A Verified Prover Based on Ordered Resolution
Anders Schlichtkrull, Jasmin Christian Blanchette, Dmitriy Traytel

To cite this version:
Anders Schlichtkrull, Jasmin Christian Blanchette, Dmitriy Traytel. A Verified Prover Based on Ordered Resolution. CPP 2019 - The 8th ACM SIGPLAN International Conference on Certified Programs and Proofs, Jan 2019, Cascais, Portugal. 10.1145/3293880.3294100. hal-01937141

HAL Id: hal-01937141
https://hal.archives-ouvertes.fr/hal-01937141
Submitted on 27 Nov 2018

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L’archive ouverte pluridisciplinaire HAL, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d’enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.
A Verified Prover Based on Ordered Resolution

Anders Schlichtkrull
DTU Compute
Technical University of Denmark
Kongens Lyngby, Denmark
andschl@dtu.dk

Jasmin Christian Blanchette
Department of Computer Science
Vrije Universiteit Amsterdam
Amsterdam, the Netherlands
j.c.blanchette@vu.nl

Dmitriy Traytel
Department of Computer Science
ETH Zürich
Zürich, Switzerland
traytel@inf.ethz.ch

Abstract

The superposition calculus, which underlies first-order theorem provers such as E, SPASS, and Vampire, combines ordered resolution and equality reasoning. As a step towards verifying modern provers, we specify, using Isabelle/HOL, a purely functional first-order ordered resolution prover and establish its soundness and refutational completeness. Methodologically, we apply stepwise refinement to obtain, from an abstract nondeterministic specification, a verified deterministic program, written in a subset of Isabelle/HOL from which we extract purely functional Standard ML code that constitutes a semidecision procedure for first-order logic.

CCS Concepts

• Theory of computation → Logic and verification; Automated reasoning;

Keywords

automatic theorem provers, proof assistants, first-order logic, stepwise refinement

ACM Reference Format:


1 Introduction

Automatic theorem provers based on superposition, such as E [42], SPASS [33], and Vampire [21], are often employed as backends in proof assistants and program verification tools [7, 20, 32]. Superposition is a highly successful calculus for first-order logic with equality, which generalizes both ordered resolution [2] and ordered completion [1].

Resolution operates on sets of clauses. A clause is an n-ary disjunction of literals \( L_1 \lor \cdots \lor L_n \) whose variables are interpreted universally. Each literal is either an atom \( A \) or its negation \( \neg A \). An atom is a symbol applied to a tuple of terms—e.g., \( \text{prime}(n) \). The empty clause is denoted by \( \bot \).

Resolution works by refutation: Conceptually, the calculus proves a conjecture \( \forall x. C \) from a set of axioms \( D \) by deriving \( \bot \) from \( D \cup C \), indicating its unsatisfiability. As an optimization, it uses a redundancy criterion to discard tautologies, subsumed clauses, and other unnecessary clauses; for example, \( p(x) \lor q(x) \) and \( p(5) \) are both subsumed by \( p(x) \). Compared with plain resolution, \emph{ordered resolution} relies on an order on the atoms to further prune the search space.

Modern superposition provers are highly optimized programs that rely on sophisticated calculi, with a rich metatheory. In this paper, we propose to verify, using Isabelle/HOL [30], a purely functional prover based on ordered resolution. Although our primary interest is in metatheory per se, there are of course applications for verified provers [50].

The verification relies on stepwise refinement [55]. Four layers are connected by three refinement steps.

Our starting point, layer 1 (Section 3), is an abstract Prolog-style nondeterministic resolution prover in a highly general form, as presented by Bachmair and Ganzinger [2] and as formalized in our earlier work [39, 40]. It operates on possibly infinite sets of clauses. Its soundness and refutational completeness are inherited by the other layers.

Layer 2 (Section 4) operates on finite multisets of clauses and introduces a priority queue to ensure that inferences are performed in a fair manner, guaranteeing completeness. Given a valid conjecture, the prover will eventually derive \( \bot \).

Layer 3 (Section 5) is a deterministic program that works on finite lists, committing to a strategy for assigning priorities to clauses. However, it is not fully executable: It abstracts over operations on atoms and employs logical specifications instead of executable functions for auxiliary notions.

Finally, layer 4 (Section 6) is a fully executable program. It provides a concrete datatype for atoms and executable definitions for all auxiliary notions, including unifiers, clause subsumption, and the order on atoms.

From layer 4, we can extract Standard ML code by invoking Isabelle’s code generator [11]. The resulting prover constitutes a proof of concept: It uses an efficient calculus (layer 1) and a reasonable strategy to ensure fairness (layers 2 and 3), but depends on inefficient list-based data structures. Further refinement steps will be required to obtain a prover that is competitive with the state of the art.
The refinement steps connect vastly different levels of abstraction. The most abstract level is occupied by an infinitary logical calculus and the semantics of first-order logic. Soundness and completeness relate these two notions. At the functional programming level, soundness amounts to a safety property: Whenever the program terminates normally, its outcome is correct, whether it is a proof or a finite saturation witnessing unprovability. Correspondingly, refutational completeness is a liveness property: If the conjecture is valid, the program will always terminate normally. We find that, far from being academic exercises, Bachmair and Ganzinger’s framework [2] and its formalization [39, 40] adequately capture the metatheory of actual provers.

To our knowledge, our program is the first verified prover for first-order logic implementing an optimized calculus. It is also the first example of the application of refinement in a first-order context. This methodology has been used to verify SAT solvers [6, 29], which decide the satisfiability of propositional formulas, but first-order logic is semidecidable—sound and complete provers are guaranteed to terminate only for unsatisfiable (i.e., provable) clause sets. This complicates the transfer of completeness results across refinement layers.

The present work is part of the IsaFoL (Isabelle Formalization of Logic) project, which aims at developing a library of results about logic and automated reasoning [3]. The IsaFoL files are available in the Archive of Formal Proofs [38, 39] and in the IsaFoL repository. The parts specific to the functional prover refinement amount to about 4000 lines of source text. A convenient way to study the files is to open them in Isabelle/jEdit [54], as explained in the repository’s readme file. The files were created using Isabelle version 2018, but the repositories will be updated to follow Isabelle’s evolution.

2 Atoms and Substitutions

The first three refinement layers are based on an abstract library of first-order atoms and substitutions. In the fourth and final layer, the abstract framework is instantiated with concrete datatypes and functions.

We start from IsaFoL’s library of clausal logic [6], which is parameterized by a type ‘a of logical atoms. Literals $L$ are defined as an inductive datatype: ‘a literal = Pos ‘a | Neg ‘a. The type of clauses $C, D, E$ is introduced as the alias ‘a clause = ‘a literal multiset, where multiset is the type constructor of finite multisets. Thus, the clause $\neg A \vee B$, where $A$ and $B$ are arbitrary atoms, is represented by the multiset {Neg $A$, Pos $B$}, and the empty clause $\bot$ is represented by the empty multiset $\emptyset$. The complement operation is defined as $\neg$ (Neg $A$ = Pos $A$ and $\neg$ Pos $A$ = Neg $A$ for any atom $A$).

In automated reasoning, it is customary to view clauses as multisets of literals rather than as sets. One reason is that multisets behave more naturally under substitution. For example, applying $\{y \mapsto x\}$ to the two-literal clause $p(x) \lor p(y)$ results in $p(x) \lor p(x)$, which preserves the clause’s structure.

The truth value of ground (i.e., variable-free) atoms is given by a Herbrand interpretation: a set $I$, of type ‘a set, of all true ground atoms. The “models” predicate $\models$ is defined as $I \models A \iff A \in I$. This definition is lifted to literals, clauses, and sets of clauses in the usual way. A set of clauses $D$ is satisfiable if there exists an interpretation $I$ such that $I \models D$.

Resolution depends on a notion of substitution and of most general unifier (MGU). These auxiliary concepts are provided by a third-party library, IsaFoR (Isabelle Formalization of Rewriting) [51]. To reduce our dependency on external libraries, we hide them behind abstract locales parameterized by a type of atoms ‘a and a type of substitutions ‘s.

We start by defining a locale substitution_ops that declares application ($\cdot$), identity (id), and composition ($\circ$):

**locale substitution_ops =**

**fixes**

id :: ‘s and $\circ : ‘s \to ‘s \to ‘s and $\cdot : ‘a \to ‘s \to ‘a

Within the locale’s scope, we introduce a number of derived concepts. Ground atoms are defined as those atoms that are left unchanged by substitutions: is_ground $\triangleq \forall s. A = A \cdot s$. A ground substitution is a substitution whose application always results in ground atoms. Nonstrict and strict generalization are defined as

$\text{generalizes } A B \triangleq \exists s. A \cdot s = B$

$\text{strictly generalizes } A B \triangleq \text{generalizes } A B$

$\land \neg \text{generalizes } B A$

The operators on atoms are lifted to literals, clauses, and sets of clauses. The grounding of a clause is defined as

$\text{grounding of } C = \{C \cdot s \mid \text{is ground } s\}$

The operator is lifted to sets of clauses in the obvious way. Clause subsumption is defined as

$\text{subsumes } C D \triangleq \exists s. C \cdot s \subseteq D$

with strictly subsumes as its strict counterpart.

The next locale, substitution, characterizes the operations defined by substitution_ops. A separate locale is necessary because we cannot interleave assumptions and definitions in a single locale. In addition, substitution fixes a function for renaming clauses apart (so that they do not share any variables) and a function that, given a list of atoms, constructs an atom with these as subterms:

**locale substitution = substitution_ops +**

**fixes**

renamingsApart :: ‘a clause list $\Rightarrow$ ‘s list and

atom_of_atms :: ‘a list $\Rightarrow$ ‘a

assumes

A · id = A

A · (s o r) = (A · s) · r

(\forall A. A · s = A · r) $\Rightarrow$ s = r

is_ground (C · s) $\Rightarrow$ \exists r. is_ground r $\land$ C · r = C · s

---

1https://bitbucket.org/isafol/isafol/wiki/Home
The above definition is presented to give a flavor of our development. We refer to the Isabelle files for the exact definitions. Inside the locale, we prove further properties of the substitution_ops operations. Notably, we prove well-foundedness of the strictly_subsumes predicate based on the well-foundedness of strictly_generalizes, which is stated as an assumption. The atm_of_atms operation is used to encode a clause as a single atom in this well-foundedness proof.

Finally, a third locale, mgu, extends substitution by fixing a function mgu :: 'a set set ⇒ 's option that computes an MGU 𝜏 given a set of unification constraints.

### 3 Bachmair and Ganzinger’s Prover

Our earlier formalization [39, 40] of a nondeterministic ordered resolution prover presented by Bachmair and Ganzinger [2] forms layer 1 of our refinement. In this paper, we restrict our focus to binary resolution, which can be implemented efficiently and forms the basis of modern provers.

The ordered resolution calculus is parameterized by a total order > ("larger than") on ground atoms. For first-order logic, the order > is extended to an order > on nonground atoms so that B > A if and only if for all ground substitutions 𝜏, we have B · 𝜏 > A · 𝜏. The calculus consists of the single rule

\[
\frac{\text{C} \lor A_1 \lor \cdots \lor A_k \leadsto \neg A \lor D}{(C \lor D) \cdot \sigma}
\]

where σ is the (canonical) MGU that solves the unification problem \(A_1 \equiv \cdots \equiv A_k \equiv A\). In addition, each \(A_i \cdot \sigma\) must be strictly >-maximal with respect to the atoms in C · σ (meaning that \(A_i\) is not ≤ any atom in C · σ), and A · 𝜏 is >-maximal with respect to the atoms in D · 𝜏. To achieve completeness, the rule must be adapted slightly to rename apart the variables occurring in different premises.

A set of clauses \(D\) is **saturated** if any conclusion from premises in \(D\) is already in \(D\). The ordered resolution calculus is refutationally complete, meaning that any unsatisfiable saturated set of clauses necessarily contains \(⊥\).

Resolution provers start with a finite set of initial clauses—the input problem—and successively add conclusions from premises in the set. If the inference rule is applied in a fair fashion, the set reaches saturation at the limit; if the set is unsatisfiable, this means \(⊥\) is eventually derived.

Crucially, not only do efficient provers add clauses to their working set, they also remove clauses that are deemed redundant. This requires a refined notion of saturation. We call a set of clauses \(D\) **saturated up to redundancy**, written saturated_up to \(D\), if any inference from nonredundant clauses in \(D\) yields a redundant conclusion.

Bachmair and Ganzinger’s nondeterministic first-order prover, called RP, captures the "dynamic" aspects of saturation. It is defined as an inductive predicate \(\leadsto\) on states, which are triples \(S = (N, P, O)\) of new clauses \(N\), processed clauses \(P\), and old clauses \(O\). Initially, \(N\) is the input problem, and \(P \cup O\) is empty. Clauses can be removed if they are tautological or subsumed or after subsumption resolution has been applied. When all clauses in \(N\) have been processed (either removed entirely or moved to \(P\)), a clause \(C\) from \(P\) can be chosen for inference computation: \(C\) is then moved from \(P\) to \(O\), and all its conclusions with premises from the other old clauses form the new \(N\).

Formally:

\[
\text{inductive } \leadsto :: \text{ 'a state } \Rightarrow \text{ 'a state } \Rightarrow \text{ bool where}
\]

\[
\begin{align*}
\text{Neg } A \in C \land \text{ Pos } A \in C &\quad \Rightarrow \\
(N \cup \{C\}, P, O) \leadsto 1 (N, P, O) &\quad | \\
D \in P \cup O \land \text{ subsumes } D C &\quad \Rightarrow \\
(N \cup \{C\}, P, O) \leadsto 2 (N, P, O) &\quad | \\
D \in N \land \text{ strictly subsumes } D C &\quad \Rightarrow \\
(N, P \cup O \cup \{C\}) \leadsto 4 (N, P, O) &\quad | \\
D \in N \land \text{ strictly subsumes } D C &\quad \Rightarrow \\
(N, P \cup O \cup \{C\}) \leadsto 4 (N, P, O) &\quad | \\
(0, P \cup O \cup \{C\}) \leadsto 2 (N, P, O) &\quad | \\
(\text{concl_of } \text{ 'infers between } O \cup C, P, O \cup \{C\}) \leadsto
\end{align*}
\]

Subscripts on \(\leadsto\) identify the rules. The notation \(f \cdot X\) stands for the image of \(X\) under \(f\), \(\text{infers between } O \cup C\) calculates all the ordered resolution inferences whose premises are a subset of \(O \cup C\) that contains \(C\), and reduces \(D C L\) is defined as \(\exists D' \cdot L' \cdot D = D' \cup L' \land L' \cdot D' \cdot L' \cup C \subseteq C\).

The following derivation shows that RP can diverge even on unsatisfiable clause sets:

\[
\begin{align*}
\{\neg p(a, a), p(x, y) \lor p(x, y), \}, \emptyset, \emptyset, \} \leadsto^+ \{\emptyset, \{\neg p(a, a), p(x, y) \lor p(x, y), \}, \} \leadsto^9 \{\emptyset, \{\neg p(a, a), p(x, x), \}, \{\neg p(f(x), y) \lor p(x, y), \} \}
\end{align*}
\]

We can leave \(\neg p(a, a)\) in \(P\) forever and always generate more clauses of the form \(p(x, f^i(x))\), for increasing values of \(i\). This emphasizes the importance of a fair strategy for selecting clauses to move from \(P\) to \(O\) using rule 9.

Formally, a derivation is a possibly infinite sequence of states \(S_0 \leadsto S_1 \leadsto S_2 \leadsto \cdots\). In Isabelle, this is expressed by the codatatype of lazy lists:
The canonical way of expressing the unsatisfiability of a set of states is that the limit of a fair derivation
\[ \text{Liminf } S \]
interpreted as the unsatisfiability of its grounding. If all positions of \( X_s \) are needed to allow finite chains. Chains cannot be empty. Coinduction is used to allow infinite chains. The base case is needed to allow infinite chains. Chains cannot be empty.

Another important notion is that of the limit of a sequence \( X_s \) of sets. It is defined as the set of elements that are members of all positions of \( X_s \) except for an at most finite prefix:

**definition** \( \text{Liminf } :: \) a set \( \text{llist} \) \( \Rightarrow \) a set where

\[ \text{Liminf } X_s = \bigcup_{i < |X_s|} \bigcap_{j | i < |X_s|} \text{lnth } X_s j \]

Liminf and other operators working on clause sets are lifted pointwise to states. For example, the limit of a sequence of states is defined as \( \text{Liminf } S_s = (\text{Liminf } N_s, \text{Liminf } P_s, \text{Liminf } O_s) \), where \( N_s, P_s, \) and \( O_s \) are the projections of the \( N, P, \) and \( O \) components of \( S_s \).

The soundness theorem states that if RP derives \( \bot \) (i.e., \( \emptyset \)) from a set of clauses, that set must be unsatisfiable:

**theorem** \( \text{RP sound:} \)

\[ \emptyset \in \text{clss \_of } (\text{Liminf } S_s) \Rightarrow \]

\[ \neg \text{satisfiable (grounding \_of } (\text{lhd } S_s)) \]

In the above, \( \text{clss \_of } (N, P, O) = N \cup P \cup O \).

A stronger, finer-grained notion of soundness relates models before and after a transition:

**theorem** \( \text{RP model:} \)

\[ S \Rightarrow S' \Rightarrow (I \models \text{grounding \_of } S') \iff (I \models \text{grounding \_of } S) \]

The canonical way of expressing the unsatisfiability of a set or multiset of first-order clauses with respect to Herbrand interpretations is as the unsatisfiability of its grounding.

Completeness of the prover can only be guaranteed when its rules are executed in a fair order, such that clauses do not get stuck forever in \( N \) or \( P \). Accordingly, fairness is defined as \( \text{Liminf } N_s = \text{Liminf } P_s = \emptyset \). The completeness theorem states that the limit of a fair derivation \( S_s \) is saturated:

**theorem** \( \text{RP saturated if fair:} \)

\[ \text{fair } S_s \Rightarrow \text{saturated \_upto } (\text{Liminf } \text{grounding \_of } S_s) \]

In particular, if the initial problem is unsatisfiable, \( \bot \) must appear in the \( O \) component of the limit of any fair derivation:

**corollary** \( \text{RP complete if fair:} \)

\[ \text{fair } S_s \land \neg \text{satisfiable (grounding \_of } (\text{lhd } S_s)) \Rightarrow \emptyset \in O \_of \ (\text{Liminf } S_s) \]

### 4 Ensuring Fairness

The second refinement layer is the prover \( \text{RP}_w \), which ensures fairness by assigning a weight to every clause and by organizing the set of processed clauses—the \( P \) state component—as a priority queue, where lighter clauses are chosen first. By assigning somewhat heavier weights to newer clauses, we can guarantee that all derivations are fair.

Another necessary ingredient for fairness is that derivations must be complete. For example, the incomplete derivation consisting of the single state \( (\{C\}, \emptyset, \emptyset) \) is not fair. This requirement is expressed formally as \( \text{full \_chain } (\Rightarrow a) S_s \).

For the rest of this section, we fix a full chain \( S_s \) such that \( S'_w \) is not fair. This completes the theorem.

The larger the timestamp, the newer the clause. A state is now a quadruple \( S = (N, P, O, t) \), where the first three components are finite multisets and \( t \) is the timestamp to assign to the next generation of clauses. Formally, we have the following type abbreviations:

**type synonym** \( a \) \( \text{wclause} = \) a clause \( \times \) nat

**type synonym** \( a \) \( \text{wstate} = \)

\[ \text{a wclause multiset} \times \text{a wclause multiset} \]

\[ \times \text{a wclause multiset} \times \text{nat} \]

We extend the \( \text{FO resolution prover} \) locale, in which RP is defined, with a weight function that, for any given clause, is strictly monotone with respect to the timestamp, so that older copies of a clause are preferred to newer ones:

**locale** \( \text{weighted FO resolution prover} = \)

\[ \text{FO resolution prover} + \]

**fixes** \( \text{weight :: a wclause } \Rightarrow \text{nat} \)

**assumes** \( i < j \Rightarrow \text{weight } (C, i) < \text{weight } (C, j) \)

The weight function is otherwise arbitrary. This gives nearly unlimited freedom when selecting clauses, which is possibly the most crucial heuristic in modern provers [43]. For example, breadth-first search corresponds to the instance where weight \( (C, i) \) is defined as \( i \).

The \( \text{RP}_w \) prover uses \( a \) \( \text{wclause} \) for clauses. It is defined inductively as follows:

**inductive** \( a \) \( \text{wstate} \Rightarrow \) a wstate \( \Rightarrow \) bool where

\[ \neg A \in C \land \text{Pos } A \in C \Rightarrow \]

\[ (N \cup \{(C, i)\}, P, O, t) \sim_{w_1} (N, P, O, t) \]

\[ |D | \in \text{fst } (P \cup O) \land \text{subsumes } D C \Rightarrow \]

\[ (N + \{(C, i)\}, P, O, t) \sim_{w_2} (N, P, O, t) \]
A Verified Prover Based on Ordered Resolution

CPP ’19, January 14–15, 2019, Cascais, Portugal

| $D \in \text{fst} \{N \wedge C \in \text{fst} \{P \wedge \text{strictly_subsumes} \quad D \quad C \implies \quad (N', P, O, t) \sim_{w_3} (N, \{E, k \in P \wedge C \neq C \}, O, t)$
| $D \in \text{fst} \{N' \wedge \text{strictly_subsumes} \quad D \quad C \implies \quad (N', P, O \cup \{(C, i)\}, t) \sim_{w_4} (N', P, O, t)$
| $D \in \text{fst} \{N' \wedge \text{strictly_subsumes} \quad D \quad C \implies \quad (N' \cup \{(C, i)\}, \{P \cup \{C\}\}, O, t)$
| $D \in \text{fst} \{N' \wedge \text{strictly_subsumes} \quad D \quad C \implies \quad (N' \cup \{(C, i)\}, \{P \cup \{C\}\}, O, t)$

where $\text{fst}$ is the function that returns the first component of a pair, $\text{mset_set}$ converts a set to the multisets with exactly one copy of each element in the set, and $\text{set}_\text{mset}$ converts a multiset to the set of elements in the multiset.

The most important differences with RP are in the last transition rule. This rule, which computes inferences, assigns timestamp $t$ to each newly computed clause $D$ and increments $t$. Moreover, since we want $P$ to work as a priority queue, RP chooses a clause $C$ with the smallest weight.

Another difference is that RP uses finite multisets for representing $N$, $P$, and $O$. They offer a compromise between sets in layer 1 and lists in layer 3. Finite multisets also help eliminate some unfair derivations. Finiteness guarantees that each clause in $N'$ gets the opportunity to move to $P$ (and further to $O$). Moreover, whereas the set-based RP allows idle transitions, such as $(N' \cup \{C\}, P, O) \rightarrow (N', P \cup \{C\}, O)$ for $C \in N' \cap P$, the use of multisets and $\cup$ precludes such transitions in RP.$w$.

Timesteps are preserved when clauses are moved between $N$, $P$, and $O$. They are also preserved by reduction steps (rules 5 to 7). This works because reduction can only take place finitely many times—a $k$-literal clause can be reduced at most $k$ times. Therefore, there is no risk of divergence due to an infinite chain of reductions.

Timesteps introduce a new danger. It may be the case that a clause $C$ is in the limit if we project away the timestamps, but that no single timestamped clause $(C, i)$ belongs to the limit because the timestamps keep changing, as in the infinite sequence $\{(C, 0)\}, \{(C, 1)\}, \{(C, 2)\}, \ldots$. This could in principle arise due to subsumption, leading to derivations such as the following:

$$\vdash (\ldots \cup \{(C, 0)\}, \ldots) \sim_w (\ldots \cup \{(C, 0), (C, 1)\}, \ldots \sim_w (\ldots \cup \{(C, 1), (C, 2)\}, \ldots \sim_w (\ldots \cup \{(C, 2), \ldots \sim_w \ldots \$$

To prevent this, the RP$w$ rules are formulated so that whenever they remove the earliest copy of any clause $C \in P$, they also remove all its copies from $P$. This property is captured by the following lemma:

**Lemma** preserve_min$P$:

$$S \sim_w S' \wedge (C, i) \in P \wedge C \in \text{fst} \{P \wedge C \in \text{fst} \{P \wedge \text{of} \quad S \quad \wedge \quad (\forall k. (C, k) \in P \wedge S \implies k \geq i) \implies (C, i) \in P \wedge S'$$

This completes our review of RP$w$. As an intermediate step towards a more concrete prover, we restrict the weight function to be a linear equation that considers both timestamps and clause sizes:

**locale** weighted$FO$_resolution_prover_with_size$\_

**fixes** size_factor :: nat $\wedge$ timestamp_factor :: nat

**assumes** timestamp_factor $> 0$

**begin**

**fun** weight :: 'a wclause $\Rightarrow$ nat where

weight $(C, i) = \text{size_factor} \ast |C| + \text{timestamp_factor} \ast i$

**end**

where $|C| = \sum_{A \in E} C \sim_{A \in C} |A|$. It is easy to prove that this definition of weight is strictly monotone and hence that this locale is a sublocale of weighted$FO$ resolution prover. This gives us a correspondingly specialized version of RP$w$, that will form the basis of further refinement steps.

The idea of organizing $P$ as a priority queue is well known in the automated reasoning community. Bachmann and Ganzinger [2, p. 44] mention it in a footnote, but they require the weight to be monotone not only in the timestamp but also in the clause size, claiming that this is necessary to ensure fairness. Our proof reveals that clause size is irrelevant, even in the presence of reductions. This demonstrates how working out the details and making all assumptions explicit using a proof assistant can help clarify fine theoretical points.

**Refinement Proofs.** To lift the soundness and completeness results about RP to RP$w$, we must first show that any possible behavior of RP$w$ on states of wstate is a possible behavior of RP on the corresponding values of type state:

**Lemma** weighted$RP$ imp$RP$:

$$S \sim_w S' \implies \text{state_of} \quad S \quad \sim \quad \text{state_of} \quad S'$$

The proof is by induction on the rules of RP$w$, with one difficult case. Inference computation (rule 9) converts a set to a finite multiset using mset_set, which is undefined for infinite sets. Thus, we must show only a finite set of inferences may be performed from a finite clause set:

**Lemma** finite$ord$ $FO$ resolution inferences between:

finite $D \implies$ finite (inferences between $D \quad C$)

A binary resolution inference takes two premises, of the form $CAA = C \lor A_1 \lor \cdots \lor A_k$ and $DA \lor E = \neg A \lor D$, and produces a conclusion $E = (C \lor D) \lor \sigma$. It can be represented compactly by a tuple of the form $(CAA, DA, AA, A, E)$, where $AA = A_1 \lor \cdots \lor A_k$. We must show that the set of such
tuples produced by inferers_between is finite, assuming \( D \) is finite. First, observe that the last component \( E \) of a tuple is determined by the other four. Hence it suffices to consider quadruples \((CA, DA, AA, A)\). Let \( DC = D \cup \{C\} \), and let \( n \) be the length of the longest clause in \( DC \). Moreover, let \( A = \bigcup_{D \in DC} \text{atoms of } D \) and \( AA = \{B \mid \text{set\_mset } B \subseteq A \land |B| \leq n\} \). Then all inferences between \( D \) and \( C \) belong to \( DC \times DC \times AA \times AA \), a cartesian product of finite sets.

**Soundness and Completeness Proofs.** Using the refinement lemma weighted_RP_imp_RP, it is easy to lift the RP_model theorem (Section 3) to \( \text{RP}_w \):

**Theorem**: \( S \sim_{\text{w}} S' \Rightarrow (I \models \text{grounding of } S' \iff I \models \text{grounding of } S) \)

Completeness is considerably more difficult. We first show that the use of timestamps ensures that all full \( \text{RP}_w \) derivations are fair. In principle, a full derivation could be unfair by virtue of being finite and ending in a state such as \( N \) or \( P \) nonempty. However, this is impossible because the transition of rule 8 or 9 could then be taken from the last state, contradicting the hypothesis that the derivation is full. Hence, finite full derivations are necessarily fair:

**Lemma**: \( \text{fair\_if\_finite} \): \( \text{finite } S_0 \Rightarrow \text{fair } (\text{imap state of } S_0) \)

There are two ways in which an infinite derivation \( S_0 \) in \( \text{RP}_w \) could be unfair: A clause could get stuck forever in \( N \), or in \( P \). We show that the \( N \) case is impossible by defining a measure on states that decreases with respect to the lexicographic extension of \( > \) on \( \text{nat} \) to pairs:

**Abbreviation**: \( \text{RP}_\text{basic\_measure} := \langle \text{a wstate } \Rightarrow \text{nat} \rangle \)

The first component of the pair is the total size of all the clauses in the state, plus 1 for each clause to ensure that empty clauses are also counted. The second component is the number of clauses in \( N \). It is easy to see why the measure is decreasing. Rule 9, inference computation, is not applicable due to our assumption that a clause remains stuck in \( N \). Rule 8, which moves a clause from \( N \) to \( P \), decreases the measure’s second component while leaving the first component unchanged. The other rules decrease the first component since they remove clauses or literals. Formally:

**Lemma**: \( \text{weighted_RP\_basic\_measure\_decreasing-N} \): \( S \sim_{\text{w}} S' \land (C, _) \in N' \iff S \Rightarrow \langle \text{RP}_\text{basic\_measure } S', \text{RP}_\text{basic\_measure } S \rangle \in \text{RP}_\text{basic\_rel} \)

where \( \text{RP}_\text{basic\_rel} = \text{natLess } <\text{lex} \rangle \text{natLess } \text{natLess } = \{ (m, n) \mid m < n \} \).

If a clause \( C \) is stuck in \( P \)? Lemma \( \text{preserve\_min\_P} \) states that in any step, either all copies of \( C \) are removed or the one with the lowest timestamp is kept. Hence, \( C \)'s timestamp will either remain stable or decrease over time. Since \( > \) is well founded on natural numbers, eventually a fixed \( i \) will be reached and will belong to the limit:

**Lemma**: \( \text{persistent\_wclause\_in\_P\_if\_persistent\_clause} \): \( C \in \operatorname{Liminf} (\text{imap } P . \text{of } (\text{imap state of } S_i)) \Rightarrow \exists i. (C, i) \in \operatorname{Liminf} (\text{imap } \text{set\_mset} \circ P . \text{of } S_i) \)

Again, we define a measure, but it must also decrease when inferences are computed and new clauses appear in \( N \). (In this case, \( \text{RP}_\text{basic\_measure} \) may increase.) Our new measure is parameterized by a predicate \( p \) that can be used to filter out undesirable clauses:

**Abbreviation**: \( \text{RP}_\text{filtered\_measure} := \langle \text{a wclause } \Rightarrow \text{bool} \rangle \Rightarrow \langle \text{a wstate } \Rightarrow \text{nat} \rangle \)

The measure \( \text{RP}_\text{filtered\_measure} \) decreases for steps occurring between inference computations and for all steps once we have reached a state where \( t > w \). As a consequence of strict monotonicity of weight, any clauses generated by inference computation from that point on will have weights above \( C \)'s, and if \( C \) remains stuck, then so must these clauses. Thus, we can ignore these clauses altogether, by using \( \lambda (C, i). \ i \leq w \) as the filter \( p \). We adapt the corresponding relation to consider the extra argument:

**Abbreviation**: \( \text{RP}_\text{filtered\_rel} := (\text{nat}^2)^2 \text{ set where } \)

The measure \( \text{RP}_\text{filtered\_measure} \) decreases for steps occurring between inference computations and for all steps once we have reached a state where \( t > w \) (at which point all inference computations are blocked by \( C \)). To obtain a measure that also decreases on inference computation, we add a component \( w + 1 - t \) to the measure. We also add a component \( \text{RP}_\text{basic\_measure} \) to ensure that the measure decreases when a clause \( (C, i) \) such that \( i > w \) is simplified. This yields the combined measure:

**Abbreviation**: \( \text{RP}_\text{combined\_measure} := \langle \text{nat} \Rightarrow \langle \text{a wstate } \Rightarrow \text{nat} \times \text{nat} \rangle \times \text{nat}^3 \rangle \)

\( \text{RP}_\text{combined\_measure} w S \equiv \langle w + 1 - t \rangle \text{ of } S \),

\( \text{RP}_\text{filtered\_measure} (\lambda (C, i). \ i \leq w) S \),

\( \text{RP}_\text{basic\_measure} S \)
This measure is indeed decreasing with respect to a left-to-right lexicographic order:

**Lemma** `weighted_RP_basic_measure_decreasing_P`:

\[
S \leadsto P \wedge Ci \in \mathcal{P} \text{ of } S \implies \\
\text{(RP\textunderscore combined\textunderscore measure\textunderscore weight } Ci) S', \\
\text{RP\textunderscore combined\textunderscore measure\textunderscore weight } Ci S
\in \text{nat\textless } < \text{RP\textunderscore filtered\textunderscore rel } < \text{RP\textunderscore basic\textunderscore rel}
\]

By combining the two lemmas `weighted_RP_basic_measure_decreasing_N` and `weighted_RP_basic_measure_decreasing_P`, we can prove all derivations starting with \( \mathcal{P} = \mathcal{O} = \emptyset \) fair:

**Theorem** `weighted_RP_fair`: fair (limap state of \( S_S \))

Since all derivations are fair and \( \mathcal{P}_w \) derivations correspond to \( \mathcal{P} \)-derivations, it is trivial to lift \( \mathcal{P} \)'s saturation and completeness theorems:

**Corollary** `weighted_RP_saturated`:

\[ \text{saturated\textunderscore upto (Liminf (limap \text{grounding\textunderscore of } S_S))} \]

**Corollary** `weighted_RP_complete`:

\[ \neg \text{satisfiable (grounding\textunderscore of (Ihd } S_S)) \implies \emptyset \in \mathcal{O} \text{ of (Liminf (limap state of } S_S))} \]

5 Eliminating Nondeterminism

The third refinement layer defines a functional program \( \mathcal{P}_d \) that embodies a specific rule application strategy, thereby eliminating \( \mathcal{P}_w \)'s nondeterminism. Clauses are represented by lists, and multisets of clauses by lists of lists.

**Definition.** Our prover corresponds roughly to the following pseudocode:

**Function** `RP_d(N, P, O, t)` is

repeat forever
  if \( \perp \in \mathcal{P} \cup \mathcal{O} \) then
    return \( \mathcal{P} \cup \mathcal{O} \)
  else if \( N = P = 0 \) then
    return \( \mathcal{O} \)
  else if \( N = 0 \) then
    let \( C \) be a minimal-weight clause in \( \mathcal{P} \);
    \( N := \text{conclusions of all inferences from } \mathcal{O} \cup \{C\} \)
    involving \( C \), with timestamp \( t \);
    move \( C \) from \( \mathcal{P} \) to \( \mathcal{O} \);
    \( t := t + 1 \)
  else
    remove an arbitrary clause \( C \) from \( \mathcal{N} \);
    reduce \( C \) using \( \mathcal{P} \cup \mathcal{O} \);
    if \( C = \perp \) then
      return \( \{\perp\} \)
    else if \( C \) is neither a tautology nor subsumed by
    a clause in \( \mathcal{P} \cup \mathcal{O} \) then
      reduce \( \mathcal{P} \) using \( C \);
      reduce \( \mathcal{O} \) using \( C \), moving any reduced
      clauses from \( \mathcal{O} \) to \( \mathcal{P} \);
      remove all clauses from \( \mathcal{P} \) and \( \mathcal{O} \) that are
      strictly subsumed by \( C \);
      add \( C \) to \( \mathcal{P} \)

The function should be invoked with \( \mathcal{N} \) as the input problem,
\( \mathcal{P} = \mathcal{O} = \emptyset \), and an arbitrary timestamp \( t \) (e.g., 0). The loop
is loosely modeled after Vampire’s proof procedure [52].

In Isabelle, the list-based representations compel us to introduce the following type abbreviations:

**Type Synonym** `a lclause` = `a literal list`

**Type Synonym** `a dclause` = `a lclause × nat`

**Type Synonym** `a dstate` = `a dclause list × a dclause list × a dclause list × nat`

The prover is defined inside a locale that inherits `weighted_FO_resolution_prover_with_size_timestamp_factors`. The core function, \( \text{RP}_d \_ \text{step} \), performs a single iteration of the main loop. Here is the definition, excluding auxiliary functions:

**Function** `RP_d_step :: (a dstate) → (a dstate)`

\[
\text{RP}_d \_ \text{step} (N, \mathcal{P}, \mathcal{O}, t) = \\
\text{if } \exists C \in \mathcal{P} @ \mathcal{O}, \text{ fst } C < [] \text{ then} \\
\text{else if } N = P = 0 \text{ then} \\
\text{else if } N = 0 \text{ then} \\
\text{else}
\]

\[
\text{let } (C, i) = \text{select\_min\_weight\_clause } P_0 \mathcal{P}; \\
\text{N} = \text{map } (\lambda D. (D, i)) \text{ (remdup)} \\
\text{resolve\_rename } C \_ C @ \text{ concat (map } \\
\text{resolve\_rename\_both\_ways } C @ \text{ (fst } O)); \\
\mathcal{P} = \text{ filter } (\lambda (D, j). \text{ mset } D \neq \text{ mset } C) \mathcal{P}; \\
\mathcal{O} = (C, i) \# \mathcal{O}; \\
t = t + 1
\]

\[
in (N, \mathcal{P}, \mathcal{O}, t)
\]

\[
\| (C, i) \# N \Rightarrow \\
\text{let } C = \text{ reduce (map } \text{ (fst } (\mathcal{P} @ \mathcal{O})) [C] \text{ in} \\
\text{if } C = [] \text{ then} \\
\text{else if } \text{is\_tautology } C \\
\text{∨ subsume (map } \text{ (fst } (\mathcal{P} @ \mathcal{O})) C \text{ then} \\
\text{(N, } \mathcal{P}, \mathcal{O}, t)
\]

\[
\text{else let } \\
\mathcal{P} = \text{ reduce\_all } C \mathcal{P}; \\
(\text{back\_to } \mathcal{P}, \mathcal{O}) = \text{ reduce\_all2 } C \mathcal{O}; \\
\mathcal{P} = \text{ back\_to } \mathcal{P} @ \mathcal{P}; \\
\mathcal{O} = \text{ filter } ((\neg) \circ \text{ strictly\_subsume } C \circ \text{ (fst }); \mathcal{P}; \\
\mathcal{P} = \text{ filter } ((\neg) \circ \text{ strictly\_subsume } C \circ \text{ (fst } \mathcal{P}; \\
\mathcal{P} = (C, i) \# \mathcal{P}
\]

\[
in (N, \mathcal{P}, \mathcal{O}, t)
\]

The # operator abbreviates the Cons constructor, and @ is the append operator.

The existential quantifier above is unproblematic because it ranges over a finite set, but some of the auxiliary functions use infinite quantification. Notably, subsumption of a clause
null
A Verified Prover Based on Ordered Resolution

\[ \sim_W \] steps. This chain satisfies the conditions postulated on \( S \)'s in Section 4, allowing us to lift the results presented there.

The soundness results are proved in a nameless locale, or context, that assumes termination of \( R_P \):

\[
\text{fixes } R :: \text{a lclause list}
\]

\[
\text{assumes } R_P \ S_0 = \text{Some } R
\]

The definition of \( R_P \), using \textbf{partial_function}, gives us an induction rule restricted to the case where \( R_P \) terminates (i.e., returns a Some value). This rule can be used to prove that \( S \)'s and hence \( wS \)'s and \( ss\,wS \)'s are finite sequences.

Soundness takes the form of a proof of a theorem that lifts \textit{weighted_RP_model} and \textit{weighted_RP_saturated}:

\[
\text{theorem deterministic_RP_model:}
I \vdash \text{grounding_of } N'_0 \iff I \vdash \text{grounding_of } R
\]

\[
\text{theorem deterministic_RP_saturated:}
\text{saturated_upto } ( \text{grounding_of } R )
\]

In most applications, all that matters is the satisfiability status of the set \( N_0 \). It can be retrieved syntactically:

\[
\text{corollary deterministic_RP_refutation:}
\sim \text{satisfiable } ( \text{grounding_of } N'_0 ) \iff \emptyset \in R
\]

Completeness is proved in a separate context that assumes nontermination: \( R_P \ S_0 = \text{None}. The strongest result we prove is that this assumption implies the satisfiability of \( N'_0 \):

\[
\text{theorem deterministic_RP_complete:}
\text{satisfiable } ( \text{grounding_of } N'_0 )
\]

The proof is by contradiction:

Assume that \( \sim \text{satisfiable } ( \text{grounding_of } N'_0 ) \). Hence, by \textit{weighted_RP_complete} we have \( \emptyset \in O_0 \) of \( ss\,wS \)'s. It is easy to show that \( ss\,wS \)'s limit is a subset of \( wS \)'s limit; hence \( \emptyset \in O_0 \) of \( wS \)'s. This implies the existence of a natural number \( k \) such that \( \emptyset \in O_0 \) of \( (\text{Int } wS \ k) \). Hence \( \emptyset \in O_0 \) of \( (\text{RP} s_{\text{step}}^k \ S_0 ) \). However, by an induction on \( k \), we can show that \( R_P \) must terminate after at most \( k \) iterations, contradicting the assumption that \( R_P \) diverges.

A Coinductive Puzzle. A single “big” step of the deterministic prover \( R_P \) may correspond to many “small” steps of the weighted prover \( R_w \). To transfer the results from \( R_P \) to \( R_w \), we must expand the big steps. The core of the expansion is an abstract property of chains and transitive closure:

Let \( R \) be a relation and \( xs \) a chain of \( R^+ \) transitions. There exists a chain of \( R \) transitions that embeds \( xs \)—i.e., that contains all elements of \( xs \) in the same order and with only finitely many elements inserted between each pair of consecutive elements of \( xs \).

On finite chains, this property can be proved by straightforward induction. But the completeness proof must also consider infinite chains. Coinduction and corecursion up-to techniques are useful for such tasks.

The desired property is stated formally as follows:

\[
\text{lemma chain_trancp_imp_exists_chain:}
\text{chain } R^+ \ xs \implies \\
\exists \text{ys. chain } R \text{ ys } \land \text{ xs } \subseteq \text{ ys } \land \text{ lhd } xs = \text{ lhd } ys \\
\land \text{ llast } xs = \text{ llast } ys
\]

where the embedding \( \subseteq \) of lazy lists is defined coinductively using \( + \), which preprends a finite list to a lazy list:

\[
\text{coinductive } \subseteq : \text{a llist } \Rightarrow \text{a llist } \Rightarrow \text{bool where}
\text{infinite } xs \Rightarrow \text{LNil } \subseteq xs \\
| xs \subseteq ys \Rightarrow \text{LCons } x \text{ xs } \subseteq \text{ zs } + + \text{ LCons } x \text{ ys}
\]

\[
\text{fun } + + : \text{a llist } \Rightarrow \text{a llist } \Rightarrow \text{a llist where}
| [] + + xs = xs \\
| (z # zs) + + xs = \text{ LCons } z \text{ (zs } + + xs)
\]

The definition of \( \subseteq \) ensures that infinite lazy lists only embed other infinite lazy lists, but not the finite ones: \( xs \subseteq ys \implies \) (infinite \( xs \) implies infinite \( ys \)). The unguarded calls to \( \text{ llast } \) may seem worrying, but the function is conveniently defined to always return the same unspecified element for infinite lists.

To prove the lemma above, we instantiate the existential quantifier by the following corecursively defined witness:

\[
\text{corec wit } : (\text{a } \Rightarrow (\text{a } \Rightarrow \text{bool})) \Rightarrow \text{a llist } \Rightarrow \text{a llist where}
\text{wit } R \text{ xs } = (\text{case } xs \text{ of}
\text{LCons } x \text{ (LCons } y \text{ ys } ) \Rightarrow \\
\text{LCons } x \text{ (pick } R \text{ x y } + + \text{ wit } R \text{ (LCons y ys))}
| _\Rightarrow ) \implies xs)
\]

Here pick \( R \times y \) returns an arbitrary finite list of \( R \)-related states connecting the \( R^+ \)-related \( x \) and \( y \). Its definition is pick \( R \times y = (\text{SOME } zs \cdot \text{chain } R \text{ (llist_of } (x \# zs @ [y] ))) \), where \( \text{llist_of} \) converts finite lists into lazy lists and \( \text{SOME} \) is Hilbert’s choice operator. Thus, pick satisfies the characteristic property \( R^+ \times y \implies \text{chain } R \text{ (llist_of } (x \# \text{pick } R \times y @ [y] ))) \). The nonexecutability entailed by the use of Hilbert choice is unproblematic because the wit function is used only in the proofs and not in the prover’s code.

The definition of \( \text{wit} \) is not primitively corecursive. Although there is a guarding \( \text{LCons} \) constructor, the corecursive call occurs under \( + + \), which makes the productivity of this function nontrivial. This syntactic structure of the definition is called \textit{corecursive up to} \( + + \). Ultimately, \( \text{wit} \) is productive because \( + + \) does not remove any \( \text{LCons} \) constructors from its second arguments. A slightly weaker requirement, called \textit{friendliness}, is supported by Isabelle’s \textit{corec} command [5]. For the above definition to be accepted \( + + \) must be registered as a “friend.” This involves a one-line proof.

The four conjuncts in \textit{chain_trancp_imp_exists_chain} are discharged in turn under the assumption chain \( R^+ \times xs \). In order of increasing difficulty: lhd \( (\text{wit } R \text{ xs }) = \text{lhd } xs \) follows by simple rewriting. Next, \( \text{llast } (\text{wit } R \text{ xs } ) = \text{llast } xs \) requires an induction in the case of finite chains \( xs \). For any infinite chain \( zs \), \( \text{llast } zs \) is defined as a fixed unspecified ‘a value. The properties \( xs \subseteq \text{wit } R \text{ xs } \) and chain \( R \text{ (wit } R \text{ xs } ) \) require a coinduction on \( \subseteq \) and chain, respectively. In keeping with the
where

vars

To simplify notation, in this paper we fix fresh variable names relies on ′ the variables contained in a list of clauses. The creation of IsaFoR an arbitrary (but executable) linear order.

Iterate terms set set 

Fun

atm

substitutions with ′ instantiate the type substitution (unify includes a wealth of theorems, including the correctness of unify, polymorphic types are used whenever possible. IsaFoR also defines the standard monadic term substitution :: term ⇒ (′u → term) ⇒ term and a unify :: (term × term) list ⇒ lsubst ⇒ lsusb function, where lsubst = (′u × term) list is the list-based representation of a finite substution. The function unify computes the MGU for a list of unification constraints that is compatible with a given substitution. IsaFoR includes a wealth of theorems, including the correctness of unify and the well-foundedness of strict term generalization, defined as (∃σ. s · σ = t) ∧ (∀σ. t · σ = s).

This infrastructure allows us to conveniently instantiate our locales substitution_ops, substitution, and mgu. We instantiate the type ′a of atoms with term and the type ′s of substitutions with ′u → term and the constants · id, · ∘, and atm_of_atms with ·. Var, λx. x, σ · τ, and (arbitrarily) Fun 0. For the MGU computation, there is a slight type mismatch: IsaFoR offers a list-based unifier, whereas our locale requires the type term set set ⇒ (′u ⇒ term) option. It is easy to translate a finite set of finite sets of terms into a finite list of pairs of constraints. To be executable, the translation requires us to sort the terms belonging to set with respect to an arbitrary (but executable) linear order.

Only the function renamings_apart was not present in IsaFoR. We supply a definition:

fun renamings_apart :: term clause list ⇒ (′u ⇒ term) list where

renamings_apart [] = [] | renamings_apart (C # Cs) =

let as = renamings_apart Cs in

(λu. v + max (({0} ∪ vars_clause_list (Cs · as))) + 1) # as

where vars_clause_list :: term clause list ⇒ ′u set returns the variables contained in a list of clauses. The creation of fresh variable names relies on ′u = nat.

Finally, the FO_resolution_prover locale requires that the type of atoms supports two comparison operators: a well-order → and a comparison > that is stable under substitution (i.e., B → A ⇒ B · σ → A · σ). Moreover, → and > must coincide on ground atoms. We instantiate > with the Knuth-Bendix order [19] on terms, provided by IsaFoR [46]. This order is executable, stable under substitution, well-founded, and total on ground terms. The well-order >, which must be total on all terms, is then defined as an arbitrary extension of a partial well-founded order → to a well-order, using Hilbert choice. This makes > non executable, but this is acceptable since it is >, not →, that is used in the prover’s code.

Clause Subsumption. The second hurdle concerns clause subsumption. Its mathematical definition, subsumes C D ⇐⇒ ∃σ. C · σ ⊆ D, involves an infinite quantification.

The problem of deciding whether such a substitution exists is NP-complete [18]. We start with the following naive code. In contrast to the mathematical definition, which operates on multisets of literals, our function operates on lists:

fun subsumes_list :: term literal list ⇒

term literal list ⇒ (′u ⇒ term option) ⇒ bool

where

subsumes_list [] Ks σ = True | subsumes_list (L # Ls) Ks σ =

(∃K ∈ set Ks. is_pos K = is_pos L ∧

case match_term_list [(atm_of L, atm_of K)] σ of

None ⇒ False | Some ρ ⇒ subsumes_list Ls (remove1 K Ks) ρ)

In the Cons case, we must consider all possible matching literals for L from Ks compatible with the substitution σ. The bounded existential quantification that expresses this non-determinism can be executed by iterating over the finite list Ks. The functions is_pos and atm_of are the discriminator and selector for literals. The function match_term_list is provided by IsaFoR. It attempts to extend a given substitution into Some matcher for a list of matching constraints, given as term pairs. If the extension is impossible, match_term_list returns None. This substitution-passing style is typical of purely functional implementations of matching.

It is easy to prove that the above executable function implements clause subsumption: subsumes (mset Ls) (mset Ks) = subsumes_list Ls Ks (λx. None), where mset converts lists to multisets by forgetting the order of the elements. After the registration of this equation, Isabelle’s code generator will rewrite any code that contains the nonexecutable left-hand side to use the executable right-hand side instead.

Clause subsumption is a hot spot in a resolution prover [41]. Following Tammet [49], we implement a heuristic that often reduces the number of calls to match_term_list, which is linear in the size of the input terms, by first performing a simpler, imprecise comparison. For example, terms with different root symbols will never match, and these can be compared in
constant time. Similarly, literals with opposite polarities cannot match. We sort our (list-represented) clauses with respect to a literal quasi-order (i.e., a transitive and reflexive relation) \( \text{leq}_\text{lit} \) such that \( \text{leq}_\text{lit} L K \) only if \( \text{is\_pos} L = \text{is\_pos} K \) and \( \text{match\_term\_list} \left[ \text{atom\_of} L, \text{atom\_of} K \right] \) \( \sigma \) = Some \( \rho \) for some \( \sigma \) and \( \rho \). Any quasi-order satisfying this property can be used in a refinement of \( \text{subsumes\_list} \) to remove too small literals (with respect to \( \text{leq}_\text{lit} \)), as highlighted in gray below:

```plaintext
fun subsumes\_list' [] Ks \sigma = True
| subsumes\_list' (L # Ls) Ks \sigma =
let Ks = filter (leq\_lit L) Ks in
(\( \exists K \in \text{set} Ks. \text{is\_pos} K = \text{is\_pos} L \land \)
case match\_term\_list \left[ \text{atom\_of} L, \text{atom\_of} K \right] \) \sigma of
None \( \Rightarrow \) False
| Some \( \rho \) \( \Rightarrow \) subsumes\_list' Ls (remove1 K Ks \( \rho \))
```

The lemma \( \text{subsumes\_list} Ls Ks \rho = \text{subsumes\_list'} \) (sort \( \text{leq\_lit} Ls \)) \( \text{Ks} \rho \) allows the code generator to refine the original version. In \( \text{RP}_x \), we let \( \text{leq\_lit} \) be a quasi-order that (1) considers negative literals smaller than positive ones; (2) considers variables smaller than nonvariables; and (3) sorts atoms according to a total order on their root symbols.

This refinement is a local optimization: It requires us to explicitly sort one of the input clauses. A potentially more efficient refinement would be to ensure that all clauses in the prover’s state are sorted with respect to \( \text{leq\_lit} \). Sorting \( Ls \) at each invocation of subsumption could then be avoided, and filtering \( Ks \) could be performed more efficiently. However, maintaining the invariant would require changes throughout the prover’s code.

**The End Result.** Finally, Isabelle can export our prover to Standard ML, Haskell, OCaml, or Scala. The command

```plaintext
export\_code \text{RP}_x \text{ in } \text{SML module name} \text{ RP}
```

generates an ML module containing the implementation of our prover in about 1000 lines of code, including dependencies. The generated module exports the function \( \text{RP}_x : (\text{term literal list } \times \text{nat}) \text{ list} \rightarrow \text{bool} \). The input is the \( \mathcal{N} \) component of an initial state, which consists of pairs of clauses and arbitrary timestamps (e.g., 0).

Even though in Isabelle we have proved that for any unsatisfiable input \( \text{RP}_x \) will terminate and return False, the code generator guarantees only partial correctness of its output: If the ML program terminates on the ML input generated from the Isabelle term \( t \) and evaluates to the Boolean result \( b \), the proposition \( \text{RP}_x t = b \) is provable in Isabelle; by soundness, \( b \) indicates the satisfiability of the input clause set. There is recent work towards providing stronger guarantees and reducing the generator’s trusted code base [14].

**Empirical Evaluation.** To measure the gap with the state of the art, we compare our prover’s performance with that of three other provers on a benchmark suite. TPTP (Thousands of Problems for Theorem Provers) [48] is the de facto standard library for benchmarking automatic provers. We extended \( \text{RP}_x \) with the trusted TPTP parser from Metis [15]. We benchmarked \( \text{E} 2.1 \), Vampire 4.2.2, Metis 2.4, and \( \text{RP}_x \) on 1000 randomly selected equality-free problems from the TPTP’s FOF (first-order formulas) and CNF (first-order formulas in conjunctive normal form) categories. We converted all FO problems to CNF using E’s clausifier. Each prover was run on each problem for 60 s on an Intel Core i9-7900X (3.3 GHz 10-Core) with 128 GB of RAM.

The results are summarized in the following table, showing for each prover how many unsatisfiable and satisfiable problems were solved and how many seconds were needed on average by each prover on the problems that were solved by all four:

<table>
<thead>
<tr>
<th></th>
<th>Vampire</th>
<th>E</th>
<th>Metis</th>
<th>\text{RP}_x</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unsatisfiable</td>
<td>675</td>
<td>655</td>
<td>436</td>
<td>331</td>
</tr>
<tr>
<td>Satisfiable</td>
<td>158</td>
<td>135</td>
<td>91</td>
<td>22</td>
</tr>
<tr>
<td>Average time (s)</td>
<td>0.032</td>
<td>0.014</td>
<td>0.637</td>
<td>3.126</td>
</tr>
</tbody>
</table>

The detailed results of the evaluation are available online, together with instructions for reproducing them.³

As expected, \( \text{RP}_x \) is not competitive. A prover’s performance comes from its calculus, its heuristics, and its indexing data structures. \( \text{RP}_x \) employs an excellent calculus but mediocre heuristics and data structures. Better performance could be achieved by working on these last two aspects. Heuristics are often easy to verify, because their input–output specifications are permissive, but formalizing optimized data structures can be very laborious [10].

Nevertheless, sometimes the calculus is all that matters. Benchmark MSC015 from the TPTP library is a particularly challenging family \( \Phi_n \) of first-order problems, each consisting of the following \( n + 2 \) clauses:

\[
\neg p(b, \ldots, b) \lor p(a, \ldots, a)
\]
\[
\neg p(a, b, \ldots, b) \lor p(b, a, \ldots, a)
\]
\[
\neg p(x_1, a, b, \ldots, b) \lor p(x_1, b, a, \ldots, a)
\]
\[
\vdots
\]
\[
\neg p(x_1, \ldots, x_{n-2}, a, b) \lor p(x_1, \ldots, x_{n-2}, b, a)
\]
\[
\neg p(x_1, \ldots, x_{n-2}, x_{n-1}, a) \lor p(x_1, \ldots, x_{n-2}, x_{n-1}, b)
\]

A comment in the benchmark warns us that back in 2007, no prover could solve the \( \Phi_{23} \) within an hour. Even in 2018, only one prover solves \( \Phi_{32} \) within 300 s, and four provers solve \( \Phi_{20} \) within 300 s. \( \text{RP}_x \) solves \( \Phi_{20} \) in 100 s and \( \Phi_{22} \) in 200 s. Presumably, the reason for this success is that \( \text{RP}_x \) fortuitously chooses an instance of the Knuth–Bendix order that is well suited to this benchmark.

³[http://matryoshka.gforge.inria.fr/pubs/fun_rp_data.tar.gz](http://matryoshka.gforge.inria.fr/pubs/fun_rp_data.tar.gz)
7 Discussion and Related Work

We found Bachmair and Ganzinger’s [2] chapter and its formalization [39, 40] suitable as a starting point for a verified prover. Nonetheless, we faced some difficulties, notably concerning the identification of suitable refinement layers. We developed layers 2, 3, and 4 largely in parallel, with each of the authors working on a separate layer. Bringing layer 2 into a state such that it both ensures fairness and could be refined further by layer 3 required several iterations.

Stepwise refinement helped us achieve separation of concerns: fairness, determinism, and executability were achieved successively. Another strength of this methodology is that it allows us to prove results at a high level of abstraction; for example, fairness is established at layer 2 already and is inherited by subsequent layers. The main difficulty with refinement is that some nontrivial machinery is necessary to lift results from one layer to the next. We believe the gain in modularity makes this worthwhile.

It took us quite some time to design a suitable measure to prove the fairness of the layer 2 prover $RP_w$. Our solution amounts to advancing to a state carrying a suitably high timestamp and filtering out all overly heavy clauses. Initially, our proof consisted of two steps—advancing and filtering—each with its own measure. This proof gave us the assurance that $RP_w$ was fair, but we found that combining the measures is both more succinct and more intelligible.

Our main objective was not to reach $\text{qed}$ as quickly as possible but rather to investigate how to harness a modern proof assistant to formalize the metatheory of automatic theorem provers. We found Isabelle suitable for this verification task. The Isar proof language allows us to state key intermediate steps, as in a paper proof. Standard tactics, including Isabelle’s simplifier, can be used to discharge proof obligations. The Sledgehammer tool [32] employs superposition provers and SMT (satisfiability modulo theories) solvers to swiftly identify which lemmas can be used to prove a goal; standard Isabelle tactics are then used to reconstruct the proof. Isabelle’s support for coinductive methods, including the coinductive, codatatype, and corec commands, helps us reason about infinite processes. Locales are a useful abstraction for defining the refinement layers. And Isabelle’s libraries, the Archive of Formal Proofs, and IsaFoR certainly saved us months of labor.

The Archive also includes a refinement framework [25], which has been used in a separate effort to connect the imperative code of an efficient SAT solver to an abstract calculus [6]. The framework is helpful in a variety of situations, including when the refinement relation between a concrete and an abstract data representation is not a function. But since converting a list to a multiset (between our levels 3 and 2) or a multiset to a set (between levels 2 and 1) is a function, we did not see a need to employ it. Moreover, the framework is currently not designed for refining semidecision procedures, as acknowledged privately by its developer. We conjecture that its support for separation logic could be useful if we were to refine the prover further to obtain imperative code.

Thanks to the verification, we can trust to a very high extent that our ordered resolution prover is sound and complete. To make the prover’s performance competitive with E, SPASS, and Vampire, we would need to extend the current work along two axes. First, we should use superposition, together with its extensive simplification machinery, as the base calculus. A good starting point would be to apply our methodology to Peltier’s [33] formalization of superposition. Given that a large part of a modern superposition prover’s code consists of heuristics, which are easy to verify, the full verification of a competitive superposition prover appears to be a realistic objective for a forthcoming Ph.D. thesis. Second, the refinement chain should be continued to cover optimized algorithms and data structures. These could be specified by refining layer 4 further, along the lines of Fleury et al.’s [10] refinement of an imperative SAT solver.

In computer science, a metatheory may inspire an implementation, or vice versa, but the connection is seldom made explicit. By formalizing the metatheory, the implementation, and their connection, we can demonstrate not only the implementation’s correctness but also the metatheory’s adequacy for describing potential implementations. In particular, we have now confirmed that Bachmair and Ganzinger [2] accurately describe the abstract principles of an executable functional prover (with a few exceptions [40]), even though they provide few details beyond layer 1.

We built the prover on our earlier formalization [39, 40] of ordered resolution. Related efforts developed using Isabelle/HOL include Peltier’s [33] formalization of superposition and Schlichtkrull’s [37] formalization of unordered resolution. These developments cover only logical calculi; had we started with any of them, the first step would have been to define an abstract prover in the style of layer 1 and prove basic properties about it. Another related effort is Hirokawa et al.’s [13] formalization of ordered completion, which (like ordered resolution) can be regarded as a special case of superposition.

Formalizing a theorem proving tool using a theorem proving tool is a thrilling (if self-referential) prospect for many researchers. An early result is Ridge and Marguetson’s [35] verified first-order prover, based on a sequent calculus for first-order logic without full first-order terms but only variables. Kumar et al. [24] formalized the soundness of a proof assistant for higher-order logic. Jensen et al. [16] verified the soundness of a kernel for a proof assistant for first-order logic that includes a tableau prover. There are several verified SAT solvers [6, 27–29, 31, 44]. SAT being a decidable problem, termination has been proved for most solvers. First-order logic, on the other hand, is semidecidable.

A pragmatic approach to combining the efficiency of unverified code with the trustworthiness of verified code involves checking certificates produced by reasoning tools—
e.g., proofs produced by SAT solvers [9, 26]. Researchers from the first-order theorem proving community are now advocating this approach for their systems [34]. An ad hoc version of this approach is used in Sledgehammer and HOLyHammer to reconstruct proofs found by external automatic provers [4, 17].

8 Conclusion

Starting from an abstract description of an ordered resolution prover [39, 40], we verified, through a refinement chain, a purely functional prover that uses lists as its main data structure. The resulting program is interesting in its own right and could be refined further to obtain an implementation that is competitive with the state of the art.

Stepwise refinement is a keystone of our methodology, and we found it adequate. Each refinement step cleanly isolates concerns, yielding intelligible proof obligations. Refinement also helps us identify an unnecessary assumption in Bachmair and Ganzinger’s [2] chapter and clarify the argument. Lifting results from one layer to another required some thought, especially the completeness results, which correspond to liveness properties.

Having now established a methodology and built basic formal libraries, we expect that verifying other provers, using Isabelle or other systems, will be substantially easier. Because it is based on Bachmair and Ganzinger’s framework, our approach generally applies to all saturation-based provers, with or without redundancy. This includes resolution, paramodulation, ordered rewriting, superposition, and variants thereof, covering many of the most successful provers for equational [8, 12], first-order [21, 42, 53], and higher-order logic [45].

Acknowledgments

Johannes Hölzl gave us some useful advice on how to specify and reason about possibly nonterminating functions in Isabelle/HOL. Alexander Bentkamp, Mathias Fleury, Andreas Halkjær From, Carsten Fuhs, Peter Lammich, Mark Summerfield, Jørgen Villadsen, and the anonymous reviewers suggested many textual improvements. Eugene Kotelevik, Stephan Schulz, and Geoff Sutcliffe graciously answered our questions about Vampire, E, and TPTP.

Schlichtkrull has received funding from a Ph.D. scholarship in the Algorithms, Logic and Graphs section of DTU Compute and from the European Research Council (ERC) under the European Union’s Horizon 2020 research and innovation program (grant agreement No. 700321, LIGHTTest). Blanchette has received funding from the ERC under the European Union’s Horizon 2020 research and innovation program (grant agreement No. 713999, Matryoshka). An earlier version of this paper was included as a chapter of Schlichtkrull’s Ph.D. thesis [36] with the same authors’ list.

References
