Revisiting the Equivalence of Shininess and Politeness

Filipe Casal[1] and João Rasga[2]

[1] SQIG, Instituto de Telecomunicações, Lisboa, Portugal
filipe.casal@ist.utl.pt
[2] Dep. Matemática, Instituto Superior Técnico, Universidade de Lisboa, Portugal,
and
SQIG, Instituto de Telecomunicações, Lisboa, Portugal
jfr@math.ist.utl.pt

Abstract. The Nelson-Oppen method [4] allows the combination of satisfiability procedures of stably infinite theories with disjoint signatures. Due to its importance, several attempts to extend the method to different and wider classes of theories were made. In 2005, it was shown that shiny [9] and polite [6] theories could be combined with an arbitrary theory (the relationship between these classes was analysed in [6]). Later, a stronger notion of polite theory was proposed, see [3], in order to overcome a subtle issue with a proof in [6]. In this paper, we analyse the relationship between shiny and strongly polite theories in the one-sorted case. We show that a shiny theory with a decidable quantifier-free satisfiability problem is strongly polite and provide two different sufficient conditions for a strongly polite theory to be shiny. Based on these results, we derive a combination method for the union of a polite theory with an arbitrary theory.

Keywords: combination of satisfiability procedures, Nelson-Oppen method, polite theories, strongly polite theories, shiny theories

1 Introduction

The problem of modularly combining satisfiability procedures of two theories into a satisfiability procedure for their union is of great interest in the area of automated reasoning: for instance, verification systems such as CVC4 [1] and SMTInterpol [2] rely on such a combination procedure.

The first and most well-known method for the combination of satisfiability procedures is due to Nelson and Oppen, [4]. In this seminal paper, the authors provide a combination method to decide the satisfiability of quantifier-free formulas in the union of two theories, provided that both theories have their own procedure for deciding the satisfiability problem of quantifier-free formulas. After a correction, see [5], the two main restrictions of the Nelson-Oppen method are:

– the theories are *stably infinite*,

– their signatures are disjoint.

It is also worth mentioning another correctness proof of the Nelson-Oppen method given by Tinelli and Harandi in [7].

Concerned about the fact that many theories of interest, such as those admitting only finite models, are not stably infinite, Tinelli and Zarba, in [9], showed that the Nelson-Oppen combination procedure still applies when the stable infiniteness condition is replaced by the requirement that all but one of the theories is *shiny*. However, a shiny theory must be equipped with a particular function called mincard, which is inherently hard to compute.

In order to overcome the problem of computing the mincard function and of the shortage of shiny theories, Ranise, Ringeissen and Zarba proposed an alternative requirement, *politeness*, in [6], and analysed its relationship with shininess. A polite theory has to be equipped with a witness function, which was thought to be easier to compute than the mincard function. They show that given a polite theory and an arbitrary one, the Nelson-Oppen combination procedure is still valid when the signatures are disjoint and both theories have their own procedure for deciding the satisfiability problem of quantifier-free formulas. Some time later, in [3], Jovanović and Barrett reported that the politeness notion provided in [6] allowed, after all, witness functions that are not sufficiently strong to prove the combination theorem. In order to solve the problem they provided a seemingly stronger notion of politeness, in the sequel called *strongly politeness*, equipped with a seemingly stronger witness function, s-witness, that allowed to prove the combination theorem. However, the authors left open the relationship between the two notions of politeness and between the strong politeness notion and shininess.

In this paper we investigate the relationship between shiny and strongly polite theories in the one-sorted case. We show that a shiny theory with a decidable quantifier-free satisfiability problem is strongly polite. For the other direction, we provide two different sets of conditions under which a strongly polite theory is shiny (see Figure 1 for a more detailed global view of the results). Moreover, we show that, under some conditions, a polite theory is also strongly polite and so there is a way to transform a witness function into a strong witness function. Given the constructive nature of the proofs we were able to design such a procedure.

1.1 Organization of the Paper

The paper is organized as follows: in Section 2 we recall some relevant definitions. In Section 3 we begin by recalling the definitions of shininess and of (strong) politeness and then we proceed to show the equivalence between these notions. In Section 4 we analyse what was done in the paper and provide directions for further research.

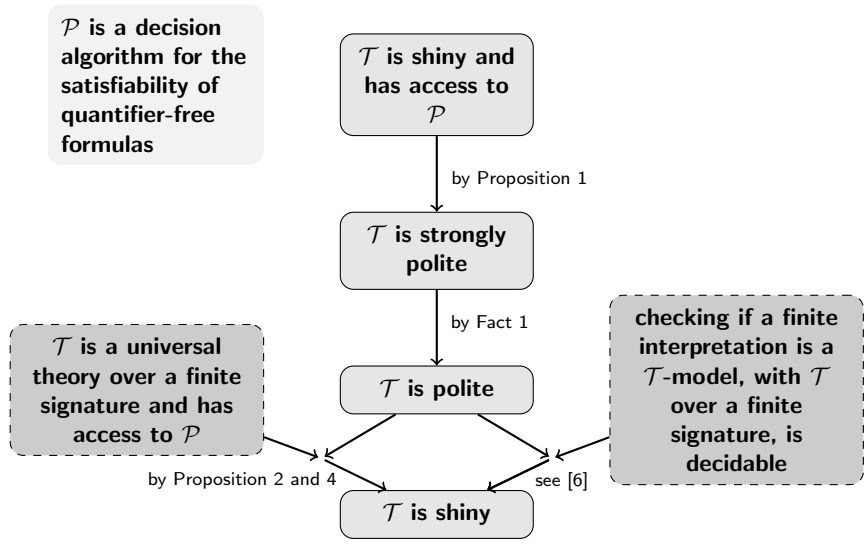

Fig. 1: Schematic representation of the results in the paper

2 Preliminaries

The results in this paper concern first-order logic with equality. We assume given a countably infinite set of variables. We mainly follow the notation in [9].

2.1 Syntax

A *signature* is a tuple $\Sigma = \langle \Sigma^F, \Sigma^P \rangle$ where Σ^F is the set of function symbols and Σ^P is the set of predicate symbols. We use $\cong$ to denote the equality logic symbol and assume the standard definitions of Σ-*atom* and Σ-*term*. A Σ-formula is inductively defined as usual over Σ-atoms and Σ-terms using the connectives $\wedge, \vee, \neg, \rightarrow$ or the quantifiers $\forall$ and $\exists$. We denote by $\mathsf{QF}(\Sigma)$ the set of Σ-formulas with no occurrences of quantifiers and, given a Σ-formula φ, by $\mathsf{vars}(\varphi)$ the set of free variables of φ. We say that a Σ-formula is a Σ-*sentence* if it has no free variables. In the sequel, when there is no ambiguity, we will omit the reference to the signature when referring to atoms, terms, formulas and sentences.

Definition 1 (Arrangement formula). *Given a finite set of variables Y and an equivalence relation $E \subseteq Y^2$, the* arrangement formula *induced by E over Y, denoted by δ_E^Y, is*

$$\bigwedge_{(x,y)\in E} (x \cong y) \wedge \bigwedge_{(x,y)\in Y^2\setminus E} \neg(x \cong y)$$

In the sequel, we may simply denote δ_E^Y by δ_E if there is no confusion to which variable set the formula refers to.

2.2 Semantics

Given a signature Σ, a *Σ-interpretation* $\mathcal{A}$ with domain A over a set of variables X is a map that interprets each variable $x \in X$ as an element $x^{\mathcal{A}} \in A$, each function symbol $f \in \Sigma^F$ of arity n as a map $f^{\mathcal{A}} : A^n \to A$ and each predicate symbol $p \in \Sigma^P$ of arity n as a a subset $P^{\mathcal{A}}$ of A^n. We denote by $\mathsf{dom}(\mathcal{A})$ the domain of an interpretation $\mathcal{A}$. In the sequel, when there is no ambiguity, we will omit the reference to the signature when referring to interpretations.

Given an interpretation $\mathcal{A}$ and a term t, we denote by $t^{\mathcal{A}}$ the interpretation of t under $\mathcal{A}$. Similarly, we denote by $\varphi^{\mathcal{A}}$ the truth value of the formula φ under the interpretation $\mathcal{A}$. Furthermore, given a set Γ of formulas, we denote by $[\![\Gamma]\!]^{\mathcal{A}}$ the set $\{\varphi^{\mathcal{A}} : \varphi \in \Gamma\}$, and similarly for a set of terms. We write $\mathcal{A} \Vdash \varphi$ when the formula φ is true under the interpretation $\mathcal{A}$, i.e., $\mathcal{A}$ satisfies φ.

A formula φ is *satisfiable* if it is true under some interpretation, and *unsatisfiable* otherwise.

Given a set of variables Y we say that two interpretations $\mathcal{A}$ and $\mathcal{B}$ over a set X of variables are *Y-equivalent* whenever $\mathsf{dom}(\mathcal{A}) = \mathsf{dom}(\mathcal{B})$, $f^{\mathcal{A}} = f^{\mathcal{B}}$ for each function symbol f, $p^{\mathcal{A}} = p^{\mathcal{B}}$ for each predicate symbol p, and $x^{\mathcal{A}} = x^{\mathcal{B}}$ for each variable x in $X \setminus Y$.

We also say that an *interpretation is finite (infinite)* when its domain is finite (infinite).

2.3 Theories

Given a signature Σ, a *Σ-theory* is a set of Σ-sentences and given a Σ-theory $\mathcal{T}$, a *$\mathcal{T}$-model* is a Σ-interpretation that satisfies all sentences of $\mathcal{T}$. We say that a formula φ is *$\mathcal{T}$-satisfiable* when there is a $\mathcal{T}$-model that satisfies it and say that two formulas are *$\mathcal{T}$-equivalent* if they are interpreted to the same truth value in every $\mathcal{T}$-model. In the sequel, when there is no ambiguity, we will omit the reference to the signature when referring to theories.

Given a Σ_1-theory $\mathcal{T}_1$ and a Σ_2-theory $\mathcal{T}_2$, their union, $\mathcal{T}_1 \oplus \mathcal{T}_2$, is a $\Sigma_1 \cup \Sigma_2$-theory defined by the union of the sentences of $\mathcal{T}_1$ with the sentences of $\mathcal{T}_2$.

The following definitions introduce some of the conditions used in the results presented in this paper.

Definition 2 (Smoothness). *We say that a theory $\mathcal{T}$ is* smooth *if for every $\mathcal{T}$-satisfiable quantifier-free formula φ, $\mathcal{T}$-model $\mathcal{A}$ satisfying φ and cardinal $\kappa \geq |\mathcal{A}|$ there exists a $\mathcal{T}$-model $\mathcal{B}$ satisfying φ such that $|\mathcal{B}| = \kappa$.*

Definition 3 (Stable finiteness). *We say that a theory $\mathcal{T}$ is* stably finite *if for every $\mathcal{T}$-satisfiable quantifier-free formula φ there exists a finite $\mathcal{T}$-model of φ.*

Definition 4 (Stable infiniteness). *We say that a theory $\mathcal{T}$ is* stably infinite *if for every $\mathcal{T}$-satisfiable quantifier-free formula φ there exists an infinite $\mathcal{T}$-model of φ.*

Definition 5 (Finite witnessability, [6]). *We say that a theory $\mathcal{T}$ over a signature Σ is* finitely witnessable *if there exists a computable function* $\mathsf{witness} : \mathsf{QF}(\Sigma) \to \mathsf{QF}(\Sigma)$ *such that for every quantifier-free formula φ the following conditions hold:*

- *φ and $\exists \vec{w}\ \mathsf{witness}(\varphi)$ are $\mathcal{T}$-equivalent, where $\vec{w}$ are the variables in $\mathsf{witness}(\varphi)$ which do not occur in φ;*
- *if $\mathsf{witness}(\varphi)$ is satisfiable in $\mathcal{T}$ then there exists a $\mathcal{T}$-model $\mathcal{A}$ such that $\mathcal{A} \Vdash \mathsf{witness}(\varphi)$ and $\mathsf{dom}(\mathcal{A}) = [\![\mathsf{vars}(\mathsf{witness}(\varphi))]\!]^{\mathcal{A}}$.*

A function satisfying the above properties is called a *witness function for $\mathcal{T}$*. In [3], a stronger finite witnessability notion was defined in order to clarify an issue found on [6].

Definition 6 (Strong finite witnessability, [3]). *We say that a theory $\mathcal{T}$ over a signature Σ is* strongly finitely witnessable *if there exists a computable function* $\mathsf{s\text{-}witness} : \mathsf{QF}(\Sigma) \to \mathsf{QF}(\Sigma)$ *such that for every quantifier-free formula φ the following conditions hold:*

- *φ and $\exists \vec{w}\ \mathsf{s\text{-}witness}(\varphi)$ are $\mathcal{T}$-equivalent, where $\vec{w}$ are the variables in $\mathsf{s\text{-}witness}(\varphi)$ which do not occur in φ;*
- *for every finite set of variables Y and relation $E \subseteq Y^2$, if $\mathsf{s\text{-}witness}(\varphi) \wedge \delta_E^Y$ is satisfiable in $\mathcal{T}$ then there exists a $\mathcal{T}$-model $\mathcal{A}$ such that $\mathcal{A} \Vdash \mathsf{s\text{-}witness}(\varphi) \wedge \delta_E^Y$ and $\mathsf{dom}(\mathcal{A}) = [\![\mathsf{vars}(\mathsf{s\text{-}witness}(\varphi) \wedge \delta_E^Y)]\!]^{\mathcal{A}}$.*

A function satisfying the above properties is called a *strong witness function for $\mathcal{T}$*. The following notion was introduced by Tinelli and Zarba in [9] and its computability is one of the conditions a theory should satisfy to be shiny.

Definition 7 ($\mathsf{mincard}$ function). *Given a theory $\mathcal{T}$ over a signature Σ, let $\mathsf{mincard}_{\mathcal{T}}$ be the function from $\mathsf{QF}(\Sigma)$ to $\mathbb{N}^+$ such that*

$$\mathsf{mincard}_{\mathcal{T}}(\varphi) = \min\{k : \mathcal{A} \text{ is a } \mathcal{T}\text{-model, } \mathcal{A} \Vdash \varphi \text{ and } |\mathsf{dom}(\mathcal{A})| = k\}$$

if φ is $\mathcal{T}$-satisfiable, otherwise $\mathsf{mincard}_{\mathcal{T}}(\varphi)$ is undefined.

So, when φ is $\mathcal{T}$-satisfiable the function $\mathsf{mincard}_{\mathcal{T}}$ returns the cardinality of the smallest $\mathcal{T}$-model of φ. When there is no ambiguity to which theory the function refers to we will simply write $\mathsf{mincard}$.

3 Shiny and (Strongly) Polite Theories

3.1 Relating Shiny and Strongly Polite Theories

Here we analyse the relationship between shiny and strongly polite theories. We start by showing that a shiny theory is strongly polite when assuming that it has a decidable quantifier-free satisfiability problem, but first we recall what is a shiny theory, see [9], and a strongly polite one, see [3].

Definition 8 (Shininess, [9]). *A theory is* shiny *whenever it is smooth, stably finite and its* mincard *function is computable.*

Several theories were proved to be shiny, such as the theory of equality, the theory of partial orders and the theory of total orders, in [9].

Definition 9 (Strong politeness, [3]). *A theory is* strongly polite *whenever it is smooth and strongly finitely witnessable.*

Proposition 1. *A shiny theory with a decidable quantifier-free satisfiability problem is strongly polite.*

Proof. Let $\mathcal{T}$ be a shiny theory over a signature Σ and $\mathcal{P}$ an algorithm for its quantifier-free satisfiability problem. Since a shiny theory is by definition smooth, we are left to prove that $\mathcal{T}$ is strongly finitely witnessable in order to conclude that $\mathcal{T}$ is strongly polite. In the sequel, given a $\mathcal{T}$-satisfiable quantifier-free formula φ and $E \subseteq \mathsf{vars}(\varphi)^2$ such that $\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)}$ is $\mathcal{T}$-satisfiable, we denote by k_E^φ the result of $\mathsf{mincard}_\mathcal{T}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)})$.

Let

$$\mathsf{s\text{-}witness} : \mathsf{QF}(\Sigma) \to \mathsf{QF}(\Sigma)$$

be the map such that $\mathsf{s\text{-}witness}(\varphi) = \varphi \wedge \Omega$, where Ω is

$$\bigwedge_{\substack{E \subseteq \mathsf{vars}(\varphi)^2 \\ \mathcal{P}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)})=1}} \left(\delta_E^{\mathsf{vars}(\varphi)} \to \gamma_{k_E^\varphi}\right)$$

and $\gamma_{k_E^\varphi}$ is

$$\bigwedge_{\substack{i,j=1 \\ i \neq j}}^{k_E^\varphi} w_i \cong w_j$$

and $w_1, \ldots, w_k$ are distinct variables not occurring in φ and in $\gamma_{k_{E'}^\varphi}$ for all $E' \neq E$ contained in $\mathsf{vars}(\varphi)^2$ with $\mathcal{P}(\varphi \wedge \delta_{E'}^{\mathsf{vars}(\varphi)}) = 1$. It is immediate to conclude that $\mathsf{s\text{-}witness}$ is computable since:

- there is a finite number of sets E contained in $\mathsf{vars}(\varphi)^2$ since $\mathsf{vars}(\varphi)$ is finite;
- formula $\delta_E^{\mathsf{vars}(\varphi)}$ can be computed in a finite number of steps since E and $\mathsf{vars}(\varphi)$ are finite;
- the value k_E^φ is computable since: (i) the $\mathsf{mincard}$ function is computable; (ii) we can decide the satisfiability of $\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)}$ with $\mathcal{P}$; and (iii) $\mathcal{T}$ is stably finite;
- the formula $\gamma_{k_E^\varphi}$ is computable in a finite number of steps because k_E^φ is a natural number.

Let φ be a quantifier free formula. We now show that φ and $\exists \vec{w}\ \mathsf{s\text{-}witness}(\varphi)$ are $\mathcal{T}$-equivalent. Let $\mathcal{A}$ be a $\mathcal{T}$-model. Assume that $\mathcal{A} \Vdash \exists \vec{w}\ \mathsf{s\text{-}witness}(\varphi)$. Then $\mathcal{A} \Vdash \varphi \wedge \exists \vec{w}\ \Omega$, and so $\mathcal{A} \Vdash \varphi$. For the other direction, assume $\mathcal{A} \Vdash \varphi$. We need to show that

$$\mathcal{A} \Vdash \exists \vec{w} \bigwedge_{\substack{E \subseteq \mathsf{vars}(\varphi)^2 \\ \mathcal{P}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)})=1}} \left(\delta_E^{\mathsf{vars}(\varphi)} \rightarrow \gamma_{k_E^\varphi}\right).$$

Let $\mathcal{A}'$ be an interpretation $\vec{w}$-equivalent to $\mathcal{A}$ (and so with the same domain and the same interpretation of functions, predicates and of all variables except possibly $\vec{w}$) such that:

- if their domain is infinite then $w_1^{\mathcal{A}'} \neq w_2^{\mathcal{A}'}$ for every $w_1, w_2 \in \vec{w}$;
- if their domain is finite then for each $E \subseteq \mathsf{vars}(\varphi)^2$ with $\mathcal{P}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)}) = 1$:
  - if $k_E^\varphi \leq |\mathsf{dom}(\mathcal{A}')|$ then $w_1^{\mathcal{A}'} \neq w_2^{\mathcal{A}'}$ for every $w_1, w_2 \in \vec{w}$;
  - otherwise, set $w_1^{\mathcal{A}'} = w_2^{\mathcal{A}'}$ for every $w_1, w_2 \in \mathsf{vars}(\gamma_{k_E^\varphi})$.

Then

$$\mathcal{A}' \Vdash \bigwedge_{\substack{E \subseteq \mathsf{vars}(\varphi)^2 \\ \mathcal{P}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)})=1}} \left(\delta_E^{\mathsf{vars}(\varphi)} \rightarrow \gamma_{k_E^\varphi}\right),$$

since for each $E \subseteq \mathsf{vars}(\varphi)^2$ with $\mathcal{P}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)}) = 1$ either

- $\mathcal{A}' \nVdash \delta_E^{\mathsf{vars}(\varphi)}$ and so $\mathcal{A}' \Vdash \delta_E^{\mathsf{vars}(\varphi)} \rightarrow \gamma_{k_E^\varphi}$; or
- $\mathcal{A}' \Vdash \delta_E^{\mathsf{vars}(\varphi)}$ and so $\mathcal{A}' \Vdash \varphi \wedge \delta_E^{\mathsf{vars}(\varphi)}$ since $\mathcal{A} \Vdash \varphi$ and $\mathcal{A}$ and $\mathcal{A}'$ only differ in the interpretation of the variables in $\vec{w}$ not occurring in φ. Since $\mathcal{A}'$ is a model for $\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)}$, its cardinality has to be greater or equal than $k_E^\varphi = \mathsf{mincard}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)})$. Hence $\mathcal{A}' \Vdash \gamma_{k_E^\varphi}$ and so $\mathcal{A}' \Vdash \delta_E^{\mathsf{vars}(\varphi)} \rightarrow \gamma_{k_E^\varphi}$.

We now show that given an equivalence relation E' over a finite set of variables Y, if $\varphi \wedge \Omega \wedge \delta_{E'}^Y$ is $\mathcal{T}$-satisfiable, then there exists a $\mathcal{T}$-model $\mathcal{A}$ that satisfies $\varphi \wedge \Omega \wedge \delta_{E'}^Y$ such that $\mathsf{dom}(\mathcal{A}) = [\![\mathsf{vars}(\varphi \wedge \Omega \wedge \delta_{E'}^Y)]\!]^{\mathcal{A}}$. So, let E' be an equivalence relation over a finite set of variables Y such that $\varphi \wedge \Omega \wedge \delta_{E'}^Y$ is $\mathcal{T}$-satisfiable. Let p be a natural number and $Y_1, \ldots, Y_p$ finite pairwise disjoint non-empty sets of variables such that

- $Y = Y_1 \cup \ldots \cup Y_p$; and
- for each $i = 1, \ldots, p$, and $y \in Y_i$,
  - $(y \cong x)$ and $(x \cong y)$ are in $\delta_{E'}^Y$ for each $x \in Y_i$;
  - $\neg(y \cong x)$ and $\neg(x \cong y)$ are in $\delta_{E'}^Y$ for each $x \in Y \setminus Y_i$;

and observe that the variables in Y can be either in $\mathsf{vars}(\varphi)$ or in $\mathsf{vars}(\gamma_{k_E})$ for some E or not in $\mathsf{vars}(\varphi \wedge \Omega)$. Let $\mathcal{A}$ be a $\mathcal{T}$-model that satisfies

$$\varphi \wedge \Omega \wedge \delta_{E'}^Y$$

and let $\delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)}$ be the arrangement formula induced by $E_\mathcal{A} = \{(x, y) : x, y \in \mathsf{vars}(\varphi) \text{ and } x^\mathcal{A} = y^\mathcal{A}\}$. Then, obviously, $\delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)}$ is satisfied by $\mathcal{A}$. Moreover, no

other formula in $\{\delta_E^{\mathsf{vars}(\varphi)} : E \subseteq \mathsf{vars}(\varphi)^2 \text{ and } \mathcal{P}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)}) = 1\}$ is satisfied by $\mathcal{A}$. Since $\varphi \wedge \delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)}$ is satisfiable we have that the cardinality of its smallest model is $k_{E_\mathcal{A}}^\varphi = \mathsf{mincard}(\varphi \wedge \delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)})$. Let $K = \max\{k_{E_\mathcal{A}}^\varphi, p\}$. By the smoothness of $\mathcal{T}$ and since $\varphi \wedge \delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)}$ is $\mathcal{T}$-satisfiable, let $\mathcal{B}$ be a $\mathcal{T}$-model such that

$$\mathcal{B} \Vdash \varphi \wedge \delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)} \quad \text{and} \quad |\mathsf{dom}(\mathcal{B})| = K,$$

and let $d_1, \ldots, d_p$ be distinct elements of $\mathsf{dom}(\mathcal{B})$ such that

$$d_i = y^\mathcal{B} \text{ if } Y_i \cap \mathsf{vars}(\varphi) \neq \emptyset \text{ and } y \in Y_i \cap \mathsf{vars}(\varphi)$$

for $i = 1, \ldots, p$, and assuming that the variables of $\gamma_{k_{E_\mathcal{A}}^\varphi}$ are $w_1 \ldots, w_{k_{E_\mathcal{A}}^\varphi}$ let $e_1, \ldots, e_{k_{E_\mathcal{A}}^\varphi}$ be distinct elements of $\mathsf{dom}(\mathcal{B})$ such that

$$e_j = d_i \text{ if } w_j \in Y_i$$

for $j = 1, \ldots, k_{E_\mathcal{A}}^\varphi$. Observe that distinct variables in $w_1 \ldots, w_{k_{E_\mathcal{A}}^\varphi}$ are in distinct sets in $Y_1, \ldots, Y_p$ since $\mathcal{A} \Vdash \delta_{E'}^Y$ and $\mathcal{A} \Vdash \gamma_{k_{E_\mathcal{A}}^\varphi}$ taking into account that $\mathcal{A} \Vdash \delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)}$ and $\mathcal{A} \Vdash \Omega$. Let $\mathcal{B}'$ be the $\mathcal{T}$-model $(\vec{w} \cup (Y \setminus \mathsf{vars}(\varphi)))$-equivalent to $\mathcal{B}$ such that

$$x^{\mathcal{B}'} = \begin{cases} d_i & \text{if } x \in Y_i \text{ for some } i \in \{1, \ldots, p\} \\ e_j & \text{if } x \notin Y \text{ and } x \text{ is } w_j \text{ with } w_j \in \mathsf{vars}(\gamma_{k_{E_\mathcal{A}}}) \\ x^\mathcal{B} & \text{if } x \notin Y \text{ and } x \notin \mathsf{vars}(\gamma_{k_{E_\mathcal{A}}}) \end{cases}$$

for each $x \in \vec{w} \cup (Y \setminus \mathsf{vars}(\varphi))$. Let us now prove that $\mathcal{B}' \Vdash \varphi \wedge \Omega \wedge \delta_{E'}^Y$:
(a) $\mathcal{B}' \Vdash \varphi$. This follows immediately taking into account that $\mathcal{B} \Vdash \varphi$ and that $\mathcal{B}$ and $\mathcal{B}'$ may only differ in variables in $\vec{w} \cup (Y \setminus \mathsf{vars}(\varphi))$ not occurring in φ;
(b) $\mathcal{B}' \Vdash \Omega$. Observe that $\mathcal{B}' \Vdash \varphi \wedge \delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)}$ since $\mathcal{B}$ and $\mathcal{B}'$ may only differ in variables in $\vec{w} \cup (Y \setminus \mathsf{vars}(\varphi))$ not occurring in $\varphi \wedge \delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)}$. Moreover $\mathcal{B}' \Vdash \gamma_{k_{E_\mathcal{A}}}$ and so $\mathcal{B}' \Vdash \delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)} \to \gamma_{k_{E_\mathcal{A}}}$. Since $\mathcal{B}' \Vdash \delta_{E_\mathcal{A}}^{\mathsf{vars}(\varphi)}$, we have that $\mathcal{B}' \nVdash \delta_E^{\mathsf{vars}(\varphi)}$ for all $E \neq E_\mathcal{A}$ with $E \subseteq \mathsf{vars}(\varphi)^2$. Hence $\mathcal{B}' \Vdash \delta_E^{\mathsf{vars}(\varphi)} \to \gamma_{k_E}$ for all $E \subseteq \mathsf{vars}(\varphi)^2$ and so $\mathcal{B}' \Vdash \Omega$;
(c) $\mathcal{B}' \Vdash \delta_{E'}^Y$. We only need to verify that $\mathcal{B}'$ satisfies the equalities and disequalities induced by E'. This holds since by construction, it assigns the same value to variables in the same Y_i set, and assigns different values to variables in different sets.

Finally it remains to show that $\mathsf{dom}(\mathcal{B}') = [\![\mathsf{vars}(\varphi \wedge \Omega \wedge \delta_{E'}^Y)]\!]^{\mathcal{B}'}$:
($\subseteq$): Let $d \in \mathsf{dom}(\mathcal{B}')$. Then d is either a d_i for some $i = 1, \ldots, p$ or a e_j for some $j = 1, \ldots, k_{E_\mathcal{A}}$. In the case that $d = d_i$ then we have that $d = x^{\mathcal{B}'}$ for all $x \in Y_i$. On the other hand, if $d = e_j$ then $d = w_j^{\mathcal{B}'}$ for the w_j variable in $\mathsf{vars}(\gamma_{k_{E_\mathcal{A}}})$;
($\supseteq$): From the construction described above we obtain for every $x \in \mathsf{vars}(\varphi \wedge$

$\Omega \wedge \delta^{Y}_{E'}$) how to define $x^{\mathcal{B}'}$.

Combining the previous items, we obtain that a shiny theory is strongly finitely witnessable, hence strongly polite. □

3.2 Relating Polite and Shiny Theories

In this section, we relate polite and shiny theories using results from [6] and making use of a sufficient condition for the computability of the mincard function [9].

Begin by recalling the notion of *politeness* by Ranise, Ringeissen and Zarba [6].

Definition 10 (Politeness). *We say that a theory is* polite *whenever it is smooth and finitely witnessable.*

We prove that a polite theory is stably infinite, as mentioned in Remark 10 of [6].

Proposition 2. *A polite theory is stably finite.*

Proof. Let $\mathcal{T}$ be a polite theory, witness a witness function for $\mathcal{T}$, and φ a $\mathcal{T}$-satisfiable quantifier-free formula. Hence $\mathsf{witness}(\varphi)$ is $\mathcal{T}$-satisfiable and so there is a $\mathcal{T}$-model $\mathcal{A}$ satisfying $\mathsf{witness}(\varphi)$ with $\mathsf{dom}(\mathcal{A}) = [\![\mathsf{vars}(\mathsf{witness}(\varphi))]\!]^{\mathcal{A}}$. Since the number of variables in $\mathsf{witness}(\varphi)$ is finite we have that $\mathcal{A}$ is a finite model of this formula, and so of φ. Hence $\mathcal{T}$ is stably finite. □

We now recall a proposition by Ranise, Ringeissen and Zarba in [6] that provides conditions under which a polite theory is shiny.

Proposition 3 ([6]). *Let Σ be a finite signature and $\mathcal{T}$ a Σ-theory. Assume that it is decidable to check if a finite Σ-interpretation is a $\mathcal{T}$-model. Then, if $\mathcal{T}$ is polite then $\mathcal{T}$ is shiny and Algorithm 1 computes its* mincard *function.*

Algorithm 1 — $\mathsf{mincard}_{\mathsf{witness}}$ algorithm
Input: φ, where φ is a quantifier-free satisfiable formula
Output: k, where k is the cardinality of the smallest $\mathcal{T}$-model of φ
Requires: access to a witness function witness for $\mathcal{T}$

```
1: n = |vars(witness(φ))|;
2: for k = 1 to n
3:     for all non-isomorphic T-models A s.t. |dom(A)| = k do
4:         if A ⊩ φ then return k
5:     end for
6: end for
```

Observe that the conditions on the previous proposition are rather weak – for instance, if a theory $\mathcal{T}$ over Σ is finitely axiomatized then it is decidable to check if a finite Σ-interpretation is indeed a $\mathcal{T}$-model.

On the other hand, even if it is not decidable to check whether a finite interpretation is a $\mathcal{T}$-model, it is still possible to construct the mincard function provided that the theory $\mathcal{T}$ is universal as is stated in the next proposition. This proposition uses a result of Tinelli and Zarba in [9]. Observe that Algorithm 2 makes use of a *simple diagram* of an interpretation. We suggest [9] for this definition.

Proposition 4. *Let Σ be a finite signature and $\mathcal{T}$ a universal Σ-theory with a decidable quantifier-free satisfiability problem. Then, if $\mathcal{T}$ is polite then it is shiny and Algorithm 2 computes its* mincard *function.*

Proof. By Proposition 2 we obtain that $\mathcal{T}$ is stably finite. The thesis follows immediately by Proposition 23 in [9] that establishes that the mincard function of any theory is computable by Algorithm 2, if that theory is stably finite, universal, is over a finite signature, and has a decidable quantifier-free satisfiability problem. □

Algorithm 2 — $\mathsf{mincard}_{\mathcal{P}}$ algorithm, [9]
Input: φ, where φ is a quantifier-free satisfiable formula
Output: k, where k is the cardinality of the smallest $\mathcal{T}$-model of φ
Requires: access to an algorithm $\mathcal{P}$ that decides satisfiability of quantifier-free formulas and where $\Delta(\mathcal{A})$ denotes the simple diagram of $\mathcal{A}$

```
1: while true do
2:     k = 1
3:     for all non-isomorphic interpretations A s.t. |dom(A)| = k do
4:         if P(Δ(A) ∧ φ) == 1 then return k
5:     end for
6:     k = k + 1
7: end while
```

3.3 Relating Polite and Strongly Polite Theories

Finally, we state that a strongly finitely witnessable theory is also finitely witnessable.

Fact 1 *Each strongly finitely witnessable theory is finitely witnessable.*

This fact follows by observing that a strong witness function is also a witness function. Specifically, with respect to the second condition of the finite witnessability, let E and Y to be the empty set and the result follows.

3.4 Relating Shiny, Polite and Strongly Polite Theories

Combining the results in the previous sections, we obtain the equivalence between *strong politeness, shininess* and *politeness*, assuming two sets of different conditions on the theory.

Corollary 1. *Let $\mathcal{T}$ be a theory over a finite signature. If either*

- *$\mathcal{T}$ is universal; or*
- *checking whether a finite interpretation is a $\mathcal{T}$-model is decidable,*

then the following statements are equivalent:

1. *$\mathcal{T}$ is shiny;*
2. *$\mathcal{T}$ is strongly polite;*
3. *$\mathcal{T}$ is polite.*

Proof. (1. $\rightarrow$ 2.) Follows by Proposition 1.
(2. $\rightarrow$ 3.) Follows by Fact 1.
(3. $\rightarrow$ 1.) If $\mathcal{T}$ is universal, follows by Proposition 4, and if checking whether a finite interpretation is a $\mathcal{T}$-model is decidable, follows by Proposition 3. □

Capitalizing on the previous results on the relationship between strong politeness, shininess, and politeness, we now present a new algorithm, Algorithm 3, that computes a strong witness function for a smooth and finitely witnessable theory.

Theorem 1. *Let Σ be a finite signature and $\mathcal{T}$ a polite Σ-theory with a decidable quantifier-free satisfiability problem. Assume that either $\mathcal{T}$ is universal or it is decidable to check if a finite interpretation is a $\mathcal{T}$-model. Then, Algorithm 3 computes a strong witness function for $\mathcal{T}$.*

Proof. We begin by computing the mincard function. If $\mathcal{T}$ is universal, by Proposition 4 we have that the mincard function is computable and that Algorithm 2 is an algorithm for it. In the case that it is decidable to check if a finite Σ-interpretation is a $\mathcal{T}$-model, then by Proposition 3 we have that the mincard function is computed by Algorithm 1. Therefore, $\mathcal{T}$ is shiny. It is immediate to see that Algorithm 3 computes the function shown in the proof of Proposition 1 to be a strong witness function for $\mathcal{T}$, and so the thesis follows. □

Capitalizing on the relationships between the politeness, shininess and strong politeness established in the previous results, we can now establish a combination result very similar to the combination proposition of [3], Proposition 2, but instead of imposing that $\mathcal{T}_2$ is strongly finitely witnessable, imposes that $\mathcal{T}_2$ is

- finitely witnessable;
- either universal or such that checking if a finite Σ_2-interpretation is a model of $\mathcal{T}_2$ is decidable.

Algorithm 3 — Computes a strong witness function for a theory $\mathcal{T}$
Input: φ, where φ is a quantifier-free satisfiable formula
Output: $\mathsf{s\text{-}witness}(\varphi)$
Requires: access to an algorithm $\mathcal{P}$ that decides satisfiability of quantifier-free formulas, and to the function $\mathsf{mincard}$ for $\mathcal{T}$

for $E \subseteq \mathsf{vars}(\varphi)^2$
  $\delta_E^{\mathsf{vars}(\varphi)} = \varepsilon$
  for all pairs $(x, y) \in \mathsf{vars}(\varphi)^2$
    if $(x, y) \in E$
      then $\delta_E^{\mathsf{vars}(\varphi)} = \delta_E^{\mathsf{vars}(\varphi)} \wedge (x \cong y)$
      else $\delta_E^{\mathsf{vars}(\varphi)} = \delta_E^{\mathsf{vars}(\varphi)} \wedge \neg(x \cong y)$
    end if
  end for
  if $\mathcal{P}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)}) == 1$
    then $k_E = \mathsf{mincard}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)})$
      $\gamma_{k_E} = \varepsilon$
      for $i, j = 1$, $i \neq j$ **to** k_E
        $\gamma_{k_E} = \gamma_{k_E} \wedge \neg(x_i \cong x_j)$
      end for
      $\varphi = \varphi \wedge (\delta_E^{\mathsf{vars}(\varphi)} \rightarrow \gamma_{k_E})$
  end if
end for
return φ

Observe that showing these conditions may be more manageable than proving that $\mathcal{T}_2$ is strongly finitely witnessable, particularly because many theories of interest to SMT applications are either universal or finitely axiomatized.

In other words, these results show that in the one-sorted context, if a theory is either universal or is such that checking whether a finite interpretation is a model is decidable, then we can forget the strong politeness requirement and use the politeness condition by Ranise, Ringeissen and Zarba to construct both a strong witness function and the $\mathsf{mincard}$ function. These functions can then be used in the application of the Nelson-Oppen method for the combination of strongly polite theories or shiny theories with an arbitrary theory. The following result formalizes these statements in a Nelson-Oppen combination theorem.

Theorem 2. *Let Σ_2 be a finite signature and $\mathcal{T}_i$ a Σ_i-theory with a decidable quantifier-free satisfiability problem, for $i = 1, 2$, such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Assume that*

- *$\mathcal{T}_2$ is smooth;*
- *$\mathcal{T}_2$ has a witness function;*
- *either $\mathcal{T}_2$ is universal or checking if a finite Σ_2-interpretation is a model of $\mathcal{T}_2$ is decidable.*

Then, the function $\mathsf{mincard}_{\mathcal{T}_2}$ *is computable and there is a computable strong witness function,* $\mathsf{s\text{-}witness}_{\mathcal{T}_2}$*, for* $\mathcal{T}_2$*, such that the following statements are equivalent:*

1. $\Gamma_1 \wedge \Gamma_2$ *is* $\mathcal{T}_1 \oplus \mathcal{T}_2$ *satisfiable;*
2. *there exists* $E \subseteq Y^2$*, where* Y *is* $\mathsf{vars}(\Gamma_1) \cap \mathsf{vars}(\Gamma_2)$*, such that*
   - $\Gamma_1 \wedge \delta_E^Y \wedge \gamma_\kappa$ *is* $\mathcal{T}_1$*-satisfiable, where* κ *is* $\mathsf{mincard}_{\mathcal{T}_2}(\Gamma_2 \wedge \delta_E^Y)$*;*
   - $\Gamma_2 \wedge \delta_E^Y$ *is* $\mathcal{T}_2$*-satisfiable;*
3. *there exists* $E \subseteq Y^2$*, where* Y *is* $\mathsf{vars}(\mathsf{s\text{-}witness}(\Gamma_2))$*, such that*
   - $\Gamma_1 \wedge \delta_E^Y$ *is* $\mathcal{T}_1$*-satisfiable;*
   - $\mathsf{s\text{-}witness}_{\mathcal{T}_2}(\Gamma_2) \wedge \delta_E^Y$ *is* $\mathcal{T}_2$*-satisfiable;*

for every conjunction Γ_1 *of* Σ_1*-literals and* Γ_2 *of* Σ_2*-literals.*

Proof. Observe that the theory $\mathcal{T}_2$ is polite and that the $\mathsf{mincard}$ function of $\mathcal{T}_2$ is computable either by Proposition 3 if it is decidable to check if a finite Σ_2-interpretation is a model of $\mathcal{T}_2$; or by Proposition 4 if $\mathcal{T}_2$ is a universal theory. Moreover $\mathcal{T}_2$ has also a computable strong witness function by Theorem 1. Observe also that $\mathcal{T}_2$ is stably finite by Proposition 2. Then, the equivalence between (1) and (2) follows from the combination theorem in [9], Theorem 18, and the equivalence between (1) and (3) follows from the combination proposition, Proposition 2, in [3]. □

We now provide an example showing an application of the previous theorem.

Example 1. Consider the theories $\mathcal{T}_1$ and $\mathcal{T}_2$ over the empty signature such that $\mathcal{T}_1$ is axiomatized by $\forall x \forall y\ (x \cong y)$ and $\mathcal{T}_2$ is axiomatized by $\exists x \exists y\ \neg(x \cong y)$. Hence every model of $\mathcal{T}_1$ has cardinality at most one and every model of $\mathcal{T}_2$ has cardinality at least 2. Let φ denote the formula $(x \cong x)$.

Observe that, in [3], it was shown that theory $\mathcal{T}_2$ is smooth and that

$$\mathsf{witness}_{\mathcal{T}_2}(\varphi) := \varphi \wedge (w_1 \cong w_1) \wedge (w_2 \cong w_2)$$

is a witness function for $\mathcal{T}_2$. Hence this condition for the application of Theorem 2 is fulfilled. Taking into account that $\mathsf{mincard}_{\mathcal{T}_2}(\varphi) = 2$, then by Algorithm 3,

$$\begin{aligned} \mathsf{s\text{-}witness}_{\mathcal{T}_2}(\varphi) &= \varphi \wedge (x \cong x) \rightarrow \gamma_2 \\ &= \varphi \wedge (x \cong x) \rightarrow \neg(z_1 \cong z_2) \\ &= (x \cong x) \wedge \neg(z_1 \cong z_2). \end{aligned}$$

Let Γ_1 be the formula tt, Γ_2 the formula φ and Y the set $\mathsf{vars}(\mathsf{s\text{-}witness}(\Gamma_2))$ i.e. $\{x, z_1, z_2\}$. We now would like to check if there is an arrangement of δ_E^Y such that $\Gamma_1 \wedge \delta_E^Y$ is $\mathcal{T}_1$-satisfiable and $\mathsf{s\text{-}witness}(\Gamma_2) \wedge \delta_E^Y$ is $\mathcal{T}_2$-satisfiable. Note that the only arrangement satisfied in $\mathcal{T}_1$ is the one induced by $E = \{(x, z_1), (x, z_2), (z_1, z_2)\}$ since all others would require the interpretation to have cardinality greater than one. However, $\mathsf{s\text{-}witness}(\Gamma_2) \wedge \delta_E^Y$ is clearly not satisfiable. Hence, by Theorem 2, we conclude that φ is not satisfiable in $\mathcal{T}_1 \oplus \mathcal{T}_2$. In this simple case it is no difficult to see that this was the expected conclusion since there are no models that satisfy the theory resulting from the union of $\mathcal{T}_1$ and $\mathcal{T}_2$.

Observe the importance of Algorithm 3 to define in a computable way the strong witnessable function.

Examples of application of this theorem regarding interesting theories for SMT applications, such as the theory of lists and the theory of arrays, are, however, out of the scope of this paper since they are defined in a many-sorted context.

4 Conclusion and Further Research

In this paper we investigated the relationship between the notions of shininess, politeness and strong politeness. Answering a question left open by Jovanović and Barrett in [3], we showed that a shiny theory with a decidable quantifier-free satisfiability problem is strongly polite, as well as showed that a strongly polite theory is polite. Capitalizing on results relating shiny and polite theories from [6], as well as results regarding the computability of the mincard function from [9], we were able to establish that under two different sets of conditions, the notions of shininess, politeness and strong politeness are equivalent. Moreover, given the constructive nature of the proof showing that a shiny theory with a decidable quantifier-free satisfiability problem is strongly polite, we were able to devise a Nelson-Oppen procedure for the combination of a polite (with an additional restriction) and an arbitrary theory.

We leave as future work the extension of the results presented in this paper to the many-sorted case, as well as the study of the relationship between the complexity of the mincard function (already studied in [9]) and the complexity of a s-witness function. We also hope to address the extension of the results in [8] regarding constraint logic programming to shiny, polite and strongly polite theories.

Acknowledgments. We would like to acknowledge the anonymous reviewers for their helpful comments. This work was partially supported, under the MCL (Meet-Combination of Logics) and PQDR (Probabilistic, Quantum and Differential Reasoning) initiatives of SQIG at IT, by FCT and EU FEDER, namely via the FCT PEst-OE/EEI/LA0008/2013 and AMDSC UTAustin/MAT/0057/2008 projects, as well as by the European Union's Seventh Framework Programme for Research (FP7), namely through project LANDAUER (GA 318287).

References

1. C. Barrett, C. L. Conway, M. Deters, L. Hadarean, D. Jovanović, T. King, A. Reynolds, and C. Tinelli. CVC4. In *Computer aided verification*, volume 6806 of *Lecture Notes in Computer Science*, pages 171–177. Springer, Heidelberg, 2011.
2. J. Christ, J. Hoenicke, and A. Nutz. SMTInterpol: An interpolating SMT solver. In *SPIN*, volume 7385 of *Lecture Notes in Computer Science*, pages 248–254. Springer, 2012.
3. D. Jovanović and C. Barrett. Polite theories revisited. In *Proceedings of the Seventeenth International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'2010)*, volume 6397 of *LNCS*, pages 402–416, 2010.

4. G. Nelson and D. C. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1(2):245–257, 1979.
5. D. C. Oppen. Complexity, convexity and combinations of theories. *Theoretical Computer Science*, 12:291–302, 1980.
6. S. Ranise, C. Ringeissen, and C. G. Zarba. Combining data structures with nonstably infinite theories using many-sorted logic. In *Proceedings of the Fifth International Workshop on Frontiers of Combining Systems (FroCoS'2005)*, volume 3717 of *LNAI*, pages 48–64, 2005.
7. C. Tinelli and M. T. Harandi. A new correctness proof of the Nelson-Oppen combination procedure. In *Proceedings of the First International Workshop on Frontiers of Combining Systems (FroCoS'1996)*, volume 3 of *Applied Logic Series*, pages 103–119, 1996.
8. C. Tinelli and M. T. Harandi. Constraint logic programming over unions of constraint theories. *Journal of Functional and Logic Programming*, 1998(6), 1998.
9. C. Tinelli and C. G. Zarba. Combining nonstably infinite theories. *Journal of Automated Reasoning*, 34(3):209–238, 2005.