# Combining Data Structures with Nonstably Infinite Theories using Many-Sorted Logic

Silvio Ranise, Christophe Ringeissen, Calogero G. Zarba

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

# *Combining Data Structures with Nonstably Infinite Theories using Many-Sorted Logic*

Silvio Ranise — Christophe Ringeissen — Calogero Zarba

**N° 5678**

Septembre 2005

Thème SYM


ISSN 0249-6399 ISRN INRIA/RR--5678--FR+ENG

# Combining Data Structures with Nonstably Infinite Theories using Many-Sorted Logic*

Silvio Ranise† , Christophe Ringeissen‡ , Calogero Zarba§

Thème SYM — Systèmes symboliques
Projet Cassis

Rapport de recherche n° 5678 — Septembre 2005 — 39 pages

**Abstract:** Most computer programs store elements of a given nature into container-based data structures such as lists, arrays, sets, and multisets. To verify the correctness of these programs, one needs to combine a theory modeling the data structure with a theory modeling the elements. This combination can be achieved using the classic Nelson-Oppen method only if both theories are stably infinite.

The goal of this report is to relax the stable infiniteness requirement. To achieve this goal, we introduce the notion of polite theories, and we show that natural examples of polite theories include those modeling data structures such as lists, arrays, sets, and multisets. Furthemore, we provide a method that is able to combine a polite theory with any theory of the elements, regardless of whether the latter is stably infinite or not.

The results of this report generalize to many-sorted logic those recently obtained by Tinelli and Zarba for combining the so-called shiny theories with nonstably infinite theories in one-sorted logic.

**Key-words:** Combination of satisfiability procedures, Decision problems, Many-sorted logic, Automated deduction

* This work is partly supported by grants NSF ITR CCR-0113611, NSF CCR-0098114, and projects ACI GECCOO, and QSL VALDA-2.

† Silvio.Ranise@loria.fr

‡ Christophe.Ringeissen@loria.fr

§ University of New Mexico. Email: zarba@cs.unm.edu

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois, Campus scientifique,
615, rue du Jardin Botanique, BP 101, 54602 Villers-Lès-Nancy (France)
Téléphone : +33 3 83 59 30 00 —Télécopie : +33 3 83 27 83 19

# Combinaison de structures de données avec des théories non-stable infinies dans une logique multi-sortée

**Résumé :** La plupart des programmes informatiques emmagasinent des éléments d'un certain type dans des structures de données telles que listes, tableaux, ensembles et multi-ensembles. Pour vérifier la correction de ces programmes, on a besoin de combiner une théorie modélisant la structure de données avec une théorie modélisant les éléments. Cette combinaison peut être effectuée en utilisant la méthode classique de Nelson-Oppen uniquement si ces théories sont toutes les deux stable infinies.

L'objectif de ce rapport est de relacher l'hypothèse stipulant que les théories doivent être stable infinies. Pour atteindre cet objectif, nous introduisons la notion de théorie polie, et nous montrons que des exemples naturels de théories polies incluent celles modélisant des structures de données telles que listes, tableaux, ensembles et multi-ensembles. De plus, nous donnons une méthode capable de combiner une théorie polie avec une théorie pour les éléments, que cette dernière soit ou non stable infinie.

Les résultats de ce rapport généralisent au cas multi-sorté des résultats obtenus par Tinelli et Zarba permettant de combiner des théories dites brillantes avec des théories non-stable infinies dans une logique mono-sortée.

**Mots-clés :** Combinaison de procédures de satisfaisabilité, Problèmes de décision, Logique multi-sortée, Déduction automatique

# 1 Introduction

In program verification one has often to decide the satisfiability or validity of logical formulae involving data structures such as lists, arrays, sets, and multisets. These data structures can be considered as structured containers of elements of a given nature. For instance, one may want to reason about lists of integers, sets of booleans, or multisets of reals.

One way to reason about data structures over elements of a given nature is to use the Nelson-Oppen method in order to modularly combine a decision procedure for a theory $S$ modeling the data structure with a decision procedure for a theory $T$ modeling the elements. However, this solution requires that both $S$ and $T$ be *stably infinite*. Unfortunately, this requirement is not satisfied by many practically relevant theories such as, for instance, the theory of booleans, the theory of integers modulo $n$, and the theory of fixed-width bit-vectors [8].

Recently, Tinelli and Zarba [12] introduced a generalization of the one-sorted version of the Nelson-Oppen method in order to combine theories that are not stably infinite. More precisely, they introduce the notion of *shiny* theories, and prove that a shiny theory $S$ can be combined with any other arbitrary theory $T$, even if the latter is not stably infinite. They also provide a list of shiny theories which includes the theory of equality, the theory of partial orders, the theory of total orders, and the theory of bounded lattices.

Despite these promising results, Tinelli and Zarba's method has two drawbacks.

First, when combining a shiny theory $S$, one has to compute a function $mincard_S$. This function takes as input an $S$-satisfiable conjunction $\Gamma$ of literals, and returns the minimal cardinality $k$ for which there is a $T$-model of $\Gamma$ of cardinality $k$. Although $mincard_S$ is computable for a wide class of theories, its complexity is in general $NP$-hard. Due to this high complexity, it is natural to study how to avoid the computation of $mincard_S$.

Second, the notion of shininess is too strong, and it may be very difficult to find further examples of practically relevant shiny theories. We believe that this difficulty is due to the fact that the notion of shiny theories was introduced in one-sorted logic.

In this report we are interested in the problem of combining a theory $S$ modeling a data structure with a nonstably infinite theory $T$ modeling the elements. More in detail, the contributions of this report are:

1. In order to sidestep the difficulties of finding shiny theories, we operate in many-sorted logic rather than in one-sorted logic.

2. We introduce the notion of *polite* theories, and we prove that natural examples of polite theories are those modeling data structures such as lists, arrays, sets, and multisets.

3. We provide a new combination method that is able to combine a polite theory $S$ with any theory $T$, regardless of whether $T$ is stably infinite or not.

4. We generalize the notion of shininess from one-sorted logic to many-sorted logic, and we prove that—under rather weak assumptions—shininess is equivalent to politeness in one-sorted logic. The equivalence is less clear in many-sorted logic.

The crux of our combination method is to modify the Nelson-Oppen method. The nondeterministic version of this method consists in guessing an arrangement over the set of shared variables. This arrangement is used to build equalities and disequalities between variables, to constrain simultaneously the inputs of decision procedures for component theories. Our modification is related to the variables involved in an arrangement; precisely:

**Modification 1:** Guess an arrangement over an extended set of variables, and not just the shared ones. For correctness, the extended arrangement must also contain opportunely introduced fresh variables, whose role is to witness that certain facts hold for the data structure.

Our method does not require the computation of a $mincard_S$ function, and it is therefore easier to implement than the one presented in [12].

**Related work.** Implicit versions of Modification 1 were already used by Zarba in order to combine the theory of sets [14] and the theory of multisets [13] with any arbitrary theory $T$ of the elements, even if $T$ is not stably infinite.

The first explicit version of Modification 1 is due to Fontaine and Gribomont [6] who combine the theory of arrays with any other nonstably infinite theory $T$ not containing the sort array. Their result applies to conjunctions of literals not containing disequalities between terms of sort array.

The latest explicit version of Modification 1 was used by Fontaine, Ranise, and Zarba [7], in order to combine a nonstably infinite theory $T$ of the elements with the theory $T_{\mathsf{length}}$ of lists of elements with length constraints.

Baader and Ghilardi [1, 2] have recently introduced a new method for combining theories over nondisjoint signatures using many-sorted logic. Their result for theo-

ries over nondisjoint signatures—together with ours for nonstably infinite theories—shows that it is very convenient to combine theories using many-sorted logic.

**Organization of the report.** In Section 2 we introduce some preliminary notions, as well as the concept of polite theories. In Section 3 we prove some auxiliary propositions that are useful when proving that certain theories are polite. In Section 4 we present our combination method. In Section 5 we compare the notion of polite theories with the notion of shiny theories. In Sections 6–10 we prove that natural examples of polite theories are those modeling data structures, as well as the ubiquitous theory of equality. In Section 11 we draw conclusions from our work.

# 2 Preliminaries

## 2.1 Syntax

A *signature* $\Sigma$ is a triple $(S, F, P)$ where $S$ is a set of sorts, $F$ is a set of function symbols, $P$ is a set of predicate symbols, and all the symbols in $F, P$ have arities constructed using the sorts in $S$. Given a signature $\Sigma = (S, F, P)$, we write $\Sigma^{\mathrm{S}}$ for $S$, $\Sigma^{\mathrm{F}}$ for $F$, and $\Sigma^{\mathrm{P}}$ for $P$. If $\Sigma_1 = (S_1, F_1, P_1)$ and $\Sigma_2 = (S_2, F_2, P_2)$ are signatures, their *union* is the signature $\Sigma_1 \cup \Sigma_2 = (S_1 \cup S_2, F_1 \cup F_2, P_1 \cup P_2)$.

Given a signature $\Sigma$, we assume the standard notions of $\Sigma$-*term*, $\Sigma$-*literal*, and $\Sigma$-*formula*. A $\Sigma$-*sentence* is a $\Sigma$-formula with no free variables. A literal is *flat* if it is of the form $x \approx y$, $x \not\approx y$, $x \approx f(y_1, \ldots, y_n)$, $p(y_1, \ldots, y_n)$, and $\neg p(y_1, \ldots, y_n)$, where $x, y, y_1, \ldots, y_n$ are variables, $f$ is a function symbol, and $p$ is a predicate symbol.

If $t$ is a term, we denote with $vars_\sigma(t)$ the set of variables of sort $\sigma$ occurring in $t$. Similarly, if $\varphi$ is a formula, we denote with $vars_\sigma(\varphi)$ the set of free variables of sort $\sigma$ occurring in $t$. If $\varphi$ is either a term or a formula, we denote with $vars(\varphi)$ the set $\bigcup_\sigma vars_\sigma(\varphi)$. Finally, if $\Phi$ is a set of terms or a set of formulae, we let $vars_\sigma(\Phi) = \bigcup_{\varphi \in \Phi} vars_\sigma(\varphi)$ and $vars(\Phi) = \bigcup_{\varphi \in \Phi} vars(\varphi)$.

In the rest of this paper, we identify conjunctions of formulae $\varphi_1 \wedge \cdots \wedge \varphi_n$ with the set $\{\varphi_1, \ldots, \varphi_n\}$.

## 2.2 Semantics

**Definition 1.** Let $\Sigma$ be a signature, and let $X$ be a set of variables whose sorts are in $\Sigma^{\mathrm{S}}$. A $\Sigma$-INTERPRETATION $\mathcal{A}$ over $X$ is a map which interprets each sort $\sigma \in \Sigma^{\mathrm{S}}$ as a non-empty domain $A_\sigma$, each variable $x \in X$ of sort $\sigma$ as an element $x^{\mathcal{A}} \in A_\sigma$, each function symbol $f \in \Sigma^{\mathrm{F}}$ of arity $\sigma_1 \times \cdots \times \sigma_n \to \tau$ as a function

$f^{\mathcal{A}} : A_{\sigma_1} \times \cdots \times A_{\sigma_n} \to A_\tau$, and each predicate symbol $p \in \Sigma^{\mathrm{P}}$ of arity $\sigma_1 \times \cdots \times \sigma_n$ as a subset $p^{\mathcal{A}}$ of $A_{\sigma_1} \times \cdots \times A_{\sigma_n}$.

A $\Sigma$-STRUCTURE is a $\Sigma$-interpretation over an empty set of variables. □

A $\Sigma$-formula $\varphi$ over a set $X$ of variables is *satisfiable* if it is true in some $\Sigma$-interpretation over $X$. Two $\Sigma$-formulae $\varphi$ and $\psi$ over a set $X$ of variables are *equivalent* if $\varphi^{\mathcal{A}} = \psi^{\mathcal{A}}$, for all $\Sigma$-interpretations over $X$.

Let $\mathcal{A}$ be an $\Omega$-interpretation over some set $V$ of variables. For a signature $\Sigma \subseteq \Omega$ and a set of variables $U \subseteq V$, we denote with $\mathcal{A}^{\Sigma,U}$ the interpretation obtained from $\mathcal{A}$ by restricting it to interpret only the symbols in $\Sigma$ and the variables in $U$. Furthermore, we let $\mathcal{A}^{\Sigma} = \mathcal{A}^{\Sigma,\emptyset}$.

## 2.3 Theories

Following Ganzinger [9], we define theories as sets of structures rather than as sets of sentences. More formally, we give the following definition.

**Definition 2.** A $\Sigma$-THEORY is a pair $(\Sigma, \mathbf{A})$ where $\Sigma$ is a signature and $\mathbf{A}$ is a class of $\Sigma$-structures. Given a theory $T = (\Sigma, \mathbf{A})$, a $T$-INTERPRETATION is a $\Sigma$-interpretation $\mathcal{A}$ such that $\mathcal{A}^{\Sigma} \in \mathbf{A}$. □

Given a $\Sigma$-theory $T$, a $\Sigma$-formula $\varphi$ over a set $X$ of variables is *$T$-satisfiable* if it is true in some $T$-interpretation over $X$. We write $\mathcal{A} \models_T \varphi$ when $\mathcal{A}$ is a $T$-interpretation satisfying $\varphi$. Given a $\Sigma$-theory $T$, two $\Sigma$-formulae $\varphi$ and $\psi$ over a set $X$ of variables are *$T$-equivalent* if $\varphi^{\mathcal{A}} = \psi^{\mathcal{A}}$, for all $T$-interpretations over $X$.

Given a $\Sigma$-theory $T$, the *quantifier-free satisfiability problem* of $T$ is the problem of deciding, for each quantifier-free $\Sigma$-formula $\varphi$, whether or not $\varphi$ is $T$-satisfiable.

**Definition 3 (Combination).** Let $T_i = (\Sigma_i, \mathbf{A}_i)$ be a theory, for $i = 1, 2$. The COMBINATION of $T_1$ and $T_2$ is the theory $T_1 \oplus T_2 = (\Sigma, \mathbf{A})$ where $\Sigma = \Sigma_1 \cup \Sigma_2$ and $\mathbf{A} = \{\mathcal{A} \mid \mathcal{A}^{\Sigma_1} \in \mathbf{A}_1 \text{ and } \mathcal{A}^{\Sigma_2} \in \mathbf{A}_2\}$. □

If $\Phi$ is a set of $\Sigma$-sentences, we let $\mathit{Theory}^{\Sigma}(\Phi) = (\Sigma, \mathbf{A})$ be the theory such that $\mathbf{A}$ is the class of all $\Sigma$-structures satisfying $\Phi$.

**Proposition 4.** *Let $\Phi_i$ be a set of $\Sigma_i$-sentences, for $i = 1, 2$. Then*

$$\mathit{Theory}^{\Sigma_1}(\Phi_1) \oplus \mathit{Theory}^{\Sigma_2}(\Phi_2) = \mathit{Theory}^{\Sigma_1 \cup \Sigma_2}(\Phi_1 \cup \Phi_2)\,. \qquad \square$$

PROOF. Let

$$\begin{aligned}(\Sigma, \mathbf{A}_1) &= \mathit{Theory}^{\Sigma_1}(\Phi_1)\,,\\ (\Sigma, \mathbf{A}_2) &= \mathit{Theory}^{\Sigma_2}(\Phi_2)\,,\\ (\Sigma, \mathbf{A}) &= \mathit{Theory}^{\Sigma_1\cup\Sigma_2}(\Phi_1 \cup \Phi_2)\,,\\ (\Sigma, \mathbf{B}) &= \mathit{Theory}^{\Sigma_1}(\Phi_1) \oplus \mathit{Theory}^{\Sigma_2}(\Phi_2)\end{aligned}$$

Then:

$$\begin{aligned}\mathcal{A} \in \mathbf{B} \quad &\iff \quad \mathcal{A}^{\Sigma_1} \in \mathbf{A}_1 \text{ and } \mathcal{A}^{\Sigma_2} \in \mathbf{A}_2\\ &\iff \quad \mathcal{A}^{\Sigma_1} \text{ satisfies } \Phi_1 \text{ and } \mathcal{A}^{\Sigma_2} \text{ satisfies } \Phi_2\\ &\iff \quad \mathcal{A} \text{ satisfies } \Phi_1 \cup \Phi_2\\ &\iff \quad \mathcal{A} \in \mathbf{A}\,.\end{aligned}$$

■

We introduce below several classes of theories. We will see how they relate in Remark 10.

**Definition 5 (Finite model property).** Let $\Sigma$ be a signature, let $S \subseteq \Sigma^{\mathrm{S}}$ be a set of sorts, and let $T$ be a $\Sigma$-theory. We say that $T$ has the FINITE MODEL PROPERTY with respect to $S$ if for every $T$-satisfiable quantifier-free $\Sigma$-formula $\varphi$ there exists a $T$-interpretation $\mathcal{A}$ satisfying $\varphi$ such that $A_\sigma$ is finite, for each sort $\sigma \in S$. □

**Definition 6 (Stable infiniteness).** Let $\Sigma$ be a signature, let $S \subseteq \Sigma^{\mathrm{S}}$ be a set of sorts, and let $T$ be a $\Sigma$-theory. We say that $T$ is STABLY INFINITE with respect to $S$ if for every $T$-satisfiable quantifier-free $\Sigma$-formula $\varphi$ there exists a $T$-interpretation $\mathcal{A}$ satisfying $\varphi$ such that $A_\sigma$ is infinite, for each sort $\sigma \in S$. □

**Definition 7 (Smoothness).** Let $\Sigma$ be a signature, let $S = \{\sigma_1, \ldots, \sigma_n\} \subseteq \Sigma^{\mathrm{S}}$ be a set of sorts, and let $T$ be a $\Sigma$-theory. We say that $T$ is SMOOTH with respect to $S$ if:

- for every $T$-satisfiable quantifier-free $\Sigma$-formula $\varphi$,
- for every $T$-interpretation $\mathcal{A}$ satisfying $\varphi$,
- for every cardinal number $\kappa_1, \ldots, \kappa_n$ such that $\kappa_i \geq |A_{\sigma_i}|$, for $i = 1, \ldots, n$,

there exists a $T$-interpretation $\mathcal{B}$ satisfying $\varphi$ such that

$$|B_{\sigma_i}| = \kappa_i\,, \qquad \text{for } i = 1, \ldots, n\,.$$ □

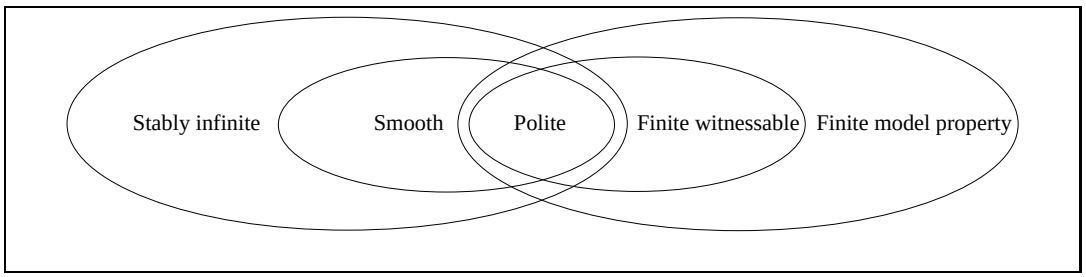


**Figure 1:** Relationships between classes of theories.

**Definition 8 (Finite witnessability).** Let $\Sigma$ be a signature, let $S \subseteq \Sigma^{\mathrm{S}}$ be a set of sorts, and let $T$ be a $\Sigma$-theory. We say that $T$ is FINITELY WITNESSABLE with respect to $S$ if there exists a computable function *witness* that for every quantifier-free $\Sigma$-formula $\varphi$ returns a quantifier-free $\Sigma$-formula $\psi = \mathit{witness}(\varphi)$ such that:

(i) $\varphi$ and $(\exists \bar{v})\psi$ are $T$-equivalent, where $\bar{v} = \mathit{vars}(\psi) \setminus \mathit{vars}(\varphi)$;

(ii) if $\psi$ is $T$-satisfiable then there exists a $T$-interpretation $\mathcal{A}$ satisfying $\psi$ such that $A_\sigma = [\mathit{vars}_\sigma(\psi)]^{\mathcal{A}}$, for each $\sigma \in S$. □

**Definition 9 (Politeness).** Let $\Sigma$ be a signature, let $S \subseteq \Sigma^{\mathrm{S}}$ be a set of sorts, and let $T$ be a $\Sigma$-theory. We say that $T$ is POLITE with respect to $S$ if it is both smooth and finitely witnessable with respect to $S$. □

**Remark 10.** Let $\Sigma$ be a signature, let $S \subseteq \Sigma^{\mathrm{S}}$, and let $T$ be a $\Sigma$-theory. Then the following holds (cf. Figure 1):

- If $T$ is smooth with respect to $S$ then $T$ is stably infinite with respect to $S$.
- If $T$ is finitely witnessable with respect to $S$ then $T$ has the finite model property with respect to $S$. □

# 3 Flat literals

In the rest of this report we will prove that several theories are polite.

For convenience, when proving that a $\Sigma$-theory $T$ is smooth with respect to a set $S$ of sorts, we will restrict ourselves to conjunctions of flat $\Sigma$-literals. Furthermore, when proving that $T$ is finitely witnessable with respect to $S$, we will define the

function $witness_T$ by restricting ourselves to conjunctions $\Gamma$ of flat $\Sigma$-literals such that $vars_\sigma(\Gamma) \neq \emptyset$, for each sort $\sigma \in S$.

The following two propositions show that this can be done without loss of generality.

**Proposition 11.** *Let $\Sigma$ be a signature, let $S = \{\sigma_1, \ldots, \sigma_n\} \subseteq \Sigma^S$ be a set of sorts, and let $T$ be a $\Sigma$-theory. Assume that for every conjunction $\Gamma$ of flat $\Sigma$-literals, for every $T$-interpretation $\mathcal{A}$ satisfying $\Gamma$, for every sort $\tau \in S$, and for every cardinal number $\kappa > |A_\tau|$, there exists a $T$-interpretation $\mathcal{B}$ satisfying $\Gamma$ such that*

$$|B_\tau| = \kappa\,,$$

*and*

$$|B_\sigma| = |A_\sigma|\,, \qquad \text{for } \sigma \in S \setminus \{\tau\}\,.$$

*Then $T$ is smooth with respect to $S$.* □

PROOF. It suffices to note that every quantifier-free $\Sigma$-formula is $T$-equivalent to a DNF $\Gamma_1 \vee \cdots \vee \Gamma_n$ such that all the $\Gamma_i$ belong to $L$. ■

**Proposition 12.** *Let $\Sigma$ be a signature, let $S = \{\sigma_1, \ldots, \sigma_n\} \subseteq \Sigma^S$ be a set of sorts, and let $T$ be a $\Sigma$-theory. Also, let $L$ be the set of all conjunctions $\Gamma$ of flat $\Sigma$-literals such that $vars_\sigma(\Gamma) \neq \emptyset$, for each sort $\sigma \in S$.*

*Assume that there exists a computable function $w$ that, for every conjunction $\Gamma$ in $L$, returns a quantifier-free $\Sigma$-formula $\psi = w(\Gamma)$ such that:*

*(i) $\Gamma$ and $(\exists \bar{v})\psi$ are $T$-equivalent, where $\bar{v} = vars(\psi) \setminus vars(\Gamma)$;*

*(ii) if $\psi$ is $T$-satisfiable then there exists a $T$-interpretation $\mathcal{A}$ satisfying $\psi$ such that $A_\sigma = [vars_\sigma(\psi)]^{\mathcal{A}}$, for each $\sigma \in S$.*

*Then $T$ is finitely witnessable with respect to $S$.* □

PROOF. We want to define a witness function *witness* on all quantifier-free $\Sigma$-formulae by using as a black box the function $w$ defined on $L$.

To do so, let $\varphi$ be a quantifier-free $\Sigma$-formula, and perform the following:

- convert $\varphi$ into a $T$-equivalent DNF $\Gamma_1 \vee \cdots \vee \Gamma_n$ such that $vars_\sigma(\Gamma) \neq \emptyset$, for each $\sigma \in S$;
- let $witness(\varphi) = w(\Gamma_1) \vee \cdots \vee w(\Gamma_n)$. ■

# 4 The combination method

Let $T_i$ be a $\Sigma_i$-theory, for $i = 1, 2$, and let $S = \Sigma_1^{\mathrm{S}} \cap \Sigma_2^{\mathrm{S}}$. Assume that:

- the quantifier-free satisfiability problem of $T_i$ is decidable, for $i = 1, 2$;
- $\Sigma_1^{\mathrm{F}} \cap \Sigma_2^{\mathrm{F}} = \emptyset$ and $\Sigma_1^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}} = \emptyset$;
- $T_2$ is polite with respect to $S$.

In this section we describe a method for combining the decision procedures for the quantifier-free satisfiability problems of $T_1$ and of $T_2$ in order to decide the quantifier-free satisfiability problem of $T_1 \oplus T_2$. Without loss of generality, we restrict ourselves to conjunctions of literals.

The combination method consists of four phases: *variable abstraction*, *witness introduction*, *decomposition*, and *check*.

**First phase: variable abstraction.** Let $\Gamma$ be a conjunction of $(\Sigma_1 \cup \Sigma_2)$-literals. The output of the variable abstraction phase is a conjunction $\Gamma_1 \cup \Gamma_2$ satisfying the following properties:

(a) each literal in $\Gamma_i$ is a $\Sigma_i$-literal, for $i = 1, 2$;

(b) $\Gamma_1 \cup \Gamma_2$ is $(T_1 \oplus T_2)$-satisfiable if and only if $\Gamma$ is $(T_1 \oplus T_2)$-satisfiable.

Note that properties (a) and (b) can be effectively enforced with the help of fresh variables. We call $\Gamma_1 \cup \Gamma_2$ a conjunction of literals in *separate* form.

**Second phase: witness introduction.** Let $\Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form returned in the variable abstraction phase. In the witness introduction phase we compute $\psi_2 = \mathit{witness}_{T_2}(\Gamma_2)$, and we output $\Gamma_1 \cup \{\psi_2\}$. Intuitively, this phase introduces the fresh variables in $\mathit{vars}(\psi_2) \setminus \mathit{vars}(\Gamma)$, whose role is to witness that certain facts hold for the polite theory $T_2$.[1]

[1] For instance, in the theory of arrays a literal $a \not\approx_{\mathsf{array}} b$ implies that there is an index $i$ such that $\mathsf{read}(a, i) \not\approx \mathsf{read}(b, i)$. Then, $i$ can be thought of as a witness of $a \not\approx_{\mathsf{array}} b$.

**Third phase: decomposition.** Let $\Gamma_1 \cup \{\psi_2\}$ be the conjunction obtained in the witness introduction phase. Let $V_\sigma = vars_\sigma(\psi_2)$ for each $\sigma \in S$, and let $V = \bigcup_{\sigma \in S} V_\sigma$. In the decomposition phase we nondeterministically guess a family $E$ of equivalence relations $E = \{E_\sigma \subseteq V_\sigma \times V_\sigma \mid \sigma \in S\}$. Then, we construct the *arrangement* of $V$ induced by $E$, defined by

$$\begin{aligned} arr(V,E) = \{&x \approx y \mid (x,y) \in E_\sigma \text{ and } \sigma \in S\} \cup \\ &\{x \not\approx y \mid (x,y) \in (V_\sigma \times V_\sigma) \setminus E_\sigma \text{ and } \sigma \in S\}\,, \end{aligned}$$

and we output the conjunction $\Gamma_1 \cup \{\psi_2\} \cup arr(V,E)$.

**Fourth phase: check.** Let $\Gamma_1 \cup \{\psi_2\} \cup arr(V,E)$ be a conjunction obtained in the decomposition phase. The check phase consists in performing the following steps:

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

**Step 2.** If $\{\psi_2\} \cup arr(V,E)$ is $T_2$-satisfiable go to the next step; otherwise output `fail`.

**Step 3.** output `succeed`.

### 4.1 An example

Let $\Sigma_1$ be the signature containing a sort $\mathsf{elem}$, as well as two constant symbols $a$ and $b$ of sort $\mathsf{elem}$. Consider the $\Sigma_1$-theory $T_1 = Theory^{\Sigma_1}(\Phi_1)$, where

$$\Phi_1 = \{(\forall_{\mathsf{elem}}\ x)(x \approx a\ \vee\ x \approx b)\}\ .$$

Clearly, for every $T_1$-interpretation $\mathcal{A}$, we have $|A_{\mathsf{elem}}| \leq 2$. Therefore, $T_1$ is not stably infinite with respect to $\{\mathsf{elem}\}$.

Next, consider the $\Sigma_{\mathsf{set}}$-theory $T_{\mathsf{set}}$ of sets of elements. The signature $\Sigma_{\mathsf{set}}$ contains, among other set-theoretical symbols, a sort $\mathsf{elem}$ for elements, and a sort $\mathsf{set}$ for sets of elements. The theory $T_{\mathsf{set}}$ will be defined more formally in Subsection 9. For this example, it suffices to know that $T_{\mathsf{set}}$ is polite with respect to $\{\mathsf{elem}\}$.

Next, consider the following conjunction $\Gamma$ of $(\Sigma_1 \cup \Sigma_{\mathsf{set}})$-literals:

$$\Gamma = \left\{ \begin{array}{l} a \approx b\,, \\ x \not\approx \emptyset\,, \\ y \not\approx \emptyset\,, \\ x \cap y \approx \emptyset \end{array} \right\}\,,$$

where $x$ and $y$ are $\mathsf{set}$-variables.

Note that $\Gamma$ is $(T_1 \oplus T_{\mathsf{set}})$-unsatisfiable. To see this, assume by contradiction that $\mathcal{A}$ is a $(T_1 \oplus T_{\mathsf{set}})$-interpretation such that $\Gamma$ is true in $\mathcal{A}$. By the first literal in $\Gamma$, we have $|A_{\mathsf{elem}}| = 1$. However, by the three last literals in $\Gamma$, we have $|A_{\mathsf{elem}}| \geq 2$, a contradiction.

We want to formally detect that $\Gamma$ is $(T_1 \oplus T_{\mathsf{set}})$-unsatisfiable by using our combination method.

Since all literals in $\Gamma$ are either $\Sigma_1$-literals or $\Sigma_{\mathsf{set}}$-literals, in the variable abstraction phase we do not need to introduce fresh variables, and we simply return the two conjunctions:

$$\Gamma_1 = \left\{ \; a \approx b \; \right\}, \qquad\qquad \Gamma_{\mathsf{set}} = \left\{ \begin{array}{l} x \not\approx \emptyset\,, \\ y \not\approx \emptyset\,, \\ x \cap y \approx \emptyset \end{array} \right\}.$$

In the witness introduction phase we need to compute $\mathit{witness}_{\mathsf{set}}(\Gamma_{\mathsf{set}})$. The intuition behind the computation of $\mathit{witness}_{\mathsf{set}}(\Gamma_{\mathsf{set}})$ is as follows.[2]

The literal $x \not\approx \emptyset$ implies the existence of an element $w_x$ in $x$. Likewise, the literal $y \not\approx \emptyset$ implies the existence of an element $w_y$ in $y$. The output of $\mathit{witness}_{\mathsf{set}}(\Gamma_{\mathsf{set}})$ is a conjunction $\Delta_{\mathsf{set}}$ that makes explicit the existence of the elements $w_x$ and $w_y$. We can do this by letting

$$\Delta_{\mathsf{set}} = \left\{ \begin{array}{l} w_x \in x\,, \\ w_y \in y\,, \\ x \cap y \approx \emptyset \end{array} \right\}.$$

Note that $\Gamma_{\mathsf{set}}$ and $(\exists_{\mathsf{elem}}\; w_x)(\exists_{\mathsf{elem}}\; w_y)\Delta_{\mathsf{set}}$ are $T_{\mathsf{set}}$-equivalent.

In the decomposition phase we need to guess an equivalence relation $E_{\mathsf{elem}}$ over the variables in $\mathit{vars}_{\mathsf{elem}}(\Delta_{\mathsf{set}})$. Since $\mathit{vars}_{\mathsf{elem}}(\Delta_{\mathsf{set}}) = \{w_x, w_y\}$, there are two possible choices: either we guess $(w_x, w_y) \in E_{\mathsf{elem}}$ or we guess $(w_x, w_y) \notin E_{\mathsf{elem}}$.

If we guess $(w_x, w_y) \in E_{\mathsf{elem}}$ then we have that $\Delta_{\mathsf{set}} \cup \{w_x \approx w_y\}$ is $T_{\mathsf{set}}$-unsatisfiable, and we will output `fail` in step 2 of the check phase. If instead we guess $(w_x, w_y) \notin E_{\mathsf{elem}}$ then we have that $\Gamma_1 \cup \{w_x \not\approx w_y\}$ is $T_1$-unsatisfiable, and we will output `fail` in step 1 of the check phase.

Since the check phase outputs `fail` for any equivalence relation $E_{\mathsf{elem}}$ of $\mathit{vars}_{\mathsf{elem}}(\Delta_{\mathsf{set}})$, our combination method correctly concludes that $\Gamma$ is $(T_1 \oplus T_{\mathsf{set}})$-unsatisfiable.

[2] A formal definition of a function $\mathit{witness}_{\mathsf{set}}$ can be found in Subsection 9. For this example, we prefer to stick to intuitive arguments.

### 4.2 Correctness and complexity

The correctness of our combination method is based on the following Combination Theorem, which is a particular case of a combination result holding for order-sorted logic [11].

**Theorem 13 (Combination).** *Let $\Sigma_1$ and $\Sigma_2$ be signatures such that $\Sigma_1^{\mathrm{F}} \cap \Sigma_2^{\mathrm{F}} = \emptyset$ and $\Sigma_1^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}} = \emptyset$. Also, let $\Phi_i$ be a set of $\Sigma_i$-formulae, for $i = 1, 2$. Then $\Phi_1 \cup \Phi_2$ is satisfiable if and only if there exists an interpretation $\mathcal{A}$ satisfying $\Phi_1$ and an interpretation $\mathcal{B}$ satisfying $\Phi_2$ such that:*

*(i) $|A_\sigma| = |B_\sigma|$, for every $\sigma \in \Sigma_1^{\mathrm{S}} \cap \Sigma_2^{\mathrm{S}}$;*

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

**Proposition 14.** *Let $T_i$ be a $\Sigma_i$-theory such that $\Sigma_1^{\mathrm{F}} \cap \Sigma_2^{\mathrm{F}} = \emptyset$ and $\Sigma_1^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}} = \emptyset$, for $i = 1, 2$. Assume that $T_2$ is polite with respect to $S = \Sigma_1^{\mathrm{S}} \cap \Sigma_2^{\mathrm{S}}$. Also, let $\Gamma_1 \cup \Gamma_2$ be a conjunction of literals in separate form, and let $\psi_2 = witness_{T_2}(\Gamma_2)$. Finally, let $V_\sigma = vars_\sigma(\psi_2)$, for each $\sigma \in S$, and let $V = \bigcup_{\sigma \in S} V_\sigma$. Then the following are equivalent:*

1. *$\Gamma_1 \cup \Gamma_2$ is $(T_1 \oplus T_2)$-satisfiable;*
2. *There exists a family $E$ of equivalence relations*

$$E = \{E_\sigma \subseteq V_\sigma \times V_\sigma \mid \sigma \in S\},$$

*such that $\Gamma_1 \cup arr(V, E)$ is $T_1$-satisfiable and $\{\psi_2\} \cup arr(V, E)$ is $T_2$-satisfiable.*

□

Proof. ($1 \Rightarrow 2$). Assume that $\Gamma_1 \cup \Gamma_2$ is $(T_1 \oplus T_2)$-satisfiable. Let $\bar{v} = vars(\psi_2) \setminus vars(\Gamma_2)$. Since $\Gamma_2$ and $(\exists \bar{v})\psi_2$ are $T_2$-equivalent, it follows that $\Gamma_1 \cup \{\psi_2\}$ is also $(T_1 \oplus T_2)$-satisfiable. Thus, we can fix a $(T_1 \oplus T_2)$-interpretation $\mathcal{A}$ satisfying $\Gamma_1 \cup \{\psi_2\}$. Next, let $E = \{E_\sigma \mid \sigma \in S\}$ where

$$E_\sigma = \{(x, y) \mid x, y \in V_\sigma \text{ and } x^{\mathcal{A}} = y^{\mathcal{A}}\}, \qquad \text{for } \sigma \in S.$$

By construction, we have that $\Gamma_1 \cup arr(V, E)$ is $T_1$-satisfiable and $\{\psi_2\} \cup arr(V, E)$ is $T_2$-satisfiable.

($2 \Rightarrow 1$). Let $\mathcal{A}$ be a $T_1$-interpretation satisfying $\Gamma_1 \cup arr(V, E)$, and let $\mathcal{B}$ be a $T_2$-interpretation satisfying $\{\psi_2\} \cup arr(V, E)$. Since $T_2$ is finitely witnessable, we can assume without loss of generality that $B_\sigma = V_\sigma^{\mathcal{B}}$, for each $\sigma \in S$.

Thus, for each $\sigma \in S$, we have

$$\begin{aligned} |B_\sigma| &= |V_\sigma^{\mathcal{B}}| && \text{since } B_\sigma = V_\sigma^{\mathcal{B}} \\ &= |V_\sigma^{\mathcal{A}}| && \text{since both } \mathcal{A} \text{ and } \mathcal{B} \text{ satisfy } arr(V,E) \\ &\leq |A_\sigma| && \text{since } V_\sigma^{\mathcal{A}} \subseteq A_\sigma\,. \end{aligned}$$

But then, by the smoothness of $T_2$, there exists a $T_2$-interpretation $\mathcal{C}$ satisfying $\{\psi_2\} \cup arr(V,E)$ such that $|C_\sigma| = |A_\sigma|$, for each $\sigma \in S$. We can therefore apply Theorem 13 to $\mathcal{A}$ and $\mathcal{C}$, obtaining the existence of a $(T_1 \oplus T_2)$-interpretation $\mathcal{F}$ satisfying $\Gamma_1 \cup \{\psi_2\} \cup arr(V,E)$. Since $\Gamma_2$ and $(\exists \bar{v})\psi_2$ are $T_2$-equivalent, it follows that $\mathcal{F}$ also satisfies $\Gamma_1 \cup \Gamma_2$. ■

Using Proposition 14 and the fact that our combination method is terminating, we obtain the correctness of our combination method.

**Theorem 15 (Correctness and complexity).** *Let $T_i$ be a $\Sigma_i$-theory, for $i = 1, 2$. Assume that:*

- *the quantifier-free satisfiability problem of $T_i$ is decidable, for $i = 1, 2$;*
- *$\Sigma_1^{\mathrm{F}} \cap \Sigma_2^{\mathrm{F}} = \emptyset$ and $\Sigma_1^{\mathrm{P}} \cap \Sigma_2^{\mathrm{P}} = \emptyset$;*
- *$T_2$ is polite with respect to $\Sigma_1^{\mathrm{S}} \cap \Sigma_2^{\mathrm{S}}$.*

*Then the quantifier-free satisfiability problem of is decidable.*

*Moreover, if the quantifier-free satisfiability problems of $T_1$ and of $T_2$ are in NP, and $witness_{T_2}$ is computable in polynomial time, then the quantifier-free satisfiability problem of $T_1 \oplus T_2$ is NP-complete.* □

PROOF. Clearly, the decidability of the quantifier-free satisfiability problem of $T_1 \oplus T_2$ follows by Proposition 14 and the fact that our combination method is terminating.

Concerning $NP$-hardness, note that if we can solve the quantifier-free satisfiability problem of $T_1 \oplus T_2$, then we can also solve propositional satisfiability.

Concerning membership in $NP$, assume that the quantifier-free satisfiability problems of $T_1$ and of $T_2$ are in $NP$, and that $witness_{T_2}$ is computable in polynomial time. Without loss of generality, it is enough to show that in nondeterministic polynomial time we can check the $(T_1 \oplus T_2)$-satisfiability of conjunctions of $(\Sigma_1 \cup \Sigma_2)$-literals. To see this, note that the execution of our combination method requires to guess an arrangement over a set of variables whose cardinality is polynomial with respect to the size of the input. This guess can be done in nondeterministic polynomial time.

■

Theorem 15 can be repeatedly applied to consider the union of $n$ theories $T_1 \oplus \cdots \oplus T_n$, where $T_2, \ldots, T_n$ are polite with respect to the set of shared sorts. This leads to the following generalization of Theorem 15 for $n$ theories.

**Theorem 16.** *Let $n \geq 2$, and let $T_i$ be a $\Sigma_i$-theory, for $1 \leq i \leq n$. Also, let $S = \bigcup_{i \neq j}(\Sigma_i^{\mathrm{S}} \cap \Sigma_j^{\mathrm{S}})$. Assume that:*

- *the quantifier-free satisfiability problem of $T_i$ is decidable, for $1 \leq i \leq n$;*
- *$\bigcup_{i \neq j}(\Sigma_i^{\mathrm{S}} \cap \Sigma_j^{\mathrm{S}}) = \bigcap_i \Sigma_i^{\mathrm{S}}$;*
- *$\Sigma_i^{\mathrm{F}} \cap \Sigma_j^{\mathrm{F}} = \emptyset$ and $\Sigma_i^{\mathrm{P}} \cap \Sigma_j^{\mathrm{P}} = \emptyset$, for $1 \leq i < j \leq n$;*
- *$T_i$ is polite with respect to $S$, for $2 \leq i \leq n$.*

*Then the quantifier-free satisfiability problem of $T_1 \oplus \cdots \oplus T_n$ is decidable.*

*Moreover, if the quantifier-free satisfiability problem of $T_i$ is in NP, for $1 \leq i \leq n$, and $witness_{T_i}$ is computable in polynomial time, for $2 \leq i \leq n$, then the quantifier-free satisfiability problem of $T_1 \oplus \cdots \oplus T_n$ is NP-complete.* □

Proof. We proceed by induction on $n$. If $n = 2$ we can apply our combination method to $T_1$ and $T_2$, and the claim follows by Theorem 15. If instead $n > 2$, it suffices to apply our combination method first to $T_1$ and $T_2$, and subsequently to $T_1 \oplus T_2$, $T_3$, ..., $T_n$. ■

## 5 Shiny theories

Shiny theories were introduced by Tinelli and Zarba [12] in order to extend the one-sorted version of the Nelson-Oppen method to the combination of nonstably infinite theories. Shiny theories are interesting because every shiny theory $S$ can be combined with any other theory $T$, even if the latter is not stably infinite.

The notion of shininess was originally introduced in one-sorted logic, and in this section we generalize it to many-sorted logic. We also prove that, under rather weak assumptions, shininess is equivalent to politeness in one-sorted logic. The equivalence is less clear in many-sorted logic.

**Definition 17.** Let $T$ be a $\Sigma$-theory, let $S \subseteq \Sigma^{\mathrm{S}}$, and let $\varphi$ be a $T$-satisfiable quantifier-free $\Sigma$-formula. We denote with $mincard_{T,S}(\varphi)$ the minimum of the following set of cardinal numbers:

$$\left\{ \left( \max_{\sigma \in S} |A_\sigma| \right) \;\middle|\; \mathcal{A} \models_T \varphi \right\}. \qquad \square$$

**Remark 18.** Let $T$ be a $\Sigma$-theory that has the finite model property with respect to $S$. Then, for every $T$-satisfiable quantifier-free $\Sigma$-formula $\varphi$, we have $mincard_{T,S}(\varphi) \in \mathbb{N}^+$. □

**Definition 19 (Shininess).** Let $\Sigma$ be a signature, let $S \subseteq \Sigma^{\mathrm{S}}$ be a set of sorts, and let $T$ be a $\Sigma$-theory. We say that $T$ is SHINY with respect to $S$ if:

- $T$ is smooth with respect to $S$;
- $T$ has the finite model property with respect to $S$;
- $mincard_{T,S}$ is computable. □

The following proposition shows that shininess always implies politeness.

**Proposition 20.** *Let $T$ be a shiny theory with respect to a set $S$ of sorts. Then $T$ is polite with respect to $S$.* □

PROOF. By assumption, $T$ is smooth with respect to $S$. To prove that $T$ is also finitely witnessable with respect to $S$, let $\varphi$ be a $T$-satisfiable quantifier-free $\Sigma$-formula, and let $n = mincard_{T,S}(\varphi)$.

Then there exists a $T$-interpretation $\mathcal{A}$ satisfying $\varphi$ such that $|A_\sigma| \leq n$, for each $\sigma \in S$. Therefore, for each $\sigma \in S$, we can let $A_\sigma = \{a^\sigma_1, \ldots, a^\sigma_{k_\sigma}\}$, with $k_\sigma < n$.

For each sort $\sigma \in S$, let $w^\sigma_1, \ldots, w^\sigma_n$ be fresh variables of sort $\sigma$ not occurring in $\varphi$. Consider the formula:

$$\psi : \quad \varphi \ \wedge \ \bigwedge_{\sigma \in S} \bigwedge_{i=1}^{n} (w^\sigma_i \approx w^\sigma_i)\,.$$

Clearly, $\varphi$ and $(\exists \bar{w})\psi$ are $T$-equivalent, where $\bar{w} = vars(\psi) \setminus vars(\varphi)$. Moreover, $\psi$ is true in the $T$-interpretation $\mathcal{B}$ obtained by extending $\mathcal{A}$ as follows:

$$(w^\sigma_i)^{\mathcal{B}} = \begin{cases} a^\sigma_i\,, & \text{if } i \leq k_\sigma\,, \\ a^\sigma_1\,, & \text{if } i > k_\sigma\,. \end{cases}$$

But then, we can define a witness function for $T$ by letting $witness(\varphi) = \psi$. ■

The following proposition establishes sufficient conditions under which politeness implies shininess.

**Proposition 21.** *Let $\Sigma$ be a signature, let $S \subseteq \Sigma^{\mathrm{S}}$ be a set of sorts, and let $T$ be a $\Sigma$-theory. Assume that:*

- $\Sigma^{\mathrm{S}} = S$;
- *$\Sigma$ is finite;*
- *For each $\Sigma$-interpretation $\mathcal{A}$ such that $\bigcup_{\sigma \in S} A_\sigma$ is finite, it is decidable to check whether $\mathcal{A}$ is a $T$-interpretation or not;*
- *$T$ is polite with respect to $S$.*

*Then $T$ is shiny with respect to $S$.* □

PROOF. By assumption, $T$ is smooth with respect to $S$. Also, $T$ has the finite model property with respect to $S$.

Next, we claim that the function $mincard_{T,S}$ can be effectively computed by the procedure MINCARD in Figure 2. To see this, we need to show that the procedure MINCARD is terminating and partially correct.

Concerning termination, just note that since $\Sigma^{\mathrm{S}} = S$, it follows that, for each $k > 0$, the number of interpretations enumerated (modulo isomorphism) in line 4 is finite.

Concerning partial correctness, assume that the procedure MINCARD exits at line 6. Then there exists an integer $k$ such that $\varphi^{\mathcal{A}} = \mathit{true}$, for some $T$-interpretation $\mathcal{A}$ such that $|A_\sigma| \leq k$, for all $\sigma \in S$. Moreover, for all $T$-interpretations $\mathcal{B}$ such that $|B_\sigma| \leq k - 1$, for all $\sigma \in S$, we have $\varphi^{\mathcal{B}} = \mathit{false}$. Therefore, $mincard_{T,S}(\varphi) = k$.

Next, assume that the procedure MINCARD exits at line 7. It follows that for all $T$-interpretations $\mathcal{B}$ such that $|B_\sigma| \leq n - 1$, for all $\sigma \in S$, we have $\varphi^{\mathcal{B}} = \mathit{false}$. This implies that $mincard_{T,S}(\varphi) \geq n$. Moreover, since

$$n = \max\{j \mid j = |vars_\sigma(witness(\varphi))| \text{ and } \sigma \in S\} ,$$

it follows that there exists a $T$-interpretation $\mathcal{A}$ such that $\varphi^{\mathcal{A}} = \mathit{true}$ and $|A_\sigma| \leq n$, for all $\sigma \in S$. This implies that $mincard_{T,S}(\varphi) \leq n$.

Since $mincard_{T,S}(\varphi) \geq n$ and $mincard_{T,S}(\varphi) \leq n$, we obtain $mincard_{T,S}(\varphi) = n$. ■

When $\left|\Sigma^S\right| = 1$, Proposition 21 tells us that in the one-sorted case politeness and shininess are the same concept for all practical purposes. When $\left|\Sigma^S\right| > 1$, the hypothesis $\Sigma^{\mathrm{S}} = S$ may be too strong. Consequently, the equivalence between politeness and shininess is less clear in the many-sorted case.

**Input:** A $T$-satisfiable quantifier-free $\Sigma$-formula $\varphi$
**Output:** $mincard_{T,S}(\varphi)$

```
1: procedure MINCARD(φ)
2:     n ← max{j | j = |vars_σ(witness(φ))| and σ ∈ S}
3:     for k ← 1 to n − 1 do
4:         for all Σ-interpretations A over vars(φ) s.t. k = max_{σ∈S} |A_σ| do
5:             if A ⊨_T φ then
6:                 return k
7:     return n
```

**Figure 2:** A procedure for computing $mincard_{T,\sigma}$.

# 6 Equality

**Definition 22.** The THEORY OF EQUALITY with signature $\Sigma$ is the theory $T_{\approx}^{\Sigma} = \langle \Sigma, \mathbf{A} \rangle$, where $\mathbf{A}$ is the class of all $\Sigma$-structures. □

## 6.1 Smoothness

**Proposition 23.** *Let $\Sigma$ be a signature, and let $\tau \in \Sigma^{\mathrm{S}}$. Also, let $\Gamma$ be a satisfiable conjunction of flat $\Sigma$-literals, let $\mathcal{A}$ be a $\Sigma$-interpretation satisfying $\Gamma$, and let $\kappa > |A_\tau|$.*

*Then there exists a $\Sigma$-interpretation $\mathcal{B}$ satisfying $\Gamma$ such that*

$$|B_\sigma| = \begin{cases} \kappa\,, & \text{if } \sigma = \tau\,, \\ |A_\sigma|\,, & \text{otherwise.} \end{cases}$$

□

PROOF. Let $V_\sigma = vars_\sigma(\Gamma)$, for $\sigma \in \Sigma^{\mathrm{S}}$, and let $V = \bigcup_{\sigma \in \Sigma^{\mathrm{S}}} V_\sigma$. We construct a $\Sigma$-interpretation $\mathcal{B}$ over $V$ as follows. Fix a set $A'$ such that $|A_\tau \cup A'| = \kappa$, and let

$$B_\sigma = \begin{cases} A_\tau \cup A'\,, & \text{if } \sigma = \tau\,, \\ A_\sigma\,, & \text{otherwise}\,, \end{cases}$$

and

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

In order to define $\mathcal{B}$ over the symbols in $\Sigma$, fix an element $a_0^\sigma$ in $A_\sigma$, for each $\sigma \in \Sigma^{\mathrm{S}}$. Then, we let:

- for function symbols $f$ of arity $\sigma_1 \times \cdots \times \sigma_n \to \sigma$:

$$f^{\mathcal{B}}(a_1, \ldots, a_n) = \begin{cases} f^{\mathcal{A}}(a_1, \ldots, a_n)\,, & \text{if } a_1 \in A_{\sigma_1}, \ldots, a_n \in A_{\sigma_n}\,, \\ a_0^{\sigma}\,, & \text{otherwise}\ , \end{cases}$$

- for predicate symbols $p$ of arity $\sigma_1 \times \cdots \times \sigma_n$:

$$(a_1, \ldots, a_n) \in p^{\mathcal{B}} \iff a_1 \in A_{\sigma_1}, \ldots, a_n \in A_{\sigma_n} \text{ and } (a_1, \ldots, a_n) \in p^{\mathcal{A}}\,.$$

By construction, $\mathcal{B}$ is a $T^{\Sigma}_{\approx}$-interpretation such that $|B_\tau| = \kappa$ and $|B_\sigma| = |A_\sigma|$, for $\sigma \neq \tau$. Next, we show that $\mathcal{B}$ satisfies all literals in $\Gamma$.

**Literals of the form $x = y$ and $x \neq y$.** Immediate.

**Literals of the form $x = f(y_1, \ldots, y_n)$, where $f$ is a function symbol of arity $\sigma_1 \times \cdots \times \sigma_n \to \sigma$.** We have:

$$\begin{aligned} x^{\mathcal{B}} &= x^{\mathcal{A}} \\ &= f^{\mathcal{A}}\left(y_1^{\mathcal{A}}, \ldots, y_n^{\mathcal{A}}\right) \\ &= f^{\mathcal{B}}\left(y_1^{\mathcal{B}}, \ldots, y_n^{\mathcal{B}}\right) \qquad \text{since } \left(y_1^{\mathcal{A}}, \ldots, y_n^{\mathcal{A}}\right) \in A_{\sigma_1} \times \cdots \times A_{\sigma_n}\,. \end{aligned}$$

**Literals of the form $p(y_1, \ldots, y_n)$ and $\neg p(y_1, \ldots, y_n)$, where $p$ is a predicate symbol of arity $\sigma_1 \times \cdots \times \sigma_n$.** Just observe that, since $\left(y_1^{\mathcal{A}}, \ldots, y_n^{\mathcal{A}}\right) \in A_{\sigma_1} \times \cdots \times A_{\sigma_n}$, we have that $(y_1^{\mathcal{A}}, \ldots, y_n^{\mathcal{A}}) \in p^{\mathcal{A}}$ iff $(y_1^{\mathcal{B}}, \ldots, y_n^{\mathcal{B}}) \in p^{\mathcal{B}}$. ∎

**Proposition 24 (Smoothness).** *For each signature $\Sigma$, and for any non-empty set of sorts $S \subseteq \Sigma^{\mathrm{S}}$, the theory $T^{\Sigma}_{\approx}$ is smooth with respect to $S$.* □

PROOF. By Propositions 11 and 23. ∎

## 6.2 Finite witnessability

**Witness function.** A witness function $witness_{\approx}$ for $T^{\Sigma}_{\approx}$ can be defined as follows. Without loss of generality, let $\Gamma$ be a conjunction of flat $\Sigma$-literals such that $vars_\sigma(\Gamma) \neq \emptyset$, for each sort $\sigma \in S$. Then we simply let $witness_{\approx}(\Gamma) = \Gamma$.

**Proposition 25.** *Let $\Gamma$ be a conjunction of flat $\Sigma$-literals, and let $S \subseteq \Sigma^{\mathrm{S}}$. Assume that $vars_\sigma(\Gamma) \neq \emptyset$, for each sort $\sigma \in S$. Then the following are equivalent:*

1. $\Gamma$ *is satisfiable.*
2. *There exists a* $\Sigma$*-interpretation* $\mathcal{A}$ *satisfying* $\Gamma$ *such that* $A_\sigma = [vars_\sigma(\Gamma)]^{\mathcal{A}}$*, for each sort* $\sigma \in S$*.* □

PROOF. $(2 \Rightarrow 1)$. Immediate.

$(1 \Rightarrow 2)$. Let $V_\sigma = vars_\sigma(\Gamma)$, for $\sigma \in \Sigma^{\mathrm{S}}$, and let $V = \bigcup_{\sigma \in \Sigma^{\mathrm{S}}} V_\sigma$. Since $\Gamma$ is satisfiable, there exists a $\Sigma$-interpretation $\mathcal{B}$ satisfying $\Gamma$. We will use $\Gamma$ in order to construct an opportune $T^{\Sigma}_{\approx}$-interpretation $\mathcal{A}$.

For $\sigma \in S$, denote with $\sim_\sigma$ the equivalence relation over the $\Sigma$-terms over $V$ of sort $\sigma$, defined by $s \sim_\sigma t$ iff $s^{\mathcal{B}} = t^{\mathcal{B}}$. In the following, we write $\sim$ in place of $\sim_\sigma$ when the sort $\sigma$ is clear from the context.

Next, let $T_\sigma$ be the set of terms of sort $\sigma$ that occur in $\Gamma$. If for a sort $\sigma$ we have $T_\sigma = \emptyset$, fix a fresh variable $x_0^\sigma$ of sort $\sigma$.

Let $\mathcal{A}$ be the $\Sigma$-interpretation over $V$ and the variables $x_0^\sigma$ constructed as follows. First, we let

$$A_\sigma = \begin{cases} T_\sigma / \sim , & \text{if } T_\sigma \neq \emptyset , \\ \{[x_0^\sigma]_\sim\} , & \text{otherwise} . \end{cases}$$

and

$$x^{\mathcal{A}} = [x]_\sim , \qquad \text{for each variable } x .$$

In order to define $\mathcal{A}$ over the symbols in $\Sigma$, fix an element $a_0^\sigma$ in $A_\sigma$, for each $\sigma \in \Sigma^{\mathrm{S}}$. Then, we let:

- for function symbols $f$ of arity $\sigma_1 \times \cdots \times \sigma_n \to \sigma$:

$$f^{\mathcal{A}}([t_1]_\sim, \ldots, [t_n]_\sim) = \begin{cases} [f(t_1, \ldots, t_n)]_\sim , & \text{if } f(t_1, \ldots, t_n) \in T_\sigma , \\ a_0^\sigma , & \text{otherwise} , \end{cases}$$

- for predicate symbols $p$ of arity $\sigma_1 \times \cdots \times \sigma_n$:

$$([t_1]_\sim, \ldots, [t_n]_\sim) \in p^{\mathcal{A}} \qquad \Longleftrightarrow \qquad \left(t_1^{\mathcal{B}}, \ldots, t_n^{\mathcal{B}}\right) \in p^{\mathcal{B}} .$$

Note that $\mathcal{A}$ is a well-defined $\Sigma$-interpretation, and that $A_\sigma = [vars_\sigma(\Gamma)]^{\mathcal{A}}$, for each sort $\sigma \in S$. Next, we show that $\mathcal{A}$ satisfies all literals in $\Gamma$.

**Literals of the form $x = y$ and $x \neq y$.** Immediate.

**Literals of the form $x = f(y_1, \ldots, y_n)$, where $f$ is a function symbol of arity $\sigma_1 \times \cdots \times \sigma_n \to \sigma$.** We have:

$$\begin{aligned} x^{\mathcal{A}} &= [x]_\sim \\ &= [f(y_1, \ldots, y_n)]_\sim \\ &= f^{\mathcal{A}}([y_1]_\sim, \ldots, [y_n]_\sim) && \text{since } f(y_1, \ldots, y_n) \in T_\sigma \\ &= f^{\mathcal{A}}\left(y_1^{\mathcal{A}}, \ldots, y_n^{\mathcal{A}}\right) . \end{aligned}$$

**Literals of the form $p(y_1, \ldots, y_n)$ and $\neg p(y_1, \ldots, y_n)$, where $p$ is a predicate symbol of arity $\sigma_1 \times \cdots \times \sigma_n$.** Just observe that:

$$\begin{aligned} \left(y_1^{\mathcal{B}}, \ldots, y_n^{\mathcal{B}}\right) \in p^{\mathcal{B}} &\iff ([y_1]_\sim, \ldots, [y_n]_\sim) \in p^{\mathcal{A}} \\ &\iff \left(y_1^{\mathcal{A}}, \ldots, y_n^{\mathcal{A}}\right) \in p^{\mathcal{A}} . \end{aligned}$$

■

**Proposition 26 (Finite witnessability).** *For each signature $\Sigma$, and for any nonempty set of sorts $S \subseteq \Sigma^{\mathrm{S}}$, the theory $T^{\Sigma}_{\approx}$ is finite witnessable with respect to $S$.* □

Proof. By Propositions 12 and 25. ■

### 6.3 Politeness

**Theorem 27 (Politeness).** *For each signature $\Sigma$, and for any nonempty set of sorts $S \subseteq \Sigma^{\mathrm{S}}$, the theory $T^{\Sigma}_{\approx}$ is polite with respect to $S$.* □

Proof. By Propositions 24 and 26. ■

## 7 Lists

Let $A$ be a nonempty set. A *list* $x$ over $A$ is a sequence $\langle a_1, \ldots, a_n \rangle$, where $n \geq 0$ and $\{a_1, \ldots, a_n\} \subseteq A$. We denote with $A^*$ the set of lists over $A$.

The theory of lists $T_{\mathsf{list}}$ has a signature $\Sigma_{\mathsf{list}}$ containing a sort $\mathsf{elem}$ for elements and a sort $\mathsf{list}$ for lists of elements, plus the following symbols:

- the constant symbol $\mathsf{nil}$, of sort $\mathsf{list}$;
- the function symbols

– car, of arity list $\rightarrow$ elem;
– cdr, of arity list $\rightarrow$ list;
– cons, of arity elem $\times$ list $\rightarrow$ list.

**Definition 28.** A STANDARD list-INTERPRETATION $\mathcal{A}$ is a $\Sigma_{\mathsf{list}}$-interpretation satisfying the following conditions:

- $A_{\mathsf{list}} = (A_{\mathsf{elem}})^*$;
- $\mathsf{nil}^{\mathcal{A}} = \langle\rangle$;
- $\mathsf{car}^{\mathcal{A}}(\langle e_1, \ldots, e_n\rangle) = e_1$, for each $n > 0$ and $e_1, \ldots, e_n \in A_{\mathsf{elem}}$;
- $\mathsf{cdr}^{\mathcal{A}}(\langle e_1, \ldots, e_n\rangle) = \langle e_2, \ldots, e_n\rangle$, for each $n > 0$ and $e_1, \ldots, e_n \in A_{\mathsf{elem}}$;
- $\mathsf{cons}^{\mathcal{A}}(e, \langle e_1, \ldots, e_n\rangle) = \langle e, e_1, \ldots, e_n\rangle$, for each $n \geq 0$ and $e, e_1, \ldots, e_n \in A_{\mathsf{elem}}$.

The THEORY OF LISTS is the pair $T_{\mathsf{list}} = \langle \Sigma_{\mathsf{list}}, \mathbf{A}\rangle$, where $\mathbf{A}$ is the class of all standard list-structures. □

## 7.1 Smoothness

**Proposition 29.** *Let $\mathcal{A}$ be a $T_{\mathsf{list}}$-interpretation satisfying a conjunction $\Gamma$ of flat $\Sigma_{\mathsf{list}}$-literals, and such that $A_{\mathsf{elem}}$ is finite. Then there exists a $T_{\mathsf{list}}$-interpretation $\mathcal{B}$ satisfying $\Gamma$ such that $|B_{\mathsf{elem}}| = \kappa$, for each cardinal number $\kappa > |A_{\mathsf{elem}}|$.* □

PROOF. Let $V_\sigma = vars_\sigma(\Gamma)$, for $\sigma \in \{\mathsf{elem}, \mathsf{list}\}$. We construct a $T_{\mathsf{list}}$-interpretation $\mathcal{B}$ over $V_{\mathsf{elem}} \cup V_{\mathsf{list}}$ as follows. Fix a set $A'$ such that $|A_{\mathsf{elem}} \cup A'| = \kappa$, and let

$$B_{\mathsf{elem}} = A_{\mathsf{elem}} \cup A' \,,$$

and

$$\begin{aligned} e^{\mathcal{B}} &= e^{\mathcal{A}} \,, && \text{for each elem-variable } e \in V_{\mathsf{elem}} \,, \\ x^{\mathcal{B}} &= x^{\mathcal{A}} \,, && \text{for each list-variable } x \in V_{\mathsf{list}} \,. \end{aligned}$$

By construction, $\mathcal{B}$ is a $T_{\mathsf{list}}$-interpretation such that $|B_{\mathsf{elem}}| = \kappa$. Moreover, it is trivial to check that $\mathcal{B}$ satisfies all literals in $\Gamma$. ■

**Proposition 30 (Smoothness).** *The theory $T_{\mathsf{list}}$ is smooth with respect to* {elem}. □

PROOF. By Propositions 11 and 29. ■

### 7.2 Auxiliary functions

In order to prove that the theory $T_{\mathsf{list}}$ is finitely witnessable with respect to $\{\mathsf{elem}\}$, we will use the auxiliary functions *compress* and $\delta$.

Given $x \in A^*$ and $X \subseteq A$, the function *compress* returns the list obtained from $x$ by removing all elements that are not in $X$. Formally:

$$\mathit{compress}(\langle\alpha_1,\ldots,\alpha_n\rangle, X) = \begin{cases} \langle\rangle\,, & \text{if } n = 0\,, \\ \langle\alpha_1\rangle \circ \mathit{compress}(\langle\alpha_2,\ldots,\alpha_n\rangle, X)\,, & \text{if } n > 0 \text{ and } \alpha_1 \in X\,, \\ \mathit{compress}(\langle\alpha_2,\ldots,\alpha_n\rangle, X)\,, & \text{otherwise,} \end{cases}$$

where $\circ$ is the concatenation operator over lists.

Given $x, y \in A^*$, the function $\delta$ tests whether $x = y$ or $x \neq y$. Formally:

$$\delta([\alpha_1,\ldots,\alpha_n],[\beta_1,\ldots,\beta_m]) = \begin{cases} \emptyset\,, & \text{if } n = 0 \text{ and } m = 0\,, \\ \{\alpha_1\}\,, & \text{if } n > 0 \text{ and } m = 0\,, \\ \{\beta_1\}\,, & \text{if } n = 0 \text{ and } m > 0\,, \\ \{\alpha_1,\beta_1\}\,, & \text{if } n, m > 0 \text{ and } \alpha_1 \neq \beta_1\,, \\ \delta([\alpha_2,\ldots,\alpha_n],[\beta_2,\ldots,\beta_m])\,, & \text{otherwise.} \end{cases}$$

**Proposition 31.** *For all lists $x, y$, the following holds:*

*(a) $x \neq y$ if and only if $\delta(x, y) \neq \emptyset$;*

*(b) for any set $X$, if $x \neq y$ and $\delta(x, y) \subseteq X$ then $\mathit{compress}(x, X) \neq \mathit{compress}(y, X)$.*

□

### 7.3 Finite witnessability

**Witness function.** A witness function $\mathit{witness}_{\mathsf{list}}$ for the theory $T_{\mathsf{list}}$ can be defined as follows. Without loss of generality, let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{list}}$-literals such that $\mathit{vars}_{\mathsf{elem}}(\Gamma) \neq \emptyset$. We let $\mathit{witness}_{\mathsf{list}}(\Gamma)$ be the result of applying to $\Gamma$ the following transformations:

- Replace each literal of the form $e \approx \mathsf{car}(x)$ in $\Gamma$ with the formula $x \not\approx \mathsf{nil} \rightarrow x \approx \mathsf{cons}(e, y')$, where $y'$ is a fresh $\mathsf{list}$-variable.
- Replace each literal of the form $x \approx \mathsf{cdr}(y)$ in $\Gamma$ with the formula $x \not\approx \mathsf{nil} \rightarrow y \approx \mathsf{cons}(e', x)$, where $e'$ is a fresh $\mathsf{elem}$-variable.

- For each literal of the form $x \not\approx_{\mathsf{list}} y$ in $\Gamma$, generate two fresh $\mathsf{elem}$-variables $w'_{x,y}$ and $w''_{x,y}$, and add the literals $w'_{x,y} \approx w'_{x,y}$ and $w''_{x,y} \approx w''_{x,y}$ to $\Gamma$.

**Remark 32.** Let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{list}}$-literals, let $\Delta = \mathit{witness}_{\mathsf{list}}(\Gamma)$, and let $\bar{v} = \mathit{vars}(\Delta) \setminus \mathit{vars}(\Gamma)$. Then $\Gamma$ and $(\exists \bar{v})\Delta$ are $T_{\mathsf{list}}$-equivalent. □

**Proposition 33.** *Let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{list}}$-literals such that $\mathit{vars}_{\mathsf{elem}}(\Gamma) \neq \emptyset$, and not containing any literal of the form $e \approx \mathsf{car}(x)$ and $x \approx \mathsf{cdr}(y)$. Also, let $k$ be the number of literals of the form $x \not\approx_{\mathsf{list}} y$ occurring in $\Gamma$. Then the following are equivalent:*

1. *$\Gamma$ is $T_{\mathsf{list}}$-satisfiable.*
2. *There exists a $T_{\mathsf{list}}$-interpretation $\mathcal{A}$ satisfying $\Gamma$ such that*

$$A_{\mathsf{elem}} = [\mathit{vars}_{\mathsf{elem}}(\Gamma)]^{\mathcal{A}} \cup A' \,,$$

*where $|A'| \leq 2k$.* □

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

$(1 \Rightarrow 2)$. Let $V_\sigma = \mathit{vars}_\sigma(\Gamma)$, for $\sigma \in \{\mathsf{elem}, \mathsf{list}\}$. Since $\Gamma$ is $T_{\mathsf{list}}$-satisfiable, there exists a $T_{\mathsf{list}}$-interpretation $\mathcal{B}$ satisfying $\Gamma$. We will use $\mathcal{B}$ in order to construct an opportune $T_{\mathsf{list}}$-interpretation $\mathcal{A}$.

More specifically, we let $\mathcal{A}$ be the unique $T_{\mathsf{list}}$-interpretation constructed by letting

$$\begin{aligned} A_{\mathsf{elem}} = {} & V^{\mathcal{B}}_{\mathsf{elem}} \cup \\ & \left\{ \alpha \in \delta\left(x^{\mathcal{B}}, y^{\mathcal{B}}\right) \mid \text{the literal } x \not\approx y \text{ is in } \Gamma \right\} , \end{aligned}$$

and

$$\begin{aligned} e^{\mathcal{A}} &= e^{\mathcal{B}} \,, && \text{for each } \mathsf{elem}\text{-variable } e \in V_{\mathsf{elem}} \,, \\ x^{\mathcal{A}} &= \mathit{compress}\left(x^{\mathcal{B}}, A_{\mathsf{elem}}\right) \,, && \text{for each } \mathsf{list}\text{-variable } x \in V_{\mathsf{list}} \,. \end{aligned}$$

Note that $\mathcal{A}$ is a well-defined $T_{\mathsf{list}}$-interpretation, and that $A_{\mathsf{elem}} = V^{\mathcal{A}}_{\mathsf{elem}} \cup A'$, for a set $A'$ such that $|A'| \leq 2k$. Next, we show that $\mathcal{A}$ satisfies all literals in $\Gamma$.

**Literals of the form $e_1 \approx_{\mathsf{elem}} e_2$ and $e_1 \not\approx_{\mathsf{elem}} e_2$.** Immediate.

**Literals of the form $x \approx_{\mathsf{list}} y$.** We have

$$\begin{aligned} x^{\mathcal{A}} &= \mathit{compress}\left(x^{\mathcal{B}}, A_{\mathsf{elem}}\right) \\ &= \mathit{compress}\left(y^{\mathcal{B}}, A_{\mathsf{elem}}\right) \\ &= y^{\mathcal{A}}\,. \end{aligned}$$

**Literals of the form $x \not\approx_{\mathsf{list}} y$.** By Proposition 31 (with $X = A_{\mathsf{elem}}$).

**Literals of the form $x \approx \mathsf{nil}$.** We have

$$\begin{aligned} x^{\mathcal{A}} &= \mathit{compress}\left(x^{\mathcal{B}}, A_{\mathsf{elem}}\right) \\ &= \mathit{compress}(\langle\rangle, A_{\mathsf{elem}}) \\ &= \langle\rangle\,. \end{aligned}$$

**Literals of the form $x \approx \mathsf{cons}(e, y)$.** We have

$$\begin{aligned} x^{\mathcal{A}} &= \mathit{compress}\left(x^{\mathcal{B}}, A_{\mathsf{elem}}\right) \\ &= \mathit{compress}\left(\left\langle e^{\mathcal{B}}\right\rangle \circ y^{\mathcal{B}}, A_{\mathsf{elem}}\right) \\ &= \left\langle e^{\mathcal{B}}\right\rangle \circ \mathit{compress}\left(y^{\mathcal{B}}, A_{\mathsf{elem}}\right) && \text{since } e^{\mathcal{B}} \in A_{\mathsf{elem}} \\ &= \left\langle e^{\mathcal{A}}\right\rangle \circ y^{\mathcal{A}} \end{aligned}$$

■

**Proposition 34 (Finite witnessability).** *The theory $T_{\mathsf{list}}$ is finitely witnessable with respect to $\{\mathsf{elem}\}$.* □

PROOF. By Propositions 12, Remark 32, and Proposition 33. ■

## 7.4 Politeness

**Theorem 35 (Politeness).** *The theory $T_{\mathsf{list}}$ is polite with respect to $\{\mathsf{elem}\}$.* □

PROOF. By Propositions 30 and 34. ■

## 7.5 A conjecture.

We conjecture that a more efficient witness function $\mathit{witness}'_{\mathsf{list}}$ for $T_{\mathsf{list}}$ can be defined as follows. Without loss of generality, let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{list}}$-literals such that $\mathit{vars}_{\mathsf{elem}}(\Gamma) \neq \emptyset$. We let $\mathit{witness}'_{\mathsf{list}}$ be the result of applying to $\Gamma$ the following transformation:

- Replace each literal of the form $x \approx \mathsf{cdr}(y)$ in $\Gamma$ with the formula $x \not\approx \mathsf{nil} \rightarrow y \approx \mathsf{cons}(e', x)$, where $e'$ is a fresh elem-variable.

We do not have yet a formal proof of this claim.

# 8 Arrays

The theory of arrays $T_{\mathsf{array}}$ has a signature $\Sigma_{\mathsf{array}}$ containing a sort elem for elements, a sort index for indices, and a sort array for arrays, plus the following two function symbols:

- read, of sort array $\times$ index $\rightarrow$ elem;
- write, of sort array $\times$ index $\times$ elem $\rightarrow$ array.

**Notation.** Given $a : I \rightarrow E$, $i \in I$ and $e \in E$, we define $a_{i \mapsto e} : I \rightarrow E$ as follows: $a_{i \mapsto e}(i) = e$ and $a_{i \mapsto e}(j) = a(j)$, for $j \neq i$.

**Definition 36.** A STANDARD array-INTERPRETATION $\mathcal{A}$ is a $\Sigma_{\mathsf{array}}$-interpretation satisfying the following conditions:

- $A_{\mathsf{array}} = (A_{\mathsf{elem}})^{A_{\mathsf{index}}}$;
- $\mathsf{read}^{\mathcal{A}}(a, i) = a(i)$, for each $a \in A_{\mathsf{array}}$ and $i \in A_{\mathsf{index}}$;
- $\mathsf{write}^{\mathcal{A}}(a, i, e) = a_{i \mapsto e}$, for each $a \in A_{\mathsf{array}}$, $i \in A_{\mathsf{index}}$, and $e \in A_{\mathsf{elem}}$.

The THEORY OF ARRAYS is the pair $T_{\mathsf{array}} = \langle \Sigma_{\mathsf{array}}, \mathbf{A} \rangle$, where $\mathbf{A}$ is the class of all standard array-structures. □

## 8.1 Smoothness

**Proposition 37.** *Let $\mathcal{A}$ be a $T_{\mathsf{array}}$-interpretation satisfying a conjunction $\Gamma$ of flat $\Sigma_{\mathsf{array}}$-literals, and such that $A_{\mathsf{index}}$ is finite. Then there exists a $T_{\mathsf{array}}$-interpretation $\mathcal{B}$ satisfying $\Gamma$ such that $|B_{\mathsf{elem}}| = |A_{\mathsf{elem}}|$ and $|B_{\mathsf{index}}| = \kappa$, for each cardinal number $\kappa > |A_{\mathsf{index}}|$.* □

PROOF. Let $V_\sigma = vars_\sigma(\Gamma)$, for $\sigma \in \{\mathsf{elem}, \mathsf{index}, \mathsf{array}\}$. We constructs a $T_{\mathsf{array}}$-interpretation $\mathcal{B}$ over $V_{\mathsf{elem}} \cup V_{\mathsf{index}} \cup V_{\mathsf{array}}$ as follows. Fix a set $A'$ such that $|A_{\mathsf{index}} \cup A'| = \kappa$, and let

$$\begin{aligned} B_{\mathsf{index}} &= A_{\mathsf{index}} \cup A' \,, \\ B_{\mathsf{elem}} &= A_{\mathsf{elem}} \,, \end{aligned}$$

and

$$\begin{aligned} i^{\mathcal{B}} &= i^{\mathcal{A}} \,, && \text{for each } \mathsf{index}\text{-variable } i \in V_{\mathsf{index}} \,, \\ e^{\mathcal{B}} &= e^{\mathcal{A}} \,, && \text{for each } \mathsf{elem}\text{-variable } e \in V_{\mathsf{elem}} \,. \end{aligned}$$

In order to define $\mathcal{B}$ over the $\mathsf{array}$-variables, fix an element $e_0 \in A_{\mathsf{elem}}$. Then, for each $\mathsf{array}$-variable $a \in V_{\mathsf{array}}$, we let

$$a^{\mathcal{B}}(i) = \begin{cases} a^{\mathcal{A}}(i) \,, & \text{if } i \in A_{\mathsf{index}} \,, \\ e_0 \,, & \text{otherwise} \,. \end{cases}$$

By construction, $\mathcal{B}$ is a $T_{\mathsf{array}}$-interpretation such that $|B_{\mathsf{elem}}| = |A_{\mathsf{elem}}|$ and $|B_{\mathsf{index}}| = \kappa$. Next, we show that $\mathcal{B}$ satisfies all literals in $\Gamma$.

**Literals of the form $e_1 \approx_{\mathsf{elem}} e_2$, $e_1 \not\approx_{\mathsf{elem}} e_2$, $i \approx_{\mathsf{index}} j$, and $i \not\approx_{\mathsf{index}} j$.** Immediate.

**Literals of the form $a \approx_{\mathsf{array}} b$.** Let $i \in B_{\mathsf{index}}$. If $i \in A_{\mathsf{index}}$ then $a^{\mathcal{B}}(i) = a^{\mathcal{A}}(i) = b^{\mathcal{A}}(i) = b^{\mathcal{B}}(i)$. If $i \notin A_{\mathsf{index}}$ then $a^{\mathcal{B}}(i) = e_0 = a^{\mathcal{B}}(i)$. Thus, $a^{\mathcal{B}} = b^{\mathcal{B}}$.

**Literals of the form $a \not\approx_{\mathsf{array}} b$.** Since $a^{\mathcal{A}} \neq b^{\mathcal{A}}$, there exists an index $i \in A_{\mathsf{index}}$ such that $a^{\mathcal{A}}(i) \neq b^{\mathcal{A}}(i)$. It follows that $a^{\mathcal{B}}(i) \neq b^{\mathcal{B}}(i)$, which implies $a^{\mathcal{B}} \neq b^{\mathcal{B}}$.

**Literals of the form $e \approx \mathsf{read}(a, i)$.** We have:

$$\begin{aligned} e^{\mathcal{B}} &= e^{\mathcal{A}} \\ &= [\mathsf{read}(a, i)]^{\mathcal{A}} \\ &= a^{\mathcal{A}}\left(i^{\mathcal{A}}\right) \\ &= a^{\mathcal{B}}\left(i^{\mathcal{B}}\right) && \text{since } i^{\mathcal{A}} \in A_{\mathsf{index}} \,. \end{aligned}$$

**Literals of the form** $a = \mathsf{write}(b, i, e)$. We have $a^{\mathcal{B}}(i^{\mathcal{B}}) = a^{\mathcal{A}}(i^{\mathcal{A}}) = e^{\mathcal{A}} = e^{\mathcal{B}}$. Next, let $j \in B_{\mathsf{index}}$ such that $j \neq i^{\mathcal{B}}$. If $j \in A_{\mathsf{index}}$ then we have $a^{\mathcal{B}}(j) = a^{\mathcal{A}}(j) = b^{\mathcal{A}}(j) = b^{\mathcal{B}}(j)$. If instead $j \notin A_{\mathsf{index}}$ then $a^{\mathcal{B}}(j) = e_0 = b^{\mathcal{B}}(j)$. Thus, $a^{\mathcal{B}} = b^{\mathcal{B}}_{i^{\mathcal{B}} \mapsto e^{\mathcal{B}}}$. ■

**Proposition 38.** *Let $\mathcal{A}$ be a $T_{\mathsf{array}}$-interpretation satisfying a conjunction $\Gamma$ of flat $\Sigma_{\mathsf{array}}$-literals, and such that $A_{\mathsf{elem}}$ is finite. Then there exists a $T_{\mathsf{array}}$-interpretation $\mathcal{B}$ satisfying $\Gamma$ such that $|B_{\mathsf{index}}| = |A_{\mathsf{index}}|$ and $|B_{\mathsf{elem}}| = \kappa$, for each $\kappa > |A_{\mathsf{elem}}|$.* □

Proof. Similar to the proof of Proposition 37. ■

**Proposition 39 (Smoothness).** *For any non-empty set of sorts $S \subseteq \{\mathsf{elem}, \mathsf{index}\}$, the theory $T_{\mathsf{array}}$ is smooth with respect to $S$.* □

Proof. By Propositions 11, 37, and 38. ■

## 8.2 Finite witnessability

**Witness Function.** A witness function $witness_{\mathsf{array}}$ for the theory $T_{\mathsf{array}}$ can be defined as follows. Without loss of generality, let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{array}}$-literals such that $vars_{\mathsf{index}}(\Gamma) \neq \emptyset$ and $vars_{\mathsf{elem}}(\Gamma) \neq \emptyset$. We let $witness_{\mathsf{array}}(\Gamma)$ be the result of applying to $\Gamma$ the following transformation:

- Replace each literal of the form $a \not\approx_{\mathsf{array}} b$ in $\Gamma$ with a literal of the form $\mathsf{read}(a, i') \not\approx \mathsf{read}(b, i')$, where $i'$ is a fresh $\mathsf{index}$-variable.

**Remark 40.** Let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{array}}$-literals, let $\Delta = witness_{\mathsf{array}}(\Gamma)$, and let $\bar{v} = vars(\Delta) \setminus vars(\Gamma)$. Then $\Gamma$ and $(\exists \bar{v})\Delta$ are $T_{\mathsf{array}}$-equivalent. □

**Proposition 41.** *Let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{array}}$-literals such that $vars_{\mathsf{index}}(\Gamma) \neq \emptyset$ and $vars_{\mathsf{elem}}(\Gamma) \neq \emptyset$, and not containing any literal of the form $x \not\approx_{\mathsf{array}} y$. Then the following are equivalent:*

1. *$\Gamma$ is $T_{\mathsf{array}}$-satisfiable.*
2. *There exists a $T_{\mathsf{array}}$-interpretation $\mathcal{A}$ satisfying $\Gamma$ such that $A_{\mathsf{index}} = [vars_{\mathsf{index}}(\Gamma)]^{\mathcal{A}}$ and $A_{\mathsf{elem}} = [vars_{\mathsf{elem}}(\Gamma)]^{\mathcal{A}}$.* □

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

$(1 \Rightarrow 2)$. Let $V_\sigma = vars_\sigma(\Gamma)$, for $\sigma \in \{\mathsf{elem}, \mathsf{index}, \mathsf{array}\}$. Since $\Gamma$ is $T_{\mathsf{array}}$-satisfiable, there exists a $T_{\mathsf{array}}$-interpretation $\mathcal{B}$ satisfying $\Gamma$. We will use $\mathcal{B}$ in order to construct an opportune $T_{\mathsf{array}}$-interpretation $\mathcal{A}$.

More specifically, we let $\mathcal{A}$ be the $T_{\mathsf{array}}$-interpretation over $V_{\mathsf{elem}} \cup V_{\mathsf{index}} \cup V_{\mathsf{array}}$ constructed as follows. First, we let

$$A_{\mathsf{index}} = V_{\mathsf{index}}^{\mathcal{B}}\,,$$
$$A_{\mathsf{elem}} = V_{\mathsf{elem}}^{\mathcal{B}}\,,$$

and

$$i^{\mathcal{A}} = i^{\mathcal{B}}\,, \qquad \text{for each } \mathsf{index}\text{-variable } i \in V_{\mathsf{index}}\,,$$
$$e^{\mathcal{A}} = e^{\mathcal{B}}\,, \qquad \text{for each } \mathsf{elem}\text{-variable } e \in V_{\mathsf{elem}}\,.$$

In order to define $\mathcal{A}$ over the $\mathsf{array}$-variables, fix an $e_0 \in A_{\mathsf{elem}}$. Then, for each $a \in V_{\mathsf{array}}$ and $i \in V_{\mathsf{index}}$, we let

$$a^{\mathcal{A}}\left(i^{\mathcal{A}}\right) = \begin{cases} a^{\mathcal{B}}(i^{\mathcal{B}})\,, & \text{if } a^{\mathcal{B}}(i^{\mathcal{B}}) \in A_{\mathsf{elem}}\,, \\ e_0\,, & \text{otherwise}\,. \end{cases}$$

Note that $\mathcal{A}$ is a well-defined $T_{\mathsf{array}}$-interpretation, and that $A_\sigma = [vars_\sigma(\Gamma)]^{\mathcal{A}}$, for $\sigma \in \{\mathsf{index}, \mathsf{elem}\}$. Next, we show that $\mathcal{A}$ satisfies all literals in $\Gamma$.

**Literals of the form $e_1 \approx_{\mathsf{elem}} e_2$, $e_1 \not\approx_{\mathsf{elem}} e_2$, $i \approx_{\mathsf{index}} j$, and $i \not\approx_{\mathsf{index}} j$.** Immediate.

**Literals of the form $a \approx_{\mathsf{array}} b$.** Let $i \in A_{\mathsf{index}}$. If $a^{\mathcal{B}}\left(i^{\mathcal{B}}\right) \in A_{\mathsf{elem}}$ then $a^{\mathcal{A}}\left(i^{\mathcal{A}}\right) = a^{\mathcal{B}}\left(i^{\mathcal{B}}\right) = b^{\mathcal{B}}\left(i^{\mathcal{B}}\right) = b^{\mathcal{A}}\left(i^{\mathcal{A}}\right)$. If instead $a^{\mathcal{B}}\left(i^{\mathcal{B}}\right) \notin A_{\mathsf{elem}}$ then $a^{\mathcal{A}}(i^{\mathcal{A}}) = e_0 = b^{\mathcal{A}}(i^{\mathcal{A}})$.

**Literals of the form $e \approx \mathsf{read}(a, i)$.** We have:

$$\begin{aligned} e^{\mathcal{A}} &= e^{\mathcal{B}} \\ &= [\mathsf{read}(a,i)]^{\mathcal{B}} \\ &= a^{\mathcal{B}}\left(i^{\mathcal{B}}\right) \\ &= a^{\mathcal{A}}\left(i^{\mathcal{A}}\right) && \text{since } a^{\mathcal{B}}\left(i^{\mathcal{B}}\right) \in A_{\mathsf{elem}}\,. \end{aligned}$$

**Literals of the form $a = \mathsf{write}(b, i, e)$.** Since $a^{\mathcal{B}}\left(i^{\mathcal{B}}\right) = e^{\mathcal{B}} \in A_{\mathsf{elem}}$, we have we have $a^{\mathcal{A}}\left(i^{\mathcal{A}}\right) = b^{\mathcal{B}}\left(i^{\mathcal{B}}\right) = e^{\mathcal{B}} = e^{\mathcal{A}}$. Next, let $j \in A_{\mathsf{index}}$ such that $j \neq i^{\mathcal{A}}$. If $a^{\mathcal{B}}(j) \in A_{\mathsf{elem}}$ then $a^{\mathcal{A}}(j) = a^{\mathcal{B}}(j) = b^{\mathcal{B}}(j) = b^{\mathcal{A}}(j)$. If instead $a^{\mathcal{B}}(j) \notin A_{\mathsf{elem}}$ then $a^{\mathcal{A}}(j) = e_0 = b^{\mathcal{A}}(j)$. ∎

**Proposition 42 (Finite witnessability).** *For any nonempty set of sorts* $S \subseteq \{\mathsf{elem}, \mathsf{index}\}$*, the theory* $T_{\mathsf{array}}$ *is finite witnessable with respect to* $S$*.* □

PROOF. By Propositions 12, Remark 40, and Proposition 41. ■

### 8.3 Politeness

**Theorem 43 (Politeness).** *For any nonempty set of sorts* $S \subseteq \{\mathsf{elem}, \mathsf{index}\}$*, the theory* $T_{\mathsf{array}}$ *is polite with respect to* $S$*.* □

PROOF. By Propositions 39 and 42. ■

## 9 Sets

The theory of sets $T_{\mathsf{set}}$ has a signature $\Sigma_{\mathsf{set}}$ containing a sort $\mathsf{elem}$ for elements and a sort $\mathsf{set}$ for sets of elements, plus the following symbols:

- the constant symbol $\emptyset$, of sort $\mathsf{set}$;
- the function symbols:
  - $\{\cdot\}$, of sort $\mathsf{elem} \to \mathsf{set}$;
  - $\cup$, $\cap$, and $\setminus$, of sort $\mathsf{set} \times \mathsf{set} \to \mathsf{set}$;
- the predicate symbol $\in$, of sort $\mathsf{elem} \times \mathsf{set}$.

**Definition 44.** A STANDARD set-INTERPRETATION $\mathcal{A}$ is a $\Sigma_{\mathsf{set}}$-interpretation satisfying the following conditions:

- $A_{\mathsf{set}} = \mathcal{P}(A_{\mathsf{elem}})$;
- the symbols $\emptyset$, $\{\cdot\}$, $\cup$, $\cap$, $\setminus$, and $\in$ are interpreted according to their standard interpretation over sets.

The THEORY OF SETS is the pair $T_{\mathsf{set}} = \langle \Sigma_{\mathsf{set}}, \mathbf{A} \rangle$, where $\mathbf{A}$ is the class of all standard set-structures. □

## 9.1 Smoothness

**Proposition 45.** *Let $\mathcal{A}$ be a $T_{\mathsf{set}}$-interpretation satisfying a conjunction $\Gamma$ of flat $\Sigma_{\mathsf{set}}$-literals, and such that $A_{\mathsf{elem}}$ is finite. Then there exists a $T_{\mathsf{set}}$-interpretation $\mathcal{B}$ satisfying $\Gamma$ such that $|B_{\mathsf{elem}}| = \kappa$, for each $\kappa > |A_{\mathsf{elem}}|$.* □

PROOF. Let $V_\sigma = vars_\sigma(\Gamma)$, for $\sigma \in \{\mathsf{elem}, \mathsf{set}\}$. We construct a $T_{\mathsf{set}}$-interpretation $\mathcal{B}$ over $V_{\mathsf{elem}} \cup V_{\mathsf{set}}$ as follows. Fix a set $A'$ such that $|A_{\mathsf{elem}} \cup A'| = \kappa$, and let

$$B_{\mathsf{elem}} = A_{\mathsf{elem}} \cup A' ,$$

and

$$\begin{aligned} e^{\mathcal{B}} &= e^{\mathcal{A}} , && \text{for each } \mathsf{elem}\text{-variable } e \in V_{\mathsf{elem}} , \\ x^{\mathcal{B}} &= x^{\mathcal{A}} , && \text{for each } \mathsf{set}\text{-variable } x \in V_{\mathsf{set}} . \end{aligned}$$

By construction $\mathcal{B}$ is a $T_{\mathsf{set}}$-interpretation such that $|B_{\mathsf{elem}}| = \kappa$. Moreover, it is trivial to check that $\mathcal{B}$ satisfies all literals in $\Gamma$. ■

**Proposition 46 (Smoothness).** *The theory $T_{\mathsf{set}}$ is smooth with respect to the sort* elem. □

PROOF. By Propositions 11 and 45. ■

## 9.2 Finite witnessability

**Witness Function.** A witness function $witness_{\mathsf{set}}$ for the theory $T_{\mathsf{set}}$ can be defined as follows. Without loss of generality, let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{set}}$-literals such that $vars_{\mathsf{elem}}(\Gamma) \neq \emptyset$. We let $witness_{\mathsf{set}}(\Gamma)$ be the result of applying to $\Gamma$ the following transformation:

- Replace each literal of the form $x \not\approx_{\mathsf{set}} y$ in $\Gamma$ with a literal of the form $e' \in (x \setminus y) \cup (y \setminus x)$, where $e'$ is a fresh $\mathsf{elem}$-variable.

**Remark 47.** Let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{set}}$-literals, let $\Delta = witness_{\mathsf{set}}(\Gamma)$, and let $\bar{v} = vars(\Delta) \setminus vars(\Gamma)$. Then $\Gamma$ and $(\exists \bar{v})\Delta$ are $T_{\mathsf{set}}$-equivalent. □

**Proposition 48.** *Let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{set}}$-literals such that $vars_{\mathsf{elem}}(\Gamma) \neq \emptyset$, and not containing any literal of the form $x \not\approx_{\mathsf{set}} y$. Then the following are equivalent:*

1. $\Gamma$ *is* $T_{\mathsf{set}}$*-satisfiable.*
2. *There exists a* $T_{\mathsf{set}}$*-interpretation* $\mathcal{A}$ *satisfying* $\Gamma$ *such that* $A_{\mathsf{elem}} = [vars_{\mathsf{elem}}(\Gamma)]^{\mathcal{A}}$.

□

PROOF. $(2 \Rightarrow 1)$. Immediate.

$(1 \Rightarrow 2)$. Let $V_\sigma = vars_\sigma(\Gamma)$, for $\sigma \in \{\mathsf{elem}, \mathsf{set}\}$. Since $\Gamma$ is $T_{\mathsf{set}}$-satisfiable, there exists a $T_{\mathsf{set}}$-interpretation $\mathcal{B}$ satisfying $\Gamma$. We will use $\mathcal{B}$ in order to construct an opportune $T_{\mathsf{set}}$-interpretation $\mathcal{A}$.

More specifically, we let $\mathcal{A}$ be the $T_{\mathsf{set}}$-interpretation over $V_{\mathsf{elem}} \cup V_{\mathsf{set}}$ constructed by letting

$$A_{\mathsf{elem}} = V_{\mathsf{elem}}^{\mathcal{B}} ,$$

and

$$\begin{aligned} e^{\mathcal{A}} &= e^{\mathcal{B}} , && \text{for each } \mathsf{elem}\text{-variable } e \in V_{\mathsf{elem}} , \\ x^{\mathcal{A}} &= x^{\mathcal{B}} \cap A_{\mathsf{elem}} , && \text{for each } \mathsf{set}\text{-variable } x \in V_{\mathsf{set}} . \end{aligned}$$

By construction, $\mathcal{A}$ is a well-defined $T_{\mathsf{set}}$-intepretation such that $A_{\mathsf{elem}} = [vars_{\mathsf{elem}}(\Gamma)]^{\mathcal{A}}$. Next, we show that $\mathcal{A}$ satisfies all literals in $\Gamma$.

**Literals of the form** $e_1 \approx_{\mathsf{elem}} e_2$ **and** $e_1 \not\approx_{\mathsf{elem}} e_2$**.** Immediate.

**Literals of the form** $x \approx_{\mathsf{set}} y$**.** We have $x^{\mathcal{A}} = x^{\mathcal{B}} \cap A_{\mathsf{elem}} = y^{\mathcal{B}} \cap A_{\mathsf{elem}} = y^{\mathcal{A}}$.

**Literals of the form** $x \approx \emptyset$**.** We have $x^{\mathcal{A}} = x^{\mathcal{B}} \cap A_{\mathsf{elem}} = \emptyset \cap A_{\mathsf{elem}} = \emptyset$.

**Literals of the form** $x \approx \{e\}$**.** We have $x^{\mathcal{A}} = x^{\mathcal{B}} \cap A_{\mathsf{elem}} = \{e^{\mathcal{B}}\} \cap A_{\mathsf{elem}} = \{e^{\mathcal{B}}\}$.

**Literals of the form** $x \approx y \cup z$**.** We have $x^{\mathcal{A}} = x^{\mathcal{B}} \cap A_{\mathsf{elem}} = (y^{\mathcal{B}} \cup z^{\mathcal{B}}) \cap A_{\mathsf{elem}} = (y^{\mathcal{B}} \cap A_{\mathsf{elem}}) \cup (z^{\mathcal{B}} \cap A_{\mathsf{elem}}) = y^{\mathcal{A}} \cup z^{\mathcal{A}}$.

**Literals of the form** $x \approx y \cap z$**.** We have $x^{\mathcal{A}} = x^{\mathcal{B}} \cap A_{\mathsf{elem}} = (y^{\mathcal{B}} \cap z^{\mathcal{B}}) \cap A_{\mathsf{elem}} = (y^{\mathcal{B}} \cap A_{\mathsf{elem}}) \cap (z^{\mathcal{B}} \cap A_{\mathsf{elem}}) = y^{\mathcal{A}} \cap z^{\mathcal{A}}$.

**Literals of the form** $x \approx y \setminus z$**.** We have $x^{\mathcal{A}} = x^{\mathcal{B}} \cap A_{\mathsf{elem}} = (y^{\mathcal{B}} \setminus z^{\mathcal{B}}) \cap A_{\mathsf{elem}} = (y^{\mathcal{B}} \cap A_{\mathsf{elem}}) \setminus (z^{\mathcal{B}} \cap A_{\mathsf{elem}}) = y^{\mathcal{A}} \setminus z^{\mathcal{A}}$.

**Literals of the form $e \in x$ and $e \notin x$.** Just observe that $e^{\mathcal{A}} \in A_{\mathsf{elem}}$. ■

**Proposition 49 (Finite witnessability).** *The theory $T_{\mathsf{set}}$ is finitely witnessable with respect to* $\{\mathsf{elem}\}$. □

PROOF. By Proposition 12, Remark 47, and Proposition 48. ■

### 9.3 Politeness

**Theorem 50 (Politeness).** *The theory $T_{\mathsf{set}}$ is polite with respect to* $\{\mathsf{elem}\}$. □

PROOF. By Propositions 46 and 49. ■

## 10 Multisets

Multisets—also known as bags—are collections that may contain duplicate elements. Formally, a multiset $x$ is a function $x : A \to \mathbb{N}$, for some set $A$.

We use the symbol $[\![\,]\!]$ to denote the empty multiset. When $n \geq 0$, we write $[\![e]\!]^{(n)}$ to denote the multiset containing exactly $n$ occurrences of $e$ and nothing else. When $n < 0$, we let $[\![e]\!]^n = [\![\,]\!]$.

Let $x, y$ be two multisets. Then:

- their *union* $x \cup y$ is the multiset $z$ such that, for each element $e$, the equality $z(e) = \max(x(e), y(e))$ holds;
- their *sum* $x \uplus y$ is the multiset $z$ such that, for each element $e$, the equality $z(e) = x(e) + y(e)$ holds;
- their *intersection* $x \cap y$ is the multiset $z$ such that, for each element $e$, the equality $z(e) = \min(x(e), y(e))$ holds.

The theory of multisets $T_{\mathsf{bag}}$ has a signature $\Sigma_{\mathsf{bag}}$ containing a sort $\mathsf{int}$ for integers, a sort $\mathsf{elem}$ for elements, and a sort $\mathsf{bag}$ for multisets, plus the following symbols:

- the constant symbols:
  - 0 and 1, of sort $\mathsf{int}$;
  - $[\![\,]\!]$, of sort $\mathsf{bag}$;
- the function symbols:

  - $+$, $-$, max, and min, of sort $\mathsf{int} \times \mathsf{int} \to \mathsf{int}$;
  - $[\![\cdot]\!]^{(\cdot)}$, of sort $\mathsf{elem} \times \mathsf{int} \to \mathsf{bag}$;
  - $\cup$, $\uplus$, and $\cap$, of sort $\mathsf{bag} \times \mathsf{bag} \to \mathsf{bag}$;
  - count, of sort $\mathsf{elem} \times \mathsf{bag} \to \mathsf{int}$;
- the predicate symbol $<$, of sort $\mathsf{int} \times \mathsf{int}$.

**Definition 51.** A STANDARD bag-INTERPRETATION $\mathcal{A}$ is a $\Sigma_{\mathsf{bag}}$-interpretation satisfying the following conditions:

- $A_{\mathsf{int}} = \mathbb{Z}$;
- $A_{\mathsf{bag}} = \mathbb{N}^{A_{\mathsf{elem}}}$;
- the symbols 0, 1, $+$, $-$, max, min, and $<$ are interpreted according to their standard interpretation over the integers;
- the symbol $[\![\,]\!]$, $\cup$, $\cap$, $\setminus$, $[\![\cdot]\!]^{(\cdot)}$ are interpreted according to their standard interpretation over multisets;
- $\mathsf{count}^{\mathcal{A}}(e, x) = x(e)$, for each $e \in A_{\mathsf{elem}}$ and $x \in A_{\mathsf{bag}}$.

The THEORY OF MULTISETS is the pair $T_{\mathsf{bag}} = \langle \Sigma_{\mathsf{bag}}, \mathbf{A} \rangle$, where $\mathbf{A}$ is the class of all standard bag-structures. □

## 10.1 Smoothness

**Proposition 52.** *Let $\mathcal{A}$ be a $T_{\mathsf{bag}}$-interpretation satisfying a conjunction $\Gamma$ of flat $\Sigma_{\mathsf{bag}}$-literals, and such that $A_{\mathsf{elem}}$ is finite. Then there exists a $T_{\mathsf{bag}}$-interpretation $\mathcal{B}$ satisfying $\Gamma$ such that $|B_{\mathsf{elem}}| = \kappa$, for each $\kappa > |A_{\mathsf{elem}}|$.* □

PROOF. Let $V_\sigma = vars_\sigma(\Gamma)$, for $\sigma \in \{\mathsf{elem}, \mathsf{int}, \mathsf{bag}\}$. We construct a $T_{\mathsf{bag}}$-interpretation $\mathcal{B}$ over $V_{\mathsf{elem}} \cup V_{\mathsf{int}} \cup V_{\mathsf{bag}}$ as follows. Fix a set $A'$ such that $|A_{\mathsf{elem}} \cup A'| = \kappa$, and let

$$B_{\mathsf{elem}} = A_{\mathsf{elem}} \cup A' \,,$$

and

$$\begin{aligned} e^{\mathcal{B}} &= e^{\mathcal{A}} \,, && \text{for each } \mathsf{elem}\text{-variable } e \in V_{\mathsf{elem}} \,, \\ u^{\mathcal{B}} &= u^{\mathcal{A}} \,, && \text{for each } \mathsf{int}\text{-variable } u \in V_{\mathsf{int}} \,. \end{aligned}$$

Furthermore, for every bag-variable $x \in V_{\mathsf{bag}}$ and $e \in B_{\mathsf{elem}}$, we let

$$x^{\mathcal{B}}(e) = \begin{cases} x^{\mathcal{A}}(e)\,, & \text{if } e \in A_{\mathsf{elem}}\,, \\ 0\,, & \text{otherwise}\,. \end{cases}$$

By construction, $\mathcal{B}$ is a $T_{\mathsf{bag}}$-interpretation such that $|B_{\mathsf{elem}}| = \kappa$. Next, we show that $\mathcal{B}$ satisfies all literals in $\Gamma$.

**Literals of the form $e_1 \approx_{\mathsf{elem}} e_2$, $e_1 \not\approx_{\mathsf{elem}} e_2$, $u \approx_{\mathsf{int}} v$, and $u \not\approx_{\mathsf{int}} v$.** Immediate.

**Literals of the form $x \approx_{\mathsf{bag}} y$.** Let $e \in B_{\mathsf{elem}}$. If $e \in A_{\mathsf{elem}}$ then $x^{\mathcal{B}}(e) = x^{\mathcal{A}}(e) = y^{\mathcal{A}}(e) = y^{\mathcal{B}}(e)$. If $e \notin A_{\mathsf{index}}$ then $x^{\mathcal{B}}(e) = 0 = y^{\mathcal{B}}(e)$. Thus, $x^{\mathcal{B}} = y^{\mathcal{B}}$.

**Literals of the form $x \not\approx_{\mathsf{bag}} y$.** Since $x^{\mathcal{A}} \neq y^{\mathcal{A}}$, there exists an $e \in A_{\mathsf{elem}}$ such that $x^{\mathcal{A}}(e) \neq y^{\mathcal{A}}(e)$. It follows that $x^{\mathcal{B}}(e) \neq y^{\mathcal{B}}(e)$, which implies $x^{\mathcal{B}} \neq y^{\mathcal{B}}$.

**Literals of the form $u \approx 0$, $u \approx 1$, $u \approx v + w$, $u \approx v - w$, $u \approx \mathsf{max}(v, w)$, $u \approx \mathsf{min}(v, w)$.** Immediate.

**Literals of the form $x \approx [\![e]\!]^{(u)}$.** Since $e^{\mathcal{B}} \in A_{\mathsf{elem}}$, we have $x^{\mathcal{B}}(e^{\mathcal{B}}) = x^{\mathcal{A}}(e^{\mathcal{A}}) = u^{\mathcal{A}} = u^{\mathcal{B}}$. Next, let $e' \in B_{\mathsf{elem}}$ such that $e' \neq e^{\mathcal{B}}$. If $e' \in A_{\mathsf{elem}}$ then $x^{\mathcal{B}}(e') = x^{\mathcal{A}}(e') = 0$. If instead $e' \notin A_{\mathsf{elem}}$ then $x^{\mathcal{B}}(e') = 0$. Thus $x^{\mathcal{B}} = [\![e^{\mathcal{B}}]\!]^{(u^{\mathcal{B}})}$.

**Literals of the form $x \approx y \cup z$, $x \approx y \uplus z$, and $x \approx y \cap z$.** This case is similar to the case of literals of the form $x \approx [\![e]\!]^{(u)}$.

**Literals of the form $u \approx \mathsf{count}(x, e)$.** Since $e^{\mathcal{B}} \in A_{\mathsf{elem}}$, we have $u^{\mathcal{B}} = u^{\mathcal{A}} = x^{\mathcal{A}}\left(e^{\mathcal{A}}\right) = x^{\mathcal{B}}\left(e^{\mathcal{B}}\right)$. ∎

**Proposition 53 (Smoothness).** *The theory $T_{\mathsf{bag}}$ is smooth with respect to* $\{\mathsf{elem}\}$. □

Proof. By Propositions 11 and 52. ∎

## 10.2 Finite witnessability

**Witness Function.** A witness function $witness_{\mathsf{bag}}$ for the theory $T_{\mathsf{bag}}$ can be defined as follows. Without loss of generality, let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{bag}}$-literals such that $vars_{\mathsf{elem}}(\Gamma) \neq \emptyset$. We let $witness_{\mathsf{bag}}(\Gamma)$ be the result of applying to $\Gamma$ the following transformation:

- Replace each literal of the form $x \not\approx_{\mathsf{bag}} y$ in $\Gamma$ with a literal of the form $\mathsf{count}(e', x) \not\approx \mathsf{count}(e', y)$, where $e'$ is a fresh $\mathsf{elem}$-variable.

**Remark 54.** Let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{bag}}$-literals, let $\Delta = witness_{\mathsf{bag}}(\Gamma)$, and let $\bar{v} = vars(\Delta) \setminus vars(\Gamma)$. Then $\Gamma$ and $(\exists \bar{v})\Delta$ are $T_{\mathsf{bag}}$-equivalent. □

**Proposition 55.** *Let $\Gamma$ be a conjunction of flat $\Sigma_{\mathsf{bag}}$-literals such that $vars_{\mathsf{elem}}(\Gamma) \neq \emptyset$, and not containing any literal of the form $x \not\approx_{\mathsf{bag}} y$. Then the following are equivalent:*

1. *$\Gamma$ is $T_{\mathsf{bag}}$-satisfiable.*
2. *There exists a $T_{\mathsf{bag}}$-interpretation $\mathcal{A}$ satisfying $\Gamma$ such that $A_{\mathsf{elem}} = [vars_{\mathsf{elem}}(\Gamma)]^{\mathcal{A}}$.*

□

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

$(1 \Rightarrow 2)$. Let $V_\sigma = vars_\sigma(\Gamma)$, for $\sigma \in \{\mathsf{elem}, \mathsf{int}, \mathsf{bag}\}$. Since $\Gamma$ is $T_{\mathsf{bag}}$-satisfiable, there exists a $T_{\mathsf{bag}}$-interpretation $\mathcal{B}$ satisfying $\Gamma$. We will use $\mathcal{B}$ in order to construct an opportune $T_{\mathsf{bag}}$-interpretation $\mathcal{A}$.

More specifically, we let $\mathcal{A}$ be the $T_{\mathsf{bag}}$-interpretation over $V_{\mathsf{elem}} \cup V_{\mathsf{int}} \cup V_{\mathsf{bag}}$ constructed by letting

$$A_{\mathsf{elem}} = V_{\mathsf{elem}}^{\mathcal{B}} ,$$

and

$$\begin{aligned} e^{\mathcal{A}} &= e^{\mathcal{B}} , && \text{for each } \mathsf{elem}\text{-variable } e \in V_{\mathsf{elem}} , \\ u^{\mathcal{A}} &= u^{\mathcal{B}} , && \text{for each } \mathsf{int}\text{-variable } u \in V_{\mathsf{int}} . \end{aligned}$$

Furthermore, for every $\mathsf{bag}$-variable $x \in V_{\mathsf{bag}}$, we let

$$x^{\mathcal{A}}(e) = x^{\mathcal{B}}(e) , \qquad \text{for each } e \in A_{\mathsf{elem}} .$$

By contruction $\mathcal{A}$ is a $T_{\mathsf{bag}}$-interpretation such that $A_{\mathsf{elem}} = [vars_{\mathsf{elem}}(\Gamma)]^{\mathcal{A}}$. Next, we show that $\mathcal{A}$ satisfies all literals in $\Gamma$.

**Literals of the form $e_1 \approx_{\mathsf{elem}} e_2$, $e_1 \not\approx_{\mathsf{elem}} e_2$, $u \approx_{\mathsf{int}} v$, and $u \not\approx_{\mathsf{int}} v$.** Immediate.

**Literals of the form $x \approx_{\mathsf{bag}} y$.** Since for each $e \in A_{\mathsf{elem}}$, we have $x^{\mathcal{A}}(e) = x^{\mathcal{B}}(e) = y^{\mathcal{B}}(e) = y^{\mathcal{A}}(e)$, it follows that $x^{\mathcal{A}} = y^{\mathcal{A}}$.

**Literals of the form $u \approx 0$, $u \approx 1$, $u \approx v + w$, $u \approx v - w$, $u \approx \mathsf{max}(v, w)$, $u \approx \mathsf{min}(v, w)$.** Immediate.

**Literals of the form $x \approx [\![e]\!]^{(u)}$.** Since $e^{\mathcal{B}} \in A_{\mathsf{elem}}$, we have $x^{\mathcal{A}}(e^{\mathcal{A}}) = x^{\mathcal{B}}(e^{\mathcal{B}}) = u^{\mathcal{B}} = u^{\mathcal{A}}$. Next, let $e' \in A_{\mathsf{elem}}$ and $e' \neq e^{\mathcal{B}}$. Then $x^{\mathcal{A}}(e') = x^{\mathcal{B}}(e') = 0$.

**Literals of the form $x \approx y \cup z$, $x \approx y \uplus z$, and $x \approx y \cap z$.** This case is similar to the case of literals of the form $x \approx [\![e]\!]^{(u)}$.

**Literals of the form $u \approx \mathsf{count}(x, e)$.** Since $e^{\mathcal{B}} \in A_{\mathsf{elem}}$, we have $u^{\mathcal{A}} = u^{\mathcal{B}} = x^{\mathcal{B}}\left(e^{\mathcal{B}}\right) = x^{\mathcal{A}}\left(e^{\mathcal{A}}\right)$. ∎

**Proposition 56 (Finite witnessability).** *The theory $T_{\mathsf{bag}}$ is finitely witnessable with respect to the sort* elem. □

PROOF. By Proposition 12, Remark 54, and Proposition 55. ∎

### 10.3 Politeness

**Theorem 57 (Politeness).** *The theory $T_{\mathsf{bag}}$ is polite with respect to* $\{\mathsf{elem}\}$. □

PROOF. By Proposition 53 and 56. ∎

## 11 Conclusion

We addressed the problem of combining a theory $S$ modeling a data structure containing elements of a given nature with a theory $T$ of the elements. We were particularly interested in the case in which $T$ is not stably infinite.

To solve this problem, we defined the notion of polite theories, and we showed that a polite theory $S$ can be combined with any theory $T$, regardless of whether $T$ is stably infinite or not. We then proved that natural examples of polite theories are given by the theory of equality, lists, arrays, sets, and multisets.

Our results were developed using many-sorted logic rather than one-sorted logic. In our experience, combining nonstably infinite theories in one-sorted logic is difficult. By moving to many-sorted logic, we were able to find many practically relevant theories (e.g., lists, arrays, sets, and multisets) that can be combined with nonstably infinite theories.

Concerning future research, we wish to study how polite theories relate to observable theories [3] and local theory extensions [10]. We also wish to implement our combination method in **haRVey** [5], and apply it to the verification of set-based specifications of smart-cards [4].

## Acknowledgments

We are grateful to Pascal Fontaine, Deepak Kapur, and Cesare Tinelli for pleasant discussions on the problem of combining nonstably infinite theories. We are also grateful to the anonymous reviewers for their constructive feedback. Full credit for the results of Section 5 goes to the reviewers.

## References

[1] Franz Baader and Silvio Ghilardi. Connecting many-sorted structures and theories through adjoint functions. In Bernhard Gramlich, editor, *Frontiers of Combining Systems*, Lecture Notes in Computer Science. Springer, 2005.

[2] Franz Baader and Silvio Ghilardi. Connecting many-sorted theories. In Robert Nieuwenhuis, editor, *Automated Deduction – CADE-20*, volume 3632 of *Lecture Notes in Computer Science*. Springer, 2005.

[3] Michel Bidoit and Rolf Hennicker. Behavioural theories and the proof of behavioural properties. *Theoretical Computer Science*, 165(1):3–55, 1996.

[4] Jean-François Couchot, David Déharbe, Alain Giorgetti, and Silvio Ranise. Scalable automated proving and debugging of set-based specifications. *Journal of the Brazilian Computer Society*, 9(2):17–36, 2004.

[5] David Déharbe and Silvio Ranise. Light-weight theorem proving for debugging and verifying units of code. In *Software Engineering and Formal Methods*, pages 220–228. IEEE Computer Society, 2003.

[6] Pascal Fontaine and Pascal Gribomont. Combining non-stably infinite, non-first order theories. In Silvio Ranise and Cesare Tinelli, editors, *Pragmatics of Decision Procedures in Automated Reasoning*, 2004.

[7] Pascal Fontaine, Silvio Ranise, and Calogero G. Zarba. Combining lists with non-stably infinite theories. In Franz Baader and Andrei Voronkov, editors, *Logic for Programming, Artificial Intelligence, and Reasoning*, volume 3452 of *Lecture Notes in Computer Science*, pages 51–66. Springer, 2005.

[8] Vijay Ganesh, Sergey Berezin, and David L. Dill. A decision procedure for fixed-width bit-vectors. Unpublished, 2005.

[9] Harald Ganzinger. Shostak light. In Andrei Voronkov, editor, *Automated Deduction – CADE-18*, volume 2392 of *Lecture Notes in Computer Science*, pages 332–346. Springer, 2002.

[10] Viorica Sofronie-Stokkermans. Hierarchic reasoning in local theory extensions. In Robert Nieuwenhuis, editor, *Automated Deduction – CADE-20*, volume 3632 of *Lecture Notes in Computer Science*. Springer, 2005.

[11] Cesare Tinelli and Calogero G. Zarba. Combining decision procedures for sorted theories. In José Júlio Alferes and João Alexandre Leite, editors, *Logics in Artificial Intelligence*, volume 3229 of *Lecture Notes in Computer Science*, pages 641–653. Springer, 2004.

[12] Cesare Tinelli and Calogero G. Zarba. Combining nonstably infinite theories. *Journal of Automated Reasoning*, 2005. To appear.

[13] Calogero G. Zarba. Combining multisets with integers. In Andrei Voronkov, editor, *Automated Deduction – CADE-18*, volume 2392 of *Lecture Notes in Computer Science*, pages 363–376. Springer, 2002.

[14] Calogero G. Zarba. Combining sets with elements. In Nachum Dershowitz, editor, *Verification: Theory and Practice*, volume 2772 of *Lecture Notes in Computer Science*, pages 762–782. Springer, 2004.

Unité de recherche INRIA Lorraine
LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rhône-Alpes : 655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399