Recent Advances in Combined Decision Problems

Silvio Ghilardi Enrica Nicolini Daniele Zucchelli

Abstract

Questo articolo vuol essere un'esposizione aggiornata, benché necessariamente parziale, dello stato dell'arte della ricerca relativa all'integrazione modulare di procedure di decisione nella logica elementare. Nello specifico, date due teorie T_1 e T_2 il cui frammento universale è decidibile, si è interessati ad individuare quali siano le condizioni che permettono di trasferire tale decidibilità alla teoria ottenuta dall'unione di T_1 e T_2. Allo scopo di dare un quadro il più possibile completo ed approfondito delle ricerche in questo campo, vengono presentati anche risultati sulla possibilità di trasferire alla teoria unione la decidibilità del problema della parola e viene descritto un ambiente di ordine superiore in cui esprimere svariati problemi di combinazione. Infine, viene fornita la descrizione ad alto livello di alcune delle tecniche più comunemente utilizzate nell'implementazione di efficienti sistemi per la combinazione.

Many areas of computer science (like software and hardware verification, artificial intelligence, knowledge representation and even computational algebra) are interested in the study and in the development of combination and integration techniques for existing decision procedures: this is so because there is a need to reason in heterogeneous domains, so that modularity in combining and re-using algorithms and concrete implementations becomes crucial.

In this paper we consider two decision problems: first, given a first-order theory T in a signature Σ,[1] the *word problem* for T is that of deciding whether

$$T \models t = u$$

holds for the Σ-terms t and u. Second, the *constraint satisfiability problem* for T is the problem of deciding whether the conjunction of a finite set of Σ-literals is satisfiable in a model of T.

[1] All the signatures we consider are finite, and the equality symbol is considered as a logical symbol like boolean connectives and quantifiers.

An important remark is that constraint satisfiability is not the same as satisfiability of arbitrary first-order sentences: there is at least a great difference in complexity, even whenever both problems are decidable. One may observe that an equivalent formulation of the constraint satisfiability problem is the problem of deciding the consistency *modulo the theory* T of a conjunction of ground literals in the signature $\Sigma \cup A$, where A is a finite set of new constants.

Moreover, deciding the constraint satisfiability problem for a theory T means to be able to decide all the universal consequences of T: in fact, the complementary *constraint unsatisfiability problem* (i.e., the problem of deciding whether a finite set of Σ-literals is unsatisfiable in all the models of T) can be easily reduced to the *clausal word problem* for T (i.e. to the problem of deciding whether $T \models C$ holds for a Σ-clause C). This is because: a) the T-unsatisfiability of $A_1 \wedge \cdots \wedge A_n$ is the same as the relation $T \models \neg\exists\underline{x}(A_1 \wedge \cdots \wedge A_n)$ (for an appropriate existential closure prefix $\exists\underline{x}$), that is as the relation $T \models \forall\underline{x}(\neg A_1 \vee \cdots \vee \neg A_n)$; b) conversely, $T \models C$ (where C is the clause $B_1 \vee \cdots \vee B_m$) is equivalent to $T \models \forall\underline{x}C$ and hence to the T-unsatisfiability of $\neg B_1 \wedge \cdots \wedge \neg B_m$. From these considerations, it follows in particular that deciding constraint satisfiability problems means to be able to decide conditional equations and, therefore, solving the word problem.

In concrete applications, instead of a simple conjunction of literals, one is given a boolean combination of ground literals in an expanded signature $\Sigma \cup A$ to be tested for T-consistency. This is the reason why a solver for the constraint satisfiability problem has to be combined with a SAT-solver. The most commonly used SAT-solvers are those based on the calculus designed in the Davis, Putnam, Logemann and Loveland's famous work (see [16] and [31]).

In any involved area, the combination and integration of existing decision procedures are non trivial tasks mainly because of the heterogeneity of the techniques used by the component decision procedures. If we consider the theories which are suitable for software verification, decision procedures for the constraint satisfiability problems are obtained in many different ways: sometimes (for example when T is the empty theory, the theory of lists or the theory of arrays) the standard superposition calculus decides constraint satisfiability (see [2]), but in many other cases (for example whenever arithmetic constraints are involved) ad hoc procedures are needed.

If we move to the fields of artificial intelligence and knowledge representation, local and global satisfiability problems are decidable for various modal, temporal, dynamic and description logics. The *local satisfiability problem* is that of deciding whether

$$\mathcal{M} \models_w \varphi$$

holds for a propositional formula φ in a world w of a suitable (Kripke-like) model $\mathcal{M}$. By contrast, the *relativized satisfiability problem* is that of deciding whether $\mathcal{M} \models_w \varphi$ holds in a model $\mathcal{M}$ where another formula ψ is supposed to be true in all possible worlds. If the logic L we are concerned with is *'algebraizable'* (i.e. it corresponds to a variety V of boolean algebras with operators) and is *(strongly)*

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

Kripke complete for the intended class of models, then the local satisfiability problem is the complement of the word problem in a theory T_V axiomatizing the variety V; on the other hand, the relativized satisfiability problem is precisely the constraint satisfiability problem in the theory T_V.

As in the case of software verification, there are many different methods to get decidability for our local and global satisfiability problems: among such methods there are tableaux-based methods (more precisely, extensions of the DPLL algorithm which perform considerably well from a computational point of view), automata techniques, filtrations, mosaics, reductions to Rabin's tree theorem, translation to first-order fragments and so on. Again, the problem of combining such different techniques naturally arises.

1 Combining First-Order Constraints

Suppose we are given two first-order theories T_1 and T_2 over the signatures Σ_1 and Σ_2 respectively (notice that it may happen that the signatures Σ_1 and Σ_2 are non-disjoint). If we are able to solve the word problem (respectively the constraint satisfiability problem) in both T_1 and T_2, we wonder whether it is possible to solve the same problem in $T_1 \cup T_2$.

In order to be able to re-use any existing decision procedure, it is useful to adopt a so-called *black-box approach*. This means the following: we assume that a decision procedure $\mathcal{P}_1$ solves the problem for the theory T_1 and a decision procedure $\mathcal{P}_2$ solves the problem for the theory T_2. The provers $\mathcal{P}_1$ and $\mathcal{P}_2$ can exchange information only externally, according to a protocol to be specified: in any case, $\mathcal{P}_1$ and $\mathcal{P}_2$ cannot be internally modified.

The Nelson-Oppen Procedure

One of the simplest methodologies for the combination of decision procedures following the black-box approach is represented by the *Nelson-Oppen procedure* (see [25]), which was originally designed only for the disjoint signatures case. The Nelson-Oppen procedure can be summarized essentially in two steps, namely the *purification* preprocessing and the *exchange loop*.

Purification The preprocessing step consists in the transformation of the initial finite set Γ of $(\Sigma_1 \cup \Sigma_2 \cup A)$-ground literals into a set

$$\Gamma_1 \cup \Gamma_2$$

where (for some A') Γ_1 is a set of $(\Sigma_1 \cup A \cup A')$-ground literals and Γ_2 is a set of $(\Sigma_2 \cup A \cup A')$-ground literals. This transformation preserves satisfiability; in standard implementations, purification is linear (equations $c = t$, for new constants c and alien subterms t, are successively added).

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

Exchange Loop Whenever the decision procedure $\mathcal{P}_i$ ($i \in \{1,2\}$) finds a disjunction C of ground $(\Sigma_0 \cup A \cup A')$-atoms (here $\Sigma_0 := \Sigma_1 \cap \Sigma_2$) such that $\Gamma_i \cup \{\neg C\}$ is unsatisfiable modulo T_i, C is added to Γ_j ($j \in \{1,2\}, j \neq i$) if it is not already present.

Alternatively, one can limit the exchange to atoms instead of clauses: obviously case splitting and backtracking mechanisms are required. However, if the theories T_i are Σ_0-convex, the exchange of atoms becomes deterministic.[2]

The exchange loop returns *unsatisfiabile* if Γ_1 (or Γ_2) eventually becomes unsatisfiable modulo T_1 (modulo T_2, respectively). It returns *satisfiable* if it terminates without finding any inconsistency.

The deterministic Nelson-Oppen procedure is guaranteed to be terminating and complete under the following assumptions: (i) Σ_1 and Σ_2 are disjoint; (ii) the theories T_1 and T_2 are Σ_0-convex and (iii) they admit only non trivial models (i.e. only models having cardinality bigger than 1).[3] In the non deterministic case, we can eliminate assumption (iii) and weaken the convexity assumption (ii) to: (ii') the theories T_1 and T_2 are stably infinite. Here a theory T over the signature Σ is said to be *stably infinite* iff any quantifier-free Σ-formula φ which is satisfiable in a model of T is satisfiable in a model of T whose domain is infinite. It is interesting to notice that theories which are both convex and do not admit trivial models are also stably infinite (see [12]).

The above formulation of Nelson-Oppen procedure applies also to the case of non disjoint signatures, but some extra conditions are needed to guarantee termination and completeness (in general, completeness cannot be ensured by the mere exchange of information concerning $(\Sigma_0 \cup A)$-atoms, because Craig's interpolants may not have this form).

A first attempt to drop the assumption of disjointness of the signatures that is able to capture some relevant theories can be found in [20]. Let T_0 be a universal theory in the signature Σ_0 such that $T_0 \subseteq T_1$ and $T_0 \subseteq T_2$ (we can freely consider that T_0 is always given: in fact, in applications T_0 will be the universal Σ_0-reduct of T_1 and T_2). To guarantee the termination of the procedure, it is sufficient to assume T_0 to be locally finite: a universal theory T_0 over the signature Σ_0 is *locally finite* iff Σ_0 is finite and for every finite set A of new free constants, one can compute finitely many $(\Sigma_0 \cup A)$-ground terms $t_1, \ldots, t_{n_A}$ such that for every further $(\Sigma_0 \cup A)$-ground term u, we have $T_0 \models u = t_i$ (for some $i \in \{1, \ldots, n_A\}$). Local finiteness trivially holds when Σ_1 and Σ_2 are disjoint, but it holds in many other interesting situations, for instance when T_0 is the theory of Boolean algebras (this is the relevant case for applications to fusion decidability transfer in modal logic, see below).

[2] Following [30], a theory T on the signature Σ is said to be Σ_0-convex ($\Sigma_0 \subseteq \Sigma$) iff whenever $T \cup \Gamma \models A_1 \vee \cdots \vee A_n$ (for a finite set of $\Sigma \cup A$-literals Γ, for $n \geq 1$ and for ground $\Sigma_0 \cup A$-atoms $A_1, \ldots, A_n$), there is $k \in \{1, \ldots, n\}$ such that $T \cup \Gamma \models A_k$.

[3] The latter is not a real limitation: it is easy to adjust our deterministic procedure in order to drop it.

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

On the other hand, a sufficient hypothesis for completeness is T_0-compatibility: we say that T_i is T_0-*compatible* iff T_0 has a model completion $T_0^\star$ (see [15]) and every model of T_i embeds into a model of $T_i \cup T_0^\star$.

Theorem ([20]). *Under the assumption of local finiteness of T_0 and of T_0-compatibility of T_1 and T_2, the Nelson-Oppen procedure decides the constraint satisfiability for $T_1 \cup T_2$.*

In the case of disjoint signatures, T_0-compatibility of T_i means that models of T_i embeds into infinite models of T_i, thus recovering the stable infiniteness hypothesis of the original non-deterministic Nelson-Oppen procedure. Moreover, every variety of Boolean algebras with operators is BA-compatible (where BA is the theory of Boolean algebras): this observation is sufficient to prove algebraically the well-known fusion transfer result for decidability of global consequence relation in modal logic (see [33]). Refined version of the above theorem may be integrated in standard superposition calculus, with the aim of blocking inferences involving mixed signature clauses (see [20] again).

The Shostak Procedure

Shostak defined a class of theories that are "solvable" and "canonizable", i.e. theories that admit procedures for reducing terms to canonical forms and algorithms for solving equations (see [29]). The interest in that class relies in the fact that *canonizers* and *solvers* represent efficient ways to derive entailed equalities.

However, there are two main drawbacks in Shostak theories: first, under some reasonable assumptions, if the union $T_1 \cup T_2$ of the stably infinite theories T_1 and T_2 admits canonizer, then $T_1 \cup T_2$ does not have a solver (see [24]). Second, the theory of equality (ubiquitous in virtually any application where combination of procedures are needed) does not admit a solver.

In [29] a procedure to decide the universal fragment of the theory of equality that can be combined with decision procedures for solvable and canonizable theories is introduced. Although being implemented in several theorem provers, only recently the theory underlying Shostak's method has been enlightened by presenting it in a more abstract and transparent way, thus exploiting the relationships between the Nelson-Oppen and the Shostak schemata: in many works the latter is seen as a refinement of the former. For example, the relation between Nelson-Oppen and Shostak schemata already hinted in [18] seems to be fully exploited in [19]; on the other hand, a method for the composition of the two procedures has been suggested in [27].

It is interesting to note that in [18] the following general result is presented:

Theorem ([18]). *Let T be a Σ-theory such that the constraint satisfiability problem for T is decidable. Then, for every signature $\Omega \supseteq \Sigma$, the constraint satisfiability problem for T with respect to Ω-literals is decidable.*

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

Moreover, in [19] is presented a general schema (which includes the Nelson-Oppen procedure as an instance) for combination of decision procedures for first-order theories in which every decision procedure is formalized as an inference system, and their combination is formalized through the so-called inference modules.

More in detail, an *inference system* for a theory T is given in terms of logical state and inference rules; usually a logical state is interpreted as a disjunction of conjunctions of formulas, and the requirements on the inference rules are that they keep equi-satisfiability, induce a well founded order on the set of logical states and, if no inference rules can be applied to a logical state, then that state is either T-satisfiable or is equal to $\bot$.

An *inference module* is the formal description of an inference system in which every state is made up by the pair local state/shared state. The shared state is interpreted as an interface for inputs and outputs that guarantees different modules to exchange formulas on a shared signature. The method for combining decision procedures is formalized by defining the composition operator which allows two modules to communicate each other through the shared state. The original Nelson-Oppen procedure and the combination method arising from the results in [20] can be seen as instances of the combination of inference modules.

Moreover, the notion of *modular refinement* is used to compare two inference modules $\mathcal{I}$, $\mathcal{J}$: the exact definition is quite technical, but it can be summarized saying that $\mathcal{I}$ refines $\mathcal{J}$ if every inference step in $\mathcal{I}$ can be 'simulated' by inference steps in $\mathcal{J}$. As a relevant example, the Shostak procedure is shown to be a modular refinement of the Nelson-Oppen one.

Further Extensions

As already said, the standard superposition calculus can decide the constraint satisfiability problem for some computer science motivated theories (see [1]). It is interesting to note that, under some technical assumptions, superposition calculus can also become a satisfiability decision procedure for a theory of the kind $\bigcup_{i=1}^{n} T_i$, where T_i's do not share function symbols and the constraint satisfiability problem for each T_i is decidable by superposition (for this purpose, see [3]).

In the case of disjoint signatures, some attempts have been made to drop the stable infiniteness limitation of the original Nelson-Oppen procedure: this is mainly because many interesting theories, such as those admitting only finite models, are not stably infinite. For example, in [32], an asymmetric procedure that does not require stable infiniteness for the component theories is introduced: the method works by propagating equality constraints as well as a minimal cardinality constraint.

The 'dual' notion of stable infiniteness is stable finiteness: a Σ-theory T is *stably finite* iff every T-satisfiable quantifier-free Σ-formula φ is satisfiable in a model of T whose domain is finite.

The theory T is *smooth* iff for every quantifier-free Σ-formula φ, for every

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

model $\mathcal{M}$ of T satisfying φ and for every cardinal number $\kappa > |\mathcal{M}|$ there exists a model $\mathcal{N}$ of T satisfying φ such that $|\mathcal{N}| = \kappa$; moreover, T is *shiny* iff (i) T is smooth; (ii) T is stably finite; (iii) $mincard_T$ is computable (this is the function that, once applied to a T-satisfiable conjunction Γ of Σ-literals, returns the minimal cardinality k of a model satisfying Γ).

Theorem ([32]). *Let $T = T_1 \cup \cdots \cup T_n$ be the union of pairwise signature-disjoint theories such that: (i) T_1 is arbitrary; (ii) $T_2, \ldots, T_n$ are shiny. If all the constraint satisfiability problems for $T_1, \ldots, T_n$ are decidable, so does the constraint satisfiability problem for T.*

An interesting fact is that for every signature Ω, the empty Ω-theory is shiny, thus immediately getting as a corollary the theorem in [18] cited above.

Another attempt to weaken the stable infiniteness requirement can be found in [28]. This paper concerns theories of practical interest for software verification: in this context, combination problems often involve a first theory S modeling a certain data structure (such as lists, arrays, sets, multisets and so on) considered as structured container for elements modeled by a second theory T. Unfortunately, many of the theories used in the software verification area are not stably infinite, like for instance the theory of integers modulo n or the theory of fixed-width bit-vectors.

Relying on the notion of politeness of a theory S with respect to a theory T, a procedure that is able to combine a polite theory S with any theory T, regardless whether T is stably infinite or not, is provided. Moreover, two drawbacks of [32] are addressed: the $\mathcal{NP}$-hard function $mincard_S$ is replaced by the function $witness_S$; furthermore, a generalization of the notion of a shiny theory (too strong to include many practically relevant examples) is provided within a many-sorted framework.

Instead of examining the union of two theories, it is possible to consider their *connection*. Suppose that the theories T_1 and T_2 are many-sorted and that they share some sorts as well as some functions and predicates; to obtain their connection, one (i) renames the shared symbols, (ii) takes (disjoint) union of symbols and axioms, and (iii) adds *connecting function symbols*, together with axioms saying that they are interpreted as homomorphisms among the reducts to the originally shared signature. In this way a new schema of combination is obtained: under appropriate 'algebraic' conditions, explained in [5] and in [4], decidability of constraint satisfiability problems transfers from the component theories to their connection.

2 A Comprehensive Framework for Combination

Nelson-Oppen methodology can be pushed further in order to solve in a uniform way as many problems as possible: when joined to model-theoretic results, it

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

succeeds in dealing with various classes of combination problems, often quite far from the originally intended application domain.

In this perspective, the Nelson-Oppen schema has been plugged into an higher-order framework: in [22], type-theoretic signatures in Church's style are adopted. The choice of a higher-order framework is justified by the fact that quite often the semantic specification language for decision problem is intrinsically higher-order, even if in practice problems themselves are not really such. For example, in the case of modal logic, decision problems are specified through so-called standard translations: clearly, the problem of finding a structure satisfying the standard translation of a modal formula is (at least in principle) higher-order because the predicates symbols occurring in the problem are genuine second order variables.

The interest of this approach relies on existence of tractable fragments of general type theory whose 'combination' often turns out to be tractable too. To develop the plan of plugging Nelson-Oppen procedure into a higher-order context, a suitable notion of a fragment is needed. An *algebraic fragment* is a pair $\langle \mathcal{L}, T \rangle$ where T is a recursive set of terms (of the higher-order typed language $\mathcal{L}$) which (i) is closed under substitution of terms from T for terms from T, and (ii) contains all variables of any type τ, which is either the type of some $t \in T$ or the type of a variable occurring free in some $t \in T$. An algebraic fragment can be endowed with a class $\mathcal{S}$ of structures closed under isomorphisms, thus defining what we call an *interpreted algebraic fragment*[4] (or, sometimes, a *fragment* tout court)

$$\Phi = \langle \mathcal{L}, T, \mathcal{S} \rangle.$$

In this framework, a constraint satisfiability problem for Φ is reformulated as the problem of deciding whether a Φ-constraint (i.e. a finite conjunction of equations and inequations between Φ-terms) is satisfiable in some structure $\mathcal{M} \in \mathcal{S}$.

Let's now analyze the problem of transferring decidability of constraints satisfiability problems from given fragments Φ_1, Φ_2 - sharing a certain fragment Φ_0 - to their combination $\Phi_1 \oplus \Phi_2$ (shared and combined fragments are defined in the expected way). Our definition of a fragment is sufficient to substantially reproduce Nelson-Oppen steps, but we still have to face termination and completeness issues: for these, additional hypotheses are needed. Such hypotheses will be formulated as hypotheses that each of the Φ_1, Φ_2 *separately* must satisfy with respect to Φ_0.

In general, we say that a fragment $\Phi = \langle \mathcal{L}, T, \mathcal{S} \rangle$ is an *extension* of $\Phi_0 = \langle \mathcal{L}_0, T_0, \mathcal{S}_0 \rangle$ iff $\mathcal{L}_0 \subseteq \mathcal{L}$, $T_0 \subseteq T$ and all the $\mathcal{L}_0$-reducts of the structures from $\mathcal{S}$ belong to $\mathcal{S}_0$.

Below, we shall need to consider *simple expansions* of an interpreted algebraic fragment Φ_0: these are the interpreted algebraic fragments of the kind $\Phi_0(A) = \langle \mathcal{L}_0(A), T_0(A), \mathcal{S}_0(A) \rangle$ obtained from $\Phi_0 = \langle \mathcal{L}_0, T_0, \mathcal{S}_0 \rangle$ by expanding

[4] The idea of using a class of models to introduce satisfiability problems (instead of specifying syntactically a theory) is recent and seems to be promising (see also [18, 28]).

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

the signature $\mathcal{L}_0$ with finitely many fresh constants A of appropriate types (T_0 and $\mathcal{S}_0$ are accordingly 'expanded' to respectively $T_0(A)$ and $\mathcal{S}_0(A)$ in the obvious way).

In order to ensure termination, one can once again assume a suitable local finiteness property for the shared fragment Φ_0. However, local finiteness can be weakened to noetherianity: a fragment Φ_0 is *noetherian* iff, for every finite set of variables $\underline{x}$, every infinite ascending chain

$$\Theta_1 \subseteq \Theta_2 \subseteq \cdots \subseteq \Theta_n \subseteq \cdots$$

of sets of equation between Φ_0-terms over the variables $\underline{x}$ is eventually constant for Φ_0-consequence (meaning that there is an n such that for all m and $A \in \Theta_m$, we have $\mathcal{M} \models A$ for every $\mathcal{M} \in \mathcal{S}_0$ such that $\mathcal{M} \models \Theta_n$). Noetherianity notion is borrowed from algebra: in fact, conditional word problems arising in computational algebra for suitable 'noetherianly-behaved' classes of structures can be turned into constraint satisfiability problems for noetherian fragments in our sense.

To exploit noetherianity of the shared fragment Φ_0 in a combined constraint satisfiability problem, we need the following definition.[5] Φ is said to be a *noetherian expansion of* Φ_0 iff: (i) Φ_0 is noetherian; (ii) Φ is an extension of Φ_0; (iii) a suitable relative compactness property is satisfied and (iv) there exists a computational device enumerating (up to redundancy) the Φ_0-positive clauses which are Φ-consequences of a set of Φ-constraints Γ.

The T_0-compatibility requirement in [20] is recaptured in the following way. We say that $\Phi_0^\star = \langle \mathcal{L}_0, T_0, \mathcal{S}_0^\star \rangle$ is a *specialization* of $\Phi_0 = \langle \mathcal{L}_0, T_0, \mathcal{S}_0 \rangle$ iff $\mathcal{S}_0 \subseteq \mathcal{S}_0^\star$ and for every finite set A of constants of appropriate types, for every structure $\mathcal{M} \in \mathcal{S}_0(A)$, there exists $\mathcal{M}' \in \mathcal{S}_0^\star(A)$ such that $\mathcal{M}$ and $\mathcal{M}'$ satisfy the same $\Phi_0(A)$-closed atoms. Moreover, a fragment $\Phi = \langle \mathcal{L}, T, \mathcal{S} \rangle$ extending Φ_0 is *compatible* with respect to a given specialization $\Phi_0^\star$ of Φ_0 iff $\Phi^\star = \langle \mathcal{L}, T, \mathcal{S}^\star \rangle$ is a specialization of Φ, where $\mathcal{S}^\star$ contains exactly those $\mathcal{L}$-structures from $\mathcal{S}$ whose $\mathcal{L}_0$-reduct belongs to $\mathcal{S}_0^\star$.

To guarantee the completeness of the combination procedure in our context, Craig Interpolation Theorem is replaced by powerful model-theoretic and semantically driven tools, the so-called *structural operations*: a structural operation on a fragment $\Phi = \langle \mathcal{L}, T, \mathcal{S} \rangle$ is a family of correspondences (varying A) $O_A : \mathcal{S}(A) \to \mathcal{S}(A)$ such that $\mathcal{M}$ and $O_A(\mathcal{M})$ satisfy the same $\Phi(A)$-closed atoms.

To be useful, these structural operations are required to admit an isomorphism theorem. Roughly speaking, an isomorphism theorem is a theorem saying that the application of certain semantic operation makes $\mathcal{L}(A)$-isomorphic two structures which satisfy the same $\Phi(A)$-atoms. An example of structural oper-

[5] This definition is explained here only in a qualitative way for space reasons, see [22] for details. We remark that in case Φ_0 is locally finite, the notion of a noetherian expansion trivializes to that of an expansion.

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

ations admitting an isomorphism theorem (for fragments consisting of all first-order formulas interpreted in an elementary class) are ultrapowers: *Keisler-Shelah isomorphism theorem* (see [15]) proves that two $\mathcal{L}(A)$-models $\mathcal{A}$ and $\mathcal{B}$ are elementarily equivalent iff there is an ultrafilter $\mathcal{U}$ such that the ultrapowers $\prod_{\mathcal{U}} \mathcal{A}$ and $\prod_{\mathcal{U}} \mathcal{B}$ are $\mathcal{L}(A)$-isomorphic. Another example of isomorphism theorem, operating on certain monadic first-order fragments, is given by disjoint unions (this is the isomorphism theorem useful to get fusion decidability transfer results in modal logic).

More formally, a collection $\mathcal{O}$ of structural operations for $\Phi = \langle \mathcal{L}, T, \mathcal{S} \rangle$ admits a Φ-*isomorphism theorem* iff for every finite set of free constants A and for every $\mathcal{M}, \mathcal{N} \in S(A)$ satisfying the same $\Phi(A)$-closed atoms, there exist two operations $O, O' \in \mathcal{O}$ such that the structures $O_A(\mathcal{M})$ and $O'_A(\mathcal{N})$ are $\mathcal{L}(A)$-isomorphic.

If Φ' is an extension of the fragment Φ, the structural operation O is Φ'-*extensible* iff the following happens: after applying O to the $\mathcal{L}(A)$-reduct of a certain $\Phi'(A')$-structure $\mathcal{M}$, one is always guaranteed to obtain a structure that is $\mathcal{L}(A)$-isomorphic to the $\mathcal{L}(A)$-reduct of a $\Phi'(A')$-structure $\mathcal{N}$ satisfying the same $\Phi'(A')$-closed atoms as $\mathcal{M}$.[6] We can now state a general decidability transfer result:

Theorem ([22])**.** *Nelson-Oppen procedure decides combined constraint satisfiability for $\Phi_1 \oplus \Phi_2$ under the assumption that: (i) Φ_1, Φ_2 have decidable constraint satisfiability problems; (ii) Φ_1, Φ_2 are both noetherian extensions of their shared fragment Φ_0; (iii) Φ_1, Φ_2 are Φ_0-compatible with respect to a specialization $\Phi_0^\star$ of Φ_0; (iv) there is a collection $\mathcal{O}$ of $\Phi_1^\star$- and $\Phi_2^\star$-extensible structural operations admitting a $\Phi_0^\star$-isomorphism theorem.*

This general decidability transfer result covers as special cases, besides new applications, the aforesaid extension of Nelson-Oppen procedure to non-disjoint signatures, the fusion transfer for decidability of global consequence relation in modal logic, and the fusion transfer of decidability of A-Boxes with respect to T-Boxes axioms in local abstract description systems (see [11]); in addition, it reduces decidability of modal and temporal monodic fragments to their extensional (i.e. non modal) and one-variable components (see [33]).

3 Combined word problems

Let us now turn to the first-order context and examine the case of combined word problems. We wish to solve combined word problems in the union $T_1 \cup T_2$ of two first-order theories T_1 and T_2 by adopting the usual black-box approach: the first idea is that of using the Nelson-Oppen procedure as it is (purification plus information exchange concerning shared equations), but this is inadequate,

[6] Here $A \subseteq A'$ denotes the set of those constants in A' whose type is the type of a Φ-variable.

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

because a new difficulty arises. This is because *conditional* word problems are necessarily generated in non trivial cases of combination and it can happen that the input algorithms are not able to handle them (they are supposed to solve just plain word problems). However, even if combined word problems are more difficult for the above-mentioned reason, there are two orthogonal results that allows us to give positive solutions under suitable hypotheses (the general case is known to lead to undecidability).

The first result is due to [7] (and, independently, to [17]). We suppose that T_1 and T_2 are both equational theories (in the signatures Σ_1 and Σ_2 respectively) and that they are also conservative extensions of a shared equational theory T_0 in the signature $\Sigma_0 = \Sigma_1 \cap \Sigma_2$. Moreover, T_1 and T_2, must be *constructible* over T_0; this means that (for $i \in \{1, 2\}$) there exists a class G_i of Σ_i-terms (containing variables and closed under renamings) such that every Σ_i-term factors (uniquely modulo T_i) as $u(g_1, \ldots, g_n)$, where $g_i \in G_i$ and u is a Σ_0-term. In order to obtain a real algorithm for the solution of combined word problems, this factorization must be effective.

Theorem ([7],[17])**.** *If the equational theories T_1 and T_2 are both constructible over a shared theory T_0, then word problem decidability transfers from T_1 and T_2 to the combined theory $T_1 \cup T_2$.*

Both proofs are complex, although based on different techniques: the proof given by [7] uses a careful and deep modification (based on transformation rules) of the Nelson-Oppen procedure, whereas the proof by [17] makes use of Knuth-Bendix completion over pushout presentations of categories with products. There are many examples of theories fulfilling the constructibility hypothesis of the above theorem: for instance, commutative rings with unit are constructible over abelian groups, abelian groups endowed with an endomorphism are constructible over abelian groups, differential rings are constructible over commutative rings with unit, etc.

Instead of constructibility, the main ingredient of the second combination result for word problems is the requirement of gaussianity of the shared equational theory T_0.

A first order formula is an *e-formula* if it is a conjunction of equations, and a first order theory T is *gaussian* iff for every e-formula $\varphi(\underline{x}, y)$ one can effectively determine an e-formula $C(\underline{x})$ and a term $s(\underline{x}, \underline{z})$ with fresh variables $\underline{z}$ such that

$$T \models \varphi(\underline{x}, y) \leftrightarrow [C(\underline{x}) \wedge \exists \underline{z}(y = s(\underline{x}, \underline{z}))] .$$

The formula $C(\underline{x})$ is called the *solvability condition* of $\varphi(\underline{x}, y)$ with respect to y, and the term $s(\underline{x}, \underline{z})$ a *(local) solver* of $\varphi(\underline{x}, y)$ with respect to y.

Among examples of gaussian theories we can mention the empty theory in the empty signature and the theories of K-vector spaces,[7] acyclic lists, and

[7] Here the property at issue is a consequence of the Gauss elimination algorithm, whence the name 'gaussian'.

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

Boolean rings. In the latter case, classical results on boolean unification show that the solver of the formula $t(\underline{x}, y) = 0$ is $z + t(\underline{x}, z) * (1 + t(\underline{x}, 1) * t(\underline{x}, 0)) * (z + 1 + t(\underline{x}, 1))$.

The combination theorem now can be stated as follows (T_1 and T_2 are still equational theories on signatures Σ_1 and Σ_2 respectively, and T_0 is a shared theory in the signature $\Sigma_0 = \Sigma_1 \cap \Sigma_2$):

Theorem ([9]). *Word problem decidability transfers from T_1, T_2 to $T_1 \cup T_2$, under the hypothesis that: (i) T_0 is locally finite; (ii) T_1 and T_2 are both T_0-compatible conservative extensions of T_0; (iii) T_0 is gaussian.*

The combination algorithm can be outlined as follows: first of all, two convergent rewriting systems for Σ_1- and Σ_2-ground terms (with purification constants) are induced by the Nelson-Oppen purification procedure; then the information exchange of equations is turned into a rewrite rules exchange through skolemized solvers; at the end of the exchange process, normalization by any of the two final rewriting systems decides the input word problem. The termination of this algorithm is guaranteed mainly by the assumption of the local finiteness of the shared theory; moreover, the updating of the two rewriting systems is designed in such a way that it keeps them convergent.

A corollary of this theorem is an unlimited fusion transfer of decidability for (classical) modal logics: it is indeed a quite strong result, because the question about decidability transfer was a long standing open problem for the non normal case. We finally remark that the theorems described in this section both regain, as particular case, the transfer decidability result for the disjoint signatures case, see [26].

4 Implemented Systems for Combination

We have already hinted at some systems for satisfiability modulo theories: these systems are able to deal with the problem of the satisfiability of boolean combinations (not simply of conjunctions) of ground literals with respect to background theories for which specialized decision procedures exist.[8] Among such theories there are the theory of lists, of arrays, and linear arithmetic; examples of systems are the following:

- Argo-lib (`http://www.matf.bg.ac.yu/~janicic/argo/`);
- DPLL(T) (`http://www.lsi.upc.es/~oliveras/`);
- CVC Lite (`http://verify.stanford.edu/CVCL/`);
- haRVey (`http://www.loria.fr/equipes/cassis/softwares/haRVey/`);

[8] Such background theories have disjoint signatures in the existing implementations.

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

- ICS (`http://www.icansolve.com/`);
- Math-SAT (`http://mathsat.itc.it/`);
- Tsat++ (`http://argo.lira.dist.unige.it/drwho/Tsat/`);
- UCLID (`http://www.cs.cmu.edu/~uclid/`).

The general idea is to integrate a boolean solver (usually based on DPLL algorithm) with a satisfiability procedure for a theory T (see for example [31]). The systems are based on a cycle consisting of the following steps: (a) the input formula φ which has to be tested for satisfiability modulo T is 'abstracted' into a propositional formula φ^p; (b) the boolean solver enumerates the propositional assignment satisfying φ^p that can be 're-instantiated' as a conjunction of literals; (c) each conjunction of literals is checked for T-satisfiability. The advantage of this idea is that the satisfiability procedure is not invoked whenever the inconsistency can be detected at a propositional level.

The above schema is usually refined to minimize the (generally unavoidable) exponential blow-up determined by the exponentially many calls to the decision procedure for T: suppose that the satisfiability procedure, besides returning messages establishing the satisfiability status for the input set of literals, it is also capable of return a 'minimal' (as far as possible) subset π of them which is still unsatisfiable (this set is called *conflict set*). One can use the negation of the (abstraction of the) conflict set to lead the DPLL procedure to 'prune' all the satisfiable propositional assignments that are eventually unsatisfiable modulo the theory T: this technique is very useful in practice, and makes these systems well-performing.

Nevertheless, this approach implies some further difficulties whenever it is used in a combination context, in particular with respect to the generation of the conflict set. Given two satisfiability decision procedures for T_1 and T_2 both capable of generating conflict sets, and a satisfiability procedure for the theory $T = T_1 \cup T_2$ built up by the Nelson-Oppen combination schema, the problem of generating conflict sets for T immediately arises. In fact, the purification process naturally enlarge the signature introducing new constants: in order to map the conflict set on the extended signature to a subset of the original set of literals on the signature of T one needs to 'track' the equalities exchanged by the two procedures.

Recently, a new approach overcomes the complexity of building conflict sets and has the further advantage of avoiding backtracking when handling non-convex theories. In this approach, called *Delayed Theory Combination* (see [13]), the idea is to use DPLL to generate a propositional assignment not only for (the abstraction of) the input formula, but also for (the abstraction of) the Robinson diagram over the shared signature (extended by the symbols introduced by the purification step, if necessary). The communication between the satisfiability procedures is no more necessary, because it is done via the SAT solver which guesses

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

(an abstraction of) a Robinson diagram and passes the resulting conjunction of literals to both procedures so that they can agree on the shared variables. The generation of the Robinson diagrams is lead by the decision procedures (using conflict sets technique described above) to avoid the investigation of all possible (exponentially many) Robinson diagrams.

For further information about implemented systems for combination and initiatives on this area, it is possible to consult the web page of the *Satisfiability Modulo Theory Library* (`http://combination.cs.uiowa.edu/smtlib/`). A library of examples and a benchmark suite for system evaluations are available; moreover, the competition SMT-COMP is periodically organized.

Acknowledgments

The authors are very grateful to Silvio Ranise for his useful comments and suggestions on a preliminary draft of this paper.

Bibliography

[1] Alessandro Armando, Silvio Ranise, and Michaël Rusinowitch. Uniform derivation of decision procedures by superposition. In Laurent Fribourg, editor, *Proceedings on the Annual Conference on Computer Science Logic (CSL01)*, volume 2142 of *Lecture Notes in Computer Science*, pages 513–527. Springer-Verlag, 2001.

[2] Alessandro Armando, Silvio Ranise, and Michaël Rusinowitch. A rewriting approach to satisfiability procedures. *Information and Computation*, 183(2): 140–164, 2003.

[3] Alessandro Armando, Maria Paola Bonacina, Silvio Ranise, and Stephan Schulz. On a rewriting approach to satisfiability procedures: extension, combination of theories and an experimental appraisal. In Bernhard Gramlich, editor, *Proceedings of the Fifth International Workshop on Frontiers of Combining Systems (FroCoS-05)*, volume 3717 of *Lecture Notes in Artificial Intelligence*, pages 65–80. Springer-Verlag, 2005.

[4] Franz Baader and Silvio Ghilardi. Connecting many-sorted theories. In *Proceedings of the 20th International Conference on Automated Deduction (CADE-05)*, Lecture Notes in Artificial Intelligence, Tallinn (Estonia), 2005. Springer-Verlag.

[5] Franz Baader and Silvio Ghilardi. Connecting many-sorted structures and theories through adjoint functions. In *Proceedings of the 5th International Workshop on Frontiers of Combining Systems (FroCoS-05)*, Lecture Notes in Artificial Intelligence, Wien (Austria), 2005. Springer-Verlag.

[6] Franz Baader and Cesare Tinelli. Combining equational theories sharing non-collapse-free constructors. In H. Kirchner and Ch. Ringeissen, editors,

Proceedings of the 3rd International Workshop on Frontiers of Combining Systems, FroCoS'2000, Nancy (France), volume 1794 of *Lecture Notes in Artificial Intelligence*, pages 260–274. Springer-Verlag, 2000.

[7] Franz Baader and Cesare Tinelli. Deciding the word problem in the union of equational theories. *Information and Computation*, 178(2):346–390, December 2002.

[8] Franz Baader and Cesare Tinelli. Deciding the word problem in the union of equational theories sharing constructors. In P. Narendran and M. Rusinowitch, editors, *Proceedings of the 10th International Conference on Rewriting Techniques and Applications (Trento, Italy)*, volume 1631 of *Lecture Notes in Computer Science*, pages 175–189. Springer-Verlag, 1999.

[9] Franz Baader, Silvio Ghilardi, and Cesare Tinelli. A new combination procedure for the word problem that generalizes fusion decidability results in modal logics. *Information and Computation*. (To appear).

[10] Franz Baader, Silvio Ghilardi, and Cesare Tinelli. A new combination procedure for the word problem that generalizes fusion decidability results in modal logics. In *Proceedings of the Second International Joint Conference on Automated Reasoning (IJCAR'04)*, volume 3097 of *Lecture Notes in Artificial Intelligence*, pages 183–197, Cork (Ireland), 2004. Springer-Verlag.

[11] Franz Baader, Carsten Lutz, Holger Sturm, and Frank Wolter. Fusions of description logics and abstract description systems. *Journal of Artificial Intelligence Research*, 16:1–58, 2002.

[12] Clark W. Barrett, David L. Dill, and Aaron Stump. A generalization of Shostak's method for combining decision procedures. In A. Armando, editor, *Proceedings of the 4th International Workshop on Frontiers of Combining Systems, FroCoS'2002 (Santa Margherita Ligure, Italy)*, volume 2309 of *Lecture Notes in Computer Science*, pages 132–147, 2002.

[13] Marco Bozzano, Roberto Bruttomesso, Alessandro Cimatti, Tommi Junttila, Peter van Rossum, Silvio Ranise, and Roberto Sebastiani. Efficient theory combination via boolean search. *Information and Computation*. (To appear).

[14] Marco Bozzano, Roberto Bruttomesso, Alessandro Cimatti, Tommi Junttila, Peter van Rossum, Silvio Ranise, and Roberto Sebastiani. Efficient satisfiability modulo theories via delayed theory combination. In *Proceedings of the 17th International Conference on Computer Aided Verification (CAV-05)*, volume 3576 of *Lecture Notes in Computer Science*. Springer-Verlag, 2005.

[15] Chen-Chung Chang and H. Jerome Keisler. *Model Theory*. North-Holland, Amsterdam-London, 3rd edition, 1990.

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

[16] Martin Davis, George Logemann, and Donald Loveland. A machine program for theorem-proving. *Communications of the ACM*, 5(7):394–397, 1962.

[17] Camillo Fiorentini and Silvio Ghilardi. Combining word problems through rewriting in categories with products. *Theoretical Computer Science*, 294: 103–149, 2003.

[18] Harald Ganzinger. Shostak light. In A. Voronkov, editor, *Proceedings of the 18th International Conference on Automated Deduction*, volume 2392 of *Lecture Notes in Computer Science*, pages 332–346. Springer-Verlag, July 2002.

[19] Harald Ganzinger, Harald Rueß, and Natarajan Shankar. Modularity and refinement in inference systems. In *Notes of the Third Workshop on Pragmatics of Decision Procedures in Automated Reasoning (PDPAR'05), colocated with the Seventeenth International Conference on Computer Aided Verification (CAV'05)*, Edinburgh (Scotland), July 2005.

[20] Silvio Ghilardi. Model-theoretic methods in combined constraint satisfiability. *Journal of Automated Reasoning*, 33(3–4):221–249, 2005.

[21] Silvio Ghilardi. Quantifier elimination and provers integration. In Ingo Dahn and Laurent Vigneron, editors, *Proceedings of the 4th International Workshop on First-Order Theorem Proving, FTP 2003*, Valencia, Spain, 2003. Published as Volume 86, Issue 1, of the Electronic Notes in Theoretical Computer Science.

[22] Silvio Ghilardi, Enrica Nicolini, and Daniele Zucchelli. A comprehensive framework for combined decision procedures. In Bernhard Gramlich, editor, *Proceedings of the Fifth International Workshop on Frontiers of Combining Systems (FroCoS-05)*, volume 3717 of *Lecture Notes in Artificial Intelligence*, pages 1–30, Vienna (Austria), 2005. Springer-Verlag.

[23] Silvio Ghilardi, Enrica Nicolini, and Daniele Zucchelli. A comprehensive framework for combined decision procedures. Rapporto Interno 304-05, Dipartimento di Scienze dell'Informazione - Università degli Studi di Milano, Milano (Italy), 2005. Available at http://homes.dsi.unimi.it/~zucchell/publications/techreport/GhiNiZuRI304-05.pdf.

[24] Sava Krstić and Sylvain Conchon. Canonization for disjoint unions of theories. In Franz Baader, editor, *Proceedings of the 19th International Conference on Automated Deduction (CADE-19)*, volume 2741 of *Lecture Notes in Computer Science*, Miami Beach, FL, USA, July 2003. Springer Verlag.

[25] Greg Nelson and Derek C. Oppen. Simplification by cooperating decision procedures. *ACM Trans. on Programming Languages and Systems*, 1(2): 245–257, October 1979.

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

[26] Don Pigozzi. The join of equational theories. *Colloquium Mathematicum*, 30(1):15–25, 1974.

[27] Silvio Ranise, Cristophe Ringeissen, and Duc-Khanh Tran. Nelson-Oppen, Shostak, and the extended canonizer: A family picture with a newborn. In *First International Colloquium on Theoretical Aspects of Computing (ICTAC'04)*, volume 3407 of *Lecture Notes in Computer Science*, Guiyang (China), September 2004. Springer-Verlag.

[28] Silvio Ranise, Christophe Ringeissen, and Calogero 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-05)*, Lecture Notes in Artificial Intelligence, Vienna (Austria), 2005. Springer-Verlag.

[29] Robert E. Shostak. Deciding combinations of theories. *Journal of the ACM*, 31:1–12, 1984.

[30] Cesare Tinelli. Cooperation of background reasoners in theory reasoning by residue sharing. *Journal of Automated Reasoning*, 30(1):1–31, January 2003.

[31] Cesare Tinelli. A DPLL-based calculus for ground satisfiability modulo theories. In Giovambattista Ianni and Sergio Flesca, editors, *Proceedings of the 8th European Conference on Logics in Artificial Intelligence (Cosenza, Italy)*, volume 2424 of *Lecture Notes in Artificial Intelligence*. Springer, 2002.

[32] Cesare Tinelli and Calogero Zarba. Combining non-stably infinite theories. *Journal of Automated Reasoning*, 2005. (To appear).

[33] Frank Wolter. Fusions of modal logics revisited. In M. Kracht, M. de Rijke, H. Wansing, and M. Zakharyaschev, editors, *Advances in Modal Logic*. CSLI, Stanford, CA, 1998.

Silvio Ghilardi
Dipartimento di Scienze dell'Informazione
Università degli Studi di Milano
Via Comelico, 39 - 20135 Milano, Italy
e-mail: ghilardi@dsi.unimi.it
web-site: `http://homes.dsi.unimi.it/~ghilardi/`

Enrica Nicolini
Dipartimento di Matematica
Università degli Studi di Milano
Via Saldini, 50 - 20133 Milano, Italy
e-mail: nicolini@mat.unimi.it

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*

Daniele Zucchelli
Dipartimento di Scienze dell'Informazione
Università degli Studi di Milano
Via Comelico, 39 - 20135 Milano, Italy
e-mail: zucchelli@dsi.unimi.it
web-site: `http://homes.dsi.unimi.it/~zucchell/`

E. Ballo, M. Franchella (eds) *Logic and Philosophy in Italy*