_{\mathbb{Z}} \cup T_{\mathbb{E}})$-interpretation $\mathcal{A}$ can be obtained by letting $A = \mathbb{Z}$ and $x^{\mathcal{A}} = 1$, $y^{\mathcal{A}} = 2$, $z^{\mathcal{A}} = 3$, $f^{\mathcal{A}}(a) = a$ for each $a \in \mathbb{Z}$.

The Variable Abstraction phase does not introduce new variables, and simply returns the pure conjunctions

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

Since $shared(\Gamma_{\mathbb{Z}}, \Gamma_{\mathbb{E}}) = \{x, y\}$, there are only two equivalence relations to examine: either xEy or not xEy. In the former case $\Gamma_{\mathbb{E}} \cup \{x = y\}$ is $T_{\mathbb{E}}$-unsatisfiable. However, in the latter case we have that $\Gamma_{\mathbb{Z}} \cup \{x \neq y\}$ is $T_{\mathbb{Z}}$-satisfiable and that $\Gamma_{\mathbb{E}} \cup \{x \neq y\}$ is $T_{\mathbb{E}}$-satisfiable. Thus, we correctly conclude that Γ is $(T_{\mathbb{Z}} \cup T_{\mathbb{E}})$-satisfiable. □

In the previous example the conclusion of the Nelson-Oppen method was correct because both theories were stably infinite. The next example shows that when one of the combined theories is not stably infinite the Nelson-Oppen method may not be correct.

Example 5. Let $\Sigma = \{a, b\}$, where a and b are constants, and consider the combination of the theory $T_{\mathbb{E}}$ of equality with the Σ-theory

$$T = \{(\forall x)(x = a \vee x = b)\} .$$

Recall that in Example 1 we saw that T is not stably infinite.

The conjunction

$$\Gamma = \left\{ \begin{array}{l} a = b\,, \\ f(x) \neq f(y) \end{array} \right\}$$

is $(T \cup T_{\mathbb{E}})$-unsatisfiable. In fact $T \cup \{a = b\}$ entails $(\forall u, v)(u = v)$, which contradicts the disequality in Γ.

After the Variable Abstraction phase we obtain the conjunctions

$$\Gamma_1 = \{a = b\}\,, \qquad\qquad \Gamma_{\mathbb{E}} = \{f(x) \neq f(y)\}\,.$$

Since $shared(\Gamma_1, \Gamma_{\mathbb{E}}) = \emptyset$, we only need to check Γ_1 for T-satisfiability and $\Gamma_{\mathbb{E}}$ for $T_{\mathbb{E}}$-satisfiability.

We have that Γ_1 is T-satisfiable: a satisfying T-interpretation $\mathcal{A}$ is obtained by letting $A = \{\bullet\}$ and $a^{\mathcal{A}} = b^{\mathcal{A}} = \bullet$. In addition, $\Gamma_{\mathbb{E}}$ is also $T_{\mathbb{E}}$-satisfiable: a $T_{\mathbb{E}}$-interpretation $\mathcal{B}$ satisfying $\Gamma_{\mathbb{E}}$ is obtained by letting $B = \{\bullet, \circ\}$ and $x^{\mathcal{B}} = \bullet$, $f^{\mathcal{B}}(\bullet) = \bullet$, $y^{\mathcal{B}} = \circ$, $f^{\mathcal{B}}(\circ) = \circ$.

Since Γ_1 is T-satisfiable and $\Gamma_{\mathbb{E}}$ is $T_{\mathbb{E}}$-satisfiable, the Nelson-Oppen method *incorrectly* concludes that Γ is $(T \cup T_{\mathbb{E}})$-satisfiable. □

3.4 Correctness

The correctness of the Nelson-Oppen combination method is based upon the following fundamental theorem, whose proof can be found in the appendix.

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

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

(i) $|A| = |B|$,
(ii) $x^{\mathcal{A}} = y^{\mathcal{A}}$ *if and only if* $x^{\mathcal{B}} = y^{\mathcal{B}}$, *for every variable* $x, y \in shared(\Phi_1, \Phi_2)$. □

The following theorem shows that the Nelson-Oppen combination method is correct.

Theorem 3. *Let T_i be a stably infinite Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \emptyset$. Also, let $\Gamma_1 \cup \Gamma_2$ be a conjunction of literals in $\langle \Sigma_1, \Sigma_2 \rangle$-separate form.*

Then $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable if and only if there exists an equivalence relation E of $V = shared(\Gamma_1, \Gamma_2)$ such that $\Gamma_i \cup \alpha(V, E)$ is T_i-satisfiable, for $i = 1, 2$. □

Proof. Let $\mathcal{M}$ be a $(T_1 \cup T_2)$-interpretation satisfying $\Gamma_1 \cup \Gamma_2$. We define an equivalence relation E of V by letting xEy if and only if $x^{\mathcal{M}} = y^{\mathcal{M}}$, for every variable $x, y \in V$. By construction, $\mathcal{M}$ is a T_i-interpretation satisfying $\Gamma_i \cup \alpha(V, E)$, for $i = 1, 2$.

Vice versa, assume that there exists an equivalence relation E of V such that $\Gamma_i \cup \alpha(V, E)$ is T_i-satisfiable, for $i = 1, 2$. Since T_1 is stably infinite, there exists a T_1-interpretation $\mathcal{A}$ satisfying $\Gamma_1 \cup \alpha(V, E)$ such that A is countably infinite. Similarly, there exists a T_2-interpretation $\mathcal{B}$ satisfying $\Gamma_2 \cup \alpha(V, E)$ such that B is countably infinite.

But then $|A| = |B|$, and $x^{\mathcal{A}} = y^{\mathcal{A}}$ if and only if $x^{\mathcal{B}} = y^{\mathcal{B}}$, for every variable $x, y \in V$. We can therefore apply Theorem 2, and obtain the existence of a $(T_1 \cup T_2)$-interpretation satisfying $\Gamma_1 \cup \Gamma_2$. ■

Combining Theorem 3 with the observation that there is only a finite number of equivalence relations of any finite set of variables, we obtain the following decidability result.

Theorem 4. *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 quantifier-free $(T_1 \cup T_2)$-satisfiability problem is decidable. □

The following theorem generalizes Theorem 4 for any number n of theories, with $n \geq 2$.

Theorem 5. *Let T_i be a stably infinite Σ_i-theory, for $i = 1, \ldots, n$, and let $\Sigma_i \cap \Sigma_j = \emptyset$, for $i \neq j$. Also, assume that the quantifier-free T_i-satisfiability problem is decidable.*

Then the quantifier-free $(T_1 \cup \cdots \cup T_n)$-satisfiability problem is decidable. □

Proof. By induction on n, we will prove the stronger result that $T_1 \cup \cdots \cup T_n$ is a stably infinite theory with a decidable quantifier-free satisfiability problem.

For the base case ($n = 2$), by Theorem 4 we know that the quantifier-free $(T_1 \cup T_2)$-satisfiability problem is decidable. In addition, as a corollary of the proof of Theorem 3, it follows that $T_1 \cup T_2$ is stably infinite.

For the inductive step ($n > 2$), we can obtain a decision procedure for the quantifier-free $(T_1 \cup \cdots \cup T_n)$-satisfiability problem by applying a Nelson-Oppen combination between the theories $T_1 \cup \cdots \cup T_{n-1}$ and T_n. Note that this is possible because by the inductive hypothesis we have that $T_1 \cup \cdots \cup T_{n-1}$ is a stably infinite theory with a decidable quantifier-free satisfiability problem. Note also that $(T_1 \cup \cdots \cup T_{n-1}) \cup T_n$ is stably infinite (corollary of the proof of Theorem 3). ■

n	B_n
1	1
2	2
3	5
4	15
5	52
6	203
7	877
8	4,140
9	21,147
10	115,975
11	678,570
12	4,213,597

Fig. 1. Bell numbers.

3.5 Complexity

The main source of complexity of the nondeterministic version of the Nelson-Oppen combination method is given by the Check phase. In this phase, the decision procedures for T_1 and T_2 are called once for each equivalence relation E of the set of shared variables $shared(\Gamma_1, \Gamma_2)$. The number of such equivalence relations, also known as a *Bell number* [5], grows exponentially in the number of variables in $shared(\Gamma_1, \Gamma_2)$ (see [15] for an in-depth asymptotic analysis).

Figure 1 shows the first 12 Bell numbers. Note when $shared(\Gamma_1, \Gamma_2)$ has 12 variables, there are already more than 4 million equivalence relations!

Despite these discouraging numbers, the nondeterministic version of the Nelson-Oppen combination method provides the following $\mathcal{NP}$-completeness result due to Oppen [40].

Theorem 6. *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 in $\mathcal{NP}$.*

Then the quantifier-free $(T_1 \cup T_2)$-satisfiability problem is in $\mathcal{NP}$. □

PROOF. It suffices to note that it is possible to guess an equivalence relation of any set of n elements using a number of choices that is polynomial in n. ■

3.6 More on Stable Infiniteness

In Section 3.4 we proved that the Nelson-Oppen method is correct under the assumption that the theories T_1, T_2 are stably infinite.

It turns out that stable infiniteness is not a necessary condition for the correctness of the method, but only a *sufficient* one. To see this, consider two theories T_1, T_2 over disjoint signatures for which there exists an integer $n > 0$ such that

$$T_k \models (\exists x_1) \cdots (\exists x_n) \left[\left(\bigwedge_{i \neq j} x_i \neq x_j \right) \wedge (\forall y) \left(\bigvee_{i=1}^{n} y = x_i \right) \right] , \quad \text{for } k = 1, 2 .$$

In other words, all interpretations satisfying T_i have cardinality n.

Despite the fact that T_1 and T_2 are not stably infinite, in this case the Nelson-Oppen combination method can still be applied correctly, as the following theorem shows.

Theorem 7. *Let T_i be a Σ_i theory, for $i = 1, 2$, let $\Sigma_1 \cap \Sigma_2 = \emptyset$, and assume that there exists a positive integer n such that all T_i-interpretations have cardinality n. Also, assume that the quantifier-free T_i-satisfiability problem is decidable.*

Then the quantifier-free $(T_1 \cup T_2)$-satisfiability problem is decidable. □

Proof. The proof follows, with minor variations, the same pattern of Section 3.4. ■

4 Nelson-Oppen (Deterministic)

Because the number of equivalence relations of a set grows exponentially in the number of elements of the set (cf. Figure 1), the nondeterministic version of the Nelson-Oppen combination method is not amenable of a practical and efficient implementation.

A more practical approach is given by the deterministic version of the Nelson-Oppen combination method. In this version we do not enumerate all possible equivalence relations among shared variables, but instead we use the given decision procedures for each theory in order to detect all equalities that must necessarily hold given the input conjunction Γ.

4.1 The Procedure

Let T_i be a stably infinite Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \emptyset$. Also, let Γ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals.

The deterministic version of the Nelson-Oppen combination method is obtained from the nondeterministic version by replacing the Check phase with an Equality Propagation phase.

Instead of enumerating all possible equivalence relations among shared variables, in the Equality Propagation phase we manipulate *derivations* that take the form of a tree labeled with states. A *state* is either the logical symbol *false*, or a triple of the form

$$\langle \Gamma_1, \Gamma_2, E \rangle$$

where

- Γ_i is a set of Σ_i-literals, for $i = 1, 2$;
- E is a set of equalities among variables.

Contradiction rule

$$\frac{\langle \Gamma_1, \Gamma_2, E\rangle}{\mathit{false}} \qquad \text{if } \Gamma_i \cup E \text{ is } T_i\text{-unsatisfiable, for some } i \in \{1,2\}$$

Equality Propagation rule

$$\frac{\langle \Gamma_1, \Gamma_2, E\rangle}{\langle \Gamma_1, \Gamma_2, E \cup \{x = y\}\rangle} \qquad \begin{array}{l}\text{if } x, y \in \mathit{shared}(\Gamma_1, \Gamma_2) \text{ and } x = y \notin E \text{ and} \\ \quad T_i \cup \Gamma_i \cup E \models x = y, \text{ for some } i \in \{1,2\}\end{array}$$

Case Split rule

$$\frac{\langle \Gamma_1, \Gamma_2, E\rangle}{\langle \Gamma_1, \Gamma_2, E \cup \{x_1 = y_1\}\rangle \;\; | \;\; \cdots \;\; | \;\; \langle \Gamma_1, \Gamma_2, E \cup \{x_n = y_n\}\rangle}$$

$$\begin{array}{l}\text{if } x_1, \ldots, x_n, y_1, \ldots, y_n \in \mathit{shared}(\Gamma_1, \Gamma_2) \text{ and} \\ \quad \{x_1 = y_1, \ldots, x_n = y_n\} \cap E = \emptyset \text{ and} \\ \quad T_i \cup \Gamma_i \cup E \models \bigvee_{j=1}^{n} x_j = y_j, \text{for some } i \in \{1,2\}\end{array}$$

Fig. 2. Nelson-Oppen rules

For instance, the triple

$$\langle \{1 \leq x, y \leq 2\},\ \{f(x) \neq f(y)\},\ \{x = y\}\rangle\,.$$

is a state.

Given a conjunction $\Gamma_1 \cup \Gamma_2$ of literals in $\langle \Sigma_1, \Sigma_2\rangle$-separate form, the *initial derivation* D_0 is a tree with only one node labeled with the state

$$\langle \Gamma_1, \Gamma_2, \emptyset\rangle\,.$$

Then, we use the rules in Figure 2 to construct a succession of derivations $\mathsf{D}_0, \mathsf{D}_1, \ldots, \mathsf{D}_n$. The rules are to be applied as follows. Assume that D_i is a derivation containing one leaf labeled with the premise s of a rule of the form

$$\frac{s}{s_1 \;\; | \;\; \cdots \;\; | \;\; s_n}$$

Then we can construct a new derivation D_{i+1} which is the same as D_i, except that the leaf labeled with s has now n children labeled with $s_1, \ldots, s_n$.

Intuitively, the Contradiction rule detects inconsistencies, and the Equality Propagation and Case Split rules increase the set E of equalities in order to incrementally construct the desired equivalence relation.

If during the Equality Propagation phase we obtain a derivation in which all leaves are labeled with *false*, then we declare that the initial conjunction Γ is $(T_1 \cup T_2)$-unsatisfiable. If instead we obtain a derivation containing a branch whose leaf node is not labeled with *false*, and no rule can be applied to it, then we declare that Γ is $(T_1 \cup T_2)$-satisfiable.

We will show the correctness of the method in Section 4.3.

4.2 Examples

Example 6. Let us consider the combination of the theory $T_{\mathbb{R}}$ of reals with the theory $T_{\mathbb{E}}$ of equality. Note that the conjunction[3]

$$\Gamma = \left\{ \begin{array}{l} f(f(x) - f(y)) \neq f(z)\,, \\ x \leq y\,, \\ y + z \leq x\,, \\ 0 \leq z \end{array} \right\}$$

is $(T_{\mathbb{R}} \cup T_{\mathbb{E}})$-unsatisfiable. In fact, the last three literals imply $x = y$ and $z = 0$, so that the first literal simplifies to $f(0) \neq f(0)$.

After applying the Variable Abstraction phase, we obtain the pure conjunctions

$$\Gamma_{\mathbb{R}} = \left\{ \begin{array}{l} x \leq y\,, \\ y + z \leq x\,, \\ 0 \leq z\,, \\ w_3 = w_1 - w_2 \end{array} \right\} \qquad \Gamma_{\mathbb{E}} = \left\{ \begin{array}{l} f(w_3) \neq f(z)\,, \\ w_1 = f(x)\,, \\ w_2 = f(y) \end{array} \right\}$$

Since $\mathit{shared}(\Gamma_{\mathbb{R}}, \Gamma_{\mathbb{E}}) = \{x, y, z, w_1, w_2, w_3\}$, Figure 1 tells us that there are 203 possible equivalence relations among the shared variables. Clearly, it is infeasible to enumerate all of them by hand. Nevertheless, we can quickly detect that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{E}})$-unsatisfiable with the following derivation.

$$\begin{array}{c} s_0 : \langle \Gamma_{\mathbb{R}}, \Gamma_{\mathbb{E}}, \emptyset \rangle \\ | \\ s_1 : \langle \Gamma_{\mathbb{R}}, \Gamma_{\mathbb{E}}, \{x = y\} \rangle \\ | \\ s_2 : \langle \Gamma_{\mathbb{R}}, \Gamma_{\mathbb{E}}, \{x = y, w_1 = w_2\} \rangle \\ | \\ s_3 : \langle \Gamma_{\mathbb{R}}, \Gamma_{\mathbb{E}}, \{x = y, w_1 = w_2, z = w_3\} \rangle \\ | \\ s_4 : \mathit{false} \end{array}$$

In the above derivation, the inferences can be justified as follows:

- s_1 follows by the Equality Propagation rule since $T_{\mathbb{R}} \cup \Gamma_{\mathbb{R}} \models x = y$;
- s_2 follows by the Equality Propagation rule since $T_{\mathbb{E}} \cup \Gamma_{\mathbb{E}} \cup \{x = y\} \models w_1 = w_2$;
- s_3 follows by the Equality Propagation rule since $T_{\mathbb{R}} \cup \Gamma_{\mathbb{R}} \cup \{w_1 = w_2\} \models z = w_3$;

[3] Taken from [35].

– s_4 follows by the Contradiction rule since $\Gamma_{\mathbb{E}} \cup \{z = w_3\}$ is $T_{\mathbb{E}}$-unsatisfiable.

Hence, we conclude that Γ is $(T_{\mathbb{R}} \cup T_{\mathbb{E}})$-unsatisfiable. □

Example 7. Consider the theory $T_{\mathbb{Z}}$ of integers and the theory $T_{\mathbb{E}}$ of equality. In Example 3 we showed that the conjunction

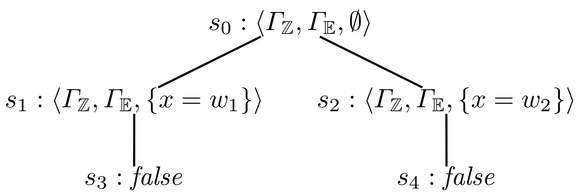
$$\Gamma = \left\{ \begin{array}{l} 1 \leq x\,, \\ x \leq 2\,, \\ f(x) \neq f(1)\,, \\ f(x) \neq f(2) \end{array} \right\}$$

is $(T_{\mathbb{Z}} \cup T_{\mathbb{E}})$-unsatisfiable using the nondeterministic version of the Nelson-Oppen combination method. Let us now use the deterministic version.

After the Variable Abstraction phase we obtain the pure conjunctions

$$\Gamma_{\mathbb{Z}} = \left\{ \begin{array}{l} 1 \leq x\,, \\ x \leq 2\,, \\ w_1 = 1\,, \\ w_2 = 2 \end{array} \right\}, \qquad \Gamma_{\mathbb{E}} = \left\{ \begin{array}{c} f(x) \neq f(w_1)\,, \\ f(x) \neq f(w_2) \end{array} \right\}.$$

We have the following derivation



Note that the inferences can be justified as follows:

– s_1 and s_2 follow by the Case Split rule since $T_{\mathbb{Z}} \cup \Gamma_{\mathbb{Z}} \models x = w_1 \vee x = w_2$;
– s_3 follows from s_1 by the Contradiction rule since $\Gamma_{\mathbb{E}} \cup \{x = w_1\}$ is $T_{\mathbb{E}}$-unsatisfiable;
– s_4 follows from s_2 by the Contradiction rule since $\Gamma_{\mathbb{E}} \cup \{x = w_2\}$ is $T_{\mathbb{E}}$-unsatisfiable.

Since all leaves are labeled with *false*, we conclude that Γ is $(T_{\mathbb{Z}} \cup T_{\mathbb{E}})$-unsatisfiable. □

4.3 Correctness

We now prove that the deterministic version of the Nelson-Oppen combination method is correct.

The following lemma shows that the inference rules are terminating.

Lemma 1. *The inference rules in Figure 2 form a terminating inference system.* □

Proof. The claim easily follows by noting that since there is only a finite number of shared variables, the Equality Propagation and Case Split rules can be applied only a finite number of times. ■

Next, we show that the inference rules are sound.

Definition 8. We say that a state $\langle \Gamma_1, \Gamma_2, E \rangle$ is $(T_1 \cup T_2)$-*satisfiable* if and only if so is $\Gamma_1 \cup \Gamma_2 \cup E$. □

Lemma 2. *For each inference rule in Figure 2, the state above the line is* $(T_1 \cup T_2)$-*satisfiable if and only if at least one state below the line is* $(T_1 \cup T_2)$-*satisfiable.* □

Proof. We only prove the soundness of the Equality Propagation rule (the other rules can be handled similarly).

Thus, assume that $\langle \Gamma_1, \Gamma_2, E \rangle$ is $(T_1 \cup T_2)$-satisfiable, and that $T_i \cup \Gamma_i \cup E \models x = y$. Let $\mathcal{A}$ be a $(T_1 \cup T_2)$-interpretation satisfying $\Gamma_1 \cup \Gamma_2 \cup E$. Since $T_i \cup \Gamma_i \cup E \models x = y$, it follows that $x^{\mathcal{A}} = y^{\mathcal{A}}$, and therefore $\mathcal{A}$ is a $(T_1 \cup T_2)$-interpretation satisfying $\langle \Gamma_1, \Gamma_2, E \cup \{x = y\} \rangle$.

Vice versa, if $\langle \Gamma_1, \Gamma_2, E \cup \{x = y\} \rangle$ is $(T_1 \cup T_2)$-satisfiable then clearly $\langle \Gamma_1, \Gamma_2, E \rangle$ is also $(T_1 \cup T_2)$-satisfiable. ■

Lemma 3. *Let* $\langle \Gamma_1, \Gamma_2, E \rangle$ *be a state such that no rule in Figure 2 can be applied to it. Then* $\Gamma_1 \cup \Gamma_2 \cup E$ *is* $(T_1 \cup T_2)$-*satisfiable.* □

Proof. Since the Contradiction rule cannot be applied to $\langle \Gamma_1, \Gamma_2, E \rangle$, we have that $\Gamma_i \cup E$ is T_i-satisfiable, for $i = 1, 2$.

We claim that there exists a T_1-interpretation $\mathcal{A}$ satisfying $\Gamma_1 \cup E$ such that $x^{\mathcal{A}} \neq y^{\mathcal{A}}$, for each $x, y \in \mathit{shared}(\Gamma_1, \Gamma_2)$ such that $x = y \notin E$. To see that this is the case, let $S = \{(x, y) : x, y \in \mathit{shared}(\Gamma_1, \Gamma_2) \text{ and } x = y \notin E\}$, and consider the disjunction

$$\psi : \bigvee_{(x,y) \in S} x = y\,.$$

If $T_1 \cup \Gamma_1 \not\models \psi$ then our claim is verified. If instead $T_1 \cup \Gamma_1 \models \psi$ then, by the Case Split rule, there exists a pair $(x, y) \in S$ such that $x = y \in E$, a contradiction.

Similarly, there exists a T_2-interpretation $\mathcal{B}$ satisfying $\Gamma_2 \cup E$ such that $x^{\mathcal{B}} \neq y^{\mathcal{B}}$, for each $x, y \in \mathit{shared}(\Gamma_1, \Gamma_2)$ such that $x = y \notin E$.

But then $x^{\mathcal{A}} = y^{\mathcal{A}}$ if and only if $x^{\mathcal{B}} = y^{\mathcal{B}}$, for every variable $x, y \in \mathit{shared}(\Gamma_1, \Gamma_2)$. In addition, since T_1 and T_2 are stably infinite, we can assume without loss of generality that both A and B are countably infinite. We can therefore apply Theorem 2, and obtain the existence of a $(T_1 \cup T_2)$-interpretation satisfying $\Gamma_1 \cup \Gamma_2 \cup E$. ■

Combining Lemmas 1, 2 and 3, we obtain the correctness of the deterministic version of the Nelson-Oppen combination method.

Theorem 8. *Let* T_i *be a stably infinite* Σ_i-*theory, for* $i = 1, 2$, *and let* $\Sigma_1 \cap \Sigma_2 = \emptyset$. *Then the inference rules in Figure 2 provide a decision procedure for the quantifier-free* $(T_1 \cup T_2)$-*satisfiability problem.* □

4.4 Convexity

There is an interesting difference between the derivation in Example 6 and the one in Example 7. In Example 6 we never used the Case Split rule. In contrast, in Example 7 we *had to* use the Case Split rule, and no proof can be obtained if we use only the Contradiction and Equality Propagation rules.

Clearly, for efficiency reasons it would be desirable to avoid case splits as much as possible. Indeed, the Case Split rule can be avoided altogether when the combined theories are *convex*.

Definition 9. A Σ-theory T is *convex* if for every conjunction Γ of Σ-literals and for every disjunction $\bigvee_{i=1}^{n} x_i = y_i$,

$$T \cup \Gamma \models \bigvee_{i=1}^{n} x_i = y_i \qquad \text{iff} \qquad T \cup \Gamma \models x_j = y_j, \text{for some } j \in \{1, \ldots, n\}. \quad \square$$

Examples of convex theories include the theory $T_{\mathbb{E}}$ of equality, the theory $T_{\mathbb{R}}$ of reals, and the theory $T_{\mathbb{L}}$ of lists, whereas examples of non-convex theories are the theory $T_{\mathbb{Z}}$ of integers, and the theory $T_{\mathbb{A}}$ of arrays.

We refer to [37] for a proof of the convexity of $T_{\mathbb{R}}$, and to [38] for a proof of the convexity of $T_{\mathbb{E}}$ and $T_{\mathbb{L}}$. To see that $T_{\mathbb{Z}}$ and $T_{\mathbb{A}}$ are not convex, just note that:

- in $T_{\mathbb{Z}}$, the conjunction $\{x = 1, y = 2, 1 \leq z, z \leq 2\}$ entails $x = z \vee y = z$ but does not entail neither $x = z$ nor $y = z$;
- in $T_{\mathbb{A}}$, the conjunction $\{\mathit{read}(\mathit{write}(a, i, e), j) = x, \mathit{read}(a, j) = y\}$ entails $x = e \vee x = y$ but does not entail neither $x = e$ nor $x = y$.

The following theorem states that when both the combined theories are convex, the deterministic version of the Nelson-Oppen combination method remains correct even if we omit the Case Split rule.

Theorem 9. *Let T_i be a stably infinite and convex Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \emptyset$. Then the Contradiction and Equality Propagation rules alone provide a decision procedure for the quantifier-free $(T_1 \cup T_2)$-satisfiability problem.* □

Proof. In the proofs of Section 4.3, the only place where we used the Case Split rule was in Lemma 3. But the proof of Lemma 3 works fine even if instead of the Case Split rule we use the hypothesis of convexity. ■

A simple complexity analysis of the procedure presented in this section shows the following complexity result.

Theorem 10. *Let T_i be a stably infinite and convex Σ_i-theory, for $i = 1, 2$, and let $\Sigma_1 \cap \Sigma_2 = \emptyset$. Also, assume that the problem of checking the T_i-satisfiability of conjunctions of quantifier-free Σ_i-formulae can be decided in polynomial time, for $i = 1, 2$.*

Then the problem of checking the $(T_1 \cup T_2)$-satisfiability of conjunctions of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae can be decided in polynomial time. □

We conclude this section by mentioning the following result, first proved in [4], relating the notions of convexity and stable infiniteness.

Theorem 11. *If* T *is a convex theory then* $T \cup \{(\exists x)(\exists y)x \neq y\}$ *is stably infinite.* □

Proof. Let $T' = T \cup \{(\exists x)(\exists y)x \neq y\}$, and assume, for a contradiction, that T' is not stably infinite. Then there exists a conjunction Γ of literals such that $T' \cup \Gamma$ is satisfiable in some finite interpretation but not in an infinite interpretation.

By the compactness theorem, there must be a positive integer n and an interpretation $\mathcal{A}$ such that:

- $|A| = n$;
- $\mathcal{A}$ satisfies $T' \cup \Gamma$;
- all interpretations having cardinality greater than n do not satisfy $T' \cup \Gamma$.

Let $x_1, \ldots, x_n, x_{n+1}, x', y'$ be distinct fresh variables not occurring in Γ, and consider the disjunction

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

By the pigeonhole principle, we have that

$$T \cup \{x' \neq y'\} \cup \Gamma \models \bigvee_{i \neq j} x_i = x_j$$

but

$$T \cup \{x' \neq y'\} \cup \Gamma \not\models x_i = x_j\,, \qquad \text{for all } i, j \text{ such that } i \neq j\,,$$

which contradicts the fact that T is convex. ■

5 Shostak

In 1984, Shostak [50] presented a method for combining the theory $T_{\mathbb{E}}$ of equality with theories $T_1, \ldots, T_n$ satisfying certain conditions.

According to Shostak, such theories must admit so called *canonizers* and *solvers*. These canonizers and solvers are first combined into one single canonizer and solver for the union theory $T = T_1 \cup \cdots \cup T_n$. Then, Shostak's actual procedure is called, and the theory T is combined with the theory $T_{\mathbb{E}}$.

Unfortunately, Shostak's original paper contains several mistakes. First, as pointed out in [28, 30], it is not always possible to combine the solvers for the theories $T_1, \ldots, T_n$ into a single solver for the union theory $T = T_1 \cup \cdots \cup T_n$. Secondly, as pointed out in [46], Shostak's procedure combining T with $T_{\mathbb{E}}$ is incomplete and potentially nonterminating.

Nevertheless, all these mistakes can be elegantly fixed if Shostak's method is recast as an instance of the Nelson-Oppen combination method.

To do this, we introduce the notion of a *Shostak theory*, and we show how a solver for a Shostak theory T_i can be used to produce a decision procedure for

T_i. Then, if $T_1, \ldots, T_n$ are Shostak theories, we do not combine their solvers, but instead we use the Nelson-Oppen combination method to combine the decision procedures for $T_1, \ldots, T_n$ with a decision procedure for $T_{\mathbb{E}}$.

In addition, we show how a solver for a Shostak theory can be used to efficiently detect implied equalities when applying the Nelson-Oppen combination method.

5.1 Solvers

Before defining Shostak theories, we need to define what is a *solver.*

Definition 10 (Solver). A *solver* for a Σ-theory T is a computable function solve that takes as input Σ-equalities of the form $s = t$ and

– if $T \models s = t$ then $\mathsf{solve}(s = t) = \mathit{true}$;
– if $T \models s \neq t$ then $\mathsf{solve}(s = t) = \mathit{false}$;
– otherwise, $\mathsf{solve}(s = t)$ returns a substitution

$$\sigma = \{x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n\}$$

such that:
- $x_i \in \mathit{vars}(s = t)$, for all i;
- $x_i \notin \mathit{vars}(t_j)$, for all i, j;
- the following equivalence is T-valid:

$$s = t \;\leftrightarrow\; (\exists y_1) \cdots (\exists y_k) \left[\bigwedge_{i=1}^{n} x_i = t_i \right],$$

where $y_1, \ldots, y_k$ are newly introduced variables, that is

$$\{y_1, \ldots, y_k\} = \left(\bigcup_{i=1}^{n} \mathit{vars}(t_i) \right) \setminus \mathit{vars}(s = t).$$

A theory is *solvable* if it has a solver. □

Example 8. Every inconsistent theory is *not* solvable. To see this, let T be an inconsistent Σ-theory, and let solve be a solver for T.

Since T is inconsistent, for every Σ-equality $s = t$, we have both $T \models s = t$ and $T \models s \neq t$. Thus, $\mathsf{solve}(s = t) = \mathit{true}$ and $\mathsf{solve}(s = t) = \mathit{false}$ at the same time. This is a contradiction, because solve is a function. □

Example 9. The simplest solvable theory is the trivial theory

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

A solver for T returns *true* on every input. □

Example 10. A more interesting solvable theory is the theory $T_{\mathbb{R}}$ of reals. Given an equality $s = t$, a solver for $T_{\mathbb{R}}$ can be implemented by employing the following steps:

1. rewrite $s = t$ as $s - t = 0$;
2. combining like terms, rewrite $s - t = 0$ as an equality of the form

$$a_0 + a_1 x_1 + \cdots + a_n x_n = 0 \,,$$

   where $a_i \neq 0$, for $i = 1, \ldots, n$;
3. return *true*, *false*, or a substitution σ, according to the following:
   – if $n = 0$ and $a_0 = 0$, return *true*;
   – if $n = 0$ and $a_0 \neq 0$, return *false*;
   – if $n > 0$, return the substitution $\sigma = \left\{x_1 \leftarrow -\frac{a_0}{a_1} - \frac{a_2}{a_1}x_2 - \cdots - \frac{a_n}{a_1}x_n\right\}$.

For instance, the equation

$$2x - y + z = 2y + z - 1$$

is solved by

1. transposing the right-hand side, obtaining the equation

$$2x - y + z - (2y + z - 1) = 0 \,,$$

2. combining like terms, obtaining the equation

$$2x - 3y + 1 = 0 \,,$$

3. returning the substitution

$$\sigma = \left\{ x \leftarrow \frac{3}{2}y - \frac{1}{2} \right\} .$$

Similarly, we have

$$\mathsf{solve}(x + x = 2x) = \mathsf{solve}(x + x - 2x = 0) = \mathsf{solve}(0 = 0) = \mathit{true}$$

and

$$\mathsf{solve}(1 = 2) = \mathsf{solve}(1 - 2 = 0) = \mathsf{solve}(-1 = 0) = \mathit{false} \,. \qquad \square$$

Example 11. We now show that no solver can exist for the theory $T_{\mathbb{E}}$ of equality. To see this, suppose, for a contradiction, that solve is a solver for $T_{\mathbb{E}}$, and consider the equation

$$f(x) = a \,,$$

where x is a variable, a is a constant, and f is a function symbol.

Since $T_{\mathbb{E}} \not\models f(x) = a$ and $T_{\mathbb{E}} \not\models f(x) \neq a$, we have that

$$\mathsf{solve}(f(x) = a) = \{x \leftarrow t\} \,,$$

for some term t such that $x \notin \mathit{vars}(t)$. In addition

$$T_{\mathbb{E}} \models f(x) = a \leftrightarrow (\exists y_1) \cdots (\exists y_k)(x = t) \,,$$

where $\{y_1, \ldots, y_k\} = \mathit{vars}(t)$. But this is a contradiction, since for any term t, the equivalence $f(x) = a \leftrightarrow (\exists y_1) \cdots (\exists y_k)(x = t)$ is not $T_{\mathbb{E}}$-valid. $\square$

5.2 Shostak Theories

Definition 11. A Σ-theory T is a *Shostak theory* if

- Σ does not contain predicate symbols, that is, $\Sigma^{\mathrm{P}} = \emptyset$;
- T is convex;
- T is solvable. □

The trivial theory $T = \{(\forall x)(\forall y)(x = y)\}$ is a Shostak Theory. In fact, in Example 9 we saw that T is solvable. In addition, T is also convex, since for every conjunction Γ and every disjunction of equalities $\bigvee_{i=1}^{n} x_i = y_i$, if $T \cup \Gamma \models \bigvee_{i=1}^{n} x_i = y_i$ then $T \models x_i = y_i$, for all $i = 1, \ldots, n$.

The classical example of a Shostak theory is the theory $T_{\mathbb{R}}^{-}$ obtained by restricting the theory $T_{\mathbb{R}}$ of reals to the functional signature $\Sigma_{\mathbb{R}}^{-} = \{0, 1, +, -\}$ (we remove the predicate symbol $\leq$). In example 10 we saw that $T_{\mathbb{R}}$ is solvable, and in Section 4.4 we noted that $T_{\mathbb{R}}$ is convex. Thus $T_{\mathbb{R}}^{-}$ is both solvable and convex.

On the other hand, the theory $T_{\mathbb{E}}$ of equality is *not* a Shostak theory, since it is not solvable (cf. Example 11).

5.3 The Procedure

Let T be a Shostak Σ-theory. We now present a decision procedure that, using the solver for the theory T, decides the T-satisfiability of any quantifier-free Σ-formula. The decision procedure presented here is a rule-based version of the decision procedure in [4].

As usual, we restrict ourselves to conjunctions of Σ-literals. Since Σ does not contain predicate symbols, each conjunction is of the form

$$s_1 = t_2, \ldots, s_m = t_m, s_1' \neq t_1', \ldots, s_n' \neq t_n' \,. \tag{1}$$

Thus, let Γ be a conjunction of Σ-literals of the form (1). The decision procedure consists of applying the inference rules in Figure 3, until nothing more can be done.

Intuitively, the Contradiction rules detect the inconsistencies, and the Equality Elimination rule is used to remove all the equalities from the conjunction Γ.

If the literal *false* is deduced, then we declare that the initial conjunction Γ is T-unsatisfiable. If instead the literal *false* is not deduced and no rule can be applied, then we declare that Γ is T-satisfiable.

5.4 An Example

Example 12. Consider the Shostak theory $T_{\mathbb{R}}^{-}$. The conjunction

$$\Gamma = \left\{ \begin{array}{l} x + 2y = 3z \,, \\ x - y = 0 \,, \\ y \neq z \end{array} \right\}$$

is $T_{\mathbb{R}}^{-}$-unsatisfiable. In fact, subtracting the second equation from the first one yields $3y = 3z$, which contradicts the disequality $y \neq z$.

The following derivation shows that Γ is $T_{\mathbb{R}}^{-}$-unsatisfiable.

Contradiction rule 1

$$\frac{\Gamma \cup \{s \neq t\}}{\mathit{false}} \qquad \text{if } \mathsf{solve}(s = t) = \mathit{true}$$

Contradiction rule 2

$$\frac{\Gamma \cup \{s = t\}}{\mathit{false}} \qquad \text{if } \mathsf{solve}(s = t) = \mathit{false}$$

Equality Elimination rule

$$\frac{\Gamma \cup \{s = t\}}{\Gamma\sigma} \qquad \text{if } \mathsf{solve}(s = t) = \sigma$$

Fig. 3. Shostak rules.

$$\Gamma : \{x + 2y = 3z,\ x - y = 0,\ y \neq z\}$$

$$\mathsf{solve}(x + 2y = 3z) = \{x \leftarrow -2y + 3z\}$$

$$\Gamma_1 : \{-2y + 3z - y = 0,\ y \neq z\}$$

$$\mathsf{solve}(-2y + 3z - y = 0) = \{y \leftarrow z\}$$

$$\Gamma_2 : \{z \neq z\}$$

$$\mathsf{solve}(z = z) = \mathit{true}$$

$$\Gamma_3 : \mathit{false}$$

Note that Γ_1 and Γ_2 follow by the Equality Elimination rule, and that Γ_3 follows by the Contradiction rule 1. □

5.5 Correctness

In this section we show that our Shostak-based decision procedure is correct. Clearly, the procedure must terminate, as the following lemma states.

Lemma 4. *The inference rules in Figure 3 form a terminating inference system.* □

Proof. It suffices to note that any application of the inference rules in Figure 3 either deduces *false* or decreases the number of literals in the conjunction. ■

The following lemma shows that the inference rules in Figure 3 are sound.

Lemma 5. *For each inference rule in Figure 3, the conjunction above the line is T-satisfiable if and only if so is the conjunction below the line.* □

PROOF. The lemma trivially holds for the Contradiction rules.

Concerning the Equality Elimination rule, assume that $\Gamma \cup \{s = t\}$ is T-satisfiable, and let $\mathcal{A}$ be a T-interpretation satisfying $\Gamma \cup \{s = t\}$. Also, let $\sigma = \mathsf{solve}(s = t) = \{x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n\}$. Since the equivalence

$$s = t \;\leftrightarrow\; (\exists y_1) \cdots (\exists y_k) \left[\bigwedge_{i=1}^{n} x_i = t_i \right]$$

is T-valid, we can extend $\mathcal{A}$ over the variables $y_1, \ldots, y_k$ in such a way that $x_i^{\mathcal{A}} = t_i^{\mathcal{A}}$, for all i. But then, by basic model-theoretic properties of substitutions, it follows that $\Gamma\sigma$ is true in $\mathcal{A}$.

Vice versa, assume that $\Gamma\sigma$ is T-satisfiable, where $\sigma = \mathsf{solve}(s = t) = \{x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n\}$, and let $\mathcal{A}$ be a T-interpretation satisfying $\Gamma\sigma$. Since the variables x_i do not occur in $\Gamma\sigma$, we can redefine $\mathcal{A}$ on the x_i by letting $x_i^{\mathcal{A}} = t_i^{\mathcal{A}}$, for all i. But then, by the definition of solver, we have $s^{\mathcal{A}} = t^{\mathcal{A}}$, and by basic model-theoretic properties of substitutions it follows that Γ is true in $\mathcal{A}$. ■

Lemma 6. *If upon termination of the procedure the final result is not false, then the final conjunction is T-satisfiable.* □

PROOF. Assume that upon termination the final result is not *false*. Then the final conjunction must be of the form

$$s_1 \neq t_1, \ldots, s_n \neq t_n \,,$$

where $\mathsf{solve}(s_i = t_i) \neq \mathit{true}$, for each $i = 1, \ldots, n$. It follows that $s_i \neq t_i$ is T-satisfiable, for $i = 1, \ldots, n$, and by the convexity of T, we have that the final conjunction is T-satisfiable. ■

Combining Lemmas 4, 5 and 6, we obtain the following decidability result.

Theorem 12. *Let T be Shostak Σ-theory. Then the quantifier-free T-satisfiability problem is decidable.* □

5.6 Integration in Nelson-Oppen

Let $T_1, \ldots, T_\ell, T_{\ell+1}, \ldots, T_n$ be stably infinite Σ_i-theories such that $\Sigma_i \cap \Sigma_j = \emptyset$, for $i \neq j$. Also, assume that $T_{\ell+1}, \ldots, T_n$ are Shostak theories.

Using the results of Section 5.3, we know how to obtain, for each $i = \ell + 1, \ldots, n$, a decision procedure for the T_i-satisfiability of quantifier-free Σ_i-formulae. Thus, if we assume that we also have, for each $i = 1, \ldots, \ell$, a decision procedure for the T_i-satisfiability of quantifier-free Σ_i-formulae, we can employ the Nelson-Oppen combination method to obtain a decision procedure for the $(T_1 \cup \cdots \cup T_n)$-satisfiability of $(\Sigma_1 \cup \cdots \cup \Sigma_n)$-formulae. This can be summarized in the following theorem.

Theorem 13. *Let $T_1, \ldots, T_\ell, T_{\ell+1}, \ldots, T_n$ be stably infinite Σ_i-theories such that $\Sigma_i \cap \Sigma_j = \emptyset$, for $i \neq j$, and let $T_{\ell+1}, \ldots, T_n$ be Shostak theories. Also, assume that the quantifier-free T_i-satisfiability problem is decidable, for $i = 1, \ldots, \ell$.*

Then the quantifier-free $(T_1 \cup \cdots \cup T_n)$-satisfiability problem is decidable. □

Note that a special case of the above theorem is the combination of the theory $T_{\mathbb{E}}$ of equality with n Shostak theories.

In addition, it turns out that when we combine the theory $T_{\mathbb{E}}$ of equality with n Shostak theories $T_1, \ldots, T_n$ then we can obtain a decision procedure for the theory $T_{\mathbb{E}} \cup T_1 \cup \cdots \cup T_n$ even if $T_1, \ldots, T_n$ are not stably infinite.

Theorem 14. *Let $T_{\mathbb{E}}$ be the theory of equality, and let $T_1, \ldots, T_n$ be Shostak theories such that $\Sigma_i \cap \Sigma_j = \emptyset$, for $i \neq j$,*

Then the quantifier-free $(T_{\mathbb{E}} \cup T_1 \cup \cdots \cup T_n)$-satisfiability problem is decidable. □

Proof. Let $T = T_{\mathbb{E}} \cup T_1 \cup \cdots \cup T_n$.

Observe that every set of formulae is satisfiable if and only if it is either true under an interpretatin $\mathcal{A}$ such that $|A| = 1$, or true under an interpretation $\mathcal{A}$ such that $|A| > 1$. Thus, we can obtain a decision procedure for the quantifier-free T-satisfiability problem if we are able to obtain a decision procedure for the quantifier-free satisfiability problem of $T \cup \{(\forall x)(\forall y)(x = y)\}$, and a decision procedure for the quantifier-free satisfiability problem of $T \cup \{(\exists x)(\exists y)(x \neq y)\}$.

Case 1: $T \cup \{(\exists x)(\exists y)(x \neq y)\}$**.**

Note that for every conjuction Γ we have that Γ is $(T_i \cup \{(\exists x)(\exists y)(x \neq y)\})$-satisfiable if and only if $\Gamma \cup \{x' \neq y'\}$ is T_i-satisfiable, where x' and y' are fresh variables not occurring in Γ. Since T_i is a Shostak theory, by applying Theorem 12, we obtain that the quantifier-free satisfiability problem for $T_i \cup \{(\exists x)(\exists y)(x \neq y)\}$ is decidable. In addition, by Theorem 11, it follows that $T_i \cup \{(\exists x)(\exists y)(x \neq y)\}$ is a stably infinite theory. We can therefore apply the Nelson-Oppen combination method between the following theories:

- $T_{\mathbb{E}}$;
- $T_i \cup \{(\exists x)(\exists y)(x \neq y)\}$, for all i,

and obtain a decision procedure for the quantifier-free satisfiability problem of $T \cup \{(\exists x)(\exists y)(x \neq y)\}$.

Case 2: $T \cup \{(\forall x)(\forall y)(x = y)\}$**.**

In this case we apply the Nelson-Oppen combination method between the following theories:

- $T_{\mathbb{E}} \cup \{(\forall x)(\forall y)(x = y)\}$;
- $T_i \cup \{(\forall x)(\forall y)(x = y)\}$, for all i,

even though none of these theories is stably infinite. To see that this is still correct, first note that all the above theories have decidable quantifier-free problems. In addition, the domain of any interpretation satisfying any of the above theories must have cardinality one, and therefore an application of Theorem 7 allows us to obtain a decidion procedure for the quantifier-free satisfiability problem of $T \cup \{(\forall x)(\forall y)(x = y)\}$. ■

5.7 Using a Solver to Detect Implied Equalities

In this section we show how it is possible to use a solver for a Shostak theory to detect implied equalities.

To do this, we need to extend the definition of a solver to operate on conjunctions of equalities.

Definition 12. Let solve be a solver for a Shostak Σ-theory T. We let

$$\begin{aligned} \mathsf{solve}(\emptyset) &= \epsilon \\ \mathsf{solve}(\Gamma \cup \{s = t\}) &= \sigma \circ \mathsf{solve}(\Gamma\sigma)\,, \qquad \text{where } \sigma = \mathsf{solve}(s = t). \end{aligned} \qquad \square$$

Let solve be a solver for a Shostak Σ-theory T, let Γ be a conjunction of equalities, and let Δ be a conjunction of disequalities. Also, let $\lambda = \mathsf{solve}(\Gamma)$, and assume that $\Gamma \cup \Delta$ is T-satisfiable. We claim that

$$T \cup \Gamma \cup \Delta \models x = y \qquad \text{iff} \qquad \mathsf{solve}(x\lambda = y\lambda) = \mathit{true}\,. \tag{2}$$

Clearly, (2) provides a way to detect implied equalities using the solver for the Shostak theory T.

Example 13. Let us consider the combination of the theory $T_{\mathbb{E}}$ of equality with the Shostak theory $T_{\mathbb{R}}^{-}$.

Note that the conjunction[4]

$$\Gamma = \left\{ \begin{array}{l} f(x-1) - 1 = x + 1\,, \\ f(y) + 1 = y - 1\,, \\ y + 1 = x \end{array} \right\}$$

is $(T_{\mathbb{E}} \cup T_{\mathbb{R}}^{-})$-unsatisfiable. In fact, the first and third equalities imply $f(y) = y + 3$, and the second equality implies $f(y) = y - 2$. But then $y + 3 = y - 2$, a contradiction.

We will use the Nelson-Oppen combination method and a solver for $T_{\mathbb{R}}^{-}$ to show that Γ is $(T_{\mathbb{E}} \cup T_{\mathbb{R}}^{-})$-unsatisfiable.

After the Variable Abstraction phase we obtain the conjunctions

$$\Gamma_{\mathbb{E}} = \left\{ \begin{array}{l} w_1 = f(w_2)\,, \\ w_3 = f(y) \end{array} \right\}, \qquad \Gamma_{\mathbb{R}} = \left\{ \begin{array}{l} w_1 - 1 = x + 1\,, \\ w_2 = x - 1\,, \\ w_3 + 1 = y - 1\,, \\ y + 1 = x \end{array} \right\}.$$

We have the following derivation.

[4] Taken from [46].

$$
\begin{array}{l}
s_0 : \langle \Gamma_{\mathbb{E}}, \Gamma_{\mathbb{R}}, \emptyset \rangle \\
\quad \big| \; T_{\mathbb{R}}^{-} \cup \Gamma_{\mathbb{R}} \models y = w_2 \\
s_1 : \langle \Gamma_{\mathbb{E}}, \Gamma_{\mathbb{R}}, \{y = w_2\} \rangle \\
\quad \big| \; T_{\mathbb{E}} \cup \Gamma_{\mathbb{E}} \cup \{y = w_2\} \models w_1 = w_3 \\
s_2 : \langle \Gamma_{\mathbb{E}}, \Gamma_{\mathbb{R}}, \{y = w_2, w_1 = w_3\} \rangle \\
\quad \big| \; T_{\mathbb{R}}^{-} \cup \Gamma_{\mathbb{R}} \cup \{y = w_2, w_1 = w_3\} \models w_1 \neq w_3 \\
s_3 : \mathit{false}
\end{array}
$$

The inference from state s_1 to state s_2 is obvious. To justify the inference from state s_0 to state s_1, let us compute $\lambda = \mathsf{solve}(\Gamma_{\mathbb{R}})$.

$$
\begin{aligned}
\mathsf{solve}(\Gamma_{\mathbb{R}}) &= \mathsf{solve}(\{w_1 - 1 = x + 1, w_2 = x - 1, w_3 + 1 = y - 1, \underbrace{y + 1 = x}_{\text{solves to } \{x \leftarrow y+1\}}\}) \\
&= \{x \leftarrow y + 1\} \circ \mathsf{solve}(\{w_1 - 1 = y + 2, w_2 = y, \underbrace{w_3 + 1 = y - 1}_{\text{solves to } \{y \leftarrow w_3+2\}}\}) \\
&= \{x \leftarrow w_3 + 3, y \leftarrow w_3 + 2\} \circ \mathsf{solve}(\{w_1 - 1 = w_3 + 4, \underbrace{w_2 = w_3 + 2}_{\text{solves to } \{w_2 \leftarrow w_3+2\}}\}) \\
&= \{x \leftarrow w_3 + 3, y \leftarrow w_3 + 2, w_2 \leftarrow w_3 + 2\} \circ \mathsf{solve}(\{\underbrace{w_1 - 1 = w_3 + 4}_{\text{solves to } \{w_1 \leftarrow w_3+5\}}\}) \\
&= \{x \leftarrow w_3 + 3, y \leftarrow w_3 + 2, w_2 \leftarrow w_3 + 2, w_1 \leftarrow w_3 + 5\}
\end{aligned}
$$

Clearly, $\mathsf{solve}(y\lambda = w_2\lambda) = \mathit{true}$, and therefore $T_{\mathbb{R}}^{-} \cup \Gamma_{\mathbb{R}} \models y = w_2$.

To justify the inference from state s_2 to state s_3, note that

$$\mathsf{solve}(w_1\lambda = w_3\lambda) = \mathsf{solve}(w_3 + 5 = w_3) = \mathit{false}\,.$$

Thus, $T_{\mathbb{R}}^{-} \cup \Gamma_{\mathbb{R}} \models w_1 \neq w_3$, which implies that $\Gamma_{\mathbb{R}} \cup \{y = w_2, w_1 = w_3\}$ is $T_{\mathbb{R}}^{-}$-unsatisfiable. □

Theorem 15 below formally shows that (2) holds. But before proving it, we need two auxiliary lemmas.

Lemma 7. *Let $\sigma = \{x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n\}$ be a substitution such that $x_i \notin vars(t_j)$, for all i, j.*

Then for any theory T and for any conjunction Γ of literals:

$$T \cup \Gamma \cup \{x_1 = t_1, \ldots, x_n = t_n\} \models x = y \qquad \textit{iff} \qquad T \cup \Gamma\sigma \models x\sigma = y\sigma\,. \quad \square$$

Proof. Let $T \cup \Gamma \cup \{x_1 = t_1, \ldots, x_n = t_n\} \models x = y$ and assume that $\mathcal{A}$ is an interpretation satisfying $T \cup \Gamma\sigma$. Thus $x^{\mathcal{A}} = y^{\mathcal{A}}$. Since the variables x_i do not occur in $\Gamma\sigma$, we can redefine $\mathcal{A}$ on the x_i by letting $x_i^{\mathcal{A}} = t_i^{\mathcal{A}}$, for all i. But then, by basic model-theoretic properties of substitutions, it follows that $x\sigma = y\sigma$ is true under $\mathcal{A}$.

Vice versa, let $T \cup \Gamma\sigma \models x\sigma = y\sigma$, and let $\mathcal{A}$ be an interpretation satisfying $T \cup \Gamma \cup \{x_1 = t_1, \ldots, x_n = t_n\}$. Then $[x\sigma]^{\mathcal{A}} = [y\sigma]^{\mathcal{A}}$. In addition $x_i^{\mathcal{A}} = t_i^{\mathcal{A}}$, for all i, and by basic model-theoretic properties of substitutions, it follows that $x = y$ is true under $\mathcal{A}$. ∎

Lemma 8. *Let T be a convex theory, Γ a conjunction of equalities, and Δ a conjunction of disequalities. Also, assume that $\Gamma \cup \Delta$ is T-satisfiable.*

Then

$$T \cup \Gamma \cup \Delta \models x = y \qquad \textit{iff} \qquad T \cup \Gamma \models x = y\,. \qquad \square$$

Proof. Clearly, if $T \cup \Gamma \models x = y$ then $T \cup \Gamma \cup \Delta \models x = y$.

Vice versa, assume that $T \cup \Gamma \cup \Delta \models x = y$. Then

$$T \cup \Gamma \models \left(\bigvee_{s \neq t \in \Delta} s = t \right) \vee x = y\,.$$

Since T is convex, either $T \cup \Gamma \models x = y$ or there exists a disequality $s \neq t$ in Δ such that $T \cup \Gamma \models s = t$. In the former case, the lemma is proved. In the latter case, we have that $\Gamma \cup \Delta$ is T-unsatisfiable, a contradiction. ∎

The following theorem proves (2), thus showing how a solver for a Shostak theory can be used to detect implied equalities.

Theorem 15. *Let* solve *be a solver for a Shostak Σ-theory T, let Γ be a conjunction of equalities, and let Δ be a conjunction of disequalities.*

If $\Gamma \cup \Delta$ is T-satisfiable then

$$T \cup \Gamma \cup \Delta \ \models \ x = y \qquad \textit{iff} \qquad \mathsf{solve}(x\lambda = y\lambda) = \textit{true}$$

where $\lambda = \mathsf{solve}(\Gamma)$. □

Proof. Since $\mathsf{solve}(x\lambda = y\lambda) = \textit{true}$ if and only if $T \models x\lambda = y\lambda$, we only need to prove that

$$T \cup \Gamma \cup \Delta \ \models \ x = y \qquad \text{iff} \qquad T \models x\lambda = y\lambda$$

We proceed by induction on the number of literals in Γ. For the base case, if $\Gamma = \emptyset$ then $\lambda = \mathsf{solve}(\Gamma) = \epsilon$ and

$$\begin{aligned} T \cup \Gamma \cup \Delta \models x = y \quad & \text{iff} \quad T \cup \Delta \models x = y \\ & \text{iff} \quad T \models x = y \qquad \text{(by Lemma 8)} \\ & \text{iff} \quad \mathsf{solve}(x\epsilon = y\epsilon) = \textit{true}\,. \end{aligned}$$

For the inductive step, let $\Gamma = \Gamma' \cup \{s = t\}$. Also let

$$\begin{aligned} \sigma &= \mathsf{solve}(s = t) = \{x_1 \leftarrow t_1, \ldots, x_n \leftarrow t_n\} \\ \tau &= \mathsf{solve}(\Gamma'\sigma) \\ \lambda &= \mathsf{solve}(\Gamma) = \sigma \circ \tau\,. \end{aligned}$$

Then

$$
\begin{array}{llll}
T\cup\Gamma\cup\Delta\models x=y & \text{iff} & T \cup \Gamma' \cup \{s = t\} \cup \Delta \models x = y & \\
 & \text{iff} & T \cup \Gamma' \cup \{s = t\} \models x = y & \text{(by Lemma 8)} \\
 & \text{iff} & T \cup \Gamma' \cup \{x_1 = t_1, \ldots, x_n = t_n\} \models x = y & \text{(by Definition 10)} \\
 & \text{iff} & T \cup \Gamma'\sigma \models x\sigma = y\sigma & \text{(by Lemma 7)} \\
 & \text{iff} & T \models x\sigma\tau = y\sigma\tau & \text{(by induction)} \\
 & \text{iff} & T \models x\lambda = y\lambda\,. & \blacksquare
\end{array}
$$

6 Non-disjoint Combination

In this section we consider the problem of combining theories over non-disjoint signatures.

More precisely, 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 T_i-satisfiability of quantifier-free Σ_i-formulae.

Using as black boxes the decision procedures P_1 and P_2, we show how to obtain a procedure $P_{1\&2}$ that is sound and complete for the $(T_1 \cup T_2)$-unsatisfiability of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae. In other words, if φ is $(T_1 \cup T_2)$-unsatisfiable, then $P_{1\&2}$ eventually stops, and reports the unsatisfiability. If instead φ is $(T_1 \cup T_2)$-satisfiable, then $P_{1\&2}$ runs forever.

Indeed, Zarba [61] showed that soundness and completeness hold even if φ is not quantifier-free, but in this paper we prefer to restrict our attention to quantifier-free formulae for clarity of presentation.

For technical reasons, we will assume that the theories T_1 and T_2 are *universal.*

Definition 13. A formula is *universal* if it is of the form $(\forall x_1) \cdots (\forall x_n)\psi$, where ψ is quantifier-free.

A theory is *universal* if all its sentences are universal. □

The condition that the theories T_1 and T_2 be universal is necessary for the completeness proof, because only for universal formulae the following Theorem 16 holds, a theorem that can be seen as a positive version of the well-known Herbrand Theorem.

Theorem 16 (Herbrand). *Let Φ be a set of universal Σ-formulae, where $\Sigma^{\mathrm{C}} \neq \emptyset$. Then Φ is satisfiable if and only if there exists an interpretation $\mathcal{A}$ satisfying Φ such that for each element $a \in A$ there exists a Σ-term t such that $vars(t) \subseteq vars(\Phi)$ and $t^{\mathcal{A}} = a$.* □

6.1 The Procedure

Let Σ_1 and Σ_2 be two arbitrary signatures which are non necessarily disjoint, and let T_i be an universal Σ_i-theory, for $i = 1, 2$.

Contradiction rule

$$\frac{\langle \Gamma_1, \Gamma_2 \rangle}{\mathit{false}} \qquad \text{if } \Gamma_i \text{ is } T_i\text{-unsatisfiable, for some } i \in \{1,2\}$$

Abstraction rule 1

$$\frac{\langle \Gamma_1, \Gamma_2 \rangle}{\langle \Gamma_1 \cup \{t = w\}, \Gamma_2 \cup \{w = w\} \rangle} \qquad \begin{array}{l}\text{where } t \text{ is any } \Sigma_1\text{-term and}\\ w \text{ is a new variable}\end{array}$$

Abstraction rule 2

$$\frac{\langle \Gamma_1, \Gamma_2 \rangle}{\langle \Gamma_1 \cup \{w = w\}, \Gamma_2 \cup \{t = w\} \rangle} \qquad \begin{array}{l}\text{where } t \text{ is any } \Sigma_2\text{-term and}\\ w \text{ is a new variable}\end{array}$$

Decomposition rule

$$\frac{\langle \Gamma_1, \Gamma_2 \rangle}{\langle \Gamma_1 \cup \{\psi\}, \Gamma_2 \cup \{\psi\} \rangle \quad | \quad \langle \Gamma_1 \cup \{\neg\psi\}, \Gamma_2 \cup \{\neg\psi\} \rangle}$$

where ψ is an atom either of the form $x = y$ or of the form $P(x_1, \ldots, x_n)$, with $x, y, x_1, \ldots, x_n \in \mathit{shared}(\Gamma_1, \Gamma_2)$ and $P \in \Sigma_1^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}}$

Fig. 4. Non-disjoint combination rules

We now present a procedure that is sound and complete for the $(T_1 \cup T_2)$-unsatisfiabilty of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae. As usual, we restict ourselves to conjunctions of $(\Sigma_1 \cup \Sigma_2)$-literals.

Thus, let Γ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. We first apply the Variable Abstraction phase from Section 3.2, obtaining a conjunction $\Gamma_1 \cup \Gamma_2$ of literals in $\langle \Sigma_1, \Sigma_2 \rangle$-separate form such that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable if and only if so is Γ. Then, we construct the *initial state*

$$\langle \Gamma_1, \Gamma_2 \rangle ,$$

and we repeatedly apply the rules in Figure 4.

As usual, the Contradiction rule is used to detect the inconsistencies. The intuition behind the Abstraction rules is as follows. 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 1, the decision procedure for T_2 is aware of the existence of t. Finally, the Decomposition rule is used to let the decision procedures for T_1 and T_2 agree on the truth value of each atom ψ.

If we obtain a derivation in which all leaves are labeled with *false*, we declare that the initial conjunction Γ is $(T_1 \cup T_2)$-unsatisfiable.

6.2 An Example

Example 14. Let us consider the combination of the theory $T_{\mathbb{Z}}$ of integers with the Σ-theory

$$T = \{ \ (\forall x)(\forall y)(x \leq y \rightarrow f(x) \leq f(y)) \ \} ,$$

where $\Sigma = \{\leq, f\}$. Note that $\Sigma_{\mathbb{Z}} \cap \Sigma = \{\leq\} \neq \emptyset$.

The conjunction

$$\Gamma = \left\{ \begin{array}{l} x + y = z\,, \\ 0 \leq y\,, \\ \neg(f(x) \leq f(z)) \end{array} \right\}$$

is $(T_{\mathbb{Z}} \cup T)$-unsatisfiable. In fact, the first two literals imply $x \leq z$, and by the monotonicity of f we have $f(x) \leq f(z)$, which contradicts the third literal.

After the Variable Abstraction phase we get the conjunctions

$$\Gamma_{\mathbb{Z}} = \left\{ \begin{array}{l} x + y = z\,, \\ 0 \leq y \end{array} \right\}, \qquad \Gamma_2 = \{\neg(f(x) \leq f(z))\}\,.$$

We have the following derivation.

$$s_0 : \langle \Gamma_{\mathbb{Z}}, \Gamma_2 \rangle$$

$$s_1 : \langle \Gamma_{\mathbb{Z}} \cup \{x \leq z\}, \Gamma_2 \cup \{x \leq z\} \rangle \qquad s_2 : \langle \Gamma_{\mathbb{Z}} \cup \{\neg(x \leq z)\}, \Gamma_2 \cup \{\neg(x \leq z)\} \rangle$$

$$s_3 : \mathit{false} \qquad s_4 : \mathit{false}$$

The inferences can be justified as follows.

- s_1 and s_2 follow by the Decomposition rule;
- s_3 follows from s_1 by the Contradiction rule since $\Gamma_2 \cup \{x \leq z\}$ is T_2-unsatisfiable;
- s_4 follows from s_2 by the Contradiction rule since $\Gamma_{\mathbb{Z}} \cup \{\neg(x \leq z)\}$ is $T_{\mathbb{Z}}$-unsatisfiable. □

Hence, we conclude that Γ is $(T_{\mathbb{Z}} \cup T)$-unsatisfiable.

6.3 Soundness and Completeness

We now prove that the rules in Figure 4 form a sound and complete inference system for the $(T_1 \cup T_2)$-unsatisfiability of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae.

Let us start with soundness.

Definition 14. A state $\langle \Gamma_1, \Gamma_2 \rangle$ is $(T_1 \cup T_2)$-*satisfiable* if and only if $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable. □

Lemma 9 (soundness). *For each inference rule in Figure 4, the state above the line is $(T_1 \cup T_2)$-satisfiable if and only if at least one of the states below the line is $(T_1 \cup T_2)$-satisfiable* □

PROOF. We only prove the soundness of the Decomposition rule (the other rules can be handled similarly).

Thus, assume that $\langle \Gamma_1, \Gamma_2 \rangle$ is $(T_1 \cup T_2)$-satisfiable, and let $\mathcal{A}$ be a $(T_1 \cup T_2)$-interpretation satisfying $\Gamma_1 \cup \Gamma_2$. If $\psi^{\mathcal{A}}$ is true then $\langle \Gamma_1 \cup \{\psi\}, \Gamma_2 \cup \{\psi\} \rangle$ is

$(T_1 \cup T_2)$-satisfiable. If instead $\psi^{\mathcal{A}}$ is false then $\langle \Gamma_1 \cup \{\neg\psi\}, \Gamma_2 \cup \{\neg\psi\}\rangle$ is $(T_1 \cup T_2)$-satisfiable.

Vice versa, if either $\langle \Gamma_1 \cup \{\psi\}, \Gamma_2 \cup \{\psi\}\rangle$ or $\langle \Gamma_1 \cup \{\neg\psi\}, \Gamma_2 \cup \{\neg\psi\}\rangle$ is $(T_1 \cup T_2)$-satisfiable, then clearly $\langle \Gamma_1, \Gamma_2\rangle$ is $(T_1 \cup T_2)$-satisfiable. ■

The completeness proof is based upon the following Combination Theorem, due independently to Ringeissen [45] and Tinelli and Harandi [56], and whose proof can be found in the appendix.

Theorem 17 (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 $V_i = vars(\Phi_i)$.*

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

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

Lemma 10 (Completeness). *Let $\Gamma_1 \cup \Gamma_2$ be a $(T_1 \cup T_2)$-unsatisfiable conjunction of literals in $\langle \Sigma_1, \Sigma_2\rangle$-separate form.*

Then there exists a derivation whose initial state is $\langle \Gamma_1, \Gamma_2\rangle$ and such that all its leaves are labeled with false. □

Proof. Assume, for a contradiction, that no such derivation exists. Starting from the initial state $\langle \Gamma_1, \Gamma_2\rangle$, apply exhaustively the rules in Figure 4, obtaining a "limit" derivation D^∞. This derivation must contain some branch B such that none of its nodes is labeled with *false*. Thus

$$\mathsf{B} \;=\; \langle \Gamma_1^{(0)}, \Gamma_2^{(0)}\rangle,\; \langle \Gamma_1^{(1)}, \Gamma_2^{(1)}\rangle, \ldots,\; \langle \Gamma_1^{(n)}, \Gamma_2^{(n)}\rangle, \ldots$$

where $\Gamma_1^{(0)} = \Gamma_1$, $\Gamma_2^{(0)} = \Gamma_2$, and for each $n \geq 0$, $i = 1, 2$ we have $\Gamma_i^{(n)} \subseteq \Gamma_i^{(n+1)}$.

Let Γ_1^∞ and Γ_2^∞ be the set of literals defined by

$$\Gamma_1^\infty = \bigcup_{n=0}^{\infty} \Gamma_1^i , \qquad\qquad \Gamma_2^\infty = \bigcup_{n=0}^{\infty} \Gamma_2^i ,$$

and let $S = shared(\Gamma_1^\infty, \Gamma_2^\infty)$.

We claim that Γ_i^∞ is T_i-satisfiable, for $i = 1, 2$. To see this, note that $\Gamma_i^{(n)}$ is T_i-satisfiable, for each $n \geq 0$. It follows that every finite subset of Γ_i^∞ is T_i-satisfiable, and by the Compactness Theorem, Γ_i^∞ is T_i-satisfiable.

Let $\mathcal{A}$ be a T_1-interpretation satisfying Γ_1^∞. Since T_1 is universal, by the Herbrand Theorem 16 we can assume without loss of generality that $A = [T(\Sigma_1, vars(\Gamma_1^\infty)]^{\mathcal{A}}$. Thus, by Abstraction rule 1 we have $A = S^{\mathcal{A}}$.

Similarly, there exists a T_2-interpretation $\mathcal{B}$ satisfying Γ_2^∞ such that $B = S^{\mathcal{B}}$.

The next step of the proof is to merge the interpretations $\mathcal{A}$ and $\mathcal{B}$ into a single $(T_1 \cup T_2)$-interpretation $\mathcal{M}$ satisfying $\Gamma_1^\infty \cup \Gamma_2^\infty$. Clearly, this goal can be accomplished by an application of the Combination Theorem 17 if we can show that $\mathcal{A}^{\Sigma_1 \cap \Sigma_2, S} \cong \mathcal{B}^{\Sigma_1 \cap \Sigma_2, S}$. Accordingly, we define a function $h : A \to B$ by letting

$$h(a) = [name_{\mathcal{A}}(a)]^{\mathcal{B}}\,, \qquad \text{for each } a \in A\,,$$

where $name_{\mathcal{A}} : A \to S$ is any fixed function such that

$$[name_{\mathcal{A}}(a)]^{\mathcal{A}} = a\,, \qquad \text{for each } a \in A\,.$$

It is easy, albeit tedious, to verify that h is an isomorphism of $\mathcal{A}^{\Sigma_1 \cap \Sigma_2, S}$ into $\mathcal{B}^{\Sigma_1 \cap \Sigma_2, S}$. We can therefore apply the Combination Theorem 17 and obtain a $(T_1 \cup T_2)$-interpretation satisfying $\Gamma_1^\infty \cup \Gamma_2^\infty$. Since $\Gamma_1 \cup \Gamma_2 \subseteq \Gamma_1^\infty \cup \Gamma_2^\infty$, it follows that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \cup T_2)$-satisfiable, a contradiction. ■

Combining lemmas 9 and 10 we obtain the following result.

Theorem 18. *Let T_i be an universal Σ_i-theory such that, for $i = 1, 2$, there exists a decision procedure for the T_i-satisfiability of quantifier-free Σ-formulae.*

Then the rules in Figure 4 provide a semi-decision procedure for the $(T_1 \cup T_2)$-unsatisfiability of quantifier-free $(\Sigma_1 \cup \Sigma_2)$-formulae. □

6.4 Why Universal Theories?

Theorem 18 proves that the procedure presented in this section is sound and complete under the assumption that the combined theories T_1 and T_2 are universal. As an example of what can go wrong when one of the theories is not universal, consider the following theories

$$T_1 = \{(\exists x)\neg P(x)\}\,, \qquad T_2 = \{(\forall x)P(x)\}\,,$$

and the literal $u \neq v$.

Since $T_1 \cup T_2$ is unsatisfiable, it follows that $u \neq v$ is $(T_1 \cup T_2)$-unsatisfiable, but the decision procedure presented in this section is unable to detect the unsatisfiability.

7 Conclusions

The problem of combining decision procedures is important for the development of program analysis and program verification systems. The problem can be stated as follows: Given decision procedures P_1 and P_2 for the quantifier-free validity problem of theories T_1 and T_2, how can we obtain a decision procedure $P_{1\&2}$ for the quantifier-free validity problem of $T_1 \cup T_2$?

We saw that if T_1 and T_2 are stably infinite and the signatures of the theories T_1 and T_2 are disjiont, then we can construct the decision procedure $P_{1\&2}$ using the Nelson-Oppen combination method.

Despite being more than 20 years old, the Nelson-Oppen combination method is the current state of the art solution for the problem of combining decision procedures in the disjiont case. The Nelson-Oppen method is also a generalization of Shostak's method.

The problem of combining decision procedures for theories over non-disjoint signatures is much more difficult, and has only recently been attacked by researchers. We showed that if T_1 and T_2 are universal, then it is always possible to combine the decision procedures P_1 and P_2, although only a semi-decision result is obtained in general. Further research needs to be done in order to find special cases in which decidability holds.

Acknowledgments

We thank the anonymous referee, Clark W. Barrett, Cesar Sanchez, Emilia Katz, Sriram Sankaranarayanan, Henny B. Sipma, and Matteo Slanina for useful comments.

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, by ARPA/AF contracts F33615-00-C-1693 and F33615-99-C-3014, and by NAVY/ONR contract N00014-03-1-0939.

References

1. W. Ackermann. *Solvable Cases of the Decision Problem.* North-Holland Publishing Company, 1954.
2. F. Baader and K. U. Schulz. Combining constraint solving. In H. Comon, C. Marché, and R. Treinen, editors, *Constraints in Computational Logics*, volume 2002 of *Lecture Notes in Computer Science*, pages 104–158, 2001.
3. C. W. Barrett, D. L. Dill, and J. L. Levitt. Validity checking for combinations of theories with equality. In *Formal Methods in Computer-Aided Design*, volume 1166 of *Lecture Notes in Computer Science*, pages 187–201, 1996.
4. C. W. Barrett, D. L. Dill, and A. Stump. A generalization of Shostak's method for combining decision procedures. In A. Armando, editor, *Frontiers of Combining Systems*, volume 2309 of *Lecture Notes in Computer Science*, pages 132–146. Springer, 2002.
5. E. T. Bell. Exponential numbers. *American Mathematical Monthly*, 41:411–419, 1934.
6. N. S. Bjørner. *Integrating Decision Procedures for Temporal Verification.* PhD thesis, Stanford University, 1998.
7. N. S. Bjørner, A. Browne, M. Colón, B. Finkbeiner, Z. Manna, H. B. Sipma, and T. E. Uribe. Verifying temporal properties of reactive systems: A STeP tutorial. *Formal Methods in System Design*, 16(3):227–270, 2000.
8. D. Cantone and C. G. Zarba. A new fast tableau-based decision procedure for an unquantified fragment of set theory. In R. Caferra and G. Salzer, editors, *Automated Deduction in Classical and Non-Classical Logics*, volume 1761 of *Lecture Notes in Computer Science*, pages 127–137. Springer, 2000.
9. A. Church. A note on the Entscheidungsproblem. *Journal of Symbolic Logic*, 1:101–102, 1936.
10. G. E. Collins. Quantifier elimination for the elementary theory of real closed fields by cylindrical algebraic decomposition. In H. Brakhage, editor, *Automata Theory and Formal Languages*, volume 33 of *Lecture Notes in Computer Science*, pages 134–183. Springer, 1975.

11. D. C. Cooper. Theorem proving in arithmetic without multiplication. In B. Meltzer and D. Michie, editors, *Machine Intelligence*, volume 7, pages 91–99. Edinburgh University Press, 1972.
12. D. Craigen, S. Kromodimoeljo, I. Meisels, B. Pase, and M. Saaltink. EVES: An overview. In S. Prehen and H. Toetenel, editors, *Formal Software Development Methods*, volume 552 of *Lecture Notes in Computer Science*, pages 389–405. Springer, 1991.
13. D. Cyrluk, P. Lincoln, and N. Shankar. On Shostak's decision procedure for combinations of theories. In M. A. McRobbia and J. K. Slaney, editors, *Automated Deduction – CADE-13*, volume 1104 of *Lecture Notes in Computer Science*, pages 463–477. Springer, 1996.
14. J. H. Davenport and J. Heintz. Real quantifier elimination is doubly exponential. *Journal of Symbolic Computation*, 5:29–35, 1988.
15. N. G. de Bruijn. *Asymptotic Methods in Analysis*. North-Holland Publishing Company, 1958.
16. D. L. Detlefs, K. Rustan, M. Leino, G. Nelson, and J. B. Saxe. Extended static checking. Technical Report 159, Compaq System Research Center, 1998.
17. P. Downey and R. Sethi. Assignment commands with array references. *Journal of the Association for Computing Machinery*, 25(4):652–666, 1978.
18. P. J. Downey, R. Sethi, and R. E. Tarjan. Variations on the common subexpression problem. *Journal of the Association for Computing Machinery*, 27(4):758–771, 1980.
19. H. B. Enderton. *A Mathematical Introduction to Logic*. Academic Press, 2nd edition, 2000.
20. J. Ferrante and C. Rackoff. A decision procedure for the first order theory of real addition with order. *SIAM Journal on Computing*, 4(1):69–76, 1975.
21. J.-C. Filliâtre, S. Owre, H. Rueß, and N. Shankar. ICS: Integrated Canonizer and Solver. In G. Berry, H. Comon, and F. Alain, editors, *Computer Aided Verification*, volume 2102 of *Lecture Notes in Computer Science*, pages 246–249, 2001.
22. M. J. Fischer and M. O. Rabin. Super-exponential complexity of Presburger arithmetic. In R. M. Karp, editor, *Complexity of Computation*, volume 7 of *SIAM-AMS proceedings*, pages 27–42. American Mathematical Society, 1974.
23. H. Ganzinger. Shostak light. In A. Voronkov, editor, *Automated Deduction – CADE-18*, volume 2392 of *Lecture Notes in Computer Science*, pages 332–346. Springer, 2002.
24. D. Kapur. A rewrite rule based framework for combining decision procedures. In A. Armando, editor, *Frontiers of Combining System*, volume 2309 of *Lecture Notes in Computer Science*, pages 87–102. Springer, 2002.
25. L. G. Khachiyan. A polynomial algorithm in linear programming. *Soviet Mathematics Doklady*, 20:191–194, 1979.
26. D. Kozen. Complexity of finitely presented algebras. In *Proceedings of the ninth annual ACM symposium on Theory of computing*, pages 164–177, 1977.
27. G. Kreisel and J. L. Krivine. *Elements of Mathematical Logic*. Studies in Logic and the Foundations of Mathematics. North-Holland Publishing Company, 1967.
28. S. Krstić and S. Conchon. Canonization for disjoint union of theories. Technical Report CSE-03-003, Oregon Health and Science University, 2003.
29. J.-L. Lassez and M. J. Mahler. On Fourier's algorithm for linear constraints. *Journal of Automated Reasoning*, 9(3):373–379, 1992.
30. J. L. Levitt. *Formal Verification Techniques for Digital Systems*. PhD thesis, Stanford University, 1998.

31. B. Levy, I. Filippenko, L. Marcus, and T. Menas. Using the state delta verification system (SDVS) for hardware verification. In T. F. Melham, V. Stavridou, and R. T. Boute, editors, *Theorem Prover in Circuit Design: Theory, Practice and Experience*, pages 337–360. Elsevier Science, 1992.
32. D. C. Luckham, S. M. German, F. W. von Henke, R. A. Karp, P. W. Milne, D. C. Oppen, W. Polak, and W. L. Scherlis. Stanford pascal verifier user manual. Technical Report STAN-CS-79-731, Stanford University, 1979.
33. Y. V. Matiyasevich. Diophantine representation of recursively enumerable predicates. In J. E. Fenstad, editor, *Second Scandinavian Logic Symposium*, volume 63 of *Studies in Logic and the Foundations of Mathematics*, pages 171–177. North-Holland Publishing Company, 1971.
34. J. McCarthy. Towards a mathematical science of computation. In *IFIP Congress 62*, 1962.
35. G. Nelson. Techniques for program verification. Technical Report CSL-81-10, Xerox Palo Alto Research Center, 1981.
36. G. Nelson. Combining satisfiability procedures by equality sharing. In W. W. Bledsoe and D. W. Loveland, editors, *Automated Theorem Proving: After 25 Years*, volume 29 of *Contemporary Mathematics*, pages 201–211. American Mathematical Society, 1984.
37. G. Nelson and D. C. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1(2):245–257, 1979.
38. G. Nelson and D. C. Oppen. Fast decision procedures based on congruence closure. *Journal of the Association for Computing Machinery*, 27(2):356–364, 1980.
39. D. C. Oppen. A $2^{2^{2^{pn}}}$ upper bound on the complexity of Presburger arithmetic. *Journal of Computer and System Sciences*, 16(3):323–332, 1978.
40. D. C. Oppen. Complexity, convexity and combinations of theories. *Theoretical Computer Science*, 12:291–302, 1980.
41. D. C. Oppen. Reasoning about recursively defined data structures. *Journal of the Association for Computing Machinery*, 27(3):403–411, 1980.
42. S. Owre, S. Rajan, J. M. Rushby, N. Shankar, and M. K. Srivas. PVS: Combining specification, proof checking and model checking. In R. Alur and T. A. Henzinger, editors, *Computer Aided Verification*, volume 1102 of *Lecture Notes in Computer Science*, pages 411–414. Springer, 1996.
43. C. H. Papadimitriou. On the complexity of integer programming. *Journal of the Association for Computing Machinery*, 28(4):765, 768, 1981.
44. M. Presburger. Über die vollständigkeit eines gewissen systems der arithmetik ganzer zahlen, in welchen die addition als einzige operation hervortritt. In *Comptes Rendus du Premier Congrès des Mathématicienes des Pays Slaves*, pages 92–101, 1929.
45. C. Ringeissen. Cooperation of decision procedures for the satisfiability problem. In F. Baader and K. U. Schulz, editors, *Frontiers of Combining Systems*, volume 3 of *Applied Logic Series*, pages 121–140. Kluwer Academic Publishers, 1996.
46. H. Rueß and N. Shankar. Deconstructing Shostak. In *Sixteenth Annual IEEE Symposium on Logic in Computer Science*, pages 19–28. IEEE Computer Society, 2001.
47. N. Shankar and H. Rueß. Combining Shostak theories. In S. Tison, editor, *Rewriting Techniques and Applications*, volume 2378 of *Lecture Notes in Computer Science*, pages 1–18. Springer, 2002.
48. R. E. Shostak. An algorithm for reasoning about equality. *Communications of the Association for Computing Machinery*, 21(7):583–585, 1978.

49. R. E. Shostak. A practical decision procedure for arithmetic with function symbols. *Journal of the Association for Computing Machinery*, 26(2):351–360, 1979.
50. R. E. Shostak. Deciding combination of theories. *Journal of the Association for Computing Machinery*, 31(1):1–12, 1984.
51. A. Stump, C. W. Barret, and D. L. Dill. CVC: A cooperating validity checker. In E. Brinksma and K. G. Larsen, editors, *Computer Aided Verification*, volume 2404 of *Lecture Notes in Computer Science*, pages 500–504, 2002.
52. A. Stump, C. W. Barret, D. L. Dill, and J. Levitt. A decision procedure for an extensional theory of arrays. In *Sixteenth Annual IEEE Symposium on Logic in Computer Science*, pages 29–37. IEEE Computer Society, 2001.
53. N. Suzuki and D. Jefferson. Verification decidability of Presburger array programs. *Journal of the Association for Computing Machinery*, 27(1):191–205, 1980.
54. A. Tarski. *A Decision Method for Elementary Algebra and Geometry.* University of California Press, 1951.
55. C. Tinelli. Cooperation of background reasoners in theory reasoning by residue sharing. Technical Report 02-03, Department of Computer Science, University of Iowa, 2002.
56. C. Tinelli and M. T. Harandi. A new correctness proof of the Nelson-Oppen combination procedure. In F. Baader and K. U. Schulz, editors, *Frontiers of Combining Systems*, volume 3 of *Applied Logic Series*, pages 103–120. Kluwer Academic Publishers, 1996.
57. C. Tinelli and C. Ringeissen. Unions of non-disjoint theories and combinations of satisfiability procedures. *Theoretical Computer Science*, 290(1):291–353, 2003.
58. A. Tiwari. *Decision Procedures in Automated Deduction.* PhD thesis, State University of New York at Stony Brook, 2000.
59. A. M. Turing. On computable numbers, with an application to the Entscheidungsproblem. *Proceedings of the London Mathematical Society*, 42:230–265, 1936.
60. C. G. Zarba. Combining multisets with integers. In A. Voronkov, editor, *Automated Deduction – CADE-18*, volume 2392 of *Lecture Notes in Computer Science*, pages 363–376. Springer, 2002.
61. C. G. Zarba. A tableau calculus for combining non-disjoint theories. In U. Egly and C. G. Fermüller, editors, *Automated Reasoning with Analytic Tableaux and Related Methods*, volume 2381 of *Lecture Notes in Computer Science*, pages 315–329. Springer, 2002.

Appendix

We prove the Combination Theorem 17, and then we prove the Combination Theorem for Disjoint Theories 2 as a corollary of the Combination Theorem 17.

We will use the following lemma.

Lemma 11. *Let $\mathcal{A}$ and $\mathcal{B}$ be Σ-interpretations over some set V of variables, and assume that $\mathcal{A} \cong \mathcal{B}$. Then $\varphi^{\mathcal{A}} = \varphi^{\mathcal{B}}$, for each Σ-formula φ whose free variables are in V.* □

Theorem 17 (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 $V_i = vars(\Phi_i)$.*

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. To make the notation more concise, let $\Sigma = \Sigma_1 \cap \Sigma_2$ and $V = V_1 \cap V_2$.

Next, assume that $\Phi_1 \cup \Phi_2$ is satisfiable, and let $\mathcal{M}$ be an interpretation satisfying $\Phi_1 \cup \Phi_2$. Then, by letting $\mathcal{A} = \mathcal{M}^{\Sigma_1,V_1}$ and $\mathcal{B} = \mathcal{M}^{\Sigma_2,V_2}$, we clearly have that:

- $\mathcal{A}$ satisfies Φ_1;
- $\mathcal{B}$ satisfies Φ_2;
- $\mathcal{A}^{\Sigma,V} \cong \mathcal{B}^{\Sigma,V}$.

Vice versa, assume that there exists an interpretation $\mathcal{A}$ satisfying Φ_1 and an interpretation $\mathcal{B}$ satisfying Φ_2 such that $\mathcal{A}^{\Sigma,V} \cong \mathcal{B}^{\Sigma,V}$, and let $h : A \to B$ be an isomorphism of $\mathcal{A}$ into $\mathcal{B}$. We define an interpretation $\mathcal{M}$ by letting $M = A$ and:

- for variables and constants:

$$u^{\mathcal{M}} = \begin{cases} u^{\mathcal{A}}\,, & \text{if } u \in (\Sigma_1^{\mathrm{C}} \cup V_1)\,, \\ h^{-1}(u^{\mathcal{B}})\,, & \text{if } u \in (\Sigma_2^{\mathrm{C}} \cup V_2) \setminus (\Sigma_1^{\mathrm{C}} \cup V_1)\,, \end{cases}$$

- for function symbols of arity n:

$$f^{\mathcal{M}}(a_1, \ldots, a_n) = \begin{cases} f^{\mathcal{A}}(a_1, \ldots, a_n)\,, & \text{if } f \in \Sigma_1^{\mathrm{F}}\,, \\ h^{-1}(f^{\mathcal{B}}(h(a_1), \ldots, h(a_n)))\,, & \text{if } f \in \Sigma_2^{\mathrm{F}} \setminus \Sigma_1^{\mathrm{F}}\,, \end{cases}$$

- for predicate symbols of arity n:

$$\begin{aligned} (a_1, \ldots, a_n) \in P^{\mathcal{M}} &\Longleftrightarrow (a_1, \ldots, a_n) \in P^{\mathcal{A}}\,, && \text{if } P \in \Sigma_1^{\mathrm{P}} \\ (a_1, \ldots, a_n) \in P^{\mathcal{M}} &\Longleftrightarrow (h(a_1), \ldots, h(a_n)) \in P^{\mathcal{B}}\,, && \text{if } P \in \Sigma_2^{\mathrm{P}} \setminus \Sigma_1^{\mathrm{P}}\,. \end{aligned}$$

By construction, $\mathcal{M}^{\Sigma_1,V_1} \cong \mathcal{A}$. In addition, it is easy to verify that h is an isomorphism of $\mathcal{M}^{\Sigma_2,V_2}$ into $\mathcal{B}$. Thus, by Lemma 11, $\mathcal{M}$ satisfies $\Phi_1 \cup \Phi_2$. ∎

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

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

(i) $|A| = |B|$,
(ii) $x^{\mathcal{A}} = y^{\mathcal{A}}$ *if and only if* $x^{\mathcal{B}} = y^{\mathcal{B}}$, *for every variable* $x, y \in$ *shared*(Φ_1, Φ_2). □

PROOF. Clearly, if there exists an interpretation $\mathcal{M}$ satisfying $\Phi_1 \cup \Phi_2$, then the only if direction holds by letting $\mathcal{A} = \mathcal{M}$ and $\mathcal{B} = \mathcal{M}$.

Concerning the if direction, assume that there exists a Σ_1-interpretation $\mathcal{A}$ satisfying Φ_1 and a Σ_2-interpretation $\mathcal{B}$ satisfying Φ_2 such that both (i) and (ii) hold. Also, let $V =$ *shared*(Φ_1, Φ_2).

In order to apply Theorem 17, we define a function $h : V^{\mathcal{A}} \to V^{\mathcal{B}}$ by letting $h(x^{\mathcal{A}}) = x^{\mathcal{B}}$, for every $x \in V^{\mathcal{A}}$. Note that this position is sound because property (ii) holds.

We claim that h is a bijective function. To show that h is injective, let $h(a_1) = h(a_2)$. Then there exist variables $x, y \in V$ such that $a_1 = x^{\mathcal{A}}$, $a_2 = y^{\mathcal{A}}$, and $x^{\mathcal{B}} = y^{\mathcal{B}}$. By property (ii), we have $x^{\mathcal{A}} = y^{\mathcal{A}}$, and therefore $a_1 = a_2$. To show that h is surjective, let $b \in V^{\mathcal{B}}$. Then there exists a variable $x \in V^{\mathcal{B}}$ such that $x^{\mathcal{B}} = b$. But then $h(x^{\mathcal{A}}) = b$, proving that h is surjective.

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

Clearly, by construction h' is an isomorphism of $\mathcal{A}^V$ into $\mathcal{B}^V$. Thus, we can apply Theorem 17, and obtain the existence of an interpretation $\mathcal{M}$ satisfying $\Phi_1 \cup \Phi_2$. ■