TÉCNICO LISBOA

On Nelson-Oppen Techniques

Filipe Manuel Rodrigues Casal

Thesis to obtain the Master of Science Degree in

Mathematics and Applications

Examination Committee

Chairperson: Prof. Maria Cristina Sales Viana Serôdio Sernadas
Supervisor: Prof. João Filipe Quintas dos Santos Rasga
Members of the Committee: Prof. Jaime Arsénio de Brito Ramos
Prof. João Marcos de Almeida

July 2013

Acknowledgments

First and foremost, I would like to thank my advisor Professor João Rasga for the mentoring and incredible support provided during the duration of this thesis, as well as for proposing the topic of the thesis. I would also like to thank those who contributed the most to my education in logic and computation, specially Professor Amílcar Sernadas, Professor Cristina Sernadas, Professor Carlos Caleiro, Professor João Rasga, Professor Jaime Ramos and Professor Paulo Mateus. I also would like to thank Professor Manuel Ricou as well as Professor Margarida Mendes Lopes for sharing their passion with mathematics with me. A special acknowledgment also goes to Diogo Poças for the wonderful discussions on the topic of this thesis, as well as for his friendship during the last five years.

I would like to thank Professor Cristina Sernadas, Professor Jaime Ramos and Professor João Marcos for their participation in the evaluation of this dissertation.

Finally, I also want to thank my family and friends for supporting me in pursuing what I love the most, specially Guilherme Ramos, André Reis, Pedro Nascimento, Cátia Nunes and Rita Garcia.

Resumo

O método de Nelson-Oppen [7] permite a combinação modular de procedimentos de satisfação de fórmulas sem quantificadores em teorias de primeira ordem num procedimento de satisfação de fórmulas sem quantificadores para a união das teorias. Este método, no entanto, requer que as teorias a unir tenham assinaturas disjuntas e que sejam estavelmente infinitas. Dada a importância do método, várias propostas com vista à extensão do método para outras classes de teorias foram feitas. Recentemente, duas extensões do método de Nelson-Oppen foram feitas, substituindo o requisito de que as teorias a unir tenham de ser estavelmente infinitas: em [14] é requerido que todas menos uma teoria sejam *shiny*, e em [9] é necessário que, quando se combinam duas teorias, uma delas seja *polite*. As relações entre teorias *shiny* e teorias *polite* é analisada em [9]. Mais tarde, uma noção mais forte de teorias *polite* foi proposta [6], de modo a superar um pormenor técnico na demonstração da correcção do método de Nelson-Oppen em [9]. Nesta tese, descrevemos o método original de Nelson e Oppen, assim como as suas extensões a teorias *shiny*, *polite* e fortemente *polite*. Respondendo a uma questão deixada em aberto em [6], analisamos as relações entre teorias *shiny* e fortemente *polite*. Mostramos que uma teoria *shiny* com o problema de satisfação de fórmulas sem quantificadores decidível é fortemente *polite* e provamos que sob dois conjuntos de hipóteses, uma teoria fortemente *polite* é *shiny*.

Palavras-chave: combinação de procedimentos de satisfação, método de Nelson-Oppen, teorias *polite*, teorias fortemente *polite*, teorias *shiny*

Abstract

The Nelson-Oppen method [7] allows the modular combination of quantifier-free satisfiability procedures of first-order theories into a quantifier-free satisfiability procedure for the union of the theories. However, this method requires the theories to have disjoint signatures and to be stably infinite. Due to the importance of the result, several attempts to extend the method to different and wider classes of theories were made. Recently, two different extensions of the Nelson-Oppen method were proposed, where the stably infinite requirement was replaced by another condition: in [14] it was required that all but one of the theories are shiny, and in [9] it was required that, when combining two theories, one of them is polite. The relationship between shiny and polite theories was analyzed in [9]. Later, a stronger notion of polite theory was proposed, see [6], in order to overcome a subtle issue with the proof of the Nelson-Oppen method in [9]. In this thesis, we describe the original Nelson-Oppen method, as well as its extensions to shiny, polite and strongly polite theories. Answering an open question from [6], we also analyze 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 sets of sufficient conditions for a strongly polite theory to be shiny.

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

Contents

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 [2] and SMTInterpol [3] 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, [7]. 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 [8], the two main restrictions of the Nelson-Oppen method are:

- the theories $\mathcal{T}_1$ and $\mathcal{T}_2$ are *stably infinite*,
- the signatures of $\mathcal{T}_1$ and $\mathcal{T}_2$ are disjoint.

Concerned about the fact that many theories of interest, such as those admitting only finite models, are not stably infinite, Tinelli and Zarba, in [14], 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. The authors also provide a combination theorem for theories that only admit finite models. They also study the mincard function in terms of computability and complexity, being able to provide sufficient conditions for it to be computable as well as proving that computing the mincard function for the equality theory is NP-hard.

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 [9]. 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. The authors also investigate the relationship between polite and shiny theories, proving that shiny theories are polite and that under rather weak assumptions, the converse also holds. Some time later, in [6], Jovanović and Barrett reported that the politeness notion provided in [9] allowed, after all, witness functions that are not sufficiently strong to prove the combination theorem. In order to clarify the proof, they provide a seemingly stronger definition of polite theories, in the sequel called *strongly polite theories*, equipped with a strong 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 strong politeness and shininess.

In this thesis, we strive to make a thorough and detailed presentation of the described results in a self-contained way, using a uniform notation. Furthermore, we present new results concerning the relation between the stronger politeness notion and shininess. This leads to a newly found relation between the notions of politeness and strong politeness.

1.1 Organization

This thesis is organized as follows: in Chapter 2 we introduce the notation used in the document; in Chapter 3 we motivate and prove the correctness of the Nelson-Oppen method for stably infinite theories; in Chapter 4 we present the Nelson-Oppen method for the combination of theories with only finite models. We also define shiny theories and present the Nelson-Oppen method for the combination of an arbitrary theory and a shiny theory, and provide conditions on the computability of the mincard function, as well as analyze its theoretical complexity. In Chapter 5, we introduce the notion of polite and strongly polite theories, proving the combination theorem for an arbitrary theory and a strongly polite theory. In Chapter 6, we investigate the relationship between shiny, polite and strongly polite theories. Finally, in Chapter 7, we conclude this thesis and suggest directions for further research.

2 – Notation

In this section we define concepts and fix notation that will be used across the document. For this, we mainly follow [10] for the notation concerning first order logic and [14] for concepts specific to the theory combination area.

2.1 Syntax

A *signature* is a tuple $\Sigma = \langle F, P\rangle$ where F is the set of function symbols and P is the set of predicate symbols. We use $\cong$ to denote the equality logical symbol and assume it is a logical symbol and not a predicate symbol in P. Furthermore, we assume set once and for all the denumerable set of variables X. We inductively define the set of Σ-*terms*, T_Σ as $x \in T_\Sigma$ whenever $x \in X$ and $f(t_1, \ldots, t_n) \in T_\Sigma$ whenever $t_1, \ldots, t_n \in T_\Sigma$ and $f \in F$. A Σ-*atom* is either $p(t_1, \ldots, t_n)$ for $t_1, \ldots, t_n \in T_\Sigma$ and $p \in P$ or $s \cong t$ where s, t are Σ-terms. 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 QF(Σ) the set of Σ-formulas with no occurrences of quantifiers, by vars(φ) the set of variables occurring in φ and by fvars(φ) 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 2.1 (Arrangement formula)**.** Given a finite set of variables Y, and an equivalence relation $E \subseteq Y^2$ the formula

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

is the *arrangement formula* induced by E over Y, denoted by δ_E^Y. In the sequel, we will simply denote δ_E^Y by δ_E if there is no confusion to which variable set the formula refers to.

In the sequel we will need to certify that a given theory only has models with higher cardinality than some integer. For this, consider the following family of formulas.

Definition 2.2 (γ-formulas)**.** Given a positive integer k, we denote by γ_k the formula

$$\bigwedge_{\substack{i,j=1\\ i\neq j}}^{k} w_i \ncong w_j$$

where $w_1, \ldots, w_k$ are variables.

2.2 Semantics

Given a signature Σ, a Σ-*interpretation* $\mathcal{A}$ is a tuple $\langle D, \_^F, \_^P \rangle$ where D is the domain of $\mathcal{A}$, $\_^F$ is a map that for each nonnegative integer n, interprets each function symbol $f \in F$ of arity n as a function $f^F : D^n \to D$ and $\_^P$ is a map that for each positive integer n, interprets each predicate symbol $p \in P$ of arity n as a subset p^P of D^n. We denote by $\text{dom}(\mathcal{A})$ the domain of an interpretation $\mathcal{A}$. An *assignment* ρ over an interpretation $\mathcal{A}$ is a map $\rho : X \to \text{dom}(\mathcal{A})$ from the variable set to the domain of $\mathcal{A}$.

Given a Σ-interpretation $\mathcal{A}$, an assignment ρ over $\mathcal{A}$ and a Σ-term t, we denote by $[\![t]\!]^{\mathcal{A}\,\rho}$ the interpretation of t under $\mathcal{A}$ and ρ. Similarly, we denote by $[\![\varphi]\!]^{\mathcal{A}\,\rho}$ the truth value of the formula φ under the interpretation $\mathcal{A}$ and assignment ρ. Furthermore, given a set Γ of formulas, we denote by $[\![\Gamma]\!]^{\mathcal{A}\,\rho}$ the set $\{[\![\varphi]\!]^{\mathcal{A}\,\rho} : \varphi \in \Gamma\}$. The generalization for a set of terms is made analogously.

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

Given a set of variables Y we say that two assignments σ, ρ over an interpretation $\mathcal{A}$ are Y-*equivalent*, $\sigma \equiv_Y \rho$, when $\sigma(x) = \rho(x)$ for all $x \in X \setminus Y$.

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

We define the *reduct* along a signature $\Sigma' \subseteq \Sigma$ of an interpretation structure $\mathcal{A}$ over signature Σ, denoted by $\mathcal{A}|_{\Sigma'}$, as the interpretation with the same domain as $\mathcal{A}$, but only containing the interpretations of function and predicate symbols of Σ'.

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.

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 Σ_1-sentences of $\mathcal{T}_1$ with the Σ_2-sentences of $\mathcal{T}_2$.

We say that a Σ-theory $\mathcal{T}$ has a decidable quantifier-free satisfiability problem when there is an algorithm $\mathsf{Sat}_{\mathcal{T}} : \mathsf{QF}(\Sigma) \to \{0, 1\}$ behaves as follows:

$$\mathsf{Sat}_{\mathcal{T}} = \lambda\varphi. \begin{cases} 1 & \text{if } \varphi \text{ is } \mathcal{T}\text{-satisfiable} \\ 0 & \text{otherwise.} \end{cases}$$

3 – The Nelson-Oppen technique

3.1 Motivation and historical overview

In this chapter we will introduce the Nelson-Oppen method in its first version, proposed by Nelson and Oppen in 1979, [7]. At that time, the authors realized that program verifiers, symbolic evaluators and "high level" program manipulation systems could make the programming process more automatic and would be able to formally verify assertions about the programs. However, at that time, these program verifiers and manipulators highly depended on theorem provers that were not efficient or could not even deal with most of the cases presented. An example where a new method was required is the following: a program manipulator system finds important to change (for compiling optimization) the order in which a for loop is executed (running for $i = n$ to 0 instead of for $i = 0$ to n). However, in order to verify this transformation, the program manipulator needs to call a theorem prover that proves that what is in fact done inside the loop can be executed both ways with the same effect. Suppose that inside the loop only the instruction $a[i] = f(i)$ is made, where a is an array and f some function not involving a. The theorem prover had to verify if

$$\mathsf{store}(\mathsf{store}(a, i, f(i)), i+1, f(i+1)) = \mathsf{store}(\mathsf{store}(a, i+1, f(i+1)), i, f(i)),$$

where $\mathsf{store}(a, i, e)$ denotes array a where in position i, element e is placed. However, observe that the theorem prover needs to be able to reason both about the theory of arrays (due to the store function), the theory of integers (due to the presence of the addition symbol) and the theory of uninterpreted functions (due to the function f). This type of reasoning about assertions over multiple theories was not well studied and was made on a case by case basis such as the work of Suzuki and Jefferson [11] on the theory of arrays and Presburger arithmetic.

With this is mind, the goal of the authors was to devise a method to modularly combine satisfiability procedures of two generic theories into a satisfiability procedure for the union of the theories. Formally, given two theories $\mathcal{T}_1$ and $\mathcal{T}_2$ over disjoint signatures Σ_1 and Σ_2 with a decidable quantifier-free satisfiability decision procedure, we want to design a quantifier-free satisfiability procedure for the theory $\mathcal{T}_1 \oplus \mathcal{T}_2$. In the sequel, we will see that additional conditions will have to be imposed on the theories in order to be possible to construct such procedure.

3.2 The Nelson-Oppen technique

Let $\mathcal{T} = \mathcal{T}_1 \oplus \mathcal{T}_2$ be a theory over the signature $\Sigma = \Sigma_1 \cup \Sigma_2$, such that $\Sigma_1 \cap \Sigma_2 = \emptyset$, and consider a quantifier-free Σ-formula φ. If it is the case that $\varphi = \bigwedge_{i=1}^{n} \varphi_i$, with $\phi_1 = \bigwedge_{i=1}^{k} \varphi_i \in \mathsf{QF}(\Sigma_1)$ and $\phi_2 = \bigwedge_{i=k+1}^{n} \varphi_i \in \mathsf{QF}(\Sigma_2)$ such that $\mathsf{vars}(\phi_1) \cap \mathsf{vars}(\phi_2) = \emptyset$, then a simple procedure could be constructed to decide the satisfiability of φ in $\mathcal{T}$: we simply have to apply the decision procedure $\mathsf{Sat}_{\mathcal{T}_1}$ to ϕ_1 and $\mathsf{Sat}_{\mathcal{T}_2}$ to ϕ_2. Since there is no variable sharing between the formulas this procedure would decide if φ is satisfiable in $\mathcal{T}$ iff ϕ_1 is $\mathcal{T}_1$-satisfiable and ϕ_2 is $\mathcal{T}_2$-satisfiable. However, this is not always the case – it may happen that the formulas of the different signatures share variables, or even that there are terms containing symbols from both signatures. If this is the case, a *purification procedure* must first be applied to the formula.

Definition 3.1 (Pure term, alien term, pure literal, purification procedure)**.** Given disjoint signatures Σ_1 and Σ_2, and a term t in $\Sigma = \Sigma_1 \cup \Sigma_2$, we say that t is *pure* when it is a term over Σ_1 or over Σ_2. A term is said to be *alien* when it is not pure. A literal in Σ is *pure* when it is of the form $p(t_1, \ldots, t_n)$ and there is an i in $\{1, 2\}$ such that $t_1, \ldots, t_n$ are pure terms from Σ_i and p is a predicate symbol in Σ_i. A *purification procedure* is an algorithm that given a conjunction of literals returns an equivalent conjunction of pure literals. This is done by replacing each alien term by a fresh variable and adding an additional equality between the replaced term and the fresh variable. This procedure is recursively applied until all terms are pure.

The following example illustrates this method.

Example 3.1. *Consider the following literal in* $\Sigma_1 \cup \Sigma_2$

$$p_1(f_1(x_1, c_2), g_2(x_2), f_1'(x_1), c_2'),$$

where p_1, f_1, f_1' *belong to* Σ_1 *and* c_2, g_2, c_2' *belong to* Σ_2*. The first alien term found is* c_2 *in* $f_1(x_1, c_2)$*. We replace* c_2 *by* y_1 *and add the equality* $c_2 \cong y_1$ *obtaining*

$$p_1(f_1(x_1, y_1), g_2(x_2), f_1'(x_1), c_2') \wedge c_2 \cong y_1.$$

Continuing the procedure in a similar fashion, we obtain the equivalent conjunction of pure terms

$$p_1(f_1(x_1, y_1), y_2, f_1'(x_1), y_3) \wedge c_2 \cong y_1 \wedge g_2(x_2) \cong y_2 \wedge y_3 \cong c_2'.$$

We now show that the purification procedure preserves satisfiability of the formula in the theory.

Proposition 3.2. *Let* φ *be a conjunction of literals over* $\Sigma = \Sigma_1 \cup \Sigma_2$ *and* $\mathcal{T}$ *a theory over* Σ*. Then, after the purification procedure we obtain the formulas* φ_i *over* Σ_i *for* $i \in \{1, 2\}$*, such that*

$$\varphi \textit{ is satisfiable in } \mathcal{T} \textit{ iff } \varphi_1 \wedge \varphi_2 \textit{ is satisfiable in } \mathcal{T}.$$

Proof. $(\rightarrow)$ Let $\mathcal{A}$ be a $\mathcal{T}$-model and ρ an assignment over $\mathcal{A}$ such that $\mathcal{A}\ \rho \Vdash \varphi$.

Let ρ' be an assignment such that

- $\rho'(x) = \rho(x)$, for $x \in \mathsf{vars}(\varphi)$;
- $\rho'(y) = [\![t]\!]^{\mathcal{A}}\,\rho$, for each variable y and term t such that y is not in $\mathsf{vars}(\varphi)$, y is in $\mathsf{vars}(\varphi_1 \wedge \varphi_2)$ and the equality between y and t was introduced in the purification procedure.

Then $\mathcal{A}\ \rho' \Vdash \varphi_1 \wedge \varphi_2$.

($\leftarrow$) In fact, if we have a $\mathcal{T}$-model $\mathcal{A}$ and an assignment ρ over $\mathcal{A}$ such that $\mathcal{A}\ \rho \Vdash \varphi_1 \wedge \varphi_2$ then $\mathcal{A}\ \rho \Vdash \varphi$. □

The following proposition provides a necessary condition for a formula to be satisfiable in the union of two theories, in terms of their subformulas being satisfiable in their original theories.

Proposition 3.3. *Let $\varphi_1 \wedge \varphi_2$ a formula obtained after a purification procedure for φ. If $\varphi_1 \wedge \varphi_2$ is satisfiable in $\mathcal{T} = \mathcal{T}_1 \oplus \mathcal{T}_2$ then there exists $E \subseteq Y^2$, where Y is $\mathsf{vars}(\varphi_1) \cap \mathsf{vars}(\varphi_2)$, such that*

- *$\varphi_1 \wedge \delta_E^Y$ is $\mathcal{T}_1$-satisfiable;*
- *$\varphi_2 \wedge \delta_E^Y$ is $\mathcal{T}_2$-satisfiable.*

Proof. Let $\mathcal{A}$ be a $\mathcal{T}$-interpretation and ρ an assignment over $\mathcal{A}$ such that $\mathcal{A}\ \rho \Vdash \varphi_1 \wedge \varphi_2$. Then, the arrangement formula $\delta_{E_\rho}^Y$ induced by $E_\rho = \{(x, y) : x, y \in Y \text{ and } \rho(x) = \rho(y)\}$ is satisfied by $\mathcal{A}$ and ρ, by construction. Therefore, $\mathcal{A}|_{\Sigma_1}$ is a $\mathcal{T}_1$ model of $\varphi_1 \wedge \delta_{E_\rho}^Y$ and $\mathcal{A}|_{\Sigma_2}$ is a $\mathcal{T}_2$ model of $\varphi_2 \wedge \delta_{E_\rho}^Y$. □

Unfortunately, an additional requirement is needed to prove the converse of the previous proposition to ultimately prove the correctness of the combination procedure. As we will show in Example 3.2, problems might arise when one of the theories only admits finite models.

Definition 3.4 (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.

Several theories have been proved to be stably infinite. This is the case for the theory of equality, the theory of integer arithmetic or the theory of arrays. On the other hand, it is worthwhile mentioning that a theory with an infinite model does not directly imply it is stably infinite. Consider the case of a theory defined by $\forall x \forall y \forall z\ p(z) \rightarrow\ (x \cong y)$. The theory admits infinite models, however the formula $p(z)$ is also satisfiable but only in the trivial models of the theory.

Proposition 3.5. *Let $\Sigma = \Sigma_1 \cup \Sigma_2$ such that $\Sigma_1 \cap \Sigma_2 = \emptyset$, and let $\mathcal{T}_i$ be stably infinite theories. If there exists a relation $E \subseteq Y^2$, where Y is $\mathsf{vars}(\varphi_1) \cap \mathsf{vars}(\varphi_2)$ such that*

- *$\varphi_1 \wedge \delta_E^Y$ is $\mathcal{T}_1$-satisfiable;*
- *$\varphi_2 \wedge \delta_E^Y$ is $\mathcal{T}_2$-satisfiable,*

then $\varphi_1 \wedge \varphi_2$ is $\mathcal{T}_1 \oplus \mathcal{T}_2$-satisfiable.

Proof. Since $\varphi_1 \wedge \delta_E^Y$ is $\mathcal{T}_1$-satisfiable and $\varphi_2 \wedge \delta_E^Y$ is $\mathcal{T}_2$-satisfiable, we have that

- there exists an interpretation structure $\mathcal{A}_1$ over Σ_1 such that $\mathcal{A}_1 \Vdash \mathcal{T}_1$ and an assignment ρ_1 over $\mathcal{A}_1$ such that $\mathcal{A}_1\ \rho_1 \Vdash \varphi_1 \wedge \delta_E^Y$;
- there exists an interpretation structure $\mathcal{A}_2$ over Σ_2 such that $\mathcal{A}_2 \Vdash \mathcal{T}_2$ and an assignment ρ_2 over $\mathcal{A}_2$ such that $\mathcal{A}_2\ \rho_2 \Vdash \varphi_2 \wedge \delta_E^Y$.

Since the theories are stably infinite, we can assume without loss of generality that $\mathcal{A}_1$ and $\mathcal{A}_2$ are infinite models. Hence

$$\mathcal{A}_1 \Vdash \exists(\varphi_1 \wedge \delta_E^Y) \text{ and } \mathcal{A}_2 \Vdash \exists(\varphi_2 \wedge \delta_E^Y)$$

and so

$$\mathcal{A}_1 \Vdash \mathcal{T}_1 \cup \{\exists(\varphi_1 \wedge \delta_E^Y)\} \text{ and } \mathcal{A}_2 \Vdash \mathcal{T}_2 \cup \{\exists(\varphi_2 \wedge \delta_E^Y)\}.$$

We conclude that the theories

$$\mathcal{T}_1' = \mathcal{T}_1 \cup \{\exists(\varphi_1 \wedge \delta_E^Y)\} \text{ and } \mathcal{T}_2' = \mathcal{T}_2 \cup \{\exists(\varphi_2 \wedge \delta_E^Y)\}$$

have infinite models. By the upwards Löwenheim-Skolem theorem, there is a cardinal α high enough so that there exist models of $\mathcal{T}_1'$ and $\mathcal{T}_2'$ with cardinality α. Hence, we have

- a $\mathcal{T}_1'$-model $\mathcal{A}_1'$; and
- a $\mathcal{T}_2'$-model $\mathcal{A}_2'$;

such that $\mathcal{A}_1'$ and $\mathcal{A}_2'$ have the same cardinality.

Let ρ_1' and ρ_2' be assignments such that

$$\mathcal{A}_1'\ \rho_1' \Vdash \varphi_1 \wedge \delta_E^Y \text{ and } \mathcal{A}_2'\ \rho_2' \Vdash \varphi_2 \wedge \delta_E^Y.$$

Considering Y as $\mathsf{vars}(\varphi_1) \cap \mathsf{vars}(\varphi_2)$, let $\eta : [\![Y]\!]^{\mathcal{A}_1'\ \rho_1'} \to [\![Y]\!]^{\mathcal{A}_2'\ \rho_2'}$ such that $\eta(\rho_1'(x)) = \rho_2'(x)$ for all $x \in Y$. This map is well defined since both assignments satisfy the same equalities and inequalities of δ_E^Y and is one-to-one. Furthermore, since the models $\mathcal{A}_1'$ and $\mathcal{A}_2'$ have the same cardinality, we can extend the bijection η to their domains.

Based on bijection η, we now build an interpretation structure $\mathcal{A}$ extending $\mathcal{A}_1'$ and $\mathcal{A}_2'$ to signature Σ, $\mathcal{A} = \langle D, \_^F, \_^P \rangle$. Define D as the domain of $\mathcal{A}_1'$, the denotations of function and predicate symbols from Σ_1 are made as in $\mathcal{A}_1'$ and the denotations of the function and predicate symbols from Σ_2 are as in $\mathcal{A}_2'$, but viewing the elements of D as elements in the domain of $\mathcal{A}_2'$ via the bijection η. With this construction we obtain directly that

$$\mathcal{A}|_{\Sigma_i} \text{ is } \mathcal{A}_i' \text{ modulo isomorphism}$$

which concludes that $\mathcal{A}$ is a model of $\mathcal{T}_1'$ and $\mathcal{T}_2'$, and furthermore of $\mathcal{T}_1 \oplus \mathcal{T}_2$. Moreover, defining σ as an assignment over $\mathcal{A}$ such that $\sigma(x) = \rho_1'(x)$ we have that

$$\mathcal{A}\ \sigma \Vdash \varphi_1 \wedge \delta_E^Y \text{ and } \mathcal{A}\ \sigma \Vdash \varphi_2 \wedge \delta_E^Y$$

implying that

$$\mathcal{A}\ \sigma \Vdash \varphi_1 \wedge \varphi_2,$$

and concluding that $\varphi_1 \wedge \varphi_2$ is satisfiable in $\mathcal{T}_1 \oplus \mathcal{T}_2$. □

Observation: Notice that in the proof of Proposition 3.5 we have proved the following theorem:

Theorem 3.6. *Let $\mathcal{T}_i$ be Σ_i-theories for $i = 1, 2$ such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Denote by Σ the signature $\Sigma_1 \cup \Sigma_2$ and by $\mathcal{T}$ the theory $\mathcal{T}_1 \oplus \mathcal{T}_2$ and let Γ_i be a set of Σ_i literals for $i = 1, 2$ and $V = \mathsf{vars}(\Gamma_1) \cap \mathsf{vars}(\Gamma_2)$. If there exists*

- *a $\mathcal{T}_1$-model $\mathcal{A}$ and assignment ρ such that $\mathcal{A}\ \rho \Vdash \Gamma_1 \wedge \delta_E^V$;*
- *a $\mathcal{T}_2$-model $\mathcal{B}$ and assignment μ such that $\mathcal{B}\ \mu \Vdash \Gamma_2 \wedge \delta_E^V$;*
- *and $|\mathsf{dom}(\mathcal{B})| = |\mathsf{dom}(\mathcal{A})|$,*

then there exists a $\mathcal{T}_1 \oplus \mathcal{T}_2$-model $\mathcal{C}$ and assignment σ such that $\mathcal{C}\ \sigma \Vdash \Gamma_1 \wedge \Gamma_2 \wedge \delta_E^V$ and $\mathcal{C}|_{\Sigma_1} = \mathcal{A}$ and $\mathcal{C}|_{\Sigma_2} = \mathcal{B}$ modulo isomorphism.

We are now able to present one version of the original Nelson-Oppen algorithm for the decision of satisfiability of quantifier-free formulas in the union of stably infinite theories.

Algorithm 1 — Nelson-Oppen algorithm
Input: φ, where φ is a quantifier-free formula over Σ
Output: $Sat_{\mathcal{T}}(\varphi)$

1: **find** φ_i over Σ_i such that φ is equivalent to $\varphi_1 \wedge \varphi_2$ by purifying φ
2: **if** $\mathsf{Sat}_{\mathcal{T}_1}(\varphi_1) == 0$ or $\mathsf{Sat}_{\mathcal{T}_2}(\varphi_2) == 0$
3: **then** return 0
4: **end if**
5: **if** there exists a relation $E \subseteq Y^2$, where $Y = \mathsf{vars}(\varphi_1) \cap \mathsf{vars}(\varphi_2)$ such that $\mathsf{Sat}_{\mathcal{T}_1}(\varphi_1 \wedge \delta_E^Y) == 1$ and $\mathsf{Sat}_{\mathcal{T}_2}(\varphi_2 \wedge \delta_E^Y) == 1$
6: **then** return 1
7: **else** return 0
8: **end if**

Proposition 3.7. *Let $\mathcal{T}_i$ be stably infinite Σ_i-theory for $i = 1, 2$ such that $\Sigma_1 \cap \Sigma_2 = \emptyset$ and with a decidable quantifier-free satisfiability problem. Then Algorithm 1 is a decidable satisfiability procedure for quantifier-free formulas of $\mathcal{T}_1 \oplus \mathcal{T}_2$.*

Proof. We start by proving that Algorithm 1 always terminates when given a quantifier-free formula in Σ. The purification procedure always terminates since the formula is finite. Step 2 of the algorithm is computable and always terminates since the decision procedures $\mathsf{Sat}_{\mathcal{T}_i}$ are computable by hypothesis. The fifth instruction of the algorithm is also computable since the set $Y = \mathsf{vars}(\varphi_1) \cap \mathsf{vars}(\varphi_2)$ is finite and therefore there are a finite number of relations $E \subseteq Y^2$.

Considering the correctness of the algorithm, we have that the first instruction preserves satisfiability of the formula (by Proposition 3.2). Considering instruction 2, if one of the subformulas φ_1 or φ_2 is not satisfiable, then their conjunction is also not satisfiable (by Proposition 3.3). Now, if the algorithm returns

0 in line 7, this means that there is no $E \subseteq Y^2$ such that at least one of $\varphi_i \wedge \delta_E^Y$ is satisfiable. Then, we conclude by Proposition 3.3 that $\varphi_1 \wedge \varphi_2$ is not $\mathcal{T}_1 \oplus \mathcal{T}_2$ satisfiable. On the other hand, if the algorithm returns 1 in line 6, we have by Proposition 3.5 that $\varphi_1 \wedge \varphi_2$ is $\mathcal{T}_1 \oplus \mathcal{T}_2$-satisfiable. □

Capitalizing on the previous results and the presented algorithm, we are now able to state the combination theorem for stably infinite theories with disjoint signatures.

Theorem 3.8 ([13])**.** *Let $\mathcal{T}_i$ be Σ_i-theory for $i = 1, 2$ such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Let Γ_i be a conjunction of Σ_i literals for $i = 1, 2$. Assume that $\mathcal{T}_1$ and $\mathcal{T}_2$ are stably infinite. Then the following statements are equivalent:*

1. *$\Gamma_1 \wedge \Gamma_2$ is $\mathcal{T}_1 \oplus \mathcal{T}_2$ satisfiable.*
2. *There exists an arrangement δ_E^V such that $\Gamma_1 \wedge \delta_E^V$ is $\mathcal{T}_1$-satisfiable and $\Gamma_2 \wedge \delta_E^V$ is $\mathcal{T}_2$-satisfiable, for $V = \mathsf{vars}(\Gamma_1) \cap \mathsf{vars}(\Gamma_2)$.*

The following example shows that problems might arise when one of the theories is not stably infinite, imposing it as a sufficient condition for this method to work.

Example 3.2. *Let $\mathcal{T}_1$ be a theory only admitting models with cardinality at most 2 and $\mathcal{T}_2$ a theory admitting models with any cardinality over a signature disjoint from the signature of $\mathcal{T}_1$ and denote by $\mathcal{T}$ the union $\mathcal{T}_1 \oplus \mathcal{T}_2$. Assume that f is a function symbol from Σ_1 and g a function symbol from Σ_2. Consider the formula*

$$\varphi := f(x) \not\cong f(y) \wedge g(x) \not\cong g(z) \wedge g(y) \not\cong g(z).$$

Since the terms are pure terms, using theorem 3.8 we obtain that $\Gamma_1 := f(x) \not\cong f(y)$ and $\Gamma_2 := g(x) \not\cong g(z) \wedge g(y) \not\cong g(z)$. Since the shared variables between the two formulas is the set $s = \{x, y\}$ we now need to check the satisfiability of Γ_i with the arrangements over s, which are either $x \cong y$ or $x \not\cong y$.

Considering the first arrangement, we obtain that $\Gamma_1 \wedge x \cong y = f(x) \not\cong f(y) \wedge x \cong y$ is clearly not satisfiable. Considering the second arrangement, we have that $\Gamma_1 \wedge x \not\cong y = f(x) \not\cong f(y) \wedge x \not\cong y$ is $\mathcal{T}_1$-satisfiable and $\Gamma_2 \wedge x \not\cong y = g(x) \not\cong g(z) \wedge g(y) \not\cong g(z) \wedge x \not\cong y$ is $\mathcal{T}_2$-satisfiable. By blindly applying theorem 3.8 we would conclude that $\Gamma_1 \wedge \Gamma_2$ is satisfiable in the union of the theories. However, we have that

$$\mathcal{T} \models \varphi \rightarrow (x \not\cong y \wedge x \not\cong z \wedge y \not\cong z)$$

which makes φ unsatisfiable in the union of the theories, since as $\mathcal{T}_1$, the union only admits models with cardinality at most 2. The combination theorem fails in this case since $\mathcal{T}_1$ is not stably infinite.

The previous example, on the one hand shows that the stable infiniteness property is needed, but on the other hand it provides a hint on how the procedure could be generalized to theories with only finite models. Assuming that there exists a theory specific procedure that given a satisfiable formula is able to compute the cardinality of a model for it, checking if cardinality constraints on the theory are violated would be quite simple. This is a development that will be further explored in the following chapter and is due to Tinelli and Zarba, in [14].

3.3 Summary of the chapter

In this chapter we began by motivating the seminal work by Nelson and Oppen in 1979 when they first started to combine satisfiability procedures for different theories into one procedure for the union of the theories. We then present the results that prove the correctness of the combination procedure for stably infinite theories. These results follow the work and can be found (possibly with different notation than the one used in the present document) in Nelson and Oppen [7], Oppen [8], Tinelli and Harandi [12] and Tinelli and Ringeissen [13]. Furthermore, we presented an example showing that the stably infinite restriction on the theories is indeed required for this combination procedure to work.

4 – Shiny theories

Despite the Nelson-Oppen method being a huge step forward in improving theorem provers, as seen in the end of the previous chapter, the original method fails when one of the theories is not stably infinite. Two problems emerged at this time: on one hand, people wanted to know for which classes of theories similar combination methods existed; on the other hand, a more practical necessity emerged since many theories of interest were not stably infinite.

In this chapter, following the work by Tinelli and Zarba, in [14], we detail a new combination procedure that deals with theories that have only finite models. Moreover, we also provide another combination method for the union of an arbitrary theory with a *shiny* theory. For this, consider the following definitions.

Definition 4.1 (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 4.2 ($\mathsf{mincard}_{\mathcal{T}}$ 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

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

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 as to which theory the function refers to we will simply write $\mathsf{mincard}$.

In this chapter, unless mentioned otherwise, when a Nelson-Oppen combination algorithm is presented we assume that upon input, the purification procedure is promptly executed and are only interested in the verification phase of the purified input. Also, we assume the algorithm receives with the input an arrangement formula over the shared variables of the two purified subformulas of the input, δ_E. This means that the real decision procedure will have to execute the presented algorithms for all arrangement formulas, instead of explicitly searching for δ_E as in Algorithm 1.

4.1 Theories with finite models

We will now introduce a combination method for theories with finite models such as the one in [14]. Let Σ_1 and Σ_2 be disjoint signatures and $\mathcal{T}_1$ and $\mathcal{T}_2$ be Σ_1 and Σ_2 theories, respectively. Assume for the duration of this section that

- $\mathcal{T}_1$ and $\mathcal{T}_2$ are stably finite;
- the $\mathsf{mincard}_{\mathcal{T}_i}$ function is computable for $i = 1, 2$;
- $\mathcal{T}_1$ has only finite models;
- the quantifier-free satisfiability problem is decidable for both theories.

Consider the following algorithm for deciding the satisfiability of quantifier-free formulas in $\mathcal{T} = \mathcal{T}_1 \oplus \mathcal{T}_2$.

Algorithm 2 — first adaptation of the Nelson-Oppen algorithm
Input: $\Gamma = \Gamma_1 \wedge \Gamma_2 \wedge \delta_E$, where Γ is a quantifier-free satisfiable formula over Σ
Output: $\mathsf{Sat}_{\mathcal{T}}(\Gamma)$, where $\mathcal{T} = \mathcal{T}_1 \oplus \mathcal{T}_2$

```
1: N = 1
2: while true do
3:     if exists i such that Sat_{T_i}(Γ_i ∧ δ_E ∧ γ_N) == 0 then
4:         return 0
5:     else if exists i such that mincard_{T_i}(Γ_i ∧ δ_E ∧ γ_N) == m > N
6:         then N = m
7:         else return 1
```

We first prove this algorithm always terminates.

Proposition 4.3. *Algorithm 2 terminates when given a purified quantifier-free formula Γ.*

Proof. Assume, in view of an absurd that Algorithm 2 does not terminate. This implies that $\mathsf{Sat}_{\mathcal{T}_1}(\Gamma_1 \wedge \delta_E \wedge \gamma_N) = 1$ for any increasing N which implies (by compactness) that $\Gamma_1 \wedge \delta_E$ is satisfiable in an infinite $\mathcal{T}_1$-model, contradicting the hypothesis that all $\mathcal{T}_1$ models are finite. □

Proposition 4.4. *If the purified quantifier-free formula Γ is $\mathcal{T}$-satisfiable then Algorithm 2 returns 1.*

Proof. Let $\mathcal{A}$ be a $\mathcal{T}$-model satisfying Γ. Since $\mathcal{A}$ is a $\mathcal{T}$-model we conclude that it also is a $\mathcal{T}_1$-model and hence that the cardinality of $\mathsf{dom}(\mathcal{A})$ is a finite number, κ. Since Algorithm 2 terminates by Proposition 4.3, let $k_1, \ldots, k_n$ be the sequence of numbers taken by N in the execution of the algorithm. We now prove that $k_j \leq \kappa$ for $j = 1, \ldots, n$. The base case holds trivially. Now, assume that $k_j \leq \kappa$. By construction, there is an i such that $k_{j+1} = \mathsf{mincard}_{\mathcal{T}_i}(\Gamma_i \wedge \delta_E \wedge \gamma_{k_j})$. But since $\mathcal{A}$ satisfies $\Gamma_i \wedge \delta_E \wedge \gamma_{k_j}$, we have that $k_{j+1} \leq \kappa$. Since all values taken by N are less than or equal to the cardinality of $\mathcal{A}$, we have that the procedure must return 1. □

Proposition 4.5. *If the Algorithm 2 returns 1 for a purified quantifier-free formula Γ then Γ is $\mathcal{T}$-satisfiable.*

Proof. If k is the last value N takes before the program returns 1, then this means that for $i = 1, 2$ that $\mathsf{Sat}_{\mathcal{T}_i}(\Gamma_i \wedge \delta_E \wedge \gamma_k) == 1$ and that $\mathsf{mincard}_{\mathcal{T}_i}(\Gamma_i \wedge \delta_E \wedge \gamma_k) == k$. In other words, this means that $\Gamma_i \wedge \delta_E$ is $\mathcal{T}_i$-satisfiable by a $\mathcal{T}_i$-model of cardinality k. Hence, we can apply Theorem 3.6, obtaining a $\mathcal{T}$-model satisfying Γ. □

4.2 Shiny theories

In this section, we analyze a combination method for the union of a shiny theory and an arbitrary theory presented by Tinelli and Zarba, in [14]. Despite shininess being a stronger notion than stable infiniteness, this way we are able to combine shiny theories with any first-order theory, only requiring they have disjoint signatures.

Definition 4.6 (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 $\kappa \geq |\mathsf{dom}(\mathcal{A})|$ there exists a $\mathcal{T}$-model $\mathcal{B}$ satisfying φ such that $|\mathsf{dom}(\mathcal{B})| = \kappa$.

Definition 4.7 (Shininess, [14])**.** A theory is *shiny* whenever it is smooth, stably finite and its $\mathsf{mincard}$ 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 [14].

The following procedure describes how to decide the satisfiability of a quantifier-free formula in the union of a shiny theory and an arbitrary theory.

Algorithm 3 — Nelson-Oppen algorithm for $\mathcal{T}_1$ arbitrary and $\mathcal{T}_2$ shiny
Input: $\Gamma = \Gamma_1 \wedge \Gamma_2 \wedge \delta_E$, where Γ is a quantifier-free satisfiable formula over Σ
Output: $\mathsf{Sat}_{\mathcal{T}}(\Gamma)$, where $\mathcal{T} = \mathcal{T}_1 \oplus \mathcal{T}_2$

```
1: if Sat_{T2}(Γ2 ∧ δE) == 0
2:     then return 0
3:     else N = mincard_{T2}(Γ2 ∧ δE)
4: if Sat_{T1}(Γ1 ∧ δE ∧ γN) == 0
5:     then return 0
6:     else return 1
```

Observation: Algorithm 3 always terminates since functions $\mathsf{Sat}_{\mathcal{T}_i}$ and $\mathsf{mincard}_{\mathcal{T}_2}$ are computable.

Proposition 4.8. *If the purified quantifier-free formula Γ is $\mathcal{T}$-satisfiable then Algorithm 3 returns 1.*

Proof. Let $\mathcal{A}$ be a $\mathcal{T}$-model satisfying Γ. Then, the reduct of $\mathcal{A}$ along Σ_2 satisfies $\Gamma_2 \wedge \delta_E$ and hence, the procedure does not enter line 2 and assigns to N the value of $\mathsf{mincard}_{\mathcal{T}_2}(\Gamma_2 \wedge \delta_E)$. By the definition of $\mathsf{mincard}$, we have that $N \leq |\mathsf{dom}(\mathcal{A})|$, which implies that the reduct of $\mathcal{A}$ along Σ_1 satisfies γ_N, and hence $\mathcal{A}|_{\Sigma_1}$ satisfies $\Gamma_1 \wedge \delta_E \wedge \gamma_N$. Therefore, the procedure does not enter line 5 and returns 1 in line 6. □

Proposition 4.9. *If the Algorithm 3 returns 1 for a purified quantifier-free formula Γ then Γ is $\mathcal{T}$-satisfiable.*

Proof. If the algorithm returns 1, then this means that $\Gamma_2 \wedge \delta_E$ is $\mathcal{T}_2$-satisfiable and that $\Gamma_1 \wedge \delta_E \wedge \gamma_N$ is $\mathcal{T}_1$-satisfiable. Therefore, let $\mathcal{A}_1$ be a $\mathcal{T}_1$-model of $\Gamma_1 \wedge \delta_E \wedge \gamma_N$ and $\mathcal{A}_2$ be a $\mathcal{T}_2$-model of $\Gamma_2 \wedge \delta_E$ with cardinality $N = \mathsf{mincard}_{\mathcal{T}_2}(\Gamma_2 \wedge \delta_E)$. By definition of γ_N, we have that $|\mathsf{dom}(\mathcal{A}_1)| \geq N$. Using the smoothness of $\mathcal{T}_2$, we can assume that $|\mathsf{dom}(\mathcal{A}_2)| = |\mathsf{dom}(\mathcal{A}_1)|$. With this set, we can apply Theorem 3.6 obtaining a $\mathcal{T}$-model satisfying Γ. □

From these results, we obtain the Nelson-Oppen combination theorem for the union of a shiny and an arbitrary theory.

Theorem 4.10 ([14]). *Let $\mathcal{T}_i$ be a Σ_i-theory for $i = 1, 2$ such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Let Γ_i be a conjunction of Σ_i literals for $i = 1, 2$. Assume that $\mathcal{T}_2$ is shiny. Then the following statements are equivalent:*

1. *$\Gamma_1 \wedge \Gamma_2$ is $\mathcal{T}_1 \oplus \mathcal{T}_2$ satisfiable.*
2. *There exists an arrangement δ_E^V such that $\Gamma_1 \wedge \delta_E^V \wedge \gamma_\kappa$ is $\mathcal{T}_1$-satisfiable and $\Gamma_2 \wedge \delta_E^V$ is $\mathcal{T}_2$-satisfiable, for $V = \mathsf{vars}(\Gamma_1) \cap \mathsf{vars}(\Gamma_2)$ and $\kappa = \mathsf{mincard}_{\mathcal{T}_2}(\Gamma_2 \wedge \delta_E^V)$.*

We will now return to Example 3.2 from Chapter 3 and show that by using the combination method for a shiny with an arbitrary theory we obtain a correct answer.

Example 4.1. *Recall, from Example 3.2, that after purification we obtained that $\Gamma_1 := f(x) \not\cong f(y)$ and $\Gamma_2 := g(x) \not\cong g(z) \wedge g(y) \not\cong g(z)$. In this new method, and following Algorithm 3, since the shared variables between the two formulas is the set $s = \{x, y\}$ we now need to check the satisfiability of Γ_2 with the arrangements over s, which are $x \cong y$ and $x \not\cong y$.*

- *Considering $x \cong y$, we have that $\Gamma_2 \wedge x \cong y$ is $\mathcal{T}_2$-satisfiable. Also, we can easily deduce that its smallest model has cardinality two. Then, we need to check whether $\Gamma_1 \wedge x \cong y \wedge \gamma_2$ is satisfiable in $\mathcal{T}_1$. This is not the case, directly from the fact that $\Gamma_1 \wedge x \cong y$ is not $\mathcal{T}_1$-satisfiable.*
- *Considering $x \not\cong y$, we have that $\Gamma_2 \wedge x \not\cong y$ is $\mathcal{T}_2$-satisfiable. Also, we can easily deduce that its smallest model has cardinality three. Then, we need to check whether $\Gamma_1 \wedge x \cong y \wedge \gamma_3$ is satisfiable in $\mathcal{T}_1$. It is the case that $\Gamma_1 \wedge x \cong y$ is $\mathcal{T}_1$-satisfiable, however γ_3 is not $\mathcal{T}_1$-satisfiable since $\mathcal{T}_1$ only admits models with cardinality at most two, and γ_3 requires, by definition, a model of cardinality at least three to be satisfiable.*

Therefore, we conclude that φ is not $\mathcal{T}_1 \oplus \mathcal{T}_2$-satisfiable.

4.3 Computability of the mincard function

In this section we study the computability of the mincard function and provide two different sets of conditions on the underlying theory under which the mincard function is computable.

4.3.1 Universal theories

Here we show that a stably finite universal theory with a decidable quantifier-free satisfiability problem has a computable mincard function. To prove this, we first need to introduce several notions such as *embedding* and *diagram*.

Definition 4.11 (Embedding). Given two interpretations $\mathcal{A}$ and $\mathcal{A}'$ over the same signature, we say that a map $h : \mathsf{dom}(\mathcal{A}) \to \mathsf{dom}(\mathcal{A}')$ is an *embedding* from $\mathcal{A}$ to $\mathcal{A}'$, written $h : \mathcal{A} \to \mathcal{A}'$, if it is injective and satisfies

- $h(f^F(d_1, \ldots, d_n)) = f^{F'}(h(d_1), \ldots, h(d_n))$;
- $p^P(d_1, \ldots, d_n) = p^{P'}(h(d_1), \ldots, h(d_n))$,

for all function and predicate symbols from the underlying signature.

Lemma 4.12. *Let $h : \mathcal{A} \to \mathcal{A}'$ be an embedding and ρ be an assignment over $\mathcal{A}$. Then, for every term t,*

$$h([\![t]\!]^{\mathcal{A}\ \rho}) = [\![t]\!]^{\mathcal{A}'\ h\circ\rho}.$$

Proof. The proof follows by induction on the structure of the term. The base case is when t is a variable x or a constant c. Then,

$$\begin{aligned} h([\![x]\!]^{\mathcal{A}\ \rho}) &= h(\rho(x)) \\ &= [\![x]\!]^{\mathcal{A}'\ h\circ\rho} \end{aligned}$$

or

$$\begin{aligned} h([\![c]\!]^{\mathcal{A}\ \rho}) &= h(c^F) \\ &= c^{F'} \\ &= [\![c]\!]^{\mathcal{A}'\ h\circ\rho} \end{aligned}$$

If t is $f(t_1, \ldots, t_n)$ then we have that

$$\begin{aligned} h([\![f(t_1, \ldots, t_n)]\!]^{\mathcal{A}\ \rho}) &= h(f^F([\![t_1]\!]^{\mathcal{A}\ \rho}, \ldots, [\![t_n]\!]^{\mathcal{A}\ \rho})) \\ &= f^{F'}(h([\![t_1]\!]^{\mathcal{A}\ \rho}), \ldots, h([\![t_n]\!]^{\mathcal{A}\ \rho})) \\ &= f^{F'}([\![t_1]\!]^{\mathcal{A}'\ h\circ\rho}, \ldots, [\![t_n]\!]^{\mathcal{A}'\ h\circ\rho}) \end{aligned}$$

□

Proposition 4.13. *Let $h : \mathcal{A} \to \mathcal{A}'$ be an embedding. Then, for each $\varphi \in \mathsf{QF}(\Sigma)$ and assignment ρ over $\mathcal{A}$,*

1. *$\mathcal{A}\ \rho \Vdash \varphi$ iff $\mathcal{A}'\ h \circ \rho \Vdash \varphi$;*
2. *$\mathcal{A}\ \rho \Vdash \forall x_1 \ldots \forall x_n\ \varphi$ when $\mathcal{A}'\ h \circ \rho \Vdash \forall x_1 \ldots \forall x_n\ \varphi$;*
3. *$\mathcal{A} \Vdash \forall\ \varphi$ when $\mathcal{A}' \Vdash \forall\ \varphi$.*

Proof. 1. The proof is done by induction on the structure of the formula φ. If φ is $p(t_1, \ldots, t_n)$ then

$$\begin{aligned} \mathcal{A}\ \rho \Vdash p(t_1, \ldots, t_n) \text{ iff } & p^P([\![t_1]\!]^{\mathcal{A}\ \rho}, \ldots, [\![t_n]\!]^{\mathcal{A}\ \rho}) = 1 \\ \text{iff } & p^{P'}([\![t_1]\!]^{\mathcal{A}'\ h\circ\rho}, \ldots, [\![t_n]\!]^{\mathcal{A}'\ h\circ\rho}) = 1, \text{ since } h \text{ is an embedding} \\ \text{iff } & \mathcal{A}'\ h \circ \rho \Vdash p(t_1, \ldots, t_n) \end{aligned}$$

Now, consider φ as $(\neg\psi)$. Then,

$$\begin{aligned}\mathcal{A}\ \rho \Vdash (\neg\psi) &\text{ iff } \mathcal{A}\ \rho \nVdash \psi\\ &\text{iff } \mathcal{A}'\ h\circ\rho \nVdash \psi\\ &\text{iff } \mathcal{A}'\ h\circ\rho \Vdash (\neg\psi)\end{aligned}$$

Finally, if φ is $(\psi_1 \to \psi_2)$. Then,

$$\begin{aligned}\mathcal{A}\ \rho \Vdash (\psi_1 \to \psi_2) &\text{ iff } \mathcal{A}\ \rho \nVdash \psi_1 \text{ or } \mathcal{A}\ \rho \Vdash \psi_2\\ &\text{iff } \mathcal{A}'\ h\circ\rho \nVdash \psi_1 \text{ or } \mathcal{A}'\ h\circ\rho \Vdash \psi_2\\ &\text{iff } \mathcal{A}'\ h\circ\rho \Vdash (\psi_1 \to \psi_2)\end{aligned}$$

2. Assume that $\mathcal{A}'\ h\circ\rho \Vdash \forall x_1 \ldots \forall x_n\ \varphi$ holds. The proof follows by induction on n that $\mathcal{A}\ \rho \Vdash \forall x_1 \ldots \forall x_n\ \varphi$. The base case holds from 1. Now, let σ be a x_1-equivalent assignment to ρ. Then, $\mathcal{A}'\ h\circ\sigma \Vdash \forall x_2 \ldots \forall x_n\ \varphi$ since $h\circ\rho \equiv_{x_1} h\circ\sigma$ and by definition of satisfiability of a universal quantifier. By induction hypothesis we have that $\mathcal{A}\ \sigma \Vdash \forall x_2 \ldots \forall x_n\ \varphi$. Again, by the definition of satisfiability of a universal quantifier we obtain $\mathcal{A}\ \rho \Vdash \forall x_1 \ldots \forall x_n\ \varphi$.

3. Is a direct consequence of 2.

□

Definition 4.14 (Universal formula)**.** We say that a formula φ is a *universal formula* if it is of the form $\forall x_1 \ldots \forall x_n\ \phi$ where $n \geq 0$ and ϕ is quantifier-free.

Definition 4.15 (Universal theory)**.** We say that a theory is *universal* if it is axiomatized exclusively by universal formulas.

Lemma 4.16. *Let $\mathcal{T}$ be a universal theory over Σ, $\mathcal{M}$ a $\mathcal{T}$-model and $\mathcal{A}$ a generic interpretation. If there exists an embedding $h : \mathcal{A} \to \mathcal{M}$ then $\mathcal{A}$ is also a model of $\mathcal{T}$.*

Proof. This is a direct consequence of Proposition 4.13 and the structure of the sentences in a universal theory. □

Definition 4.17 (Simple diagrams)**.** Given a Σ-interpretation $\mathcal{A} = \langle D, \_^F, \_^P\rangle$ and an assignment ρ over $\mathcal{A}$, define Σ^+ as the signature Σ enriched by a new constant symbol $\bar{d}$ for each $d \in D$. The *simple diagram of* $\mathcal{A}$, denoted by $\Delta(\mathcal{A})$, is the set

$$\left\{ [\varphi]^{x_1,\ldots,x_n}_{\rho(\bar{x_1}),\ldots,\rho(\bar{x_n})} : \varphi \in \mathsf{QF}(\Sigma), \mathsf{fvars}(\varphi) = \{x_1, \ldots, x_n\}, \mathcal{A}\ \rho \Vdash \varphi \right\}.$$

Observation: The extension of $\mathcal{A}$ to Σ^+, denoted by $\bar{\mathcal{A}}$, such that $\bar{\mathcal{A}}|_\Sigma = \mathcal{A}$ and $[\![\bar{d}]\!]^{\bar{\mathcal{A}}}_{\Sigma^+} = d$ for all $d \in \mathsf{dom}(\mathcal{A})$ satisfies $\Delta(\mathcal{A})$ by construction.

With these definitions and preliminary results, we are now able to prove the main proposition of the section. For this, consider Algorithm 4.

Algorithm 4 — $\mathsf{mincard}^{\mathsf{Sat}}$ algorithm, [14]
Input: Γ, where Γ is a quantifier-free satisfiable conjunction of literals over Σ
Output: k, where k is the cardinality of the smallest $\mathcal{T}$-model of Γ
Requires: access to $\mathsf{Sat}_{\mathcal{T}}$

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

Proposition 4.18 ([14])**.** *Let $\mathcal{T}$ be a stably finite universal theory with a decidable quantifier-free satisfiability problem. Then, the* $\mathsf{mincard}_{\mathcal{T}}$ *function is computed by Algorithm 4.*

Proof. Let Γ be a satisfiable conjunction of literals. Since $\mathcal{T}$ is stably finite, by hypothesis we have that there exists a $\mathcal{T}$-model $\mathcal{A}$ and an assignment ρ that satisfy Γ and such that $|\mathsf{dom}(\mathcal{A})| = k$ for some positive integer k. By construction of $\Delta(\mathcal{A})$, we have that $\Delta(\mathcal{A}) \wedge \Gamma$ is satisfied by $\bar{\mathcal{A}}$ and ρ and that $\bar{\mathcal{A}}$ is also a $\mathcal{T}$-model. We are therefore guaranteed that the procedure terminates given a quantifier-free satisfiable conjunction of literals.

Regarding the correctness of the procedure, assume that the procedure outputs k. Then there is a $\mathcal{T}$-model $\mathcal{B}$ that satisfies $\Delta(\mathcal{A}) \wedge \Gamma$ such that $|\mathsf{dom}(\mathcal{A})| = k$. Consider now the function $h : \mathcal{A} \to \mathcal{B}$ defined by $h(d) = [\![\bar{d}]\!]^{\mathcal{B}}_{\Sigma^+}$ for each d in the domain of $\mathcal{A}$. We show that h is an embedding:

- h is injective: let $d_1, d_2 \in \mathsf{dom}(\mathcal{A})$ be such that $d_1 \neq d_2$. Then, considering ρ such that $\rho(x_1) = d_1$ and $\rho(x_2) = d_2$ we have that $\mathcal{A}\ \rho \Vdash \neg(x_1 \cong x_2)$, and hence $\neg(\bar{d_1} \cong \bar{d_2}) \in \Delta(\mathcal{A})$. Therefore since $\mathcal{B}$ satisfies the diagram of $\mathcal{A}$, we have that $\mathcal{B} \Vdash \neg(\bar{d_1} \cong \bar{d_2})$ and so

$$h(d_1) = [\![\bar{d_1}]\!]^{\mathcal{B}}_{\Sigma^+} \neq [\![\bar{d_2}]\!]^{\mathcal{B}}_{\Sigma^+} = h(d_2).$$

- $h(f^F(d_1, \ldots, d_n)) = f^{F'}(h(d_1), \ldots, h(d_n))$: let ρ be such that $\rho(x_i) = d_i$ and $\rho(x) = f^F(d_1, \ldots, d_n)$. Then, $\mathcal{A}\ \rho \Vdash f(x_1, \ldots, x_n) \cong x$, and hence $f(\bar{d_1}, \ldots, \bar{d_n}) \cong f^F(d_1, \bar{\ldots}, d_n) \in \Delta(\mathcal{A})$. Therefore, $\mathcal{B} \Vdash f(\bar{d_1}, \ldots, \bar{d_n}) \cong f^F(d_1, \bar{\ldots}, d_n)$ and so

$$\begin{aligned}
[\![f(\bar{d_1}, \ldots, \bar{d_n})]\!]^{\mathcal{B}} &= [\![f^F(d_1, \bar{\ldots}, d_n)]\!]^{\mathcal{B}} \\
f^{F'}([\![\bar{d_1}]\!]^{\mathcal{B}}, \ldots, [\![\bar{d_n}]\!]^{\mathcal{B}}) &= [\![f^F(d_1, \bar{\ldots}, d_n)]\!]^{\mathcal{B}} \\
f^{F'}(h(d_1), \ldots, h(d_n)) &= h(f^F(d_1, \ldots, d_n))
\end{aligned}$$

- $p^P(d_1, \ldots, d_n) = p^{P'}(h(d_1), \ldots, h(d_n))$: first consider the case in which $p^P(d_1, \ldots, d_n) = 1$. Considering ρ as $\rho(x_i) = d_i$ we have that $\mathcal{A}\ \rho \Vdash p(x_1, \ldots, x_n)$ and so $p(\bar{d_1}, \ldots, \bar{d_n}) \in \Delta(\mathcal{A})$. Therefore,

$\mathcal{B} \Vdash p(\bar{d_1}, \ldots, \bar{d_n})$ and so

$$p^{P'}([\![\bar{d_1}]\!]^{\mathcal{B}}, \ldots, [\![\bar{d_n}]\!]^{\mathcal{B}}) = 1$$
$$\text{iff } p^{P'}(h(d_1), \ldots, h(d_n)) = 1.$$

Now consider the case in which $p^P(d_1, \ldots, d_n) = 0$. Then, considering ρ as $\rho(x_i) = d_i$ we have that $\mathcal{A}\ \rho \Vdash \neg p(x_1, \ldots, x_n)$ and so $\neg p(\bar{d_1}, \ldots, \bar{d_n}) \in \Delta(\mathcal{A})$. Therefore, $\mathcal{B} \Vdash \neg p(\bar{d_1}, \ldots, \bar{d_n})$ and so

$$p^{P'}([\![\bar{d_1}]\!]^{\mathcal{B}}, \ldots, [\![\bar{d_n}]\!]^{\mathcal{B}}) = 0$$
$$\text{iff } p^{P'}(h(d_1), \ldots, h(d_n)) = 0.$$

Recalling, we have that there is a $\mathcal{T}$-model $\mathcal{B}$ that satisfies $\Delta(\mathcal{A}) \wedge \Gamma$ such that $|\mathsf{dom}(\mathcal{A})| = k$ and an embedding $h : \mathcal{A} \to \mathcal{B}$. By Lemma 4.16, considering that $\mathcal{T} \cup \Delta(\mathcal{A}) \cup \Gamma$ is a universal theory (since $\mathcal{T}$ is universal by hypothesis and we can consider the variables of $\Delta(\mathcal{A}) \cup \Gamma$ as constants) we have that $\mathcal{A}$ also satisfies $\mathcal{T} \cup \Delta(\mathcal{A}) \cup \Gamma$. From this we obtain that $\mathsf{mincard}(\Gamma) \leq k$ since $|\mathsf{dom}(\mathcal{A})| = k$. To see why $\mathsf{mincard}(\Gamma) = k$, assume by contradiction that $\mathsf{mincard}(\Gamma) < k$. Then there exists a $\mathcal{T}$-model $\mathcal{C}$ with cardinality $q < k$ that satisfies Γ. But then, $\mathcal{C}$ also satisfies $\mathcal{T} \cup \Delta(\mathcal{C}) \cup \Gamma$ and so the procedure should have stopped at the q-th iteration. □

4.3.2 Other theories

In this section, we show that a stably finite theory with a rather weak "decidability" property gives also a sufficient condition for the mincard function to be computable. The idea behind this is that, in a stably finite theory, we are sure that a satisfiable formula will have a model with finite cardinality. In order to find a model with the smallest possible cardinality, we enumerate finite interpretations and need to verify whether (i) it is a model of the theory; (ii) it satisfies the formula. Since we are only considering finite interpretations and finite formulas, step (ii) is obviously computable. However, it might not be decidable to verify if an arbitrary finite interpretation is a model of the theory. To put it otherwise, provided that it is decidable to check if a finite interpretation is a model of the theory at hand, then we are able to compute the mincard function. We show this result in the following proposition.

Proposition 4.19. *Let Σ be a finite signature and $\mathcal{T}$ a Σ-theory. Assume that given a finite Σ-interpretation $\mathcal{A}$, it is decidable to check whether $\mathcal{A}$ is a $\mathcal{T}$-model. Then, if $\mathcal{T}$ is stably finite then the* mincard *function is computable.*

Proof. Consider the Algorithm 5 for computing the mincard function.

Regarding the termination of the algorithm, since we are considering a stably finite theory, we are guaranteed that there exists a positive integer p such that there is a model of the theory with cardinality p that satisfies the given formula. Furthermore, we can create all non-isomorphic finite interpretations (since the signature is finite, and there is a finite number of ways of defining the denotations of the function and predicate symbols) and check if it is a model of the theory since, by hypothesis, it is

Algorithm 5 — mincard algorithm
Input: φ, where φ is a quantifier-free satisfiable formula over Σ
Output: k, where k is the cardinality of the smallest $\mathcal{T}$-model of φ

```
1: k = 0
2: while true do
3:     k = k + 1
4:     for all non-isomorphic T-models A s.t. |dom(A)| = k and ρ over A do
5:         if A ρ ⊩ φ then return k
6:     end for
7: end while
```

decidable to check if a finite interpretation is a model of the theory.

Considering the correctness of the procedure, if the algorithm returns m, for some $\mathcal{T}$-model $\mathcal{A}$, then this means that for all models with smaller cardinality than m, none satisfied φ, from what follows that m is the cardinality of the smallest model of φ. □

Regarding the imposed condition on the theory, one might wonder whether this requirement is too strong. We believe this is not the case, since, for example, all finitely axiomatized theories are included, independently of the structure of the axioms (the theory is not imposed to be universal). However, it is left open whether or not there exist stably finite theories in which checking if a finite interpretation is a model is not decidable.

4.4 Complexity of the mincard function

In this section we relate the complexity of computing the mincard function to a colorability problem from graph theory. Specifically, we provide a polynomial time reduction from an NP-complete problem to a problem similar to computing the mincard function. For this, consider the following two problems.

k-cardinality problem: Given a set of satisfiable quantifier-free formulas Γ and $k \in \mathbb{N}$, is there a model of Γ with cardinality k?

k-colorability problem: Given a undirected finite graph $\mathcal{G} = \langle V, E\rangle$, we say that $\mathcal{G}$ is *k-colorable* if there exists a map $\chi : V \to \{1, \ldots, k\}$ that assigns different colours to adjacent vertices. This problem is known to be in NP-complete, [5].

Proposition 4.20. *Let $\mathcal{G} = \langle V, E\rangle$ be a finite undirected graph. Define Γ as the set $\{u \not\cong v : u, v \in V$ and $(u, v) \in E\}$. Then Γ is satisfied by a model of cardinality k iff $\mathcal{G}$ is k-colorable.*

Proof. $(\rightarrow)$ Let $\mathcal{A}$ and ρ be the model and assignment that satisfy Γ. For each $v \in \mathsf{vars}(\Gamma)$, if $\rho(v) = a_i \in \mathsf{dom}(\mathcal{A})$ then set $\chi(v) = i$. This way we have that for every $u \not\cong v \in \Gamma$, $\chi(u) \neq \chi(v)$, making $\chi : V \to \{1, \ldots, k\}$ a k-coloration of $\mathcal{G}$.

$(\leftarrow)$ Let $\chi : V \to \{1, \ldots, k\}$ be a k-coloration of $\mathcal{G}$. Define $\mathcal{A} = \langle\{1, \ldots, k\}, \emptyset, \emptyset\rangle$ and an assignment ρ defined by $\rho(v) = \chi(v)$. Then $\mathcal{A}\ \rho \Vdash \Gamma$. □

Observation: Notice that the translation $\mathcal{G} \mapsto \Gamma$ can be made polynomially on the size of $\mathcal{G}$.

The result just proved implies that the k-cardinality problem is NP-hard since there is a polynomial-time reduction from a k-colorability solution for a graph $\mathcal{G}$ to a k-cardinality solution for a set of formulas Γ

induced by $\mathcal{G}$ and the k-colorability problem is NP-complete. We now only need to relate the k-cardinality problem to computing the mincard function, which can be done quite directly.

Proposition 4.21. *The problem of computing the* mincard *function for the theory of equality over the empty signature is* NP $-$ hard*.*

Proof. We need to polynomially reduce the k-cardinality to computing the mincard function. Suppose we want to check the k-cardinality problem for a set of literals Γ. Then, compute $m = \text{mincard}(\Gamma)$. There are two cases:

- $m \leq k$ and then, by the smoothness of the theory of equality, we obtain that Γ has a model with cardinality k;
- $m > k$ and then by the definition of mincard we have that there are no models of Γ with cardinality k.

□

In this section we showed that computing the mincard function is an inherently hard problem to solve. This was one of the problems that motivated the search for a notion similar to shininess (in the sense that allowed combination with an arbitrary theory) but did not require the computation of the mincard function. This will be the topic discussed in the next chapter, where we present the notion of *polite theories*.

4.5 Summary of the chapter

In this chapter we focused on the "migration" of the standard Nelson-Oppen method to different classes of theories. The first method presented concerns the combination of satisfiability procedures for theories with only finite models and with computable mincard functions. We proceeded to present the combination procedure for an arbitrary and a shiny theory. This version of the Nelson-Oppen method is of huge importance, since it was the first method that could be applied to the combination of an arbitrary theory with a restricted theory. However, shiny theories require the computability of the mincard function. We also present two different classes of theories under which the mincard function is computable. Also, the theoretical complexity of this function is studied. The results in this chapter mainly follow the works of Tinelli and Zarba [14] and of Ranise, Ringeissen and Zarba [9].

5 – Polite theories

In this chapter we introduce the notions of *polite* and *strongly polite* theories. The politeness property was introduced by Ranise, Ringeissen and Zarba in [9] as an attempt to solve some issues with the shininess notion introduced in the previous chapter, namely the inherent hardness of computing the mincard function. Polite theories must, however, be equipped with a witness function. Similarly to the shininess notion, the combination theorem would be valid when considering the union of a polite theory and an arbitrary one. However, in [6], Jovanović and Barrett showed that the politeness notion introduced in [9] is not strong enough and allows witness functions that make the combination theorem false. Because of this, they introduce a stronger notion of politeness, which we call *strong politeness*.

5.1 Polite theories

Definition 5.1 (Finite witnessability, [9])**.** 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 Σ-formula φ

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

If a function satisfies the above properties for a theory $\mathcal{T}$ to be finitely witnessable, we say that it is a *witness function for* $\mathcal{T}$.

Definition 5.2 (Politeness, [9])**.** A theory is *polite* whenever it is smooth and finitely witnessable.

Similarly to the extension of the Nelson-Oppen result for a shiny and arbitrary theory, Ranise, Ringeissen and Zarba in [9] proposed the polite version of the Nelson-Oppen combination theorem. However, as we will see in the sequel, this result does not hold with the politeness notion as is.

Proposal 5.3. *Let $\mathcal{T}_i$ be a Σ_i-theory for $i = 1, 2$ such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Let Γ_i be a conjunction of Σ_i literals for $i = 1, 2$. Assume that $\mathcal{T}_2$ is polite and that* witness *is a witness function for $\mathcal{T}_2$. Then the following statements are equivalent:*

1. $\Gamma_1 \wedge \Gamma_2$ *is $\mathcal{T}_1 \oplus \mathcal{T}_2$ satisfiable.*

2. *There exists an arrangement* δ_E^V *such that* $\Gamma_1 \wedge \delta_E^V$ *is* $\mathcal{T}_1$*-satisfiable and* $\mathsf{witness}_{\mathcal{T}_2}(\Gamma_2) \wedge \delta_E^V$ *is* $\mathcal{T}_2$*-satisfiable, for* $V = \mathsf{vars}(\mathsf{witness}(\Gamma_2))$.

As mentioned previously, the politeness notion allows witness functions that contradict the combination theorem. The following example, from [6], will make this clear.

Example 5.1 ([6])**.** *Consider two theories* $\mathcal{T}_1, \mathcal{T}_2$ *over the empty signature such that* $\mathcal{T}_1$ *is axiomatized by* $\forall x \forall y \ (x \cong y)$ *(meaning that if a model satisfies* $\mathcal{T}_1$ *then it has cardinality 1) and* $\mathcal{T}_2$ *axiomatized by* $\exists x \exists y \ \neg(x \cong y)$ *(meaning that if a model satisfies* $\mathcal{T}_2$ *then it has cardinality at least 2). We are trying to decide the satisfiability of* $\varphi := (x \cong x)$ *in the union of* $\mathcal{T}_1$ *and* $\mathcal{T}_2$*. Since the union of these theories has no models that satisfy it, we conclude that* φ *will not be satisfiable.*

Observe that $\mathcal{T}_2$ *is clearly smooth – since its signature is empty, if a formula* φ *is satisfiable, then we can simply add elements to the domain of this model to obtain the desired cardinality. We claim that*

$$\mathsf{witness}(\varphi) := \varphi \wedge w_1 \cong w_1 \wedge w_2 \cong w_2$$

where w_1, w_2 *are fresh variables, is a witness function for* $\mathcal{T}_2$*. Let* φ *be a quantifier-free conjunction of literals. Clearly,* φ *and* $\exists w_1 \exists w_2 \ \mathsf{witness}(\varphi)$ *are* $\mathcal{T}_2$*-equivalent.*

For the second finite witnessability property, if $\exists w_1 \exists w_2 \ \varphi \wedge w_1 \cong w_1 \wedge w_2 \cong w_2$ *is satisfiable, we need to provide a* $\mathcal{T}$*-model* $\mathcal{I}$ *and assignment* ρ *such that* $\mathcal{I} \ \rho \Vdash \mathsf{witness}(\varphi)$ *and* $\mathsf{dom}(\mathcal{I}) = [\![\mathsf{vars}(\mathsf{witness}(\varphi))]\!]^\rho$*. If* $\exists w_1 \exists w_2 \ \mathsf{witness}(\varphi)$ *is satisfiable, then there is a* $\mathcal{T}$*-model* $\mathcal{B}$ *and an assignment* σ *such that* $\mathcal{B} \ \sigma \Vdash \mathsf{witness}(\varphi)$*. The desired interpretation structure and assignment must satisfy* $\mathsf{dom}(\mathcal{I}) = [\![\mathsf{vars}(\mathsf{witness}(\varphi))]\!]^\rho$*. With this in mind, define* $\mathsf{dom}(\mathcal{I})$ *as* $[\![\mathsf{vars}(\mathsf{witness}(\varphi))]\!]^\sigma$ *and* $\rho = \sigma$*. The model* $\mathcal{I}$ *obviously satisfies* $\exists w_1, w_2 \ \mathsf{witness}(\varphi)$ *but it may happen that* $[\![\mathsf{vars}(\mathsf{witness}(\varphi))]\!]^\sigma$ *contains only one element. However, if this happens we can modify* σ *so that* $\sigma(w_1) \neq \sigma(w_2)$ *while still preserving the satisfiability of* φ*. This way, we guarantee that* $[\![\mathsf{vars}(\mathsf{witness}(\varphi))]\!]^\sigma$ *has at least two elements and therefore* $\mathcal{I}$ *and* ρ *are such that* $\mathcal{I} \ \rho \Vdash \mathsf{witness}(\varphi)$ *and* $\mathsf{dom}(\mathcal{I}) = [\![\mathsf{vars}(\mathsf{witness}(\varphi))]\!]^\rho$*. We therefore conclude that* $\mathcal{T}_2$ *is polite.*

Now, let us apply the proposed combination theorem to decide the satisfiability of $\varphi := (x \cong x)$ *in the union of* $\mathcal{T}_1$ *and* $\mathcal{T}_2$*. Let* $\Gamma_1 = \mathsf{true}$*,* $\Gamma_2 = \varphi$ *and* $V = \mathsf{vars}(\mathsf{witness}(\Gamma_2)) = \{x, w_1, w_2\}$*. We now would like to check if there is an arrangement of* δ_E^V *such that* $\Gamma_1 \wedge \delta_E^V$ *is* $\mathcal{T}_1$*-satisfiable and* $\mathsf{witness}(\Gamma_2) \wedge \delta_E^V$ *is* $\mathcal{T}_2$*-satisfiable. By letting* $\delta_E^V := x \cong w_1 \wedge x \cong w_2 \wedge w_1 \cong w_2$*, we have that* $\Gamma_1 \wedge \delta_E^V$ *is clearly* $\mathcal{T}_1$*-satisfiable and* $\mathsf{witness}(\Gamma_2) \wedge \delta_E^V$ *is* $\mathcal{T}_2$*-satisfiable. By this combination method, we would conclude that* φ *is satisfiable in* $\mathcal{T}_1 \oplus \mathcal{T}_2$*, but this is absurd since this theory has no models.*

5.2 Strongly polite theories

In light of the above counterexample, Jovanović and Barrett proposed a new politeness notion in [6], which we call *strong politeness* in this thesis. As seen in the example, the problem with the previous definition was that it allowed witness functions that were not strong enough. Due to this, Jovanović and Barrett proposed the following definitions.

Definition 5.4 (Strong finite witnessability, [6])**.** We say that a theory $\mathcal{T}$ over a signature Σ is *strongly finitely witnessable* if there exists a computable function $\text{s-witness} : \text{QF}(\Sigma) \to \text{QF}(\Sigma)$ such that for every quantifier-free formula φ the following conditions hold:

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

A function satisfying the above properties is called a *strong witness function for* $\mathcal{T}$.

Definition 5.5 (Strong politeness, [6])**.** A theory is *strongly polite* whenever it is smooth and strongly finitely witnessable.

With this new definition, replacing the politeness definition by strong politeness in the theorem proposal, we are now able to prove it.

Theorem 5.6 ([6])**.** *Let $\mathcal{T}_i$ be a Σ_i-theory for $i = 1, 2$ such that $\Sigma_1 \cap \Sigma_2 = \emptyset$. Let Γ_i be a conjunction of Σ_i literals for $i = 1, 2$. Assume that $\mathcal{T}_2$ strongly polite and that* s-witness *is a strong witness function for $\mathcal{T}_2$. Then the following statements are equivalent:*

1. *$\Gamma_1 \wedge \Gamma_2$ is $\mathcal{T}_1 \oplus \mathcal{T}_2$ satisfiable.*
2. *There exists an arrangement δ_E^V such that $\Gamma_1 \wedge \delta_E^V$ is $\mathcal{T}_1$-satisfiable and $\text{s-witness}(\Gamma_2) \wedge \delta_E^V$ is $\mathcal{T}_2$-satisfiable, for $V = \text{vars}(\text{s-witness}(\Gamma_2))$.*

Proof. ($\rightarrow$) Assume that $\Gamma_1 \wedge \Gamma_2$ is $\mathcal{T}_1 \oplus \mathcal{T}_2$ satisfiable. By the definition of strong politeness and s-witness being a strong witness function for $\mathcal{T}_2$, we have that $\Gamma_1 \wedge \text{s-witness}(\Gamma_2)$ is also $\mathcal{T}_1 \oplus \mathcal{T}_2$-satisfiable. Hence, let $\mathcal{A}$ be a $\mathcal{T}$-model and ρ an assignment over $\mathcal{A}$ such that $\mathcal{A}\ \rho \Vdash \Gamma_1 \wedge \text{s-witness}(\Gamma_2)$. Then the arrangement formula $\delta_{E_\rho}^V$ induced by $E_\rho = \{(x, y) : x, y \in V \text{ and } \rho(x) = \rho(y)\}$ is satisfied by $\mathcal{A}$ and ρ. Therefore, $\mathcal{A}|_{\Sigma_1}$ is a $\mathcal{T}_1$ model of $\Gamma_1 \wedge \delta_{E_\rho}^V$ and $\mathcal{A}|_{\Sigma_2}$ is a $\mathcal{T}_2$ model of $\text{s-witness}(\Gamma_2) \wedge \delta_{E_\rho}^V$.

($\leftarrow$) Let $\mathcal{A}$ be a $\mathcal{T}_1$-model and ρ an assignment satisfying $\Gamma_1 \wedge \delta_E^V$ and $\mathcal{B}$ be a $\mathcal{T}_2$-model and an assignment σ satisfying $\text{s-witness}(\Gamma_2) \wedge \delta_E^V$. By the strong finite witnessability of $\mathcal{T}_2$, $\mathcal{B}$ may assumed to be such that $\text{dom}(\mathcal{B}) = [\![V]\!]^\sigma$. From this, we have that

$$\begin{aligned} |\text{dom}(\mathcal{B})| &= |[\![V]\!]^{\mathcal{B}\ \sigma}| && \text{since } \text{dom}(\mathcal{B}) = [\![V]\!]^\sigma \\ &= |[\![V]\!]^{\mathcal{A}\ \rho}| && \text{since } \mathcal{A} \text{ and } \mathcal{B} \text{ satisfy } \delta_E^V \\ &\leq |\text{dom}(\mathcal{A})| && \text{since } [\![V]\!]^{\mathcal{A}\ \rho} \subseteq \text{dom}(\mathcal{A}). \end{aligned}$$

By the smoothness of $\mathcal{T}_2$, let $\mathcal{C}$ be a $\mathcal{T}_2$-model and μ an assignment over $\mathcal{C}$ such that $\mathcal{C}\ \mu \Vdash \text{s-witness}(\Gamma_2) \wedge \delta_E^V$ and $|\text{dom}(\mathcal{C})| = |\text{dom}(\mathcal{A})|$. Recapping, we have

- a $\mathcal{T}_1$-model $\mathcal{A}$ and an assignment ρ such that $\mathcal{A}\ \rho \Vdash \Gamma_1 \wedge \delta_E^V$;

- a $\mathcal{T}_2$-model $\mathcal{C}$ and an assignment μ such that $\mathcal{C}\ \rho \Vdash \text{s-witness}(\Gamma_2) \wedge \delta_E^V$;
- $|\text{dom}(\mathcal{C})| = |\text{dom}(\mathcal{A})|$.

By theorem 3.6, we have that there is a $\mathcal{T}_1 \oplus \mathcal{T}_2$-model $\mathcal{D}$ and an assignment τ such that $\mathcal{C}\ \tau \Vdash \Gamma_1 \wedge \text{s-witness}(\Gamma_2) \wedge \delta_E^V$. Since $\exists \vec{w}\ \text{s-witness}(\Gamma_2)$ and Γ_2 are $\mathcal{T}_2$-equivalent, $\mathcal{D}$ and τ satisfies $\Gamma_1 \wedge \Gamma_2$.

□

5.3 Summary of the chapter

In this chapter, following the works by Ranise, Ringeissen and Zarba [9] and Jovanović and Barrett [6], we presented a Nelson-Oppen method to combine satisfiability procedures for an arbitrary theory and a strongly polite theory, mainly motivated by the hardness of computing the mincard function for shiny theories. However, strongly polite theories also require the computation of a s-witness function which may also be as hard to compute as the mincard function. At this point, the study of the relation between shiny, polite and strongly polite theories was needed to evaluate how different these classes of theories are and how they relate to each other. This analysis was firstly performed by Ranise, Ringeissen and Zarba [9] for shiny and polite theories. However, after the issue mentioned in Example 5.1 and the creation of the strong politeness notion, the relation between the two politeness notions and between strong politeness and shininess notions was not studied. This is the objective of the next chapter.

6 – On the equivalence of shininess and politeness

In this chapter we study the relationship between shininess and politeness, between shininess and strong politeness as well as between the two politeness notions. The relationship between shininess and politeness was first analyzed by Ranise, Ringeissen and Zarba in [9]. However, since Jovanović and Barrett in [6] showed that the combination theorem for a polite and an arbitrary theory does not hold (using a witness function), the original politeness notion was rewritten as the strong politeness notion and somewhat forgotten. Because of this, the relationship between the two politeness notions has not been studied. On the other hand, the study of the relationship between the strong politeness notion and shininess was left as an open problem in [6]. We show that a shiny theory with a decidable quantifier-free satisfiability problem is strongly polite. We also show that a strongly polite theory is a polite theory, and using results from [9] and [14], that under each one of two sets of restrictions, the shininess, politeness and strong politeness notions are equivalent (see Figure 6.1 for a global view of the results). From this, we are able to devise a Nelson-Oppen procedure for the combination of a polite and an arbitrary theory (using the fact that we can construct the mincard function and a strong witness function from a witness function).

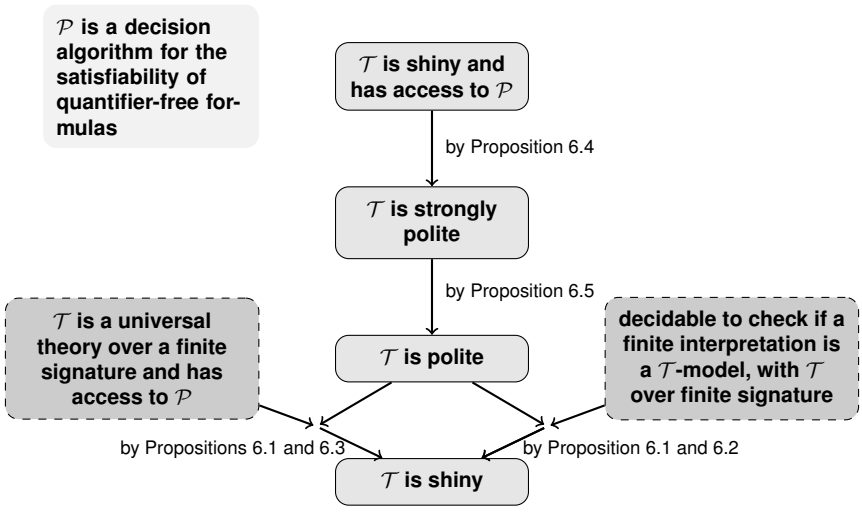

Figure 6.1: Schematic representation of the results in the chapter

6.1 Shininess and politeness

In this section we present results by Ranise, Ringeissen and Zarba from [9] relating the notions of shininess and politeness. We begin by noting that a polite theory is always stably infinite.

Proposition 6.1. *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 $\mathcal{A}$ and an assignment ρ satisfying $\mathsf{witness}(\varphi)$ with $\mathsf{dom}(\mathcal{A}) = [\![\mathsf{vars}(\mathsf{witness}(\varphi))]\!]^{\rho}$. 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. □

Observe that given this result, in order to relate politeness with shininess, we are only left to prove that the mincard function is computable. Capitalizing on results from Chapter 4, in particular Propositions 4.18 and 4.19, we can now prove that under the requirements of the mentioned propositions, a polite theory is in fact shiny.

Proposition 6.2 ([9])**.** *Let Σ be a finite signature and $\mathcal{T}$ a Σ-theory. Assume that given a finite Σ-interpretation $\mathcal{A}$, it is decidable to check whether $\mathcal{A}$ is a $\mathcal{T}$-model. Then, if $\mathcal{T}$ is a polite Σ-theory then $\mathcal{T}$ is shiny and Algorithm 5 computes the* mincard *function.*

Proof. By Proposition 6.1, we obtain that $\mathcal{T}$ is stably finite. Hence, by Proposition 4.19, we have that the mincard function is computed by Algorithm 5. □

Observe that the conditions on the previous proposition are rather weak – for instance, if a theory $\mathcal{T}$ is finitely axiomatized then it is decidable to check if a finite Σ-interpretation is indeed a $\mathcal{T}$-model. However, if it is not decidable to check whether a finite interpretation is a $\mathcal{T}$-model, we will still be able to construct the mincard function, provided that the theory $\mathcal{T}$ is universal. This proposition makes use of a result by Tinelli and Zarba, see [14].

Proposition 6.3. *Let Σ be a finite signature and $\mathcal{T}$ a universal Σ-theory with a decidable quantifier-free satisfiability problem. If $\mathcal{T}$ is polite then it is shiny. Furthermore, Algorithm 4 computes its* mincard *function.*

Proof. By proposition 6.1 we obtain that $\mathcal{T}$ is stably finite. Hence, by Proposition 4.18, since $\mathcal{T}$ a universal Σ-theory with a decidable quantifier-free satisfiability problem and stably finite, we have that the mincard function is computed by Algorithm 4. □

The presented results in this section relate the politeness notion with shininess. We have shown that under two different sets of restrictions a polite theory is shiny. Refer to Figure 6.2 for a schematic representation of these results.

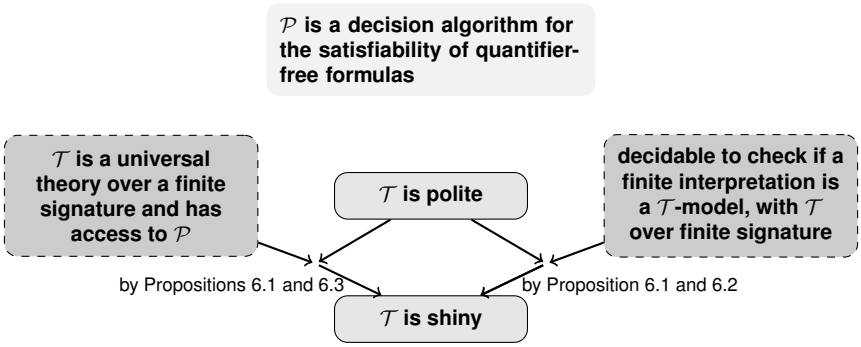

Figure 6.2: Schematic representation of the results in the section

6.2 Shininess and strong politeness

In this section we investigate the relationship between shiny and strongly polite theories. We show that a shiny theory with a decidable quantifier-free satisfiability problem is strongly polite. Furthermore we provide two different sets of conditions under which a strongly polite theory is shiny. These results do not contradict the results by Jovanović and Barrett in [6] stating that the polite theories allow witness functions that disprove the combination theorem. We show that, given some conditions, a polite theory is also strongly polite and what this means is that there is a way to transform a witness function into a strong witness function. Moreover, given the constructive nature of the proofs we were able to design such a procedure.

Proposition 6.4. *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

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

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

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

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 s-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 $\mathsf{vars}(\varphi)^2$ 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 and ρ an assignment over $\mathcal{A}$. Assume that $\mathcal{A}\ \rho \Vdash \exists \vec{w}\ \mathsf{s\text{-}witness}(\varphi)$. Then $\mathcal{A}\ \rho \Vdash \varphi \wedge \exists \vec{w}\ \Omega$, and so $\mathcal{A}\ \rho \Vdash \varphi$. For the other direction, assume $\mathcal{A}\ \rho \Vdash \varphi$. We need to show that

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

Let ρ' be an assignment $\vec{w}$-equivalent to ρ (and so mapping all variables as ρ except possibly for variables in $\vec{w}$) such that:

- if the domain of $\mathcal{A}$ is infinite then $\rho'(w_1) \neq \rho'(w_2)$ for every $w_1, w_2 \in \vec{w}$;
- if the domain of $\mathcal{A}$ 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 $\rho'(w_1) \neq \rho'(w_2)$ for every $w_1, w_2 \in \mathsf{vars}(\gamma_{k_E^\varphi})$;
  - otherwise, set $\rho'(w_1) = \rho'(w_2)$ for every $w_1, w_2 \in \mathsf{vars}(\gamma_{k_E^\varphi})$.

Then

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

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

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

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 $\mathcal{A}$ and an assignment ρ that satisfies $\varphi \wedge \Omega \wedge \delta_{E'}^Y$ such that $\mathsf{dom}(\mathcal{A}) = [\![\mathsf{vars}(\varphi \wedge \Omega \wedge \delta_{E'}^Y)]\!]^\rho$. 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 $Y_1, \ldots, Y_p$ be 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 $\delta^Y_{E'}$ for each $x \in Y_i$;
  - $\neg(y \cong x)$ and $\neg(x \cong y)$ are in $\delta^Y_{E'}$ 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 and ρ an assignment over $\mathcal{A}$ that satisfy

$$\varphi \wedge \Omega \wedge \delta^Y_{E'}$$

and let $\delta^{\mathsf{vars}(\varphi)}_{E_\rho}$ be the arrangement formula induced by $E_\rho = \{(x, y) : x, y \in \mathsf{vars}(\varphi) \text{ and } \rho(x) = \rho(y)\}$. Then, obviously, $\delta^{\mathsf{vars}(\varphi)}_{E_\rho}$ is satisfied by $\mathcal{A}$ and ρ. Moreover, no other formula in $\{\delta^{\mathsf{vars}(\varphi)}_E : E \subseteq \mathsf{vars}(\varphi)^2 \text{ and } \mathcal{P}(\varphi \wedge \delta^{\mathsf{vars}(\varphi)}_E) = 1\}$ is satisfied by $\mathcal{A}$ and ρ. Since $\varphi \wedge \delta^{\mathsf{vars}(\varphi)}_{E_\rho}$ is satisfiable we have that the cardinality of its smallest model is $k^\varphi_{E_\rho} = \mathsf{mincard}(\varphi \wedge \delta^{\mathsf{vars}(\varphi)}_{E_\rho})$. Let $K = \max\{k^\varphi_{E_\rho}, p\}$. By the smoothness of $\mathcal{T}$ and since $\varphi \wedge \delta^{\mathsf{vars}(\varphi)}_{E_\rho}$ is $\mathcal{T}$-satisfiable, let $\mathcal{B}$ be a $\mathcal{T}$-model and σ be an assignment over $\mathcal{B}$ such that

$$\mathcal{B}\ \sigma \Vdash \varphi \wedge \delta^{\mathsf{vars}(\varphi)}_{E_\rho} \quad \text{and} \quad |\mathsf{dom}(\mathcal{B})| = K,$$

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

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

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

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

for $j = 1, \ldots, k^\varphi_{E_\rho}$. Observe that distinct variables in $w_1 \ldots, w_{k^\varphi_{E_\rho}}$ are in distinct sets in $Y_1, \ldots, Y_p$ since $\mathcal{A}\ \rho \Vdash \delta^Y_{E'}$ and $\mathcal{A}\ \rho \Vdash \gamma_{k^\varphi_{E_\rho}}$ taking into account that $\mathcal{A}\ \rho \Vdash \delta^{\mathsf{vars}(\varphi)}_{E_\rho}$ and $\mathcal{A}\ \rho \Vdash \Omega$. Let σ' be an assignment $(\vec{w} \cup (Y \setminus \mathsf{vars}(\varphi)))$-equivalent to σ such that

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

for each $x \in \vec{w} \cup (Y \setminus \mathsf{vars}(\varphi))$. Let us now prove that $\mathcal{B}\ \sigma' \Vdash \varphi \wedge \Omega \wedge \delta^Y_{E'}$:

(a) $\mathcal{B}\ \sigma' \Vdash \varphi$. This follows immediately taking into account that $\mathcal{B}\ \sigma \Vdash \varphi$ and that σ and σ' may only differ in variables in $\vec{w} \cup (Y \setminus \mathsf{vars}(\varphi))$ not occurring in φ;

(b) $\mathcal{B}\ \sigma' \Vdash \Omega$. Observe that $\mathcal{B}\ \sigma' \Vdash \varphi \wedge \delta^{\mathsf{vars}(\varphi)}_{E_\rho}$ since σ and σ' may only differ in variables in $X_\gamma \cup (Y \setminus \mathsf{vars}(\varphi))$ not occurring in $\varphi \wedge \delta^{\mathsf{vars}(\varphi)}_{E_\rho}$. Moreover $\mathcal{B}\ \sigma' \Vdash \gamma_{k_{E_\rho}}$ and so $\mathcal{B}\ \sigma' \Vdash \delta^{\mathsf{vars}(\varphi)}_{E_\rho} \rightarrow \gamma_{k_{E_\rho}}$. Since $\mathcal{B}\ \sigma' \Vdash \delta^{\mathsf{vars}(\varphi)}_{E_\rho}$, we have that $\mathcal{B}\ \sigma' \nVdash \delta^{\mathsf{vars}(\varphi)}_E$ for all $E \neq E_\rho$ with $E \subseteq \mathsf{vars}(\varphi)^2$. Hence $\mathcal{B}\ \sigma' \Vdash \delta^{\mathsf{vars}(\varphi)}_E \rightarrow \gamma_{k_E}$ for all $E \subseteq \mathsf{vars}(\varphi)^2$ and so $\mathcal{B}\ \sigma' \Vdash \Omega$;

(c) $\mathcal{B}\ \sigma' \Vdash \delta_{E'}^{Y}$. We only need to verify that $\mathcal{B}$ and σ' satisfy the equalities and inequalities 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 $\mathsf{dom}(\mathcal{B}) = [\![\mathsf{vars}(\varphi \wedge \Omega \wedge \delta_{E'}^{Y})]\!]^{\sigma'}$:

($\subseteq$): Let $d \in \mathsf{dom}(\mathcal{B})$. Then d is either a d_i for some $i = 1, \ldots, p$ or an e_j for some $j = 1, \ldots, k_{E_\rho}$. In the case that $d = d_i$ then we have that $d = \sigma'(x)$ for all $x \in Y_i$. On the other hand, if $d = e_j$ then $d = \sigma'(w_j)$ for the w_j variable in $\mathsf{vars}(\gamma_{k_{E_\rho}})$;

($\supseteq$): From the construction described above we show for every $x \in \mathsf{vars}(\varphi \wedge \Omega \wedge \delta_{E'}^{Y})$ how to define $\sigma'(x)$.

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

We now prove that a strongly finitely witnessable theory is always finitely witnessable.

Proposition 6.5. *Each strongly finitely witnessable theory is finitely witnessable.*

Proof. Let $\mathcal{T}$ be a strongly finitely witnessable Σ-theory and $\mathsf{s\text{-}witness}$ a strong witness function for $\mathcal{T}$. We now show that $\mathsf{s\text{-}witness}$ is also a witness for $\mathcal{T}$. The first condition follows immediately. With respect to the second condition assume that $\mathsf{s\text{-}witness}(\varphi)$ is satisfiable in $\mathcal{T}$. Let E and Y be empty sets. Then δ_E^Y is true and so $\mathsf{s\text{-}witness}(\varphi) \wedge \delta_E^Y$ is satisfiable in $\mathcal{T}$. Hence the thesis follows immediately by the second condition of the definition of strong finite witnessability since $\mathsf{s\text{-}witness}$ is a strong witness function for $\mathcal{T}$. □

Combining the previous results, we proved that the equivalence between *strong politeness, shininess* and *politeness* holds, assuming one out of two different sets of conditions on the theory.

A consequence of these results is that we are now able to design a procedure to obtain a strong witness function starting from a witness function (which is easier to find than a strong witness function), provided that the theory has a decidable quantifier-free satisfiability problem and is either universal or it is decidable to check if a finite interpretation is a model for it. This implies that if a polite theory satisfies one of these requirements, then we are able to design a Nelson-Oppen combination procedure to decide the satisfiability of quantifier-free formulas in its union with an arbitrary theory. This result seems, at first, contradictory with Example 5.1, where it was shown that the politeness notion allowed witness functions that made the combination theorem for a polite and an arbitrary theory false. However, this counterexample only shows that it is not possible to use the Nelson-Oppen combination procedure with witness functions and what we show is that from a witness function we are able to construct a strong witness function and then use the combination procedures seen in Chapter 5. For this, consider Algorithms 4, 5 and 6.

Theorem 6.6. *Let Σ be a finite signature and $\mathcal{T}$ be a polite Σ-theory with a decidable quantifier-free satisfiability problem. Assume either that $\mathcal{T}$ is universal or that it is decidable to check if a finite interpretation is a $\mathcal{T}$-model. Then, Algorithm 6 computes a strong witness function for $\mathcal{T}$.*

Proof. We begin by computing the $\mathsf{mincard}$ function. If $\mathcal{T}$ is universal, by Proposition 6.3 we have that the $\mathsf{mincard}$ function is computable and that Algorithm 4 is an algorithm for it. In the case that it is decidable

Algorithm 6 — algorithm for a strong witness function s-witness for a theory $\mathcal{T}$
Input: φ, where φ is a quantifier-free satisfiable formula
Output: s-witness(φ)
Requires: access to an algorithm $\mathcal{P}$ that decides satisfiability of quantifier-free formulas, and to the function mincard for $\mathcal{T}$

1: **for** $E \subseteq \mathsf{vars}(\varphi)^2$
2: $\quad \delta_E^{\mathsf{vars}(\varphi)} = \varepsilon$
3: $\quad$ **for** all pairs $(x, y) \in \mathsf{vars}(\varphi)^2$
4: $\quad\quad$ **if** $(x, y) \in E$
5: $\quad\quad\quad$ **then** $\delta_E^{\mathsf{vars}(\varphi)} = \delta_E^{\mathsf{vars}(\varphi)} \wedge (x \cong y)$
6: $\quad\quad\quad$ **else** $\delta_E^{\mathsf{vars}(\varphi)} = \delta_E^{\mathsf{vars}(\varphi)} \wedge \neg(x \cong y)$
7: $\quad\quad$ **end if**
8: $\quad$ **end for**
9: $\quad$ **if** $\mathcal{P}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)}) == 1$
10: $\quad\quad$ **then** $k_E = \mathsf{mincard}(\varphi \wedge \delta_E^{\mathsf{vars}(\varphi)})$
11: $\quad\quad\quad \gamma_{k_E} = \varepsilon$
12: $\quad\quad\quad$ **for** $i, j = 1, i \neq j$ **to** k_E
13: $\quad\quad\quad\quad \gamma_{k_E} = \gamma_{k_E} \wedge \neg(x_i \cong x_j)$
14: $\quad\quad\quad$ **end for**
15: $\quad\quad\quad \varphi = \varphi \wedge (\delta_E^{\mathsf{vars}(\varphi)} \rightarrow \gamma_{k_E})$
16: $\quad$ **end if**
17: **end for**
18: **return** φ

to check if a finite Σ-interpretation is a $\mathcal{T}$-model, then by Proposition 4.19 we have that the mincard function is computed by Algorithm 5. Therefore, $\mathcal{T}$ is shiny. It is immediate to see that Algorithm 6 computes the function shown in the proof of Proposition 6.4 to be a strong witness function for $\mathcal{T}$, and so the result follows.

□

From the previous result, we developed a mechanism to construct the mincard function and a strong witness function from a witness function, provided the theory satisfies one of the two sets of restrictions. In other words, we showed that if a polite theory over a finite signature is either universal or it is decidable to check whether a finite interpretation is a model of the theory then the theory is both shiny and strongly polite. This way, since in Chapter 4 we provided a combination theorem for a shiny and an arbitrary theory and in Chapter 5 we provided a combination theorem for a strongly polite and an arbitrary theory, we can use these combinations method to combine a polite theory and an arbitrary theory, provided the polite theory satisfies one of the described conditions.

Theorem 6.7. *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. By theorem 6.6, the functions $\mathsf{mincard}_{\mathcal{T}_2}$ and $\mathsf{s\text{-}witness}_{\mathcal{T}_2}$ are computable. Furthermore, from Proposition 6.1 we obtain that $\mathcal{T}_2$ is stably finite. We conclude that $\mathcal{T}_2$ is both shiny and strongly polite. The equivalence between (1) and (2) follows from the combination Theorem 4.10 and the equivalence between (1) and (3) follows from the combination Theorem 5.6. □

We now exemplify an application of the previous theorem, showing how it could be applied to solve the counterexample provided by Example 5.1.

Example 6.1. *Recall from Example 5.1 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 two. Let* φ *denote the formula* $(x \cong x)$*.*

Also recall, from Example 5.1 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 6.7 is fullfilled. Taking into account that* $\mathsf{mincard}_{\mathcal{T}_2}(\varphi) = 2$*, then by Algorithm 6,*

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

Let Γ_1 *be the formula* true*,* 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 6.7, 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 6 to define in a computable way the strong witness function for $\mathcal{T}_2$.

6.3 Summary of the chapter

In this chapter we studied the relationship between shininess and politeness, between shininess and strong politeness as well as between the two politeness notions. The relationship between shininess and politeness was first analyzed by Ranise, Ringeissen and Zarba in [9]. However, after the introduction of the strong politeness notion, the relationship between the two politeness notions had not been studied. On the other hand, the study of the relationship between the strong politeness notion and shininess was left as an open problem in [6]. In this chapter we show that a shiny theory with a decidable quantifier-free satisfiability problem is strongly polite. We also show that a strongly polite theory is a polite theory, and using results from [9] and [14], that under each one of two sets of restrictions, the shininess, politeness and strong politeness notions are equivalent (see Figure 6.1 for a global view of the results). From this, we are able to devise a Nelson-Oppen procedure for the combination of a polite and an arbitrary theory, provided the polite theory satisfies some conditions.

7 – Conclusion

The first and most well-known method for the combination of satisfiability procedures is due to Nelson and Oppen, [7]. In their 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, have disjoint signatures and are stably infinite. At that time, this result had great impact on the area of automated reasoning since it provided a general combination method, which at the time was made on a case by case basis such as in the work of Suzuki and Jefferson [11] on the combination of the theory of arrays and Presburger arithmetic. However, the class of theories to which this method applied seemed too restrictive and several extensions or "migrations" of the method were proposed, namely the extension to shiny theories in [14], to polite theories in [9] and to strongly polite theories in [6]. In this document we presented these combination methods in a self-contained and detailed manner. Furthermore, we answered a question left open by Jovanović and Barrett in [6], and obtained results on the relationship between shiny and strongly polite theories, as well as presenting known results on the relationship between shiny and polite theories. With this set of results, we were able to devise a Nelson-Oppen procedure for the combination of a polite and an arbitrary theory by constructing the mincard function and a strong witness function from a witness function.

7.1 Directions for further research

In this document, we focused on extending the original Nelson-Oppen method to theories that were not stably infinite. However, the less studied requirement of the Nelson-Oppen method, theories having disjoint signatures, is also of great interest and recently has had surprising applications in other fields of logic, in particular on the union of logics, specifically on the *fusion* of modal logics [1].

Also, we leave as future work the generalization to the many-sorted case of the proposition stating that a shiny theory is strongly polite.

Bibliography

[1] F. Baader, S. Ghilardi, and C. Tinelli. A new combination procedure for the word problem that generalizes fusion decidability results in modal logics. *Information and Computation*, 204(10):1413–1452, 2006.

[2] 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.

[3] 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.

[4] P. Fontaine, S. Ranise, and C. G. Zarba. Combining lists with non-stably infinite theories. In *Proceedings of the Eleventh International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'2004)*, volume 3452 of *LNCS*, pages 51–66. Springer, 2005.

[5] M. R. Garey and D. S. Johnson. *Computers and Intractability; A Guide to the Theory of NP-Completeness*. W. H. Freeman & Co., New York, NY, USA, 1990.

[6] 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.

[7] G. Nelson and D. C. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1(2):245–257, 1979.

[8] D. C. Oppen. Complexity, convexity and combinations of theories. *Theoretical Computer Science*, 12:291–302, 1980.

[9] 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.

[10] A. Sernadas and C. Sernadas. *Foundations of Logic and Theory of Computation*, volume 10 of *Texts in Computing*. College Publications, London, 2008.

[11] N. Suzuki and D. Jefferson. Verification decidability of Presburger array programs. In *Proceedings of a Conference on Theoretical Computer Science (Univ. Waterloo, Waterloo, Ont., 1977)*, pages 202–212. Comput. Sci. Dept., Univ. Waterloo, Waterloo, Ont., 1978.

[12] 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.

[13] C. Tinelli and C. Ringeissen. Unions of non-disjoint theories and combinations of satisfiability procedures. *Theoretical Computer Science*, 290(1):291–353, 2003.

[14] C. Tinelli and C. G. Zarba. Combining nonstably infinite theories. *Journal of Automated Reasoning*, 34(3):209–238, 2005.