Completeness of Resolution and Superposition Calculi

Rolf Socher-Ambrosius

Max-Planck-Institut für Informatik, Im Stadtwald,
D-W-6600 Saarbrücken, Germany
email: socher@mpi-sb.mpg.de

Abstract: We modify Bezem's [Be] completeness proof for ground resolution in order to deal with ordered resolution, redundancy, and equational reasoning in form of superposition. The resulting proof is completely independent of the cardinality of the set of clauses.

1 Introduction

M. Bezem [Be] presented a completeness proof for ground resolution that is independent of the cardinality of both the language and the set of clauses. As a corollary, he obtained a completeness result for (first-order) resolution that does not appeal to Herbrand's theorem. This proof technique easily extends to the following resolution strategies: Semantic resolution, Hyperresolution, and Ordered Hyperresolution. In this paper, we give a very similar completeness proof for Ordered Resolution. Moreover, we define a notion of redundancy similar to that of [BG] and show that (Ordered) Resolution is still complete if redundant clauses are deleted. Finally, we use the same techniques to prove completeness of a particular superposition calculus for equational clauses.

In the following, $\mathcal{L}$ is an arbitrary set of propositional *atoms*. A *clause* is a pair $(\mathcal{A},\mathcal{B})$, written in the form $\mathcal{A} \to \mathcal{B}$, where both $\mathcal{A}$ and $\mathcal{B}$ are finite sets of atoms. The clause $\mathcal{A} \to \mathcal{B}$ is written $\to \mathcal{B}$, if $\mathcal{A} = \emptyset$, —in which case $\mathcal{A} \to \mathcal{B}$ is called *positive*—and $\mathcal{A} \to$, if $\mathcal{B} = \emptyset$. We shall usually write $\mathcal{A},A$ instead of $\mathcal{A} \cup \{A\}$.

An interpretation $\Im$ is a subset of $\mathcal{L}$. We write $\Im \models \mathcal{A} \to \mathcal{B}$, ($\Im$ *satisfies* $\mathcal{A} \to \mathcal{B}$), iff $\mathcal{A} \not\subseteq \Im$ or $\mathcal{B} \cap \Im \neq \emptyset$. A set S of clauses is called *satisfiable*, if there exists an interpretation $\Im$ that satisfies each member clause of S, in which case $\Im$ is called a *model* of S. We write $S \models \mathcal{A} \to \mathcal{B}$, if each model of S is also a model of C. The set S is called *consistent*, iff it does not contain the empty clause.

If $C = \mathcal{A} \to A,\mathcal{B}$, and $D = \mathcal{A}',A \to \mathcal{B}'$, then the clause $\mathcal{A},\mathcal{A}' \to \mathcal{B},\mathcal{B}'$ is called a *resolvent* of (the *parent clauses*) C and D *upon the atom* A. A *resolution derivation* from a set S is a sequence $S = S_0, S_1, \ldots$ such that $S_{i+1} = S_i \cup \{C_i\}$, where C_i is a resolvent of clauses in S_i. A *resolution refutation* of S is a finite derivation $S = S_0, S_1, \ldots, S_n$, such that S_n contains the empty clause.

The most important properties of logical calculi are *correctness* and *completeness*. Resolution is easily proved to be correct, since both satisfiability and unsatisfiability of a clause sets are preserved, when resolvents are added. Completeness of resolution is usually proved in two steps, first by showing completeness of ground resolution, and then by proving that any ground refutation can be lifted to the first order level. Our general proceeding for proving (certain restrictions of) ground resolution to be complete, consists in showing that a consistent set of ground clauses that is closed under resolution is satisfiable.

Before proving completeness of ordered resolution, we shall briefly sketch Bezem's proof. (His proof is more general, but this sketch will be sufficient for our purposes). Given a consistent set S of ground clauses that is closed under resolution, we construct an interpretation for S as follows: Let S^+ be the set consisting of all clauses of S that are positive, and let X be the set of atoms which occur in clauses from S^+. A subset Y of X is said to *cover* S^+, if each element of S^+ contains an atom of Y. Now let $\Im$ be a minimal subset of X covering S^+. As S^+ may be uncountable, the construction of $\Im$ requires the use of Zorn's lemma. Now the crucial point is that for each $A \in \Im$, there is a clause in S^+ containing A, but no other atom from $\Im$. By construction, $\Im$ satisfies S^+. Assume $\Im$ does not satisfy some clause $C = \mathcal{A} \rightarrow \mathcal{B}$ in S–S^+. We can choose C in a way such that $|\mathcal{A}|$ is minimal. Then $\mathcal{A} \neq \emptyset$, $\mathcal{A} \subseteq \Im$ and $\mathcal{B} \cap \Im = \emptyset$ holds. Let $A \in \mathcal{A}$ and let $D = \rightarrow \mathcal{B}'$ be a clause in S^+ with $\Im \cap \mathcal{B}' = \{A\}$. Let $R = \mathcal{A}–\{A\} \rightarrow \mathcal{B},\mathcal{B}'–\{A\}$ be the resolvent of C and D, which is in S by the closure assumption. It is easy to check that $\Im$ does not satisfy R, which contradicts the minimality assumption on C. The assumption that $\Im$ does not satisfy C thus leads to a contradiction, which proves that $\Im$ satisfies S.

2 Ordered Resolution

A *well ordering* of a set S is an ordering such that each non-empty subset of S contains a smallest element. In particular, a well ordering $>$ is total, that is, two elements can always be compared by $>$. Zermelo's well-ordering theorem states that every set can be well–ordered. In the following we assume a well-ordering $>$ on the set $\mathcal{L}$ of atoms. The ordering $>$ on clauses is defined to be the multiset extension of $>$ (regarding a clause as the set of its atoms).

Ordered Resolution is a restriction of resolution, requiring that the atom resolved upon be maximal in both parent clauses. In [Be], a variant of hyperresolution, called *ordered hyperresolution*, is shown to be complete. This ordering restriction is certainly weaker than ordered resolution, since it requires the atom resolved upon to be maximal only in one of the parent clauses (the so called *nucleus*).

In his paper, Bezem remarks that the minimal covering set $\Im$ may not be unique. When dealing with ordered hyperresolution, we have to choose $\Im$ in a way, such that for each $A \in \Im$, there is a clause in S^+ containing *A as a maximal atom*, and no other atom from $\Im$. For ordered resolution, we additionally have to modify the definition of the set S^+.

For any clause C, $\max(C)$ denotes the maximal atom occuring in (the antecedent or succedent of) C. Given a consistent set S of ground clauses that is closed under Ordered Resolution, let S^+ be the set $\{\mathcal{A} \rightarrow \mathcal{B} \in S \mid \max(\mathcal{A} \rightarrow \mathcal{B}) \in \mathcal{B}\}$.

The following construction of a minimal model of S^+ is due to Bezem. We start with $X_0 := \{A \mid \text{there is } C \in S^+, \text{ with } A = \max(C)\}$ and construct inductively sets X_α with $X_{\alpha+1} = X_\alpha - \{\min\{A \mid A \in X_\alpha \text{ and } (X_\alpha - \{A\}) \text{ satisfies } S^+\}\}$ for all ordinals α for which X_α is not a minimal model of S^+. We thus obtain a set $\Im$, which is a model of S^+ satisfying the following property:

For each $A \in \Im$, there exists a clause $\mathcal{A} \rightarrow \mathcal{B}, A$ in S^+, such that

(i) A is maximal in $\mathcal{A} \cup \mathcal{B}$ and
(ii) $\mathcal{A} \subseteq \Im$ and $\mathcal{B} \cap \Im = \emptyset$.

Now let $C = \mathcal{A}' \rightarrow \mathcal{B}'$ be a minimal (w.r.t. $>$) clause in $S - S^+$, such that $\Im$ does not satisfy C. This implies $\mathcal{A}' \subseteq \Im$ and $\mathcal{B}' \cap \Im = \emptyset$. Let $A \in \mathcal{A}'$ be maximal in $\mathcal{A}' \cup \mathcal{B}'$. Since $A \in \Im$, there exists a clause $D = \mathcal{A} \rightarrow \mathcal{B}, A$ in S^+ such that $A = \max(D)$ and $\mathcal{A} \subseteq \Im$ and $\mathcal{B} \cap \Im = \emptyset$ holds. Thus the clause

$$R = \mathcal{A}' - \{A\},\mathcal{A} \rightarrow \mathcal{B}',\mathcal{B}$$

is an ordered resolvent of C and D, and it is easy to see that $\Im$does not satisfy R, either. Moreover, $C > R$ holds, thus contradicting the choice of C.

The assumption that $\Im$ does not satisfy C thus leads to a contradiction, which proves that $\Im$ satisfies S. □

We remark that the previous result also holds for any ordering $>$ on $\mathcal{L}$ that is not necessarily total, but is *contained* in a (total) well-ordering. Such an ordering is always well-founded, that is, each subset of $\mathcal{L}$ contains a minimal element.

3 Equational Reasoning

3.1 Equational Clauses, Interpretations, and Orderings

In this chapter, we use the model construction techniques to prove completeness of a particular superposition calculus for equational clauses. For the following definitions, see also [BG] or [NR].

We write $A[t]$ to indicate that A contains t as a subexpression. An *equation* is a term pair $s \approx t$. An (equational) *clause* is a pair $\mathcal{A} \rightarrow \mathcal{B}$, where both $\mathcal{A}$ and $\mathcal{B}$ are finite sets of equations. In the following we are interested particularly in *ground clauses*, that is, equations containing no variables.

An equivalence relation ~ on terms is called a *congruence*, if $s \sim t$ implies $u[s] \sim u[t]$ for all terms u, s, and t. If E is a set of ground equations, we denote by E^* the smallest congruence containing E.

An (equality Herbrand) *interpretation* $\Im$ *over* E is a congruence E'^*, where E' is a subset of E. We write $\Im \models \mathcal{A} \rightarrow \mathcal{B}$, ($\Im$ *satisfies* $\mathcal{A} \rightarrow \mathcal{B}$), iff $\mathcal{A} \not\subseteq \Im$ or $\mathcal{B} \cap \Im \neq \emptyset$. A set S of clauses is called *satisfiable*, if there exists an interpretation $\Im$ that satisfies each member clause of S.

A binary relation $\rightarrow$ on terms is called a *rewrite relation*, iff $s \rightarrow t$ implies $u[s\sigma] \rightarrow u[t\sigma]$ for all terms u and all substitutions σ. A transitive, well-founded rewrite relation is called a *reduction ordering*. By $\rightarrow^*$ we denote the transitive, reflexive closure of $\rightarrow$ and by $\leftrightarrow^*$ the symmetric, transitive, and reflexive closure.

A set E of equations is called a *rewrite system* with respect to an ordering $>$ if $s > t$ or $t > s$ holds for all equations $s \approx t$ in E. By $\rightarrow_E$, we denote the smallest rewrite relation containing E. A term t is called *irreducible* with respect to the rewrite system E, if there is no term s with $t \rightarrow_E s$, and *reducible* otherwise. A well-founded rewrite relation $\rightarrow$ is said to be *convergent*, if $s \leftrightarrow^* t$ implies the existence of a term u with $s \rightarrow^* u$ and $t \rightarrow^* u$. A rewrite system E is called *left-reduced*, if for every rule $s \approx t$ in E with $s > t$, the term s is irreducible by $E - \{s \approx t\}$. It is well-known that left-reduced, well-founded ground rewrite systems are convergent [Hu].

We assume given a reduction ordering $>$ on the set of terms, which is total on the set of ground terms. We define the ordering $>^e$ on equations to be the multiset extension of $>$. We identify an *occurrence* of an equation $s \approx t$ in the antecedent of a clause with the multiset $\{\{s,s\},\{t,t\}\}$, and an *occurrence* in the succedent with the multiset $\{\{s\},\{t\}\}$. In a similar way, we identify clauses with multisets of occurrences of equations. Occurrences of equations are ordered by $>^o$, which is the twofold multiset extension of $>$, and clauses are ordered by $>^c$, which is the multiset extension of $>^o$. We point out that the ordering $>^c$ on clauses is different from the multiset extension of the ordering $>^e$ on equations. For instance, if $a > b > c$, then $a \approx b >^e a \approx c$ holds, however, we have $\mathcal{A}, a \approx c \rightarrow \mathcal{B} >^c \mathcal{A} \rightarrow \mathcal{B}, a \approx b$, as the occurrence of $a \approx c$ in the antecedent is larger than the occurrence of $a \approx b$ in the succedent.

Techniques to remove redundant clauses in theorem proving derivations are most common to all theorem provers. Bachmair and Ganzinger [BG] developed a notion of redundancy that covers all commonly known simplification techniques like simplification by rewriting, subsumption, etc. A *theorem proving derivation* from a set S is a sequence $S = S_0, S_1, \ldots$ such that $S_{i+1} = S_i \cup \{C_i\}$, where C_i is a clause with $S_i \models C_i$ or $S_{i+1} = S_i - \{C_i\}$, where C_i is redundant in S_i. Completeness of such derivations is shown by proving that a consistent set of clauses that is *relatively closed* under ordered resolution has a model. A set S of clauses is *relatively* closed under an inference system, if any result of an inference step with premises in S is in S or redundant in S.

In the following, equations are always written in the form $s \approx t$, such that $t \not> s$ holds.

3.2 An Inference System for Equational Logic

In the following we define a superposition inference system I for *ground clauses*. There exist more refined superposition calculi, for instance [BG], [Ru], our intention, however, is to provide a completeness proof without going too much into the details of the inference system.

The system I consists of the following rules:

Equality resolution:
$$\frac{\mathcal{A},\, t \approx t \to \mathcal{B}}{\mathcal{A} \to \mathcal{B}}$$

where $t \approx t$ is a maximal occurrence in $\mathcal{A} \cup \mathcal{B}$.

Superposition left:
$$\frac{\mathcal{A} \to \mathcal{B},\, s \approx t \quad \mathcal{A}',\, u[s] \approx v \to \mathcal{B}'}{\mathcal{A},\, \mathcal{A}',\, u[t] \approx v \to \mathcal{B},\, \mathcal{B}'}$$

where both $s \approx t$ and $u \approx v$ are maximal occurrences in their respective clauses.

Superposition right:
$$\frac{\mathcal{A} \to \mathcal{B},\, s \approx t \quad \mathcal{A}' \to \mathcal{B}',\, u[s] \approx v}{\mathcal{A},\, \mathcal{A}' \to \mathcal{B},\, \mathcal{B}',\, u[t] \approx v}$$

where both $s \approx t$ and $u \approx v$ are maximal occurrences in their respective clauses.

Equality factoring:
$$\frac{\mathcal{A} \to \mathcal{B},\, s \approx t,\, s \approx t'}{\mathcal{A},\, t \approx t' \to \mathcal{B},\, s \approx t'}$$

where $s \approx t$ is a maximal occurrences in its clause.

As a first observation, we state that a clause derived by one of the inference rules is always smaller than the maximal parent clause, which is the major reason for our particular choice of the clause ordering $>^c$.

In the following proof, we use the model construction technique of the previous section.

Given a consistent set S of ground (equational) clauses, let S^+ be the set $\{\mathcal{A} \to \mathcal{B} \in S \mid \mathcal{B}$ contains the maximal element of $\mathcal{A} \cup \mathcal{B}\}$. We shall construct a minimal model of S^+ in the following way: Starting with $X_0 = \{s \approx t \mid s \approx t$ occurs maximally in a clause of $S^+\}$, we construct a sequence X_0, $X_1, \ldots, X_\alpha, \ldots$ by removing from each X_α the smallest *redundant* equation $s \approx t$. A clause $C = \mathcal{A} \to \mathcal{B}, e$ with maximal atom e is *redundant* in some X_α, iff C is satisfied by the interpretation $\Im_e := \{e' \in X_\alpha \mid e > e'\}^*$ or if there is a clause $C' = \mathcal{A}' \to \mathcal{B}', e$ with $C' < C$ that is not satisfied by $\Im_e$. An equation $s \approx t$ is redundant in X_α, if f s is reducible by $X_\alpha - \{s \approx t\}$ or every clause of S^+ containing $s \approx t$ as a maximal atom is redundant in X_α. Formally, we have:

$$X_{\alpha+1} = X_\alpha - \{e_\alpha\}, \text{ where } e_\alpha = \min\{e \in X_\alpha \mid e \text{ is redundant in } X_\alpha\}$$

We thus obtain $\mathfrak{R} := \bigcap X_\alpha$. From the construction immediately follows that $\mathfrak{R}$is a left-reduced, hence convergent equational system.

1 Lemma *An equation e or a clause $C = \mathcal{A} \to \mathcal{B}, e$ with maximal atom e is redundant in some X_α with $e_\alpha > e$ iff it is redundant in every X_β with $\beta > \alpha$ iff it is redundant in $\mathfrak{R}$.* □

Consequently, we shall simply speak of redundancy without referring to a particular X_α. Obviously, the interpretation $\mathfrak{R}^*$ satisfies each redundant clause. In the following, we assume that S is relatively closed under I, that is, each result of an inference step of I with premises in S is in S or redundant in S.

2 Lemma *For each $s \approx t \in \mathfrak{R}$, there exists a clause $C = \mathcal{A} \to \mathcal{B}, s \approx t$ in S^+, such that*

(i) *$s \approx t$ is maximal in C and*

(ii) *$\mathcal{A} \subseteq \mathfrak{R}^*$ and $\mathcal{B} \cap \mathfrak{R}^* = \emptyset$ holds.*

Proof. Let $s \approx t \in \mathfrak{R}$. Then $s \approx t$ is non-redundant, and in particular s is irreducible by $\mathfrak{R} - \{s \approx t\}$. Moreover, there exists a non-redundant clause $C = \mathcal{A} \to \mathcal{B}, s \approx t$ satisfying (i). We thus can conclude that $\mathcal{A} \subseteq \{u \approx v \in \mathfrak{R} \mid s \approx t > u \approx v\}^* \subseteq \mathfrak{R}^*$ holds. In order to prove the second part of (ii), assume there is an equation $s' \approx t'$ in $\mathcal{B} \cap \mathfrak{R}^*$. Since C is non-redundant, we have $s' \approx t' \notin \{u \approx v \in \mathfrak{R} \mid s \approx t > u \approx v\}^*$. The system $\mathfrak{R}$ is convergent, hence $s \not> s'$. As the ordering $>$ is assumed to be total and $s \approx t$ is maximal in C, we obtain $s = s'$. The set S is relatively closed under equality factoring and thus the clause $D = \mathcal{A}, t \approx t' \to \mathcal{B}', s \approx t'$ is in S or redundant in S. If D is redundant in S, then the interpretation $\{u \approx v \in \mathfrak{R} \mid s \approx t' > u \approx v\}^*$ satisfies D, hence also C, which implies that C is redundant in S, too, which is a contradiction. The clause D is thus non-redundant. We can assume without loss of generality that $s \approx t'$ is maximal in D. The equations $s \approx t$ and $s \approx t'$ are both in $\mathfrak{R}^*$, hence also $t \approx t' \in \mathfrak{R}^*$. This implies $s \approx t' \in \mathfrak{R}$, contradicting the irreducibility of $s \approx t$. We now have proved the second half of (ii), thus concluding the proof of the lemma. □

3 Theorem *The interpretation $\mathfrak{I} := \mathfrak{R}^*$ satisfies S.*

Proof. Let $C = \mathcal{A} \to \mathcal{B}$ be a minimal clause, such that $\mathfrak{I}$ does not satisfy C, and let $s \approx t$ be the maximal atom in $\mathcal{A} \cup \mathcal{B}$.

Case 1: $C \in S^+$. Then $s \approx t \in \mathcal{B}$, and from $\mathcal{B} \cap \mathfrak{I} = \emptyset$ follows $s \approx t \notin \mathfrak{I}$. From the construction of $\mathfrak{I}$ we can conclude that s is reducible by some equation $u \approx v \in \mathfrak{R}$ with $s \approx t > u \approx v$. Let $D = \mathcal{A}' \to \mathcal{B}', u \approx v$ be a clause in S^+, such that $u \approx v$ is maximal in $\mathcal{A}' \cup \mathcal{B}'$ and $\mathcal{A}' \subseteq \mathfrak{I}$ and $\mathcal{B}' \cap \mathfrak{I} = \emptyset$ hold. Then the *superposition right* rule applies to C and D, yielding a clause

$$R = \mathcal{A}, \mathcal{A}' \to \mathcal{B} - \{s \approx t\}, \mathcal{B}', s[v] \approx t$$

It is easy to check that $\mathfrak{I}$ does not satisfy R, either. Hence R is not redundant in S, and by the closedness of S, $R \in S$ holds. Moreover, R is smaller than C, which contradicts the choice of C.

Case 2: $C \in S - S^+$. In this case, we have $s \approx t \in \mathcal{A}$, and from $\mathcal{A} \subseteq \mathfrak{I}$ follows $s \approx t \in \mathfrak{I}$. If s is reducible by some equation $u \approx v \in \mathfrak{R}$, then we can—similarly to case 1—infer the existence of a clause $R < C$, derived from C by an application of the *superposition left* rule, such that $\mathfrak{I}$ does not satisfy R. We can thus assume that s is irreducible by the convergent rewrite system $\mathfrak{R}$. From $s \approx t \in \mathfrak{R}^*$ thus follows $s \not> t$, which in turn implies $s = t$. Now the equality resolution rule applies to C yielding the clause $C' := \mathcal{A} - \{t \approx t\} \to \mathcal{B}$. Again, $\mathfrak{I}$ does not satisfy C', which is smaller than C, thus contradicting the choice of C.

In both cases, we obtain a contradiction to the minimality of C, which proves that $\mathfrak{I}$ satisfies every clause in S. □

In fact, all we used in this completeness proof are the following closure properties of S:

(C1) S is relatively closed under equality resolution and equality factoring.

(C2) If S contains clauses $C = \mathcal{A} \to \mathcal{B}, u \approx v$, and D, such that D contains an atom $s[u] \approx t$ in the antecedent or in the succedent, then there exists a clause R in S, such that (i) $D < R$, and (ii) if $\mathfrak{I}$ is an interpretation that satisfies $u \approx v$ and falsifies both $\mathcal{A} \to \mathcal{B}$ and D, then it falsifies R, too.

Bachmair & Ganzinger [BG] provide another characterization of redundant clauses. They define a ground clause C to be *composite* in a set S of ground clauses, if $\{C\} > S$ and $S \models C$ both hold.

4 Lemma *If $C$is composite in S, then it is redundant in S.*

Proof. Let $C = \mathcal{A} \to \mathcal{B}, s \approx t$, such that $s \approx t$ is maximal in C. There is a subset S' of S with $\{C\} > S'$ and $S' \models C$. Suppose all clauses $C' < C$ with maximal atom $s \approx t$ are satisfied by $\mathfrak{I}' := \{u \approx v \in \mathfrak{R} \mid s$

$\approx t > u \approx v\}^*$. From the proof of theorem 3, it is easy to see that $\Im'$ satisfies each clause in S with maximal atom smaller than $s \approx t$. The interpretation $\Im'$ thus satisfies every clause smaller than C, and in particular, $\Im'$ satisfies S'. From $S' \models C$ follows that $\Im'$ satisfies C, which implies the assertion of the lemma. □

4 Another Model Construction

While the model construction technique described in the previous sections uses a *minimizing* procedure, it is also possible to construct an equational model for a consistent and closed set of clauses in a more traditional *incremental* fashion.

Let S be a consistent set of ground equational clauses that is closed under the inference system I. Let $A = \{t_1, t_2, \ldots, t_\alpha, \ldots\}$ be the set of terms occurring in clauses of S. For any clause C, let maxterm(C) be the maximal term occurring in equational atoms of C. Moreover, let $S^\alpha = \{C \in S \mid \text{maxterm}(C) \leq t_\alpha\}$.

We define a clause $C := \mathcal{A} \rightarrow \mathcal{B}, s \approx t$ with $s \approx t$ maximal in C to be *regular* w.r.t. the interpretation $\Im$, iff (i) $\Im$ satisfies C and (ii) $\mathcal{A} \subseteq \Im$ and $\mathcal{B} \cap \Im = \emptyset$.

5 Lemma *Let C and D be clauses with $C < D$, such that C is regular w.r.t. the interpretation $\Im$, and let R be the result of a superposition step of C and D. If $\Im$ satisfies R, then it satisfies D, too.*

Proof. Let $C = \mathcal{A} \rightarrow \mathcal{B}, s \approx t$ with $s \approx t$ maximal in C, and let $D = \mathcal{A}' \rightarrow \mathcal{B}', u \approx v$ with $u \approx v$ maximal in D. From the assumption of the lemma follows $u = u[s]$. We have $R = \mathcal{A}, \mathcal{A}' \rightarrow \mathcal{B}, \mathcal{B}', u[t] \approx v$. Suppose $\Im$ does not satisfy D. Then $\mathcal{A} \cup \mathcal{A}' \subseteq \Im$ and $(\mathcal{B} \cup \mathcal{B}') \cap \Im = \emptyset$ and from $u[s] \approx v \notin \Im$ and $s \approx t \in \Im$ follows $u[t] \approx v \notin \Im$. Altogether, $\Im$ does not satisfy R either.

The case where the maximal atom $u \approx v$ occurs in the antecedent of D is treated analogously. □

We define inductively sets $\Re_0 \subseteq \Re_1 \subseteq \ldots \subseteq \Re_a \subseteq \ldots$, $a \in A$, and $\Im_\alpha := \Re^*_\alpha$ by $\Re_0 = \emptyset$ and:

$$\Re_{\alpha+1} = \begin{cases} \Re_\alpha, & \text{if } \Im_\alpha \models S^{\alpha+1} \\ \Re_\alpha \cup \{t_{\alpha+1} \approx s\}, & \text{where } s \text{ is the smallest term with } (\Re_\alpha \cup \{t_{\alpha+1} \approx s\})^* \models S^{\alpha+1} \end{cases}$$

for successor ordinals, and $\Re_\alpha = \bigcup_{\beta<\alpha} \Re_\beta$ for limit ordinals. In order to ensure that $\Re_a$ is well-defined, we have to prove that there always exists a term s, such that $\Im_\alpha \cup \{t_{\alpha+1} \approx s\}$ satisfies $S^{\alpha+1}$, provided that $\Im_\alpha$ satisfies S^α and does not satisfy $S^{\alpha+1}$.

6 Lemma *For every α, the following holds*

a) $\Re_\alpha$ *is a left-reduced rewrite system*

b) *If α is a successor ordinal and $\Im_{\alpha-1}$ does not satisfy S^α, then S^α contains a regular clause with maximal atom $t_\alpha \approx s$.*

c) *If α is a successor ordinal and $\Im_{\alpha-1}$ does not satisfy S^α, then* $(\Re_\alpha \cup \{t_\alpha \approx s\})^* \models S^\alpha$

Proof. By transfinite induction on α. If α is a limit ordinal, then $\Re_\beta$ is left-reduced for each $\beta < \alpha$, hence $\Re_\alpha = \bigcup_{\beta<\alpha} \Re_\beta$ is left-reduced. Now suppose α is a successor ordinal. Let $t := t_\alpha$ and let D be a minimal clause in S^α, such that $\Im_{\alpha-1}$ does not satisfy D. Since $\Im_{\alpha-1}$ satisfies $S^{\alpha-1}$ by induction hypothesis, we have $D \in S^\alpha - S^{\alpha-1}$, that is, D contains an equation of the form $t \approx s$ as a maximal occurrence.

a) Assume that t is reducible by $\Re_{\alpha-1}$. Then $t \approx t[u]$, $u < t$, and there is an equation $u \approx v$ in $\Re_{\alpha-1}$. By induction hypothesis, there exists a regular clause $C \in S$, such that $u \approx v$is maximal in C. Then a superposition step applies to C and D, yielding a clause $R < D$. By lemma 5, $\Im_{\alpha-1}$ does not satisfy R, which is a contradiction to the minimality of D. This proves that t is irreducible by $\Re_{\alpha-1}$ and using the induction hypothesis, we can conclude that $\Re_\alpha$ is a left-reduced system.

b) We show that D is regular w.r.t. $\mathfrak{I}_\alpha$. First, condition (i) is trivially satisfied. Assume, $t \approx s$ occurs in the antecedent of D. Then we have $t \approx s \in \mathfrak{I}_{\alpha-1}$. As $\mathfrak{R}_\alpha$ is left-reduced, hence convergent, we can infer $t = s$. Then an equational resolution step applies to D, yielding a clause $D' < D$, such that $\mathfrak{I}_{\alpha\text{-}1}$ does not satisfy C', contradicting the minimality of D. This shows that $t \approx s$ occurs in the succedent of D. Let $D = \mathcal{A} \rightarrow \mathcal{B}, t \approx s$. As $\mathfrak{I}_{\alpha-1}$ does not satisfy D, we have $\mathcal{A} \subseteq \mathfrak{I}_{\alpha-1} \subseteq \mathfrak{I}_\alpha$. Assume that $\mathcal{B} \cap \mathfrak{I}_\alpha \neq \emptyset$. As $\mathcal{B} \cap \mathfrak{I}_{\alpha-1} = \emptyset$, $\mathcal{B}$ contains an equation $u \approx v$ with $u \approx v \in \mathfrak{I}_\alpha - \mathfrak{I}_{\alpha-1}$. Since $\mathfrak{R}_\alpha$ is a convergent rewrite system, there is a term u' with $u \rightarrow_{\mathfrak{R}_\alpha} u'$ and $v \rightarrow_{\mathfrak{R}_\alpha} u'$. If $u < t$, then obviously $u \rightarrow_{\mathfrak{R}_{\alpha-1}} u'$ and $v \rightarrow_{\mathfrak{R}_{\alpha-1}} u'$ hold, contradicting the fact that $u \approx v \notin \mathfrak{I}_{\alpha-1}$. Hence $u = t$, and D is of the form $\mathcal{A} \rightarrow \mathcal{B}, t \approx v, t \approx s$. Then the equality factoring rule applies to D, yielding a clause $D' = \mathcal{A}, s \approx v \rightarrow \mathcal{B}, t \approx s$ with $D' < D$. Moreover, from $t \approx s \in \mathfrak{I}_\alpha$ and $t \approx v \in \mathfrak{I}_\alpha$ follows $s \approx v \in \mathfrak{I}_\alpha$, and since $s < t$, we obtain $s \approx v \in \mathfrak{I}_{\alpha-1}$. This shows that $\mathfrak{I}_{\alpha-1}$ cannot satisfy D', which contradicts the minimality of D. Hence $\mathcal{B} \cap \mathfrak{I}_\alpha = \emptyset$ holds, thus concluding the proof of b).

c) Let C be a minimal clause in S^α, such that $\mathfrak{I}_\alpha$ does not satisfy C. Since $\mathfrak{I}_\alpha$ satisfies $S^{\alpha-1}$, C contains an equation of the form $t \approx s'$ in the antecedent or in the succedent as a maximal occurrence. Then a superposition step applies to C and D yielding a clause $R < C$. Again, $\mathfrak{I}_\alpha$ does not satisfy C, contradicting the choice of C. This proves that $\mathfrak{I}_\alpha$ satisfies S^α. □

From the previous lemma follows immediately that the interpretation $\mathfrak{I} := \bigcup_\alpha \mathfrak{I}_\alpha$ is a model of S.

(E-)Semantic trees [Pe, Ro, HR] are a well-known means to prove completeness of resolution and superposition calculi. They also serve to illustrate the model construction technique described in this chapter. Given a set A of (equational) atoms that is ordered by a well-founded ordering $>$, a *partial (equational) interpretation* $\mathfrak{I}_{A_e}$ of A is an (equational) interpretation over an initial segment $A_e = \{e' \in A \mid e' < e\}$ of A. We define a well-founded ordering $>_I$ on the class of partial interpretations of A by

$$\mathfrak{I}_{A''} >_I \mathfrak{I}_{A'} \text{ iff } A' \subset A'' \text{ and } \mathfrak{I}_{A''} \cap A' = \mathfrak{I}_{A'}$$

The collection of all partial (equational) interpretations of A together with the ordering $>_I$ is called the (E-)semantic tree for A. If $\mathfrak{I}_{A'}$ is a successor of $\mathfrak{I}_{A''}$ w.r.t. $>_I$, then we call $\mathfrak{I}_{A'}$ the *right* successor of $\mathfrak{I}_{A''}$, iff $\mathfrak{I}_{A''} = \mathfrak{I}_{A'}$, and the *left* successor, iff $\mathfrak{I}_{A''} \subset \mathfrak{I}_{A'}$. An interpretation of A can be thought of as a maximal path in the semantic tree. Let S be a set of clauses over A. Let A' be a node in the semantic tree, and let t_α be the maximal term occurring in A'. Then A' is called a *failure node* w.r.t. S, if the corresponding partial interpretation $\mathfrak{I}_{A'}$ does not satisfy S^α, and if no ancestor node of A' is a failure node. The construction of a model for a clause set S can be seen as the construction of a maximal path in the semantic tree that does not contain a failure node w.r.t. S.

Our construction proceeds in the following way: Having constructed a path $\mathfrak{I}_{A'}$ without a failure node, we choose the rightmost successor of $\mathfrak{I}_{A'}$, if this is not a failure node. If, however, it is a failure node, then there exists a leftmost successor of $\mathfrak{I}_{A'}$, and by lemma 6, this node is not a failure node. Continuing this way, we obtain a maximal path in the semantic tree. This construction is illustrated by figure 1. Failure nodes of the semantic tree are squared.

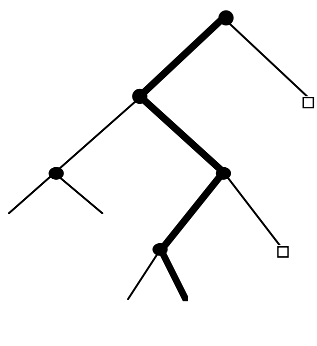

fig. 1

The role of *composite* clauses in the context of semantic trees is clarified by the observation that a partial interpretation $\mathfrak{I}$ falsifying a clause C that is composite in S, falsifies some clause in S. Any failure node w.r.t. $\{C\}$ is a failure node w.r.t. S, and removal of redundant clauses thus preserves the failure nodes in the semantic tree.

5 Theorem Proving for First-Order Logic

In the previous sections we have proved various calculi to be refutational complete for sets of *ground clauses*. Completeness of these calculi for arbitrary first-order clauses can be proved as follows: Let S be a consistent set of first-order clauses that is closed under an inference system I, and let $\overline{S}$ be the set of all ground instances of clauses in S. We use a lifting lemma to show that $\overline{S}$ satisfies a certain closure property w.r.t. I. Then by the completeness of I for ground clauses, we can infer the existence of a model for $\overline{S}$, which in turn is a model for S, too. To show completeness of first-order resolution with factorization, for instance, it is sufficient to show that for any set S that is closed under resolution and factorization, the set $\overline{S}$ is closed, too, which is accomplished by an application of the lifting lemma. For equational reasoning, things are slightly more complicated. We shall use the following inference system I for first-order (equational) clauses.

Equality resolution: $$\frac{\mathcal{A},\, t \approx t' \to \mathcal{B}}{\mathcal{A}\sigma \to \mathcal{B}\sigma}$$

where σ is a most general unifier for t and t' and $t\sigma \approx t'\sigma$ is a maximal occurrence in $\mathcal{A}\sigma,\, t\sigma \approx t'\sigma \to \mathcal{B}\sigma$.

Superposition left: $$\frac{\mathcal{A} \to \mathcal{B},\, s \approx t \quad \mathcal{A}',\, u[s'] \approx v \to \mathcal{B}'}{\mathcal{A}\sigma,\, \mathcal{A}'\sigma,\, u[t]\sigma \approx v\sigma \to \mathcal{B}\sigma,\, \mathcal{B}'\sigma}$$

where (i) σ is a most general unifier for s and s', (ii) $s\sigma \approx t\sigma$ is a maximal occurrence in $\mathcal{A}\sigma \to \mathcal{B}\sigma,\, s\sigma \approx t\sigma$, (iii) $u\sigma \approx v\sigma$ is a maximal occurrence in $\mathcal{A}'\sigma,\, u\sigma \approx v\sigma \to \mathcal{B}'\sigma$, and (iv) s' is not a variable.

Superposition right: $$\frac{\mathcal{A} \to \mathcal{B},\, s \approx t \quad \mathcal{A}' \to \mathcal{B}',\, u[s'] \approx v}{\mathcal{A}\sigma,\, \mathcal{A}'\sigma \to \mathcal{B}\sigma,\, \mathcal{B}'\sigma,\, u[t]\sigma \approx v\sigma}$$

where (i) σ is a most general unifier for s and s', (ii) $s\sigma \approx t\sigma$ is a maximal occurrence in $\mathcal{A}\sigma \to \mathcal{B}\sigma,\, s\sigma \approx t\sigma$, (iii) $u\sigma \approx v\sigma$ is a maximal occurrence in $\mathcal{A}'\sigma \to \mathcal{B}'\sigma,\, u\sigma \approx v\sigma$, and (iv) s' is not a variable.

Equality factoring: $$\frac{\mathcal{A} \to \mathcal{B},\, s \approx t,\, s' \approx t'}{\mathcal{A}\sigma,\, t\sigma \approx t'\sigma \to \mathcal{B}\sigma,\, s\sigma \approx t'\sigma}$$

where (i) σ is a most general unifier for s and s', (ii) $s\sigma \approx t\sigma$ is a maximal occurrence in $\mathcal{A}\sigma \to \mathcal{B}\sigma,\, s\sigma \approx t\sigma,\, s'\sigma \approx t\sigma$.

The notion of redundancy is generalized to first-order clauses in the following way: A clause C is redundant in a set S, iff each ground instance of C is redundant in the set $\overline{S}$ of all ground instances of clauses in S.

In the following, we shall show that given a set S of first-order (equational) clauses that is relatively closed under I, the set $\overline{S}$ satisfies properties (C1) and (C2). First, S is relatively closed under equational resolution and equality factoring. Suppose, the clause $C\sigma \in \overline{S}$ is the premise of an equational resolution or equality factoring step yielding a clause D'. Then an appropriate inference step applies to the clause C resulting in some clause D with $D' = D\sigma$. If $D \in S$, then $D' \in \overline{S}$. Otherwise, if D is redundant in S, then D' is redundant in $\overline{S}$. Hence $\overline{S}$ satisfies (C1).

Now suppose, $\overline{S}$ contains clauses $C\sigma = \mathcal{A}\sigma \to \mathcal{B}\sigma,\, u\sigma \approx v\sigma$, and $D\sigma$, such that $D\sigma$ contains an atom $s\sigma[u'\sigma] \approx t\sigma$ with $u\sigma = u'\sigma$. If u' is not a variable, then an application of the lifting lemma shows the existence of a clause R, which is the result of a superposition step of C and D. Now R is in

S or redundant in S, hence $R\sigma$ is in $\overline{S}$ or redundant in $\overline{S}$. Consequently, $\overline{S}$ satisfies property (C2). If, however, u' is a variable, then the clause $D\overline{\sigma}$ is in $\overline{S}$, where $\overline{\sigma}$ is defined by

$$x\overline{\sigma} = \begin{cases} x\sigma, \text{ if } x \neq u' \\ v\sigma, \text{ if } x = u' \end{cases}$$

Now the clause $D\overline{\sigma}$ satisfies condition (C2).

References

[Be] Bezem, M. Completeness of Resolution Revisited. *Theoretical Computer Science* **74** (1990) 227-237.

[BG] Bachmair, L. & Ganzinger, H. Rewrite-Based Equational Theorem Proving With Selection and Simplification. Technical Report MPI-I-91-208, Max-Planck-Institut f. Informatik, Saarbrücken 1991.

[Hu] Huet, G. Confluent Reductions: Abstract Properties and Applications to Term Rewriting Systems. *JACM*, **27/4** (1980), 797-821.

[Ru] Rusinowitch, M. Theorem Proving with resolution and superposition: An extension of the Knuth and Bendix procedure as a complete set of inference rules. *J. of Symbolic Computation* **11** (1991).