

INTERPOLATION IN LOCAL THEORY EXTENSIONS

VIORICA SOFRONIE-STOKKERMANS

Max-Planck-Institut für Informatik, Campus E1.4, Saarbrücken, Germany
e-mail address: sofronie@mpi-inf.mpg.de

ABSTRACT. In this paper we study interpolation in local extensions of a base theory. We identify situations in which it is possible to obtain interpolants in a hierarchical manner, by using a prover and a procedure for generating interpolants in the base theory as black-boxes. We present several examples of theory extensions in which interpolants can be computed this way, and discuss applications in verification, knowledge representation, and modular reasoning in combinations of local theories.

1. INTRODUCTION

Many problems in mathematics and computer science can be reduced to proving satisfiability of conjunctions of (ground) literals modulo a background theory. This theory can be a standard theory, the extension of a base theory with additional functions, or a combination of theories. It is therefore very important to find efficient methods for reasoning in standard as well as complex theories. However, it is often equally important to find local causes for inconsistency. In distributed databases, for instance, finding local causes of inconsistency can help in locating errors. Similarly, in abstraction-based verification, finding the cause of inconsistency in a counterexample at the concrete level helps to rule out certain spurious counterexamples in the abstraction.

The problem we address in this paper can be described as follows: Let \mathcal{T} be a theory and A and B be sets of ground clauses in the signature of \mathcal{T} , possibly with additional constants. Assume that $A \wedge B$ is inconsistent with respect to \mathcal{T} . Can we find a ground formula I , containing only constants and function symbols common to A and B , such that I is a consequence of A with respect to \mathcal{T} , and $B \wedge I$ is inconsistent modulo \mathcal{T} ? If so, I is a (*Craig*) *interpolant* of A and B , and can be regarded as a “local” explanation for the inconsistency of $A \wedge B$.

In this paper we study possibilities of obtaining ground interpolants in theory extensions. We identify situations in which it is possible to do this in a hierarchical manner, by using a prover and a procedure for generating interpolants in the base theory as “black-boxes”.

1998 ACM Subject Classification: F.4.1, I.2.3, D.2.4, F.3.1, I.2.4.

Key words and phrases: Logic, Interpolation, Complex theories, Verification, Knowledge representation.

We consider a special type of extensions of a base theory – namely local theory extensions – which we studied in [15]. We showed that in this case hierarchical reasoning is possible. i.e. proof tasks in the extension can be reduced to proof tasks in the base theory. Here we study possibilities of hierarchical interpolant generation in local theory extensions.

The main contributions of the paper are summarized below:

- First, we identify new examples of local theory extensions.
- Second, we present a method for generating interpolants in local extensions of a base theory. The method is general, in the sense that it can be applied to an extension \mathcal{T}_1 of a theory \mathcal{T}_0 provided that:
 - (i) \mathcal{T}_0 is convex;
 - (ii) \mathcal{T}_0 is P -interpolating for a specified set P of predicates (cf. the definition in Section 5.2);
 - (iii) in \mathcal{T}_0 every inconsistent conjunction of ground clauses $A \wedge B$ allows a ground interpolant;
 - (iv) the extension is defined by clauses of a special form (type (5.1) in Section 5.2).
- The method is *hierarchical*: the problem of finding interpolants in \mathcal{T}_1 is reduced to that of finding interpolants in the base theory \mathcal{T}_0 . We can use the properties of \mathcal{T}_0 to control the form of interpolants in the extension \mathcal{T}_1 .
- Third, we identify examples of theory extensions with properties (i)–(iv).
- Fourth, we discuss application domains such as: modular reasoning in combinations of local theories (characterization of the type of information which needs to be exchanged), reasoning in distributed databases, and verification.

The existence of ground interpolants has been studied in several recent papers, mainly motivated by abstraction-refinement based verification [7, 8, 9, 19, 6]. In [8] McMillan presents a method for generating ground interpolants from proofs in an extension of linear rational arithmetic with uninterpreted function symbols. The use of free function symbols is sometimes too coarse (cf. the example in Section 2.2). Here, we show that similar results also hold for other types of extensions of a base theory, provided that the base theory has some of the properties of linear rational arithmetic. Another method for generating interpolants for combinations of theories over disjoint signatures from Nelson-Oppen-style unsatisfiability proofs was proposed by Yorsh and Musuvathi in [19]. Although we impose similar conditions on \mathcal{T}_0 , our method is orthogonal to theirs, as it can also handle combinations of theories over non-disjoint signatures. In [6] a different interpolation property – stronger than the property under consideration in this paper – is studied, namely the existence of ground interpolants for *arbitrary formulae* – which is proved to be equivalent to the theory having quantifier elimination. This limits the applicability of the results in [6] to situations in which the involved theories allow quantifier elimination. If the theory considered has quantifier elimination then we can use this for obtaining ground interpolants for arbitrary formulae. The goal of our paper is to identify theories – possibly without quantifier elimination – in which, nevertheless, ground interpolants for ground formulae exist.

Structure of the paper: We start by providing motivation for the study in Section 2. In Section 3 the basic notions needed in the paper are introduced. Section 4 contains results on local theory extensions. In Section 5 local extensions allowing hierarchical interpolation are identified, and based on this, in Section 6 a procedure for computing interpolants hierarchically is given. In Section 7 applications to modular reasoning in combinations of

theories, reasoning in complex databases, and verification are presented. In Section 8 we draw conclusions, discuss the relationship with existing work, and sketch some plans for future work. For the sake of clarity in presentation, all the proofs that are not directly related to the main thread of the paper can be found in the appendix. (These results concern illustrations of the fact that certain theory extensions are local, or satisfy assumptions that guarantee that interpolants can be computed hierarchically.)

2. MOTIVATION

In this section we present two fields of applications in which it is important to efficiently compute interpolants: knowledge representation and verification.

2.1. Knowledge representation. Consider a simple (and faulty) terminological database for chemistry, consisting of two extensions of a common kernel **Chem** (basic chemistry): **AChem** (inorganic (anorganic) chemistry) and **BioChem** (biochemistry). Assume that **Chem** contains a set $C_0 = \{\text{process, reaction, substance, organic, inorganic}\}$ of concepts and a set Γ_0 of constraints:

$$\Gamma_0 = \{\text{organic} \wedge \text{inorganic} = \emptyset, \text{organic} \subseteq \text{substance}, \text{inorganic} \subseteq \text{substance}\}.$$

Let **AChem** be an extension of **Chem** with concepts $C_1 = \{\text{cat-oxydation, oxydation}\}$, a rôle $R_1 = \{\text{catalyzes}\}$, terminology T_1 and constraints Γ_1 :

$$T_1 = \{\text{cat-oxydation} = \text{substance} \wedge \exists \text{catalyzes}(\text{oxydation})\}$$

$$\Gamma_1 = \{\text{reaction} \subseteq \text{oxydation}, \text{cat-oxydation} \subseteq \text{inorganic}, \text{cat-oxydation} \neq \emptyset\}.$$

Let **BioChem** be an extension of **Chem** with the concept $C_2 = \{\text{enzyme}\}$, the rôles $R_2 = \{\text{produces, catalyzes}\}$, terminology T_2 and constraints Γ_2 :

$$T_2 = \{\text{reaction} = \text{process} \wedge \exists \text{produces}(\text{substance}), \text{enzyme} = \text{organic} \wedge \exists \text{catalyzes}(\text{reaction})\}$$

$$\Gamma_2 = \{\text{enzyme} \neq \emptyset\}.$$

The combination of **Chem**, **AChem** and **BioChem** is inconsistent (we wrongly added to Γ_1 the constraint $\text{reaction} \subseteq \text{oxydation}$ instead of $\text{oxydation} \subseteq \text{reaction}$). This can be proved as follows: By results in [14] (p.156 and p.166) the combination of **Chem**, **AChem** and **BioChem** is inconsistent if and only if

$$\Gamma_0 \wedge (T_1 \wedge \Gamma_1) \wedge (T_2 \wedge \Gamma_2) \models_{\mathcal{T}} \perp \quad (2.1)$$

where \mathcal{T} is the extension $\text{SLat} \wedge \bigcup_{f \in R_1 \cup R_2} \text{Mon}(f)$ of the theory of semilattices with smallest element 0 and monotone function symbols corresponding to $\exists r$ for each rôle $r \in R_1 \cup R_2$. Using, for instance, the hierarchical calculus presented in [15] (see also Section 4), the contradiction can be found in polynomial time. In order to find the mistake we look for an explanation for the inconsistency in the common language of **AChem** and **BioChem**. (Common to **AChem** and **BioChem** are the concepts **substance**, **organic**, **inorganic**, **reaction** and the rôle **catalyzes**.) This can be found by computing an interpolant for the conjunction in (2.1) in the theory of semilattices with monotone operators. In this paper we show how such interpolants can be found in an efficient way. The method is illustrated on the example above in Section 7.2.

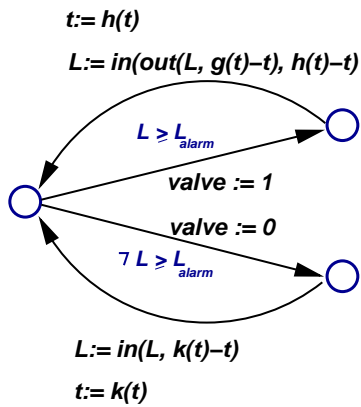
2.2. Verification. In [8], McMillan proposed a method for abstraction-based verification in which interpolation (e.g. for linear arithmetic + free functions) is used for abstraction refinement. The idea is the following: Starting from a concrete, precise description of a (possibly infinite-state) system one can obtain a finite abstraction, by merging the states into equivalence classes. A transition exists between two abstract states if there exists a transition in the concrete systems between representatives in the corresponding equivalence classes. Literals describing the relationships between the state variables at the concrete level are represented – at the abstract level – by predicates on the abstract states (equivalence classes of concrete states). Classical methods (e.g. BDD-based methods) can be used for checking whether there is a path in the abstract model from an initial state to an unsafe state. We distinguish the following cases:

- (1) No unsafe state is reachable from an initial state in the abstract model. Then, due to the way transitions are defined in the abstraction, this is the case also at the concrete level. Hence, the concrete system is guaranteed to be safe.
- (2) There exists a path in the abstract model from an initial state to an unsafe state. This path may or may not have a correspondent at the concrete level. In order to check this, we analyse the counterpart of the counterexample in the concrete model. This can be reduced to testing the satisfiability of a set of constraints:

$$\text{Init}(s_0) \wedge \text{Tr}(s_0, s_1) \wedge \cdots \wedge \text{Tr}(s_{n-1}, s_n) \wedge \neg \text{Safe}(s_n)$$

- (2.1) If the set of constraints is satisfiable then an unsafe state is reached from the initial state also in the concrete system. Thus, the concrete system is not safe.
- (2.2) If the set of constraints is unsatisfiable, then the counterexample obtained due to the abstraction was spurious. This means that the abstraction was too coarse. In order to refine it we need to take into account new predicates or relationships between the existing predicates. Interpolants provide information about which new predicates need to be used for refining the abstraction.

We illustrate these ideas below. Consider a water level controller modeled as follows: Changes in the water level by inflow/outflow are represented as functions in, out , depending on time t and water level L . Alarm and overflow levels $L_{\text{alarm}} < L_{\text{overflow}}$, as well as upper/lower bounds for mode durations $0 \leq \delta t \leq \Delta t$ are parameters of the systems.



- If $L \geq L_{\text{alarm}}$ then a valve is opened until time $g(t)$, time changes to $t' := h(t)$ and the water level to $L' := \text{in}(\text{out}(L, g(t) - t), h(t) - t)$.
- If $L < L_{\text{alarm}}$ then the valve is closed; time changes to $t' := k(t)$, and the water level to $L' := \text{in}(L, k(t) - t)$.

We impose restrictions \mathcal{K} on h, g, k and on in and out :

$$\begin{aligned} \forall t \quad (0 \leq \delta t \leq g(t) - t \leq h(t) - t \leq \Delta t) \\ \forall t \quad (0 \leq k(t) - t \leq \Delta t) \\ \forall L, t \quad (L < L_{\text{alarm}} \wedge 0 \leq t \leq \Delta t \rightarrow \text{in}(L, t) < L_{\text{overflow}}) \\ \forall L, t \quad (L < L_{\text{overflow}} \wedge t \geq \delta t \rightarrow \text{out}(L, t) < L_{\text{alarm}}). \end{aligned}$$

We want to show that if initially $L < L_{\text{alarm}}$ then the water level always remains below L_{overflow} .

We start with an abstraction in which the predicates are:

$$\begin{aligned}
p : & \quad L < L_{\text{alarm}} \\
r_1 : & \quad t' \approx k(t) & r_2 : & \quad t_1'' \approx g(t') & r_3 : & \quad t_2'' \approx h(t') \\
p_1 : & \quad L' \approx \text{in}(L, t' - t) & p_2 : & \quad L' \geq L_{\text{alarm}} & p_3 : & \quad L'' \approx \text{in}(\text{out}(L', t_1'' - t'), t_2'' - t') \\
q : & \quad \neg L'' < L_{\text{overflow}}
\end{aligned}$$

and no other relations between these predicates are specified. We can, for instance, use finite model checking for the finite abstraction obtained this way. Note for instance that

$$p \wedge p_1 \wedge p_2 \wedge p_3 \wedge r_1 \wedge r_2 \wedge r_3 \wedge q$$

is satisfiable, i.e. in the abstract model there exists a path (of length 2) from the initial state to an unsafe state. We analyze the corresponding path in the concrete model to see if this counterexample to safety is spurious, i.e. we check whether there exist $l, l', l'', t, t', t_1'', t_2'' \in \mathbb{R}$ such that the conjunction:

$$\begin{aligned}
G = & \quad l < L_{\text{alarm}} \wedge l' \approx \text{in}(l, t' - t) \wedge t' \approx k(t) \wedge l' \geq L_{\text{alarm}} \wedge \\
& \quad l'' \approx \text{in}(\text{out}(l', t_1'' - t'), t_2'' - t') \wedge t_1'' \approx g(t') \wedge t_2'' \approx h(t') \wedge \neg l'' < L_{\text{overflow}}
\end{aligned}$$

is true. If $h, g, k, \text{in}, \text{out}$ are regarded as free function symbols this conjunction is satisfiable, so the spuriousness of the counterexample cannot be detected. G can however be proved to be unsatisfiable if we take into account the additional conditions \mathcal{K} on the functions $\text{in}, \text{out}, g, h$ and k . Interpolants can be used for determining the cause of inconsistency, and can therefore help in refining the abstraction. The hierarchical interpolation method we present here allows us to efficiently generate ground interpolants for extensions with functions satisfying axioms of the type considered here and also for a whole class of more general axioms. An illustration of this method on the formulae in the example presented here is given in Section 7.3.

Besides the application to verification by abstraction-refinement, computation of Craig interpolants has other potential applications (e.g. to goal-directed overapproximation for achieving faster termination, or to automatic invariant generation).

3. PRELIMINARIES

In this section we introduce the main notions and definitions concerning theories, models and interpolants needed in the paper.

3.1. Theories and models. Theories can be regarded as sets of formulae or as sets of models. In this paper, whenever we speak about a theory \mathcal{T} – if not otherwise specified – we implicitly refer to the set $\text{Mod}(\mathcal{T})$ of all models of \mathcal{T} .

Definition 3.1. Let \mathcal{T} be a theory in a given signature $\Pi = (\Sigma, \text{Pred})$, where Σ is a set of function symbols and Pred a set of predicate symbols. Let ϕ and ψ be formulae over the signature Π with variables in a set X . The notion of truth of formulae and of entailment is the usual one in logic. We say that:

- ϕ is true with respect to \mathcal{T} (denoted $\models_{\mathcal{T}} \phi$) if ϕ is true in each model \mathcal{M} of \mathcal{T} .
- ϕ is satisfiable with respect to \mathcal{T} if there exists at least one model \mathcal{M} of \mathcal{T} and an assignment $\beta : X \rightarrow \mathcal{M}$ such that $(\mathcal{M}, \beta) \models \phi$. Otherwise we say that ϕ is unsatisfiable.
- We say that ϕ entails ψ with respect to \mathcal{T} (denoted $\phi \models_{\mathcal{T}} \psi$) if for every model \mathcal{M} of \mathcal{T} and every valuation β , if $(\mathcal{M}, \beta) \models \phi$ then $(\mathcal{M}, \beta) \models \psi$.

Note that ϕ is unsatisfiable with respect to \mathcal{T} if and only if $\phi \models_{\mathcal{T}} \perp$ (\perp stands for **false**).

3.2. Interpolation. A theory \mathcal{T} has interpolation if, for all formulae ϕ and ψ in the signature of \mathcal{T} , if $\phi \models_{\mathcal{T}} \psi$ then there exists a formula I containing only symbols which occur in both ϕ and ψ such that $\phi \models_{\mathcal{T}} I$ and $I \models_{\mathcal{T}} \psi$. First order logic has interpolation but – for an arbitrary theory \mathcal{T} – even if ϕ and ψ are e.g. conjunctions of ground literals, I may still be an arbitrary formula, containing alternations of quantifiers (cf. [6] for an example of ground formulae ϕ and ψ in the language of the theory $\text{Th}_{\text{arrays}}$ of arrays whose conjunction is unsatisfiable, but there is no ground interpolant over the common variables of ϕ and ψ). It is often important to identify situations in which ground clauses have ground interpolants.

Definition 3.2. We say that a theory \mathcal{T} has the *ground interpolation property* (or, shorter, that \mathcal{T} has *ground interpolation*) if for all ground clauses $A(\bar{c}, \bar{d})$ and $B(\bar{c}, \bar{e})$, if $A(\bar{c}, \bar{d}) \wedge B(\bar{c}, \bar{e}) \models_{\mathcal{T}} \perp$ then there exists a ground formula $I(\bar{c})$, containing only the constants \bar{c} occurring both in A and B , such that $A(\bar{c}, \bar{d}) \models_{\mathcal{T}} I(\bar{c})$ and $B(\bar{c}, \bar{e}) \wedge I(\bar{c}) \models_{\mathcal{T}} \perp$.

There exist results which relate ground interpolation to amalgamation or the injection transfer property [5, 2, 18] and thus allow us to recognize many theories with ground interpolation. We present these results in Appendix A.

Theorem 3.3. *The following theories allow ground interpolation¹:*

- (1) *The theory of pure equality (without function symbols).*
- (2) *Linear rational and real arithmetic.*
- (3) *The theory of posets.*
- (4) *The theories of (a) Boolean algebras, (b) semilattices, (c) distributive lattices.*

Proof. The proof is given in Appendix A. □

Other examples of theories which allow ground interpolation are the equational classes of (abelian) groups and lattices. In many applications one needs to consider extensions or combinations of theories, and proving amalgamation properties can be complicated. On the other hand, just knowing that ground interpolants exist is usually not sufficient: we would like to construct the interpolants fast.

In the examples considered in Theorem 3.3, methods for constructing interpolants exist. For the theories of pure equality and of posets interpolants can be constructed for instance from proofs [8, 19]. For linear rational or real arithmetic they can either be constructed from proofs [8] or by constructing linear programming problems and solving these problems using an off-the-shelf sound solver [11]². For the theories of Boolean algebras, distributive lattices and semilattices they can be reconstructed from resolution proofs associated with the translation of the satisfiability problems to propositional logic [13]; the construction is similar to the one described in the proof of Theorem 5.4 in Appendix C.

We would like to use the advantages of modular or hierarchical reasoning for constructing interpolants in theory extensions in an efficient way. This is why in this paper we aim at giving methods for *constructing* interpolants in a hierarchical way. Since in [15] we identified a

¹In fact, the theories (1) and (4) allow equational interpolation (cf. Definition A.2 in Appendix A). Similar results were also established for (2) in [11].

²Some off-the-shelf linear programming solvers may not be sound, so care is needed when choosing them.

class of theory extensions – namely, local theory extensions – in which hierarchical reasoning was possible, in what follows we will study interpolation in local theory extensions.

4. LOCAL THEORY EXTENSIONS

Let \mathcal{T}_0 be a theory with signature $\Pi_0 = (\Sigma_0, \text{Pred})$. We consider extensions $\mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ of \mathcal{T}_0 with signature $\Pi = (\Sigma, \text{Pred})$, where $\Sigma = \Sigma_0 \cup \Sigma_1$ (i.e. the signature is extended by new *function symbols*) and \mathcal{T}_1 is obtained from \mathcal{T}_0 by adding a set \mathcal{K} of (universally quantified) clauses. Thus, $\text{Mod}(\mathcal{T}_1)$ consists of all Π -structures \mathcal{M} which are models of \mathcal{K} and whose reduct $\mathcal{M}|_{\Pi_0}$ to Π_0 is a model of \mathcal{T}_0 .

Definition 4.1. A *partial Π -structure* is a structure $\mathcal{M} = (M, \{f_M\}_{f \in \Sigma}, \{P_M\}_{P \in \text{Pred}})$, where $M \neq \emptyset$ and for every $f \in \Sigma$ with arity n , f_M is a partial function from M^n to M .

Any variable assignment $\beta : X \rightarrow M$ extends in a natural way to terms, such that $\beta(f(t_1, \dots, t_n)) = f_M(\beta(t_1), \dots, \beta(t_n))$. Thus, the notion of evaluating a term t with respect to a variable assignment $\beta : X \rightarrow M$ for its variables in a partial structure \mathcal{M} is the same as for total algebras, except that this evaluation is undefined if $t = f(t_1, \dots, t_n)$ and at least one of $\beta(t_i)$ is undefined, or else $(\beta(t_1), \dots, \beta(t_n))$ is not in the domain of f_M .

Definition 4.2. Let \mathcal{M} be a partial Π -structure, C a clause and $\beta : X \rightarrow M$. Then $(\mathcal{M}, \beta) \models_w C$ if and only if either

- (i) for some term t in C , $\beta(t)$ is undefined, or else
- (ii) $\beta(t)$ is defined for all terms t of C , and there exists a literal L in C such that $\beta(L)$ is true in \mathcal{M} .

\mathcal{M} *weakly satisfies* C (notation: $\mathcal{M} \models_w C$) if $(\mathcal{M}, \beta) \models_w C$ for all assignments β . We say that \mathcal{M} *weakly satisfies a set of clauses* \mathcal{K} or \mathcal{M} *is a weak partial model of* \mathcal{K} (notation: $\mathcal{M} \models_w \mathcal{K}$) if $\mathcal{M} \models_w C$ for all $C \in \mathcal{K}$.

4.1. Local theory extensions: definitions. Let \mathcal{T}_0 be a theory with signature $\Pi_0 = (\Sigma_0, \text{Pred})$ and let \mathcal{K} be a set of (universally quantified) clauses in the signature $\Pi = (\Sigma, \text{Pred})$, where $\Sigma = \Sigma_0 \cup \Sigma_1$. In what follows, when referring to sets G of ground clauses we assume they are in the signature $\Pi^c = (\Sigma \cup \Sigma_c, \text{Pred})$ where Σ_c is a set of new constants. For the sake of simplicity, we will use the same notation for a structure and for its universe.

A (total) model of $\mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ is a Π -structure A s.t. $A \models \mathcal{K}$ and $A|_{\Pi_0}$ is a model of \mathcal{T}_0 . Let $\text{PMod}_w(\Sigma_1, \mathcal{T}_1)$ be the class of all weak partial models P of \mathcal{K} , in which the Σ_1 -functions are partial and such that $P|_{\Pi_0}$ is a total model of \mathcal{T}_0 .

An extension $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ is *local* if, in order to prove unsatisfiability of a set G of clauses with respect to $\mathcal{T}_0 \cup \mathcal{K}$, it is sufficient to use only those instances $\mathcal{K}[G]$ of \mathcal{K} in which the terms starting with extension functions are in the set $\text{st}(G, \mathcal{K})$ of ground terms which already occur in G or \mathcal{K} .

Definition 4.3. We consider the following properties of an extension $\mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ of a theory \mathcal{T}_0 with additional function symbols satisfying a set \mathcal{K} of clauses.

- (Loc) For every set G of ground clauses, $G \models_{\mathcal{T}_1} \perp$ if and only if there is no partial Π^c -structure P such that $P|_{\Pi_0}$ is a total model of \mathcal{T}_0 , all terms in $\text{st}(\mathcal{K}, G)$ are defined in P , and P weakly satisfies $\mathcal{K}[G] \wedge G$.

A weaker notion (Loc^f) is defined by requiring that the locality condition only holds for *finite* sets G of ground clauses.

- (Loc^f) For every *finite* set G of ground clauses, $G \models_{\mathcal{T}_1} \perp$ if and only if there is no partial Π^c -structure P such that $P|_{\Pi_0}$ is a total model of \mathcal{T}_0 , all terms in $\text{st}(\mathcal{K}, G)$ are defined in P , and P weakly satisfies $\mathcal{K}[G] \wedge G$.

Since (Loc^f) is the property we are interested in, we will only refer to this form of locality in what follows. We will say that the extension $\mathcal{T}_0 \subseteq \mathcal{T}_1$ is *local* if it satisfies condition (Loc^f).

4.2. Embeddability and locality. In [15, 17] we showed that embeddability of certain weak partial models into total models implies locality of an extension. Consider condition:

- (Emb_w^{fd}) Every $A \in \text{PMod}_w(\Sigma_1, \mathcal{T}_1)$ in which all extension functions have a *finite definition domain* weakly embeds into a total model of \mathcal{T}_1 .

Definition 4.4. A non-ground clause is Σ_1 -*flat* if function symbols (including constants) do not occur as arguments of functions in Σ_1 . A Σ_1 -flat non-ground clause is called Σ_1 -*linear* if whenever a variable occurs in two terms in the clause which start with function symbols in Σ_1 , the two terms are identical, and if no term which starts with a function in Σ_1 contains two occurrences of the same variable.

Theorem 4.5 ([15, 17]). *Let \mathcal{K} be a set of clauses in which all terms starting with a function symbol in Σ_1 are flat and linear. If the extension $\mathcal{T}_0 \subseteq \mathcal{T}_1$ satisfies (Emb_w^{fd}) then it satisfies (Loc^f).*

4.3. Examples. Using a variant of Theorem 4.5, in [15] we gave several examples of local theory extensions: any extension of a theory with free functions; extensions with selector functions for a constructor which is injective in the base theory; extensions of \mathbb{R} with a Lipschitz function in a point x_0 ; extensions of partially ordered theories – in a class Ord consisting of the theories of posets, (dense) totally-ordered sets, semilattices, (distributive) lattices, Boolean algebras, or \mathbb{R} – with a monotone function f , i.e. satisfying:

$$(\text{Mon}(f)) \quad \bigwedge_{i=1}^n x_i \leq y_i \rightarrow f(x_1, \dots, x_n) \leq f(y_1, \dots, y_n).$$

Generalized monotonicity conditions – combinations of monotonicity in some arguments and antitonicity in other arguments – were studied in [17]. Below, we give some additional examples with particular relevance in verification.

Theorem 4.6. *We consider the following base theories \mathcal{T}_0 : (1) \mathcal{P} (posets), (2) \mathcal{TO} (totally-ordered sets), (3) SLat (semilattices), (4) DLat (distributive lattices), (5) Bool (Boolean algebras), (6) the theory \mathbb{R} of reals resp. $\text{LI}(\mathbb{R})$ (linear arithmetic over \mathbb{R}), or the theory \mathbb{Q} of rationals resp. $\text{LI}(\mathbb{Q})$ (linear arithmetic over \mathbb{Q}), or (a subtheory of) the theory of integers (e.g. Presburger arithmetic). The following theory extensions are local:*

- (a) *Extensions of any theory \mathcal{T}_0 for which \leq is reflexive with functions satisfying boundedness ($\text{Bound}^t(f)$) or guarded boundedness ($\text{GBound}^t(f)$) conditions*

$$(\text{Bound}^t(f)) \quad \forall x_1, \dots, x_n (f(x_1, \dots, x_n) \leq t(x_1, \dots, x_n))$$

$$(\text{GBound}^t(f)) \quad \forall x_1, \dots, x_n (\phi(x_1, \dots, x_n) \rightarrow f(x_1, \dots, x_n) \leq t(x_1, \dots, x_n)),$$

where $t(x_1, \dots, x_n)$ is a term in the base signature Π_0 and $\phi(x_1, \dots, x_n)$ a conjunction of literals in the signature Π_0 , whose variables are in $\{x_1, \dots, x_n\}$.

- (b) Extensions of any theory \mathcal{T}_0 in (1)–(6) with $\text{Mon}(f) \wedge \text{Bound}^t(f)$, if $t(x_1, \dots, x_n)$ is a term in the base signature Π_0 in the variables x_1, \dots, x_n such that for every model of \mathcal{T}_0 the associated function is monotone in the variables x_1, \dots, x_n .
- (c) Extensions of any theory in (1)–(6) with functions satisfying $\text{Leq}(f, g) \wedge \text{Mon}(f)$.
 $(\text{Leq}(f, g)) \quad \forall x_1, \dots, x_n (\bigwedge_{i=1}^n x_i \leq y_i \rightarrow f(x_1, \dots, x_n) \leq g(y_1, \dots, y_n))$
- (d) Extensions of any totally-ordered theory above (i.e. (2) and (6)) with functions satisfying $\text{SGc}(f, g_1, \dots, g_n) \wedge \text{Mon}(f, g_1, \dots, g_n)$.
 $(\text{SGc}(f, g_1, \dots, g_n)) \quad \forall x_1, \dots, x_n, x (\bigwedge_{i=1}^n x_i \leq g_i(x) \rightarrow f(x_1, \dots, x_n) \leq x)$
- (e) Extensions of any theory in (1)–(3) with functions satisfying $\text{SGc}(f, g_1) \wedge \text{Mon}(f, g_1)$.

All the extensions above satisfy condition Loc^f .

Proof. The proof is given in Appendix B. □

4.4. Hierarchic reasoning in local theory extensions. Let $\mathcal{T}_0 \subseteq \mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ be a local theory extension. To check the satisfiability of a set G of ground clauses with respect to \mathcal{T}_1 we can use the following hierarchical procedure to reduce the problem to a satisfiability problem in the base theory (for details cf. [15]):

Step 1: *Use locality.* By the locality condition, we know that G is unsatisfiable with respect to \mathcal{T}_1 if and only if $\mathcal{K}[G] \wedge G$ has no weak partial model in which all the subterms of $\mathcal{K}[G] \wedge G$ are defined, and whose restriction to Π_0 is a total model of \mathcal{T}_0 .

Step 2: *Flattening and purification.* As in $\mathcal{K}[G]$ and G the functions in Σ_1 have as arguments only ground terms, $\mathcal{K}[G] \wedge G$ can be purified and flattened by introducing new constants for the arguments of the extension functions as well as for the (sub)terms $t = f(g_1, \dots, g_n)$ starting with extension functions $f \in \Sigma_1$, together with new corresponding definitions $c_t \approx t$. The set of clauses thus obtained has the form $\mathcal{K}_0 \wedge G_0 \wedge D$, where D is a set of ground unit clauses of the form $f(c_1, \dots, c_n) \approx c$, where $f \in \Sigma_1$ and c_1, \dots, c_n, c are constants, and \mathcal{K}_0, G_0 are clauses without function symbols in Σ_1 .

Step 3: *Reduction to testing satisfiability in \mathcal{T}_0 .* We reduce the problem of testing satisfiability of G with respect to \mathcal{T}_1 to a satisfiability test in \mathcal{T}_0 as shown in Theorem 4.7.

Theorem 4.7 ([15]). *Assume that $\mathcal{T}_0 \cup \mathcal{K}$ is a local extension of \mathcal{T}_0 with a set \mathcal{K} of clauses. With the notation above, the following are equivalent:*

- (1) $\mathcal{T}_0 \wedge \mathcal{K} \wedge G$ has a model.
- (2) $\mathcal{T}_0 \wedge \mathcal{K}[G] \wedge G$ has a weak partial model where all terms in $\text{st}(\mathcal{K}, G)$ are defined.
- (3) $\mathcal{T}_0 \wedge \mathcal{K}_0 \wedge G_0 \wedge D$ has a weak partial model with all terms in $\text{st}(\mathcal{K}, G)$ defined.
- (4) $\mathcal{T}_0 \wedge \mathcal{K}_0 \wedge G_0 \wedge \text{Con}[D]_0$ has a (total) Σ_0 -model, where

$$\text{Con}[D]_0 = \bigwedge \left\{ \bigwedge_{i=1}^n c_i \approx d_i \rightarrow c \approx d \mid f(c_1, \dots, c_n) \approx c, f(d_1, \dots, d_n) \approx d \in D \right\}.$$

is the set of instances of the congruence axioms for the functions in Σ_1 corresponding to the extension terms in D .

Example 4.8. Let $\mathcal{T}_1 = \text{SLat} \cup \text{SGc}(f, g) \cup \text{Mon}(f, g)$ be the extension of the theory of semilattices with two monotone functions f, g satisfying the semi-Galois condition $\text{SGc}(f, g)$. Consider the following ground formulae A, B in the signature of \mathcal{T}_1 :

$$A: d \leq g(a) \wedge a \leq c \quad B: b \leq d \wedge f(b) \not\leq c.$$

where c and d are shared constants. By Theorem 4.6(e), \mathcal{T}_1 is a local extension of the theory of semilattices. To prove that $A \wedge B \models_{\mathcal{T}_1} \perp$ we proceed as follows:

Step 1: Use locality. By the locality condition, $A \wedge B$ is unsatisfiable with respect to $\text{SLat} \wedge \text{SGc}(f, g) \wedge \text{Mon}(f, g)$ iff $\text{SLat} \wedge \text{SGc}(f, g)[A \wedge B] \wedge \text{Mon}(f, g)[A \wedge B] \wedge A \wedge B$ has no weak partial model in which all terms in A and B are defined. The extension terms occurring in $A \wedge B$ are $f(b)$ and $g(a)$, hence:

$$\begin{aligned} \text{Mon}(f, g)[A \wedge B] &= \{a \leq a \rightarrow g(a) \leq g(a), \quad b \leq b \rightarrow f(b) \leq f(b)\} \\ \text{SGc}(f, g)[A \wedge B] &= \{b \leq g(a) \rightarrow f(b) \leq a\} \end{aligned}$$

Step 2: Flattening and purification. We purify and flatten the formula $\text{SGc}(f, g) \wedge \text{Mon}(f, g)$ by replacing the ground terms starting with f and g with new constants. The clauses are separated into a part containing definitions for terms starting with extension functions, $D_A \wedge D_B$, and a conjunction of formulae in the base signature, $A_0 \wedge B_0 \wedge \text{SGc}_0 \wedge \text{Mon}_0$.

Step 3: Reduction to testing satisfiability in \mathcal{T}_0 . As the extension $\text{SLat} \subseteq \mathcal{T}_1$ is local, by Theorem 4.7 we know that

$$A \wedge B \models_{\mathcal{T}_1} \perp \quad \text{if and only if} \quad A_0 \wedge B_0 \wedge \text{SGc}_0 \wedge \text{Mon}_0 \wedge \text{Con}_0 \text{ is unsatisfiable with respect to } \text{SLat},$$

where $\text{Con}_0 = \text{Con}[A \wedge B]_0$ consists of the flattened form of those instances of the congruence axioms containing only f - and g -terms which occur in D_A or D_B , and $\text{SGc}_0 \wedge \text{Mon}_0$ consists of those instances of axioms in $\text{SGc}(f, g) \wedge \text{Mon}(f, g)$ containing only f - and g -terms which occur in D_A or D_B .

Extension	Base	
$D_A \wedge D_B$	$A_0 \wedge B_0 \wedge \text{SGc}_0 \wedge \text{Mon}_0 \wedge \text{Con}_0$	
$a_1 \approx g(a)$	$A_0 = d \leq a_1 \wedge a \leq c$	$\text{SGc}_0 = b \leq a_1 \rightarrow b_1 \leq a$
$b_1 \approx f(b)$	$B_0 = b \leq d \wedge b_1 \not\leq c$	$\text{Con}_A \wedge \text{Mon}_A = a \triangleleft a \rightarrow a_1 \triangleleft a_1, \triangleleft \in \{\approx, \leq\}$
		$\text{Con}_B \wedge \text{Mon}_B = b \triangleleft b \rightarrow b_1 \triangleleft b_1, \triangleleft \in \{\approx, \leq\}$

It is easy to see that $A_0 \wedge B_0 \wedge \text{SGc}_0 \wedge \text{Mon}_0 \wedge \text{Con}_0$ is unsatisfiable with respect to \mathcal{T}_0 : $A_0 \wedge B_0$ entails $b \leq a_1$, together with SGc_0 this yields $b_1 \leq a$, which together with $a \leq c$ and $b_1 \not\leq c$ leads to a contradiction.

5. HIERARCHICAL INTERPOLANT COMPUTATION

Let $\mathcal{T}_0 \subseteq \mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ be a theory extension by means of a set of clauses \mathcal{K} . Assume that $A \wedge B \models_{\mathcal{T}_1} \perp$, where A and B are two sets of ground clauses. Our goal is to find a ground *interpolant*, that is a ground formula I containing only constants and extension functions which are common to A and B such that

$$A \models_{\mathcal{T}_1} I \quad \text{and} \quad I \wedge B \models_{\mathcal{T}_1} \perp.$$

Flattening and purification do not influence the existence of ground interpolants:

Lemma 5.1. *Let A and B be two sets of ground clauses in the signature Π^c . Let $A_0 \wedge D_A$ and $B_0 \wedge D_B$ be obtained from A resp. B by purification and flattening. If I is an interpolant of $(A_0 \wedge D_A) \wedge (B_0 \wedge D_B)$ then the formula \bar{I} , obtained from I by replacing, recursively, all newly introduced constants with the terms in the original signature which they represent, is an interpolant for $A \wedge B$.*

Proof. If I is an interpolant of $(A_0 \wedge D_A) \wedge (B_0 \wedge D_B)$, then $A_0 \wedge D_A \models_{\mathcal{T}_1} I$ and $B_0 \wedge D_B \wedge I \models_{\mathcal{T}_1} \perp$. Let \bar{I} be obtained from I by replacing, recursively, all newly introduced constants with the terms in the original signature which they represent. Then:

- (i) $A \wedge \neg \bar{I}$ and $A_0 \wedge D_A \wedge \neg I$ are equisatisfiable with respect to \mathcal{T}_1 , so $A \models_{\mathcal{T}_1} \bar{I}$.
- (ii) $B \wedge \bar{I}$ and $B_0 \wedge D_B \wedge I$ are equisatisfiable with respect to \mathcal{T}_1 , so $B \wedge \bar{I} \models_{\mathcal{T}_1} \perp$. □

Therefore we can restrict without loss of generality to finding interpolants for the *purified and flattened* conjunction of formulae $(A_0 \wedge D_A) \wedge (B_0 \wedge D_B)$.

We focus on interpolation in *local theory extensions*. Let $\mathcal{T}_0 \subseteq \mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ be a local theory extension. From Theorem 4.7 we know that in such extensions hierarchical reasoning is possible: if A and B are sets of ground clauses in a signature Π^c , and $A_0 \wedge D_A$ (resp. $B_0 \wedge D_B$) are obtained from A (resp. B) by purification and flattening then:

$$(A_0 \wedge D_A) \wedge (B_0 \wedge D_B) \models_{\mathcal{T}_1} \perp \quad \text{if and only if} \quad \mathcal{K}_0 \wedge A_0 \wedge B_0 \wedge \text{Con}[D_A \wedge D_B]_0 \models_{\mathcal{T}_0} \perp,$$

where \mathcal{K}_0 is obtained from $\mathcal{K}[D_A \wedge D_B]$ by replacing the Σ_1 -terms with the corresponding constants contained in the definitions D_A and D_B and

$$\text{Con}[D_A \wedge D_B]_0 = \bigwedge_{i=1}^n \{ \bigwedge_{i=1}^n c_i \approx d_i \rightarrow c \approx d \mid f(c_1, \dots, c_n) \approx c, f(d_1, \dots, d_n) \approx d \in D_A \cup D_B \}.$$

In general we cannot use Theorem 4.7 for generating a ground interpolant because:

- (i) $\mathcal{K}[D_A \wedge D_B]$ (hence also \mathcal{K}_0) may contain free variables.
- (ii) If some clause in \mathcal{K} contains two or more different extension functions, it is unlikely that these extension functions can be separated in the interpolants.
- (iii) The clauses in $\mathcal{K}[D_A \wedge D_B]$ and the instances of congruence axioms (and therefore the clauses in $\mathcal{K}_0 \wedge \text{Con}[D_A \wedge D_B]_0$) may contain combinations of constants and extension functions from A and B .

To avoid (i), we will need to take into account only extensions with sets \mathcal{K} of clauses in which all variables occur below some extension term. To solve (ii), we define a relation \sim between extension functions, where $f \sim g$ if f and g occur in the same clause in \mathcal{K} . This defines an equivalence relation \sim on Σ_1 . We henceforth consider that a function $f \in \Sigma_1$ is common to A and B if there exist $g, h \in \Sigma_1$ such that $f \sim g$, $f \sim h$, g occurs in A and h occurs in B .

Example 5.2. Consider the reduction to the base theory in Example 4.8. We explain the problems mentioned above.

Ad (ii) As $\text{SGc}(f, g)$ contains occurrences of both f and g , it is not likely to find an interpolant with no occurrence of f and g , even if g only occurs in A and f only occurs in B . We therefore assume that $f \sim g$, i.e. that both f and g are shared.

Ad (iii) The clause $b \leq a_1 \rightarrow b_1 \leq a$ of SGc_0 is mixed, i.e. contains combinations of constants from A and B .

The idea for solving problem (iii) is presented below.

5.1. Main Idea. The idea of our approach is to separate mixed instances of axioms in \mathcal{K}_0 , or of congruence axioms in $\text{Con}[D_A \wedge D_B]_0$, into an A -part and a B -part. This is, if $A \wedge B \models_{\tau_1} \perp$ we find a set T of $\Sigma_0 \cup \Sigma_1$ -terms containing only constants and extension functions common to A and B , such that $\mathcal{K}[A \wedge B]$ can be separated into a part $\mathcal{K}[A, T]$ consisting of instances with extension terms occurring in A and T , and a part $\mathcal{K}[B, T]$ containing only instances with extension terms in B and T , such that:

$$\mathcal{K}[A, T] \wedge A_0 \wedge \text{Con}[D_A \wedge D_T] \wedge \mathcal{K}[B, T] \wedge B_0 \wedge \text{Con}[D_B \wedge D_T]$$

has no weak partial model where all ground terms in \mathcal{K}, D_A, D_B, T are defined.

Example 5.3. Consider the conjunction $A_0 \wedge D_A \wedge B_0 \wedge D_B \wedge \text{Con}[D_A \wedge D_B]_0 \wedge \text{Mon}_0 \wedge \text{SGc}_0$ in Example 4.8. The A and B -part share the constants c and d , and no function symbols. However, as f and g occur together in SGc , $f \sim g$, so they are considered to be all shared. (Thus, the interpolant is allowed to contain both f and g .) We obtain a separation for the clause $b \leq a_1 \rightarrow b_1 \leq a$ of SGc_0 as follows:

- (i) We note that $A_0 \wedge B_0 \models b \leq a_1$.
- (ii) We can find an SLat -term t containing only shared constants of A_0 and B_0 such that $A_0 \wedge B_0 \models b \leq t \wedge t \leq a_1$. (Indeed, such a term is $t = d$.)
- (iii) We show that, instead of the axiom $b \leq g(a) \rightarrow f(b) \leq a$, whose flattened form is in SGc_0 , we can use, without loss of unsatisfiability:
 - (1) an instance of the monotonicity axiom for f : $b \leq d \rightarrow f(b) \leq f(d)$,
 - (2) another instance of SGc , namely: $d \leq g(a) \rightarrow f(d) \leq a$.
 For this, we introduce a new constant $c_{f(d)}$ for $f(d)$ (its definition, $c_{f(d)} \approx f(d)$, is stored in a set D_T), and the corresponding instances $\mathcal{H}_{\text{sep}} = \mathcal{H}_{\text{sep}}^A \wedge \mathcal{H}_{\text{sep}}^B$ of the congruence, monotonicity and $\text{SGc}(f, g)$ -axioms, which are now separated into an A -part ($\mathcal{H}_{\text{sep}}^A : d \leq a_1 \rightarrow c_{f(d)} \leq a$) and a B -part ($\mathcal{H}_{\text{sep}}^B : b \leq d \rightarrow b_1 \leq c_{f(d)}$). We thus obtain a separated conjunction $\overline{A}_0 \wedge \overline{B}_0$ (where $\overline{A}_0 = \mathcal{H}_{\text{sep}}^A \wedge A_0$ and $\overline{B}_0 = \mathcal{H}_{\text{sep}}^B \wedge B_0$), which can be proved to be unsatisfiable in $\mathcal{T}_0 = \text{SLat}$.
- (iv) To compute an interpolant in SLat for $\overline{A}_0 \wedge \overline{B}_0$ note that \overline{A}_0 is logically equivalent to the conjunction of unit literals $d \leq a_1 \wedge a \leq c \wedge c_{f(d)} \leq a$ and \overline{B}_0 is logically equivalent to $b \leq d \wedge b_1 \not\leq c \wedge b_1 \leq c_{f(d)}$. An interpolant is $I_0 = c_{f(d)} \leq c$.
- (v) By replacing the new constants with the terms they denote we obtain the interpolant $I = f(d) \leq c$ for $A \wedge B$.

Note that in order to be able to perform in general the succession of steps in Example 5.3 it is necessary that \mathcal{K}_0 is ground and the theory extension and the base theory have certain properties:

- (i) it always is possible to find an axiom instance such that all its premises are entailed by $A_0 \wedge B_0$;
- (ii) we can find separating terms (in the joint signature) for the entailed literals;
- (iii) the axioms come in pairs with corresponding monotonicity axioms which are then used to separate mixed rules;
- (iv) we can compute ground interpolants in \mathcal{T}_0 .

Theory extensions satisfying these conditions appear in a natural way in a wide variety of applications ranging from knowledge representation to verification. In what follows we will give several examples of theories with properties (i)–(iv).

5.2. Examples of theory extensions with hierarchic interpolation. We identify a class of theory extensions for which interpolants can be computed hierarchically (and efficiently) using a procedure for generating interpolants in the base theory \mathcal{T}_0 . This allows us to exploit specific properties of \mathcal{T}_0 for obtaining simple interpolants in \mathcal{T}_1 . We make the following assumptions about \mathcal{T}_0 :

Assumption 1: \mathcal{T}_0 is *convex* with respect to the set Pred of all predicates (including equality \approx), i.e., for all conjunctions Γ of ground atoms, relations $R_1, \dots, R_m \in \text{Pred}$ and ground tuples of corresponding arity $\bar{t}_1, \dots, \bar{t}_m$, if $\Gamma \models_{\mathcal{T}_0} \bigvee_{i=1}^m R_i(\bar{t}_i)$ then there exists $j \in \{1, \dots, m\}$ such that $\Gamma \models_{\mathcal{T}_0} R_j(\bar{t}_j)$.

Assumption 2: \mathcal{T}_0 is *P-interpolating* with respect to $P \subseteq \text{Pred}$, i.e. for all conjunctions A and B of ground literals, all binary predicates $R \in P$ and all constants a and b such that a occurs in A and b occurs in B (or vice versa), if $A \wedge B \models_{\mathcal{T}_0} aRb$ then there exists a term t containing only constants common to A and B with $A \wedge B \models_{\mathcal{T}_0} aRt \wedge tRb$. (If we can always find a term t containing only constants common to A and B with $A \models_{\mathcal{T}_0} aRt$ and $B \models_{\mathcal{T}_0} tRb$ we say that \mathcal{T}_0 is *strongly P-interpolating*.)

Assumption 3: \mathcal{T}_0 has ground interpolation.

Some examples of theories satisfying these properties are given below.

Theorem 5.4. *The following theories have ground interpolation and are convex and P-interpolating with respect to the indicated set P of predicate symbols:*

- (1) *The theory of \mathcal{EQ} of pure equality without function symbols (for $P = \{\approx\}$).*
- (2) *The theory PoSet of posets (for $P = \{\approx, \leq\}$).*
- (3) *Linear rational arithmetic $\text{LI}(\mathbb{Q})$ and linear real arithmetic $\text{LI}(\mathbb{R})$ (convex with respect to $P = \{\approx\}$, strongly P-interpolating for $P = \{\leq\}$).*
- (4) *The theories Bool of Boolean algebras, SLat of semilattices and DLat of distributive lattices (strongly P-interpolating for $P = \{\approx, \leq\}$).*

Proof. The proof is given in Appendix C. □

We make the following assumption about the extension \mathcal{T}_1 of \mathcal{T}_0 .

Assumption 4: $\mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ is a local extension of \mathcal{T}_0 with the property that in all clauses in \mathcal{K} each variable occurs also below some extension function.

For the sake of simplicity we only consider sets A, B of unit clauses, i.e. conjunctions of ground literals. This is not a restriction, since if we can obtain interpolants for conjunctions of ground literals then we also can construct interpolants for conjunctions of arbitrary clauses by using standard methods³ discussed e.g. in [8] or [19].

By Lemma 5.1, we can restrict without loss of generality to finding an interpolant for the purified and flattened conjunction of unit clauses $A_0 \wedge B_0 \wedge D_A \wedge D_B$. By Theorem 4.7,

$$A_0 \wedge D_A \wedge B_0 \wedge D_B \models_{\mathcal{T}_1} \perp \quad \text{if and only if} \quad \mathcal{K}_0 \wedge A_0 \wedge B_0 \wedge \text{Con}[D_A \wedge D_B]_0 \models_{\mathcal{T}_0} \perp,$$

³E.g. in a DPLL-style procedure partial interpolants are generated for the unsatisfiable branches and then recombined using ideas of Pudlák.

where \mathcal{K}_0 is obtained from $\mathcal{K}[D_A \wedge D_B]$ by replacing the Σ_1 -terms with the corresponding constants contained in the definitions $D_A \wedge D_B$ and

$$\text{Con}[D_A \wedge D_B]_0 = \bigwedge_{i=1}^n \{ \bigwedge_{i=1}^n c_i \approx d_i \rightarrow c \approx d \mid f(c_1, \dots, c_n) \approx c, f(d_1, \dots, d_n) \approx d \in D_A \cup D_B \}.$$

In general, $\text{Con}[D_A \wedge D_B]_0 = \text{Con}_0^A \wedge \text{Con}_0^B \wedge \text{Con}_{\text{mix}}$ and $\mathcal{K}_0 = \mathcal{K}_0^A \wedge \mathcal{K}_0^B \wedge \mathcal{K}_{\text{mix}}$, where $\text{Con}_0^A, \mathcal{K}_0^A$ only contain extension functions and constants which occur in A , $\text{Con}_0^B, \mathcal{K}_0^B$ only contain extension functions and constants which occur in B , and $\text{Con}_{\text{mix}}, \mathcal{K}_{\text{mix}}$ contain mixed clauses with constants occurring in both A and B . Our goal is to separate Con_{mix} and \mathcal{K}_{mix} into an A -local and a B -local part. We show that, under Assumptions 1 and 2, Con_{mix} can always be separated, and \mathcal{K}_{mix} can be separated if \mathcal{K} contains the following type of combinations of clauses:

$$\begin{cases} x_1 R_1 s_1 \wedge \dots \wedge x_n R_n s_n \rightarrow f(x_1, \dots, x_n) R g(y_1, \dots, y_n) \\ x_1 R_1 y_1 \wedge \dots \wedge x_n R_n y_n \rightarrow f(x_1, \dots, x_n) R f(y_1, \dots, y_n) \end{cases} \quad (5.1)$$

where $n \geq 1$, x_1, \dots, x_n are variables, R_1, \dots, R_n, R are binary relations with $R_1, \dots, R_n \in P$ and R transitive, and each s_i is either a variable among the arguments of g , or a term of the form $f_i(z_1, \dots, z_k)$, where $f_i \in \Sigma_1$ and all the arguments of f_i are variables occurring among the arguments of g .⁴

We therefore make the following additional assumption about the theory extension \mathcal{T}_1 :

Assumption 5: $\mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ is an extension of \mathcal{T}_0 with a set of clauses \mathcal{K} which only contains combinations of clauses of type (5.1).

Example 5.5. The following local extensions satisfy Assumptions 4 and 5:

- (a) Any extension with free functions ($\mathcal{K} = \emptyset$).
- (b) Extensions of any theory in **Ord** (cf. Section 4.3) with monotone functions.
- (c) Extensions of any totally-ordered theory in **Ord** with functions satisfying

$$\text{SGc}(f, g_1, \dots, g_n) \wedge \text{Mon}(f, g_1, \dots, g_n).$$

- (d) Extensions of theories in **Ord** with functions satisfying

$$\text{SGc}(f, g_1) \wedge \text{Mon}(f, g_1).$$

- (e) Extensions of theories in **Ord** with functions satisfying $\text{Leq}(f, g) \wedge \text{Mon}(f)$.

Remark 5.6. If the clauses in \mathcal{K} are of type (5.1), then $\mathcal{K}_0 = \mathcal{K}_0^A \wedge \mathcal{K}_0^B \wedge \mathcal{K}_{\text{mix}}$, where

$$\begin{aligned} \mathcal{K}_0^A = \{ & (\bigwedge_{i=1}^n c_i R_i d_i) \rightarrow c R d \mid (\bigwedge_{i=1}^n x_i R_i s_i(\bar{y})) \rightarrow f(x_1, \dots, x_n) R g(\bar{y}) \in \mathcal{K}, \\ & d_i \approx s_i(\bar{e}) \in D_A, d \approx g(\bar{e}) \in D_A, c \approx f(c_1, \dots, c_n) \in D_A \} \cup \\ & \{ (\bigwedge_{i=1}^n c_i R_i d_i) \rightarrow c R d \mid (\bigwedge_{i=1}^n x_i R_i y_i) \rightarrow f(x_1, \dots, x_n) R f(y_1, \dots, y_n) \in \mathcal{K}, \\ & d \approx f(d_1, \dots, d_n) \in D_A, c \approx f(c_1, \dots, c_n) \in D_A \}, \end{aligned}$$

⁴More general types of clauses, in which instead of variables we can consider arbitrary base terms, can be handled if \mathcal{T}_0 has a P -interpolation property for terms instead of constants. Due to space limitations, such extensions are not discussed here.

similarly for \mathcal{K}_0^B , and

$$\begin{aligned} \mathcal{K}_{\text{mix}} = & \{ \bigwedge_{i=1}^n c_i R_i d_i \rightarrow c R d \mid \bigwedge_{i=1}^n x_i R_i s_i(\bar{y}) \rightarrow f(x_1, \dots, x_n) R g(\bar{y}) \in \mathcal{K}, d_i \approx s_i(\bar{e}) \in D_A, \\ & d \approx g(\bar{e}) \in D_A \setminus D_B, c \approx f(c_1, \dots, c_n) \in D_B \setminus D_A \} \cup \\ & \{ \bigwedge_{i=1}^n c_i R_i d_i \rightarrow c R d \mid \bigwedge_{i=1}^n x_i R_i y_i \rightarrow f(x_1, \dots, x_n) R f(y_1, \dots, y_n) \in \mathcal{K}, \\ & d \approx f(d_1, \dots, d_n) \in D_A \setminus D_B, c \approx f(c_1, \dots, c_n) \in D_B \setminus D_A \} \cup \\ & \{ \bigwedge_{i=1}^n c_i R_i d_i \rightarrow c R d \mid \bigwedge_{i=1}^n x_i R_i s_i(\bar{y}) \rightarrow f(x_1, \dots, x_n) R g(\bar{y}) \in \mathcal{K}, d_i \approx s_i(\bar{e}) \in D_B, \\ & d \approx g(\bar{e}) \in D_B \setminus D_A, c \approx f(c_1, \dots, c_n) \in D_A \setminus D_B \} \cup \\ & \{ \bigwedge_{i=1}^n c_i R_i d_i \rightarrow c R d \mid \bigwedge_{i=1}^n x_i R_i y_i \rightarrow f(x_1, \dots, x_n) R f(y_1, \dots, y_n) \in \mathcal{K}, \\ & d \approx f(d_1, \dots, d_n) \in D_B \setminus D_A, c \approx f(c_1, \dots, c_n) \in D_A \setminus D_B \}. \end{aligned}$$

All clauses in \mathcal{K}_0 are of the form $C = \bigwedge_{i=1}^n c_i R_i d_i \rightarrow c R d$, where $R_i \in P$, R is transitive, and c_i, d_i, c, d are constants. Moreover, the cardinality of $\mathcal{K}_0 \cup \text{Con}[D_A \wedge D_B]_0$ is quadratic in the size of $A \wedge B$ for a fixed \mathcal{K} .

Proposition 5.7. *Assume that \mathcal{T}_0 satisfies Assumptions 1 and 2. Let \mathcal{H} be a set of Horn clauses $(\bigwedge_{i=1}^n c_i R_i d_i) \rightarrow c R d$ in the signature Π_0^c (with R transitive and $R_i \in P$) which are instances of flattened and purified clauses of type (5.1) and of congruence axioms. Let A_0 and B_0 be conjunctions of ground literals in the signature Π_0^c such that $A_0 \wedge B_0 \wedge \mathcal{H} \models_{\mathcal{T}_0} \perp$. Then \mathcal{H} can be separated into an A and a B part by replacing the set \mathcal{H}_{mix} of mixed clauses*

$$\begin{aligned} \mathcal{H}_{\text{mix}} = & \{ \bigwedge_{i=1}^n c_i R_i d_i \rightarrow c R d \in \mathcal{H} \mid c_i, c \text{ constants in } A, d_i, d \text{ constants in } B \} \cup \\ & \{ \bigwedge_{i=1}^n c_i R_i d_i \rightarrow c R d \in \mathcal{H} \mid c_i, c \text{ constants in } B, d_i, d \text{ constants in } A \} \end{aligned}$$

with a separated set of formulae \mathcal{H}_{sep} . The following hold:

- (1) *There exists a set T of $\Sigma_0 \cup \Sigma_c$ -terms containing only constants common to A_0 and B_0 such that $A_0 \wedge B_0 \wedge (\mathcal{H} \setminus \mathcal{H}_{\text{mix}}) \wedge \mathcal{H}_{\text{sep}} \models_{\mathcal{T}_0} \perp$, where*

$$\begin{aligned} \mathcal{H}_{\text{sep}} = & \{ (\bigwedge_{i=1}^n c_i R_i t_i \rightarrow c R c_{f(t_1, \dots, t_n)}) \wedge (\bigwedge_{i=1}^n t_i R_i d_i \rightarrow c_{f(t_1, \dots, t_n)} R d) \mid \\ & \bigwedge_{i=1}^n c_i R_i d_i \rightarrow c R d \in \mathcal{H}_{\text{mix}}, d_i \approx s_i(e_1, \dots, e_n), d \approx g(e_1, \dots, e_n) \in D_B, \\ & c \approx f(c_1, \dots, c_n) \in D_A \text{ or vice versa} \} = \mathcal{H}_{\text{sep}}^A \wedge \mathcal{H}_{\text{sep}}^B \end{aligned}$$

and $c_{f(t_1, \dots, t_n)}$ are new constants in Σ_c (considered to be common) introduced for the corresponding terms $f(t_1, \dots, t_n)$.

- (2) *$A_0 \wedge B_0 \wedge (\mathcal{H} \setminus \mathcal{H}_{\text{mix}}) \wedge \mathcal{H}_{\text{sep}}$ is logically equivalent with respect to \mathcal{T}_0 with the following separated conjunction of ground literals:*

$$\begin{aligned} \overline{A}_0 \wedge \overline{B}_0 = & A_0 \wedge B_0 \wedge \bigwedge \{ c R d \mid \Gamma \rightarrow c R d \in \mathcal{H} \setminus \mathcal{H}_{\text{mix}} \} \\ & \wedge \bigwedge \{ c R c_{f(\bar{t})} \wedge c_{f(\bar{t})} R d \mid (\Gamma \rightarrow c R c_{f(\bar{t})}) \wedge (\Gamma \rightarrow c_{f(\bar{t})} R d) \in \mathcal{H}_{\text{sep}} \}. \end{aligned}$$

- (3) *If \mathcal{T}_0 is strongly P -interpolating then the A -part (B -part) of $A_0 \wedge B_0 \wedge (\mathcal{H} \setminus \mathcal{H}_{\text{mix}}) \wedge \mathcal{H}_{\text{sep}} \models_{\mathcal{T}_0} \perp$ is logically equivalent with \overline{A}_0 (resp. \overline{B}_0) above.*

Proof. We prove (1) and (2) simultaneously by induction on the number of clauses in \mathcal{H} . If $\mathcal{H} = \emptyset$ then the initial problem is already separated into an A and a B part so we are done: we can choose $T = \emptyset$. Assume that \mathcal{H} contains at least one clause, and that for every \mathcal{H}' with fewer clauses and every conjunctions of literals A'_0, B'_0 with $A'_0 \wedge B'_0 \wedge \mathcal{H}' \models_{\mathcal{T}_0} \perp$, (1) and (2) hold.

Let \mathcal{D} be the set of all atoms $c_i R_i d_i$ occurring in premises of clauses in \mathcal{H} . As every model of $A_0 \wedge B_0 \wedge \bigwedge_{(c R d) \in \mathcal{D}} \neg(c R d)$ is also a model for $\mathcal{H} \wedge A_0 \wedge B_0 \models_{\mathcal{T}_0} \perp$ and $\mathcal{H} \wedge A_0 \wedge B_0 \models_{\mathcal{T}_0} \perp$, $A_0 \wedge B_0 \wedge \bigwedge_{(c R d) \in \mathcal{D}} \neg(c R d) \models_{\mathcal{T}_0} \perp$. Let $(A_0 \wedge B_0)^+$ be the conjunction of all atoms in $A_0 \wedge B_0$,

and $(A_0 \wedge B_0)^-$ be the set of all negative literals in $A_0 \wedge B_0$. Then

$$(A_0 \wedge B_0)^+ \models_{\mathcal{T}_0} \bigvee_{(cRd) \in \mathcal{D}} (cRd) \vee \bigvee_{\neg L \in (A_0 \wedge B_0)^-} L.$$

By Assumption 1, \mathcal{T}_0 is convex with respect to **Pred**. Moreover, $(A_0 \wedge B_0)^+$ is a conjunction of positive literals. Therefore, either

- (i) $(A_0 \wedge B_0)^+ \models L$ for some $L \in (A_0 \wedge B_0)^-$ (then $A_0 \wedge B_0$ is unsatisfiable and hence entails any atom $c_i R_i d_i$), or
- (ii) there exists $(c_1 R_1 d_1) \in \mathcal{D}$ such that $(A_0 \wedge B_0)^+ \models_{\mathcal{T}_0} c_1 R_1 d_1$.

Case 1: $A_0 \wedge B_0$ is unsatisfiable. In this case (1) and (2) hold for $T = \emptyset$.

Case 2: $A_0 \wedge B_0$ is satisfiable. Then $A_0 \wedge B_0$ is logically equivalent in \mathcal{T}_0 with $A_0 \wedge B_0 \wedge c_i R_i d_i$. If it is not the case that by adding $c_i R_i d_i$ all premises of some rule in \mathcal{H} become true we repeat the procedure for $\mathcal{D}_1 = \mathcal{D} \setminus (c_1 R_1 d_1)$: Again in this case $A_0 \wedge B_0 \wedge \bigwedge_{(cRd) \in \mathcal{D}_1} \neg(cRd) \models_{\mathcal{T}_0} \perp$ (if it has a model then $A_0 \wedge B_0 \wedge \mathcal{H}$ has one), and as before, using convexity we infer that either $A_0 \wedge B_0$ is unsatisfiable (which cannot be the case) or there exists $c_2 R_2 d_2 \in \mathcal{D}_1$ with $A_0 \wedge B_0 \models_{\mathcal{T}_0} c_2 R_2 d_2$. We can repeat the process until all the premises of some clause in \mathcal{H} are proved to be entailed by $A_0 \wedge B_0$. Let $C = \bigwedge_{i=1}^n c_i R_i d_i \rightarrow cRd$ be such a clause.

Case 2a. Assume that C contains only constants occurring in A or only constants occurring in B . Then $A_0 \wedge B_0 \wedge \mathcal{H}$ is equivalent with respect to \mathcal{T}_0 with $A_0 \wedge B_0 \wedge (\mathcal{H} \setminus C) \wedge c \approx d$. By the induction hypothesis for $A'_0 \wedge B'_0 = A_0 \wedge B_0 \wedge c \approx d$ and $\mathcal{H}' = \mathcal{H} \setminus \{C\}$, we know that there exists T' such that $A'_0 \wedge B'_0 \wedge (\mathcal{H}' \setminus \mathcal{H}'_{\text{mix}}) \wedge \mathcal{H}'_{\text{sep}} \models \perp$, and (2) holds too. Then, for $T = T'$, $A'_0 \wedge B'_0 \wedge (\mathcal{H}' \setminus \mathcal{H}'_{\text{mix}}) \wedge \mathcal{H}'_{\text{sep}}$ is logically equivalent to $A_0 \wedge B_0 \wedge (\mathcal{H} \setminus \mathcal{H}_{\text{mix}}) \wedge \mathcal{H}_{\text{sep}}$, so (1) holds. In order to prove (2), note that, by definition, $\mathcal{H}'_{\text{mix}} = \mathcal{H}_{\text{mix}}$ and $\mathcal{H}'_{\text{sep}} = \mathcal{H}_{\text{sep}}$. By the induction hypothesis, $A'_0 \wedge B'_0 \wedge (\mathcal{H}' \setminus \mathcal{H}'_{\text{mix}}) \cup \mathcal{H}'_{\text{sep}}$ is logically equivalent to a corresponding conjunction $\overline{A'_0} \wedge \overline{B'_0}$ containing as conjuncts all literals in A'_0 and B'_0 and all conclusions of rules in $\mathcal{H}' \setminus \mathcal{H}'_{\text{mix}}$ and $\mathcal{H}'_{\text{sep}}$. On the other hand, $A'_0 \wedge B'_0$ is logically equivalent to $A_0 \wedge B_0 \wedge (cRd)$, where (cRd) is the conclusion of the rule $C \in \mathcal{H} \setminus \mathcal{H}_{\text{mix}}$. This proves (2).

Case 2b. Assume now that C is mixed, for instance that c_1, \dots, c_n, c are constants in A and d_1, \dots, d_n, d are constants in B . Assume that C is obtained from an instance of a clause of the form $\bigwedge_{i=1}^n x_i R_i s_i(\overline{y}) \rightarrow f(x_1, \dots, x_n) R g(\overline{y})$. (The case when C corresponds to an instance of a monotonicity axiom is similar.) This means that there exist $c \approx f(c_1, \dots, c_n) \in D_A$ and $d_i \approx s_i(\overline{e}), d \approx g(\overline{e}) \in D_B$. C was chosen such that for each premise $c_i R_i d_i$ of C , $A_0 \wedge B_0 \models_{\mathcal{T}_0} c_i R_i d_i$, and – by Assumption 2 – \mathcal{T}_0 is P -interpolating. Thus, there exist terms t_1, \dots, t_n containing only constants common to A_0 and B_0 such that for all $i \in \{1, \dots, n\}$

$$A_0 \wedge B_0 \models_{\mathcal{T}_0} c_i R_i t_i \wedge t_i R_i d_i. \quad (5.2)$$

Let $c_{f(t_1, \dots, t_n)}$ be a new constant, denoting the term $f(t_1, \dots, t_n)$, and let

$$C_A = \bigwedge_{i=1}^n c_i R_i t_i \rightarrow c R c_{f(t_1, \dots, t_n)} \quad \text{and} \quad C_B = \bigwedge_{i=1}^n t_i R_i d_i \rightarrow c_{f(t_1, \dots, t_n)} R d.$$

Thus, C_A corresponds to the monotonicity axiom $\bigwedge_{i=1}^n c_i R_i t_i \rightarrow f(c_1, \dots, c_n) R f(t_1, \dots, t_n)$,

whereas C_B corresponds to the rule $\bigwedge_{i=1}^n t_i R_i s_i(\overline{e}) \rightarrow f(t_1, \dots, t_n) R g(\overline{e})$. As R is transitive,

by (5.2) the following holds:

$$\begin{aligned}
A_0 \wedge B_0 \wedge C_A \wedge C_B &\models_{\mathcal{T}_0} A_0 \wedge B_0 \wedge \left(\bigwedge_{i=1}^n c_i R_i t_i \wedge C_A \right) \wedge \left(\bigwedge_{i=1}^n t_i R_i d_i \wedge C_B \right) \\
&\models_{\mathcal{T}_0} A_0 \wedge B_0 \wedge cRc_{f(t_1, \dots, t_n)} \wedge c_{f(t_1, \dots, t_n)} Rd \\
&\models_{\mathcal{T}_0} A_0 \wedge B_0 \wedge cRd
\end{aligned}$$

(where $\models_{\mathcal{T}_0}$ stands for logical equivalence with respect to \mathcal{T}_0).

Hence, $A_0 \wedge B_0 \wedge C_A \wedge C_B \wedge (\mathcal{H} \setminus C) \models_{\mathcal{T}_0} A_0 \wedge B_0 \wedge cRd \wedge (\mathcal{H} \setminus C)$. On the other hand, as $A_0 \wedge B_0 \models_{\mathcal{T}_0} \bigwedge_{i=1}^n c_i R_i d_i$, $A_0 \wedge B_0 \wedge \mathcal{H}$ is logically equivalent with $A_0 \wedge B_0 \wedge cRd \wedge (\mathcal{H} \setminus C)$, so $A_0 \wedge B_0 \wedge C_A \wedge C_B \wedge (\mathcal{H} \setminus C) \models_{\mathcal{T}_0} \perp$. By the induction hypothesis for $A_0 \wedge B_0 \wedge cRc_{f(t_1, \dots, t_n)} \wedge c_{f(t_1, \dots, t_n)} Rd$ and $\mathcal{H}' = \mathcal{H} \setminus C$ we know that there exists a set T' of terms such that $A_0 \wedge B_0 \wedge cRc_{f(t_1, \dots, t_n)} \wedge c_{f(t_1, \dots, t_n)} Rd \wedge (\mathcal{H}' \setminus \mathcal{H}'_{\text{mix}}) \wedge \mathcal{H}'_{\text{sep}} \models \perp$, and also (2) holds. Then (1) holds for $T = T' \cup \{t_1, \dots, t_n\}$. (2) can be proved similarly using the induction hypothesis.

(3) follows from the same induction schema taking into account the fact that, by strong interpolation, always if $A_0 \wedge B_0 \models c_i R_i d_i$ there exists t_i (containing only constants common to A_0 and B_0) with $A_0 \models c_i R_i t_i$ and $B_0 \models t_i R_i d_i$.⁵ Then A_0 is logically equivalent (in \mathcal{T}_0) to $A_0 \wedge \bigwedge_{i=1}^n c_i R_i t_i$, hence $A_0 \wedge C_A$ is logically equivalent to $A_0 \wedge cRc_{f(t_1, \dots, t_n)}$. (Similarly, B_0 is logically equivalent to $B_0 \wedge \bigwedge_{i=1}^n t_i R_i d_i$, so $B_0 \wedge C_B$ is logically equivalent to $B_0 \wedge c_{f(t_1, \dots, t_n)} Rd$.) By using the induction hypothesis, (3) follows easily. \square

An immediate consequence of Proposition 5.7 is Proposition 5.8.

Proposition 5.8. *Assume \mathcal{T}_0 satisfies Assumptions 1 and 2, the extension $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ satisfies Assumptions 4 and 5, and $\mathcal{K}_0 \wedge A_0 \wedge B_0 \wedge \text{Con}[D_A \wedge D_B]_0 \models_{\mathcal{T}_0} \perp$. Then there exists a set T of $\Sigma_0 \cup \Sigma_c$ -terms containing only constants common to A_0 and B_0 such that (if $\text{Con}_0^D = \text{Con}_0^{DA} \wedge \text{Con}_0^{DB} = \text{Con}_{0\text{sep}}$ and $\mathcal{K}_0^D = \mathcal{K}_0^{DA} \wedge \mathcal{K}_0^{DB} = \mathcal{K}_{0\text{sep}}$):*

$$\mathcal{K}_0^A \wedge \mathcal{K}_0^B \wedge \mathcal{K}_0^D \wedge A_0 \wedge B_0 \wedge \text{Con}_0^A \wedge \text{Con}_0^B \wedge \text{Con}_0^D \models_{\mathcal{T}_0} \perp. \quad (5.3)$$

As before, Σ_c contains the new constants $c_{f(t_1, \dots, t_n)}$, considered to be common to A_0 and B_0 , introduced for terms $f(t_1, \dots, t_n)$, with $t_1, \dots, t_n \in T$.

Proof. If \mathcal{K} only contains combinations of clauses of type (5.1) then all clauses in $\mathcal{K}_0 \wedge \text{Con}[D_A \wedge D_B]_0$ satisfy the restrictions on \mathcal{H} in Proposition 5.7. Thus Proposition 5.7 holds for $\mathcal{H} = \mathcal{K}_0 \wedge \text{Con}[D_A \wedge D_B]_0$. Therefore there exists a set T of $\Sigma_0 \cup \Sigma_c$ -terms containing only constants common to A_0 and B_0 such that $A_0 \wedge B_0 \wedge (\mathcal{H} \setminus \mathcal{H}_{\text{mix}}) \wedge \mathcal{H}_{\text{sep}}$. The statement of the theorem uses the description of $\mathcal{H} \setminus \mathcal{H}_{\text{mix}}$, denoted before by $\mathcal{K}_0^A \wedge \mathcal{K}_0^B$, as well as of \mathcal{H}_{sep} as $\mathcal{K}_0^{DA} \wedge \mathcal{K}_0^{DB} \wedge \text{Con}_0^{DA} \wedge \text{Con}_0^{DB}$. \square

Corollary 5.9. *Assume that the extension $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ satisfies Assumptions 1–5, and that $\mathcal{K}_0 \wedge A_0 \wedge B_0 \wedge \text{Con}[D_A \wedge D_B]_0 \models_{\mathcal{T}_0} \perp$. With the notation in Proposition 5.8 the following holds:*

- (1) *There exists a Π_0^c -formula I_0 containing only constants common to A_0, B_0 with $\mathcal{K}_0^A \wedge \mathcal{K}_0^{DA} \wedge A_0 \wedge \text{Con}_0^A \wedge \text{Con}_0^{DA} \models_{\mathcal{T}_0} I_0$ and $\mathcal{K}_0^B \wedge \mathcal{K}_0^{DB} \wedge B_0 \wedge \text{Con}_0^B \wedge \text{Con}_0^{DB} \wedge I_0 \models_{\mathcal{T}_0} \perp$.*
- (2) *There exists a ground Π^c -formula I containing only constants and function symbols which occur both in A and B such that $A \models_{\mathcal{T}_1} I$ and $B \wedge I \models_{\mathcal{T}_1} \perp$.*

⁵In this case we may need to separate even pure A and B clauses in \mathcal{H} as in **Case 2b**, in order to guarantee the separate entailment from A_0 and B_0 .

Proof.

- (1) is a direct consequence of Proposition 5.8, since $\mathcal{K}_0^A, \mathcal{K}_0^{AD}, \mathcal{K}_0^B, \mathcal{K}_0^{BD}$ are ground and we assumed that \mathcal{T}_0 has ground interpolation.
- (2) Let I be obtained from I_0 by recursively replacing each constant c_t introduced in the separation process with the term t . We show that I is an interpolant of $(A_0 \wedge D_A) \wedge (B_0 \wedge D_B)$ with respect to \mathcal{T}_1 , i.e. that (i) $A_0 \wedge D_A \models_{\mathcal{T}_1} I$ and (ii) $I \wedge B_0 \wedge D_B \models_{\mathcal{T}_1} \perp$.
- (i) Let (M, v) be a \mathcal{T}_1 -model that satisfies $A_0 \wedge D_A$. Being a model of \mathcal{T}_1 , (M, v) satisfies all instances of the axioms in \mathcal{K} and of the congruence axioms in $\mathcal{K}_0^A \wedge \mathcal{K}_0^{DA} \wedge \text{Con}_0^A \wedge \text{Con}_0^{DA}$ (and similarly for the B part). Thus, the restriction $(M|_{\Pi_0}, v)$ of (M, v) to the base theory satisfies $\mathcal{K}_0^A \wedge \mathcal{K}_0^{DA} \wedge A_0 \wedge \text{Con}_0^A \wedge \text{Con}_0^{DA}$, hence also I_0 . We thus proved that $A_0 \wedge D_A \models_{\mathcal{T}_1} I_0 \wedge D_A$. It is easy to see that $I_0 \wedge D_A \models_{\mathcal{T}_1} I$.
- (ii) Assume that $I \wedge B_0 \wedge D_B$ has a \mathcal{T}_1 -model (M, v) . Then $(M, v) \models I_0 \wedge B_0 \wedge D_B$, so its reduct to Π_0 is a model of \mathcal{T}_0 and of $\mathcal{K}_0^B \wedge \mathcal{K}_0^{DB} \wedge B_0 \wedge \text{Con}_0^B \wedge \text{Con}_0^{DB} \wedge I_0$. This contradicts the fact that the set of clauses above is unsatisfiable with respect to \mathcal{T}_0 . Thus, $I \wedge B_0 \wedge D_B \models_{\mathcal{T}_1} \perp$. \square

6. A PROCEDURE FOR HIERARCHICAL INTERPOLATION

We obtain a procedure for computing interpolants for $A \wedge B$ described in Figure 1.

Lemma 6.1. *Assume that the cycle in Step 2 of the procedure described in Figure 1 stops after processing all mixed clauses in \mathcal{H}_{mix} and moving their separated form into the set \mathcal{H}_{sep} . The following are equivalent:*

- (1) $A_0 \wedge D_A \wedge B_0 \wedge D_B \models_{\mathcal{T}_1} \perp$.
(2) $A_0 \wedge B_0 \wedge (\mathcal{H} \setminus \mathcal{H}_{\text{mix}}) \wedge \mathcal{H}_{\text{sep}} \models_{\mathcal{T}_0} \perp$.

Proof. (1) \Rightarrow (2) is a consequence of Theorems 4.7 and Proposition 5.8. As the conjunction in (2) corresponds to a subset of instances of $\mathcal{K} \wedge A_0 \wedge D_A \wedge B_0 \wedge D_B$, (2) implies (1). \square

Note: If $\mathcal{K}_0 \wedge A_0 \wedge B_0 \wedge \text{Con}[D_A \wedge D_B]_0 \models_{\mathcal{T}_0} \perp$ then no matter which terms are chosen for separating mixed clauses in $\text{Con}[D_A \wedge D_B]_0 \wedge \mathcal{K}_0$, we obtain a separated conjunction of clauses unsatisfiable with respect to \mathcal{T}_0 . Lemma 6.1 shows that if the set of clauses obtained when the procedure stops is satisfiable then $A \wedge B$ was satisfiable, and conversely, so the procedure can be used to test satisfiability and to compute interpolants at the same time. (However, it is more efficient to first test $A \wedge B \models_{\mathcal{T}_1} \perp$.)

Theorem 6.2. *Let \mathcal{T}_0 be a theory with the following properties:*

- Assumption 1:** \mathcal{T}_0 is convex with respect to the set Pred (including equality \approx);
Assumption 2: \mathcal{T}_0 is P -interpolating with respect to a subset $P \subseteq \text{Pred}$ and the separating terms t_i can be effectively computed; and
Assumption 3: \mathcal{T}_0 has ground interpolation

(note that we assume, in particular, that \mathcal{T}_0 satisfies a stronger form of Assumption 2). Assume that the extension $\mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ of \mathcal{T}_0 has the following properties:

- Assumption 4:** \mathcal{T}_1 is a local extension of \mathcal{T}_0 ; and

Given: Local extension $\mathcal{T}_0 \subseteq \mathcal{T}_1 = \mathcal{T}_0 \cup \mathcal{K}$ which satisfies Assumptions 1–5;
 Conjunctions A and B of literals over the signature of \mathcal{T}_1 such that $A \wedge B \models_{\mathcal{T}_1} \perp$

Task: Find an interpolant for $A \wedge B$, i.e. a formula I with $A \models_{\mathcal{T}_1} I$ and $I \wedge B \models_{\mathcal{T}_1} \perp$.

Method:

Step 1: *Purify.*

Using locality, flattening and purification we obtain a set $\mathcal{H} \wedge A_0 \wedge B_0$ of formulae in the base theory, where $\mathcal{H} = \mathcal{K}_0 \wedge \text{Con}[D_A \wedge D_B]_0$.

Let $\Delta := \top$.

Step 2: *Reduction to an interpolation problem in the base theory.*

Repeat as long as possible:

Let $C \in \mathcal{H}$ whose premise is entailed by $A_0 \wedge B_0 \wedge \Delta$.

If C is mixed, compute terms t_i which separate the premises in C , and separate the clause into an instance C_1 of monotonicity and an instance C_2 of a clause in \mathcal{K} as in the proof of Case 2b in Prop. 5.7.

Remove C from \mathcal{H} , and add C_1, C_2 to \mathcal{H}_{sep} and their conclusions to Δ .

Otherwise move C to \mathcal{H}_{sep} and add its conclusion to Δ .

Step 3: *Interpolation in the base theory.*

Compute an interpolant I_0 in \mathcal{T}_0 for the separated formula $\overline{A}_0 \wedge \overline{B}_0$ (logically equivalent to $A_0 \wedge B_0 \wedge (\mathcal{H} \setminus \mathcal{H}_{\text{mix}}) \wedge \mathcal{H}_{\text{sep}}$) obtained this way.

Step 4: *Construct interpolant for the initial problem.*

Construct an interpolant I in \mathcal{T}_1 from I_0 by recursively replacing each constant c_t introduced in the separation process with the term t , as explained in Corollary 5.9(2).

Figure 1: Procedure for hierarchical interpolant computation

Assumption 5: \mathcal{K} consists of the following type of combinations of clauses:

$$\begin{cases} x_1 R_1 s_1 \wedge \cdots \wedge x_n R_n s_n \rightarrow f(x_1, \dots, x_n) R g(y_1, \dots, y_n) \\ x_1 R_1 y_1 \wedge \cdots \wedge x_n R_n y_n \rightarrow f(x_1, \dots, x_n) R f(y_1, \dots, y_n) \end{cases}$$

where $n \geq 1$, x_1, \dots, x_n are variables, R_1, \dots, R_n, R are binary relations, $R_1, \dots, R_n \in P$, R is transitive, and each s_i is either a variable among the arguments of g , or a term of the form $f_i(z_1, \dots, z_k)$, where $f_i \in \Sigma_1$ and all the arguments of f_i are variables occurring among the arguments of g (i.e. combinations of clauses of type (5.1)).

For every conjunction $A \wedge B$ of ground unit clauses in the signature Π^c of \mathcal{T}_1 (possibly containing additional constants) with $A \wedge B \models_{\mathcal{T}_1} \perp$ the procedure for hierarchical interpolation terminates and it computes an interpolant I for $A \wedge B$.

Proof. To prove termination note that at every execution of the loop in Step 2, the number of mixed clauses decreases. All entailment tests in Step 2 are decidable (their complexity is discussed separately). By Assumption (2'), terms t_i which separate the premises can be computed in finite time. This shows that Step 2 terminates. Termination of Steps 1, 3 and 4 is immediate.

We now prove correctness. We know that $A \wedge B \models_{\mathcal{T}_1} \perp$, so $A_0 \wedge D_A \wedge B_0 \wedge D_B \models_{\mathcal{T}_1} \perp$. Hence, by Lemma 6.1, when the cycle in Step 2 of the procedure terminates replacing the

set of clauses \mathcal{H}_{mix} with \mathcal{H}_{sep} , then $A_0 \wedge B_0 \wedge (\mathcal{H} \setminus \mathcal{H}_{\text{mix}}) \wedge \mathcal{H}_{\text{sep}} \models_{\mathcal{T}_0} \perp$. By construction, at termination $\mathcal{H} \setminus \mathcal{H}_{\text{mix}} \wedge \mathcal{H}_{\text{sep}}$ contains only pure (unmixed) clauses. We can use the alternative form of $\mathcal{H} \setminus \mathcal{H}_{\text{mix}}$, denoted before by $\mathcal{K}_0^A \wedge \mathcal{K}_0^B$, as well as of \mathcal{H}_{sep} as $\mathcal{K}_0^{DA} \wedge \mathcal{K}_0^{DB} \wedge \text{Con}_0^{DA} \wedge \text{Con}_0^{DB}$. In Step 3 an interpolant I_0 containing only constants common to A_0 , B_0 with $\mathcal{K}_0^A \wedge \mathcal{K}_0^{DA} \wedge A_0 \wedge \text{Con}_0^A \wedge \text{Con}_0^{DA} \models_{\mathcal{T}_0} I_0$ and $\mathcal{K}_0^B \wedge \mathcal{K}_0^{DB} \wedge B_0 \wedge \text{Con}_0^B \wedge \text{Con}_0^{DB} \wedge I_0 \models_{\mathcal{T}_0} \perp$ is computed. In Step 4, a ground Π^c -formula I containing only constants and function symbols which occur both in A and B such that $A \models_{\mathcal{T}_1} I$ and $B \wedge I \models_{\mathcal{T}_1} \perp$ is constructed starting from I as explained in Corollary 5.9. This is the interpolant of $A \wedge B$. \square

Complexity: Assume that in \mathcal{T}_0 for a formula of length n :

- (a) interpolants can be computed in time $g(n)$,
- (b) P -interpolating terms can be computed in time $h(n)$,
- (c) entailment can be checked in time $k(n)$.

The size n of the set of clauses obtained after the preprocessing phase is quadratic in the size of the input. Under the assumptions (a), (b), (c) above the procedure above computes an interpolant in time of order $n \cdot (k(n) + h(n)) + g(n)$.

Remark 6.3. If \mathcal{T}_0 satisfies Assumptions 1 and 3 at the beginning of Section 5.2. and is strongly P -interpolating, the procedure above can be changed (according to the proof of Proposition 5.7(3)) to separate *all* clauses in \mathcal{H} and store the conclusions of the separated clauses in $\Delta = \Delta_A \cup \Delta_B$. If $\mathcal{K}_0 \wedge A_0 \wedge B_0 \wedge \text{Con}[D_A \wedge D_B]_0 \models_{\mathcal{T}_0} \perp$ then there exists a set T of $\Sigma_0 \cup \Sigma_c$ -terms containing only constants common to A_0 and B_0 , and common new constants in a set Σ_c such that the terms in T can be used to separate $\text{Con}[D_A \wedge D_B]_0 \cup \mathcal{K}_0$ into $\mathcal{H}_{\text{sep}} = (\mathcal{K}_0^{DA} \wedge \text{Con}_0^{DA}) \wedge (\mathcal{K}_0^{DB} \wedge \text{Con}_0^{DB})$, where:

$$\mathcal{H}_{\text{sep}} = \{ (\bigwedge_{i=1}^n c_i R_i t_i \rightarrow c R c_{f(t_1, \dots, t_n)}) \wedge (\bigwedge_{i=1}^n t_i R_i d_i \rightarrow c_{f(t_1, \dots, t_n)} R d) \mid \bigwedge_{i=1}^n c_i R_i d_i \rightarrow c R d \in \text{Con}_0 \cup \mathcal{K}_0 \} = (\mathcal{K}_0^{DA} \wedge \text{Con}_0^{DA}) \wedge (\mathcal{K}_0^{DB} \wedge \text{Con}_0^{DB})$$

such that for each premise $c_i R_i d_i$ of a rule in $\text{Con}[D_A \wedge D_B]_0 \cup \mathcal{K}_0$, at some step in the procedure $A_0 \wedge B_0 \wedge \Delta_A \wedge \Delta_B \models c_i R_i d_i$ and there exists $t_i \in T$ such that $A_0 \wedge \Delta_A \models c_i R_i t_i$ and $B_0 \wedge \Delta_B \models t_i R_i d_i$. In this case $A_0 \wedge \mathcal{K}_0^{DA} \wedge \text{Con}_0^{DA}$ is logically equivalent to \overline{A}_0 , and $B_0 \wedge \mathcal{K}_0^{DB} \wedge \text{Con}_0^{DB}$ is logically equivalent to \overline{B}_0 , where \overline{A}_0 , \overline{B}_0 are the following conjunctions of literals:

$$\begin{aligned} \overline{A}_0 &= A_0 \wedge \bigwedge \{ c R c_{f(\bar{t})} \mid \text{conclusion of some clause } (\Gamma \rightarrow c R c_{f(\bar{t})}) \in \mathcal{K}_0^{DA} \cup \text{Con}_0^{DA} \} \\ \overline{B}_0 &= B_0 \wedge \bigwedge \{ c_{f(\bar{t})} R d \mid \text{conclusion of some clause } (\Gamma \rightarrow c_{f(\bar{t})} R d) \in \mathcal{K}_0^{DB} \cup \text{Con}_0^{DB} \}. \end{aligned}$$

Thus, if for instance in \mathcal{T}_0 interpolants for conjunctions of ground literals are always again conjunctions of ground literals, the same is also true in the extension.

Example 6.4. The following theory extensions have ground interpolation:

- (a) Extensions of any theory in Theorem 5.4(1)–(4) with free function symbols.
- (b) Extensions of the theories in Theorem 5.4(2),(4) with monotone functions.
- (c) Extensions of the theories in Theorem 5.4(2),(4) with $\text{Leq}(f, g) \wedge \text{Mon}(f)$.
- (d) Extensions of the theories in Theorem 5.4(2),(4) with $\text{SGc}(f, g_1) \wedge \text{Mon}(f, g_1)$.
- (e) Extensions of any theory in Theorem 5.4(1)–(4) with $\text{Bound}^t(f)$ or $\text{GBound}^t(f)$ (where t is a term and ϕ a set of literals in the base theory).
- (f) Extensions of the theories in Theorem 5.4(2),(4) with $\text{Mon}(f) \wedge \text{Bound}^t(f)$, if t is monotone in its variables.

- (g) $\mathbb{R} \cup (\mathbb{L}_f^\lambda)$, the extension of the theory of reals with a unary function which is λ -Lipschitz in a point x_0 , where (\mathbb{L}_f^λ) is $\forall x |f(x) - f(x_0)| \leq \lambda \cdot |x - x_0|$.

Proof. (a)–(d) are direct consequences of Corollary 5.9, since all sets of extension clauses are of type (5.1). For extensions of linear arithmetic note that due to the totality of \leq we can always assume that A and B are positive, so convexity with respect to \approx is sufficient (cf. proof of Proposition 5.7). Also, in [11] we show that being P -interpolating with respect to \leq is sufficient in this case. (e)–(g) follow from Corollary 5.9 and the fact that if each clause in \mathcal{K} contains only one occurrence of an extension function, no mixed instances can be generated when computing $\mathcal{K}[A \wedge B]$. \square

7. APPLICATIONS

7.1. Modular reasoning in local combinations of theories. Let $\mathcal{T}_i = \mathcal{T}_0 \cup \mathcal{K}_i, i = 1, 2$ be local extensions of a theory \mathcal{T}_0 with signature $\Pi_0 = (\Sigma_0, \text{Pred})$, where $\Sigma_0 = \Sigma_1 \cap \Sigma_2$. Assume that (a) all variables in \mathcal{K}_i occur below some extension function, (b) the extension $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}_1 \cup \mathcal{K}_2$ is local⁶, and (c) \mathcal{T}_0 has ground interpolation.

Let G be a set of ground clauses in the signature $\Pi^c = (\Sigma_0 \cup \Sigma_1 \cup \Sigma_2 \cup \Sigma_c, \text{Pred})$. G can be flattened and purified, so we assume without loss of generality that $G = G_1 \wedge G_2$, where G_1, G_2 are flat and linear sets of clauses in the signatures Π_1, Π_2 respectively, i.e. for $i = 1, 2$, $G_i = G_i^0 \wedge G_0 \wedge D_i$, where G_i^0 and G_0 are clauses in the base theory and D_i conjunctions of unit clauses of the form $f(c_1, \dots, c_n) = c, f \in \Sigma_i \setminus \Sigma_0$.

Theorem 7.1. *With the notations above, assume that $G_1 \wedge G_2 \models_{\mathcal{T}_1 \cup \mathcal{T}_2} \perp$. Then there exists a ground formula I , containing only constants shared by G_1 and G_2 , with $G_1 \models_{\mathcal{T}_1 \cup \mathcal{T}_2} I$ and $I \wedge G_2 \models_{\mathcal{T}_1 \cup \mathcal{T}_2} \perp$.*

Proof. By Theorem 4.7, the following are equivalent:

- (1) $\mathcal{T}_0 \cup \mathcal{K}_1 \cup \mathcal{K}_2 \cup (G_1^0 \wedge G_0 \wedge D_1) \wedge (G_2^0 \wedge G_0 \wedge D_2) \models \perp$,
- (2) $\mathcal{T}_0 \cup \mathcal{K}_1[G_1] \wedge \mathcal{K}_2[G_2] \wedge (G_1^0 \wedge G_0 \wedge D_1) \wedge (G_2^0 \wedge G_0 \wedge D_2) \models \perp$,
- (3) $\mathcal{K}_1^0 \wedge \mathcal{K}_2^0 \wedge (G_1^0 \wedge G_0) \wedge (G_2^0 \wedge G_0) \wedge \text{Con}_1 \wedge \text{Con}_2 \models_{\mathcal{T}_0} \perp$, where, for $j = 1, 2$,

$$\text{Con}_j = \bigwedge_{i=1}^n \{ \bigwedge_{i=1}^n c_i \approx d_i \rightarrow c \approx d \mid f(c_1, \dots, c_n) \approx c, f(d_1, \dots, d_n) \approx d \in D_j \},$$

and \mathcal{K}_i^0 is the formula obtained from $\mathcal{K}_i[G_i]$ after purification and flattening, taking into account the definitions from D_i . Let $A = \mathcal{K}_1^0 \wedge (G_1^0 \wedge G_0) \wedge \text{Con}_1$ and $B = \mathcal{K}_2^0 \wedge (G_2^0 \wedge G_0) \wedge \text{Con}_2$. By assumption (a), A and B are both ground. As A and B have no extension function symbols in common and only share the constants which G_1 and G_2 share, there exists an interpolant I_0 in the signature Π_0 , containing only Σ_0 -function symbols and only constants shared by G_1, G_2 , such that $A \models_{\mathcal{T}_0} I_0$ and $B \wedge I_0 \models_{\mathcal{T}_0} \perp$. An interpolant for $G_1 \wedge G_2$ with respect to \mathcal{T}_1 can now be obtained by replacing the newly introduced constants by the terms they replaced. \square

⁶If \mathcal{T}_0 is a $\forall \exists$ theory then (b) is implied by (a) and the locality of $\mathcal{T}_1, \mathcal{T}_2$ [16].

By Remark 6.3, if \mathcal{T}_0 is strongly P -interpolating and has equational interpolation then I is a conjunction of literals, so for modularly proving $G_1 \wedge G_2 \models_{\mathcal{T}_1} \perp$ only conjunctions of ground literals containing constants shared by G_1, G_2 need to be exchanged between specialized provers for \mathcal{T}_1 and \mathcal{T}_2 .

7.2. Terminological Databases. Consider the combination of databases in Section 2.1. We prove that

$$\Gamma_0 \wedge (\mathcal{T}_1 \wedge \Gamma_1) \wedge (\mathcal{T}_2 \wedge \Gamma_2) \models_{\mathcal{T}} \perp. \quad (7.1)$$

where \mathcal{T} is the extension $\text{SLat} \cup \bigcup_{f \in R_1 \cup R_2} \text{Mon}(f)$ of the theory of semilattices with 0 and monotone functions corresponding to the rôles in $R_1 \cup R_2$, where:

$$\Gamma_0 = \{\text{organic} \wedge \text{inorganic} \approx 0, \quad \text{organic} \leq \text{substance}, \quad \text{inorganic} \leq \text{substance}\}$$

$$\mathcal{T}_1 = \{\text{cat-oxydation} \approx \text{substance} \wedge \text{catalyzes}(\text{oxydation})\}$$

$$\Gamma_1 = \{\text{reaction} \leq \text{oxydation}, \text{cat-oxydation} \leq \text{inorganic}, \text{cat-oxydation} \not\approx 0\}, \Gamma_2 = \{\text{enzyme} \not\approx 0\}$$

$$\mathcal{T}_2 = \{\text{reaction} \approx \text{process} \wedge \text{produces}(\text{substance}), \quad \text{enzyme} \approx \text{organic} \wedge \text{catalyzes}(\text{reaction})\}$$

In order to find the mistake we look for an explanation for the inconsistency in the joint language of the two databases. Based on results on hierarchical reasoning in extensions of theories in [15] we can show that if we purify the problem by introducing definitions for the terms starting with an extension role symbol we can reduce the satisfiability test to a satisfiability test in the base theory. Thus, (7.1) is equivalent to the unsatisfiability of a set of clauses over the theory of semilattices, namely: $C_{T_0} \wedge C_{T_1} \wedge C_{\Gamma_1} \wedge C_{T_2} \wedge C_{\Gamma_2} \wedge N$ where C_{T_i} and C_{Γ_i} are as in the table below (the shared symbols are underlined):

	Extension	Base	
	(Definitions)	Terminology(C_T)	Constraints(C_Γ)
0			<u>organic</u> \wedge <u>inorganic</u> ≈ 0 <u>organic</u> \leq <u>substance</u> <u>inorganic</u> \leq <u>substance</u>
1	co \approx catalyzes(oxydation)	cat-oxydation \approx <u>substance</u> \wedge co	<u>reaction</u> \leq oxdation cat-oxydation \leq <u>inorganic</u> cat-oxydation $\not\approx 0$
2	ps \approx produces(substance) cr \approx catalyzes(reaction)	<u>reaction</u> \approx process \wedge ps enzyme \approx <u>organic</u> \wedge cr	enzyme $\not\approx 0$

The following instances of the congruence or monotonicity axioms need to be considered:

$$\text{oxydation} \triangleright \text{reaction} \rightarrow \text{cp} \triangleright \text{cr}, \quad \text{where } \triangleright \in \{\approx, \leq, \geq\}.$$

They are not mixed. The conjunction of formulae in the base theory is unsatisfiable in the theory of semilattices. It can be split into a part A containing only concepts in **AChem** and a part B containing only concepts in **BioChem**. An interpolant for $A \wedge B$ in the theory of semilattices with 0 is $I_0 = \text{substance} \wedge \text{cr} \leq \text{inorganic}$. Thus, $I = \text{substance} \wedge \text{catalyzes}(\text{reaction}) \leq \text{inorganic}$ is an interpolant for $A \wedge B$. This is an explanation for the inconsistency of $A \wedge B$, and may help to find the error more easily than the initial proof of unsatisfiability. For this we can, for instance, analyze the (shorter) proofs of $A \models I$ and $B \wedge I \models \perp$ and note that the constraint $\text{reaction} \leq \text{oxydation}$ is used in the proof of $A \models I$.

7.3. Verification. Consider the verification example from Section 2.2. We illustrate our method for generating interpolants for a formula corresponding to a path of length 2 from an initial state to an unsafe state:

$$G = l < L_{\text{alarm}} \wedge l' \approx \text{in}(l, t' - t) \wedge t' \approx k(t) \wedge l' \geq L_{\text{alarm}} \wedge \\ l'' \approx \text{in}(\text{out}(l', t_1'' - t'), t_2'' - t') \wedge t_1'' \approx g(t') \wedge t_2'' \approx h(t') \wedge \neg l'' < L_{\text{overflow}}.$$

Hierarchical reasoning. The extension \mathcal{T}_1 of linear arithmetic with the clauses \mathcal{K} in Section 2 is local, so to prove $G \models_{\mathcal{T}_1} \perp$ it is sufficient to consider ground instances $\mathcal{K}[G]$ in which all extension terms already occur in G . After flattening and purifying $\mathcal{K}[G] \wedge G$, we separate the problem into a definition part (**Extension**) and a base part $G_0 \wedge \mathcal{K}_0$. By Theorem 4.7 [15], the problem can be reduced to testing the satisfiability in the base theory of the conjunction $G_0 \wedge \mathcal{K}_0 \wedge \text{Con}_0$. As this conjunction is unsatisfiable with respect to \mathcal{T}_0 , G is unsatisfiable.

Extension	Base	
(Definitions)	G_0	$\mathcal{K}_0 \wedge \text{Con}_0$
$l' \approx \text{in}(l, e_1)$	$l < L_{\text{alarm}}$	$\mathcal{K}_0 : l < L_{\text{alarm}} \wedge 0 \leq e_1 \leq \Delta t \rightarrow l' < L_{\text{overflow}}$
$c_2^1 \approx \text{out}(l', e_2^1)$	$l' \geq L_{\text{alarm}}$	$c_2^1 < L_{\text{alarm}} \wedge 0 \leq e_2^1 \leq \Delta t \rightarrow l'' < L_{\text{overflow}}$
$l'' \approx \text{in}(c_2^1, e_2^2)$	$e_1 \approx t' - t$	$l' < L_{\text{overflow}} \wedge e_2^1 \geq \delta t \rightarrow c_2^1 < L_{\text{alarm}}$
$t' \approx k(t)$	$e_2^1 \approx t_1'' - t'$	$0 \leq \delta t \leq t_1'' - t' \leq t_2'' - t' \leq \Delta t$
$t_1'' \approx g(t')$	$e_2^2 \approx t_2'' - t'$	$0 \leq t' - t \leq \Delta t$
$t_2'' \approx h(t')$	$\neg l'' \leq L_{\text{overflow}}$	$\text{Con}_0 : l \approx c_2^1 \wedge e_1 \approx e_2^2 \rightarrow l' \approx l''$

Interpolation. Let A and B be given by:

$$A = l < L_{\text{alarm}} \wedge e_1 \approx t' - t \wedge l' \approx \text{in}(l, e_1) \wedge t' \approx k(l) \\ B = l' \geq L_{\text{alarm}} \wedge c_2^1 \approx \text{out}(l', e_2^1) \wedge l'' \approx \text{in}(c_2^1, e_2^2) \wedge e_2^1 \approx t_1'' - t' \wedge e_2^2 \approx t_2'' - t' \wedge \\ t_1'' \approx g(t') \wedge t_2'' \approx h(t') \wedge \neg l'' < L_{\text{overflow}}.$$

The set of constants which occur in A is $\{l, t, e_1, l', t'\}$. In B occur $\{l', t', c_2^1, l'', t_1'', t_2'', e_2^1, e_2^2\}$. The shared constants are l' and t' . To generate an interpolant for $A \wedge B$, we partition the clauses in $A_0 \wedge B_0 \wedge \mathcal{K}_0 \wedge \text{Con}_0 = A_0 \wedge B_0 \wedge \mathcal{K}_0^A \wedge \mathcal{K}_0^B \wedge \text{Con}_0$, where:

$$A_0 = l < L_{\text{alarm}} \wedge e_1 \approx t' - t \\ B_0 = l' \geq L_{\text{alarm}} \wedge e_2^1 \approx t_1'' - t' \wedge e_2^2 \approx t_2'' - t' \wedge \neg l'' \leq L_{\text{overflow}} \\ \mathcal{K}_0^A = (l < L_{\text{alarm}} \wedge 0 \leq e_1 \leq \Delta t \rightarrow l' < L_{\text{overflow}}) \wedge (0 \leq t' - t \leq \Delta t) \\ \mathcal{K}_0^B = (c_2^1 < L_{\text{alarm}} \wedge 0 \leq e_2^1 \leq \Delta t \rightarrow l'' < L_{\text{overflow}}) \wedge (l' < L_{\text{overflow}} \wedge e_2^1 \geq \delta t \rightarrow c_2^1 < L_{\text{alarm}}) \\ \wedge (0 \leq \delta t \leq t_1'' - t' \leq t_2'' - t' \leq \Delta t).$$

The clause in Con_0 is mixed. Since already the conjunction of the formulae in $A_0 \wedge B_0 \wedge \mathcal{K}_0^A \wedge \mathcal{K}_0^B$ is unsatisfiable, Con_0 is not needed to prove unsatisfiability. The conjunction of the formulae in $A_0 \wedge B_0 \wedge \mathcal{K}_0^A \wedge \mathcal{K}_0^B$ is equivalent to $A'_0 \wedge B'_0$, where

$$A'_0 = l < L_{\text{alarm}} \wedge e_1 \approx t' - t \wedge (0 \leq t' - t \leq \Delta t) \wedge l' < L_{\text{overflow}} \\ B'_0 = l' > L_{\text{alarm}} \wedge e_2^1 \approx t_1'' - t' \wedge e_2^2 \approx t_2'' - t' \wedge (0 \leq \delta t \leq t_1'' - t' \leq t_2'' - t' \leq \Delta t) \wedge \\ \neg l'' < L_{\text{overflow}} \wedge \neg c_2^1 < L_{\text{alarm}} \wedge \neg l' < L_{\text{overflow}}.$$

The interpolant for $A'_0 \wedge B'_0$ is $l' < L_{\text{overflow}}$, which is also an interpolant for $A \wedge B$.

The abstraction defined in Section 2.2 can then be refined by introducing another predicate $L' < L_{\text{overflow}}$.

8. CONCLUSIONS

We presented a method for obtaining simple interpolants in theory extensions. We identified situations in which it is possible to do this in a hierarchical manner, by using a prover and a procedure for generating interpolants in the base theory as “black-boxes”. This allows us to use the properties of \mathcal{T}_0 (e.g. the form of interpolants) to control the form of interpolants in the extension \mathcal{T}_1 . We discussed applications of interpolation in verification and knowledge representation.

The method we presented can be applied to a class of theories which is more general than that considered in McMillan [8] (extension of linear rational arithmetic with uninterpreted function symbols). Our method is orthogonal to the method for generating interpolants for combinations of theories over disjoint signatures from Nelson-Oppen-style unsatisfiability proofs proposed by Yorsh and Musuvathi in [19], as it allows us to consider combinations of theories over non-disjoint signatures.

The hierarchical interpolation method presented here was in particular used for efficiently computing interpolants in the special case of the extension of linear arithmetic with free function symbols in [11]; the algorithm we used in that paper (on which an implementation is based) differs a bit from the one presented here in being tuned to the constrained based approach used in [11]. The implementation was integrated into the predicate discovery procedure of the software verification tools BLAST [4] and ARMC [10]. First tests suggest that the performance of our method is of the same order of magnitude as the methods which construct interpolants from proofs, and considerably faster on many examples. In addition, our method can handle systems which pose problems to other interpolation-based provers: we can handle problems containing both strict and nonstrict inequalities, and it allows us to verify examples that require predicates over up to four variables. Details about the implementation and benchmarks for the special case of linear arithmetic + free function symbols are described in [11].

Although the method we presented here is based on a hierarchical reduction of proof tasks in a local extension of a given theory \mathcal{T}_0 to proof tasks in \mathcal{T}_0 , the results presented in Section 5 (in particular the separation technique described in Proposition 5.7) and in Section 6 also hold for non-purified formulae (i.e. they also hold if we do not perform the step of introducing new constant names $c_{f(d)}$ for the ground terms $f(d)$ which occur in the problem or during the separation process). Depending on the properties of \mathcal{T}_0 , techniques for reasoning and interpolant generation in the extension of \mathcal{T}_0 with free function symbols e.g. within state of the art SMT solvers can then be used. We can, therefore, use the results in Sections 5 and 6 to extend in a natural way existing methods for interpolant computation which take advantage of state of the art SMT technology (cf. e.g. [3]) to the more complex types of theory extensions with sets of axioms of type (5.1) we considered here.

An immediate application of our method is to verification by abstraction-refinement; there are other potential applications (e.g. goal-directed overapproximation for achieving faster termination, or automatic invariant generation) which we would like to study. We would also like to analyze in more detail the applications to reasoning in complex knowledge bases.

Acknowledgements. I thank Andrey Rybalchenko for interesting discussions. I thank the referees for helpful comments.

This work was partly supported by the German Research Council (DFG) as part of the Transregional Collaborative Research Center “Automatic Verification and Analysis of Complex Systems” (SFB/TR 14 AVACS). See www.avacs.org for more information.

REFERENCES

- [1] F. Baader and S. Ghilardi. Connecting many-sorted theories. In R. Nieuwenhuis, editor, *20th International Conference on Automated Deduction (CADE-20)*, LNAI 3632, pages 278–294. Springer, 2005.
- [2] P.D. Bacsich. Amalgamation properties and interpolation theorem for equational theories. *Algebra Universalis*, 5:45–55, 1975.
- [3] A. Cimatti, A. Griggio, and R. Sebastiani. Efficient Interpolant generation in satisfiability modulo theories. In *TACAS’2008: Tools and Algorithms for the Construction and Analysis of Systems, LNCS 4963*, pages 397–412, Springer, 2008.
- [4] T. A. Henzinger, R. Jhala, R. Majumdar, and K. L. McMillan. Abstractions from proofs. In *POPL’2004: Principles of Programming Languages*, pages 232–244. ACM Press, 2004.
- [5] B. Jónsson. Extensions of relational structures. In J.W. Addison, L. Henkin, and A. Tarski, editors, *The Theory of Models, Proc. of the 1963 Symposium at Berkeley*, pages 146–157, Amsterdam, 1965. North-Holland.
- [6] D. Kapur, R. Majumdar, C. Zarba. Interpolation for data structures. In *Proc. 14th ACM SIGSOFT International Symposium on Foundations of Software Engineering*, pages 105–116, ACM 2006.
- [7] K.L. McMillan. Interpolation and SAT-based model checking. In *CAV’2003: Computer Aided Verification, LNCS 2725*, pages 1–13. Springer, 2003.
- [8] K.L. McMillan. An interpolating theorem prover. In *TACAS’2004: Tools and Algorithms for the Construction and Analysis of Systems, LNCS 2988*, pages 16–30. Springer, 2004.
- [9] K.L. McMillan. Applications of Craig interpolants in model checking. In *TACAS’2005: Tools and Algorithms for the Construction and Analysis of Systems, LNCS 3440*, pages 1–12. Springer, 2005.
- [10] A. Podelski and A. Rybalchenko. ARMC: the logical choice for software model checking with abstraction refinement. In *PADL’2007: Practical Aspects of Declarative Languages, LNCS 4354*, pages 245–259, Springer, 2007.
- [11] A. Rybalchenko and V. Sofronie-Stokkermans. Constraints for interpolation. Constraint solving for interpolation. In B. Cook and A. Podelski, editors, *Proceedings of the 8th International Conference on Verification, Model Checking and Abstract Interpretation (VMCAI 2007)*, LNCS 4349, pages 346–362, Springer Verlag, 2007.
- [12] V. Sofronie-Stokkermans. On the universal theory of varieties of distributive lattices with operators: Some decidability and complexity results. In H. Ganzinger, editor, *Proceedings of CADE-16, LNAI 1632*, pages 157–171, Springer Verlag, 1999.
- [13] V. Sofronie-Stokkermans. Resolution-based decision procedures for the universal theory of some classes of distributive lattices with operators. *Journal of Symbolic Computation*, 36(6):891–924, 2003.
- [14] V. Sofronie-Stokkermans. Automated theorem proving by resolution in non-classical logics. In *4th Int. Conf. Journées de l’Informatique Messine: Knowledge Discovery and Discrete Mathematics (JIM-03)*, pages 151–167, 2003.
- [15] V. Sofronie-Stokkermans. Hierarchic reasoning in local theory extensions. In R. Nieuwenhuis, editor, *20th International Conference on Automated Deduction (CADE-20)*, LNAI 3632, pages 219–234. Springer, 2005.
- [16] V. Sofronie-Stokkermans. Hierarchical and Modular Reasoning in Complex Theories: The Case of Local Theory Extensions. In B. Konev and F. Wolter, editors, *Frontiers of Combining Systems, 6th International Symposium, (FroCoS 2007)*, LNCS 4720, pages 47–71, Springer, 2007.
- [17] V. Sofronie-Stokkermans and C. Ihlemann. Automated reasoning in some local extensions of ordered structures. *Proceedings of ISMVL 2007*, IEEE Computer Society, 2007.
- [18] A. Wroński. On a form of equational interpolation property. In *Foundations of logic and linguistics (Salzburg, 1983)*, pages 23–29, New York, 1985. Plenum.

- [19] G. Yorsh and M. Musuvathi. A combination method for generating interpolants. In R. Nieuwenhuis, editor, *20th International Conference on Automated Deduction (CADE-20)*, LNAI 3632, pages 353–368. Springer, 2005.

APPENDIX A. AMALGAMATION AND INTERPOLATION

There exist results which relate ground interpolation to amalgamation or the injection transfer property [5, 2, 18] and thus allow us to recognize many theories with ground interpolation.

If $\Pi = (\Sigma, \text{Pred})$ is a signature and \mathcal{A}, \mathcal{B} are Π -structures, we say that:

- a map $h : \mathcal{A} \hookrightarrow \mathcal{B}$ is a *homomorphism* if it preserves the truth of positive literals, i.e. has the property that if $f_A(a_1, \dots, a_n) = a$ then $f_B(h(a_1), \dots, h(a_n)) = h(a)$, and if $P_A(a_1, \dots, a_n)$ is true then $P_B(h(a_1), \dots, h(a_n))$ is true.
- a map $i : \mathcal{A} \hookrightarrow \mathcal{B}$ is an *embedding* if it preserves the truth of both positive and negative literals, i.e. $P_A(a_1, \dots, a_n)$ is true (in \mathcal{A}) if and only if $P_B(i(a_1), \dots, i(a_n))$ is true (in \mathcal{B}) for any predicate symbol, including equality. Thus, an embedding is an injective homomorphism which also preserves the truth of negative literals.

Definition A.1. Let $\Pi = (\Sigma, \text{Pred})$ be a signature, and let \mathcal{M} be a class of Π -structures.

- (1) We say that \mathcal{M} has the *amalgamation property* (AP) if for any $\mathcal{A}, \mathcal{B}_1, \mathcal{B}_2 \in \mathcal{M}$ and any embeddings $i_1 : \mathcal{A} \hookrightarrow \mathcal{B}_1$ and $i_2 : \mathcal{A} \hookrightarrow \mathcal{B}_2$ there exists a structure $\mathcal{C} \in \mathcal{M}$ and embeddings $j_1 : \mathcal{B}_1 \hookrightarrow \mathcal{C}$ and $j_2 : \mathcal{B}_2 \hookrightarrow \mathcal{C}$ such that $j_1 \circ i_1 = j_2 \circ i_2$.
- (2) \mathcal{M} has the *injection transfer property* (ITP) if for any $\mathcal{A}, \mathcal{B}_1, \mathcal{B}_2 \in \mathcal{M}$, any embedding $i_1 : \mathcal{A} \hookrightarrow \mathcal{B}_1$ and any homomorphism $f_2 : \mathcal{A} \rightarrow \mathcal{B}_2$ there exists a structure $\mathcal{C} \in \mathcal{M}$, a homomorphism $f_1 : \mathcal{B}_1 \rightarrow \mathcal{C}$ and an embedding $j_2 : \mathcal{B}_2 \hookrightarrow \mathcal{C}$ such that $f_1 \circ i_1 = j_2 \circ f_2$.

Definition A.2. An equational theory \mathcal{T} (in signature $\Pi = (\Sigma, \text{Pred})$ where $\text{Pred} = \{\approx\}$) has the *equational interpolation property* if whenever

$$\bigwedge_i A_i(\bar{a}, \bar{c}) \wedge \bigwedge_j B_j(\bar{c}, \bar{b}) \wedge \neg B(\bar{c}, \bar{b}) \models_{\mathcal{T}} \perp,$$

where A_i, B_j and B are ground atoms, there exists a conjunction $I(\bar{c})$ of ground atoms containing only the constants \bar{c} occurring both in $\bigwedge_i A_i(\bar{a}, \bar{c})$ and $\bigwedge_j B_j(\bar{c}, \bar{b}) \wedge \neg B(\bar{c}, \bar{b})$, such that $\bigwedge_i A_i(\bar{a}, \bar{c}) \models_{\mathcal{T}} I(\bar{c})$ and $I(\bar{c}) \wedge \bigwedge_j B_j(\bar{c}, \bar{b}) \models_{\mathcal{T}} B(\bar{c}, \bar{b})$

Theorem A.3 ([5, 2, 18]). *Let \mathcal{T} be a universal theory. Then:*

- (1) \mathcal{T} has ground interpolation if and only if $\text{Mod}(\mathcal{T})$ has (AP) [2]. In addition, we can guarantee that if ϕ is positive then the interpolant of $\phi \wedge \psi$ is positive if and only if $\text{Mod}(\mathcal{T})$ has the injection transfer property [2].
- (2) If \mathcal{T} is an equational theory, then \mathcal{T} has the equational interpolation property if and only if $\text{Mod}(\mathcal{T})$ has the injection transfer property [18].

Theorem A.3 can be used to prove that many equational theories have ground interpolation:

Theorem A.4. *The following theories allow ground interpolation⁷:*

- (1) *The theory of pure equality (without function symbols).*

⁷In fact, the theories (1) and (4) allow equational interpolation. Similar results were also established for (2) in [11].

- (2) *Linear rational and real arithmetic.*
- (3) *The theory of posets.*
- (4) *The theories of (a) Boolean algebras, (b) semilattices, (c) distributive lattices.*

Proof. (1), (2), (3) are well-known (for (2) we refer for instance to [8] or [19]). For proving (4) we use the fact that if a universal theory has a positive algebraic completion then it has the injection transfer property [1]. All theories in (4) are equational theories; by results in [18], for equational theories the injection transfer property is equivalent to the equational interpolation property. With these remarks, (4)(a) follows from the fact that any Gaussian theory is its own positive algebraic completion [1], and (4)(b),(c) from the fact that the theory of semilattices and that of distributive lattices have a positive algebraic completion [1]. \square

Similarly it can be proved that the equational classes of (abelian) groups and lattices have ground interpolation.

APPENDIX B. PROOF OF THEOREM 4.6

Theorem 4.6 *We consider the following base theories \mathcal{T}_0 :*

- (1) \mathcal{P} (posets),
- (2) \mathcal{TO} (totally-ordered sets),
- (3) \mathcal{SLat} (semilattices),
- (4) \mathcal{DLat} (distributive lattices),
- (5) \mathcal{Bool} (Boolean algebras).
- (6) *the theory \mathbb{R} of reals resp. $\mathcal{LI}(\mathbb{R})$ (linear arithmetic over \mathbb{R}), or the theory \mathbb{Q} of rationals resp. $\mathcal{LI}(\mathbb{Q})$ (linear arithmetic over \mathbb{Q}), or (a subtheory of) the theory of integers (e.g. Presburger arithmetic).*

The following theory extensions are local:

- (a) *Extensions of any theory \mathcal{T}_0 for which \leq is reflexive with functions satisfying boundedness ($\text{Bound}^t(f)$) or guarded boundedness ($\text{GBound}^t(f)$) conditions*

$$(\text{Bound}^t(f)) \quad \forall x_1, \dots, x_n (f(x_1, \dots, x_n) \leq t(x_1, \dots, x_n))$$

$$(\text{GBound}^t(f)) \quad \forall x_1, \dots, x_n (\phi(x_1, \dots, x_n) \rightarrow f(x_1, \dots, x_n) \leq t(x_1, \dots, x_n)),$$
where $t(x_1, \dots, x_n)$ is a term in the base signature Π_0 and $\phi(x_1, \dots, x_n)$ a conjunction of literals in the signature Π_0 , whose variables are in $\{x_1, \dots, x_n\}$.
- (b) *Extensions of any theory \mathcal{T}_0 in (1)–(6) with $\text{Mon}(f) \wedge \text{Bound}^t(f)$, if $t(x_1, \dots, x_n)$ is a term in the base signature Π_0 in the variables x_1, \dots, x_n such that for every model of \mathcal{T}_0 the associated function is monotone in the variables x_1, \dots, x_n .*
- (c) *Extensions of any theory in (1)–(6) with functions satisfying $\text{Leq}(f, g) \wedge \text{Mon}(f)$.*

$$(\text{Leq}(f, g)) \quad \forall x_1, \dots, x_n (\bigwedge_{i=1}^n x_i \leq y_i \rightarrow f(x_1, \dots, x_n) \leq g(y_1, \dots, y_n))$$
- (d) *Extensions of any totally-ordered theory above (i.e. (2) and (6)) with functions satisfying $\text{SGc}(f, g_1, \dots, g_n) \wedge \text{Mon}(f, g_1, \dots, g_n)$.*

$$(\text{SGc}(f, g_1, \dots, g_n)) \quad \forall x_1, \dots, x_n, x (\bigwedge_{i=1}^n x_i \leq g_i(x) \rightarrow f(x_1, \dots, x_n) \leq x)$$
- (e) *Extensions of any theory in (1)–(3) with functions satisfying $\text{SGc}(f, g_1) \wedge \text{Mon}(f, g_1)$.*

All the extensions above satisfy condition (Loc^f).

Proof. In what follows we will denote by Π_0 the signature of the base theory \mathcal{T}_0 , and with Σ_1 the extension functions, namely f for cases (a) and (b), f, g for case (c), f, g_1, \dots, g_n for case (d) and f, g_1 for case (e).

(a) Let (P, f_P) be a partial Π -structure which weakly satisfies $\text{Bound}^t(f)$, such that $P \in \text{Mod}(\mathcal{T}_0)$ and $f_P : P^n \rightarrow P$ is partial. Let $A = (P, f_A)$ be a total Π -structure with the same support as P , where:

$$f_A(x_1, \dots, x_n) = \begin{cases} f_P(x_1, \dots, x_n) & \text{if } f_P(x_1, \dots, x_n) \text{ defined} \\ t(x_1, \dots, x_n) & \text{otherwise.} \end{cases}$$

Then A satisfies $\text{Bound}^t(f)$. Let $i : (P, f_P) \rightarrow (A, f_A)$ be the identity. Obviously, i is a Π_0 -isomorphism; and if $f_P(x_1, \dots, x_n)$ is defined then $i(f_P(x_1, \dots, x_n)) = f_P(x_1, \dots, x_n) = f_A(x_1, \dots, x_n)$. Similar arguments also apply to $\text{GBound}^t(f)$.

(b) Let (P, f_P) be a partial Π -structure which weakly satisfies $\text{Bound}^t(f) \wedge \text{Mon}$, such that $P \in \text{Mod}(\mathcal{T}_0)$ and $f_P : P^n \rightarrow P$ is partial. In cases (1)–(3) let $A = (\mathcal{OI}(P), \bar{f})$, where $\mathcal{OI}(P)$ is the family of all order ideals of P , and

$$f_A(U_1, \dots, U_n) = \downarrow \{f_P(u_1, \dots, u_n) \mid u_i \in U_i, f_P(u_1, \dots, u_n) \text{ defined}\}.$$

f_A is clearly monotone. Let $z \in f_A(U_1, \dots, U_n)$. Then $z \leq f_P(u_1, \dots, u_n)$ for some $u_i \in U_i$ with $f_P(u_1, \dots, u_n)$ defined. As $P \models_w \text{Bound}^t(f)$, $f_P(u_1, \dots, u_n) \leq t(u_1, \dots, u_n)$. Therefore $z \in t(U_1, \dots, U_n)$. The map $i : (P, f_P) \rightarrow (A, f_A)$ defined by $i(p) = \downarrow p$ is a weak embedding.

Since DLat and Bool are locally finite, results in [15] show that in (4) and (5) it is sufficient to assume that P is finite. Let $A = (P, f_A)$, where

$$f_A(x_1, \dots, x_n) = \bigvee \{f_P(u_1, \dots, u_n) \mid u_i \leq x_i, f_P(u_1, \dots, u_n) \text{ defined}\}.$$

f_A is clearly monotone. We prove that it also satisfies the boundedness condition, i.e. that for all x_1, \dots, x_n , $f_A(x_1, \dots, x_n) \leq t(x_1, \dots, x_n)$. By definition, $f_A(x_1, \dots, x_n) = \bigvee \{f_P(u_1, \dots, u_n) \mid u_i \leq x_i, f_P(u_1, \dots, u_n) \text{ defined}\}$. As $P \models_w \text{Bound}^t(f)$ and t is monotone, we know that $f_P(u_1, \dots, u_n) \leq t(u_1, \dots, u_n) \leq t(x_1, \dots, x_n)$ for all $u_i \leq x_i$ with $f_P(u_1, \dots, u_n)$ defined. Therefore,

$$f_A(x_1, \dots, x_n) = \bigvee \{f_P(u_1, \dots, u_n) \mid u_i \leq x_i, f_P(u_1, \dots, u_n) \text{ defined}\} \leq t(x_1, \dots, x_n).$$

That the identity i is a weak embedding can be proved as before.

(c) The proof is very similar to the proof of (b). We first discuss the case (1)–(3). Let (P, f_P, g_P) be a weak partial model of \mathcal{T}_1 . Let $A = (\mathcal{OI}(P), f_A, g_A)$, where f_A is defined as in (b). We define $g(U_1, \dots, U_n)$ by

$$g_A(U_1, \dots, U_n) = \begin{cases} \downarrow g_P(x_1, \dots, x_n) & \text{if } U_i = \downarrow x_i \text{ and } g_P(x_1, \dots, x_n) \text{ defined} \\ f_A(U_1, \dots, U_n) & \text{otherwise.} \end{cases}$$

Assume that $U_1 \subseteq V_1, \dots, U_n \subseteq V_n$, and let $z \in f_A(U_1, \dots, U_n)$. Then $z \leq f_P(u_1, \dots, u_n)$ for some $u_i \in U_i \subseteq V_i$ with $f_P(u_1, \dots, u_n)$ defined. If $V_i = \downarrow x_i$ and $g_P(x_1, \dots, x_n)$ defined, then $u_i \leq x_i$ so, as $P \models_w \text{Leq}(f, g)$, we know that $f_P(u_1, \dots, u_n) \leq g_P(x_1, \dots, x_n)$. It therefore follows that in this case $z \in \downarrow g_P(x_1, \dots, x_n) = g_A(V_1, \dots, V_n)$. Otherwise, $g_A(V_1, \dots, V_n) = f_A(V_1, \dots, V_n)$, hence $f_A(U_1, \dots, U_n) \subseteq g_A(V_1, \dots, V_n)$.

For the cases (4) and (5) we again use the criterion in [15] and Theorem 4.5. Let (P, f_P, g_P) be a weak partial model of \mathcal{T}_1 . Let $a_0 \in P$ be such that $a_0 \geq f_P(p_1, \dots, p_n)$ whenever $f_P(p_1, \dots, p_n)$ is defined. We define $A = (P, f_A, g_A)$ as follows:

$$g_A(x_1, \dots, x_n) = \begin{cases} \downarrow g_P(x_1, \dots, x_n) & \text{if } g_P(x_1, \dots, x_n) \text{ defined} \\ a_0 & \text{otherwise} \end{cases}$$

$$f_A(x_1, \dots, x_n) = \bigvee \{f_P(u_1, \dots, u_n) \mid u_i \leq x_i, f_P(u_1, \dots, u_n) \text{ defined}\}.$$

f is obviously monotone. In order to prove that the second condition holds, we analyze two cases. Assume first that $g_P(y_1, \dots, y_n)$ is undefined. Then $g_A(y_1, \dots, y_n) = a_0 \geq f_P(u_1, \dots, u_n)$ for all $u_i \leq x_i$ with $f_P(u_1, \dots, u_n)$ defined, thus, $g_A(y_1, \dots, y_n) = a_0 \geq \bigvee \{f_P(u_1, \dots, u_n) \mid u_i \leq x_i, f_P(u_1, \dots, u_n) \text{ defined}\} = f_A(x_1, \dots, x_n)$. If $g_P(y_1, \dots, y_n)$ is defined, then for all $u_i \leq x_i$ with $f_P(u_1, \dots, u_n)$ we also have $u_i \leq y_i$, so $f_P(u_1, \dots, u_n) \leq g_P(y_1, \dots, y_n) = g_A(y_1, \dots, y_n)$. Again, it follows that $g_A(y_1, \dots, y_n) \leq f_A(x_1, \dots, x_n)$.

(d) Let \mathcal{T}_0 be the theory of totally ordered sets. Assume that $(P, f_P, (g_P^i))$ is a totally ordered weak partial model of $\text{SGc}(f, g_1, \dots, g_n) \wedge \text{Mon}(f, g_1, \dots, g_n)$. Let $A = (\mathcal{OI}(X), f_A, (g_A^i))$, where f_A and g_A^i are extensions of f_P, g_P^i defined as in the proof of (b). f_A, g_A^1, \dots, g_A^n are obviously monotone. We prove that the condition $\text{SGc}(f, g_1, \dots, g_n)$ holds in A . Assume that $U_i \subseteq g_A^i(V)$ for $i = 1, \dots, n$, and let $x \in f_A(U_1, \dots, U_n)$. Then there exist $u_i \in U_i = g_A^i(V_i)$ such that $f(u_1, \dots, u_n)$ is defined and $x \leq f(u_1, \dots, u_n)$. As $u_i \in g_A^i(V)$, there exist $v_i \in V$ such that $g_P^i(v_i)$ is defined and $u_i \leq g_P^i(v_i)$. Let $v = \max(v_1, \dots, v_n)$. Then $u_i \leq g_P^i(v)$. Hence $f_P(u_1, \dots, u_n) \leq v \in V$. Therefore, $x \leq f_P(u_1, \dots, u_n) \in V$ so $x \in V$. Let $i : P \rightarrow A$ defined by $i(p) = \downarrow p$. To show that it is a weak embedding we only have to show that if $g_P(x_1, \dots, x_n)$ is defined then $i(g_P(x_1, \dots, x_n)) = \downarrow g_P(x_1, \dots, x_n) = g_A(\downarrow x_1, \dots, \downarrow x_n)$. This is true by the definition of g_A .

(e) Assume that \mathcal{T}_0 is the theory of semilattices. The construction in (d) can be applied to this case without problems. The proof is similar to that of (d) with the difference that if $n = 1$ we only have one element v_1 so we do not need to compute a maximum (which for $n \geq 2$ may not exist if the order is not total).

The proof of the fact that the remaining theories satisfy (Loc^f) is based on the criterion of finite locality given in Theorem 4.5. The constructions and the proofs are similar to those in the proof of (b) resp. (c) for the cases (4) and (5). Due to the fact that we assumed that the definition domain of the extension functions is finite $\bigvee \{f_P(u_1, \dots, u_n) \mid u_i \leq x_i, f_P(u_1, \dots, u_n) \text{ defined}\}$ is a finite join, and thus exists (if f is nowhere defined it is sufficient to define it as being everywhere equal to t in case (b) or to g_A in case (c)). The fact that the definition domains are finite also ensures that in the proof of (c) an element a_0 (chosen in the definition of g_A) with the desired properties always exists. \square

APPENDIX C. PROOF OF THEOREM 5.4

Theorem 5.4. *The following theories have ground interpolation and are convex and P -interpolating with respect to the indicated set P of predicate symbols:*

- (1) *The theory of \mathcal{EQ} of pure equality without function symbols (for $P = \{\approx\}$).*
- (2) *The theory PoSet of posets (for $P = \{\approx, \leq\}$).*

- (3) *Linear rational arithmetic* $\text{LI}(\mathbb{Q})$ and *linear real arithmetic* $\text{LI}(\mathbb{R})$ (convex with respect to $P = \{\approx\}$, strongly P -interpolating for $P = \{\leq\}$).
- (4) *The theories* **Bool** of Boolean algebras, **SLat** of semilattices and **DLat** of distributive lattices (strongly P -interpolating for $P = \{\approx, \leq\}$).

Proof. Note first that if a partially-ordered theory is interpolating for \leq it is also for \approx . Assume that $A \wedge B \models_{\mathcal{T}} a \approx b$. Then $A \wedge B \models_{\mathcal{T}} a \leq b$ and $A \wedge B \models_{\mathcal{T}} b \leq a$, hence there exist terms t_1, t_2 containing only common constants of A and B such that $A \wedge B \models a \leq t_1 \wedge t_1 \leq b$ and $A \wedge B \models b \leq t_2 \wedge t_2 \leq a$. It follows that $A \wedge B \models t_1 \approx t_2$, $A \wedge B \models a \approx t_1 \wedge t_1 \approx b$.

(1) and (2): convexity is obvious; the property of being P -interpolating can be proved by induction on the structure of proofs. (3) is known (cf. e.g. [19]). A method for computing interpolating terms for $\text{LI}(\mathbb{R})$ and $\text{LI}(\mathbb{Q})$ is presented in [11].

(4) This is a constructive proof based on ideas from [12, 13]. The results presented there show, as an easy particular case, that one can reduce the problem of checking the satisfiability of a conjunction Γ of unit clauses with respect to one of the theories above to checking the satisfiability of a conjunction $\text{Ren}_{\Gamma} \wedge P_{\Gamma} \wedge N_{\Gamma}$ obtained by introducing a propositional variable P_e for each subterm e occurring in Γ , a set of renaming rules of the form

$$\begin{array}{ll} P_{e_1 \text{ op } e_2} \leftrightarrow P_{e_1} \text{ op } P_{e_2} & \text{op binary Boolean operation} \\ P_{\neg e} \leftrightarrow \neg P_e & \text{in the case of Bool,} \end{array}$$

and translations of the positive resp. negative part of Γ :

$$\begin{array}{ll} P_s \leftrightarrow P_{s'} & s \approx s' \in \Gamma \\ \neg(P_s \leftrightarrow P_{s'}) & s \not\approx s' \in \Gamma. \end{array}$$

(a) The convexity of the theory of Boolean algebras with respect to \approx follows from the fact that this is an equational class; convexity with respect to \leq follows from the fact that $x \leq y$ if and only if $x \wedge y \approx x$. We prove that the theory of Boolean algebras is \leq -interpolating, i.e. that if A and B are two conjunctions of literals and $A \wedge B \models_{\text{Bool}} a \leq b$, where a is a constant occurring in A and not in B and b a constant occurring in B and not in A , then there exists a term containing only common constants in A and B such that $A \models_{\text{Bool}} a \leq t$ and $B \models_{\text{Bool}} t \leq b$. We can assume without loss of generality that A and B consist only of atoms (otherwise one moves the negative literals to the right and uses convexity). $A \wedge B \models_{\text{Bool}} a \leq b$ if and only if the following conjunction of literals in propositional logic is unsatisfiable:

$$\begin{array}{llll} (\text{Ren}(\wedge)) & P_{e_1 \wedge e_2} & \leftrightarrow & P_{e_1} \wedge P_{e_2} & P_{g_1 \wedge g_2} & \leftrightarrow & P_{g_1} \wedge P_{g_2} \\ (\text{Ren}(\vee)) & P_{e_1 \vee e_2} & \leftrightarrow & P_{e_1} \vee P_{e_2} & P_{g_1 \vee g_2} & \leftrightarrow & P_{g_1} \vee P_{g_2} \\ (\text{Ren}(\neg)) & P_{\neg e} & \leftrightarrow & \neg P_e & P_{\neg g} & \leftrightarrow & \neg P_g \\ (\text{P}) & P_{e_1} & \leftrightarrow & P_{e_2} & P_{g_1} & \leftrightarrow & P_{g_2} & g_1 \approx g_2 \in B \\ (\text{N}) & & & P_a & & & \neg P_b \end{array}$$

for all e, e_1, e_2 subterms in A for all g, g_1, g_2 subterms in B

We obtain an unsatisfiable set of clauses $(N_A \wedge P_a) \wedge (N_B \wedge \neg P_b) \models \perp$. Propositional logic allows interpolation, so there exists an interpolant $I = f(P_{e_1}, \dots, P_{e_n})$, which is a Boolean

combination (say in CNF) of the common propositional variables occurring in N_A and N_B such that

$$(N_A \wedge P_a) \models I \quad \text{and} \quad (N_B \wedge \neg P_b) \wedge I \models \perp .$$

But then $A \models_{\text{Bool}} a \leq f(e_1, \dots, e_n)$ and $B \models_{\text{Bool}} f(e_1, \dots, e_n) \leq b$.

(4)(b) The proof is similar to that of (4)(a) with the difference that in the renaming rules in the structure-preserving translation to clause form only the conjunction rules apply, hence N_A and N_B are sets of non-negative Horn clauses. We can saturate $N_A \cup P_a$ under resolution with selection on the negative literals in linear time. The saturated set N_A^* of clauses contains all unit clauses P_e where e is subterm of A with $A \models_{\text{SLat}} a \leq e$. Only unit positive clauses P_e where e occurs in both A and B can enter into resolution inferences with clauses in $N_B \cup \neg P_b$ and lead to a contradiction. Thus we proved that

$$\bigwedge \{P_e \mid A \models_{\text{SLat}} a \leq e, e \text{ common subterm}\} \wedge N_B \wedge \neg P_b \models \perp .$$

This is equivalent to $B \models_{\text{SLat}} t \leq b$, where

$$t = \bigwedge \{e \mid A \models_{\text{SLat}} a \leq e, e \text{ common subterm of } A \text{ and } B\} .$$

Obviously, $A \models_{\text{SLat}} a \leq t$.

(4)(c) The case of distributive lattices can be treated similarly. Due to the fact that in this case the renaming rules for \vee and \wedge are taken into account, the sets N_A and N_B are not Horn. We adopt the same negative selection strategy. When saturating $N_A \cup P_a$ a finite set of positive clauses is generated, namely of the form $P_{e_1} \vee \dots \vee P_{e_n}$ where $A \models_{\text{DL}} a \leq (e_1 \vee \dots \vee e_n)$. We consider a total ordering on the propositional variables where P_e is larger than P_g if e occurs in A and not in B and g occurs in both A and in B . Then the only inferences which can lead to a contradiction with $N_B \cup \neg P_b$ are those between the clauses in N_A^* which only contain common propositional variables. Thus we proved that

$$\bigwedge \{\bigvee P_{e_i} \mid A \models_{\text{DL}} a \leq \bigvee e_i, e_i \text{ common terms}\} \wedge N_B \wedge \neg P_b \models \perp .$$

This is equivalent to $B \models_{\text{DL}} t \leq b$, where $t = \bigwedge \{\bigvee e_i \mid A \models_{\text{DL}} a \leq \bigvee e_i, \text{ where all } e_i \text{ are common subterms of } A \text{ and } B\}$. Obviously, $A \models_{\text{DL}} a \leq t$. \square