Unification

3.7.1 Definition (Unifier)

Two terms *s* and *t* of the same sort are said to be *unifiable* if there exists a well-sorted substitution σ so that $s\sigma = t\sigma$, the substitution σ is then called a well-sorted *unifier* of *s* and *t*.

The unifier σ is called *most general unifier*, written $\sigma = mgu(s, t)$, if any other well-sorted unifier τ of *s* and *t* it can be represented as $\tau = \sigma\tau'$, for some well-sorted substitution τ'.

A state of the naive standard unification calculus is a set of equations E or $\bot$, where $\bot$ denotes that no unifier exists. The set E is also called a *unification problem*.

The start state for checking whether two terms s, t, $\mathrm{sort}(s) = \mathrm{sort}(t)$, (or two non-equational atoms A, B) are unifiable is the set $E = \{s = t\}$ ($E = \{A = B\}$). A variable x is *solved* in E if $E = \{x = t\} \uplus E'$, $x \notin \mathrm{vars}(t)$ and $x \notin \mathrm{vars}(E)$.

A variable $x \in \mathrm{vars}(E)$ is called *solved* in E if $E = E' \uplus \{x = t\}$ and $x \notin \mathrm{vars}(t)$ and $x \notin \mathrm{vars}(E')$.

Standard (naive) Unification

Tautology $E \uplus \{t = t\} \;\Rightarrow_{\mathrm{SU}}\; E$

Decomposition $E \uplus \{f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)\} \;\Rightarrow_{\mathrm{SU}}$
$E \cup \{s_1 = t_1, \ldots, s_n = t_n\}$

Clash $E \uplus \{f(s_1, \ldots, s_n) = g(s_1, \ldots, s_m)\} \;\Rightarrow_{\mathrm{SU}}\; \bot$
if $f \neq g$

Substitution $E \uplus \{x = t\} \Rightarrow_{\mathrm{SU}} E\{x \mapsto t\} \cup \{x = t\}$

if $x \in vars(E)$ and $x \notin vars(t)$

Occurs Check $E \uplus \{x = t\} \Rightarrow_{\mathrm{SU}} \bot$

if $x \neq t$ and $x \in vars(t)$

Orient $E \uplus \{t = x\} \Rightarrow_{\mathrm{SU}} E \cup \{x = t\}$

if $t \notin \mathcal{X}$

3.7.2 Theorem (Soundness, Completeness and Termination of $\Rightarrow_{\mathrm{SU}}$)

If s, t are two terms with $\mathrm{sort}(s) = \mathrm{sort}(t)$ then

1. if $\{s = t\} \Rightarrow^*_{\mathrm{SU}} E$ then any equation $(s' = t') \in E$ is well-sorted, i.e., $\mathrm{sort}(s') = \mathrm{sort}(t')$.
2. $\Rightarrow_{\mathrm{SU}}$ terminates on $\{s = t\}$.
3. if $\{s = t\} \Rightarrow^*_{\mathrm{SU}} E$ then σ is a unifier (mgu) of E iff σ is a unifier (mgu) of $\{s = t\}$.
4. if $\{s = t\} \Rightarrow^*_{\mathrm{SU}} \bot$ then s and t are not unifiable.
5. if $\{s = t\} \Rightarrow^*_{\mathrm{SU}} \{x_1 = t_1, \ldots, x_n = t_n\}$ and this is a normal form, then $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ is an mgu of s, t.

Size of Unification Problems

Any normal form of the unification problem E given by

$$\{f(x_1, g(x_1, x_1), x_3, \ldots, g(x_n, x_n)) = f(g(x_0, x_0), x_2, g(x_2, x_2), \ldots, x_{n+1})\}$$

with respect to $\Rightarrow_{\mathrm{SU}}$ is exponentially larger than E.

Polynomial Unification

The second calculus, polynomial unification, prevents the problem of exponential growth by introducing an implicit representation for the mgu.

For this calculus the size of a normal form is always polynomial in the size of the input unification problem.

Tautology $E \uplus \{t = t\} \;\Rightarrow_{\text{PU}}\; E$

Decomposition $E \uplus \{f(s_1, \ldots, s_n) = f(t_1, \ldots, t_n)\} \;\Rightarrow_{\text{PU}}$
$E \uplus \{s_1 = t_1, \ldots, s_n = t_n\}$

Clash $E \uplus \{f(t_1, \ldots, t_n) = g(s_1, \ldots, s_m)\} \;\Rightarrow_{\text{PU}}\; \bot$
if $f \neq g$

Occurs Check $E \uplus \{x = t\} \Rightarrow_{\text{PU}} \bot$

if $x \neq t$ and $x \in \mathit{vars}(t)$

Orient $E \uplus \{t = x\} \Rightarrow_{\text{PU}} E \uplus \{x = t\}$

if $t \notin \mathcal{X}$

Substitution $E \uplus \{x = y\} \Rightarrow_{\text{PU}} E\{x \mapsto y\} \uplus \{x = y\}$

if $x \in \mathit{vars}(E)$ and $x \neq y$

Cycle $E \uplus \{x_1 = t_1, \ldots, x_n = t_n\} \Rightarrow_{\text{PU}} \bot$

if there are positions p_i with $t_i|_{p_i} = x_{i+1}, t_n|_{p_n} = x_1$ and some $p_i \neq \epsilon$

Merge $E \uplus \{x = t, x = s\} \Rightarrow_{\text{PU}} E \uplus \{x = t, t = s\}$

if $t, s \notin \mathcal{X}$ and $|t| \leq |s|$

3.7.4 Theorem (Soundness, Completeness and Termination of $\Rightarrow_{\text{PU}}$)

If s, t are two terms with $\text{sort}(s) = \text{sort}(t)$ then

1. if $\{s = t\} \Rightarrow^*_{\text{PU}} E$ then any equation $(s' = t') \in E$ is well-sorted, i.e., $\text{sort}(s') = \text{sort}(t')$.
2. $\Rightarrow_{\text{PU}}$ terminates on $\{s = t\}$.
3. if $\{s = t\} \Rightarrow^*_{\text{PU}} E$ then σ is a unifier (mgu) of E iff σ is a unifier (mgu) of $\{s = t\}$.
4. if $\{s = t\} \Rightarrow^*_{\text{PU}} \bot$ then s and t are not unifiable.

3.7.5 Theorem (Normal Forms Generated by $\Rightarrow_{\text{PU}}$)

Let $\{s = t\} \Rightarrow^*_{\text{PU}} \{x_1 = t_1, \ldots, x_n = t_n\}$ be a normal form. Then

1. $x_i \neq x_j$ for all $i \neq j$ and without loss of generality $x_i \notin \text{vars}(t_{i+k})$ for all i, k, $1 \leq i < n$, $i + k \leq n$.
2. the substitution $\{x_1 \mapsto t_1\}\{x_2 \mapsto t_2\} \ldots \{x_n \mapsto t_n\}$ is an mgu of $s = t$.

First-Order Resolution

As already mentioned, I still consider first-order logic without equality. First-order resolution on ground clauses corresponds to propositional resolution. Each ground atom becomes a propositional variable. However, since there are up to infinitely many ground instances for a first-oder clause set with variables and it is not a priori known which ground instances are needed in a proof, the first-order resolution calculus operates on clauses with variables.

Roughly, the relationship between ground resolution and first-order resolution corresponds to the relationship between standard tableau and free-variable tableau. However, the variables in free-variable tablea can only be instantiated once, thereas in resolution they can be instantiated arbitrarily often.

Propositional (or first-order ground) resolution is refutationally complete, without reduction rules it is not guaranteed to terminate for satisfiable sets of clauses, and inferior to the CDCL calculus.

However, in contrast to the CDCL calculus, resolution can be easily extended to non-ground clauses via unification and matching. The problem to lift the CDCL calculus lies in the lifting of the model representation of the trail. I'll discuss this in more detail in Section 3.15.

The *first-order resolution calculus* consists of the inference rules *Resolution* and *Factoring* and generalizes the propositional resolution calculus (Section 2.6).

Variables in clauses are implicitely universally quantified, so they can be instantiated in an arbitrary way. For the application of any inference or reduction rule, I can therefore assume that the involved clauses don't share any variables, i.e., variables are a priori renamed. Furthermore, clauses are assumed to be unique with respect to renaming in a set.

Resolution Inference Rules

Resolution

$(N \uplus \{D \vee A, \neg B \vee C\}) \Rightarrow_{\text{RES}} (N \cup \{D \vee A, \neg B \vee C\} \cup \{(D \vee C)\sigma\})$

if $\sigma = mgu(A, B)$ for atoms A, B

Factoring

$(N \uplus \{C \vee L \vee K\}) \Rightarrow_{\text{RES}} (N \cup \{C \vee L \vee K\} \cup \{(C \vee L)\sigma\})$

if $\sigma = mgu(L, K)$ for literals L, K

Resolution Reduction Rules

Subsumption $(N \uplus \{C_1, C_2\}) \Rightarrow_{\mathrm{RES}} (N \cup \{C_1\})$

provided $C_1\sigma \subset C_2$ for some matcher σ

Tautology Deletion $(N \uplus \{C \vee A \vee \neg A\}) \Rightarrow_{\mathrm{RES}} (N)$

Condensation $(N \uplus \{C\}) \Rightarrow_{\mathrm{RES}} (N \cup \{C'\})$

where C' is the result of removing duplicate literals from $C\sigma$ for some matcher σ and C' subsumes C

Subsumption Resolution $(N \uplus \{C_1 \vee L, C_2 \vee K\}) \Rightarrow_{\mathrm{RES}}$
$(N \cup \{C_1 \vee L, C_2\})$

where $L\sigma = \mathrm{comp}(K)$ and $C_1\sigma \subseteq C_2$

3.10.10 Theorem (Soundness and Completenss of Resolution)

The resolution calculus, inference and reduction rules, is sound and complete:

$$N \text{ is unsatisfiable iff } N \Rightarrow^*_{\mathrm{RES}} N' \text{ and } \bot \in N' \text{ for some } N'$$

The result will be a consequence of soundness and completeness of first-order superposition.