3.7 Unification

Definition 3.7.1 (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'.

Obviously, two terms of different sort cannot be made equal by well-sorted instantiation. Since well-sortedness is preserved by all rules of the unification calculus, we assume from now an that all equations, terms, and substitutions are well-sorted.

The first calculus is the naive standard unification calculus that is typically found in the (old) literature on automated reasoning [29]. 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 $x \notin \mathrm{vars}(E')$.

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

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

Clash $E \uplus \{f(s_1,\dots,s_n) = g(s_1,\dots,s_m)\} \;\Rightarrow_{\mathrm{SU}}\; \bot$
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 $\quad E \uplus \{t = x\} \;\Rightarrow_{\mathrm{SU}}\; E \cup \{x = t\}$
if $t \notin \mathcal{X}$

Theorem 3.7.2 (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 $\{s = t\} \Rightarrow^*_{\mathrm{SU}} \perp$ 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.

Proof. 1. by induction on the length of the derivation and a case analysis for the different rules.
2. for a state $E = \{s_1 = t_1, \ldots, s_n = t_n\}$ take the measure $\mu(E) := (n, M, k)$ where n is the number of unsolved variables, M the multiset of all term depths of the s_i, t_i and k the number of equations $t = x$ in E where t is not a variable. The state $\perp$ is mapped to $(0, \emptyset, 0)$. Then the lexicographic combination of $>$ on the naturals and its multiset extension shows that any rule application decrements the measure.
3. by induction on the length of the derivation and a case analysis for the different rules. Clearly, for any state where Clash, or Occurs Check generate $\perp$ the respective equation is not unifiable.
4. a direct consequence of 3.
5. if $E = \{x_1 = t_1, \ldots, x_n = t_n\}$ is a normal form, then for all $x_i = t_i$ we have $x_i \notin \mathrm{vars}(t_i)$ and $x_i \notin \mathrm{vars}(E \setminus \{x_i = t_i\})$, so $\{x_1 = t_1, \ldots, x_n = t_n\}\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\} = \{t_1 = t_1, \ldots, t_n = t_n\}$ and hence $\{x_1 \mapsto t_1, \ldots, x_n \mapsto t_n\}$ is an mgu of $\{x_1 = t_1, \ldots, x_n = t_n\}$. By 3. it is also an mgu of s, t. $\square$

Example 3.7.3 (Size of Standard 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.

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 $\quad E \uplus \{t = t\} \;\Rightarrow_{\mathrm{PU}}\; E$

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

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

Occurs Check $E \uplus \{x = t\} \;\Rightarrow_{\mathrm{PU}}\; \bot$
if $x \neq t$ and $x \in vars(t)$

Orient $E \uplus \{t = x\} \;\Rightarrow_{\mathrm{PU}}\; E \uplus \{x = t\}$
if $t \notin \mathcal{X}$

Substitution $E \uplus \{x = y\} \;\Rightarrow_{\mathrm{PU}}\; E\{x \mapsto y\} \uplus \{x = y\}$
if $x \in vars(E)$ and $x \neq y$

Cycle $E \uplus \{x_1 = t_1,\ldots,x_n = t_n\} \;\Rightarrow_{\mathrm{PU}}\; \bot$
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 $E \uplus \{x = t, x = s\} \;\Rightarrow_{\mathrm{PU}}\; E \uplus \{x = t, t = s\}$
if $t, s \notin \mathcal{X}$ and $|t| \leq |s|$

Theorem 3.7.4 (Soundness, Completeness and Termination of $\Rightarrow_{\mathrm{PU}}$)**.** If s, t are two terms with $\mathrm{sort}(s) = \mathrm{sort}(t)$ then

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

Theorem 3.7.5 (Normal Forms generated by $\Rightarrow_{\mathrm{PU}}$)**.** Let $\{s = t\} \Rightarrow^*_{\mathrm{PU}} \{x_1 = t_1,\ldots,x_n = t_n\}$ be a normal form. Then

1. $x_i \neq x_j$ for all $i \neq j$ and without loss of generality $x_i \notin \mathrm{vars}(t_{i+k})$ 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 $s = t$.

Proof. 1. If $x_i = x_j$ for some $i \neq j$ then Merge is applicable. If $x_i \in \mathrm{vars}(t_i)$ for some i then Occurs Check is applicable. If the x_i cannot be ordered in the described way, then either Substitution or Cycle is applicable.
2. Since $x_i \notin \mathrm{vars}(t_{i+k})$ the composition yields the mgu. □

Lemma 3.7.6 (Size of Unifiers)**.** Let $\{s = t\}$ be a unification problem between two non-variable terms. Then

1. if s and t are linear then for any unifier σ and any term $r \in \text{codom}(\sigma)$, $|r| < |s|$ and $|r| < |t|$ as well as $\text{depth}(r) < \text{depth}(s)$ and $\text{depth}(r) < \text{depth}(t)$,

2. if s is shallow and linear, then the mgu σ of s and t is also a matcher from s to t, i.e., $s\sigma = t$

Proof. Both parts follow directly from the structure of the terms s, t: if they are both linear then the substitution rule is never applied. If s is shallow and linear, it has the form $f(x_1, \ldots, x_n)$, all x_i different, then the unifier is $\sigma = \{x_i \mapsto t|_i \mid 1 \leq i \leq n\}$. $\square$