

Politeness and Stable Infiniteness: Stronger Together

Ying Sheng¹, Yoni Zohar¹, Christophe Ringeissen²,
Andrew Reynolds³, Clark Barrett¹, and Cesare Tinelli³

¹ Stanford University, Stanford, CA, USA

² Université de Lorraine, CNRS, Inria, LORIA, F-54000 Nancy, France

³ The University of Iowa, Iowa City, IA, USA

Abstract. We make two contributions to the study of polite combination in satisfiability modulo theories. The first is a separation between politeness and strong politeness, by presenting a polite theory that is not strongly polite. This result shows that proving strong politeness (which is often harder than proving politeness) is sometimes needed in order to use polite combination. The second contribution is an optimization to the polite combination method, obtained by borrowing from the Nelson-Oppen method. The Nelson-Oppen method is based on guessing arrangements over shared variables. In contrast, polite combination requires an arrangement over *all* variables of the shared sorts. We show that when using polite combination, if the other theory is stably infinite with respect to a shared sort, only the shared variables of that sort need be considered in arrangements, as in the Nelson-Oppen method. The time required to reason about arrangements is exponential in the worst case, so reducing the number of variables considered has the potential to improve performance significantly. We show preliminary evidence for this by demonstrating a speed-up on a smart contract verification benchmark.

1 Introduction

Solvers for satisfiability modulo theories (SMT) [5] are used in a wide variety of applications. Many of these applications require determining the satisfiability of formulas with respect to a *combination* of background theories. In order to make reasoning about combinations of theories modular and easily extensible, a combination framework is essential. Combination frameworks provide mechanisms for automatically deriving a decision procedure for the combined theories by using the decision procedures for the individual theories as black boxes. To integrate a new theory into such a framework, it then suffices to focus on the decoupled decision procedure for the new theory alone, together with its interface to the generic combination framework.

In 1979, Nelson and Oppen [16] proposed a general framework for combining theories with disjoint signatures. In this framework, a quantifier-free formula in the combined theory is purified to a conjunction of formulas, one for each theory. Each pure formula is then sent to a dedicated theory solver, along with a guessed

arrangement (a set of equalities and disequalities that capture an equivalence relation) of the variables shared among the pure formulas. For completeness [15], this method requires all component theories to be stably infinite. While many important theories are stably infinite, some are not, including the widely-used theory of fixed-length bit-vectors. To address this issue, the polite combination method was introduced by Ranise et al. [17], and later refined by Jovanovic and Barrett [12]. In polite combination, one theory must be *polite*, a stronger requirement than stable-infiniteness, but the requirement on the other theory is relaxed: specifically, it need not be stably infinite. The price for this generality is that unlike the Nelson-Oppen method, polite combination requires guessing arrangements over *all* variables of certain sorts, not just the shared ones. At a high level, polite theories have two properties: smoothness and finite witnessability (see Section 2). The polite combination theorem in [17] contained an error, which was identified in [12]. A fix was also proposed in [12], which relies on stronger requirements for finite witnessability. Following Casal and Rasga [8], we call this strengthened version *strong finite witnessability*. A theory that is both smooth and strongly finitely witnessable is called *strongly polite*.

This paper makes two contributions. First, we give an affirmative answer to the question of whether politeness and strong politeness are different notions, by giving an example of a theory that is polite but not strongly polite. The given theory is over an empty signature and has two sorts, and was originally studied in [8] in the context of shiny theories. Here we state and prove the separation of politeness and strong politeness, without using shiny theories. Proving that a theory is strongly polite is harder than proving that it is just polite. This result shows that the additional effort is sometimes needed in order to be able to use the combination theorem from [12]. We show that for empty signatures, at least two sorts are needed to present a polite theory that is not strongly polite. However, for the empty signature with only one sort, there is a finitely witnessable theory that is not strongly finite witnessable. Such a theory cannot be smooth.

Second, we explore different polite combination scenarios, where additional information is known about the theories being combined. In particular, we improve the polite combination method for the case where one theory is strongly polite w.r.t. a set S of sorts and the other is stably infinite w.r.t. a subset $S' \subseteq S$ of the sorts. For such cases, we show that it is possible to perform Nelson-Oppen combination for S' and polite combination for $S \setminus S'$. This means that for the sorts in S' , only shared variables need to be considered for the guessed arrangement, which can considerably reduce its size. We also show that the set of shared variables can be reduced for a couple of other variations of conditions on the theories. Finally, we present a preliminary case study using a challenge benchmark from a smart contract verification application. We show that the reduction of shared variables is evident and significantly improves the solving time. Verification of smart contracts using SMT (and the analyzed benchmark in particular) is the main motivation behind the second contribution of this paper.

Related Work: Polite combination is part of a more general effort to replace the stable infiniteness symmetric condition in the Nelson-Oppen approach with a

weaker condition. Other examples of this effort include the notions of *shiny* [21], *parametric* [13], and *gentle* [11] theories. Gentle, shiny, and polite theories can be combined à la Nelson-Oppen with any arbitrary theory. Shiny theories were introduced by Tinelli and Zarba [21] as a class of mono-sorted theories. Based on the same principles as shininess, politeness is particularly well-suited to deal with theories expressed in many-sorted logic. Polite theories were introduced by Ranise et al. [17] to provide a more effective combination approach compared to parametric and shiny theories, the former requiring solvers to reason about cardinalities and the latter relying on expensive computations of minimal cardinalities of models. Shiny theories were extended to many-sorted signatures in [17], where there is a sufficient condition for their equivalence with polite theories. For the mono-sorted case, a sufficient condition for the equivalence of shiny theories and strongly polite theories was given by Casal and Rasga [7]. In later work [8], the same authors proposed a generalization of shiny theories to many-sorted signatures different from the one in [17], and proved that it is equivalent to strongly polite theories with a decidable quantifier-free fragment. The strong politeness of the theory of algebraic datatypes [4] was proven in [18]. That paper also introduced *additive witnesses*, that provided a sufficient condition for a polite theory to be also strongly polite. In this paper we present a theory that is polite but not strongly polite. In accordance with [18], the witness that we provide for this theory is not additive.

The paper is organized as follows. Section 2 provides the necessary notions from first-order logic and polite theories. Section 3 discusses the difference between politeness and strong politeness and shows they are not equivalent. Section 4 gives the improvements for the combination process under certain conditions, and Section 5 demonstrates the effectiveness of these improvements for a challenge benchmark.⁴

2 Preliminaries

2.1 Signatures and Structures

We briefly review the usual definitions of many-sorted first-order logic with equality (see [10,19] for more details). A *signature* Σ consists of a set \mathcal{S}_Σ (of *sorts*), a set \mathcal{F}_Σ of function symbols, and a set \mathcal{P}_Σ of predicate symbols. We assume \mathcal{S}_Σ , \mathcal{F}_Σ and \mathcal{P}_Σ are countable. Function symbols have arities of the form $\sigma_1 \times \dots \times \sigma_n \rightarrow \sigma$, and predicate symbols have arities of the form $\sigma_1 \times \dots \times \sigma_n$, with $\sigma_1, \dots, \sigma_n, \sigma \in \mathcal{S}_\Sigma$. For each sort $\sigma \in \mathcal{S}_\Sigma$, \mathcal{P}_Σ includes an *equality symbol* $=_\sigma$ of arity $\sigma \times \sigma$. We denote it by $=$ when σ is clear from context. When $=_\sigma$ are the only symbols in Σ , we say that Σ is *empty*. If two signatures share no symbols except $=_\sigma$ we call them *disjoint*. We assume an underlying countably infinite set of variables for each sort. Terms, formulas, and literals are defined in the usual way. For a Σ -formula ϕ and a sort σ , we denote the set of free variables

⁴ Due to space constraints, some proofs are omitted. They can be found in an extended version at <https://arxiv.org/abs/2104.11738>.

in ϕ of sort σ by $\text{vars}_\sigma(\phi)$. This notation naturally extends to $\text{vars}_S(\phi)$ when S is a set of sorts. $\text{vars}(\phi)$ is the set of all free variables in ϕ . We denote by $QF(\Sigma)$ the set of quantifier-free Σ -formulas.

A Σ -structure is a many-sorted structure that provides semantics for the symbols in Σ (but not for variables). It consists of a domain $\sigma^{\mathcal{A}}$ for each sort $\sigma \in \mathcal{S}_\Sigma$, an interpretation $f^{\mathcal{A}}$ for every $f \in \mathcal{F}_\Sigma$, as well as an interpretation $P^{\mathcal{A}}$ for every $P \in \mathcal{P}_\Sigma$. We further require that $=_\sigma$ be interpreted as the identity relation over $\sigma^{\mathcal{A}}$ for every $\sigma \in \mathcal{S}_\Sigma$. A Σ -interpretation \mathcal{A} is an extension of a Σ -structure with interpretations for some set of variables. For any Σ -term α , $\alpha^{\mathcal{A}}$ denotes the interpretation of α in \mathcal{A} . When α is a set of Σ -terms, $\alpha^{\mathcal{A}} = \{x^{\mathcal{A}} \mid x \in \alpha\}$. Satisfaction is defined as usual. $\mathcal{A} \models \varphi$ denotes that \mathcal{A} satisfies φ .

A Σ -theory \mathcal{T} is a class of all Σ -structures that satisfy some set Ax of Σ -sentences. For each such set Ax , we say that \mathcal{T} is *axiomatized* by Ax . A Σ -interpretation whose variable-free part is in \mathcal{T} is called a \mathcal{T} -interpretation. A Σ -formula ϕ is \mathcal{T} -satisfiable if $\mathcal{A} \models \phi$ for some \mathcal{T} -interpretation \mathcal{A} . A set A of Σ -formulas is \mathcal{T} -satisfiable if $\mathcal{A} \models \phi$ for every $\phi \in A$. Two formulas ϕ and ψ are \mathcal{T} -equivalent if they are satisfied by the same \mathcal{T} -interpretations.

Note that for any class \mathcal{C} of Σ -structures there is a theory $\mathcal{T}_{\mathcal{C}}$ that *corresponds* to it, with the same satisfiable formulas: the Σ -theory axiomatized by the set Ax of Σ -sentences that are satisfied in every structure of \mathcal{C} . In the examples that follow, we define theories $\mathcal{T}_{\mathcal{C}}$ implicitly by specifying only the class \mathcal{C} , as done in the SMT-LIB 2 standard [2]. This can be done without loss of generality.

Example 1. Let Σ_{List} be a signature of finite lists containing the sorts elem_1 , elem_2 , and list , as well as the function symbols cons of arity $\text{elem}_1 \times \text{elem}_2 \times \text{list} \rightarrow \text{list}$, car_1 of arity $\text{list} \rightarrow \text{elem}_1$, car_2 of arity $\text{list} \rightarrow \text{elem}_2$, cdr of arity $\text{list} \rightarrow \text{list}$, and nil of arity list . The Σ_{List} -theory $\mathcal{T}_{\text{List}}$ corresponds to an SMT-LIB 2 theory of algebraic datatypes [2,4], where elem_1 and elem_2 are interpreted as some sets (of “elements”), and list is interpreted as finite lists of pairs of elements, one from elem_1 and the other from elem_2 . cons is a list constructor that takes two elements and a list, and inserts the two elements at the head of the list. The pair $(\text{car}_1(l), \text{car}_2(l))$ is the first entry in l , and $\text{cdr}(l)$ is the list obtained from l by removing its first entry. nil is the empty list. \square

Example 2. The signature Σ_{Int} includes a single sort int , all numerals $0, 1, \dots$, the function symbols $+$, $-$ and \cdot of arity $\text{int} \times \text{int} \rightarrow \text{int}$ and the predicate symbols $<$ and \leq of arity $\text{int} \times \text{int}$. The Σ_{Int} -theory \mathcal{T}_{Int} corresponds to integer arithmetic in SMT-LIB 2, and the interpretation of the symbols is the same as in the standard structure of the integers. The signature Σ_{BV4} includes a single sort BV4 and various function and predicate symbols for reasoning about bit-vectors of length 4 (such as $\&$ for bit-wise *and*, constants of the form 0110, etc.). The Σ_{BV4} -theory \mathcal{T}_{BV4} corresponds to SMT-LIB 2 bit-vectors of size 4, with the expected semantics of constants and operators. \square

Let Σ_1, Σ_2 be signatures, \mathcal{T}_1 a Σ_1 -theory, and \mathcal{T}_2 a Σ_2 -theory. The *combination* of \mathcal{T}_1 and \mathcal{T}_2 , denoted $\mathcal{T}_1 \oplus \mathcal{T}_2$, consists of all $\Sigma_1 \cup \Sigma_2$ -structures \mathcal{A} , such that \mathcal{A}^{Σ_1} is in \mathcal{T}_1 and \mathcal{A}^{Σ_2} is in \mathcal{T}_2 , where \mathcal{A}^{Σ_i} is the reduct of \mathcal{A} to Σ_i for $i \in \{1, 2\}$.

Example 3. Let $\mathcal{T}_{\text{IntBV4}}$ be $\mathcal{T}_{\text{Int}} \oplus \mathcal{T}_{\text{BV4}}$. It is the combined theory of integers and bit-vectors. It has all the sorts and operators from both theories. If we rename the sorts elem_1 and elem_2 of Σ_{List} to int and BV4 , respectively, we can obtain a theory $\mathcal{T}_{\text{ListIntBV4}}$ defined as $\mathcal{T}_{\text{IntBV4}} \oplus \mathcal{T}_{\text{List}}$. This is the theory of lists of pairs, where each pair consists of an integer and a bit-vector of size 4. \square

The following definitions and theorems will be useful in the sequel.

Theorem 1 (Theorem 9 of [19]). *Let Σ be a signature, and A a set of Σ -formulas that is satisfiable. Then there exists an interpretation \mathcal{A} that satisfies A , in which $\sigma^{\mathcal{A}}$ is countable whenever it is infinite.⁵*

Definition 1 (Arrangement). *Let V be a finite set of variables whose sorts are in S and let $\{V_\sigma \mid \sigma \in S\}$ be a partition of V such that V_σ is the set of variables of sort σ in V . A formula δ is an arrangement of V if*

$$\delta = \bigwedge_{\sigma \in S} \left(\bigwedge_{(x,y) \in E_\sigma} (x = y) \wedge \bigwedge_{x,y \in V_\sigma, (x,y) \notin E_\sigma} (x \neq y) \right),$$

where E_σ is some equivalence relation over V_σ for each $\sigma \in S$.

The following theorem from [12] is a variant of a theorem from [20].

Theorem 2 (Theorem 2.5 of [12]). *For $i = 1, 2$, let Σ_i be disjoint signatures, $S_i = \mathcal{S}_{\Sigma_i}$ with $S = S_1 \cap S_2$, \mathcal{T}_i be a Σ_i -theory, Γ_i be a set of Σ_i -literals, and $V = \text{vars}(\Gamma_1) \cap \text{vars}(\Gamma_2)$. If there exist a \mathcal{T}_1 -interpretation \mathcal{A} , a \mathcal{T}_2 interpretation \mathcal{B} , and an arrangement δ_V of V such that: 1. $\mathcal{A} \models \Gamma_1 \cup \delta_V$; 2. $\mathcal{B} \models \Gamma_2 \cup \delta_V$; and 3. $|A_\sigma| = |B_\sigma|$ for every $\sigma \in S$, then $\Gamma_1 \cup \Gamma_2$ is $\mathcal{T}_1 \oplus \mathcal{T}_2$ -satisfiable.*

2.2 Polite Theories

We now give the background definitions necessary for both Nelson-Oppen and polite combination. In what follows, Σ is an arbitrary (many-sorted) signature, $S \subseteq \mathcal{S}_\Sigma$, and \mathcal{T} is a Σ -theory. We start with stable infiniteness and smoothness.

Definition 2 (Stably Infinite). *\mathcal{T} is stably infinite with respect to S if every quantifier-free Σ -formula that is \mathcal{T} -satisfiable is also satisfiable in a \mathcal{T} -interpretation \mathcal{A} in which $\sigma^{\mathcal{A}}$ is infinite for every $\sigma \in S$.*

Definition 3 (Smooth). *\mathcal{T} is smooth w.r.t. S if for every quantifier-free formula ϕ , \mathcal{T} -interpretation \mathcal{A} that satisfies ϕ , and function κ from S to the class of cardinals such that $\kappa(\sigma) \geq |\sigma^{\mathcal{A}}|$ for every $\sigma \in S$, there exists a \mathcal{T} -interpretation \mathcal{A}' that satisfies ϕ with $|\sigma^{\mathcal{A}'}| = \kappa(\sigma)$ for every $\sigma \in S$.*

⁵ In [19] this was proven more generally, for ordered sorted logics.

We identify singleton sets with their single elements when there is no ambiguity (e.g., when saying that a theory is smooth w.r.t. a sort σ).

We next define politeness and related concepts, following the presentation in [18]. Let ϕ be a quantifier-free Σ -formula. A Σ -interpretation \mathcal{A} *finitely witnesses* ϕ for \mathcal{T} w.r.t. S (or, is a *finite witness* of ϕ for \mathcal{T} w.r.t. S), if $\mathcal{A} \models \phi$ and $\sigma^{\mathcal{A}} = \text{vars}_\sigma(\phi)^{\mathcal{A}}$ for every $\sigma \in S$. We say that ϕ is *finitely witnessed* for \mathcal{T} w.r.t. S if it is either \mathcal{T} -unsatisfiable or has a finite witness for \mathcal{T} w.r.t. S . We say that ϕ is *strongly finitely witnessed* for \mathcal{T} w.r.t. S if $\phi \wedge \delta_V$ is finitely witnessed for \mathcal{T} w.r.t. S for every arrangement δ_V of V , where V is any set of variables whose sorts are in S . A function $\text{wit} : QF(\Sigma) \rightarrow QF(\Sigma)$ is a (*strong*) *witness* for \mathcal{T} w.r.t. S if for every $\phi \in QF(\Sigma)$ we have that: 1. ϕ and $\exists \vec{w}. \text{wit}(\phi)$ are \mathcal{T} -equivalent for $\vec{w} = \text{vars}(\text{wit}(\phi)) \setminus \text{vars}(\phi)$; and 2. $\text{wit}(\phi)$ is (strongly) finitely witnessed for \mathcal{T} w.r.t. S . \mathcal{T} is (*strongly*) *finitely witnessable* w.r.t. S if there exists a computable (strong) witness for \mathcal{T} w.r.t. S . \mathcal{T} is (*strongly*) *polite* w.r.t. S if it is smooth and (strongly) finitely witnessable w.r.t. S .

3 Politeness and Strong Politeness

In this section, we study the difference between politeness and strong politeness. Since the introduction of strong politeness in [12], it has been unclear whether it is strictly stronger than politeness, that is, whether there exists a theory that is polite but not strongly polite. We present an example of such a theory, answering the open question affirmatively. This result is followed by further analysis of notions related to politeness. This section is organized as follows. In Section 3.1 we reformulate an example given in [12], showing that there are witnesses that are not strong witnesses. We then present a polite theory that is not strongly polite in Section 3.2. The theory is over a signature with two sorts that is otherwise empty. We show in Section 3.3 that politeness and strong politeness are equivalent for empty signatures with a single sort. Finally, we show in Section 3.4 that this equivalence does not hold for finite witnessability alone.

3.1 Witnesses vs. Strong Witnesses

In [12], an example was given for a witness that is not strong. We reformulate this example in terms of the notions that are defined in the current paper, that is, witnessed formulas are not the same as strongly witnessed formulas (Example 4), and witnesses are not the same as strong witnesses (Example 5).

Example 4. Let Σ_0 be a signature with a single sort σ and no function or predicate symbols, and let \mathcal{T}_0 be a Σ_0 -theory consisting of all Σ_0 -structures with at least two elements. Let ϕ be the formula $x = x \wedge w = w$. This formula is finitely witnessed for \mathcal{T}_0 w.r.t. σ , but not strongly. Indeed, for $\delta_V \equiv (x = w)$, $\phi \wedge \delta_V$ is not finitely witnessed for \mathcal{T}_0 w.r.t. σ : a finite witness would be required to have only a single element and would therefore not be a \mathcal{T}_0 -interpretation. \square

The next example shows that witnesses and strong witnesses are not equivalent.

Example 5. Take Σ_0 , σ , and \mathcal{T}_0 as in Example 4, and define $wit(\phi)$ as the function $(\phi \wedge w_1 = w_1 \wedge w_2 = w_2)$ for fresh w_1, w_2 . The function is a witness for \mathcal{T}_0 w.r.t. σ . However, it is not a strong witness for \mathcal{T} w.r.t. σ . \square

Although the theory \mathcal{T}_0 in the above examples does serve to distinguish formulas and witnesses that are and are not strong, it cannot be used to do the same for theories themselves. This is because \mathcal{T}_0 is, in fact, strongly polite, via a different witness function.

Example 6. The function $wit'(\phi) = (\phi \wedge w_1 \neq w_2)$, for some $w_1, w_2 \notin vars_\sigma(\phi)$, is a strong witness for \mathcal{T}_0 w.r.t. S , as proved in [12]. \square

A natural question, then, is whether there is a theory that can separate the two notions of politeness. The following subsection provides an affirmative answer.

3.2 A Polite Theory that is not Strongly Polite

Let Σ_2 be a signature with two sorts σ_1 and σ_2 and no function or predicate symbols (except $=$). Let $\mathcal{T}_{2,3}$ be the Σ_2 -theory from [8], consisting of all Σ_2 -structures \mathcal{A} such that either $|\sigma_1^{\mathcal{A}}| = 2 \wedge |\sigma_2^{\mathcal{A}}| \geq \aleph_0$ or $|\sigma_1^{\mathcal{A}}| \geq 3 \wedge |\sigma_2^{\mathcal{A}}| \geq 3$ [8].⁶

$\mathcal{T}_{2,3}$ is polite, but is not strongly polite. Its smoothness is shown by extending any given structure with new elements as much as necessary.

Lemma 1. $\mathcal{T}_{2,3}$ is smooth w.r.t. $\{\sigma_1, \sigma_2\}$.

For finite witnessability, consider the function wit defined as follows:

$$wit(\phi) := \phi \wedge x_1 = x_1 \wedge x_2 = x_2 \wedge x_3 = x_3 \wedge y_1 = y_1 \wedge y_2 = y_2 \wedge y_3 = y_3 \quad (1)$$

for fresh variables x_1, x_2 , and x_3 of sort σ_1 and y_1, y_2 , and y_3 of sort σ_2 . It can be shown that wit is a witness for $\mathcal{T}_{2,3}$ but there is no strong witness for it.

Lemma 2. $\mathcal{T}_{2,3}$ is finitely witnessable w.r.t. $\{\sigma_1, \sigma_2\}$.

Lemma 3. $\mathcal{T}_{2,3}$ is not strongly finitely witnessable w.r.t. $\{\sigma_1, \sigma_2\}$.

Lemmas 1 to 3 have shown that $\mathcal{T}_{2,3}$ is polite but is not strongly polite. And indeed, using the polite combination method from [12] with this theory can cause problems. Consider the theory $\mathcal{T}_{1,1}$ that consists of all Σ_2 -structures \mathcal{A} such that $|\sigma_1^{\mathcal{A}}| = |\sigma_2^{\mathcal{A}}| = 1$. Clearly, $\mathcal{T}_{1,1} \oplus \mathcal{T}_{2,3}$ is empty, and hence no formula is $\mathcal{T}_{1,1} \oplus \mathcal{T}_{2,3}$ -satisfiable. However, denote the formula *true* by Γ_1 and the formula $x = x$ by Γ_2 for some variable x of sort σ_1 . Then $wit(\Gamma_2)$ is $x = x \wedge \bigwedge_{i=1}^3 x_i = x_i \wedge y_i = y_i$. Let δ be the arrangement $x = x_1 = x_2 = x_3 \wedge y_1 = y_2 = y_3$. It can be shown that $wit(\Gamma_2) \wedge \delta$ is $\mathcal{T}_{2,3}$ -satisfiable and $\Gamma_1 \wedge \delta$ is $\mathcal{T}_{1,1}$ -satisfiable. Hence the combination method of [12] would consider $\Gamma_1 \wedge \Gamma_2$ to be $\mathcal{T}_{1,1} \oplus \mathcal{T}_{2,3}$ -satisfiable, which is impossible. Hence the fact that $\mathcal{T}_{2,3}$ is not strongly polite propagates all the way to the polite combination method.⁷

⁶ In [8], the first condition is written $|\sigma_1^{\mathcal{A}}| \geq 2$. We use equality as this is equivalent and we believe it makes things clearer.

⁷ Notice that $\mathcal{T}_{2,3}$ can be axiomatized using the following set of axioms, given the definitions in Figure 1: $\{\psi_{\geq 2}^{\sigma_1}, \psi_{\geq 3}^{\sigma_2}\} \cup \{\psi_{=2}^{\sigma_1} \rightarrow \neg \psi_{=n}^{\sigma_2} \mid n \geq 3\}$

$$\begin{aligned}
\text{distinct}(x_1, \dots, x_n) &:= \bigwedge_{1 \leq i < j \leq n} x_i \neq x_j \\
\psi_{\geq n}^\sigma &:= \exists x_1, \dots, x_n. \text{distinct}(x_1, \dots, x_n) \\
\psi_{\leq n}^\sigma &:= \exists x_1, \dots, x_n. \forall y. \bigvee_{i=1}^n y = x_i \\
\psi_{=n}^\sigma &:= \psi_{\geq n}^\sigma \wedge \psi_{\leq n}^\sigma
\end{aligned}$$

Fig. 1. Cardinality formulas for sort σ . All variables are assumed to have sort σ .

Remark 1. An alternative way to separate politeness from strong politeness using $\mathcal{T}_{2,3}$ can be obtained through shiny theories, as follows. Shiny theories were introduced in [21] for the mono-sorted case, and were generalized to many-sorted signatures in two different ways in [8] and [17]. In [8], $T_{2,3}$ was introduced as a theory that is shiny according [17], but not according to [8]. Theorem 1 of [8] states that their notion of shininess is equivalent to strong politeness for theories in which the satisfiability problem for quantifier-free formulas is decidable. Since this is the case for $T_{2,3}$, and since it is not shiny according to [8], we get that $T_{2,3}$ is not strongly polite. Further, Proposition 18 of [17] states that every shiny theory (according to their definition) is polite. Hence we get that $T_{2,3}$ is polite but not strongly polite.

We have (and prefer) a direct proof based only on politeness, without a detour through shininess. Note also that [8] dealt only with strongly polite theories and did not study the weaker notion of polite theories. In particular, the fact that strong politeness is different from politeness was not stated nor proved there.

3.3 The Case of Mono-sorted Polite Theories

Theory $\mathcal{T}_{2,3}$ includes two sorts but is otherwise empty. In this section, we show that requiring two sorts is essential for separating politeness from strong politeness in otherwise empty signatures. That is, we prove that politeness implies strong politeness otherwise. Let Σ_0 be the signature with a single sort σ and no function or predicate symbols (except $=$). We show that smooth Σ_0 -theories have a certain form and conclude strong politeness from politeness.

Lemma 4. *Let \mathcal{T} be a Σ_0 -theory. If \mathcal{T} is smooth w.r.t. σ and includes a finite structure, \mathcal{T} is axiomatized by $\psi_{\geq n}^\sigma$ from Figure 1 for some $n > 0$.*

Proposition 1. *If \mathcal{T} is a Σ_0 -theory that is polite w.r.t. σ , then it is strongly polite w.r.t. σ .*

Remark 2. We again note (as we did in Remark 1) that an alternative way to obtain this result is via shiny theories, using [17], which introduced polite theories, as well as [7], which compared strongly polite theories to shiny theories

in the mono-sorted case. Specifically, in the presence of a single sort, Proposition 19 of [17] states that:

- (*) if the question of whether a polite theory over a finite signature contains a finite structure is decidable, the theory is shiny.

In turn, Proposition 1 of [7] states that:

- (**) every shiny theory over a mono-sorted signature with a decidable satisfiability problem for quantifier-free formulas is also strongly polite.

It can be shown that the question of whether a polite Σ_0 -theory contains a finite structure is decidable. It can also be shown that satisfiability of quantifier-free formulas is decidable for such theories. Using (*) and (**), we get that in Σ_0 -theories, politeness implies strong politeness. As above (Remark 1), we prefer a direct route for showing this result, without going through shiny theories.

3.4 Mono-sorted Finite Witnessability

We have seen that for Σ_0 -theories, politeness and strong politeness are the same. Now we show that smoothness is crucial for this equivalence, i.e., that there is no such equivalence between finite witnessability and strong finite witnessability. Let $\mathcal{T}_{\text{Even}}^\infty$ be the Σ_0 -theory of all Σ_0 -structures \mathcal{A} such that $|\sigma^{\mathcal{A}}|$ is even or infinite.⁸ Clearly, this theory is not smooth.

Lemma 5. *$\mathcal{T}_{\text{Even}}^\infty$ is not smooth w.r.t. σ .*

We can construct a witness *wit* for $\mathcal{T}_{\text{Even}}^\infty$ as follows. Let ϕ be a quantifier-free Σ_0 -formula, and let E be the set of all equivalence relations over $\text{vars}(\phi) \cup \{w\}$ for some fresh variable w . Let $\text{even}(E)$ be the set of all equivalence relations in E with an even number of equivalence classes. Then, $\text{wit}(\phi)$ is $\phi \wedge \bigvee_{e \in \text{even}(E)} \delta_e$, where for each $e \in \text{even}(E)$, δ_e is the arrangement induced by e :

$$\bigwedge_{(x,y) \in e} x = y \wedge \bigwedge_{x,y \in \text{vars}(\phi) \cup \{w\} \wedge (x,y) \notin e} x \neq y$$

It can be shown that *wit* is indeed a witness, and that $\mathcal{T}_{\text{Even}}^\infty$ has no strong witness, with a proof similar to that of Lemma 3.

Lemma 6. *$\mathcal{T}_{\text{Even}}^\infty$ is finitely witnessable w.r.t. σ .*

Lemma 7. *$\mathcal{T}_{\text{Even}}^\infty$ is not strongly finitely witnessable w.r.t. σ .*

4 A Blend of Polite and Stably-Infinite Theories

In this section, we show that the polite combination method can be optimized to reduce the search space of possible arrangements. In what follows, Σ_1 and Σ_2 are disjoint signatures, $S = \mathcal{S}_{\Sigma_1} \cap \mathcal{S}_{\Sigma_2}$, \mathcal{T}_1 is a Σ_1 -theory, \mathcal{T}_2 is a Σ_2 -theory, Γ_1 is a set of Σ_1 -literals, and Γ_2 is a set of Σ_2 -literals.

⁸ Notice that $\mathcal{T}_{\text{Even}}^\infty$ can be axiomatized using the set $\{\neg\psi_{=2n+1}^\sigma \mid n \in \mathbb{N}\}$.

The Nelson-Oppen procedure reduces the $\mathcal{T}_1 \oplus \mathcal{T}_2$ -satisfiability of $\Gamma_1 \cup \Gamma_2$ to the existence of an arrangement δ over the set $V = \text{vars}_S(\Gamma_1) \cap \text{vars}_S(\Gamma_2)$, such that $\Gamma_1 \cup \delta$ is \mathcal{T}_1 -satisfiable and $\Gamma_2 \cup \delta$ is \mathcal{T}_2 -satisfiable. The correctness of this reduction relies on the fact that both theories are stably infinite w.r.t. S . In contrast, the polite combination method only requires a condition (namely strong politeness) from one of the theories, while the other theory is unrestricted and, in particular, not necessarily stably infinite. In polite combination, the $\mathcal{T}_1 \oplus \mathcal{T}_2$ -satisfiability of $\Gamma_1 \cup \Gamma_2$ is again reduced to the existence of an arrangement δ , but over a different set $V' = \text{vars}_S(\text{wit}(\Gamma_2))$, such that $\Gamma_1 \cup \delta$ is \mathcal{T}_1 -satisfiable and $\text{wit}(\Gamma_2) \cup \delta$ is \mathcal{T}_2 -satisfiable, where wit is a strong witness for \mathcal{T}_2 w.r.t. S . Thus, the flexibility offered by polite combination comes with a price. The set V' is potentially larger than V as it contains *all* variables with sorts in S that occur in $\text{wit}(\Gamma_2)$, not just those that also occur in Γ_1 . Since the search space of arrangements over a set grows exponentially with its size, this difference can become crucial. If \mathcal{T}_1 happens to be stably infinite w.r.t. S , however, we can fall back to Nelson-Oppen combination and only consider variables that are shared by the two sets. But what if \mathcal{T}_1 is stably infinite only w.r.t. to some proper subset $S' \subset S$? Can this knowledge about \mathcal{T}_1 help in finding some set V'' of variables between V and V' , such that we need only consider arrangements of V'' ? In this section we prove that this is possible by taking V'' to include only the variables of sorts in S' that are shared between Γ_1 and $\text{wit}(\Gamma_2)$, and all the variables of sorts in $S \setminus S'$ that occur in $\text{wit}(\Gamma_2)$. We also identify several weaker conditions on \mathcal{T}_2 that are sufficient for the combination theorem to hold.

4.1 Refined Combination Theorem

To put the discussion above in formal terms, we recall the following theorem.

Theorem 3 ([12]). *If \mathcal{T}_2 is strongly polite w.r.t. S with a witness wit , then the following are equivalent: 1. $\Gamma_1 \cup \Gamma_2$ is $(\mathcal{T}_1 \oplus \mathcal{T}_2)$ -satisfiable; 2. there exists an arrangement δ_V over V , such that $\Gamma_1 \cup \delta_V$ is \mathcal{T}_1 -satisfiable and $\text{wit}(\Gamma_2) \cup \delta_V$ is \mathcal{T}_2 -satisfiable, where $V = \bigcup_{\sigma \in S} V_\sigma$, and $V_\sigma = \text{vars}_\sigma(\text{wit}(\Gamma_2))$ for each $\sigma \in S$.*

Our goal is to identify general cases in which information regarding \mathcal{T}_1 can help reduce the size of the set V . We extend the definitions of stably infinite, smooth, and strongly finitely witnessable to two sets of sorts rather than one. Roughly speaking, in this extension, the usual definition is taken for the first set, and some cardinality-preserving constraints are enforced on the second set.

Definition 4. *Let Σ be a signature, S_1, S_2 two disjoint subsets of S_Σ , and \mathcal{T} a Σ -theory.*

\mathcal{T} is (strongly) stably infinite w.r.t. (S_1, S_2) if for every quantifier-free Σ -formula ϕ and \mathcal{T} -interpretation \mathcal{A} satisfying ϕ , there exists a \mathcal{T} -interpretation \mathcal{B} such that $\mathcal{B} \models \phi$, $|\sigma^{\mathcal{B}}|$ is infinite for every $\sigma \in S_1$, and $|\sigma^{\mathcal{B}}| \leq |\sigma^{\mathcal{A}}|$ ($|\sigma^{\mathcal{B}}| = |\sigma^{\mathcal{A}}|$) for every $\sigma \in S_2$.

\mathcal{T} is smooth w.r.t. (S_1, S_2) if for every quantifier-free Σ -formula ϕ , \mathcal{T} -interpretation \mathcal{A} satisfying ϕ , and function κ from S_1 to the class of cardinals

such that $\kappa(\sigma) \geq |\sigma^A|$ for each $\sigma \in S_1$, there exists a \mathcal{T} -interpretation \mathcal{B} that satisfies ϕ , with $|\sigma^B| = \kappa(\sigma)$ for each $\sigma \in S_1$, and with $|\sigma^B|$ infinite whenever $|\sigma^A|$ is infinite for each $\sigma \in S_2$.

\mathcal{T} is strongly finitely witnessable w.r.t. (S_1, S_2) if there exists a computable function $wit : QF(\Sigma) \rightarrow QF(\Sigma)$ such that for every quantifier-free Σ -formula ϕ : 1. ϕ and $\exists \vec{w}. wit(\phi)$ are \mathcal{T} -equivalent for $\vec{w} = \text{vars}(wit(\phi)) \setminus \text{vars}(\phi)$; and 2. for every \mathcal{T} -interpretation \mathcal{A} and arrangement δ of any set of variables whose sorts are in S_1 , if \mathcal{A} satisfies $wit(\phi) \wedge \delta$, then there exists a \mathcal{T} -interpretation \mathcal{B} that finitely witnesses $wit(\phi) \wedge \delta$ w.r.t. S_1 and for which $|\sigma^B|$ is infinite whenever $|\sigma^A|$ is infinite, for each $\sigma \in S_2$.

Our main result is the following.

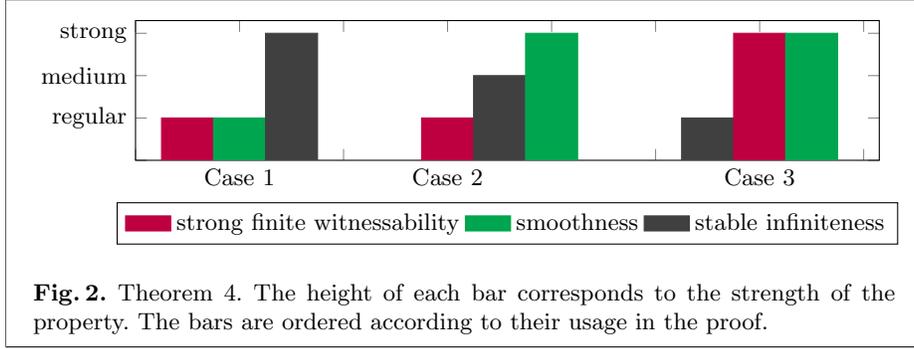
Theorem 4. *Let $S^{si} \subseteq S$ and $S^{nsi} = S \setminus S^{si}$. Suppose \mathcal{T}_1 is stably infinite w.r.t. S^{si} and one of the following holds:*

1. \mathcal{T}_2 is strongly stably infinite w.r.t. (S^{si}, S^{nsi}) and strongly polite w.r.t. S^{nsi} with a witness wit .
2. \mathcal{T}_2 is stably infinite w.r.t. (S^{si}, S^{nsi}) , smooth w.r.t. (S^{nsi}, S^{si}) , and strongly finitely witnessable w.r.t. S^{nsi} with a witness wit .
3. \mathcal{T}_2 is stably infinite w.r.t. S^{si} while smooth and strongly finitely-witnessable w.r.t. (S^{nsi}, S^{si}) with a witness wit .

Then the following are equivalent: 1. $\Gamma_1 \cup \Gamma_2$ is $(\mathcal{T}_1 \oplus \mathcal{T}_2)$ -satisfiable; 2. There exists an arrangement δ_V over V such that $\Gamma_1 \cup \delta_V$ is \mathcal{T}_1 -satisfiable, and $wit(\Gamma_2) \cup \delta_V$ is \mathcal{T}_2 -satisfiable, where $V = \bigcup_{\sigma \in S} V_\sigma$, with $V_\sigma = \text{vars}_\sigma(wit(\Gamma_2))$ for every $\sigma \in S^{nsi}$ and $V_\sigma = \text{vars}_\sigma(\Gamma_1) \cap \text{vars}_\sigma(wit(\Gamma_2))$ for every $\sigma \in S^{si}$.

All three items of Theorem 4 include assumptions that guarantee that the two theories agree on cardinalities of shared sorts. For example, in the first item, we first shrink the S^{nsi} -domains of the \mathcal{T}_2 -model using strong finite witnessability, and then expand them using smoothness. But then, to obtain infinite domains for the S^{si} sorts, stable infiniteness is not enough, as we need to maintain the cardinalities of the S^{nsi} domains while making the domains of the S^{si} sorts infinite. For this, the stronger property of strong stable infiniteness is used.

The formal proof of this theorem is provided in Section 4.2, below. Figure 2 is a visualization of the claims in Theorem 4. The theorem considers two variants of strong finite witnessability, two variants of smoothness, and three variants of stable infiniteness. For each of the three cases of Theorem 4, Figure 2 shows which variant of each property is assumed. The height of each bar corresponds to the strength of the property. In the first case, we use ordinary strong finite witnessability and smoothness, but the strongest variant of stable infiniteness; in the second, we use ordinary strong finite witnessability with the new variants of stable infiniteness and smoothness; and for the third, we use ordinary stable infiniteness and the stronger variants of strong finite witnessability and smoothness. The order of the bars corresponds to the order of their usage in the proof of each case. The stage at which stable infiniteness is used determines the required



strength of the other properties: whatever is used before is taken in ordinary form, and whatever is used after requires a stronger form.

Going back to the standard definitions of stable infiniteness, smoothness, and strong finite witnessability, we get the following corollary by using case 1 of the theorem and noticing that smoothness w.r.t. S implies strong stable infiniteness w.r.t. any partition of S .

Corollary 1. *Let $S^{si} \subseteq S$ and $S^{nsi} = S \setminus S^{si}$. Suppose \mathcal{T}_1 is stably infinite w.r.t. S^{si} and \mathcal{T}_2 is strongly finitely witnessable w.r.t. S^{nsi} with witness wit and smooth w.r.t. S . Then, the following are equivalent:*

1. $\Gamma_1 \cup \Gamma_2$ is $(\mathcal{T}_1 \oplus \mathcal{T}_2)$ -satisfiable; 2. there exists an arrangement δ_V over V such that $\Gamma_1 \cup \delta_V$ is \mathcal{T}_1 -satisfiable and $wit(\Gamma_2) \cup \delta_V$ is \mathcal{T}_2 -satisfiable, where $V = \bigcup_{\sigma \in S} V_\sigma$, with $V_\sigma = vars_\sigma(wit(\Gamma_2))$ for $\sigma \in S^{nsi}$ and $V_\sigma = vars_\sigma(\Gamma_1) \cap vars_\sigma(wit(\Gamma_2))$ for $\sigma \in S^{si}$.

Finally, the following result, which is closest to Theorem 3, is directly obtained from Corollary 1, since the strong politeness of \mathcal{T}_2 w.r.t. $S^{si} \cup S^{nsi}$ implies that it is strongly finitely witnessable w.r.t. S^{nsi} and smooth w.r.t. $S^{si} \cup S^{nsi}$.

Corollary 2. *Let $S^{si} \subseteq S$ and $S^{nsi} = S \setminus S^{si}$. If \mathcal{T}_1 is stably infinite w.r.t. S^{si} and \mathcal{T}_2 is strongly polite w.r.t. S with a witness wit , then the following are equivalent: 1. $\Gamma_1 \cup \Gamma_2$ is $(\mathcal{T}_1 \oplus \mathcal{T}_2)$ -satisfiable; 2. there exists an arrangement δ_V over V such that $\Gamma_1 \cup \delta_V$ is \mathcal{T}_1 -satisfiable and $wit(\Gamma_2) \cup \delta_V$ is \mathcal{T}_2 -satisfiable, where $V = \bigcup_{\sigma \in S} V_\sigma$, with $V_\sigma = vars_\sigma(wit(\Gamma_2))$ for each $\sigma \in S^{nsi}$ and $V_\sigma = vars_\sigma(\Gamma_1) \cap vars_\sigma(wit(\Gamma_2))$ for each $\sigma \in S^{si}$.*

Compared to Theorem 3, Corollary 2 partitions S into S^{si} and S^{nsi} and requires that \mathcal{T}_1 be stably infinite w.r.t. S^{si} . The gain from this requirement is that the set V_σ is potentially reduced for $\sigma \in S^{si}$. Note that unlike Theorem 4 and Corollary 1, Corollary 2 has the same assumptions regarding \mathcal{T}_2 as the original Theorem 3 from [12]. We show its potential impact in the next example.

Example 7. Consider the theory $\mathcal{T}_{ListIntBV4}$ from Example 3. Let Γ_1 be $x = 5 \wedge v = 0000 \wedge w = w \ \& \ v$, and let Γ_2 be $a_0 = cons(x, v, a_1) \wedge \bigwedge_{i=1}^n a_i =$

$cons(y_i, w, a_{i+1})$. Using the witness function wit from [18], $wit(\Gamma_2) = \Gamma_2$. The polite combination approach reduces the $\mathcal{T}_{ListIntBV4}$ -satisfiability of $\Gamma_1 \wedge \Gamma_2$ to the existence of an arrangement δ over $\{x, v, w\} \cup \{y_1, \dots, y_n\}$, such that $\Gamma_1 \wedge \delta$ is \mathcal{T}_{IntBV4} -satisfiable and $wit(\Gamma_2) \wedge \delta$ is \mathcal{T}_{List} -satisfiable. Corollary 2 shows that we can do better. Since \mathcal{T}_{IntBV4} is stably infinite w.r.t. $\{int\}$, it is enough to check the existence of an arrangement over the variables of sort $BV4$ that occur in $wit(\Gamma_2)$, together with the variables of sort int that are shared between Γ_1 and Γ_2 . This means that arrangements over $\{x, v, w\}$ are considered, instead of over $\{x, v, w\} \cup \{y_1, \dots, y_n\}$. As n becomes large, standard polite combination requires considering exponentially more arrangements, while the number of arrangements considered by our combination method remains the same. \square

4.2 Proof of Theorem 4

The left-to-right direction is straightforward, using the reducts of the satisfying interpretation of $\Gamma_1 \cup \Gamma_2$ to Σ_1 and Σ_2 . We now focus on the right-to-left direction, and begin with the following lemma, which strengthens Theorem 1, obtaining a many-sorted Löwenheim-Skolem Theorem, where the cardinality of the finite sorts remains the same.

Lemma 8. *Let Σ be a signature, \mathcal{T} a Σ -theory, φ a Σ -formula, and \mathcal{A} a \mathcal{T} -interpretation that satisfies φ . Let $\mathcal{S}_\Sigma = S_{\mathcal{A}}^{fin} \uplus S_{\mathcal{A}}^{inf}$, where $\sigma^{\mathcal{A}}$ is finite for every $\sigma \in S_{\mathcal{A}}^{fin}$ and $\sigma^{\mathcal{A}}$ is infinite for every $\sigma \in S_{\mathcal{A}}^{inf}$. Then there exists a \mathcal{T} -interpretation \mathcal{B} that satisfies φ such that $|\sigma^{\mathcal{B}}| = |\sigma^{\mathcal{A}}|$ for every $\sigma \in S_{\mathcal{A}}^{fin}$ and $\sigma^{\mathcal{B}}$ is countable for every $\sigma \in S_{\mathcal{A}}^{inf}$.*

The proof of Theorem 4 continues with the following main lemma.

Lemma 9 (Main Lemma). *Let $S^{si} \subseteq S$ and $S^{nsi} = S \setminus S^{si}$, Suppose \mathcal{T}_1 is stably infinite w.r.t. S^{si} and that one of the three cases of Theorem 4 holds. Further, assume there exists an arrangement δ_V over V such that $\Gamma_1 \cup \delta_V$ is \mathcal{T}_1 -satisfiable, and $wit(\Gamma_2) \cup \delta_V$ is \mathcal{T}_2 -satisfiable, where $V = \bigcup_{\sigma \in S} V_\sigma$, with $V_\sigma = vars_\sigma(wit(\Gamma_2))$ for each $\sigma \in S^{nsi}$ and $V_\sigma = vars_\sigma(\Gamma_1) \cap vars_\sigma(wit(\Gamma_2))$ for each $\sigma \in S^{si}$. Then, there is a \mathcal{T}_1 -interpretation \mathcal{A} that satisfies $\Gamma_1 \cup \delta_V$ and a \mathcal{T}_2 -interpretation \mathcal{B} that satisfies $wit(\Gamma_2) \cup \delta_V$ such that $|\sigma^{\mathcal{A}}| = |\sigma^{\mathcal{B}}|$ for all $\sigma \in S$.*

Proof: Let $\psi_2 := wit(\Gamma_2)$. Since \mathcal{T}_1 is stably infinite w.r.t. S^{si} , there is a \mathcal{T}_1 -interpretation \mathcal{A} satisfying $\Gamma_1 \cup \delta_V$ in which $\sigma^{\mathcal{A}}$ is infinite for each $\sigma \in S^{si}$. By Theorem 1, we may assume that $\sigma^{\mathcal{A}}$ is countable for each $\sigma \in S^{si}$. We consider the first case of Theorem 4 (the others are omitted due to space constraints). Suppose \mathcal{T}_2 is strongly stably infinite w.r.t. (S^{si}, S^{nsi}) and strongly polite w.r.t. S^{nsi} . Since \mathcal{T}_2 is strongly finitely-witnessable w.r.t. S^{nsi} , there exists a \mathcal{T}_2 -interpretation \mathcal{B} that satisfies $\psi_2 \cup \delta_V$ such that $\sigma^{\mathcal{B}} = V_\sigma^{\mathcal{B}}$ for each $\sigma \in S^{nsi}$. Since \mathcal{A} and \mathcal{B} satisfy δ_V , we have that for every $\sigma \in S^{nsi}$, $|\sigma^{\mathcal{B}}| = |V_\sigma^{\mathcal{B}}| = |V_\sigma^{\mathcal{A}}| \leq |\sigma^{\mathcal{A}}|$. \mathcal{T}_2 is also smooth w.r.t. S^{nsi} , and so there exists a \mathcal{T}_2 -interpretation \mathcal{B}' satisfying $\psi_2 \cup \delta_V$ such that $|\sigma^{\mathcal{B}'}| = |\sigma^{\mathcal{A}}|$ for each

$\sigma \in S^{nsi}$. Finally, \mathcal{T}_2 is strongly stably infinite w.r.t. (S^{si}, S^{nsi}) , so there is a \mathcal{T}_2 -interpretation \mathcal{B}'' that satisfies $\psi_2 \cup \delta_V$ such that $\sigma^{\mathcal{B}''}$ is infinite for each $\sigma \in S^{si}$ and $|\sigma^{\mathcal{B}''}| = |\sigma^{\mathcal{B}'}| = |\sigma^{\mathcal{A}}|$ for each $\sigma \in S^{nsi}$. By Lemma 8, we may assume that $\sigma^{\mathcal{B}''}$ is countable for each $\sigma \in S^{si}$. Thus, $|\sigma^{\mathcal{B}''}| = |\sigma^{\mathcal{A}}|$ for each $\sigma \in S$. \square

We now conclude Theorem 4: Let $\mathcal{T} := \mathcal{T}_1 \oplus \mathcal{T}_2$. Lemma 9 gives us a \mathcal{T}_1 interpretation \mathcal{A} with $\mathcal{A} \models \Gamma_1 \cup \delta_V$ and a \mathcal{T}_2 interpretation \mathcal{B} with $\mathcal{B} \models \psi_2 \cup \delta_V$, and $|\sigma^{\mathcal{A}}| = |\sigma^{\mathcal{B}}|$ for $\sigma \in S$. Set $\Gamma'_1 := \Gamma_1 \cup \delta_V$ and $\Gamma'_2 := \psi_2 \cup \delta_V$. Then, $V_\sigma = vars_\sigma(\Gamma'_1) \cap vars_\sigma(\Gamma'_2)$ for $\sigma \in S$. Now, $\mathcal{A} \models \Gamma'_1 \cup \delta_V$ and $\mathcal{B} \models \Gamma'_2 \cup \delta_V$. Also, $|\sigma^{\mathcal{A}}| = |\sigma^{\mathcal{B}}|$ for $\sigma \in S$. By Theorem 2, $\Gamma'_1 \cup \Gamma'_2$ is \mathcal{T} -satisfiable. In particular, $\Gamma_1 \cup \{\psi_2\}$ is \mathcal{T} -satisfiable, and hence also $\Gamma_1 \cup \{\exists \bar{w}. \psi_2\}$, with $\bar{w} = vars(wit(\Gamma_2)) \setminus vars(\Gamma_2)$. Finally, $\exists \bar{w}. wit(\Gamma_2)$ is \mathcal{T}_2 -equivalent to Γ_2 , hence $\Gamma_1 \cup \Gamma_2$ is \mathcal{T} -satisfiable. \square

5 Preliminary Case Study

The results presented in Section 4 was motivated by a set of smart contract verification benchmarks. We obtained these benchmarks by applying the open-source Move Prover verifier [22] to smart contracts found in the open-source Diem project [9]. The Move prover is a formal verifier for smart contracts written in the Move language [6] and was designed to target smart contracts used in the Diem blockchain [1]. It works via a translation to the Boogie verification framework [14], which in turn produces SMT-LIB 2 benchmarks that are dispatched to SMT solvers. The benchmarks we obtained involve datatypes, integers, Booleans, and quantifiers. Our case study began by running CVC4 [3] on the benchmarks. For most of the benchmarks that were solved by CVC4, theory combination took a small percentage of the overall runtime of the solver, accounting for 10% or less in all but 1 benchmark. However, solving that benchmark took 81 seconds, of which 20 seconds was dedicated to theory combination.

We implemented an optimization to the datatype solver of CVC4 based on Corollary 2. With the original polite combination method, every term that originates from the theory of datatypes with another sort is shared with the other theories, triggering an analysis of the arrangements of these terms. In our optimization, we limit the sharing of such terms to those of Boolean sort. In the language of Corollary 2, \mathcal{T}_1 is the combined theory of Booleans, uninterpreted functions, and integers, which is stably infinite w.r.t. the uninterpreted sorts and integer sorts. \mathcal{T}_2 is an instance of the theory of datatypes, which is strongly polite w.r.t. its element sorts, which in this case are the sorts of \mathcal{T}_1 .

A comparison of an original and optimized run on the difficult benchmark is shown in Figure 3. As shown, the optimization reduces the total running time by 75%, and the time spent on theory combination in particular by 83%. To further isolate the effectiveness of our optimization, we report the number of terms that each theory solver considered. In CVC4, constraints are not flattened, so shared *terms* are processed instead of shared variables. Each theory solver

	total (s)	comb (s)	DT	INT	UFB	shared
optimized	34.9	3.4	236.1	212.1	78.4	125.8
original	81.5	20.3	116.0	281.0	123.9	163.5

Fig. 3. Runtimes (in seconds) and number of terms (in thousands) added to the data structures of DT, INT, UFB, and the number of shared terms (shared).

maintains its own data structure for tracking equality information. These data structures contain terms belonging to the theory that either come from the input assertions or are shared with another theory. A data structure is also maintained that contains all shared terms belonging to any theory. The last 4 columns of Figure 4 count the number of times (in thousands) a term was added to the equality data structure for the theory of datatypes (DT), integers (INT), and uninterpreted functions and Booleans (UFB), as well as to the the shared term data structure (shared). With the optimization, the datatype solver keeps more inferred assertions internally, which leads to an increase in the number of additions of terms to its data structure. However, sharing fewer terms, reduces the number of terms in the data structures for the other theories. Moreover, while the total number of terms considered remains roughly the same, the number of shared terms decreases by 24%. This suggests that although the workload on the individual theory solvers is roughly similar, a decrease in the number of shared terms in the optimized run results in a significant improvement in the overall runtime. Although our evidence is only anecdotal at the moment, we believe this benchmark is highly representative of the potential benefits of our optimization.

6 Conclusion

This paper makes two contributions. First, we separated politeness and strong politeness, which shows that sometimes, the (typically harder) task of finding a strong witness is not a waste of effort. Then, we provided an optimization to the polite combination method, which applies when one of the theories in the combination is stably infinite w.r.t. a subset of the sorts.

We envision several directions for future work. First, the separation of politeness from strong politeness demonstrates a need to identify sufficient criteria for the equivalence of these notions — such as, for instance, the *additivity* criterion introduced by Sheng et al. [18]. Second, polite combination might be optimized by applying the witness function only to part of the purified input formula. Finally, we plan to extend the initial implementation of this approach in CVC4 and evaluate its impact based on more benchmarks.

References

1. Amsden, Z., Arora, R., Bano, S., Baudet, M., Blackshear, S., Bothra, A., Cabrera, G., Catalini, C., Chalkias, K., Cheng, E., Ching, A., Chursin, A., Danezis, G., Giacomo, G.D., Dill, D.L., Ding, H., Doudchenko, N., Gao, V., Gao, Z., Garillot, F., Gorven, M., Hayes, P., Hou, J.M., Hu, Y., Hurley, K., Lewi, K., Li, C., Li, Z., Malkhi, D., Margulis, S., Maurer, B., Mohassel, P., de Naurois, L., Nikolaenko, V., Nowacki, T., Orlov, O., Perelman, D., Pott, A., Proctor, B., Qadeer, S., Rain, Russi, D., Schwab, B., Sezer, S., Sonnino, A., Venter, H., Wei, L., Wernerfelt, N., Williams, B., Wu, Q., Yan, X., Zakian, T., Zhou, R.: The Diem Blockchain. <https://developers.diem.com/docs/technical-papers/the-diem-blockchain-paper/> (2019)
2. Barrett, C., Fontaine, P., Tinelli, C.: The SMT-LIB Standard: Version 2.6. Tech. rep., Department of Computer Science, The University of Iowa (2017), available at www.SMT-LIB.org
3. Barrett, C.W., Conway, C.L., Deters, M., Hadarean, L., Jovanovic, D., King, T., Reynolds, A., Tinelli, C.: CVC4. In: Gopalakrishnan, G., Qadeer, S. (eds.) Computer Aided Verification - 23rd International Conference, CAV 2011, Snowbird, UT, USA, July 14-20, 2011. Proceedings. Lecture Notes in Computer Science, vol. 6806, pp. 171–177. Springer (2011), https://doi.org/10.1007/978-3-642-22110-1_14
4. Barrett, C.W., Shikanian, I., Tinelli, C.: An abstract decision procedure for a theory of inductive data types. *Journal on Satisfiability, Boolean Modeling and Computation* **3**(1-2), 21–46 (2007)
5. Barrett, C.W., Tinelli, C.: Satisfiability modulo theories. In: Clarke, E.M., Henzinger, T.A., Veith, H., Bloem, R. (eds.) Handbook of Model Checking, pp. 305–343. Springer (2018), https://doi.org/10.1007/978-3-319-10575-8_11
6. Blackshear, S., Cheng, E., Dill, D.L., Gao, V., Maurer, B., Nowacki, T., Pott, A., Qadeer, S., Rain, Russi, D., Sezer, S., Zakian, T., Zhou, R.: Move: A language with programmable resources. <https://developers.diem.com/docs/technical-papers/move-paper/> (2019)
7. Casal, F., Rasga, J.: Revisiting the equivalence of shininess and politeness. In: McMillan, K.L., Middeldorp, A., Voronkov, A. (eds.) Logic for Programming, Artificial Intelligence, and Reasoning - 19th International Conference, LPAR-19, Stellenbosch, South Africa, December 14-19, 2013. Proceedings. Lecture Notes in Computer Science, vol. 8312, pp. 198–212. Springer (2013), https://doi.org/10.1007/978-3-642-45221-5_15
8. Casal, F., Rasga, J.: Many-sorted equivalence of shiny and strongly polite theories. *J. Autom. Reason.* **60**(2), 221–236 (2018), <https://doi.org/10.1007/s10817-017-9411-y>
9. diem: <https://github.com/diem/diem>
10. Enderton, H.B.: A mathematical introduction to logic. Academic Press (2001)
11. Fontaine, P.: Combinations of theories for decidable fragments of first-order logic. In: Ghilardi, S., Sebastiani, R. (eds.) Frontiers of Combining Systems, 7th International Symposium, FroCoS 2009, Trento, Italy, September 16-18, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5749, pp. 263–278. Springer (2009), https://doi.org/10.1007/978-3-642-04222-5_16
12. Jovanovic, D., Barrett, C.W.: Polite theories revisited. In: Fermüller, C.G., Voronkov, A. (eds.) Logic for Programming, Artificial Intelligence, and Reasoning - 17th International Conference, LPAR-17, Yogyakarta, Indonesia, October 10-15, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6397, pp. 402–416. Springer (2010), https://doi.org/10.1007/978-3-642-16242-8_29

13. Krstic, S., Goel, A., Grundy, J., Tinelli, C.: Combined satisfiability modulo parametric theories. In: Grumberg, O., Huth, M. (eds.) *Tools and Algorithms for the Construction and Analysis of Systems*, 13th International Conference, TACAS 2007, Held as Part of the Joint European Conferences on Theory and Practice of Software, ETAPS 2007 Braga, Portugal, March 24 - April 1, 2007, Proceedings. *Lecture Notes in Computer Science*, vol. 4424, pp. 602–617. Springer (2007), https://doi.org/10.1007/978-3-540-71209-1_47
14. Leino, K.R.M.: This is Boogie 2. manuscript KRML **178**(131), 9 (2008), <https://www.microsoft.com/en-us/research/publication/this-is-boogie-2-2/>
15. Nelson, G.: *Techniques for program verification*. Tech. Rep. CSL-81-10, Xerox, Palo Alto Research Center (1981)
16. Nelson, G., Oppen, D.C.: Simplification by cooperating decision procedures. *ACM Trans. Program. Lang. Syst.* **1**(2), 245–257 (1979), <https://doi.org/10.1145/357073.357079>
17. Ranise, S., Ringeissen, C., Zarba, C.G.: Combining data structures with nonstably infinite theories using many-sorted logic. In: Gramlich, B. (ed.) *Frontiers of Combining Systems*, 5th International Workshop, FroCoS 2005, Vienna, Austria, September 19-21, 2005, Proceedings. *Lecture Notes in Computer Science*, vol. 3717, pp. 48–64. Springer (2005), extended technical report is available at <https://hal.inria.fr/inria-00070335/>
18. Sheng, Y., Zohar, Y., Ringeissen, C., Lange, J., Fontaine, P., Barrett, C.W.: Politeness for the theory of algebraic datatypes. In: Peltier, N., Sofronie-Stokkermans, V. (eds.) *Automated Reasoning - 10th International Joint Conference, IJCAR 2020*, Paris, France, July 1-4, 2020, Proceedings, Part I. *Lecture Notes in Computer Science*, vol. 12166, pp. 238–255. Springer (2020), https://doi.org/10.1007/978-3-030-51074-9_14
19. Tinelli, C., Zarba, C.G.: Combining decision procedures for sorted theories. In: Alferes, J.J., Leite, J.A. (eds.) *Logics in Artificial Intelligence*, 9th European Conference, JELIA 2004, Lisbon, Portugal, September 27-30, 2004, Proceedings. *Lecture Notes in Computer Science*, vol. 3229, pp. 641–653. Springer (2004)
20. Tinelli, C., Zarba, C.G.: Combining decision procedures for sorted theories. In: Alferes, J.J., Leite, J.A. (eds.) *Logics in Artificial Intelligence*, 9th European Conference, JELIA 2004, Lisbon, Portugal, September 27-30, 2004, Proceedings. *Lecture Notes in Computer Science*, vol. 3229, pp. 641–653. Springer (2004), https://doi.org/10.1007/978-3-540-30227-8_53
21. Tinelli, C., Zarba, C.G.: Combining nonstably infinite theories. *J. Autom. Reason.* **34**(3), 209–238 (2005), <https://doi.org/10.1007/s10817-005-5204-9>
22. Zhong, J.E., Cheang, K., Qadeer, S., Grieskamp, W., Blackshear, S., Park, J., Zohar, Y., Barrett, C.W., Dill, D.L.: The Move prover. In: Lahiri, S.K., Wang, C. (eds.) *Computer Aided Verification - 32nd International Conference, CAV 2020*, Los Angeles, CA, USA, July 21-24, 2020, Proceedings, Part I. *Lecture Notes in Computer Science*, vol. 12224, pp. 137–150. Springer (2020), https://doi.org/10.1007/978-3-030-53288-8_7