Quantifier Elimination and Provers Integration

Silvio Ghilardi [1]

Dipartimento di Scienze dell'Informazione
Università degli Studi
Milano, Italy

Abstract

We exploit quantifier elimination in the global design of combined decision and semi-decision procedures for theories over non-disjoint signatures, thus providing in particular extensions of Nelson-Oppen results.

Keywords: Combination, Nelson-Oppen Combination Schema, Fusion, Superposition Calculus, Quantifier Elimination, Model Completions.

1 Introduction and Background

Quantifier elimination has been considered, since the early times of modern symbolic logic, a powerful technique for decision procedures. Even in actual approaches to combination problems (see e.g. [9]), specific quantifier elimination algorithms are often invoked as specialized reasoners to be integrated within a flexible general setting dealing with multiple theories. This happens, in particular, whenever numerical constraints problems need to be adequately addressed: examples of such specialized reasoners are the Fourier-Motzkin quantifier elimination procedure for linear rational arithmetic or Cooper's quantifier elimination procedure for integer Presburger arithmetic.

In contrast to this *local call* for quantifier elimination algorithms, we shall address in this paper quantifier elimination as a *global design* opportunity for integrated provers: we shall show in particular how it can be used in order to *extend Nelson-Oppen combination procedure* [11], [13], [16] *to non-disjoint signatures*. Detailed proofs of the results presented here, as well as additional information, can be found in [6].

A *signature* Σ is a set of functions and predicate symbols (each of them endowed with the corresponding arity). We assume the binary equality predicate symbol $=$ to be always present in Σ. The signature obtained from Σ by the addition of a set of new constants (= 0-ary function symbols) X is denoted

[1] Email: ghilardi@dsi.unimi.it

This is a preliminary version. The final version will be published in Electronic Notes in Theoretical Computer Science
URL: www.elsevier.nl/locate/entcs

by $\Sigma \cup X$ or by Σ^X. We have the usual notions of Σ-*term*, (full first order) -*formula*, -*atom*, -*literal*, -*clause*, -*positive clause*, etc.: e.g. atoms are just atomic formulas, literals are atoms and their negations, clauses are disjunctions of literals, positive clauses are disjunctions of atoms. Letters $\phi, \psi, \ldots$ are used for formulas, whereas letters $A, B, \ldots$ are used for literals and letters $C, D, \ldots$ are used for clauses. Terms, literals and clauses are called *ground* whenever variables do not appear in them. Formulas without free variables are called *sentences*. A Σ-*theory* T is a set of sentences (called the axioms of T) in the signature Σ; however when we write $T \subseteq T'$ for theories, we may mean not just set-theoretic inclusion but the fact that all the axioms for T are logical consequences of the axioms for T'.

From the semantic side, we have the standard notion of a Σ-*structure* $\mathcal{A}$: this is nothing but a support set endowed with an arity-matching interpretation of the predicate and function symbols from Σ. We shall notationally confuse, for the sake of simplicity, a structure with its support set. Truth of a Σ-formula in $\mathcal{A}$ is defined in any one of the standard ways (so that truth of a formula is equivalent to truth of its *universal* closure). A Σ-structure $\mathcal{A}$ is a *model* of a Σ-theory T (in symbols $\mathcal{A} \models T$) iff all axioms of T are true in $\mathcal{A}$; for models of a Σ-theory T we shall preferably use the letters $\mathcal{M}, \mathcal{N}, \ldots$ to distinguish them from arbitrary Σ-structures. If ϕ is a formula, $T \models \phi$ ('ϕ *is a logical consequence of* T') means that ϕ is true in any model of T. A Σ-theory T is *complete* iff for every Σ-sentence ϕ, either ϕ or $\neg\phi$ is a logical consequence of T; T is *consistent* iff it has a model (i.e. iff $T \not\models \bot$).

An *embedding* between two Σ-structures $\mathcal{A}$ and $\mathcal{B}$ is any map $f : \mathcal{A} \longrightarrow \mathcal{B}$ among the corresponding support sets satisfying the condition

$$(*) \qquad \mathcal{A} \models A \quad \text{iff} \quad \mathcal{B} \models A$$

for all $\Sigma^{\mathcal{A}}$ atoms A (here $\mathcal{A}$ is regarded as a $\Sigma^{\mathcal{A}}$-structure by interpreting each $a \in \mathcal{A}$ into itself and $\mathcal{B}$ is regarded as a $\Sigma^{\mathcal{A}}$-structure by interpreting each $a \in \mathcal{A}$ into $f(a)$). Notice that, as we have identity in the language, an embedding is an injective function (it also must preserve the interpretation of the function symbols and, in case it is just an inclusion, the interpretation of the predicate symbols in the smaller structure must be the restriction of the corresponding interpretation in the bigger structure). In case $(*)$ holds for all first order formulas, the embedding is said to be *elementary*.

The main problems we deal with are *word problems*, more precisely, given a Σ-theory T:
- the *word problem* for T is that of deciding whether $T \models A$ holds for a Σ-atom A;
- the *conditional word problem* for T is that of deciding whether $T \models C$ holds for a Horn Σ-clause C;
- the *clausal word problem* for T is that of deciding whether $T \models C$ holds for a Σ-clause C;

- the *elementary word problem* for T is that of deciding whether $T \models \phi$ holds for a first order Σ-formula ϕ.

A formula is *quantifier-free* iff it does not contain quantifiers. A Σ-theory T is said to *eliminate quantifiers* iff for every formula $\phi(\underline{x})$ [2] there is a quantifier-free formula $\phi'(\underline{x})$ such that $T \models \phi(\underline{x}) \leftrightarrow \phi'(\underline{x})$. There are many well-known theories [4] eliminating quantifiers, we give here some examples which can be of interest for software verification.

Example 1.1 Linear integer arithmetic (i.e. the theory of the structure of integer numbers in the signature $+, 0, 1, \leq, \equiv_n$) eliminates quantifiers; so does rational linear arithmetic (i.e. the theory of rational numbers in the signature $+, 0, \leq$). Another well-known classical example from Tarski is real arithmetic (i.e. the theory of real numbers in the signature $+, 0, \cdot, 1, \leq$).

Example 1.2 The theory of acyclic binary lists L [13], [14] eliminates quantifiers (see [6]).

The main ingredient of this paper is the well-known notion of a *model completion* of a theory. There are good chapters on that in all texbooks from Model Theory. We shall recall here just the essential definitions *for the only case of universal theories* [3] which is the relevant one for the purposes of this paper (readers may consult e.g. [4], [10], [18] for further information).

Let T be a universal Σ-theory and let $T^* \supseteq T$ a further Σ-theory; we say that T^* is a model completion of T iff i) every model of T has an embedding into a model of T^* and ii) T^* eliminates quantifiers.

It can be shown that a model completion T^* of a theory T is unique, in case it exists, and moreover that T^* has a set of $\forall\exists$-axioms, see [4].

Example 1.3 The theory of an infinite set is the model completion of pure equality theory; the theory of dense total orders without endpoints is the model completion of the theory of total orders.

Example 1.4 There are many classical examples from algebra: the theory of algebraically closed fields is the model completion of the theory of intergral domains, the theory of divisible torsion free abelian groups is the model completion of the theory of torsion free abelian groups, etc.

Example 1.5 The theory of atomless Boolean algebras [4] is the model completion of the theory of Boolean algebras (for model completions arising in the algebra of logic, see the book [8]).

Example 1.6 An old result in [18] says, in particular, that universal Horn theories T in finite signatures always have a model completion, provided the

[2] By this notation, we mean that ϕ contains free variables only among the finite set $\underline{x}$.

[3] Recall that a universal theory T is a theory having as axioms only universal closures of quantifier-free formulas.

[4] We recall that an atom in a Boolean algebra is a minimal non-zero element; a Boolean algebra is atomless iff it has no atoms.

following two conditions are satisfied: a) finitely generated models of T are all finite; b) amalgamation property holds for models of T. This fact can be used in order to prove the existence of a model completion for theories axiomatizing many interesting discrete structures (like graphs, posets, etc.).

Example 1.7 It follows from the quantifier elimination result reported in [6] that the theory L of acyclic binary lists is the model completion of itself.

Example 1.8 If a theory T^* has elimination of quantifiers, then it is the model completion of the theory T axiomatized by the set of universal sentences which are logical consequences of T, see [4].

2 Compatibility

The key ingredient for our combination procedures is the following notion:

Definition 2.1 Let T be a theory in the signature Σ and let T_0 be a universal theory in a subsignature $\Sigma_0 \subseteq \Sigma$. We say that T is T_0-compatible iff

(i) $T_0 \subseteq T$;

(ii) T_0 has a model-completion T_0^*;

(iii) every model of T embeds into a model of $T \cup T_0^*$.

Condition (iii) can be equivalently given in a slightly different form, by saying that every quantifier-free Σ-formula which is false in a model of T is false also in a model of $T \cup T_0^*$.

Example 2.2 According to this remark, it is evident that T_0-compatibility *reduces to the standard notion of stable infiniteness* (used in the disjoint Nelson-Oppen combination procedure) in case T_0 is the pure theory of equality: [5] recall in fact that in this case T_0^* (i.e. the model completion of the pure equality theory) is the theory of an infinite set.

Example 2.3 Every theory including the theory L of acyclic binary lists is compatible with L, because L is universal and $L = L^*$.

Example 2.4 If T_0 has a model completion T_0^* and if $T \supseteq T_0^*$, then T is certainly T_0-compatible: this trivial case is often interesting (we may take e.g. T_0 to be the theory of linear orders and T to be real aritmetic or rational linear arithmetic).

Example 2.5 Let T_0 be a universal theory having a model completion T_0^*; if T is any extension of T_0 with free function symbols only, then T is T_0-compatible.

More examples will be supplied in section 4. An interesting feature of T_0-compatibility is that it is a *modular* property:

[5] By the 'pure theory of equality' we mean the empty theory in the signature containing only the equality predicate.

Proposition 2.6 *Let T_1 be a Σ_1-theory and let T_2 be a Σ_2-theory; suppose they are both compatible with respect to a Σ_0-theory T_0 (where $\Sigma_0 := \Sigma_1 \cap \Sigma_2$). Then $T_1 \cup T_2$ is T_0-compatible too.*

3 Combining compatible theories

Let us progressively fix our main data for the whole paper.

Assumption (I). *T_1 is a theory in the signature Σ_1 and T_2 is a theory in the signature Σ_2; Σ_0 is the signature $\Sigma_1 \cap \Sigma_2$.*

Our main aim is that of (semi)deciding the clausal word problem for $T_1 \cup T_2$, given that the corresponding clausal word problems for T_1 and T_2 are (semi)decidable. Equivalently, this amounts to (semi)decide the consistency of

$$T_1 \cup T_2 \cup \Gamma,$$

where Γ is a finite set of ground literals in the signature $\Sigma_1 \cup \Sigma_2$, expanded with a finite set of new Skolem constants.

Γ can be *purified*: as usual, we can abstract alien subterms and add equations involving further new free constants, in such a way that our problem is reduced to the problem of establishing the consistency of a set of sentences like

$$(T_1 \cup \Gamma_1) \cup (T_2 \cup \Gamma_2), \tag{1}$$

where Γ_1, Γ_2 are as explained in the following:

Assumption (II). *For finitely many new free constants $\underline{a}$, Γ_1 is a finite set of ground literals in the signature $\Sigma_1^{\underline{a}}$ and Γ_2 is a finite set of ground literals in the signature $\Sigma_2^{\underline{a}}$.*

For trivial reasons, the consistency of (1) cannot follow from the mere separate consistency of $T_1 \cup \Gamma_1$ and of $T_2 \cup \Gamma_2$. We need some *information exchange* between a reasoner dealing with $T_1 \cup \Gamma_1$ and a reasoner dealing with $T_2 \cup \Gamma_2$.

Craig's interpolation theorem for first order logic ensures that the inconsistency of (1) can be detected by the information exchange of a single $\Sigma_0^{\underline{a}}$-sentence ϕ such that $T_1 \cup \Gamma_1 \models \phi$ and $T_2 \cup \Gamma_2 \cup \{\phi\} \models \bot$. However, as pointed out in [15], this observation is not very useful, as ϕ might be any first-order formula, whereas we would like - at least - ϕ to be quantifier-free.

Unfortunately, information exchange of quantifier-free $\Sigma_0^{\underline{a}}$-formulas alone is not sufficient, even for syntactically simple T_1 and T_2, to establish the inconsistency of (1) (see section 5 below for a counterexample). We so need a further assumption in order to get limited information echange without affecting refutational completeness (this is the relevant assumption we make, the other two being mere notational conventions):

Assumption (III). *There is a universal Σ_0-theory T_0 such that both T_1 and T_2 are T_0-compatible.*

A finite list $C_1, \ldots, C_n$ of positive ground $\Sigma_0^{\underline{a}}$-clauses such that for every $k = 1, \ldots, n$, there is $i = 1, 2$ such that

$$T_i \cup \Gamma_i \cup \{C_1, \ldots, C_{k-1}\} \models C_k.$$

is called a *positive residue chain*. We can now formulate our combination results (see [6] for proofs):

Theorem 3.1 *In the above assumptions, $(T_1 \cup \Gamma_1) \cup (T_2 \cup \Gamma_2)$ is inconsistent iff there is a positive residue chain $C_1, \ldots, C_n$ such that C_n is the empty clause.*

Thus inconsistency can be detected by repeated exchanges of positive ground clauses only; if we allow information exchange consisting on ground quantifier free formulas, a single exchange step is sufficient:

Theorem 3.2 *In the above assumptions, $(T_1 \cup \Gamma_1) \cup (T_2 \cup \Gamma_2)$ is inconsistent iff there is a ground quantifier-free $\Sigma_0^{\underline{a}}$-sentence ϕ such that*

$$T_1 \cup \Gamma_1 \models \phi \qquad \textit{and} \qquad T_2 \cup \Gamma_2 \cup \{\phi\} \models \bot.$$

Following [15], we say that our T_i's are Σ_0-convex iff whenever it happens that $T_i \cup \Gamma_i \models A_1 \vee \cdots \vee A_n$ (for $n \geq 1$ and for ground $\Sigma_0^{\underline{a}}$-atoms $A_1, \ldots, A_n$), then there is $k = 1, \ldots, n$ such that $T_i \cup \Gamma_i \models A_k$.[6] For Σ_0-convex theories, Theorem 3.1 refines in the following way:

Corollary 3.3 *In addition to the above assumptions, suppose also that T_1, T_2 are both Σ_0-convex. Then $(T_1 \cup \Gamma_1) \cup (T_2 \cup \Gamma_2)$ is inconsistent iff there is a positive residue chain $C_1, \ldots, C_n$ in which $C_1, \ldots, C_{n-1}$ are all ground Σ_0-atoms and C_n is $\bot$.*

4 The locally finite case

We say that a Σ_0-universal theory T_0 is *locally finite* iff Σ_0 is finite and for every finite set $\underline{a}$ of new free constants, there are finitely many $\Sigma_0^{\underline{a}}$-ground terms $t_1, \ldots, t_{k_{\underline{a}}}$ such that for every further $\Sigma_0^{\underline{a}}$-ground term u, we have $T_0 \models u = t_i$ (for some $i = 1, \ldots, k_{\underline{a}}$).[7] As we are mainly dealing with computational aspects, we consider part of the definition the further request that such $t_1, \ldots, t_{k_{\underline{a}}}$

[6] Among Σ_0-convex theories we have the important class of universal Horn theories, see [15] again.

[7] Local finiteness is a much weaker requirement than the notion of 'finitary modulo a renaming' introduced in [2]. The reason is because the number $k_{\underline{a}}$ depends on the cardinality of $\underline{a}$; on the contrary a Σ_0-theory T is said to be finitary modulo a renaming iff there is a finite set of Σ_0-terms S such that for every Σ_0-term u there are $t \in S$ and a renaming σ such that $T \models u = t\sigma$. Consequently, for instance, locally finite theories (like Boolean algebras) in which the number $k_{\underline{a}}$ grows more than polynomially in the cardinality of $\underline{a}$ cannot be finitary modulo a renaming.

are effectively computable from $\underline{a}$. Examples of locally finite theories are the theory of graphs, of partial orders (more generally, any theory whose signature does not contain function symbols), of commutative idempotent monoids, of Boolean algebras, etc.

In a locally finite theory T_0, there are restricted *finite* classes which are representatives, up to T_0-equivalence, of the whole classes of $\Sigma_0^{\underline{a}}$-ground literals, clauses, quantifier-free sentences, etc. (they are just the ground literals, clauses, quantifier-free sentences, etc. containing only the above mentioned terms $t_1, \ldots, t_{k_{\underline{a}}}$). As it is evident that we can limit information exchange to ground positive clauses and quantifier-free sentences in that restricted class, both Theorems 3.1, 3.2 yield *combined decision procedures for the clausal word problem in* $T_1 \cup T_2$ in case the above assumptions (I) and (III) are satisfied and in case T_0 is locally finite. In particular, Theorem 3.1 suggest the following extension of the Nelson-Oppen procedure [13]:

Algorithm 1

Step 1: Negate, skolemize and purify the universal closure of the **input clause** *C thus producing a set Γ_1 of ground $\Sigma_1^{\underline{a}}$-literals and a set Γ_2 of ground $\Sigma_2^{\underline{a}}$-literals (then $\Gamma_1 \cup \Gamma_2$ is $T_1 \cup T_2$-equisatisfiable with $\neg\forall \underline{x} C$). During the next Steps loop, positive ground $\Sigma_0^{\underline{a}}$-clauses are added to Γ_1, Γ_2.*

Step 2: Using the decision procedures for T_1, T_2, check whether $T_1 \cup \Gamma_1$ and $T_2 \cup \Gamma_2$ are consistent or not (if one of them is not, **return** *'$T_1 \cup T_2 \models C$').*

Step 3: If $T_i \cup \Gamma_i$ entails some positive ground $\Sigma_0^{\underline{a}}$-clause (atom in the Σ_0-convex case) not entailed by $T_j \cup \Gamma_j$ $(j \neq i)$ add this positive ground clause (atom) to Γ_j and go back to Step 2.

Step 4: If this step is reached, **return** *'$T_1 \cup T_2 \not\models C$'.*

Example 4.1 Let T_1 be rational linear arithmetic and let T_2 be the theory of total orders endowed with a strict monotonic function f. We take as T_0 the theory of total orders (recall that its model completion T_0^* is the theory of dense total orders without endpoints). T_1 is known to be decidable and the clausal word problem for T_2 is decidable too. As $T_1 \supseteq T_0^*$, T_1 is certainly T_0-compatible. T_2 is also T_0-compatible (to embed a model $\mathcal{M}$ of T_2 into a model $\mathcal{M}'$ of $T_0^* \cup T_2$, take as $\mathcal{M}'$ the lexicographic product of $\mathcal{M}$ with e.g. the poset of rational numbers). Thus our combination results apply and we obtain the decidability of the clausal word problem for rational linear arithmetic endowed with a strict monotonic function.

Example 4.2 A *modal algebra* is a Boolean algebra $\mathcal{B} = \langle B, \cap, 1, \cup, 0, (-)' \rangle$ endowed with an operator $\Box$ preserving binary meets and the top element. Let now Σ_1 be the signature of Boolean algebras augmented with a unary function symbol $\Box_1$ and let Σ_2 be the signature of Boolean algebras augmented with a unary function symbol $\Box_2$. T_1 is the equational theory of a variety V_1 of modal algebras and T_2 is the equational theory of another variety V_2 of modal algebras. For $i = 1, 2$, T_i is a universal Horn theory, hence it is Σ_i-convex: this

means in particular that the solvability of the conditional word problem for T_i implies the solvability of the clausal word problem for T_i. As every model of T_i embeds into a model whose Boolean reduct is atomless, we can conclude that the solvability of the conditional word problem for T_1 and T_2 implies the solvability of the conditional word problem for $T_1 \cup T_2$. Also, in case the modal operators $\Box_1, \Box_2$ are both *transitive*,[8] the solvability of the word problem for T_1 and T_2 implies the solvability of the word problem for $T_1 \cup T_2$.

We underline that the last observation, once read in terms of logics, *means exactly fusion decidability for normal extensions of* $K4$. Although this does not entirely cover Wolter's fusion decidability results [19], it puts some substantial part of them into the appropriate general combination context. For new results (based on a refinement of the combination schema explained in this section) concerning fusion of modal logics sharing a universal modality and nominals, see [7].

5 Pure deductions

In this section we give some further suggestions about a possible use of the ideas explained in section 3 within saturation-based theorem proving. We show that whenever T_0-compatibility holds it is possible to cut in a deduction the inferences which are not pure, still retatining refutational completeness. An inference among $(\Sigma_1 \cup \Sigma_2)^{\underline{a}}$-clauses

$$\frac{C_1, \ldots, C_n}{C}$$

is *pure* iff there is $i = 1, 2$ such that all the clauses $C_1, \ldots, C_n, C$ are $\Sigma_i^{\underline{a}}$-clauses. Similarly, a deduction is pure iff all inferences in it are pure. Usually pure deductions are not able to detect inconsistency of (the skolemization of) sets of sentences like $T_1 \cup \Gamma_1 \cup T_2 \cup \Gamma_2$, however we shall see that this may happen when the T_0-compatibility conditions are satisfied.

In order to realize this program, we first need to skolemize the theories T_1, T_2, thus passing to theories T_1^{sk}, T_2^{sk} in extended signatures $\Sigma_1^{sk}, \Sigma_2^{sk}$; Skolem functions will *not* be considered shared symbols, hence we still have that $\Sigma_0 = \Sigma_1^{sk} \cap \Sigma_2^{sk}$. The first problem we meet is the following: if T_i is T_0-compatible, is T_i^{sk} still T_0-compatible? We do not have a general answer for that, however there is a relevant case in which the answer is affirmative:

Proposition 5.1 *Let T be a Σ-theory which is compatible with respect to a Σ_0-theory T_0 (here Σ_0 is a subsignature of Σ). If the axioms of T are all*

[8] The modal operator $\Box_i$ is said to be transitive iff $T_i \models \Box_i x \cap \Box_i \Box_i x = \Box_i x$. For transitive modal operators it is easily seen that the conditional word problem reduces to the word problem.

$\forall\exists$*-sentences, then* T^{sk} *is* T_0*-compatible too.*

The previous Proposition motivates the following extra assumption (in addition to those from section 3):

Assumption (IV). T_1, T_2 *are axiomatized by* $\forall\exists$*-sentences;* T_1^{sk}, T_2^{sk} *are their skolemizations.*

We take into consideration here the *Superposition Calculus* $\mathcal{I}$ (see [3], [12]). We fix a *lexicographic path ordering*[9] induced by a total precedence on the symbols of $\Sigma_1^{sk} \cup \Sigma_2^{sk} \cup \{\underline{a}\}$; assuming for simplicity that our signatures are finite, this induces a reduction ordering $>$ which is total on ground terms. We give to symbols in Σ_0^a *lower precedence* than to symbols in $\Sigma_1^{sk} \setminus \Sigma_0$ and in $\Sigma_2^{sk} \setminus \Sigma_0$. This is essential: as a consequence, ground Σ_0^a-clauses will be smaller in the twofold multiset extension of $>$ than all ground clauses containing a proper Σ_1 or Σ_2-symbol.

Theorem 5.2 *In the above assumptions (I)-(IV), the set of sentences* $T_1 \cup \Gamma_1 \cup T_2 \cup \Gamma_2$ *is inconsistent iff there is a pure* $\mathcal{I}$*-derivation of the empty clause from* $T_1^{sk} \cup \Gamma_1 \cup T_2^{sk} \cup \Gamma_2$.

A possible direction for future reseach should try to take advantage from Theorem 5.2 in decision procedures based on Superposition Calculus: in fact for interesting (intrinsecally non locally finite) theories, the Superposition Calculus terminates whenever it has to test satisfiability of finite sets of ground literals [1].

Before concluding this section, we shall provide an example in which the assumptions of Theorem 5.2 are satisfied and an example in which such assumptions fail.

Example 5.3 Let T_1, T_2 be both the theory of Boolean algebras; we assume that symbols of the bounded distributivity lattice language (namely $\cap, \cup, 0, 1$) are shared but that the two complements n_1, n_2 are not. We want to prove that $T_1 \cup T_2 \models \forall x(n_1(x) = n_2(x))$. If we take T_0 to be the theory of bounded distributive lattices (i.e. of distributive lattices with 0 and 1), we see that T_1, T_2 are T_0-compatible. Skolemization and purification give for instance the two sets of literals $\Gamma_1 = \{a = n_1(c), a \neq b\}$ and $\Gamma_2 = \{b = n_2(c), a \neq b\}$. A pure $\mathcal{I}$-refutation exists: the prover SPASS produces a pure $\mathcal{I}$-refutation consisting on 28 steps. However, the system is not programmed in order to avoid impure inferences, so that, during saturation, it impurely derives also (useless) 'mixed' clauses containing both n_1 and n_2. One of them, namely the atom $b \cap n_1(n_2(a)) = b$, is also selected as a given clause.

Example 5.4 Let T_1 be the theory of Boolean algebras and let T_2 be the theory of pseudocomplemented distributive lattices; these are bounded distributive lattices endowed with a unary operator $(-)^*$ satisfying the condition

[9] It is not clear whether the results explained in this section hold in case a Knuth-Bendix ordering is adopted.

$\forall x \forall y\ (x \cap y = 0 \leftrightarrow y \leq x^*)$. This condition expresses the properties of intuitionistic negation, hence in the union theory $T_1 \cup T_2$, the operator $(-)^*$ collapses into the classical complement. This means that $T_1 \cup \Gamma_1 \cup T_2 \cup \Gamma_2$ is inconsistent, where Γ_1 is empty and Γ_2 is $\{(a^*)^* \neq a\}$. A SPASS refutation takes 43 lines and it is highly impure. In fact a pure refutation cannot exist: the Σ_0- (and even the Σ_0^a)-ground clauses deducible from either $T_1 \cup \Gamma_1$ or $T_2 \cup \Gamma_2$ are insufficient to detect inconsistency, because they are all subsumed by the three negative literals $0 \neq 1, a \neq 1, a \neq 0$. Notice that T_2 is not T_0-compatible.

6 Conclusions and related work

In this paper we have extended Nelson-Oppen combination procedure to the case of theories T_1, T_2 over non-disjoint signatures, in presence of compatibility conditions over a common universal subtheory T_0. The extension we proposed applies to examples of real interest giving, as shown in section 4, combined decidability in case T_0 is locally finite. Whenever T_0 is not locally finite, our method can be used in order to limit residue exchange (see section 3) or in order to forbid impure inferences in saturation-based theorem proving, thus yielding restrictions on the search space during refutation derivations (see section 5).

It should be noticed that quantifier-elimination *plays only an indirect role* in the paper: in this sense, the existence of a model completion for a universal theory T_0 *guarantees a certain behaviour* in combination problems *by itself*, independently on how quantifier elimination in the model completion is established (this can be established also by semantic non constructive arguments, as largely exemplified in the model-theoretic literature). In principle, the quantifier elimination complexity/decidability *has nothing to do* with the complexity/decidability of our combination methods, simply because *quantifier elimination algorithms do not enter into them.* This is crucial, because most quantifier elimination algorithms are subject to heavy complexity lower bounds, which are often structural lower bounds for the decision of the elementary word problem in the corresponding theories [5].

One may wonder how severe is the crucial condition of T_0-compatibility used in the paper: let us discuss it for a while. T_0-compatibility involves two aspects, namely the existence of a model completion T_0^* for T_0 and the embeddability of models of T_i into models of $T_i \cup T_0^*$. As we have shown in the examples, the existence of a model completion seems to be frequent for theories commonly used in software verification. On one side, numeric constraint theories often enjoy this property, in the sense that they eliminate quantifiers (thus being model completions of the theories axiomatized by their respective universal consequences). On the other side, acyclic binary lists might probably be the paradigm of situations arising in theories axiomatizing natural datatypes. Finally, notice that quantifier elimination strictly depends

on the choice of the language: every theory trivially has quantifier elimination in an extended language with infinitely many definitional axioms, hence the problem of obtaining quantifier elimination seems to be mostly a problem of choosing a sufficiently rich but still natural and manageable language.

The question concerning embeddability of models of T_i into models of $T_i \cup T_0^*$ looks more problematic, in the sense that it can fail in significant situations and, in addition, it does not look to be mechanizable. Further research is necessary on this point, however we underline that there is a relevant case in which the problem disappears. This is the case in which T_i is an extension of T_0^*: we have seen an example in section 4 where T_i is rational linear arithmetic and T_0 is the theory of linear orders. Another example is the theory of acyclic lists L (which coincides with L^*): any extension of the theory of acyclic lists with significant extra structures matches our requirements and the advantages of our method (limited residue exchange, elimination of impure inferences, etc.) apply to all combinations of theories obtained in this way.

There have been many efforts in the literature trying to extend Nelson-Oppen combination method to theories sharing function and predicate symbols (different from equality). The starting point of any attempt to generalize Nelson-Oppen procedure to the non-disjoint case should preliminarly answer the following question: what is the specific feature of the stable infiniteness requirement that we want to generalize? In the present paper we answered the question by saying that infinite models are just *existentially closed* models of the pure theory of equality and based our further investigations on this observation. On the contrary, in other approaches (see e.g. [17]), it is emphasized that infinite models are just *free* models of the pure theory of equality with infinitely many generators. This leads to completely different results, because the notion of infinitely generated free and of existentially closed structure are quite divergent and their coincidence for the pure theory of equality must be considered a rather exceptional fact.

Before closing, we would like to remark that the idea (suggested in [15]) of using interpolation theorems in order to limit residue exchange in partial theory reasoning (whenever the background reasoner has to deal with combined theories) inspired some of the material presented in section 3 above. Notice however the following difference with respect to [15]: there the input theories T_1, T_2 were assumed to share all functions symbols (alien function symbols belonging to one theory being considered as free Skolem functions for the other), whereas we tried to keep function symbols separated too, as much as possible. This is essential in our context, because otherwise e.g. local finiteness of the common subtheory T_0 would be lost (and decidability of the combined problems presented in section 4 would not be achieved as a consequence).

Aknowledgements: I wish to thank Silvio Ranise and Cesare Tinelli for e-mail discussions on the subject of this paper.

References

[1] Armando A., Ranise S., Rusinowitch M., *Uniform Derivation of Superposition Based Decision Procedures*, "Proceedings of the Annual Conference on Computer Science Logic" (CSL01), Paris, France, pp. 513-527, (2001).

[2] Baader F., Tinelli C., *Combining Decision Procedures for Positive Theories Sharing Constructors*, in Sophie Tison (ed.) "Rewriting Techniques and Applications", 13th International Conference (RTA02), Springer LNCS 2378, pp. 352-366, (2002).

[3] Bachmair L., Ganzinger H. *Equational Reasoning in Saturation-Based Theorem Proving*, in Bibel L., Schmitt P.H. (eds.) "Automated Deduction - A Basis for Applications", vol. I, pp. 353-397, Kluwer (1998).

[4] Chang C.C., Keisler H.J., *Model Theory*, IIIrd edition, North Holland (1990).

[5] Ferrante J., Rackoff C.W., *The Computational Complexity of Logical Theories*, Springer Lecture Notes in Mathematics 718, (1979).

[6] Ghilardi S., *Reasoners Cooperation and Quantifier Elimination*, Rapporto Interno n. 288-03, Dipartimento di Scienze dell'Informazione, Università degli Studi di Milano (2003).

[7] Ghilardi S., Santocanale L., *Algebraic and Model Theoretic Techniques for Fusion Decidability in Modal Logic*, preprint (2003).

[8] Ghilardi S., Zawadowski M., *Sheaves, Games and Model Completions*, Trends in Logic Series, Kluwer (2002).

[9] Janicìc P., Bundy A., *A General Setting for Flexibly Combining and Augmenting Decision Procedures*, Journal of Automated Reasoning, 28, pp.257-305 (2002).

[10] MacIntyre A., *Model Completeness*, in Barwise J. (ed.), "Handbook of Mathematical Logic", North Holland, pp. 139-180 (1977).

[11] Nelson G., Oppen D., *Simplification by Cooperating Decision Procedures*, ACM Transactions on Programming Languages and Systems, 1(2), pp. 245-257 (1979).

[12] Nieuwhenhuis R., Rubio A., *Paramodulation-Based Theorem Proving*, in Robinson A., Voronkov A., (eds.) "Handbook of Automated Reasoning", vol. I, Elsevier/MIT, pp. 371-533 (2001).

[13] Oppen D., *Complexity, Convexity and Combination of Theories*, Theoretical Computer Science, 12, pp. 291-302 (1980).

[14] Oppen D., *Reasoning about Recursively Defined Data Structures*, Journal of the ACM, 27, 3, pp. 403-411 (1980).

[15] Tinelli C., *Cooperation of Background Reasoners in Theory Reasoning by Residue Sharing*, Journal of Automated Reasoning, 2003 (to appear).

[16] Tinelli C., Harandi M., *A New Correctness Proof of the Nelson-Oppen Combination Procedure*, in Baader F., Schulz K. (eds.) "1st International Workshop on Frontiers of Combining Systems (FroCos'96)", Applied Logic Series, vol. 3, Kluwer Academic Publishers, pp. 103-120 (1996).

[17] Tinelli C., Ringeissen C., *Unions of Non-Disjoint Theories and Combination of Satisfiability Procedures*, Theoretical Computer Science 290(1), pp.291-353, (2003).

[18] Wheeler W. H., *Model-Companions and Definability in Existentially Complete Structures*, Israel Journal of Mathematics, 25, pp.305-330 (1976).

[19] Wolter F., *Fusions of Modal Logics Revisited*, in Kracht M., De Rijke M., Wansing H., Zakharyaschev M. (eds.) "Advances in Modal Logic", CSLI, Stanford (1998).