First-Order Logic with Equality

In this Chapter I combine the ideas of Superposition for first-order logic without equality, Section 3.13, and Knuth-Bendix Completion, Section 4.4, to get a calculus for equational clauses.

Recall that predicative literals can be translated into equations

$$
\begin{array}{lcl}
P(t_1, \ldots, t_n) & \Rightarrow & f_P(t_1, \ldots, t_n) \approx \mathsf{true} \\
\neg P(t_1, \ldots, t_n) & \Rightarrow & f_P(t_1, \ldots, t_n) \not\approx \mathsf{true}
\end{array}
$$

Some Motivation

The running example for this chapter is the theory of arrays $\mathcal{T}_{\text{Array}}$, see also Section 7.3, which consists of the following three axioms:

$$\forall x_A, y_I, z_V.\ \text{read}(\text{store}(x,y,z),y) \approx z$$
$$\forall x_A, y_I, y'_I, z_V.(y \not\approx y' \rightarrow \text{read}(\text{store}(x,y,z),y') \approx \text{read}(x,y'))$$
$$\forall x_A, x'_A.\exists y_I.(\text{read}(x,y) \not\approx \text{read}(x',y) \lor x \approx x').$$

The goal is to decide for an additional set of ground clauses N over the above signature plus further constants of the three different sorts, whether $\mathcal{T}_{\text{Array}} \cup N$ is satisfiable.

The ground Case

The ground inference rules corresponding to Knuth-Bendix critical pair computation generalized to clauses and Superposition Left on first-order logic wihtout equality modulo a reduction ordering $\succ$ that is total on ground terms. Then the construction of Definition 3.12.1 is lifted to equational clauses.

The multiset $\{s, t\}$ is assigned to a positive literal $s \approx t$, the multiset $\{s, s, t, t\}$ is assigned to a negative literal $s \not\approx t$. The *literal ordering* $\succ_L$ compares these multisets using the multiset extension of $\succ$. The *clause ordering* $\succ_C$ compares clauses by comparing their multisets of literals using the multiset extension of $\succ_L$. Eventually $\succ$ is used for all three orderings depending on the context.

Superposition Left

$(N \uplus \{D \vee t \approx t', C \vee s[t] \not\approx s'\}) \;\Rightarrow$
$(N \cup \{D \vee t \approx t', C \vee s[t] \not\approx s'\} \cup \{D \vee C \vee s[t'] \not\approx s'\})$

where $t \approx t'$ is strictly maximal and $s \not\approx s'$ are maximal in their respective clauses, $t \succ t'$, $s \succ s'$

Superposition Right

$(N \uplus \{D \vee t \approx t', C \vee s[t] \approx s'\}) \;\Rightarrow$
$(N \cup \{D \vee t \approx t', C \vee s[t] \approx s'\} \cup \{D \vee C \vee s[t'] \approx s'\})$

where $t \approx t'$ and $s \approx s'$ are strictly maximal in their respective clauses, $t \succ t'$, $s \succ s'$

Equality Resolution $(N \uplus \{C \vee s \not\approx s\}) \;\Rightarrow\; (N \cup \{C \vee s \not\approx s\} \cup \{C\})$

where $s \not\approx s$ is maximal in the clause

Factoring is more complicated due to more complicated partial models. Classical Herbrand interpretation not sufficient because of equality.

The solution is to define a set E of ground equations and take $T(\Sigma, \emptyset)/E = T(\Sigma, \emptyset)/{\approx_E}$ as the universe. Then two ground terms s and t are equal in the interpretation if and only if $s \approx_E t$. If E is a terminating and confluent rewrite system R, then two ground terms s and t are equal in the interpretation, if and only if $s \downarrow_R t$.

Now the problem with the standard factoring rule is that in the completeness proof for the superposition calculus without equality, the following property holds: if $C = C' \lor A$ with a strictly maximal atom A is false in the current interpretation N_C with respect to some clause set, see Definition 3.12.5, then adding A to the current interpretation cannot make any literal in C' true.

This does not hold anymore in the presence of equality. Let $b \succ c \succ d$. Assume that the current rewrite system (representing the current interpretation) contains the rule $c \to d$. Now consider the clause $b \approx c \lor b \approx d$.

Equality Factoring $(N \uplus \{C \vee s \approx t' \vee s \approx t\}) \Rightarrow (N \cup \{C \vee s \approx t' \vee s \approx t\} \cup \{C \vee t \not\approx t' \vee s \approx t'\})$

where $s \succ t'$, $s \succ t$ and $s \approx t$ is maximal in the clause

The lifting from the ground case to the first-order case with variables is then identical to the case of superposition without equality: identity is replaced by unifiability, the mgu is applied to the resulting clause, and $\succ$ is replaced by $\not\preceq$.
An addition, as in Knuth-Bendix completion, overlaps at or below a variable position are not considered. The consequence is that there are inferences between ground instances $D\sigma$ and $C\sigma$ of clauses D and C which are not ground instances of inferences between D and C. Such inferences have to be treated in a special way in the completeness proof and will be shown to be obsolete.

Superposition Right

$(N \uplus \{D \vee t \approx t', C \vee s[u] \approx s'\}) \;\Rightarrow$
$(N \cup \{D \vee t \approx t', C \vee s[u] \approx s'\} \cup \{(D \vee C \vee s[t'] \approx s')\sigma\})$

where σ is the mgu of t, u, u is not a variable $t\sigma \not\preceq t'\sigma$, $s\sigma \not\preceq s'\sigma$, $(t \approx t')\sigma$ strictly maximal in $(D \vee t \approx t')\sigma$, nothing selected and $(s \approx s')\sigma$ maximal in $(C \vee s \approx s')\sigma$ and nothing selected

Superposition Left

$(N \uplus \{D \vee t \approx t', C \vee s[u] \not\approx s'\}) \;\Rightarrow$
$(N \cup \{D \vee t \approx t', C \vee s[u] \not\approx s'\} \cup \{(D \vee C \vee s[t'] \not\approx s')\sigma\})$

where σ is the mgu of t, u, u is not a variable $t\sigma \not\preceq t'\sigma$, $s\sigma \not\preceq s'\sigma$, $(t \approx t')\sigma$ strictly maximal in $(D \vee t \approx t')\sigma$, nothing selected and $(s \not\approx s')\sigma$ maximal in $(C \vee s \not\approx s')\sigma$ or selected

Equality Resolution $(N \uplus \{C \vee s \not\approx s'\}) \;\Rightarrow\; (N \cup \{C \vee s \not\approx s'\} \cup \{C\sigma\})$

where σ is the mgu of s, s', $(s \not\approx s')\sigma$ maximal in $(C \vee s \not\approx s')\sigma$ or selected

Equality Factoring $(N \uplus \{C \vee s' \approx t' \vee s \approx t\}) \;\Rightarrow\; (N \cup \{C \vee s' \approx t' \vee s \approx t\} \cup \{(C \vee t \not\approx t' \vee s \approx t')\sigma\})$

where σ is the mgu of s, s', $s'\sigma \not\prec t'\sigma$, $s\sigma \not\prec t\sigma$, $(s \approx t)\sigma$ maximal in $(C \vee s' \approx t' \vee s \approx t)\sigma$ and nothing selected

5.2.1 Theorem (Superposition Soundness)

All inference rules of the superposition calculus are *sound*, i.e., for every rule $N \uplus \{C_1, \ldots, C_n\} \Rightarrow N \cup \{C_1, \ldots, C_n\} \cup \{D\}$ it holds that $\{C_1, \ldots, C_n\} \models D$.

5.2.2 Definition (Abstract Redundancy)

A clause C is *redundant* with respect to a clause set N if for all ground instances $C\sigma$ there are clauses $\{C_1, \ldots, C_n\} \subseteq N$ with ground instances $C_1\tau_1, \ldots, C_n\tau_n$ such that $C_i\tau_i \prec C\sigma$ for all i and $C_1\tau_1, \ldots, C_n\tau_n \models C\sigma$.
Given a set N of clauses $\text{red}(N)$ is the set of clauses redundant with respect to N.

5.2.3 Definition (Saturation)

A clause set N is *saturated up to redundancy* if for every derivation $N \setminus \mathrm{red}(N) \Rightarrow_{\mathrm{SUPE}} N \cup \{C\}$ it holds $C \in (N \cup \mathrm{red}(N))$.

5.2.4 Definition (Partial Model Construction)

Given a clause set N and an ordering $\succ$ a (partial) model $N_\mathcal{I}$ can be constructed inductively over all ground clause instances of N as follows:

$$N_C \quad := \quad \bigcup_{D \prec C}^{D \in \text{grd}(\Sigma,N)} E_D$$

$$N_\mathcal{I} \quad := \quad \bigcup_{C \in \text{grd}(\Sigma,N)} N_C$$

where N_D, $N_\mathcal{I}$, E_D are also considered as rewrite systems with respect to $\succ$. If $E_D \neq \emptyset$ then D is called *productive*.

$$E_D \quad := \quad \begin{cases} \{s \approx t\} & \text{if } D = D' \vee s \approx t, \\ & (i)\ s \approx t \text{ is strictly maximal in } D \\ & (ii)\ s \succ t \\ & (iii)\ D \text{ is false in } N_D \\ & (iv)\ D' \text{ is false in } N_D \cup \{s \to t\} \\ & (v)\ s \text{ is irreducible by } N_D \\ & (vi) \text{ no negative literal is selected in } D' \\ \emptyset & \text{otherwise} \end{cases}$$

5.2.5 Lemma (Maximal Terms in Productive Clauses)

If $E_C = \{s \to t\}$ and $E_D = \{l \to r\}$, then $s \succ l$ if and only if $C \succ D$.

5.2.6 Corollary (Partial Models are Convergent Rewrite Systems)

The rewrite systems N_C and $N_{\mathcal{I}}$ are convergent.

5.2.7 Lemma (Ordering Consequences in Productive Clauses)

If $D \preceq C$ and $E_C = \{s \rightarrow t\}$, then $s \succ r$ for every term r occurring in a negative literal in D and $s \succeq l$ for every term l occurring in a positive literal in D.

5.2.8 Corollary (Model Monotonicity True Clauses)

If D is true in N_D, then D is true in $N_\mathcal{I}$ and N_C for all $C \succ D$.

5.2.9 Corollary (Model Monotonicity False Clauses)

If $D = D' \vee s \approx t$ is productive, then D' is false and D is true in $N_{\mathcal{I}}$ and N_C for all $C \succ D$.

5.2.10 Lemma (Lifting Single Clause Inferences)

Let C be a clause and let σ be a substitution such that $C\sigma$ is ground. Then every equality resolution or equality factoring inference from $C\sigma$ is a ground instance of an inference from C.

5.2.11 Lemma (Lifting Two Clause Inferences)

Let $D = D' \vee u \approx v$ and $C = C' \vee [\neg]s \approx t$ be two clauses (without common variables) and let σ be a substitution such that $D\sigma$ and $C\sigma$ are ground. If there is a superposition inference between $D\sigma$ and $C\sigma$ where $u\sigma$ and some subterm of $s\sigma$ are overlapped and $u\sigma$ does not occur in $s\sigma$ at or below a variable position of s then the inference is a ground instance of a superposition inference from D and C.

5.2.12 Theorem (Model Construction)

Let N be a set of clauses that is saturated up to redundancy and does not contain the empty clause. Then for every ground clause $C\sigma \in \text{grd}(\Sigma, N)$ it holds that:

1. $E_{C\sigma} = \emptyset$ if and only if $C\sigma$ is true in $N_{C\sigma}$.
2. If $C\sigma$ is redundant with respect to $\text{grd}(\Sigma, N)$ then it is true in $N_{C\sigma}$.
3. $C\sigma$ is true in $N_{\mathcal{I}}$ and in N_D for every $D \in \text{grd}(\Sigma, N)$ with $D \succ C\sigma$.

5.2.13 Lemma (Lifting Models)

Let N be a set of clauses with variables and let $\mathcal{A}$ be a term-generated Σ-algebra. Then $\mathcal{A}$ is a model of $\operatorname{grd}(\Sigma, N)$ if and only if it is a model of N.

5.2.14 Theorem (Refutational Completeness: Static View)

Let N be a set of clauses that is saturated up to redundancy. Then N has a model if and only if N does not contain the empty clause.