A Sorted Datalog Hammer for Supervisor Verification Conditions Modulo Simple Linear Arithmetic

Martin Bromberger[1], Irina Dragoste[2], Rasha Faqeh[2], Christof Fetzer[2], Larry González[2], Markus Krötzsch[2], Maximilian Marx[2], Harish K Murali[1,3], and Christoph Weidenbach[1]

[1] Max Planck Institute for Informatics, Saarland Informatics Campus, Saarbrücken
[2] TU Dresden, Dresden, Germany
[3] IIITDM Kancheepuram, Chennai, India

Abstract. In a previous paper, we have shown that clause sets belonging to the Horn Bernays-Schönfinkel fragment over simple linear real arithmetic (HBS(SLR)) can be translated into HBS clause sets over a finite set of first-order constants. The translation preserves validity and satisfiability and it is still applicable if we extend our input with positive universally or existentially quantified verification conditions (conjectures). We call this translation a Datalog hammer. The combination of its implementation in SPASS-SPL with the Datalog reasoner VLog establishes an effective way of deciding verification conditions in the Horn fragment. We verify supervisor code for two examples: a lane change assistant in a car and an electronic control unit of a supercharged combustion engine. In this paper, we improve our Datalog hammer in several ways: we generalize it to mixed real-integer arithmetic and finite first-order sorts; we extend the class of acceptable inequalities beyond variable bounds and positively grounded inequalities; and we significantly reduce the size of the hammer output by a soft typing discipline. We call the result the sorted Datalog hammer. It not only allows us to handle more complex supervisor code and to model already considered supervisor code more concisely, but it also improves our performance on real world benchmark examples. Finally, we replace the before file-based interface between SPASS-SPL and VLog by a close coupling resulting in a single executable binary. Data Availability Statement: An artifact will be submitted to the AEC under EasyChair id 206.

1 Introduction

Modern dynamic dependable systems (e.g., autonomous driving) continuously update software components to fix bugs and to introduce new features. However, the safety requirement of such systems demands software to be safety certified before it can be used, which is typically a lengthy process that hinders the dynamic update of software. We adapt the *continuous certification* approach [14] for variants of safety critical software components using a *supervisor* that guarantees important aspects through *challenging*, see Fig. 1. Specifically, multiple processing units run in parallel – *certified* and *updated not-certified* variants that produce output as *suggestions* and *explications*. The supervisor compares the behavior of variants and analyses their explications. The supervisor itself consists of a rather small set of rules that can be automatically verified and run by a reasoner such as SPASS-SPL. In this paper we concentrate on the further development of our verification approach through the sorted Datalog hammer.

While supervisor safety conditions formalized as existentially quantified properties can often already be automatically verified, conjectures about invariants requiring universally

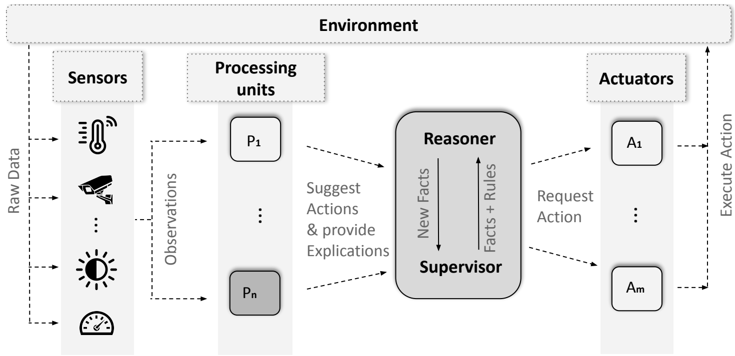

Fig. 1. The supervisor architecture.

quantified properties are a further challenge. Analogous to the Sledgehammer project [7] of Isabelle [28] that translates higher-order logic conjectures to first-order logic (modulo theories) conjectures, our sorted Datalog hammer translates first-order Horn logic modulo arithmetic conjectures into pure Datalog programs, which is equivalent to the Horn Bernays-Schönfinkel clause fragment, called HBS.

More concretely, the underlying logic for both formalizing supervisor behavior and formulating conjectures is the hierarchic combination of the Horn Bernays-Schönfinkel fragment with linear arithmetic, HBS(LA), also called *Superlog* for Supervisor Effective Reasoning Logics [14]. Satisfiability of BS(LA) clause sets is undecidable [12,20], in general, however, the restriction to simple linear arithmetic BS(SLA) yields a decidable fragment [16,19].

Inspired by the test point method for quantifier elimination in arithmetic [24] we show that instantiation with a finite number of values is sufficient to decide whether a universal or existential conjecture is a consequence of a BS(SLA) clause set.

In this paper, we improve our Datalog hammer [8] for HBS(SLA) in three directions. First, we modify our Datalog hammer so it also accepts other sorts for variables besides reals: the integers and arbitrarily many finite first-order sorts $\mathcal{F}_i$. Each non-arithmetic sort has a predefined finite domain corresponding to a set of constants $\mathbb{F}_i$ for $\mathcal{F}_i$ in our signature. Second, we modify our Datalog hammer so it also accepts more general inequalities than simple linear arithmetic allows (but only under certain conditions). In [8], we have already started in this direction by extending the input logic from pure HBS(SLA) to pure positively grounded HBS(SLA). Here we establish a soft typing discipline by efficiently approximating potential values occurring at predicate argument positions of all derivable facts. Third, we modify the test-point scheme that is the basis of our Datalog hammer so it can exploit the fact that not all all inequalities are connected to all predicate argument positions.

Our modifications have three major advantages: first of all, they allow us to express supervisor code for our previous use cases more elegantly and without any additional preprocessing. Second of all, they allow us to formalize supervisor code that would have been out of scope of the logic before. Finally, they reduce the number of required test points, which leads to smaller transformed formulas that can be solved in much less time.

For our experiments of the test point approach we consider again two case studies. First, verification conditions for a supervisor taking care of multiple software variants of a lane change assistant. Second, verification conditions for a supervisor of a supercharged combustion engine, also called an ECU for Electronical Control Unit. The supervisors in both cases are formulated by BS(SLA) Horn clauses.Via our test point technique they are translated together with the verification conditions to Datalog [2] (HBS). The translation is implemented in our Superlog reasoner SPASS-SPL. The resulting Datalog clause set is eventually explored by the Datalog engine VLog [10]. This hammer constitutes a decision procedure for both universal and existential conjectures. The results of our experiments show that we can verify non-trivial existential and universal conjectures in the range of seconds while state-of-the-art solvers cannot solve all problems in reasonable time, see Section 4.

Related Work: Reasoning about BS(LA) clause sets is supported by SMT (Satisfiability Modulo Theories) [27,26]. In general, SMT comprises the combination of a number of theories beyond LA such as arrays, lists, strings, or bit vectors. While SMT is a decision procedure for the BS(LA) ground case, universally quantified variables can be considered by instantiation [32]. Reasoning by instantiation does result in a refutationally complete procedure for BS(SLA), but not in a decision procedure. The Horn fragment HBS(LA) out of BS(LA) is receiving additional attention [17,6], because it is well-suited for software analysis and verification. Research in this direction also goes beyond the theory of LA and considers minimal model semantics in addition, but is restricted to existential conjectures. Other research focuses on universal conjectures, but over non-arithmetic theories, e.g., invariant checking for array-based systems [11] or considers abstract decidability criteria incomparable with the HBS(LA) class [31]. Hierarchic superposition [3] and Simple Clause Learning over Theories (SCL(T)) [9] are both refutationally complete for BS(LA). While SCL(T) can be immediately turned into a decision procedure for even larger fragments than BS(SLA) [9], hierarchic superposition needs to be refined to become a decision procedure already because of the Bernays-Schönfinkel part [18]. Our Datalog hammer translates HBS(SLA) clause sets with both existential and universal conjectures into HBS clause sets which are also subject to first-order theorem proving. Instance generating approaches such as iProver [22] are a decision procedure for this fragment, whereas superposition-based [3] first-order provers such as E [34], SPASS [36], Vampire [33], have additional mechanisms implemented to decide HBS. In our experiments, Section 4, we will discuss the differences between all these approaches on a number of benchmark examples in more detail.

The paper is organized as follows: after a section on preliminaries, Section 2, we present the theory of our sorted Datalog hammer in Section 3, followed by experiments on real world supervisor verification conditions, Section 4. The paper ends with a discussion of the obtained results and directions for future work, Section 5. Binaries of our tools and all benchmark problems can be found under [1]. Proofs of our lemmas and theorems can be found in the appendix and will eventually be published in an extended version.

2 Preliminaries

We briefly recall the basic logical formalisms and notations we build upon [8]. Starting point is standard many-sorted first-order language for BS with *constants* (denoted a,b,c), without non-constant function symbols, *variables* (denoted w,x,y,z), and *predicates* (denoted P,Q,R) of some fixed *arity*. *Terms* (denoted t,s) are variables or constants. We write $\bar{x}$ for a vector of variables, $\bar{a}$ for a vector of constants, and so on. An *atom* (denoted A,B) is an expression $P(\bar{t})$ for a predicate P of arity n and a term list $\bar{t}$ of length n. A *positive literal* is an atom A and a *negative literal* is a negated atom $\neg A$. We define $\text{comp}(A) = \neg A$, $\text{comp}(\neg A) = A$, $|A| = A$ and $|\neg A| = A$. Literals are usually denoted L,K,H.

A *clause* is a disjunction of literals, where all variables are assumed to be universally quantified. C,D denote clauses, and N denotes a clause set. We write atoms(X) for the set of atoms in a clause or clause set X. A clause is *Horn* if it contains at most one positive literal, and a *unit clause* if it has exactly one literal. A clause $A_1 \lor \ldots \lor A_n \lor \neg B_1 \lor \ldots \lor \neg B_m$ can be written as an implication $B_1 \land \ldots \land B_m \rightarrow A_1 \lor \ldots \lor A_n$, still omitting universal quantifiers. If Y is a term, formula, or a set thereof, vars(Y) denotes the set of all variables in Y, and Y is *ground* if $\text{vars}(Y) = \emptyset$. A *fact* is a ground unit clause with a positive literal.

Datalog and the Horn Bernays-Schönfinkel Fragment: The *Horn case of the Bernays-Schönfinkel fragment* (HBS) comprises all sets of clauses with at most one positive literal. The more general Bernays-Schönfinkel fragment (BS) in first-order logic allows arbitrary *formulas* over atoms, i.e., arbitrary Boolean connectives and leading existential quantifiers. BS formulas can be polynomially transformed into clause sets with common syntactic transformations while preserving satisfiability and all entailments that do not refer to auxiliary constants and predicates introduced in the transformation [29]. BS theories in our sense are also known as *disjunctive Datalog programs* [13], specifically when written as implications. A HBS clause set is also called a *Datalog program*. (Datalog is sometimes viewed as a second-order language. We are only interested in query answering, which can equivalently be viewed as first-order entailment or second-order model checking [2].) Again, it is common to write clauses as implications in this case.

Two types of *conjectures*, i.e., formulas we want to prove as consequences of a clause set, are of particular interest: *universal* conjectures $\forall \bar{x}.\phi$ and *existential* conjectures $\exists \bar{x}.\phi$, where ϕ is a BS formula that only uses variables in $\bar{x}$. We call such a conjecture positive if the formula only uses conjunctions and disjunctions to connect atoms. Positive conjectures are the focus of our Datalog hammer and they have the useful property that they can be transformed to one atom over a fresh predicate symbol by adding some suitable Horn clause definitions to our clause set N [29,8]. This is also the reason why we assume for the rest of the paper that all relevant universal conjectures have the form $\forall \bar{x}.P(\bar{x})$ and existential conjectures the form $\exists \bar{x}.P(\bar{x})$.

A *substitution* σ is a function from variables to terms with a finite domain $\text{dom}(\sigma) = \{x \mid x\sigma \neq x\}$ and codomain $\text{codom}(\sigma) = \{x\sigma \mid x \in \text{dom}(\sigma)\}$. We denote substitutions by σ,δ,ρ. The application of substitutions is often written postfix, as in $x\sigma$, and is homomorphically extended to terms, atoms, literals, clauses, and quantifier-free formulas. A substitution σ is *ground* if codom(σ) is ground. Let Y denote some term, literal, clause, or clause set. σ is a *grounding* for Y if $Y\sigma$ is ground, and $Y\sigma$ is a *ground instance* of Y in this case. We denote by gnd(Y) the set of all ground instances of Y, and by $\text{gnd}_B(Y)$ the set of all ground instances over a given set of constants B. The *most general unifier* $\text{mgu}(Z_1,Z_2)$ of two terms/atoms/literals Z_1 and Z_2 is defined as usual, and we assume that it does not introduce fresh variables and is idempotent.

We assume a standard many-sorted first-order logic model theory, and write $\mathcal{A} \models \phi$ if an interpretation $\mathcal{A}$ satisfies a first-order formula ϕ. A formula ψ is a logical consequence of ϕ, written $\phi \models \psi$, if $\mathcal{A} \models \psi$ for all $\mathcal{A}$ such that $\mathcal{A} \models \phi$. Sets of clauses are semantically treated as conjunctions of clauses with all variables quantified universally.

BS **with Linear Arithmetic:** The extension of BS with linear arithmetic both over real and integer variables, BS(LA), is the basis for the formalisms studied in this paper. We extend the standard *many-sorted* first-order logic with finitely many first-order sorts $\mathcal{F}_i$ and with two arithmetic sorts $\mathcal{R}$ for the real numbers and $\mathcal{Z}$ for the integer numbers. The sort $\mathcal{Z}$ is a *subsort* of $\mathcal{R}$.Given a clause set N, the interpretations $\mathcal{A}$ of our sorts S are fixed: $\mathcal{R}^{\mathcal{A}} = \mathbb{R}$, $\mathcal{Z}^{\mathcal{A}} = \mathbb{Z}$, and $\mathcal{F}_i^{\mathcal{A}} = \mathbb{F}_i$, i.e., a first-order sort interpretation $\mathbb{F}_i$ consists of the set of constants in N belonging to that sort, or a single constant out of the signature if no such constant occurs. Note that this is not a deviation from standard semantics in our context as for the arithmetic part the canonical domain is considered and for the first-order sorts BS has the finite model property over the occurring constants which is sufficent for refutation-based reasoning. This way first-order constants are distinct values.

Constant symbols, aithmetic function symbols, variables, and predicates are uniquely declared together with *sort* expressions. The unique sort of a constant symbol, variable, predicate, or term is denoted by the function sort(Y) and we assume all terms, atoms, and formulas to be well-sorted. The sort of predicate P's argument position i is denoted by sort(P,i). For arithmetic function symbols we consider the minimal sort with respect to the subsort relation between $\mathcal{R}$ and $\mathcal{Z}$. Eventually we don't consider arithmetic functions here, so eventually it boils down to substitute an integer sort variable or number for a real sort variable.

We assume *pure* clause sets, which means the only constants of sort $\mathcal{R}$ or $\mathcal{Z}$ are numbers. This means the only constants that we do allow are integer numbers $c \in \mathbb{Z}$ and the constants defining our finite first-order sorts $\mathcal{F}_i$. Satisfiability of pure BS(LA) clause sets is semi-decidable, e.g., using *hierarchic superposition* [3] or *SCL(T)* [9]. Impure BS(LA) is no longer compact and satisfiability becomes undecidable, but it can be made decidable when restricting to ground clause sets [15].

All arithmetic predicates and functions are interpreted in the usual way. An interpretation of BS(LA) coincides with $\mathcal{A}^{\text{LA}}$ on arithmetic predicates and functions, and freely interprets free predicates. For pure clause sets this is well-defined [3]. Logical satisfaction and entailment is defined as usual, and uses similar notation as for BS.

Example 1. The following BS(LA) clause from our ECU case study compares the values of speed (Rpm) and pressure (KPa) with entries in an ignition table (IgnTable) to derive the basis of the current ignition value (IgnDeg1):

$$\begin{aligned}&x_1 < 0 \lor x_1 \geq 13 \lor x_2 < 880 \lor x_2 \geq 1100 \lor \neg\text{KPa}(x_3,x_1) \lor \\ &\neg\text{Rpm}(x_4,x_2) \lor \neg\text{IgnTable}(0,13,880,1100,z) \lor \text{IgnDeg1}(x_3,x_4,x_1,x_2,z)\end{aligned} \tag{1}$$

Terms of the two arithmetic sorts are constructed from a set $\mathcal{X}$ of *variables*, the set of integer constants $c \in \mathbb{Z}$, and binary function symbols $+$ and $-$ (written infix). Atoms in BS(LA) are either *first-order atoms* (e.g., IgnTable(0,13,880,1100,z)) or *(linear) arithmetic atoms* (e.g., $x_2 < 880$). Arithmetic atoms may use the predicates $\leq,<,\neq,=,>,\geq$, which are written infix and have the expected fixed interpretation. Predicates used in first-order atoms are called *free*. *First-order literals* and related notation is defined as before. *Arithmetic literals* coincide with arithmetic atoms, since the arithmetic predicates are closed under negation, e.g., $\neg(x_2 \geq 1100) = x_2 < 1100$.

BS(LA) clauses and conjectures are defined as for BS but using BS(LA) atoms. We often write horn clauses in the form $\Lambda \parallel \Delta \rightarrow H$ where Δ is a multiset of free first-order atoms, H is either a first-order atom or $\bot$, and Λ is a multiset of LA atoms. The semantics of a clause in the form $\Lambda \parallel \Delta \rightarrow H$ is $\bigvee_{\lambda\in\Lambda} \neg\lambda \lor \bigvee_{A\in\Delta} \neg A \lor H$, e.g., the clause $x > 1 \lor y \neq 5 \lor \neg Q(x) \lor R(x,y)$ is also written $x \leq 1, y = 5 || Q(x) \rightarrow R(x,y)$.

A clause or clause set is *abstracted* if its first-order literals contain only variables or first-order constants. Every clause C is equivalent to an abstracted clause that is obtained by replacing each non-variable arithmetic term t that occurs in a first-order atom by a fresh variable x while adding an arithmetic atom $x \neq t$ to C. We asssume abstracted clauses for theory development, but we prefer non-abstracted clauses in examples for readability,e.g., a fact $P(3,5)$ is considered in the development of the theory as the clause $x=3, x=5 \,\|\, \rightarrow P(x,y)$, this is important when collecting the necessary test points. Moreover, we assume that all variables in the theory part of a clause also appear in the first order part, i.e., $\text{vars}(\Lambda) \subseteq \text{vars}(\Delta \rightarrow H)$ for every clause $\Lambda \,\|\, \Delta \rightarrow H$. If this is not the case for x in $\Lambda \,\|\, \Delta \rightarrow H$, then we can easily fix this by first introducing a fresh unary predicate Q over the sort(x), then adding the literal $Q(x)$ to Δ, and finally adding a clause $\|\rightarrow Q(x)$ to our clause set. Alternatively, x could be eliminated by LA variable elimintation in our context, however this results in a worst case exponential blow up in size. This restriction is necessary because we base all our computations for the test-point scheme on predicate argument positions and would not get any test points for variables that are not connected to any predicate argument positions.

Simpler Forms of Linear Arithmetic: The main logic studied in this paper is obtained by restricting HBS(LA) to a simpler form of linear arithmetic. We first introduce a simpler logic HBS(SLA) as a well-known fragment of HBS(LA) for which satisfiability is decidable [16,19], and later present the generalization HBS(LA)PA of this formalism that we will use.

Definition 2. *The* Horn Bernays-Schönfinkel fragment over simple linear arithmetic, HBS(SLA)*, is a subset of* HBS(LA) *where all arithmetic atoms are of the form $x \triangleleft c$ or $d \triangleleft c$, such that $c \in \mathbb{Z}$, d is a (possibly free) constant, $x \in \mathcal{X}$, and $\triangleleft \in \{\leq, <, \neq, =, >, \geq\}$.*

Example 3. The ECU use case leads to HBS(LA) clauses such as

$$\begin{aligned} &x_1 < y_1 \lor x_1 \geq y_2 \lor x_2 < y_3 \lor x_2 \geq y_4 \lor \neg\text{KPa}(x_3,x_1) \lor \\ &\neg\text{Rpm}(x_4,x_2) \lor \neg\text{IgnTable}(y_1,y_2,y_3,y_4,z) \lor \text{IgnDeg1}(x_3,x_4,x_1,x_2,z). \end{aligned} \tag{2}$$

This clause is not in HBS(SLA), e.g., since $x_1 > x_5$ is not allowed in BS(SLA). However, clause (1) of Example 1 is a BS(SLA) clause that is an instance of (2), obtained by the substitution $\{y_1 \mapsto 0, y_2 \mapsto 13, y_3 \mapsto 880, y_4 \mapsto 1100\}$. This grounding will eventually be obtained by resolution on the IgnTable predicate, because it occurs only positively in ground unit facts.

Example 3 shows that HBS(SLA) clauses can sometimes be obtained by instantiation. In fact, for the satisfiability of an HBS(LA) clause set N only those instances of clauses $(\Lambda \,\|\, \Delta \rightarrow H)\sigma$ are *relevant*, for which we can actually derive all ground facts $A \in \Delta\sigma$ by resolution from N. If A cannot be derived from N and N is satisfiable, then there always exists a satisfying interpretation $\mathcal{A}$ that interprets A as false (and thus $(\Lambda \,\|\, \Delta \rightarrow H)\sigma$ as true). Moreover, if those relevant instances can be simplified to HBS(SLA) clauses, then it is possible to extend almost all HBS(SLA) techniques (including our Datalog hammer) to those HBS(LA) clause sets.

In our case resolution means *hierarchic unit resolution*: given clause $\Lambda_1 \,\|\, L, \Delta \rightarrow H$ and unit clause $\Lambda_2 \,\|\rightarrow K$ with $\sigma = \text{mgu}(L,K)$, their *hierarchic resolvent* is $(\Lambda_1, \Lambda_2 \,\|\, \Delta \rightarrow H)\sigma$. A fact $P(\bar{a})$ is *derivable* from a pure set of HBS(LA) clauses N if there exists a clause $\Lambda \,\|\rightarrow P(\bar{t})$ that (i) is the result of a sequence of unit resolution steps from the clauses in N and (ii) has a grounding σ such that $P(\bar{t})\sigma = P(\bar{a})$ and $\Lambda\sigma$ evaluates to true. If N is satisfiable, then this means that any fact $P(\bar{a})$ derivable from N is true in all satisfiable interpretations of N, i.e., $N \models P(\bar{a})$. We denote the *set of derivable facts* for a predicate P from N by dfacts(P,N). A *refutation* is the sequence of resolution steps that produces a clause $\Lambda \,\|\rightarrow \bot$ with $\mathcal{A}^{\text{LA}} \models \Lambda\delta$

for some grounding δ. *Hierarchic unit resolution* is sound and refutationally complete for pure HBS(LA), since every set N of pure HBS(LA) clauses N is *sufficiently complete* [3], and hence *hierarchic superposition* is sound and refutationally complete for N [3,5].

So naturally if all derivable facts of a predicate P already appear in N, then only those instances of clauses can be relevant whose occurrences of P match those facts (i.e., can be resolved with them). We call predicates with this property positively grounded:

Definition 4 (Positively Grounded Predicate [8]). *Let N be a set of* HBS(LA) *clauses. A free first-order predicate P is a* positively grounded predicate *in N if all positive occurrences of P in N are in ground unit clauses (also called facts).*

Definition 5 (Positively Grounded HBS(SLA)**:** HBS(SLA)P **[8]).** *An* HBS(LA) *clause set N is out of the fragment* positively grounded HBS(SLA) (HBS(SLA)P) *if we can transform N into an* HBS(SLA) *clause set N' by first resolving away all negative occurrences of positively grounded predicates P in N, simplifying the thus instantiated* LA *atoms, and finally eliminating all clauses where those predicates occur negatively.*

As mentioned before, if all relevant instances of an HBS(LA) clause set can be simplified to HBS(SLA) clauses, then it is possible to extend almost all HBS(SLA) techniques (including our Datalog hammer) to those clause sets. HBS(SLA)P clause sets have this property and this is the reason, why we managed to extend our Datalog hammer to pure HBS(SLA)P clause sets in [8]. For instance, the set $N = \{P(1), P(2), Q(0), (x \leq y+z \,\|\, P(y), Q(z) \rightarrow R(x,y))\}$ is an HBS(LA) clause set, but not an HBS(SLA) clause set due to the inequality $x \leq y+z$. Note, however, that the predicates P and Q are positively grounded (the only positive occurrences of P and Q are the facts $P(1)$, $P(2)$, and $Q(0)$). If we resolve with the facts for P and Q and simplify, then we get the clause set $N' = \{P(1), P(2), Q(0), (x \leq 1 \,\|\rightarrow R(x,1)), (x \leq 2 \,\|\rightarrow R(x,2))\}$, which does now belong to HBS(SLA). This means N is a positively grounded HBS(SLA) clause set and our Datalog hammer can still handle it.

Positively grounded predicates are only one way to filter out irrelevant clause instances. As part of our improvements, we define in Section 3 a new logic called approximately grounded HBS(SLA) (HBS(SLA)PA) that is an extension of HBS(SLA)P and serves as the new input logic of our sorted Datalog hammer. It is based on over-approximating the set of *derivable values* $\text{dvals}(P,i,N) = \{a_i \mid P(\bar{a}) \in \text{dfacts}(P,N)\}$ for each argument position i of each predicate P in N with only finitely many derivable values (i.e., $|\text{dvals}(P,i,N)| \in \mathbb{N}$). These argument positions are also called *finite*. With regard to clause relevance, only those clause instances are relevant, where a finite argument position is instantiated by one of the derivable values. We call a set of clauses N an approximately grounded HBS(SLA) clause set if all relevant instances based on this criterion can be simplified to HBS(SLA) clauses. For instance, the set $N = \{(x \leq 1 \,\|\rightarrow P(x,1)), (x > 2 \,\|\rightarrow P(x,3)), (x \geq 0 \,\|\rightarrow Q(x,0)), (u \leq y+z \,\|\, P(x,y), Q(x,z) \rightarrow R(x,y,z,u))\}$ is an HBS(LA) clause set, but not a (positively grounded) HBS(SLA) clause set due to the inequality $z \leq y+u$ and the lack of positively grounded predicates. However, the argument positions $(P,2)$, $(Q,2)$, $(R,2)$ and $(R,3)$ only have finitely many derivable values $\text{dvals}(P,2,N) = \text{dvals}(R,2,N) = \{1,3\}$ and $\text{dvals}(Q,2,N) = \text{dvals}(R,3,N) = \{0\}$. If we instantiate all occurrences of P and Q over those values, then we get the set $N' = \{(x \leq 1 \,\|\rightarrow P(x,1)), (x > 2 \,\|\rightarrow P(x,3)), (x \geq 0 \,\|\rightarrow Q(x,0)), (u \leq 1 \,\|\, P(x,1), Q(x,0) \rightarrow R(x,1,0,u)), (u \leq 3 \,\|\, P(x,3), Q(x,0) \rightarrow R(x,3,0,u))\}$ that is an HBS(SLA) clause set. This means N is an approximately grounded HBS(SLA) clause set and our extended Datalog hammer can handle it.

Test-Point Schemes and Functions The Datalog hammer in [8] is based on the following idea: For any pure HBS(SLA) clause set N that is unsatisfiable, we only need to look at the instances $\text{gnd}_B(N)$ of N over finitely many test points B to construct a refutation. Symmetrically, if N is satisfiable, then we can extrapolate a satisfying interpretation for N from a satisfying interpretation for $\text{gnd}_B(N)$. If we can compute such a set of test points B for a clause set N, then we can transform the clause set into an equisatisfiable Datalog program. (For universal/existential conjectures exist similar properties.) A *test-point scheme* is an algorithm that can compute such a set of test points B for any HBS(SLA) clause set N (and any conjecture $N \models Q\bar{x}.P(\bar{x})$ with $Q \in \{\exists,\forall\}$).

The test-point scheme used by our original Datalog hammer computes the same set of test points for all variables and predicate argument positions. This has several disadvantages: (i) it cannot handle variables with different sorts and (ii) it often selects too many test points (per argument position) because it cannot recognize which inequalities and which argument positions are connected. The goal of this paper is to resolve these issues. However, this also means that we have to assign different test-point sets to different predicate argument positions. We do this with so-called test-point functions.

A *test-point function* (tp-function) β is a function that assigns to some argument positions i of some predicates P a set of test points $\beta(P,i)$. An argument position (P,i) is assigned a set of test points if $\beta(P,i) \subseteq \text{sort}(P,i)^{\mathcal{A}}$ and otherwise $\beta(P,i) = \bot$. A test-point function β is *total* if all argument positions (P,i) are assigned (i.e., $\beta(P,i) \neq \bot$).

A variable x of a clause $\Lambda \parallel \Delta \rightarrow H$ occurs in an argument position (P,i) if $(P,i) \in \text{depend}(x,\Lambda \parallel \Delta \rightarrow H)$, where $\text{depend}(x,Y) = \{(P,i) \mid P(\bar{t}) \in \text{atoms}(Y) \text{ and } t_i = x\}$. Similarly, a variable x of an atom $Q(\bar{t})$ occurs in an argument position (Q,i) if $(Q,i) \in \text{depend}(x,Q(\bar{t}))$. A substitution σ for a clause Y or atom Y is a *well-typed instance* over a tp-function β if it guarantees for each variable x that $x\sigma$ is an element of $\text{sort}(x)^{\mathcal{A}}$ and part of every test-point set (i.e., $x\sigma \in \beta(P,i)$) of every argument position (P,i) it occurs in (i.e., $(P,i) \in \text{depend}(x,Y)$) and that is assigned a test-point set by β (i.e., $\beta(P,i) \neq \bot$). To abbreviate this, we define a set $\text{wti}(x,Y,\beta)$ that contains all values with which a variable can fulfill the above condition, i.e., $\text{wti}(x,Y,\beta) = \text{sort}(x)^{\mathcal{A}} \cap \bigcap_{(P,i) \in \text{depend}(x,Y) \text{ and } \beta(P,i) \neq \bot} \beta(P,i)$. Following this definition, we denote by $\text{wtis}_\beta(Y)$ the *set of all well-typed instances* for a clause/atom Y over the tp-function β, or formally: $\text{wtis}_\beta(Y) = \{\sigma \mid \forall x \in \text{vars}(Y).(x\sigma) \in \text{wti}(x,Y,\beta)\}$. With the function gnd_β, we denote the *set of all well-typed ground instances* of a clause/atom Y over the tp-function β, i.e., $\text{gnd}_\beta(Y) = \{Y\sigma \mid \sigma \in \text{wtis}_\beta(Y)\}$, or a set of clauses N, i.e., $\text{gnd}_\beta(N) = \{Y\sigma \mid Y \in N \text{ and } \sigma \in \text{wtis}_\beta(Y)\}$.

The most general tp-function, denoted by β^*, assigns each argument position to the interpretation of its sort, i.e., $\beta^*(P,i) = \text{sort}(P,i)^{\mathcal{A}}$. So depending on the sort of (P,i), either to $\mathbb{R}$, $\mathbb{Z}$, or one of the $\mathbb{F}_i$. A set of clauses N is satisfiable if and only if $\text{gnd}_{\beta^*}(N)$, the set of all ground instances of N over the base sorts, is satisfiable. Since β^* is the most general tp-function, we also write $\text{gnd}(Y)$ for $\text{gnd}_{\beta^*}(Y)$ and $\text{wtis}(Y)$ for $\text{wtis}_{\beta^*}(Y)$.

If we restrict ourselves to test points, then we also only get interpretations over test points and not for the full base sorts. In order to extrapolate an interpretation from test points to their full sorts, we define extrapolation functions (ep-functions) η. An *extrapolation function* (ep-function) $\eta(P,\bar{a})$ maps an argument vector of test points for predicate P (with $a_i \in \beta(P,i)$) to the subset of $\text{sort}(P,1)^{\mathcal{A}} \times \ldots \times \text{sort}(P,n)^{\mathcal{A}}$ that is supposed to be interpreted the same as $\bar{a}$, i.e., $P(\bar{a})$ is interpreted as true if and only if $P(\bar{b})$ with $\bar{b} \in \eta(P,\bar{a})$ is interpreted as true. By default, any argument vector of test points $\bar{a}$ for P must also be an element of $\eta(P,\bar{a})$, i.e.,

$\bar{a} \in \eta(P,\bar{a})$. An extrapolation function does not have to be complete for all argument positions, i.e., there may exist argument positions from which we cannot extrapolate to all argument vectors. Formally this means that the actual set of values that can be extrapolated from (P,i) (i.e., $\bigcup_{a_1 \in \beta(P,1)} \ldots \bigcup_{a_n \in \beta(P,n)} \eta(P,\bar{a})$) may be a strict subset of $\mathrm{sort}(P,1)^{\mathcal{A}} \times \ldots \times \mathrm{sort}(P,n)^{\mathcal{A}}$. For all other values $\bar{a}$, $P(\bar{a})$ is supposed to be interpreted as false.

Covering Clause Sets and Conjectures Our goal is to create total tp-functions that restrict our solution space from the infinite reals and integers to finite sets of test points while still preserving (un)satisfiability. Based on these tp-functions, we are then able to define a Datalog hammer that transforms a clause set belonging to (an extension of) HBS(LA) into an equisatisfiable HBS clause set; even modulo universal and existential conjectures.

To be more precise, we are interested in finite tp-functions (together with matching ep-functions) that cover a clause set N or a conjecture $N \models \mathcal{Q}\bar{x}.P(\bar{x})$ with $\mathcal{Q} \in \{\exists, \forall\}$. A total tp-function β is *finite* if each argument position is assigned to a finite set of test points, i.e., $|\beta(P,i)| \in \mathbb{N}$. A tp-function β *covers a set of clauses* N if $\mathrm{gnd}_\beta(N)$ is equisatisfiable to N. A tp-function β *covers a universal conjecture* $N \models \forall\bar{x}.Q(\bar{x})$ if $\mathrm{gnd}_\beta(N) \cup N_C$ is satisfiable if and only if $N \models \forall\bar{x}.Q(\bar{x})$ is false. Here N_C is the set $\{\| \mathrm{gnd}_\beta(Q(\bar{x})) \to \bot\}$ if η is complete for Q or the empty set otherwise. A tp-function β *covers an existential conjecture* $N \models \exists\bar{x}.Q(\bar{x})$ if $\mathrm{gnd}_\beta(N) \cup \mathrm{gnd}_\beta(\| Q(\bar{x}) \to \bot)$ is satisfiable if and only if $N \models \exists\bar{x}.Q(\bar{x})$ is false.

The most general tp-function β^* obviously covers all HBS(LA) clause sets and conjectures because satisfiability of N is defined over $\mathrm{gnd}_{\beta^*}(N)$. However, β^* is not finite. The test-point scheme in [8], which assigns one finite set of test points B to all variables, also covers clause sets and universal/existential conjectures; at least if we restrict our input to variables over the reals. As mentioned before, the goal of this paper is to fix the disadvantages of this test-point scheme by assigning different test-point sets to different predicate argument positions.

3 The Sorted Datalog Hammer

Approximately Grounded We start by formulating an extension of positively grounded HBS(SLA) called approximately grounded HBS(SLA) that will be the input logic for our new test-point scheme. It is based on an over-approximation of the derivable values for each argument position. An argument position (P,i) is *(in)finite* if $\mathrm{dfacts}(P,N)$ contains (in)finitely many different values at position i, i.e., the set of *derivable values* $\mathrm{dvals}(P,i,N)$ is (in)finite. Naturally, all argument positions over first-order sorts $\mathcal{F}$ are finite argument positions. But other argument positions can be finite too, e.g., in the set of clauses $\{P(0), P(1), P(x) \to Q(x)\}$ all argument positions of all predicates are finite.

Lemma 6. *Determining the finiteness of a predicate argument position in an* HBS(LA) *clause set is undecidable.*

Determining the finiteness of a predicate argument position (and all its derivable values) is not trivial. In general, it is as hard as determining the satisfiability of a clause set, so in the case of HBS(LA) undecidable [12,20]. This is the reason, why we propose to over-approximate the finiteness of our predicate argument positions and use this over-approximation as basis for our extension of pure HBS(SLA). The idea of this approximation is to traverse clauses bottom up.

For all predicate argument positions the abstraction considers two values: finite or infinite. At start, all predicate argument positions are finite. As long as all clauses contain negative first-order literals, all argument positions remain finite, because the empty relation for all predicates is a model for the clause set. Otherwise, there must be clauses $\Lambda \,\|\!\rightarrow H$ and for all these clauses we can determine the argument values of the respective predicates: it remains finite as long as the argument position is not a variable that is not finitely bounded by the constraint Λ. Now we take these initial values for propagation through the other clauses $\Lambda \,\|\, \Delta \rightarrow H$, where argument position values only change from finite to infinite. This is repeated as long as argument positions change from finite to infinite by propagating newly detected infinite positions through clauses. The algorithm terminates because the number of all argument positions is finite. A detailed version of the approximation algorithm can be found in the appendix, Section 6.

Let $\mathrm{avals}(P,i,N) \supseteq \mathrm{dvals}(P,i,N)$ be an over-approximation of the derivable values per argument position. Then $|\mathrm{avals}(P,i,N)| \in \mathbb{N}$ is a sufficient criteria for argument position i of P being finite in N. Based on avals, we can now build a tp-function β^a that maps all finite argument positions (P,i) that our over-approximation detected to the over-approximation of their derivable values, i.e., $\beta^a(P,i) := \mathrm{avals}(P,i,N)$ if $|\mathrm{avals}(P,i,N)| \in \mathbb{N}$ and $\beta^a(P,i) := \perp$ otherwise. With β^a we derive the finitely grounded over-approximation $\mathrm{agnd}(Y)$ of a set of clauses Y, a clause Y or an atom Y. This set is equivalent to $\mathrm{gnd}_{\beta^a}(Y)$, except that we assume that all LA atoms are simplified until they contain at most one integer number and that LA atoms that can be evaluated are reduced to true and false and the respective clause simplified. Based of $\mathrm{agnd}(N)$ we define a new extension of HBS(SLA) called approximately grounded HBS(SLA):

Definition 7 (Approximately Grounded HBS(SLA)**:** HBS(SLA)A**).** *A clause set N is out of the fragment* approximately grounded HBS(SLA) *or short* HBS(SLA)A *if* $\mathrm{agnd}(N)$ *is out of the* HBS(SLA) *fragment. It is called* HBS(SLA)PA *if it is also pure.*

Connecting Argument Positions and Selecting Test Points As our second step, we are reducing the number of test points per predicate argument position by incorporating that not all argument positions are connected to all inequalities. This also means that we select different sets of test points for different argument positions. For finite argument positions, we can simply pick $\mathrm{avals}(P,i,N)$ as its set of test points. However, before we can compute the test-point sets for all other argument positions, we first have to determine to which inequalities and other argument positions they are connected.

Let N be an HBS(SLA)PA clause set and (P,i) an argument position for a predicate in N. Then we denote by $\mathrm{conArgs}(P,i,N)$ the *set of connected argument positions* and by $\mathrm{conIneqs}(P,i,N)$ the *set of connected inequalities*. Formally, $\mathrm{conArgs}(P,i,N)$ is defined as the minimal set that fulfills the following conditions: (i) two argument positions (P,i) and (Q,j) are connected if they share a variable in a clause in N, i.e., $(Q,j) \in \mathrm{conArgs}(P,i,N)$ if $(\Lambda \,\|\, \Delta \rightarrow H) \in N$, $P(\bar{t}), Q(\bar{s}) \in \mathrm{atoms}(\Delta \cup \{H\})$, and $t_i = s_j = x$; and (ii) the connection relation is transitive, i.e., if $(Q,j) \in \mathrm{conArgs}(P,i,N)$, then $\mathrm{conArgs}(P,i,N) = \mathrm{conArgs}(Q,j,N)$. Similarly, $\mathrm{conIneqs}(P,i,N)$ is defined as the minimal set that fulfills the following conditions: (i) an argument position (P,i) is connected to an instance λ' of an inequality λ if they share a variable in a clause in N, i.e., $\lambda' \in \mathrm{conIneqs}(P,i,N)$ if $(\Lambda \,\|\, \Delta \rightarrow H) \in N$, $P(\bar{t}) \in \mathrm{atoms}(\Delta \cup \{H\})$, $t_i = x$, $(\Lambda' \,\|\, \Delta' \rightarrow H') \in \mathrm{agnd}(\Lambda \,\|\, \Delta \rightarrow H)$, $\lambda' \in \Lambda'$, and $\lambda' = x \triangleleft c$ (where $\triangleleft = \{<,>,\leq,\geq,=,\neq\}$ and $c \in \mathbb{Z}$); (ii) an argument position (P,i) is connected to a value $c \in \mathbb{Z}$ if $P(\bar{t})$ with $t_i = c$ appears in a clause in N, i.e., $(x = c) \in \mathrm{conIneqs}(P,i,N)$ if $(\Lambda \,\|\, \Delta \rightarrow H) \in N$, $P(\bar{t}) \in \mathrm{atoms}(\Delta \cup \{H\})$, and $t_i = c$; (iii) an argument position (P,i) is connected to a value $c \in \mathbb{Z}$ if (P,i) is finite and $c \in \text{avals}(P,i,N)$, i.e., $(x=c) \in \text{conIneqs}(P,i,N)$ if (P,i) is finite and $c \in \text{avals}(P,i,N)$; and (iv) the connection relation is transitive, i.e., $\lambda \in \text{conArgs}(Q,j,N)$ if $\lambda \in \text{conIneqs}(P,i,N)$ and $(Q,j) \in \text{conArgs}(P,i,N)$.

Now based on these sets we can construct a set of test points as follows: For each argument position (P,i), we partition the reals $\mathbb{R}$ into intervals such that any variable bound in $\lambda \in \text{conIneqs}(P,i,N)$ is satisfied by all points in one such interval I or none. Since we are in the horn case, this is enough to ensure that we derive facts *uniformly* over those intervals and the integers/non-integers. To be more precise, we derive facts *uniformly* over those intervals and the integers because $P(\bar{a})$ is derivable from N and $a_i \in I \cap \mathbb{Z}$ implies that $P(\bar{b})$ is also derivable from N, where $b_j = a_j$ for $i \neq j$ and $b_i \in I \cap \mathbb{Z}$. Similarly, we derive facts *uniformly* over those intervals and the non-integers because $P(\bar{a})$ is derivable from N and $a_i \in I \setminus \mathbb{Z}$ implies that $P(\bar{b})$ is also derivable from N, where $b_j = a_j$ for $i \neq j$ and $b_i \in I$. As a result, it is enough to pick (if possible) one integer and one non-integer test point per interval to cover the whole clause set.

Formally we compute the interval partition $\text{iPart}(P,i,N)$ and the set of test points $\text{tps}(P,i,N)$ as follows: First we transform all variable bounds $\lambda \in \text{conIneqs}(P,i,N)$ into interval borders. A variable bound $x \triangleleft c$ with $\triangleleft \in \{\leq,<,>,\geq\}$ in $\text{conIneqs}(P,i,N)$ is turned into two interval borders. One of them is the interval border implied by the bound itself and the other its negation, e.g., $x \geq 5$ results in the interval border $[5$ and the interval border of the negation $5)$. Likewise, we turn every variable bound $x \triangleleft c$ with $\triangleleft \in \{=,\neq\}$ into all four possible interval borders for c, i.e. $c)$, $[c$, $c]$, and $(c$. The set of interval borders $\text{iEP}(P,i,N)$ is then defined as follows:

$$\begin{aligned}\text{iEP}(P,i,N) = {} & \{c],(c \mid x \triangleleft c \in \text{conIneqs}(P,i,N) \text{ where } \triangleleft \in \{\leq,=,\neq,>\}\} \cup \\ & \{c),[c \mid x \triangleleft c \in \text{conIneqs}(P,i,N) \text{ where } \triangleleft \in \{\geq,=,\neq,<\}\} \cup \{(-\infty,\infty)\}\end{aligned}$$

The interval partition $\text{iPart}(P,i,N)$ can be constructed by sorting $\text{iEP}(P,i,N)$ in an ascending order such that we first order by the border value—i.e. $\delta < \epsilon$ if $\delta \in \{c),[c,c],(c\}$, $\epsilon \in \{d),[d,d],(d\}$, and $c < d$—and then by the border type—i.e. $c) < [c < c] < (c$. The result is a sequence $[\ldots,\delta_l,\delta_u,\ldots]$, where we always have one lower border δ_l, followed by one upper border δ_u. We can guarantee that an upper border δ_u follows a lower border δ_l because $\text{iEP}(P,i,N)$ always contains $c)$ together with $[c$ and $c]$ together with $(c$ for $c \in \mathbb{Z}$, so always two consecutive upper and lower borders. Together with $(-\infty$ and $\infty)$ this guarantees that the sorted $\text{iEP}(P,i,N)$ has the desired structure. If we combine every two subsequent borders δ_l, δ_u in our sorted sequence $[\ldots,\delta_l,\delta_u,\ldots]$, then we receive our partition of intervals $\text{iPart}(P,i,N)$. For instance, if $x < 5$ and $x = 0$ are the only variable bounds in $\text{conIneqs}(P,i,N)$, then $\text{iEP}(P,i,N) = \{5),[5,0),[0,0],(0,(-\infty,\infty)\}$ and if we sort and combine them we get $\text{iPart}(P,i,N) = \{(-\infty,0),[0,0],(0,5),[5,\infty)\}$.

After constructing $\text{iPart}(P,i,N)$, we can finally construct the set of test points $\text{tps}(P,i,N)$ for argument position (P,i). If $|\text{avals}(P,i,N)| \in \mathbb{N}$, i.e., we determined that (P,i) is finite, then $\text{tps}(P,i,N) = \text{avals}(P,i,N)$. If the argument position (P,i) is over a first-order sort $\mathcal{F}_i$, i.e., $\text{sort}(P,i) = \mathcal{F}_i$, then we should always be able to determine that (P,i) is finite because $\mathbb{F}_i$ is finite. If the argument position (P,i) is over an arithmetic sort, i.e., $\text{sort}(P,i) = \mathcal{R}$ or $\text{sort}(P,i) = \mathcal{Z}$, and our approximation could not determine that (P,i) is finite, then the test-point set $\text{tps}(P,i,N)$ for (P,i) consists of at most two points per interval $I \in \text{iPart}(P,i,N)$: one integer value $a_I \in I \cap \mathbb{Z}$ if I contains integers (i.e. if $I \cap \mathbb{Z} \neq \emptyset$) and one non-integer value $b_I \in I \setminus \mathbb{Z}$ if I contains non-integers (i.e. if I is not just one integer point). Additionally, we enforce that $\text{tps}(P,i,N) = \text{tps}(Q,j,N)$ if $\text{conArgs}(P,i,N) = \text{conArgs}(Q,j,N)$ and both (P,i) and (Q,j) are infinite argument positions. (In our implementation of this test-point scheme, we optimize the test point selection even further by picking only one test point per interval—if possible an integer value and otherwise a non-integer—if all conArgs(P,i,N) and all variables x connecting them in N have the same sort. However, we do not prove this optimization explicitly here because the proofs are almost identical to the case for two test points per interval.)

Based on these sets, we can now also define a tp-function β and an ep-function η. For the tp-function, we simply assign any argument position to tps(P,i,N), i.e., $\beta(P,i) = \text{tps}(P,i,N) \cap \text{sort}(P,i)^{\mathcal{A}}$. (The intersection with sort$(P,i)^{\mathcal{A}}$ is needed to guarantee that the test-point set of an integer argument position is well-typed.) This also means that β is total and finite. For the ep-function η, we extrapolate any test-point vector $\bar{a}$ (with $\bar{a} = \bar{x}\sigma$ and $\sigma \in \text{wtis}_\beta(P(\bar{x}))$) over the (non-)integer subset of the intervals the test points belong to, i.e., $\eta(P,\bar{a}) = I'_1 \times \ldots \times I'_n$, where $I'_i = \{a_i\}$ if we determined that (P,i) is finite and otherwise I_i is the interval $I_i \in \text{iPart}(P,i,N)$ with $a_i \in I_i$ and $I'_i = I_i \cap \mathbb{Z}$ if a_i is an integer value and $I'_i = I_i \setminus \mathbb{Z}$ if a_i is a non-integer value. Note that this means that η might not be complete for every predicate P, e.g., when P has a finite argument position (P,i) with an infinite domain. However, both β and η together still cover the clause set N, cover any universal conjecture $N \models \forall \bar{x}.Q(\bar{x})$, and cover any existential conjecture $N \models \exists \bar{x}.Q(\bar{x})$.

Theorem 8. *The* tp-function β *covers* N*. The* tp-function β *covers an existential conjecture* $N \models \exists \bar{x}.Q(\bar{x})$*. The* tp-function β *covers a universal conjecture* $N \models \forall \bar{x}.Q(\bar{x})$*.*

From a Test-Point Function to a Datalog Hammer We can use the covering definitions, e.g., $\text{gnd}_\beta(N)$ is equisatisfiable to N, to instantiate our clause set (and conjectures) with numbers. As a result, we can simply evaluate all theory atoms and thus reduce our HBS(SLA)PA clause sets/conjectures to ground HBS clause sets, which means we could reduce our input into formulas without any arithmetic theory that can be solved by any Datalog reasoner. There is, however, one problem. The set $\text{gnd}_\beta(N)$ grows exponentially with regard to the maximum number of variables n_C in any clause in N, i.e. $O(|\text{gnd}_\beta(N)|) = O(|N| \cdot |B|^{n_C})$, where $B = \max_{(P,i)}(\beta(P,i))$ is the largest test-point set for any argument position. Since n_C is large for realistic examples (e.g., in our examples the size of n_C ranges from 9 to 11 variables), the finite abstraction is often too large to be solvable in reasonable time. Due to this blow-up, we have chosen an alternative approach for our Datalog hammer. This hammer exploits the ideas behind the covering definitions and will allow us to make the same ground deductions, but instead of grounding everything, we only need to (i) ground the negated conjecture over our tp-function and (ii) provide a set of ground facts that define which theory atoms are satisfied by our test points. As a result, the hammered formula is much more concise and we need no actual theory reasoning to solve the formula. In fact, we can solve the hammered formula by greedily applying unit resolution until this produces the empty clause—which would mean the conjecture is implied—or until it produces no more new facts—which would mean we have found a counter example. (In practice, greedily applying resolution is not the best strategy and we recommend to use more advanced HBS techniques for instance those used by a state-of-the-art Datalog reasoner.)

The Datalog hammer takes as input (i) a HBS(SLA)PA clause set N and (ii) optionally a universal conjecture $\forall \bar{y}.P(\bar{y})$. (The case for existential conjectures is handled by encoding the conjecture $N \models \exists \bar{x}.Q(\bar{x})$ as the clause set $N \cup \{Q(\bar{x}) \rightarrow \bot\}$, which is unsatisfiable if and only if the conjecture holds.) Given this input, the Datalog hammer first computes the tp-function β and the ep-function η as described above. Next, it computes four clause sets that will make up the Datalog formula. The first set $\text{tren}_N(N)$ is computed by abstracting away any arithmetic from the clauses $(\Lambda \parallel \Delta \rightarrow H) \in N$. This is done by replacing each theory atom A in Λ with a literal $P_A(\bar{x})$, where $\text{vars}(A) = \text{vars}(\bar{x})$ and P_A is a fresh predicate. The abstraction of the theory atoms is necessary because Datalog does not support non-constant function symbols (e.g., $+,-$) that would otherwise appear in approximately grounded theory atoms. Moreover, it is necessary to add extra sort literals $\neg Q_{(P,i,S)}(x)$ for some of the variables $x \in \text{vars}(H)$, where $H = P(\bar{t})$, $t_i = x$, $\text{sort}(x) = S$, and $Q_{(P,i,S)}$ is a fresh predicate. This is necessary in order to define over which test point set x can range if x does not appear in Λ or in Δ. It is also necessary in order to filter out any test points that are not integer values if x is an integer variable (i.e. $\text{sort}(x) = \mathcal{Z}$) but connected only to real sorted argument positions in Δ (i.e. $\text{sort}(Q,j) = \mathcal{R}$ for all $(Q,j) \in \text{depend}(x,\Delta)$). (It is possible to reduce the number of fresh predicates needed, e.g., by reusing the same predicate for two theory atoms whose variables range over the same sets of test points.) The resulting abstracted clause has then the form $\Delta_T,\Delta_S,\Delta \to H$, where Δ_T contains the abstracted theory literals (e.g. $P_A(\bar{x}) \in \Delta_T$) and Δ_S the "sort" literals (e.g. $Q_{(P,i,S)}(x) \in \Delta_S$). The second set is denoted by N_C and it is empty if we have no universal conjecture or if η does not cover our conjecture. Otherwise, N_C contains the ground and negated version ϕ of our universal conjecture $\forall \bar{y}.P(\bar{y})$. ϕ has the form $\Delta_\phi \to \bot$, where $\Delta_\phi = \text{gnd}_\beta(P(\bar{y}))$ contains all literals $P(\bar{y})$ for all groundings over β. We cannot skip this grounding but the worst-case size of Δ_ϕ is $O(\text{gnd}_\beta(P(\bar{y}))) = O(|B|^{n_\phi})$, where $n_\phi = |\bar{y}|$, which is in our applications typically much smaller than the maximum number of variables n_C contained in any clause in N. The third set is denoted by $\text{tfacts}(N,\beta)$ and contains a fact $\text{tren}_N(A)$ for every ground theory atom A contained in the theory part Λ of a clause $(\Lambda \parallel \Delta \to H) \in \text{gnd}_\beta(N)$ such that A simplifies to true. This is enough to ensure that our abstracted theory predicates evaluate every test point in every satisfiable interpretation $\mathcal{A}$ to true that also would have evaluated to true in the actual theory atom. (Alternatively, it is also possible to use a set of axioms and a smaller set of facts and let the Datalog reasoner compute all relevant theory facts for itself.) The set $\text{tfacts}(N,\beta)$ can be computed without computing $\text{gnd}_\beta(N)$ if we simply iterate over all theory atoms A in all constraints Λ of all clauses $Y = \Lambda \parallel \Delta \to H$ (with $Y \in N$) and compute all well typed groundings $\tau \in \text{wtis}_\beta(Y)$ such that $A\tau$ simplifies to true. This can be done in time $O(\mu(n_v) \cdot n_L \cdot |B|^{n_v})$ and the resulting set $\text{tfacts}(N,\beta)$ has worst-case size $O(n_A \cdot |B|^{n_v})$, where n_L is the number of literals in N, n_v is the maximum number of variables $|\text{vars}(A)|$ in any theory atom A in N, n_A is the number of different theory atoms in N, and $\mu(x)$ is the time needed to simplify a theory atom over x variables to a variable bound. The last set is denoted by $\text{sfacts}(N,\beta)$ and contains a fact $Q_{(P,i,S)}(a)$ for every fresh sort predicate $Q_{(P,i,S)}$ added during abstraction and every $a \in \beta(P,i) \cap S^{\mathcal{A}}$. This is enough to ensure that $Q_{(P,i,S)}$ evaluates to true for every test point assigned to the argument position (P,i) filtered by the sort S. Please note that already satifiability testing for BS clause is NEXPTIME-complete in general, and DEXPTIME-complete for the Horn case [23,30]. So when abstracting to a polynomially decidable clause set (ground HBS) an exponential factor is unavoidable.

Lemma 9. *N is equisatisfiable to its hammered version* $\text{tren}_N(N) \cup \text{tfacts}(N,\beta) \cup \text{sfacts}(N,\beta)$. *The conjecture $N \models \exists \bar{y}.Q(\bar{y})$ is false iff $N_D = \text{tren}'_N(N') \cup \text{tfacts}(N',\beta) \cup \text{sfacts}(N',\beta)$ is satisfiable with $N' = N \cup \{Q(\bar{y}) \to \bot\}$. The conjecture $N \models \forall \bar{y}.Q(\bar{y})$ is false iff $N_D = \text{tren}_N(N) \cup \text{tfacts}(N,\beta) \cup \text{sfacts}(N,\beta) \cup N_C$ is satisfiable.*

Note that $\text{tren}_N(N) \cup \text{tfacts}(N,\beta) \cup \text{sfacts}(N,\beta) \cup N_C$ is only a HBS clause set over a finite set of constants and not yet a Datalog input file. It is well known that such a formula can be transformed easily into a Datalog problem by adding a nullary predicate Goal and adding it

Problem	Q	Status	$\lvert B_{\max}\rvert$	$\lvert\Delta_\phi\rvert$	SPASS-SPL	$\lvert B^o\rvert$	$\lvert\Delta_\phi^o\rvert$	SPASS-SPL-v0.6	vampire	spacer	z3	cvc4
lc_e1	∃	true	9	0	**< 0.1s**	45	0	**< 0.1s**	**< 0.1s**	**< 0.1s**	0,1	**< 0.1s**
lc_e2	∃	false	9	0	**< 0.1s**	41	0	**< 0.1s**	**< 0.1s**	**< 0.1s**	timeout	timeout
lc_e3	∃	false	9	0	**< 0.1s**	37	0	**< 0.1s**	**< 0.1s**	**< 0.1s**	timeout	timeout
lc_e4	∃	true	9	0	**< 0.1s**	49	0	**< 0.1s**	**< 0.1s**	**< 0.1s**	**< 0.1s**	**< 0.1s**
lc_e5	∃	false	9	0	33.5s	-	-	N/A	**< 0.1s**	timeout	timeout	timeout
lc_e6	∃	true	9	0	42.8s	-	-	N/A	**0.1s**	3.3s	11.5s	0.4s
lc_e7	∃	false	9	0	41.4s	-	-	N/A	**< 0.1s**	7.6s	timeout	timeout
lc_e8	∃	false	9	0	32.5s	-	-	N/A	**< 0.1s**	2.1s	timeout	timeout
lc_u1	∀	false	9	27	**< 0.1s**	45	27	**< 0.1s**	**< 0.1s**	N/A	timeout	timeout
lc_u2	∀	false	9	27	**< 0.1s**	41	27	**< 0.1s**	**< 0.1s**	N/A	timeout	timeout
lc_u3	∀	true	9	27	**< 0.1s**	37	27	**< 0.1s**	**< 0.1s**	N/A	**< 0.1s**	**< 0.1s**
lc_u4	∀	false	9	27	**< 0.1s**	49	27	**< 0.1s**	**< 0.1s**	N/A	timeout	timeout
lc_u5	∀	false	9	3888	32.4s	-	-	N/A	**0.1s**	N/A	timeout	timeout
lc_u6	∀	true	9	3888	32.5s	-	-	N/A	**2.3s**	N/A	timeout	timeout
lc_u7	∀	true	9	972	32.3s	-	-	N/A	**0.2s**	N/A	timeout	timeout
lc_u8	∀	false	9	1259712	**48.8s**	-	-	N/A	2351.4s	N/A	timeout	timeout
ecu_e1	∃	false	96	0	**< 0.1s**	624	0	1.3s	0.2s	0.1s	timeout	timeout
ecu_e2	∃	true	96	0	**< 0.1s**	624	0	1.3s	0.2s	0.1s	1.4s	0.4s
ecu_e3	∃	false	196	0	50.1s	660	0	41.5s	3.1s	**0.1s**	timeout	timeout
ecu_u1	∀	true	96	37	**0.1s**	620	306	1.1s	32.8s	N/A	197.5s	0.4s
ecu_u2	∀	false	96	38	**0.1s**	620	307	1.1s	32.8s	N/A	timeout	timeout
ecu_u3	∀	true	88	760	**< 0.1s**	576	11360	0.7s	1.2s	N/A	239.5s	0.1s
ecu_u4	∀	true	486	760	**< 0.1s**	2144	237096	15.9s	1.2s	N/A	196.0s	0.1s
ecu_u5	∀	true	96	3900	**0.1s**	628	415296	31.9s	timeout	N/A	timeout	timeout
ecu_u6	∀	false	95	3120	**< 0.1s**	616	363584	14.4s	597.8	N/A	timeout	timeout
ecu_u7	∀	false	196	8400	**48.9s**	656	2004708	memout	timeout	N/A	timeout	timeout
ecu_u8	∀	true	196	8400	**48.7s**	656	2004708	memout	timeout	N/A	timeout	timeout

Fig. 2. Benchmark results and statistics

as a positive literal to any clause without a positive literal. Querying for the Goal atom returns true if the HBS clause set was unsatisfiable and false otherwise.

4 Implementation and Experiments

We have implemented the sorted Datalog hammer as an extension to the SPASS-SPL system [8] (option `-d`). The previously file-based combination with the Datalog reasoner VLog has been replaced by an integration of VLog into SPASS-SPL via the VLog API. We focus here only on the sorted extension and refer to [8] for an introduction into coupling of the two reasoners.

In order to test the progress in efficiency of our sorted hammer, we ran the benchmarks of the lane change assistant and engine ECU from [8] plus more sophisticated, extended formalizations. While for the ECU benchmarks in [8] we modeled ignition timing computation adjusted by inlet temperature measurements, the new benchmarks take also gear box protection mechanisms into account. The lane change examples in [8] only simulated the supervisor for lane change assistants over some real-world instances. The new lane change benchmarks check properties for all potential inputs. The universal ones check that any suggested action by a lane change assistant is either proven as correct or disproved by our supervisor. The existential ones check safety properties, e.g., that the supervisor never returns both a proof and a disproof for the same input. (We actually managed to discover some bugs in the original lane change supervisor with the help of SPASS-SPL and these new benchmarks.)

The names of the problems are formatted so the lane change examples start with lc and the ECU examples start with ecu. Our benchmarks are prototypical for the complexity of

HBS(SLA) reasoning in that they cover all abstract relationships between conjectures and HBS(SLA) clause sets. With respect to our two case studies we have many more examples showing respective characteristics. We would have liked to run benchmarks from other sources, but could not find any suitable HBS(SLA) problems in the SMT-LIB or CHC-COMP benchmarks.

For comparison, we also tested several state-of-the-art theorem provers for related logics (with the best settings we found): SPASS-SPL-v0.6 that uses the original version of our Datalog Hammer [8] with settings `-d` for existential and `-d -n` for universal conjectures; the satisfiability modulo theories (SMT) solver *cvc4-1.8* [4] with settings `--multi-trigger-cache --full-saturate-quant`; the SMT solver *z3-4.8.12* [25] with its default settings; the constrained horn clause (CHC) solver *spacer* [21] with its default settings; and the first-order theorem prover *vampire-4.5.1* [33] with settings `--memory_limit 8000 -p off`, i.e., with memory extended to 8GB and without proof output. For the SMT/CHC solvers, we directly transformed the benchmarks into their respective formats. For vampire, we applied our sorted Hammer before transforming to TPTP format [35].

For the experiments, we used the TACAS 22 artifact evaluation VM (Ubuntu 20.04 with 8 GB RAM and a single processor core) on a system with an Intel Core i7-9700K CPU with eight 3.60GHz cores. Each tool got a time limit of 40 minutes for each problem.

The table in Fig. 2 lists for each benchmark problem: the name of the problem (Problem); the type of conjecture (Q), i.e., whether the conjecture is existential ∃ or universal ∀; the status of the conjecture (Status), i.e., the size of the largest test-point set introduced by the sorted/original Hammer ($B_{\max}/B^o$); the size of the hammered universal conjecture ($|\Delta_\phi|/|\Delta_\phi^o|$ for sorted/original); the remaining columns list the time needed by the tools to solve the benchmark problems. An entry "N/A" means that the benchmark example cannot be expressed in the tools input format, e.g., it is not possible to encode a universal conjecture (or, to be more precise, its negation) in the CHC format and SPASS-SPL-v0.6 is not sound when the problem contains integer variables. An entry "timeout" means that the tool could not solve the problem in the given time limit of 40 minutes or returned unknown. An entry "memout" means that the tool ran out of memory before the time limit.

The experiments show that SPASS-SPL (with the sorted Hammer) is orders of magnitudes faster than SPASS-SPL-v0.6 (with the original Hammer) on problems with universal conjectures. On problems with existential conjectures, we cannot observe any major performance gain compared to the original Hammer. Sometimes SPASS-SPL-v0.6 is even slightly faster (e.g. ecu_e3). Potential explanations are: First, the number of test points has a much larger impact on universal conjectures because the size of the hammered universal conjecture increases exponentially with the number of test points. Second, our sorted Hammer needs to generate more abstracted theory facts than the original Hammer because the latter can reuse abstraction predicates for theory atoms that are identical upto variable renaming. The sorted Hammer can reuse the same predicate only if variables also range over the same sets of test points, which can be expensive to check so we have not implemented it.

Compared to the other tools, SPASS-SPL is the only one that solves all problems in reasonable time. It is also the only solver that can decide in reasonable time whether a universal conjecture is not a consequence. This is not surprising because to our knowledge SPASS-SPL is the only theorem prover that implements a decision procedure for HBS(SLA). On the problems with existential conjectures, our toolchain solves all of the problems in under a minute and with comparable times to the best tool for the problem. The only exception are problems that contain a lot of superfluous clauses, i.e., clauses that are not needed to confirm/refute the conjecture. The reason might be that Rulework (the Datalog reasoner used by SPASS-SPL) derives all facts for the input problem in a breadth-first way, which is not very efficient if there are a lot of superfluous clauses. It is therefore no surprise that a goal oriented superposition solver like Vampire coupled with our sorted Hammer seems to return the best results for those problems. Vampire performed best on the hammered problems among all first-order theorem provers we tested, including iProver [22], E [34], and SPASS [36]. We tested all provers in default theorem proving mode (with adjusted memory limits). The experiments with the first-order provers showed that our hammer also works reasonably well for them, but they do not scale well if the size and the complexity of the universal conjectures increases. For problems with existential conjectures, the CHC solver spacer is often the best, but as a trade-off it is unable to handle universal conjectures. The instantiation techniques employed by cvc4 are good for proving some universal conjectures, but both SMT solvers seem to be unable to disprove conjectures.

5 Conclusion

We have presented an extension of our previous Datalog hammer [8] supporting a more expressive input logic resulting in more elegant and more detailed supervisor formalizations, and through a soft typing discipline supporting more efficient reasoning. Our experiments show, compared to [8], that our performance on existential is at the same level as SMT and CHC solvers. The complexity of queries we can handle in reasonable time has significantly increased, see Section 4, Figure 2. Still SPASS-SPL is the only solver that can prove and disprove universal queries. The file interface between SPASS-SPL and VLog has been replaced by a close coupling resulting in a more comfortable application.

Our contribution here solves the third point for future work mentioned in [8] although there is still room to also improve our soft typing discipline. In the future, we want SPASS-SPL to produce explications that prove that its translations are correct. Another direction is to exploit specialized Datalog expressions and techniques (e.g., aggregation and stratified negation) to increase the efficiency of our tool-chain and to lift some restrictions from our input formulas. Finally, our hammer can be seen as part of an overall reasoning methodology for the class of BS(LA) formulas which we presented in [9]. We will implement and further develop this methodology and integrate our Datalog hammer.

Acknowledgments: This work was funded by DFG grant 389792660 as part of TRR 248 (CPEC), by BMBF in project ScaDS.AI, and by the Center for Advancing Electronics Dresden (cfaed).

References

1. A Git repository with binaries for SPASS-SPL and all benchmarks presented in this paper. https://github.com/mbromber/eval-sorted-datalog-hammer
2. Abiteboul, S., Hull, R., Vianu, V.: Foundations of Databases. Addison Wesley (1994)
3. Bachmair, L., Ganzinger, H., Waldmann, U.: Refutational theorem proving for hierarchic first-order theories. Applicable Algebra in Engineering, Communication and Computing, AAECC **5**(3/4), 193–212 (1994)

4. Barrett, C., Conway, C., Deters, M., Hadarean, L., Jovanović, D., King, T., Reynolds, A., Tinelli, C.: CVC4. In: CAV, LNCS, vol. 6806 (2011)
5. Baumgartner, P., Waldmann, U.: Hierarchic superposition revisited. In: Lutz, C., Sattler, U., Tinelli, C., Turhan, A., Wolter, F. (eds.) Description Logic, Theory Combination, and All That - Essays Dedicated to Franz Baader on the Occasion of His 60th Birthday. Lecture Notes in Computer Science, vol. 11560, pp. 15–56. Springer (2019)
6. Bjørner, N., Gurfinkel, A., McMillan, K.L., Rybalchenko, A.: Horn clause solvers for program verification. In: Beklemishev, L.D., Blass, A., Dershowitz, N., Finkbeiner, B., Schulte, W. (eds.) Fields of Logic and Computation II - Essays Dedicated to Yuri Gurevich on the Occasion of His 75th Birthday. Lecture Notes in Computer Science, vol. 9300, pp. 24–51. Springer (2015)
7. Böhme, S., Nipkow, T.: Sledgehammer: Judgement day. In: Giesl, J., Hähnle, R. (eds.) Automated Reasoning, 5th International Joint Conference, IJCAR 2010, Edinburgh, UK, July 16-19, 2010. Proceedings. Lecture Notes in Computer Science, vol. 6173, pp. 107–121. Springer (2010)
8. Bromberger, M., Dragoste, I., Faqeh, R., Fetzer, C., Krötzsch, M., Weidenbach, C.: A datalog hammer for supervisor verification conditions modulo simple linear arithmetic. In: Reger, G., Konev, B. (eds.) Frontiers of Combining Systems - 13th International Symposium, FroCoS 2021, Birmingham, United Kongdom, September 8-10, 2021. Proceedings. Lecture Notes in Computer Science, vol. 12941, pp. 3–24. Springer (2021)
9. Bromberger, M., Fiori, A., Weidenbach, C.: Deciding the bernays-schoenfinkel fragment over bounded difference constraints by simple clause learning over theories. In: Henglein, F., Shoham, S., Vizel, Y. (eds.) Verification, Model Checking, and Abstract Interpretation - 22nd International Conference, VMCAI 2021, Copenhagen, Denmark, January 17-19, 2021, Proceedings. Lecture Notes in Computer Science, vol. 12597, pp. 511–533. Springer (2021)
10. Carral, D., Dragoste, I., González, L., Jacobs, C., Krötzsch, M., Urbani, J.: VLog: A rule engine for knowledge graphs. In: Ghidini et al., C. (ed.) Proc. 18th Int. Semantic Web Conf. (ISWC'19, Part II). LNCS, vol. 11779, pp. 19–35. Springer (2019)
11. Cimatti, A., Griggio, A., Redondi, G.: Universal invariant checking of parametric systems with quantifier-free SMT reasoning. In: Proc. CADE-28 (2021), to appear
12. Downey, P.J.: Undecidability of presburger arithmetic with a single monadic predicate letter. Tech. rep., Center for Research in Computer Technology, Harvard University (1972)
13. Eiter, T., Gottlob, G., Mannila, H.: Disjunctive datalog. ACM Trans. Database Syst. **22**(3), 364–418 (1997)
14. Faqeh, R., Fetzer, C., Hermanns, H., Hoffmann, J., Klauck, M., Köhl, M.A., Steinmetz, M., Weidenbach, C.: Towards dynamic dependable systems through evidence-based continuous certification. In: Margaria, T., Steffen, B. (eds.) Leveraging Applications of Formal Methods, Verification and Validation: Engineering Principles - 9th International Symposium on Leveraging Applications of Formal Methods, ISoLA 2020, Rhodes, Greece, October 20-30, 2020, Proceedings, Part II. Lecture Notes in Computer Science, vol. 12477, pp. 416–439. Springer (2020)
15. Fiori, A., Weidenbach, C.: SCL with theory constraints. CoRR **abs/2003.04627** (2020), https://arxiv.org/abs/2003.04627
16. Ge, Y., de Moura, L.M.: Complete instantiation for quantified formulas in satisfiabiliby modulo theories. In: Computer Aided Verification, 21st International Conference, CAV 2009, Grenoble, France, June 26 - July 2, 2009. Proceedings. Lecture Notes in Computer Science, vol. 5643, pp. 306–320. Springer (2009)
17. Grebenshchikov, S., Lopes, N.P., Popeea, C., Rybalchenko, A.: Synthesizing software verifiers from proof rules. In: Vitek, J., Lin, H., Tip, F. (eds.) ACM SIGPLAN Conference on Programming Language Design and Implementation, PLDI '12, Beijing, China - June 11 - 16, 2012. pp. 405–416. ACM (2012)
18. Hillenbrand, T., Weidenbach, C.: Superposition for bounded domains. In: Bonacina, M.P., Stickel, M. (eds.) McCune Festschrift. LNCS, vol. 7788, pp. 68–100. Springer (2013)

19. Horbach, M., Voigt, M., Weidenbach, C.: On the combination of the bernays-schönfinkel-ramsey fragment with simple linear integer arithmetic. In: de Moura, L. (ed.) Automated Deduction - CADE 26 - 26th International Conference on Automated Deduction, Gothenburg, Sweden, August 6-11, 2017, Proceedings. Lecture Notes in Computer Science, vol. 10395, pp. 77–94. Springer (2017)
20. Horbach, M., Voigt, M., Weidenbach, C.: The universal fragment of presburger arithmetic with unary uninterpreted predicates is undecidable. CoRR **abs/1703.01212** (2017)
21. Komuravelli, A., Gurfinkel, A., Chaki, S.: SMT-based model checking for recursive programs. In: CAV. Lecture Notes in Computer Science, vol. 8559, pp. 17–34. Springer (2014)
22. Korovin, K.: iprover - an instantiation-based theorem prover for first-order logic (system description). In: Armando, A., Baumgartner, P., Dowek, G. (eds.) Automated Reasoning, 4th International Joint Conference, IJCAR 2008, Sydney, Australia, August 12-15, 2008, Proceedings. Lecture Notes in Computer Science, vol. 5195, pp. 292–298. Springer (2008)
23. Lewis, H.R.: Complexity results for classes of quantificational formulas. Journal of Compututer and System Sciences **21**(3), 317–353 (1980)
24. Loos, R., Weispfenning, V.: Applying linear quantifier elimination. The Computer Journal **36**(5), 450–462 (1993)
25. de Moura, L., Bjørner, N.: Z3: An efficient SMT solver. In: Tools and Algorithms for the Construction and Analysis of Systems, LNCS, vol. 4963 (2008)
26. de Moura, L.M., Bjørner, N.: Satisfiability modulo theories: introduction and applications. Communications of the ACM **54**(9), 69–77 (2011)
27. Nieuwenhuis, R., Oliveras, A., Tinelli, C.: Solving sat and sat modulo theories: From an abstract davis–putnam–logemann–loveland procedure to dpll(t). Journal of the ACM **53**, 937–977 (November 2006)
28. Nipkow, T., Paulson, L.C., Wenzel, M.: Isabelle/HOL — A Proof Assistant for Higher-Order Logic, LNCS, vol. 2283. Springer (2002)
29. Nonnengart, A., Weidenbach, C.: Computing small clause normal forms. In: Handbook of Automated Reasoning, pp. 335–367. Elsevier and MIT Press (2001)
30. Plaisted, D.A.: Complete problems in the first-order predicate calculus. Journal of Computer and System Sciences **29**, 8–35 (1984)
31. Ranise, S.: On the verification of security-aware e-services. Journal of Symbolic Compututation **47**(9), 1066–1088 (2012)
32. Reynolds, A., Barbosa, H., Fontaine, P.: Revisiting enumerative instantiation. In: Beyer, D., Huisman, M. (eds.) Tools and Algorithms for the Construction and Analysis of Systems - 24th International Conference, TACAS 2018, Held as Part of the European Joint Conferences on Theory and Practice of Software, ETAPS 2018, Thessaloniki, Greece, April 14-20, 2018, Proceedings, Part II. Lecture Notes in Computer Science, vol. 10806, pp. 112–131. Springer (2018)
33. Riazanov, A., Voronkov, A.: The design and implementation of vampire. AI Communications **15**(2-3), 91–110 (2002)
34. Schulz, S., Cruanes, S., Vukmirović, P.: Faster, higher, stronger: E 2.3. In: Fontaine, P. (ed.) Proc. of the 27th CADE, Natal, Brasil. pp. 495–507. No. 11716 in LNAI, Springer (2019)
35. Sutcliffe, G.: The TPTP problem library and associated infrastructure - from CNF to th0, TPTP v6.4.0. J. Autom. Reason. **59**(4), 483–502 (2017)
36. Weidenbach, C., Dimova, D., Fietzke, A., Suda, M., Wischnewski, P.: Spass version 3.5. In: Schmidt, R.A. (ed.) 22nd International Conference on Automated Deduction (CADE-22). Lecture Notes in Artificial Intelligence, vol. 5663, pp. 140–145. Springer, Montreal, Canada (August 2009)

6 Appendix

6.1 A Basic Soft-Typing Algorithm

The input of the algorithm is a set of constraint clauses N, output of the algorithm is either a finite set S or ∞ for all argument positions of predicates in N. This is implemented by a total function $\mathrm{sft}(P,i)$ that is initialized with the empty set for all predicates and argument positions.

```
SoftTyping(N)
for all predicates P and argument positions i for P
    sft(P,i) := ∅;
for all unit clauses Λ || → P(t_1,...,t_n) ∈ N
    for all argument positions 1 ≤ i ≤ n where sft(P,i) ≠ ∞
        if (t_i = c) or t_i is assigned a constant c in Λ then
            sft(P,i) := sft(P,i) ∪ {c};
        else
            if (t_i) is not finitely bound in Λ then sft(P,i) := ∞;
change := ⊤;
while (change)
    change := ⊥;
    for all positive Horn clauses Λ || Δ → P(t_1,...,t_n) ∈ N
        for all argument positions 1 ≤ i ≤ n where sft(P,i) ≠ ∞
            if [(t_i = c) or t_i is assigned a constant c in Λ and c ∉ sft(P,i)] then
                sft(P,i) := sft(P,i) ∪ {c}, change := ⊤;
            else
                if [t_i is not finitely bound in Λ and
                    all argument positions of t_i in Δ are set ∞] then
                    sft(P,i) := ∞, change := ⊤;
                else
                    if [t_i is finitely bound through argument positions in Δ by sets S_1,...,S_m
                        and ⋂_j S_j ≠ ∅ and (⋂_j S_j) ⊈ sft(P,i)] then
                        sft(P,i) := sft(P,i) ∪ (⋂_j S_j), change := ⊤;
```

A variable term t_i is finitely bound by a constraint Λ, if either t_i is of integer sort and there exists an upper and a lower bound for t_i in Λ, or t_i is of real sort and it is assigned a fixed value in Λ. A variable term t_i is finitely bound in Δ, if t_i occurs at some argument position Q,j in Δ with $\mathrm{sft}(Q,j) \neq \infty$. It may happen that SoftTyping(N) first assigns a finite set to some argument position before it eventually detects the argument position is mapped to ∞.

For each run through the while loop, at least one predicate argument position is set to ∞ or the set it is mapped to is extended by at least one constant. Argument positions set to ∞ are no longer considered. The set of constants in N as well as the number of predicate argument positions in N is finite, hence SoftTyping(N) terminates. It is correct, because in each step it over-approximates the result of a hierarchic unit resulting resolution step, see Section 2.

The above algorithm is highly inefficient. For example, it does not track dependencies between changed predicate argument position values and the occurrence of these predicates in rules. Our implementation resolves such issues and the time needed for SoftTyping(N) is neglectable compared to the afterwards solving time of SPASS-SPL. The formalizations of supervisors for the lane change assistant and the ECU do not contain any potentially infinite recursion for first-order predicates and do not require more than one first-order sort besides the two arithmetic sorts. Our current implementation makes use of both restrictions and will be extended to the general case in near future.

6.2 Proofs and Auxiliary Lemmas

Auxiliary Lemma for the Proof of Lemma 10

Lemma 10. *Let N be a set of* HBS(LA) *clauses. Let Q^f be a predicate of arity one not occurring in N. Let y be a real variable not occurring in N. Let $N' = \{(\Lambda \,\|\, \Delta \rightarrow H) \in N \mid H \neq \bot\} \cup \{(\Lambda \,\|\, \Delta \rightarrow Q^f(y)) \mid (\Lambda \,\|\, \Delta \rightarrow \bot) \in N\}$, i.e., the set of clauses N just that we gave every clause $Q^f(y)$ as head literal that previously had no head literal. Then N is satisfiable if and only if argument position 1 of Q^f is finite in N'.*

Proof. Based on $\mathcal{A}$, we can construct an interpretation $\mathcal{A}'$ that is equivalent to $\mathcal{A}$ except that it interprets Q^f for all arguments as false and satisfies N'. This is straightforward for all clauses $(\Lambda \,\|\, \Delta \rightarrow H) \in N'$ with $H \neq Q^f(y)$ because they also appear in N, but it also holds for the clauses with $H = Q^f(y)$ because $\mathcal{A}$ can only satisfy $(\Lambda \,\|\, \Delta \rightarrow \bot) \in N$ if $\bigwedge A \in (\Lambda \cup \Delta) A\sigma$ is interpreted as false by $\mathcal{A}$. Hence, $(\Lambda \,\|\, \Delta \rightarrow Q^f(y))$ is satisfied by $\mathcal{A}'$, which means the set of derivable facts dfacts(Q^f, N) for $(Q^f, 1)$ is empty and $(Q^f, 1)$ is therefore finite. Symmetrically, Q^f is only finite if there exists at least one satisfiable interpretation for N', where $\bigwedge A \in (\Lambda \cup \Delta) A\sigma$ is interpreted as false for every $(\Lambda \,\|\, \Delta \rightarrow Q^f(y)) \in N'$. The reason is that any interpretation $\mathcal{A}$ that satisfies $\bigwedge A \in (\Lambda \cup \Delta) A\sigma$ can derive all facts $Q^f(a)$ for $a \in \mathbb{R}$ (so infinitely many) from the clause $(\Lambda \,\|\, \Delta \rightarrow Q^f(y)) \in N'$. However, if $\mathcal{A}$ satisfies N' and evaluates every $\bigwedge A \in (\Lambda \cup \Delta) A\sigma$ with $(\Lambda \,\|\, \Delta \rightarrow Q^f(y)) \in N'$ as false, then $\mathcal{A}$ also satisfies N. This is straightforward for all clauses $(\Lambda \,\|\, \Delta \rightarrow H) \in N$ with $H \neq \bot$ because they also appear in N', but it also holds for the clauses with $H = \bot$ because $\mathcal{A}$ evaluates $\bigwedge A \in (\Lambda \cup \Delta) A\sigma$ as false for those clauses. Hence, N is satisfiable. □

Proof of Lemma 6

Proof. Due to Lemma 6, we know that determining the finiteness of a predicate argument position can be as hard as determining the satisfiability of an HBS(LA) clause set. Thanks to [12,20] we know that this is undecidable. □

Converting Interpretations for HBS(SLA)A Problems

Lemma 11. *Every satisfying interpretation $\mathcal{A}$ for N is also a satisfying interpretation for* agnd(N).

Proof. We know that gnd(agnd$(N)) \subseteq$ gnd(N); at least after some canonical simplifications on the theory atoms. Therefore any interpretation that satisfies N (and thus gnd(N)) also satisfies gnd(agnd(N)) and thus agnd(N). □

Lemma 12. *Let $\mathcal{A}$ be an interpretation satisfying the clause set* agnd(N). *Then we can construct a satisfying interpretation $\mathcal{A}'$ for N such that $P^{\mathcal{A}'} = \{\bar{a} \mid P(\bar{a}) \in \text{dfacts}(P, \text{agnd}(N))\}$.*

Proof. Proof by contradiction. Suppose $\mathcal{A}$ is an interpretation that satisfies agnd(N) but not gnd(N). This would mean that there must exists a clause $(\Lambda \,\|\, \Delta \rightarrow H) \in N$ and a grounding σ such that $\mathcal{A}'$ does not satisfy $(\Lambda \,\|\, \Delta \rightarrow H)\sigma$, which would mean $\mathcal{A}'$ satisfies $\Lambda\sigma$ and $\Delta\sigma$, but not $H\sigma$. $\Delta\sigma$ is satisfied by $P^{\mathcal{A}'}$ would imply that all atoms in $\Delta\sigma$ are derivable facts from agnd(N). However, since $\Lambda\sigma$ is satisfied and $\Delta\sigma$ consists of derivable facts from agnd(N), $H\sigma$ should also be a derivable fact from agnd(N). This is a contradiction because this would imply that $H\sigma$ is actually satisfied. □

Auxiliary Lemmas for the Proof of Theorem 8

Lemma 13. *Let* $\triangleleft = \{\leq,<,>,\geq,=,\neq\}$. *Let* $(x \triangleleft c) \in \text{conIneqs}(Q,i,N)$ *and let* a *and* a' *belong to* $I \in \text{iPart}(Q,i,N)$. *Then* $a \triangleleft c$ *evaluates to true if and only if* $a' \triangleleft c$ *evaluates to true.*

Proof. We make a case distinction over the different cases for $\triangleleft$:

- $\triangleleft$ is $\leq$: this means that iEP(Q,i,N) contains the interval borders $c]$ and $(c$. Therefore, I is either a subset of $(-\infty,c]$, i.e., all points in I satisfy $(x \triangleleft c)$ or $I \subseteq (c,\infty]$ so no points in I satisfy $(x \triangleleft c)$.
- $\triangleleft$ is $\geq$: this means that iEP(Q,i,N) contains the interval borders $[c$ and $c)$. Therefore, I is either a subset of $[c,\infty)$, i.e., all points in I satisfy $(x \triangleleft c)$ or $I \subseteq (-\infty,c)$ so no points in I satisfy $(x \triangleleft c)$.
- $\triangleleft$ is $<$: this means that iEP(Q,i,N) contains the interval borders $c)$ and $[c$. Therefore, I is either a subset of $(-\infty,c)$, i.e., all points in I satisfy $(x \triangleleft c)$ or $I \subseteq [c,\infty]$ so no points in I satisfy $(x \triangleleft c)$.
- $\triangleleft$ is $>$: this means that iEP(Q,i,N) contains the interval borders $(c$ and $c]$. Therefore, I is either a subset of (c,∞), i.e., all points in I satisfy $(x \triangleleft c)$ or $I \subseteq (-\infty,c]$ so no points in I satisfy $(x \triangleleft c)$.
- $\triangleleft$ is $=$: this means that iEP(Q,i,N) contains the interval $[c,c]$. Therefore, I is either $[c,c]$ or no point in I satisfies $(x \triangleleft c)$.
- $\triangleleft$ is $\neq$: this means that iEP(Q,i,N) contains the interval $[c,c]$. Therefore, I is either $[c,c]$ and no point in I satisfies $(x \triangleleft c)$ or $I \neq [c,c]$ and all points in I satisfy $(x \triangleleft c)$.

□

Lemma 14. *Let* $Q(\bar{a})$ *be derivable from* N *and let* $a_i \in \mathbb{Z}$ *belong to* $I \in \text{iPart}(Q,i,N)$. *Then* $Q(\bar{a}')$ *is also derivable from* N*, where* $a'_j = a_j$ *for* $i \neq j$ *and* $a'_i \in I \cap \mathbb{Z}$.

Proof. The case where $a'_i = a_i$ is trivial because $\bar{a}' = \bar{a}$. We prove the case for $a'_i \neq a_i$ (and therefore also $I \neq [a_i,a_i]$) by structural induction over the derivations in N.

- The base case is that $Q(\bar{a})$ was only derived using one clause, i.e., N contains a clause $\Lambda \,\|\, \rightarrow Q(\bar{t})$ with a grounding σ such that $Q(\bar{a}) = Q(\bar{t})\sigma$ and $\Lambda\sigma$ evaluates to true. We can assume that $t_i \neq a_i$ because I would be the interval $[a_i,a_i]$ otherwise. This means $t_i = x$ for a variable x. Based on Lemma 13, $\Lambda\sigma'$ (with $x\sigma' = a'_i$ and $y\sigma' = y\sigma$ for all $y \neq x$) must also evaluate to true. Therefore, $Q(\bar{a}')$ is also derivable from N.

- The induction step is that $Q(\bar{a})$ was derived using a clause $\Lambda \,\|\, \Delta \rightarrow Q(\bar{t}) \in N$ with a grounding σ such that $Q(\bar{a}) = Q(\bar{t})\sigma$, $\Lambda\sigma$ evaluates to true, and all $P(\bar{s})\sigma \in \Delta\sigma$ are derivable from N. Moreover, we can assume that $t_i \neq a_i$ because I would be the interval $[a_i,a_i]$ otherwise. Thus, $t_i = x$ for a variable x. This means we can again construct a substitution σ' with $x\sigma' = a'_i$ and $y\sigma' = y\sigma$ for all $y \neq x$. By induction we can assume that $P(\bar{s})\sigma' \in \Delta\sigma'$ is derivable from N because $P(\bar{s})\sigma$ is derivable from N. Due to Lemma 13, $\Lambda\sigma'$ is also satisfiable. Thus $Q(\bar{a'})$ is derivable from N using $(\Lambda \,\|\, \Delta \rightarrow Q(\bar{t}))\sigma'$.

□

Lemma 15. *Let $Q(\bar{a})$ be derivable from N and let $a_i \notin \mathbb{Z}$ belong to $I \in$ iPart(Q,i,N). Then $Q(\bar{a'})$ is also derivable from N, where $a'_j = a_j$ for $i \neq j$ and $a'_i \in I$.*

Proof. The case where $a'_i = a_i$ is trivial because $\bar{a'} = \bar{a}$. We prove the case for $a'_i \neq a_i$ (and therefore also $I \neq [a_i,a_i]$) by structural induction over the derivations in N.

- The base case is that $Q(\bar{a})$ was only derived using one clause, i.e., N contains a clause $\Lambda \,\|\!\rightarrow Q(\bar{t})$ with a grounding σ such that $Q(\bar{a}) = Q(\bar{t})\sigma$ and $\Lambda\sigma$ evaluates to true. We can assume that $t_i \neq a_i$ because I would be the interval $[a_i,a_i]$ otherwise. This means $t_i = x$ for a variable x and sort$(x) = \mathcal{R}$ or we could not have derived a value $a_i \notin \mathbb{Z}$. Based on Lemma 13, $\Lambda\sigma'$ (with $x\sigma' = a'_i$ and $y\sigma' = y\sigma$ for all $y \neq x$) must also evaluate to true. Therefore, $Q(\bar{a'})$ is also derivable from N.
- The induction step is that $Q(\bar{a})$ was derived using a clause $\Lambda \,\|\, \Delta \rightarrow Q(\bar{t}) \in N$ with a grounding σ such that $Q(\bar{a}) = Q(\bar{t})\sigma$, $\Lambda\sigma$ evaluates to true, and all $P(\bar{s})\sigma \in \Delta\sigma$ are derivable from N. Moreover, we can assume that $t_i \neq a_i$ because I would be the interval $[a_i,a_i]$ otherwise. Thus, $t_i = x$ for a variable x and sort$(x) = \mathcal{R}$ or we could not have derived a value $a_i \notin \mathbb{Z}$. This means we can again construct a substitution σ' with $x\sigma' = a'_i$ and $y\sigma' = y\sigma$ for all $y \neq x$. By induction we can assume that $P(\bar{s})\sigma' \in \Delta\sigma'$ is derivable from N because $P(\bar{s})\sigma$ is derivable from N. Due to Lemma 13, $\Lambda\sigma'$ is also satisfiable. Thus $Q(\bar{a'})$ is derivable from N using $(\Lambda \,\|\, \Delta \rightarrow Q(\bar{t}))\sigma'$.

□

Lemma 16. *Let $\Lambda \,\|\, \Delta \rightarrow H$ be a clause in N. Let σ be a well-typed grounding over the most general test-point* tp-function *β^* such that $\Lambda\sigma$ evaluates to true and all atoms in $\Delta\sigma$ are derivable from N. Then there exists a grounding σ' that is a* well-typed instance *over the* tp-function *β, i.e., $\sigma \in$ wtis$_\beta(\Lambda \,\|\, \Delta \rightarrow H)$, and from which we can extrapolate the interpretation for $(\Lambda \,\|\, \Delta \rightarrow H)\sigma$, i.e., $\bar{t}\sigma = \eta(P,\bar{t}\sigma')$ for all $P(\bar{t}) \in$ atoms$(\Delta \rightarrow H)$.*

Proof. Before we start with the actual proof, let us repeat and clarify the definition of our extrapolation function and the definition of a well-typed instance over β. The extrapolation $\eta(P,\bar{t}\sigma') = I'_{(P,1)} \times \ldots \times I'_{(P,n)}$ of a test-point vector $\bar{t}\sigma'$ is the cross product of the sets $I'_{(P,i)}$. One for each predicate argument position (P,i). If (P,i) is finite, then $I'_{(P,i)} = t_i\sigma'$. If (P,i) is infinite and $t_i\sigma'$ an integer value, then $I'_{(P,i)} =$ iPart$(P,i,N) \cap \mathbb{Z}$. If (P,i) is infinite and $t_i\sigma'$ a non-integer value, then $I'_{(P,i)} =$ iPart$(P,i,N) \setminus \mathbb{Z}$. A substitution σ' for a clause Y is a well-typed instance over β if it guarantees for each variable x that $x\sigma'$ is part of every test-point set (i.e., $x\sigma' \in \beta(P,i)$) of every argument position (P,i) it occurs in (i.e., $(P,i) \in$ depend(x,Y)) and that $x\sigma' \in$ sort$(x)^{\mathcal{A}}$. This means our proof only needs to show that any two argument positions (P,i) and (Q,j) in Y that share the same variable x, share a test point $b\in \text{sort}(x)^{\mathcal{A}}$ such that $x\sigma$ can be extrapolated from b, i.e., for $b=x\sigma'$: $b\in\beta(P,i)$, $b\in\beta(Q,j)$, $b\in\text{sort}(x)^{\mathcal{A}}$, and $x\sigma\in I'_{(P,i)}$ as well as $x\sigma\in I'_{(Q,j)}$.

First of all, $(x\sigma)\in\text{sort}(x)^{\mathcal{A}}$, $(x\sigma)\in\text{sort}(P,i)^{\mathcal{A}}$, and $(x\sigma)\in\text{sort}(Q,j)^{\mathcal{A}}$ because σ is well-typed over β^* and N is well-typed. Second of all, $H\sigma$ is derivable because the atoms in $\Delta\sigma$ are derivable from N and $\Lambda\sigma$ evaluates to true. Hence, $x\sigma$ must be a derivable value for both (P,i) and (Q,j). This means our condition is trivial to satisfy if (P,i) is finite and (Q,j) is finite because $\text{dvals}(P,i,N)\subseteq\beta(P,i)$ and $\text{dvals}(Q,j,N)\subseteq\beta(Q,j)$. So we can simply choose $b=(x\sigma)$ to satisfy our conditions. The case where (P,i) is finite and (Q,j) is infinite works similarly. Here we additionally need that $[x\sigma,x\sigma]\in\text{iPart}(Q,i,N)$ because $\text{conArgs}(P,i,N)=\text{conArgs}(Q,j,N)$ and thus $(x\sigma)\in\beta(Q,j)$. As a result, we can choose $b=(x\sigma)$ again to satisfy our conditions. The reverse case, where (P,i) is infinite and (Q,j) is finite, works symmetrically. In the case where (P,i) and (Q,j) are both infinite, we know that $\text{conArgs}(P,i,N) = \text{conArgs}(Q,j,N)$ because they share a variable in this clause and therefore $\text{tps}(P,i,N) = \text{tps}(Q,j,N)$. Since we know that $(x\sigma)\in\text{sort}(P,i)^{\mathcal{A}}$ and $(x\sigma)\in\text{sort}(Q,j)^{\mathcal{A}}$, we know that $\beta(P,i,N)\cap\beta(Q,j,N)$ contains a (non-)integer value b for the interval $I\in\text{iPart}(P,i,N)=\text{iPart}(Q,j,N)$ if $x\sigma\in I$ is a (non-)integer value. Hence, we can choose $b=x\sigma'$ and satisfy our conditions. □

Lemma 17. *Let $\bar{a}$ be a test-point vector for Q over β, i.e., with $a_i\in\beta(Q,i)$ for all i. Then $Q(\bar{a})$ is derivable from* $\text{gnd}(N)$ *if and only if $Q(\bar{a})$ is derivable from* $\text{gnd}_\beta(N)$.

Proof. The first direction, $Q(\bar{a})$ is derivable from $\text{gnd}(N)$ if $Q(\bar{a})$ is derivable from $\text{gnd}_\beta(N)$, is straightforward because $\text{gnd}_\beta(N)\subseteq\text{gnd}(N)$. So any derivation step in $\text{gnd}_\beta(N)$ can also be performed in $\text{gnd}(N)$. The second direction follows by structural induction:
The base case is that $Q(\bar{a})$ was only derived using one clause, i.e., N contains a clause $\Lambda\,\|\rightarrow Q(\bar{t})$ with a well-typed grounding σ over the most general tp-function β^* such that $Q(\bar{a})=Q(\bar{t})\sigma$ and $\Lambda\sigma$ evaluates to true. However, $(\Lambda\,\|\rightarrow Q(\bar{t}))\sigma$ is part of $\text{gnd}_\beta(N)$. Therefore, $Q(\bar{a})$ is also derivable from $\text{gnd}_\beta(N)$.
The induction step is that $Q(\bar{a})$ was derived using a clause $\Lambda\,\|\,\Delta\rightarrow Q(\bar{t})\in N$ with a well-typed grounding σ over the most general tp-function β^* such that $Q(\bar{a})=Q(\bar{t})\sigma$, $\Lambda\sigma$ evaluates to true, and all $P(\bar{s})\sigma\in\Delta\sigma$ are derivable from N. Since all $P(\bar{s})\sigma\in\Delta\sigma$ are derivable and $\Lambda\sigma$ evaluates to true, we can use Lemma 16 to construct a grounding σ' that is well-typed over β and such that $\bar{s}\sigma=\eta(P,\bar{s}\sigma')$ for all $P(\bar{s})\sigma\in\Delta\sigma$. By Lemmas 14 and 15, we can assume that $P(\bar{s})\sigma'$ is derivable from N because $P(\bar{s})\sigma$ is derivable from N. Following that we can assume by induction that $P(\bar{s})\sigma'\in\Delta\sigma'$ is derivable from $\text{gnd}_\beta(N)$ because $P(\bar{s})\sigma'$ is derivable from N. Due to Lemma 13, $\Lambda\sigma'$ is also satisfiable. Thus $Q(\bar{a})=Q(\bar{t})\sigma'=Q(\bar{t})\sigma$ is derivable from $\text{gnd}_\beta(N)$ using $(\Lambda\,\|\,\Delta\rightarrow Q(\bar{t}))\sigma'$. □

Lemma 18. *The* tp-function *β covers N, i.e.,* $\text{gnd}_\beta(N)$ *is equisatisfiable to N.*

Proof. If N is satisfiable, then $\text{gnd}(N)$ is satisfiable. Hence $\text{gnd}_\beta(N)$ is also satisfiable because $\text{gnd}_\beta(N)\subseteq\text{gnd}(N)$. For the reverse direction we assume that $\text{gnd}_\beta(N)$ is satisfiable. Then we show that we can extrapolate a new interpretation $\mathcal{A}$ from the derivable facts of $\text{gnd}_\beta(N)$ so it satisfies $\text{gnd}(N)$ and thus N. The extrapolation is defined as follows: $P^{\mathcal{A}} = \{\bar{b}\mid\bar{a}\in \text{dfacts}(P,\text{gnd}_\beta(N))$ and $\bar{b}\in\eta(P,\bar{a})\}$. The interpretation $\mathcal{A}$ satisfies every clause $(\Lambda\,\|\,\Delta\rightarrow H)\in \text{gnd}(N)$, i.e., every well-typed grounding $(\Lambda\,\|\,\Delta\rightarrow H)\sigma$ of every clause $(\Lambda\,\|\,\Delta\rightarrow H)\in N$ over the most general tp-function β^*, due to one of three reasons: (i) $\Lambda\sigma$ evaluates to false. (ii) An atom A from $\Delta\sigma$ is not derivable from N and since $\text{gnd}_\beta(N)$ is a subset of $\text{gnd}(N)$ the atom A is also not derivable from $\text{gnd}_\beta(N)$. By definition of $\mathcal{A}$ this means $\Delta\sigma$ is interpreted as false and the clause is thus satisfied. (iii) We can assume that $\Lambda\sigma$ evaluates to true and that all atoms A from $\Delta\sigma$ are derivable from N. This means we can use Lemma 16 to construct a grounding σ' that is well-typed over β and such that $\bar{s}\sigma = \eta(P, \bar{s}\sigma')$ for all $P(\bar{s})\sigma \in \text{atoms}((\Delta \to H)\sigma)$. Due to Lemma 13, this means $\Lambda\sigma'$ evaluates to true. Together with Lemmas 14 and 15 this implies that all atoms in $\Delta\sigma'$ and $H\sigma'$ are derivable from $\text{gnd}_\beta(N)$. Hence, $\mathcal{A}$ satisfies $H\sigma = P(\bar{s})\sigma$ and the full clause because $\bar{s}\sigma = \eta(P, \bar{s}\sigma')$ and $H\sigma'$ is derivable from $\text{gnd}_\beta(N)$. □

Lemma 19. *The* tp-function *β covers an existential conjecture $N \models \exists \bar{x}.Q(\bar{x})$, i.e.,* $\text{gnd}_\beta(N) \cup \{\text{gnd}_\beta(\| Q(\bar{x}) \to \bot)\}$ *is satisfiable if and only if $N \models \exists \bar{x}.Q(\bar{x})$ is false.*

Proof. $N \models \exists \bar{x}.Q(\bar{x})$ if $N \cup \{Q(\bar{x}) \to \bot\}$ is unsatisfiable. Hence, Lemma 18 shows that β covers the existential conjecture. □

Lemma 20. *The* tp-function *β covers a universal conjecture $N \models \forall \bar{x}.Q(\bar{x})$, i.e.,* $\text{gnd}_\beta(N) \cup N_C$ *is satisfiable if and only if $N \models \forall \bar{x}.Q(\bar{x})$ is false. Here N_C is the set* $\{\| \text{gnd}_\beta(Q(\bar{x})) \to \bot\}$ *if η is complete for Q or the empty set otherwise.*

Proof. We split the proof into four parts:

1. Assume $\text{gnd}_\beta(N) \cup N_C$ is satisfiable and η is complete for Q. This means $\text{gnd}_\beta(N)$ alone is also satisfiable and by Lemma 18 we know that N is, too. Since N_C is also satisfiable, there must exist an instance $Q(\bar{a}) \in \text{gnd}_\beta(Q(\bar{x}))$ that is not derivable from $\text{gnd}_\beta(N)$. By Lemma 17, we know this means that $Q(\bar{a})$ is also not derivable for N. Hence $N \models \forall \bar{x}.Q(\bar{x})$ is false.
2. Assume $\text{gnd}_\beta(N) \cup N_C$ is satisfiable and η does not cover Q. This means that our over-approximation detected that we cannot derive all instances for Q. The only thing left to show is that $\text{gnd}_\beta(N)$ is satisfiable implies that N is satisfiable. This follows from Lemma 18.
3. Assume $\text{gnd}_\beta(N)$ is unsatisfiable. Then due to Lemma 18, N is also unsatisfiable and hence the universal conjecture holds.
4. Assume $\text{gnd}_\beta(N)$ is satisfiable, but $\text{gnd}_\beta(N) \cup N_C$ is not. First of all, this means η is complete for Q and N is satisfiable (Lemma 18). Moreover, it means that all facts in $\text{gnd}_\beta(Q(\bar{x}))$ are derivable from $\text{gnd}_\beta(N)$. Since η is complete for Q and all instances of Q over our test-points are derivable, Lemmas 14 and 15 imply that all groundings of Q (i.e., all facts in $\text{gnd}(Q(\bar{x}))$) are derivable from N. Hence, the universal conjecture holds.

□

Proof of Theorem 8

Proof. See Lemmas 18, 19, and 20. □

Auxiliary Lemmas for the Proof of Lemma 9

Lemma 21. *Let Q be a predicate in N. Let β be a finite and covering* tp-function *for N. Let* $N_H := \text{tren}_N(N) \cup \text{tfacts}(N,\beta) \cup \text{sfacts}(N,\beta)$ *be the hammered version of N. Then any fact $Q(\bar{a})$ derivable from N_H is also derivable from* $\text{gnd}_\beta(N)$ *and vice versa.*

Proof. First, we prove that $Q(\bar{a})$ is derivable from N_H if $Q(\bar{a})$ is derivable from $\text{gnd}_\beta(N)$. We prove this by structural induction over the derivations in $\text{gnd}_\beta(N)$.

- The base case is that $Q(\bar{a})$ was only derived using one clause, i.e., N contains a clause $\Lambda \,\|\!\rightarrow Q(\bar{t})$ that has a well-typed grounding σ over β such that $Q(\bar{a}) = (Q(\bar{t})\sigma)$ and $\Lambda\sigma$ evaluates to true. However, this also means that $\text{tren}_N(N)$ contains a clause $\Delta_T, \Delta_S \rightarrow Q(\bar{t})$. Δ_T are all abstracted theory literals and all their groundings $\Delta_T\sigma$ appear as facts in tfacts(N,β) since $\Lambda\sigma$ evaluates to true. Δ_S are all sort literals $Q_{(Q,i,S)}(x)$ such that $t_i = x$ and sfacts(N,β) contains $Q_{(Q,i,S)}(x\sigma)$ because it must hold that $x\sigma \in \beta(Q,i) \cap S^{\mathcal{A}}$ or σ would not be well-typed over β. Hence, all $A \in (\Delta_T\sigma \cup \Delta_S\sigma)$ are derivable from N_H and therefore $Q(\bar{a})$ is derivable via $(\Delta_T, \Delta_S \rightarrow Q(\bar{t}))\sigma$ from N_H.
- The induction step is that $Q(\bar{a})$ was derived using a clause $(\Lambda \,\|\, \Delta \rightarrow Q(\bar{t})) \in N$ with a well-typed grounding σ over β such that $Q(\bar{a}) = Q(\bar{t})\sigma$, $\Lambda\sigma$ evaluates to true, and all $P(\bar{s})\sigma \in \Delta\sigma$ are derivable from $\text{gnd}_\beta(N)$ and N_H. This also means that $\text{tren}_N(N)$ contains a clause $\Delta_T, \Delta_S, \Delta \rightarrow Q(\bar{t})$. Δ_T are all abstracted theory literals and all their groundings $\Delta_T\sigma$ appear as facts in tfacts(N,β) since $\Lambda\sigma$ evaluates to true. Δ_S are all sort literals $Q_{(Q,i,S)}(x)$ such that $t_i = x$ and sfacts(N,β) contains $Q_{(Q,i,S)}(x\sigma)$ because it must hold that $x\sigma \in \beta(Q,i) \cap S^{\mathcal{A}}$ or σ would not be well-typed over β. Hence, all $A \in (\Delta_T\sigma \cup \Delta_S\sigma \cup \Delta\sigma)$ are derivable from N_H and therefore $Q(\bar{a})$ is derivable via $(\Delta_T, \Delta_S, \Delta \rightarrow Q(\bar{t}))\sigma$ from N_H.

Second, we prove that $Q(\bar{a})$ is derivable from $\text{gnd}_\beta(N)$ if $Q(\bar{a})$ is derivable from N_H. We prove this again by structural induction over the derivations in N_H.

- The base case is that $Q(\bar{a})$ was only derived using one clause in $\text{tren}_N(N)$, i.e., $\text{tren}_N(N)$ contains a clause $\Delta_T, \Delta_S \rightarrow Q(\bar{t})$, there exists a grounding σ such that $Q(\bar{a}) = (Q(\bar{t})\sigma)$ and such that $\Delta_T\sigma \subseteq$ tfacts(N,β) and $\Delta_S\sigma \subseteq$ sfacts(N,β). However, this also means that N contains a clause $\Lambda \,\|\!\rightarrow Q(\bar{t})$ such that $(\Delta_T, \Delta_S \rightarrow Q(\bar{t})) = \text{tren}_N(\Lambda \,\|\!\rightarrow Q(\bar{t}))$. Therefore, $\Delta_T\sigma \subseteq$ tfacts(N,β) implies that $\Lambda\sigma$ evaluates to true and that σ is well-typed over β for the variables $x \in \text{vars}(\Lambda)$. All other variables $x \in \text{vars}(Q(\bar{t})) \setminus \text{vars}(\Lambda)$ (with $t_i = x$) were added by tren_N through sort literals $Q_{(Q,i,S)}(x)$ to Δ_S and $\Delta_S\sigma \subseteq$ sfacts(N,β) ensures that σ is also well-typed over β for those variables. Hence, σ is a well-typed grounding over β for $\Lambda \,\|\!\rightarrow Q(\bar{t})$ and $\Lambda\sigma$ evaluates to true. Thus, $Q(\bar{a})$ is derivable via $(\Lambda \,\|\!\rightarrow Q(\bar{t}))\sigma$ from $\text{gnd}_\beta(N)$.
- The induction step is that $Q(\bar{a})$ was derived using a clause $(\Delta_T, \Delta_S, \Delta \rightarrow Q(\bar{t})) \in \text{tren}_N(N)$, all $P(\bar{s})\sigma \in \Delta\sigma$ are derivable from $\text{gnd}_\beta(N)$ and N_H, and there exists a grounding σ such that $Q(\bar{a}) = (Q(\bar{t})\sigma)$ and such that $\Delta_T\sigma \subseteq$ tfacts(N,β) and $\Delta_S\sigma \subseteq$ sfacts(N,β). This also means that N contains a clause $\Lambda \,\|\, \Delta \rightarrow Q(\bar{t})$ such that $(\Delta_T, \Delta_S, \Delta \rightarrow Q(\bar{t})) = \text{tren}_N(\Lambda \,\|\, \Delta \rightarrow Q(\bar{t}))$. Therefore, $\Delta_T\sigma \subseteq$ tfacts(N,β) implies that $\Lambda\sigma$ evaluates to true and that σ is well-typed over β for the variables $x \in \text{vars}(\Lambda)$. The grounding σ is also well-typed over β for all variables $x \in \text{vars}(Q(\bar{t})) \setminus \text{vars}(\Lambda)$ with $\text{sort}(x) = \mathcal{R}$ that appear in at least one literal $P(\bar{s}) \in \Delta$ with $s_j = x$ or otherwise the groundings $R(\bar{s'})\sigma$ of all literals $R(\bar{s'})$ containing x would not be derivable from $\text{gnd}_\beta(N)$. The grounding σ is also well-typed over β for all variables $x \in \text{vars}(Q(\bar{t})) \setminus \text{vars}(\Lambda)$ with $\text{sort}(x) = \mathcal{Z}$ that appear in a literal $P(\bar{s}) \in \Delta$ with $s_j = x$ and $\text{sort}(P, j) = \mathcal{Z}$ or otherwise the groundings $R(\bar{s'})\sigma$ of all literals $R(\bar{s'})$ containing x would not be derivable from $\text{gnd}_\beta(N)$. All other variables $x \in \text{vars}(Q(\bar{t})) \setminus \text{vars}(\Lambda)$ (with $t_i = x$) were added by tren_N through sort literals $Q_{(Q,i,S)}(x)$ to Δ_S and $\Delta_S\sigma \subseteq$ sfacts(N,β) ensures that σ is also well-typed over β for those variables. Hence, σ is a well-typed grounding over β for $\Lambda \,\|\, \Delta \rightarrow Q(\bar{t})$, $\Lambda\sigma$ evaluates to true, and all atoms in $\Delta\sigma$ are derivable from $\text{gnd}_\beta(N)$. Thus, $Q(\bar{a})$ is derivable via $(\Lambda \,\|\, \Delta \rightarrow Q(\bar{t}))\sigma$ from $\text{gnd}_\beta(N)$.

□

Lemma 22. *N is equisatisfiable to its hammered version* $\text{tren}_N(N) \cup \text{tfacts}(N,\beta) \cup \text{sfacts}(N,\beta)$.

Proof. Let $N_H := \text{tren}_N(N) \cup \text{tfacts}(N,\beta) \cup \text{sfacts}(N,\beta)$. We split the proof into two parts:

1. Assume $\text{gnd}_\beta(N)$ is satisfiable. Then the interpretation $\mathcal{A}$ defined by the following rules satisfies N_H: $P^\mathcal{A} := \{\bar{a} \mid P(\bar{a}) \in \text{dfacts}(P,\text{gnd}_\beta(N))\}$ if P is a predicate that appears in N, $P^\mathcal{A} := \{\bar{a} \mid P(\bar{a}) \in \text{tfacts}(N,\beta)\}$ if P is a predicate that appears in $\text{tfacts}(N,\beta)$, and $P^\mathcal{A} := \{\bar{a} \mid P(\bar{a}) \in \text{sfacts}(N,\beta)\}$ if P is a predicate that appears in $\text{sfacts}(N,\beta)$. We prove this by contradiction: Suppose $\mathcal{A}$ is an interpretation that satisfies $\text{gnd}_\beta(N)$ but not N_H. Naturally, $\mathcal{A}$ satisfies any of the facts in $\text{tfacts}(N,\beta)$ and in $\text{sfacts}(N,\beta)$. This means that there must exist a clause $(\Lambda \parallel \Delta \rightarrow H) \in N$, a clause $(\Delta_T,\Delta_S,\Delta \rightarrow H) \in \text{tren}_N(N)$ with $(\Delta_T,\Delta_S,\Delta \rightarrow H) = \text{tren}_N(\Lambda \parallel \Delta \rightarrow H)$ and a grounding σ such that $\mathcal{A}$ does not satisfy $(\Delta_T,\Delta_S,\Delta \rightarrow H)\sigma$. Formally, $\mathcal{A}$ does not satisfy $(\Delta_T,\Delta_S,\Delta \rightarrow H)\sigma$ means $\mathcal{A}$ satisfies $\Delta_T\sigma$, $\mathcal{A}$ satisfies $\Delta_S\sigma$, $\mathcal{A}$ satisfies $\Delta\sigma$, but $\mathcal{A}$ does not satisfy $H\sigma$. Since $\mathcal{A}$ satisfies $\Delta_T\sigma$, we know by definition of $\mathcal{A}$ and $\text{tfacts}(N,\beta)$ that all atoms in $\Delta_T\sigma$ must be derivable from $\text{tfacts}(N,\beta)$. Since $\mathcal{A}$ satisfies $\Delta_S\sigma$, we know by definition of $\mathcal{A}$ and $\text{sfacts}(N,\beta)$ that all atoms in $\Delta_S\sigma$ must be derivable from $\text{sfacts}(N,\beta)$. Since $\mathcal{A}$ satisfies $\Delta\sigma$, we know by definition of $\mathcal{A}$ that all facts $\Delta\sigma$ can be derived from $\text{gnd}_\beta(N)$. By Lemma 21, this means that all facts $\Delta\sigma$ can be derived from N_H, too. Thus, H must be derivable from N_H and, by Lemma 21, H must be derivable by $\text{gnd}_\beta(N)$. Hence, H would need to be interpreted as true by $\mathcal{A}$, which is the contradiction we were looking for. Thus, $\mathcal{A}$ satisfies N_H.
2. Assume N_H is satisfiable. Then the interpretation $\mathcal{A}$ defined by the following rules satisfies $\text{gnd}_\beta(N)$: $P^\mathcal{A} := \{\bar{a} \mid P(\bar{a}) \in \text{dfacts}(P,N_H)\}$ if P is a predicate that appears in N, $P^\mathcal{A} := \{\bar{a} \mid P(\bar{a}) \in \text{tfacts}(N,\beta)\}$ if P is a predicate that appears in $\text{tfacts}(N,\beta)$, and $P^\mathcal{A} := \{\bar{a} \mid P(\bar{a}) \in \text{sfacts}(N,\beta)\}$ if P is a predicate that appears in $\text{sfacts}(N,\beta)$. We prove this by contradiction: Suppose $\mathcal{A}$ is an interpretation that satisfies N_H but not $\text{gnd}_\beta(N)$. This means that there must exist a clause $(\Lambda \parallel \Delta \rightarrow H) \in N$, a clause $(\Delta_T,\Delta_S,\Delta \rightarrow H) \in \text{tren}_N(N)$ with $(\Delta_T,\Delta_S,\Delta \rightarrow H) = \text{tren}_N(\Lambda \parallel \Delta \rightarrow H)$ and a well-typed grounding σ over β such that $\mathcal{A}$ does not satisfy $(\Lambda \parallel \Delta \rightarrow H)\sigma$. Formally, $\mathcal{A}$ does not satisfy $(\Lambda \parallel \Delta \rightarrow H)\sigma$ means $\Lambda\sigma$ evaluates to true, $\mathcal{A}$ satisfies $\Delta\sigma$, but not $H\sigma$. Since $\mathcal{A}$ satisfies $\Delta\sigma$, we know by definition of $\mathcal{A}$ that all facts $\Delta\sigma$ can be derived from N_H. By Lemma 21, this means that all facts $\Delta\sigma$ can be derived from $\text{gnd}_\beta(N)$, too. Thus, H must be derivable from $\text{gnd}_\beta(N)$ and, by Lemma 21, H must be derivable by N_H. Hence, H would need to be interpreted as true by $\mathcal{A}$, which is the contradiction we were looking for. Thus, $\mathcal{A}$ satisfies N_H.

□

Lemma 23. *The conjecture* $N \models \exists \bar{y}.Q(\bar{y})$ *is false iff* $N_D = \text{tren}'_N(N') \cup \text{tfacts}(N',\beta) \cup \text{sfacts}(N',\beta)$ *is satisfiable with* $N' = N \cup \{Q(\bar{y}) \rightarrow \bot\}$.

Proof. $N \models \exists \bar{x}.Q(\bar{x})$ if $N \cup \{Q(\bar{x}) \rightarrow \bot\}$ is unsatisfiable. Hence, Lemma 22 shows that $N \models \exists \bar{y}.Q(\bar{y})$ is false iff $N_D = \text{tren}'_N(N') \cup \text{tfacts}(N',\beta) \cup \text{sfacts}(N',\beta)$ is satisfiable. □

Lemma 24. *The conjecture* $N \models \forall \bar{y}.Q(\bar{y})$ *is false iff* $N_D = \text{tren}_N(N) \cup \text{tfacts}(N,\beta) \cup \text{sfacts}(N,\beta) \cup N_C$ *is satisfiable.*

Proof. Let $N_H := \text{tren}_N(N) \cup \text{tfacts}(N,\beta) \cup \text{sfacts}(N,\beta)$. We will prove that $\psi = \text{gnd}_\beta(N) \cup N_C$ is equisatisfiable to $N_H \cup N_C$. Then we get from Theorem 8 that $N \models \forall \bar{y}.Q(\bar{y})$ is false if and only if the hammered version $N_H \cup N_C$ is satisfiable. (The case for N without conjecture follows from Lemma 22.)
We split the proof into four parts:

1. Assume $N_H \cup N_C$ is satisfiable and η does not cover Q. This means that our over-approximation detected that we cannot derive all instances for Q. The only thing left to show is that N_H is satisfiable implies that $\text{gnd}_\beta(N)$ is satisfiable. This follows from Lemma 22.
2. Assume $N_H \cup N_C$ is satisfiable and η is complete for Q. This means N_H alone is also satisfiable and by Lemma 22 this means that $\text{gnd}_\beta(N)$ is, too. Since N_C is also satisfiable, there must exist an instance $Q(\bar{a}) \in \text{gnd}_\beta(Q(\bar{x}))$ that is not derivable from N_H. By Lemma 21, we know this means that $Q(\bar{a})$ is also not derivable for $\text{gnd}_\beta(N)$.
3. Assume N_H is unsatisfiable. Then due to Lemma 22, $\text{gnd}_\beta(N)$ is also unsatisfiable and hence $N_H \cup N_C$ and $\text{gnd}_\beta(N) \cup N_C$ are both unsatisfiable.
4. Assume N_H is satisfiable, but $N_H \cup N_C$ is not. This means η is complete for Q and by Lemma 22 this means that $\text{gnd}_\beta(N)$ is satisfiable, too. Moreover, it means that all facts in $\text{gnd}_\beta(Q(\bar{x}))$ are derivable from N_H. By Lemma 21, this implies that all facts in $\text{gnd}_\beta(Q(\bar{x}))$ are also derivable from $\text{gnd}_\beta(N)$. Hence, $\text{gnd}_\beta(N) \cup N_C$ is also not satisfiable.

□

Proof of Lemma 9

Proof. See Lemmas 22, 23, and 24. □