Propositional Resolution and Prime Implicates
Generation

Nicolas Peltier
Laboratory of Informatics of Grenoble/CNRS
University Grenoble Alps

June 11, 2019

Abstract

We provide formal proofs in Isabelle-HOL (using mostly structured Isar proofs) of the soundness and completeness of the Resolution rule in propositional logic. The completeness proofs take into account the usual redundancy elimination rules (namely tautology elimination and subsumption), and several refinements of the Resolution rule are considered: ordered resolution (with selection functions), positive and negative resolution, semantic resolution and unit resolution (the latter refinement is complete only for clause sets that are Horn-renamable). We also define a concrete procedure for computing saturated sets and establish its soundness and completeness. The clause sets are not assumed to be finite, so that the results can be applied to formulas obtained by grounding sets of first-order clauses (however, a total ordering among atoms is assumed to be given).

Next, we show that the unrestricted Resolution rule is deductive-complete, in the sense that it is able to generate all (prime) implicates of any set of propositional clauses (i.e., all entailment-minimal, non-valid, clausal consequences of the considered set). The generation of prime implicates is an important problem, with many applications in artificial intelligence and verification (for abductive reasoning, knowledge compilation, diagnosis, debugging etc.). We also show that implicates can be computed in an incremental way, by fixing an ordering among all the atoms and resolving upon these atoms one by one in the considered order (with no backtracking). This feature is critical for the efficient computation of prime implicates. Building on these results, we provide a procedure for computing such implicates and establish its soundness and completeness.

Contents

1 Syntax of Propositional Clausal Logic 2
2 Semantics 4
# Inference Rules

3.1 Unrestricted Resolution ................................................. 6
3.2 Ordered Resolution ...................................................... 7
3.3 Ordered Resolution with Selection .................................... 8
3.4 Semantic Resolution ...................................................... 8
3.5 Unit Resolution .......................................................... 9
3.6 Positive and Negative Resolution ..................................... 9

# Redundancy Elimination Rules

4 .......................................................... 10

# Renaming

5 .......................................................... 13

# Soundness

6 .......................................................... 14

# Refutational Completeness

7.1 Ordered Resolution ...................................................... 16
7.2 Ordered Resolution with Selection .................................... 17
7.3 Semantic Resolution ...................................................... 18
7.4 Positive and Negative Resolution ..................................... 19
7.5 Unit Resolution and Horn Renamable Clauses ....................... 19

# Computation of Saturated Clause Sets

8 .......................................................... 20

# Prime Implicates Generation

9.1 Implicates and Prime Implicates ................................. 22
9.2 Generation of Prime Implicates ................................. 23
9.3 Incremental Prime Implicates Computation ..................... 24

## Syntax of Propositional Clausal Logic

We define the usual syntactic notions of clausal propositional logic. The set of atoms may be arbitrary (even uncountable), but a well-founded total order is assumed to be given.

theory Propositional-Resolution

imports Main

begin

locale propositional-atoms =
fixes atom-ordering :: ('at × 'at) set
assumes atom-ordering-wf : (wf atom-ordering)
and atom-ordering-total : (∀ x y. (x ≠ y → ((x,y) ∈ atom-ordering ∨ (y,x) ∈ atom-ordering)))
and \( \text{atom-ordering-trans}: \forall x y z. (x,y) \in \text{atom-ordering} \rightarrow (y,z) \in \text{atom-ordering} \rightarrow (x,z) \in \text{atom-ordering} \)
and \( \text{atom-ordering-irrefl}: \forall x y. (x,y) \in \text{atom-ordering} \rightarrow (y,x) \notin \text{atom-ordering} \)

begin

Literals are defined as usual and clauses and formulas are considered as sets. Clause sets are not assumed to be finite (so that the results can be applied to sets of clauses obtained by grounding first-order clauses).

datatype 'a Literal = Pos 'a | Neg 'a
definition atoms = { x::'at. True }

fun atom :: 'a Literal ⇒ 'a
where
(\(\text{atom (Pos } A\)) = A |
(\(\text{atom (Neg } A\)) = A

fun complement :: 'a Literal ⇒ 'a Literal
where
(\(\text{complement (Pos } A\)) = (\text{Neg } A |
(\(\text{complement (Neg } A\)) = (\text{Pos } A)

lemma atom-property : A = (atom L) \implies (L = (Pos A) \lor L = (Neg A))
⟨proof⟩

fun positive :: 'at Literal ⇒ bool
where
(\(\text{positive (Pos } A\)) = \text{True |}
(\(\text{positive (Neg } A\)) = \text{False

fun negative :: 'at Literal ⇒ bool
where
(\(\text{negative (Pos } A\)) = \text{False |}
(\(\text{negative (Neg } A\)) = \text{True

type-synonym 'a Clause = 'a Literal set

type-synonym 'a Formula = 'a Clause set

Note that the clauses are not assumed to be finite (some of the properties below hold for infinite clauses).

The following functions return the set of atoms occurring in a clause or formula.

fun atoms-clause :: 'at Clause ⇒ 'at set
where atoms-clause C = \{ A. \exists L. L ∈ C ∧ A = atom(L) \}

fun atoms-formula :: 'at Formula ⇒ 'at set
where atoms-formula S = \{ A. \exists C. C ∈ S ∧ A ∈ atoms-clause(C) \}
lemma atoms-formula-subset: $S_1 \subseteq S_2 \implies \text{atoms-formula } S_1 \subseteq \text{atoms-formula } S_2$

(\textit{proof})

lemma atoms-formula-union: \text{atoms-formula } (S_1 \cup S_2) = \text{atoms-formula } S_1 \cup \text{atoms-formula } S_2

(\textit{proof})

The following predicate is useful to state that every clause in a set fulfills some property.

\textbf{definition} all-fulfill \:: \text{('at Clause \Rightarrow bool) \Rightarrow 'at Formula \Rightarrow bool}
\textit{where} all-fulfill P S = (\forall C. (C \in S \rightarrow (P C)))

The order on atoms induces a (non total) order among literals:

\textbf{fun} literal-ordering \:: \text{('at Literal \Rightarrow 'at Literal \Rightarrow bool}
\textit{where} \quad (\text{literal-ordering } L_1 L_2) = ((\text{atom } L_1, \text{atom } L_2) \in \text{atom-ordering})

\textbf{lemma} literal-ordering-trans:
\textit{assumes} literal-ordering A B
\textit{assumes} literal-ordering B C
\textit{shows} literal-ordering A C

(\textit{proof})

\textbf{definition} strictly-maximal-literal \:: \text{('at Clause \Rightarrow 'at Literal \Rightarrow bool}
\textit{where} \quad (\text{strictly-maximal-literal } S A) \equiv (A \in S) \land (\forall B. (B \in S \land A \neq B) \implies (\text{literal-ordering } B A))

\section{Semantics}

We define the notions of interpretation, satisfiability and entailment and establish some basic properties.

\textbf{type-synonym} \text{'a Interpretation} = \text{'a set}

\textbf{fun} validate-literal \:: \text{('at Interpretation} \Rightarrow \text{'at Literal} \Rightarrow \text{bool (infix} \models \text{65})
\textit{where} \quad (\text{validate-literal } I (\text{Pos } A)) = (A \in I) |
\quad (\text{validate-literal } I (\text{Neg } A)) = (A \notin I)

\textbf{fun} validate-clause \:: \text{('at Interpretation} \Rightarrow \text{'at Clause} \Rightarrow \text{bool (infix} \models \text{65})
\textit{where} \quad (\text{validate-clause } I C) = (\exists L. (L \in C) \land (\text{validate-literal } I L))

\textbf{fun} validate-formula \:: \text{('at Interpretation} \Rightarrow \text{'at Formula} \Rightarrow \text{bool (infix} \models \text{65})
\textit{where}
(\text{validate-formula} \ I \ S) = (\forall C. (C \in S \rightarrow (\text{validate-clause} \ I \ C)))

definition \text{satisfiable} :: \text{'at Formula} \Rightarrow \text{bool}
\text{where}
(\text{satisfiable} \ S) \equiv (\exists I. (\text{validate-formula} \ I \ S))

We define the usual notions of entailment between clauses and formulas.

definition \text{entails} :: \text{'at Formula} \Rightarrow \text{'at Clause} \Rightarrow \text{bool}
\text{where}
(\text{entails} \ S \ C) \equiv (\forall I. (\text{validate-formula} \ I \ S) \rightarrow (\text{validate-clause} \ I \ C))

lemma \text{entails-member}:
\text{assumes} \ C \in S
\text{shows} \ \text{entails} \ S \ C
\langle \text{proof} \rangle

definition \text{entails-formula} :: \text{'at Formula} \Rightarrow \text{'at Formula} \Rightarrow \text{bool}
\text{where}
(\text{entails-formula} \ S1 \ S2) = (\forall C \in S2. (\text{entails} \ S1 \ C))

definition \text{equivalent} :: \text{'at Formula} \Rightarrow \text{'at Formula} \Rightarrow \text{bool}
\text{where}
(\text{equivalent} \ S1 \ S2) = (\text{entails-formula} \ S1 \ S2 \wedge \text{entails-formula} \ S2 \ S1)

lemma \text{equivalent-symmetric}:
\text{equivalent} \ S1 \ S2 \Rightarrow \text{equivalent} \ S2 \ S1
\langle \text{proof} \rangle

lemma \text{entailment-implies-validity}:
\text{assumes} \ \text{entails-formula} \ S1 \ S2
\text{assumes} \ \text{validate-formula} \ I \ S1
\text{shows} \ \text{validate-formula} \ I \ S2
\langle \text{proof} \rangle

lemma \text{validity-implies-entailment}:
\text{assumes} \ \forall I. \text{validate-formula} \ I \ S1 \rightarrow \text{validate-formula} \ I \ S2
\text{shows} \ \text{entails-formula} \ S1 \ S2
\langle \text{proof} \rangle

lemma \text{entails-transitive}:
\text{assumes} \ \text{entails-formula} \ S1 \ S2
\text{assumes} \ \text{entails-formula} \ S2 \ S3
\text{shows} \ \text{entails-formula} \ S1 \ S3
\langle \text{proof} \rangle

lemma \text{equivalent-transitive}:
\text{assumes} \ \text{equivalent} \ S1 \ S2
\text{assumes} \ \text{equivalent} \ S2 \ S3
\text{shows} \ \text{equivalent} \ S1 \ S3
\langle \text{proof} \rangle

lemma \text{entailment-subset}:
assumes \( S_2 \subseteq S_1 \)
shows \( \text{entails-formula } S_1 S_2 \)

\[ \text{(proof)} \]

lemma \( \text{entailed-formula-entails-implicates} : \)
assumes \( \text{entails-formula } S_1 S_2 \)
assumes \( \text{entails } S_2 C \)
shows \( \text{entails } S_1 C \)
\[ \text{(proof)} \]

3 Inference Rules

We first define an abstract notion of a binary inference rule.

type-synonym \( 'a \text{ BinaryRule} = 'a \text{ Clause } \Rightarrow 'a \text{ Clause } \Rightarrow 'a \text{ Clause } \Rightarrow \text{bool} \)

definition less-restrictive :: \( 'a \text{ BinaryRule } \Rightarrow 'a \text{ BinaryRule } \Rightarrow \text{bool} \)
where
\[ \text{(less-restrictive } R_1 R_2) = (\forall P_1 P_2 C. (R_2 P_1 P_2 C) \rightarrow (\exists P_1 P_2. P_1 \in S \land P_2 \in S \land (R_1 P_2 P_1 C))) \]

The following functions allow to generate all the clauses that are deducible from a given clause set (in one step).

fun all-deducible-clauses :: \( 'a \text{ BinaryRule } \Rightarrow 'a \text{ Formula } \Rightarrow 'a \text{ Formula } \)
where
\[ \text{all-deducible-clauses } R S = \{ C. \exists P_1 P_2. P_1 \in S \land P_2 \in S \land (R (R_1 P_2 P_1 C)) \} \]

fun add-all-deducible-clauses :: \( 'a \text{ BinaryRule } \Rightarrow 'a \text{ Formula } \Rightarrow 'a \text{ Formula } \)
where
\[ \text{add-all-deducible-clauses } R S = (S \cup \text{all-deducible-clauses } R S) \]

definition derived-clauses-are-finite :: \( 'a \text{ BinaryRule } \Rightarrow \text{bool} \)
where
\[ \text{derived-clauses-are-finite } R = (\forall P_1 P_2 C. (\text{finite } P_1 \rightarrow \text{finite } P_2 \rightarrow (R (R_1 P_2 P_1 C) \rightarrow \text{finite } C)) \]

lemma less-restrictive-and-finite :
assumes \( \text{less-restrictive } R_1 R_2 \)
assumes \( \text{derived-clauses-are-finite } R_1 \)
shows \( \text{derived-clauses-are-finite } R_2 \)
\[ \text{(proof)} \]

We then define the unrestricted resolution rule and usual resolution refinements.

3.1 Unrestricted Resolution

definition resolvent :: \( 'a \text{ BinaryRule} \)
where
\[ (\text{resolvent } P_1 P_2 C) \equiv \]
For technical convenience, we now introduce a slightly extended definition in which resolution upon a literal not occurring in the premises is allowed (the obtained resolvent is then redundant with the premises). If the atom is fixed then this version of the resolution rule can be turned into a total function.

```plaintext
fun resolvent-upon :: 'at Clause ⇒ 'at Clause ⇒ 'at ⇒ 'at Clause
where
(resolvent-upon P1 P2 A) = ((P1 − {Pos A}) ∪ (P2 − {Neg A}))
```

```plaintext
lemma resolvent-upon-is-resolvent :
assumes Pos A ∈ P1
assumes Neg A ∈ P2
shows resolvent P1 P2 (resolvent-upon P1 P2 A)
(proof)
```

```plaintext
lemma resolvent-is-resolvent-upon :
assumes resolvent P1 P2 C
shows ∃A. C = resolvent-upon P1 P2 A
(proof)
```

```plaintext
lemma resolvent-is-finite :
shows derived-clauses-are-finite resolvent
(proof)
```

In the next subsections we introduce various resolution refinements and show that they are more restrictive than unrestricted resolution.

### 3.2 Ordered Resolution

In the first refinement, resolution is only allowed on maximal literals.

```plaintext
definition ordered-resolvent :: 'at Clause ⇒ 'at Clause ⇒ 'at Clause ⇒ bool
where
(ordered-resolvent P1 P2 C) ≡ (∃A. ((C = ((P1 − {Pos A}) ∪ (P2 − {Neg A})))) ∧ (strictly-maximal-literal P1 (Pos A)) ∧ (strictly-maximal-literal P2 (Neg A))))
```

We now show that the maximal literal of the resolvent is always smaller than those of the premises.

```plaintext
lemma resolution-and-max-literal :
assumes R = resolvent-upon P1 P2 A
assumes strictly-maximal-literal P1 (Pos A)
assumes strictly-maximal-literal P2 (Neg A)
assumes strictly-maximal-literal R M
```
shows \((\text{atom } M, A) \in \text{atom-ordering}) \langle \text{proof} \rangle

### 3.3 Ordered Resolution with Selection

In the next restriction strategy, some negative literals are selected with highest priority for applying the resolution rule, regardless of the ordering. Relaxed ordering restrictions also apply.

**definition** \((\text{selected-part } Sel \ C) = \{ L. L \in C \land (\exists A \in Sel. L = (\text{Neg } A)) \})

**definition** ordered-sel-resolvent :: \('at set \Rightarrow 'at Clause \Rightarrow 'at Clause \Rightarrow 'at Clause \Rightarrow \text{bool})\where

\((\text{ordered-sel-resolvent } Sel \ P1 P2 C) \equiv \left( \exists A. ((C = (\ (P1 - \{ \text{Pos } A\}) \cup (P2 - \{ \text{Neg } A\}))) \land (\text{strictly-maximal-literal } P1 (\text{Pos } A)) \land ((\text{selected-part } Sel \ P1) = \{\}) \land ((\text{strictly-maximal-literal } P2 (\text{Neg } A)) \land (\text{selected-part } Sel \ P2) = \{\}) \lor (\text{strictly-maximal-literal } (\text{selected-part } Sel \ P2) (\text{Neg } A)))\right)\)

**lemma** ordered-resolvent-is-resolvent : less-restrictive resolvent ordered-resolvent \langle \text{proof} \rangle

The next lemma states that ordered resolution with selection coincides with ordered resolution if the selected part is empty.

**lemma** ordered-sel-resolvent-is-ordered-resolvent :
\begin{align*}
&\text{assumes } \text{ordered-resolvent} \ P1 P2 C \\
&\text{assumes } \text{selected-part } Sel \ P1 = \{\} \\
&\text{assumes } \text{selected-part } Sel \ P2 = \{\} \\
&\text{shows } \text{ordered-sel-resolvent} \ Sel \ P1 P2 C \langle \text{proof} \rangle
\end{align*}

**lemma** ordered-resolvent-upon-is-resolvent :
\begin{align*}
&\text{assumes } \text{strictly-maximal-literal} \ P1 (\text{Pos } A) \\
&\text{assumes } \text{strictly-maximal-literal} \ P2 (\text{Neg } A) \\
&\text{shows } \text{ordered-resolvent} \ P1 P2 (\text{resolvent-upon} \ P1 P2 A) \langle \text{proof} \rangle
\end{align*}

### 3.4 Semantic Resolution

In this strategy, resolution is applied only if one parent is false in some (fixed) interpretation. Note that ordering restrictions still apply, although they are relaxed.

**definition** validated-part :: \('at set \Rightarrow 'at Clause \Rightarrow 'at Clause
\where (\text{validated-part } I C) = \{ L. L \in C \land (\text{validate-literal } I L) \})

**definition** ordered-model-resolvent ::
\begin{align*}
&'\text{at Interpretation} \Rightarrow '\text{at Clause} \Rightarrow '\text{at Clause} \Rightarrow '\text{at Clause} \Rightarrow \text{bool}
\end{align*}
where
\[(\text{ordered-model-resolvent I } P1 P2 C) =\]
\[\exists L. (C = (P1 - \{ L \} \cup (P2 - \{ \text{complement L} \}))) \land\]
\[(\text{validated-part I } P1) = \{} \land (\text{strictly-maximal-literal P1 L}) \land (\text{strictly-maximal-literal (validated-part I } P2) (\text{complement L}))\]

lemma \textit{ordered-model-resolvent-is-resolvent : less-restrictive resolvent (ordered-model-resolvent I)}
(\textit{proof})

3.5 Unit Resolution
Resolution is applied only if one parent is unit (this restriction is incomplete).

definition Unit :: 'at Clause ⇒ bool
where (Unit C) = (\text{card} C = 1)

definition unit-resolvent :: 'at BinaryRule
where (unit-resolvent P1 P2 C) = (\exists L. (C = (P1 - \{ L \}) \cup (P2 - \{ \text{complement L} \}))))
\land L \in P1 \land (\text{complement L} \in P2) \land Unit P1

lemma \textit{unit-resolvent-is-resolvent : less-restrictive resolvent unit-resolvent}
(\textit{proof})

3.6 Positive and Negative Resolution
Resolution is applied only if one parent is positive (resp. negative). Again, relaxed ordering restrictions apply.

definition positive-part :: 'at Clause ⇒ 'at Clause
where (positive-part C) = \{ L. (\exists A. L = \text{Pos} A) \land L \in C \}

definition negative-part :: 'at Clause ⇒ 'at Clause
where (negative-part C) = \{ L. (\exists A. L = \text{Neg} A) \land L \in C \}

lemma \textit{decomposition-clause-pos-neg :}
\quad C = (negative-part C) \cup (positive-part C)
(\textit{proof})

definition ordered-positive-resolvent :: 'at Clause ⇒ 'at Clause ⇒ 'at Clause ⇒ bool
where
\[(\text{ordered-positive-resolvent P1 P2 C}) =\]
\[\exists L. (C = (P1 - \{ L \} \cup (P2 - \{ \text{complement L} \}))) \land\]
\[(\text{negative-part P1}) = \{} \land (\text{strictly-maximal-literal P1 L}) \land (\text{strictly-maximal-literal (negative-part P2} (\text{complement L}))\]
definition ordered-negative-resolvent :: 'at Clause ⇒ 'at Clause ⇒ 'at Clause ⇒ bool
where
(order-negative-resolvent P1 P2 C) =
(∃ L. (C = (P1 − { L } ∪ (P2 − { complement L }))) ∧
((positive-part P1) = {} ∧ (strictly-maximal-literal P1 L)) ∧
(strictly-maximal-literal (positive-part P2) (complement L)))

lemma positive-resolvent-is-resolvent: less-restrictive resolvent ordered-positive-resolvent
⟨proof⟩

lemma negative-resolvent-is-resolvent: less-restrictive resolvent ordered-negative-resolvent
⟨proof⟩

4 Redundancy Elimination Rules

We define the usual redundancy elimination rules.

definition tautology :: 'a Clause ⇒ bool
where
(tautology C) ≡ (∃ A. (Pos A ∈ C ∧ Neg A ∈ C))

definition subsumes :: 'a Clause ⇒ 'a Clause ⇒ bool
where
(subsumes C D) ≡ (C ⊆ D)

definition redundant :: 'a Clause ⇒ 'a Formula ⇒ bool
where
redundant C S = ((tautology C) ∨ (∃ D. (D ∈ S ∧ subsumes D C)))

definition strictly-redundant :: 'a Clause ⇒ 'a Formula ⇒ bool
where
strictly-redundant C S = ((tautology C) ∨ (∃ D. (D ∈ S ∧ (D ⊂ C))))

definition simplify :: 'at Formula ⇒ 'at Formula
where
simplify S = { C. C ∈ S ∧ ¬strictly-redundant C S }

We first establish some basic syntactic properties.

lemma tautology-monotonous: (tautology C) ⇒ (C ⊆ D) ⇒ (tautology D)
⟨proof⟩

lemma simplify-involutive:
shows simplify (simplify S) = (simplify S)
⟨proof⟩

lemma simplify-finite:
assumes all-fulfill finite S
shows all-fulfill finite (simplify S)
proof

lemma atoms-formula-simplify:
  shows atoms-formula (simplify S) ⊆ atoms-formula S

lemma subsumption-preserves-redundancy:
  assumes redundant C S
  assumes subsumes C D
  shows redundant D S

lemma subsumption-and-max-literal:
  assumes subsumes C1 C2
  assumes strictly-maximal-literal C1 L1
  assumes strictly-maximal-literal C2 L2
  assumes A1 = atom L1
  assumes A2 = atom L2
  shows (A1 = A2) ∨ (A1, A2) ∈ atom-ordering

lemma superset-preserves-redundancy:
  assumes redundant C S
  assumes S ⊆ S'
  shows redundant C S'

lemma superset-preserves-strict-redundancy:
  assumes strictly-redundant C S
  assumes S ⊆ SS'
  shows strictly-redundant C SS'

The following lemmas relate the above notions with that of semantic entailment and thus establish the soundness of redundancy elimination rules.

lemma tautologies-are-valid:
  assumes tautology C
  shows validate-clause I C

lemma subsumption-and-semantics:
  assumes subsumes C D
  assumes validate-clause I C
  shows validate-clause I D

lemma redundancy-and-semantics:
  assumes redundant C S
  assumes validate-formula I S
shows validate-clause $I \ C$
(proof)

lemma redundancy-implies-entailment:
  assumes redundant $C \ S$
  shows entails $S \ C$
(proof)

lemma simplify-and-membership :
  assumes all-fulfill finite $S$
  assumes $T = \text{simplify} \ S$
  assumes $C \in S$
  shows redundant $C \ T$
(proof)

lemma simplify-preserves-redundancy:
  assumes all-fulfill finite $S$
  assumes redundant $C \ S$
  shows redundant $C \ (\text{simplify} \ S)$
(proof)

lemma simplify-preserves-strict-redundancy:
  assumes all-fulfill finite $S$
  assumes strictly-redundant $C \ S$
  shows strictly-redundant $C \ (\text{simplify} \ S)$
(proof)

lemma simplify-preserves-semantic :
  assumes $T = \text{simplify} \ S$
  assumes all-fulfill finite $S$
  shows validate-formula $I \ S \leftrightarrow \text{validate-formula} \ I \ T$
(proof)

lemma simplify-preserves-equivalence :
  assumes $T = \text{simplify} \ S$
  assumes all-fulfill finite $S$
  shows equivalent $S \ T$
(proof)

After simplification, the formula contains no strictly redundant clause:

definition non-redundant :: ‘at Formula ⇒ bool
  where non-redundant $S = (\forall C. \ (C \in S \rightarrow \neg \text{strictly-redundant} \ C \ S))$

lemma simplify-non-redundant:
  shows non-redundant $\ (\text{simplify} \ S)$
(proof)

lemma deducible-clause-preserve-redundancy:
  assumes redundant $C \ S$
shows redundant C (add-all-deducible-clauses R S)
(proof)

5 Renaming

A renaming is a function changing the sign of some literals. We show that this operation preserves most of the previous syntactic and semantic notions.

definition rename-literal :: 'at set ⇒ 'at Literal ⇒ 'at Literal
where rename-literal A L = (if (atom L) ∈ A then (complement L) else L)

definition rename-clause :: 'at set ⇒ 'at Clause ⇒ 'at Clause
where rename-clause A C = {L. ∃LL. LL ∈ C ∧ L = (rename-literal A LL)}

definition rename-formula :: 'at set ⇒ 'at Formula ⇒ 'at Formula
where rename-formula A S = {C. ∃CC. CC ∈ S ∧ C = (rename-clause A CC)}

lemma inverse-renaming : (rename-literal A (rename-literal A L)) = L
(proof)

lemma inverse-clause-renaming : (rename-clause A (rename-clause A L)) = L
(proof)

lemma inverse-formula-renaming : rename-formula A (rename-formula A L) = L
(proof)

lemma renaming-preserves-cardinality :
  card (rename-clause A C) = card C
(proof)

lemma renaming-preserves.literal-order :
  assumes literal-ordering L1 L2
  shows literal-ordering (rename-literal A L1) (rename-literal A L2)
(proof)

lemma inverse-renaming-preserves.literal-order :
  assumes literal-ordering (rename-literal A L1) (rename-literal A L2)
  shows literal-ordering L1 L2
(proof)

lemma renaming-is-injective:
  assumes rename-literal A L1 = rename-literal A L2
  shows L1 = L2
(proof)

lemma renaming-preserves-strictly-maximal.literal :
  assumes strictly-maximal.literal C L
  shows strictly-maximal.literal (rename-clause A C) (rename-literal A L)
(proof)
lemma renaming-and-selected-part:
  selected-part UNIV C = rename-clause Sel (validated-part Sel (rename-clause Sel C))
  ⟨proof⟩

lemma renaming-preserves-tautology:
  assumes tautology C
  shows tautology (rename-clause Sel C)
  ⟨proof⟩

lemma rename-union:
  rename-clause Sel (C ∪ D) = rename-clause Sel C ∪ rename-clause Sel D
  ⟨proof⟩

lemma renaming-set-minus-subset:
  rename-clause Sel (C − {L}) ⊆ rename-clause Sel C − {rename-literal Sel L}
  ⟨proof⟩

lemma renaming-set-minus:
  rename-clause Sel (C − {L}) = (rename-clause Sel C) − {rename-literal Sel L}
  ⟨proof⟩

definition rename-interpretation :: 'at set ⇒ 'at Interpretation ⇒ 'at Interpretation
  where
  rename-interpretation Sel I = {A. (A ∈ I ∧ A /∈ Sel) } ∪ {A. (A /∈ I ∧ A ∈ Sel) }

lemma renaming-preserves-semantic:
  assumes validate-literal I L
  shows validate-literal (rename-interpretation Sel I) (rename-literal Sel L)
  ⟨proof⟩

lemma renaming-preserves-satisfiability:
  assumes satisfiable S
  shows satisfiable (rename-formula Sel S)
  ⟨proof⟩

lemma renaming-preserves-subsumption:
  assumes subsumes C D
  shows subsumes (rename-clause Sel C) (rename-clause Sel D)
  ⟨proof⟩

6 Soundness

In this section we prove that all the rules introduced in the previous section are sound. We first introduce an abstract notion of soundness.

definition Sound :: 'at BinaryRule ⇒ bool
where

\[(\text{Sound Rule}) \equiv \forall I P_1 P_2 C. (\text{Rule } P_1 P_2 C \rightarrow (\text{validate-clause } I P_1) \rightarrow (\text{validate-clause } I P_2) \rightarrow (\text{validate-clause } I C))\]

**Lemma soundness-and-entailment:**
- **Assumes:** Sound Rule
- **Assumes:** Rule $P_1 P_2 C$
- **Assumes:** $P_1 \in S$
- **Assumes:** $P_2 \in S$
- **Shows:** entails $S C$

**Lemma all-deducible-sound:**
- **Assumes:** Sound $R$
- **Shows:** entails-formula $S$ (all-deducible-clauses $R S$)

**Lemma add-all-deducible-sound:**
- **Assumes:** Sound $R$
- **Shows:** entails-formula $S$ (add-all-deducible-clauses $R S$)

If a rule is more restrictive than a sound rule then it is necessarily sound.

**Lemma less-restrictive-correct:**
- **Assumes:** less-restrictive $R_1 R_2$
- **Assumes:** Sound $R_1$
- **Shows:** Sound $R_2$

We finally establish usual concrete soundness results.

**Theorem resolution-is-correct:**
- (Sound resolvent)

**Theorem ordered-resolution-correct:** Sound ordered-resolvent

**Theorem ordered-model-resolution-correct:** Sound (ordered-model-resolvent $I$)

**Theorem ordered-positive-resolution-correct:** Sound ordered-positive-resolvent

**Theorem ordered-negative-resolution-correct:** Sound ordered-negative-resolvent

**Theorem unit-resolvent-correct:** Sound unit-resolvent
7 Refutational Completeness

In this section we establish the refutational completeness of the previous inference rules (under adequate restrictions for the unit resolution rule). Completeness is proven w.r.t. redundancy elimination rules, i.e., we show that every saturated unsatisfiable clause set contains the empty clause.

We first introduce an abstract notion of saturation.

**Definition** saturated-binary-rule :: 'a BinaryRule ⇒ 'a Formula ⇒ bool
where
\[(saturated-binary-rule \text{ Rule } S) \equiv (\forall P1 P2 C. ((P1 \in S) \land (P2 \in S) \land (\text{Rule } P1 P2 C))) \rightarrow \text{redundant } C S\]

**Definition** Complete :: 'at BinaryRule ⇒ bool
where
\[(\text{Complete Rule}) = (\forall S. ((saturated-binary-rule \text{ Rule } S) \rightarrow (\text{all-fulfill finite } S) \rightarrow (\{\} \notin S) \rightarrow \text{satisfiable } S))\]

If a set of clauses is saturated under some rule then it is necessarily saturated under more restrictive rules, which entails that if a rule is less restrictive than a complete rule then it is also complete.

**Lemma** less-restrictive-saturated:
- **Assumes** less-restrictive R1 R2
- **Assumes** saturated-binary-rule R1 S
- **Shows** saturated-binary-rule R2 S

⟨proof⟩

**Lemma** less-restrictive-complete:
- **Assumes** less-restrictive R1 R2
- **Assumes** Complete R2
- **Shows** Complete R1

⟨proof⟩

7.1 Ordered Resolution

We define a function associating every set of clauses \( S \) with a “canonic" interpretation constructed from \( S \). If \( S \) is saturated under ordered resolution and does not contain the empty clause then the interpretation is a model of \( S \). The interpretation is defined by mean of an auxiliary function that maps every atom to a function indicating whether the atom occurs in the interpretation corresponding to a given clause set. The auxiliary function is defined by induction on the set of atoms.

**Function** canonic-int-fun-ordered :: 'at ⇒ ('at Formula ⇒ bool)
where
\[(\text{canonic-int-fun-ordered } A) = (\lambda S. (\exists C. (C \in S) \land (\text{strictly-maximal.literal } C (\text{Pos } A)))\]
\[ \forall B. (\text{Pos } B \in C \rightarrow (B, A) \in \text{atom-ordering} \rightarrow (\neg (\text{canonic-int-fun-ordered } B) S))) \]
\[ \land \forall B. (\text{Neg } B \in C \rightarrow (B, A) \in \text{atom-ordering} \rightarrow ((\text{canonic-int-fun-ordered } B) S))) \]

termination \( \langle \text{proof} \rangle \)

definition canonic-int-ordered :: 'at Formula \Rightarrow 'at Interpretation
where
\( (\text{canonic-int-ordered } S) = \{ A. ((\text{canonic-int-fun-ordered } A) S) \} \)

We first prove that the canonic interpretation validates every clause having a positive strictly maximal literal

lemma int-validate-cl-with-pos-max :
  assumes strictly-maximal-literal C (Pos A)
  assumes C \in S
  shows validate-clause (canonic-int-ordered S) C
  \( \langle \text{proof} \rangle \)

lemma strictly-maximal-literal-exists :
\[ \forall C. (((\text{finite } C) \land (\text{card } C) = n \land n \neq 0 \land (\neg (\text{tautology } C)))) \rightarrow (\exists A. (\text{strictly-maximal-literal } C A)) \]

\( \langle \text{proof} \rangle \)

We then deduce that all clauses are validated.

lemma canonic-int-validates-all-clauses :
  assumes saturated-binary-rule ordered-resolvent S
  assumes all-fulfill finite S
  assumes {} \notin S
  assumes C \in S
  shows validate-clause (canonic-int-ordered S) C
  \( \langle \text{proof} \rangle \)

case 7.2 Ordered Resolution with Selection

We now consider the case where some negative literals are considered with highest priority. The proof reuses the canonic interpretation defined in the previous section. The interpretation is constructed using only clauses with no selected literals. By the previous result, all such clauses must be satisfied. We then show that the property carries over to the clauses with non empty selected part.

definition empty-selected-part Sel S = \{ C. C \in S \land (\text{selected-part Sel } C) = \{ \} \)
lemma saturated-ordered-sel-res-empty-sel:
  assumes saturated-binary-rule (ordered-sel-resolvent Sel) S
  shows saturated-binary-rule ordered-resolvent (empty-selected-part Sel S)
  ⟨proof⟩

definition ordered-sel-resolvent-upon :: 'at set ⇒ 'at Clause ⇒ 'at Clause ⇒ 'at Clause ⇒ bool
  where
  ordered-sel-resolvent-upon Sel P1 P2 C A ≡
  (((C = ( (P1 - { Pos A}) ∪ ( P2 - { Neg A })))))
  ∧ (strictly-maximal-literal P1 (Pos A)) ∧ ((selected-part Sel P1) = {})
  ∧ ( ((strictly-maximal-literal P2 (Neg A)) ∧ (selected-part Sel P2) = {})
  ∨ (strictly-maximal-literal (selected-part Sel P2) (Neg A))))

lemma ordered-sel-resolvent-upon-is-resolvent:
  assumes ordered-sel-resolvent-upon Sel P1 P2 C A
  shows ordered-sel-resolvent Sel P1 P2 C
  ⟨proof⟩

lemma resolution-decreases-selected-part:
  assumes ordered-sel-resolvent-upon Sel P1 P2 C A
  assumes Neg A ∈ P2
  assumes finite P1
  assumes finite P2
  assumes card (selected-part Sel P2) = Suc n
  shows card (selected-part Sel C) = n
  ⟨proof⟩

lemma canonic-int-validates-all-clauses-sel:
  assumes saturated-binary-rule (ordered-sel-resolvent Sel) S
  assumes all-fulfill finite S
  assumes {} ∉ S
  assumes C ∈ S
  shows validate-clause (canonic-int-ordered (empty-selected-part Sel S)) C
  ⟨proof⟩

theorem ordered-resolution-is-complete-ordered-sel:
  Complete (ordered-sel-resolvent Sel)
  ⟨proof⟩

7.3 Semantic Resolution

We show that under some particular renaming, model resolution simulates
ordered resolution where all negative literals are selected, which immediately
entails the refutational completeness of model resolution.

lemma ordered-res-with-selection-is-model-res:
  assumes ordered-sel-resolvent UNIV P1 P2 C
shows ordered-model-resolvent $Sel$ (rename-clause $Sel P1$) (rename-clause $Sel P2$)
(rename-clause $Sel C$)
⟨proof⟩

theorem ordered-resolution-is-complete-model-resolution:
  Complete (ordered-model-resolvent $Sel$)
⟨proof⟩

7.4 Positive and Negative Resolution

We show that positive and negative resolution simulate model resolution with some specific interpretation. Then completeness follows from previous results.

lemma empty-interpretation-validate :
  validate-literal $\{\}$ $L = (\exists A. (L = \text{Neg } A))$
⟨proof⟩

lemma universal-interpretation-validate :
  validate-literal $\text{UNIV } L = (\exists A. (L = \text{Pos } A))$
⟨proof⟩

lemma negative-part-lemma:
  (negative-part $C$) = (validated-part $\{\} C$)
⟨proof⟩

lemma positive-part-lemma:
  (positive-part $C$) = (validated-part $\text{UNIV } C$)
⟨proof⟩

lemma negative-resolvent-is-model-res:
  less-restrictive ordered-negative-resolvent (ordered-model-resolvent $\text{UNIV}$)
⟨proof⟩

lemma positive-resolvent-is-model-res:
  less-restrictive ordered-positive-resolvent (ordered-model-resolvent $\{\}$)
⟨proof⟩

theorem ordered-positive-resolvent-is-complete : Complete ordered-positive-resolvent
⟨proof⟩

theorem ordered-negative-resolvent-is-complete: Complete ordered-negative-resolvent
⟨proof⟩

7.5 Unit Resolution and Horn Renamable Clauses

Unit resolution is complete if the considered clause set can be transformed into a Horn clause set by renaming. This result is proven by showing that
unit resolution simulates semantic resolution for Horn-renamable clauses (for some specific interpretation).

**Definition**

\[
\text{Horn} :: \text{'at Clause} \Rightarrow \text{bool}
\]

where \((\text{Horn } C) = ((\text{card } (\text{positive-part } C)) \leq 1)\)

**Definition**

\[
\text{Horn-renamable-formula} :: \text{'at Formula} \Rightarrow \text{bool}
\]

where \(\text{Horn-renamable-formula } S = (\exists I. (\text{all-fulfill } \text{Horn } (\text{rename-formula } I S)))\)

**Theorem**

\text{unit-resolvent-complete-for-Horn-renamable-set}:

\begin{align*}
\text{assumes} & \quad \text{saturated-binary-rule unit-resolvent } S \\
\text{assumes} & \quad \text{all-fulfill finite } S \\
\text{assumes} & \quad \{\} \notin S \\
\text{assumes} & \quad \text{Horn-renamable-formula } S \\
\text{shows} & \quad \text{satisfiable } S
\end{align*}

(\text{proof})

### 8 Computation of Saturated Clause Sets

We now provide a concrete (rather straightforward) procedure for computing saturated clause sets. Starting from the initial set, we define a sequence of clause sets, where each set is obtained from the previous one by applying the resolution rule in a systematic way, followed by redundancy elimination rules. The algorithm is generic, in the sense that it applies to any binary inference rule.

**Function**

\[
\text{inferred-clause-sets} :: \text{'at BinaryRule} \Rightarrow \text{'at Formula} \Rightarrow \text{natt} \Rightarrow \text{'at Formula}
\]

where

\[
\begin{align*}
\text{inferred-clause-sets } R S 0 & = (\text{simplify } S) \\
\text{inferred-clause-sets } R S (\text{Suc } N) & = (\text{simplify } (\text{add-all-deducible-clauses } R (\text{inferred-clause-sets } R S N)))
\end{align*}
\]

The saturated set is constructed by considering the set of persistent clauses, i.e., the clauses that are generated and never deleted.

**Function**

\[
\text{saturation} :: \text{'at BinaryRule} \Rightarrow \text{'at Formula} \Rightarrow \text{'at Formula}
\]

\[
\text{saturation } R S = \{ \text{C, } \exists N. (\forall M. (M \geq N \rightarrow C \in \text{inferred-clause-sets } R S M)) \}
\]

We prove that all inference rules yield finite clauses.

**Theorem**

\text{ordered-resolvent-is-finite : derived-clauses-are-finite ordered-resolvent (proof)}

**Theorem**

\text{model-resolvent-is-finite : derived-clauses-are-finite (ordered-model-resolvent I) (proof)}

**Theorem**

\text{positive-resolvent-is-finite : derived-clauses-are-finite ordered-positive-resolvent}
proof

theorem negative-resolvent-is-finite : derived-clauses-are-finite ordered-negative-resolvent

(proof)

theorem unit-resolvent-is-finite : derived-clauses-are-finite unit-resolvent

(proof)

lemma all-deducible-clauses-are-finite:
  assumes derived-clauses-are-finite R
  assumes all-fulfill finite S
  shows all-fulfill finite (all-deducible-clauses R S)

(proof)

This entails that all the clauses occurring in the sets in the sequence are finite.

lemma all-inferred-clause-sets-are-finite:
  assumes derived-clauses-are-finite R
  assumes all-fulfill finite S
  shows all-fulfill finite (inferred-clause-sets R S N)

(proof)

lemma add-all-deducible-clauses-finite:
  assumes derived-clauses-are-finite R
  assumes all-fulfill finite S
  shows all-fulfill finite (add-all-deducible-clauses R (inferred-clause-sets R S N))

(proof)

We show that the set of redundant clauses can only increase.

lemma sequence-of-inferred-clause-sets-is-monotonous:
  assumes derived-clauses-are-finite R
  assumes all-fulfill finite S
  shows ∀ C. redundant C (inferred-clause-sets R S N)  
         ---→  redundant C (inferred-clause-sets R S (N+M::nat))

(proof)

We show that non-persistent clauses are strictly redundant in some element of the sequence.

lemma non-persistent-clauses-are-redundant:
  assumes D ∈ inferred-clause-sets R S N
  assumes D /∈ saturation R S
  assumes all-fulfill finite S
  assumes derived-clauses-are-finite R
  shows ∃ M. strictly-redundant D (inferred-clause-sets R S M)

(proof)

This entails that the clauses that are redundant in some set in the sequence are also redundant in the set of persistent clauses.
lemma persistent-clauses-subsume-redundant-clauses:
  assumes redundant C (inferred-clause-sets R S N)
  assumes all-fulfill finite S
  assumes derived-clauses-are-finite R
  assumes finite C
  shows redundant C (saturation R S)
⟨proof⟩
We deduce that the set of persistent clauses is saturated.

theorem persistent-clauses-are-saturated:
  assumes derived-clauses-are-finite R
  assumes all-fulfill finite S
  shows saturated-binary-rule R (saturation R S)
⟨proof⟩
Finally, we show that the computed saturated set is equivalent to the initial formula.

theorem saturation-is-correct:
  assumes Sound R
  assumes derived-clauses-are-finite R
  assumes all-fulfill finite S
  shows equivalent S (saturation R S)
⟨proof⟩

9 Prime Implicates Generation

We show that the unrestricted resolution rule is deductive complete, i.e. that it is able to generate all (prime) implicates of any given clause set.

theory Prime-Implicates

imports Propositional-Resolution

begin

context propositional-atoms

begin

9.1 Implicates and Prime Implicates

We first introduce the definitions of implicates and prime implicates.

definition implicates :: 'at Formula ⇒ 'at Formula
  where implicates S = { C. entails S C }
**Definition** prime-implicates :: 'at Formula ⇒ 'at Formula
where prime-implicates S = simplify (implicates S)

### 9.2 Generation of Prime Implicates

We introduce a function simplifying a given clause set by evaluating some literals to false. We show that this partial evaluation operation preserves saturatenedness and that if the considered set of literals is an implicate of the initial clause set then the partial evaluation yields a clause set that is unsatisfiable. Then the proof follows from refutational completeness: since the partially evaluated set is unsatisfiable and saturated it must contain the empty clause, and therefore the initial clause set necessarily contains a clause subsuming the implicate.

**fun** partial-evaluation :: 'a Formula ⇒ 'a Literal set ⇒ 'a Formula
where
\[
(partial-evaluation S C) = \{ E. \exists D. D \in S \land E = D - C \land \neg(\exists L. (L \in C) \land (complement L) \in D)\}
\]

**lemma** partial-evaluation-is-saturated :
assumes saturated-binary-rule resolvent S
shows saturated-binary-rule ordered-resolvent (partial-evaluation S C)
\langle proof \rangle

**lemma** evaluation-wrt-implicate-is-unsat :
assumes entails S C
assumes \neg tautology C
shows \neg satisfiable (partial-evaluation S C)
\langle proof \rangle

**lemma** entailment-and-implicates:
assumes entails-formula S1 S2
shows implicates S2 ⊆ implicates S1
\langle proof \rangle

**lemma** equivalence-and-implicates:
assumes equivalent S1 S2
shows implicates S1 = implicates S2
\langle proof \rangle

**lemma** equivalence-and-prime-implicates:
assumes equivalent S1 S2
shows prime-implicates S1 = prime-implicates S2
\langle proof \rangle

**lemma** unrestricted-resolution-is-deductive-complete :
assumes saturated-binary-rule resolvent S
assumes all-fulfill finite S

23
assumes $C \in \text{implicates } S$
shows redundant $C \text{ S}$
(proof)

lemma prime-implicates-generation-correct :
assumes saturated-binary-rule resolvent $S$
assumes non-redundant $S$
assumes all-fulfill finite $S$
shows $S \subseteq \text{prime-implicates } S$
(proof)

theorem prime-implicates-of-saturated-sets:
assumes saturated-binary-rule resolvent $S$
assumes all-fulfill finite $S$
assumes non-redundant $S$
shows $S = \text{prime-implicates } S$
(proof)

9.3 Incremental Prime Implicates Computation

We show that it is possible to compute the set of prime implicates incrementally i.e., to fix an ordering among atoms, and to compute the set of resolvents upon each atom one by one, without backtracking (in the sense that if the resolvents upon a given atom are generated at some step $i$ then no resolvents upon the same atom are generated at step $i < j$). This feature is critical in practice for the efficiency of prime implicates generation algorithms.

We first introduce a function computing all resolvents upon a given atom.

definition all-resolvents-upon :: 'at Formula ⇒ 'at ⇒ 'at Formula
where (all-resolvents-upon $S \ A) = \{ C. \ \exists P1 \ P2. \ P1 \in S \land P2 \in S \land C = (\text{resolvent-upon } P1 \ P2 \ A) \} $

lemma resolvent-upon-correct:
assumes $P1 \in S$
assumes $P2 \in S$
assumes $C = \text{resolvent-upon } P1 \ P2 \ A$
shows entails $S \ C$
(proof)

lemma all-resolvents-upon-is-finite:
assumes all-fulfill finite $S$
shows all-fulfill finite $(S \cup (\text{all-resolvents-upon } S \ A))$
(proof)

lemma atoms-formula-resolvents:
shows atoms-formula $(\text{all-resolvents-upon } S \ A) \subseteq \text{atoms-formula } S$
(proof)

24
We define a partial saturation predicate that is restricted to a specific atom.

**definition** \( \text{partial-saturation} :: 'at \text{ Formula} \Rightarrow 'at \Rightarrow 'at \text{ Formula} \Rightarrow \text{bool} \)

**where**

\[
\text{partial-saturation} \ S \ A \ R = (\forall \ P1 \ P2. \ (P1 \in S \implies P2 \in S \implies (\text{redundant} \ (\text{resolvent-upon} \ P1 \ P2 \ A) \ R)))
\]

We show that the resolvent of two redundant clauses in a partially saturated set is itself redundant.

**lemma** \( \text{resolvent-upon-and-partial-saturation} : \)

\begin{align*}
\text{assumes} & \quad \text{redundant} \ P1 \ S \\
\text{assumes} & \quad \text{redundant} \ P2 \ S \\
\text{assumes} & \quad \text{partial-saturation} \ S \ A \ (S \cup R) \\
\text{assumes} & \quad C = \text{resolvent-upon} \ P1 \ P2 \ A \\
\text{shows} & \quad \text{redundant} \ C \ (S \cup R)
\end{align*}

\(\langle \text{proof} \rangle\)

We show that if \( R \) is a set of resolvents of a set of clauses \( S \) then the same holds for \( S \cup R \). For the clauses in \( S \), the premises are identical to the resolvent and the inference is thus redundant (this trick is useful to simplify proofs).

**definition** \( \text{in-all-resolvents-upon} :: 'at \text{ Formula} \Rightarrow 'at \Rightarrow 'at \text{ Clause} \Rightarrow \text{bool} \)

**where**

\[
\text{in-all-resolvents-upon} \ S \ A \ C = (\exists \ P1 \ P2. \ (P1 \in S \land P2 \in S \land C = \text{resolvent-upon} \ P1 \ P2 \ A))
\]

**lemma** \( \text{every-clause-is-a-resolvent} : \)

\begin{align*}
\text{assumes} & \quad \text{all-fulfill} \ (\text{in-all-resolvents-upon} \ S \ A) \ R \\
\text{assumes} & \quad \text{all-fulfill} \ (\lambda x. \neg(\text{tautology} \ x)) \ S \\
\text{assumes} & \quad P1 \in S \cup R \\
\text{shows} & \quad \text{in-all-resolvents-upon} \ S \ A \ P1
\end{align*}

\(\langle \text{proof} \rangle\)

We show that if a formula is partially saturated then it stays so when new resolvents are added in the set.

**lemma** \( \text{partial-saturation-is-preserved} : \)

\begin{align*}
\text{assumes} & \quad \text{partial-saturation} \ S \ E1 \ S \\
\text{assumes} & \quad \text{partial-saturation} \ S \ E2 \ (S \cup R) \\
\text{assumes} & \quad \text{all-fulfill} \ (\lambda x. \neg(\text{tautology} \ x)) \ S \\
\text{assumes} & \quad \text{all-fulfill} \ (\text{in-all-resolvents-upon} \ S \ E2) \ R \\
\text{shows} & \quad \text{partial-saturation} \ (S \cup R) \ E1 \ (S \cup R)
\end{align*}

\(\langle \text{proof} \rangle\)

The next lemma shows that the clauses inferred by applying the resolution rule upon a given atom contain no occurrence of this atom, unless the inference is redundant.

**lemma** \( \text{resolvents-do-not-contain-atom} : \)

\begin{align*}
\text{assumes} & \quad \neg \text{tautology} \ P1
\end{align*}
assumes ¬ tautology P2
assumes C = resolvent-upon P1 P2 E2
assumes ¬ subsumes P1 C
assumes ¬ subsumes P2 C
shows (Neg E2) ∉ C ∧ (Pos E2) ∉ C
⟨proof⟩

The next lemma shows that partial saturation can be ensured by computing all (non-redundant) resolvents upon the considered atom.

**Lemma ensure-partial-saturation** :
assumes partial-saturation S E2 (S ∪ R)
assumes all-fulfill (λx. ¬(tautology x)) S
assumes all-fulfill (in-all-resolvents-upon S E2) R
assumes all-fulfill (λx. ¬redundant x S) R
shows partial-saturation (S ∪ R) E2 (S ∪ R)
⟨proof⟩

**Lemma resolvents-preserve-equivalence**:
shows equivalent S (S ∪ (all-resolvents-upon S A))
⟨proof⟩

Given a sequence of atoms, we define a sequence of clauses obtained by resolving upon each atom successively. Simplification rules are applied at each iteration step.

**Fun resolvents-sequence** :: (nat ⇒ ′at) ⇒ ′at Formula ⇒ nat ⇒ ′at Formula
where
(resolvents-sequence A S 0) = (simplify S) |
(resolvents-sequence A S (Suc N)) =
(simplify ((resolvents-sequence A S N)
∪ (all-resolvents-upon (resolvents-sequence A S N) (A N))))

The following lemma states that partial saturation is preserved by simplification.

**Lemma redundancy-implies-partial-saturation**:
assumes partial-saturation S1 A S1
assumes S2 ⊆ S1
assumes all-fulfill (λx. redundant x S2) S1
shows partial-saturation S2 A S2
⟨proof⟩

The next theorem finally states that the implicate generation algorithm is sound and complete in the sense that the final clause set in the sequence is exactly the set of prime implicates of the considered clause set.

**Theorem incremental-prime-implication-generation**:
assumes atoms-formula S = { X. ∃ I::nat. I < N ∧ X = (A I) }
assumes all-fulfill finite S
shows (prime-implicates S) = (resolvents-sequence A S N)
⟨proof⟩
end
end