4 Unification and Critical Pairs

Unification

The composition of two substitutions σ and ρ is the substitution $\sigma \circ \rho$ that maps every variable x to $(x\sigma)\rho$.

Proposition:
The composition of substitutions $\circ$ is associative.

Unification

A substitution σ is called idempotent, if $\sigma \circ \sigma = \sigma$.

Proposition:

σ is idempotent if and only if $\mathrm{Dom}(\sigma) \cap \mathrm{Codom}(\sigma) = \emptyset$.

Unification

A substitution σ is called more general than a substitution τ if $\tau = \sigma \circ \rho$ for some substitution ρ.
Notation: $\sigma \precsim \tau$.

Proposition:
(i) $\precsim$ is a quasi-ordering on substitutions (i.e., reflexive and transitive).

(ii) If $\sigma \precsim \tau$ and $\tau \precsim \sigma$, then there is a bijective variable renaming ρ such that $x\sigma\rho = x\tau$ for every x in X.

Proof:
Exercise.

Unification

A unification problem is a multiset of equations
$E = \{s_1 =^? t_1, \ldots, s_n =^? t_n\}$ with terms s_i, t_i.
(Analogously for atoms, literals, etc.)

A substitution σ is called a unifier of E
if $s_i\sigma = t_i\sigma$ for all $i \in \{1, \ldots, n\}$.

E is called unifiable, if it has a unifier.

A unifier σ of E is called a most general unifier (mgu) of E,
if $\sigma \precsim \tau$ for every unifier τ of E.

Unification

Notation:

A (most general) unifier of $\{s =^? t\}$ is also called
a (most general) unifier of s and t.

Unification

The following inference system transforms a unification problem into a simpler unification problem (or into $\bot$, denoting an unsolvable unification problem).

Unification

$$t =^? t, E \Rightarrow_U E \qquad \text{(Delete)}$$

$$f(\vec{s}) =^? f(\vec{t}), E \Rightarrow_U s_1 =^? t_1, \ldots, s_n =^? t_n, E \qquad \text{(Decompose)}$$

$$f(\vec{s}) =^? g(\vec{t}), E \Rightarrow_U \bot \qquad \text{(Clash)}$$

$$x =^? t, E \Rightarrow_U x =^? t, E\{x \mapsto t\} \qquad \text{(Eliminate)}$$

$$\text{if } x \in \mathrm{Var}(E),\ x \notin \mathrm{Var}(t)$$

$$x =^? t, E \Rightarrow_U \bot \qquad \text{(Occurs-Check)}$$

$$\text{if } x \neq t,\ x \in \mathrm{Var}(t)$$

$$t =^? x, E \Rightarrow_U x =^? t, E \qquad \text{(Orient)}$$

$$\text{if } t \notin X$$

Unification

A unification problem E is said to be in solved form, if $E = \{x_1 =^? u_1, \ldots, x_k =^? u_k\}$, with x_i pairwise distinct and $x_i \notin \mathrm{Var}(u_j)$ for all i, j.

E represents the solution $\sigma_E = \{x_1 \mapsto u_1, \ldots, x_k \mapsto u_k\}$.

Lemma:
If E is in solved form then σ_E is an idempotent mgu of E.

Unification

Lemma:

(i) If $E \Rightarrow_U E'$ then σ is a unifier of E iff σ is a unifier of E'.

(ii) If $E \Rightarrow_U^* E'$, with E' a solved form, then $\sigma_{E'}$ is an mgu of E.

(iii) If $E \Rightarrow_U^* \bot$ then E is not unifiable.

Proof:

(i) We consider the Eliminate rule (the others are obvious).
Let σ be a unifier of $x =^? t$, that is, $x\sigma = t\sigma$.
Then $y(\{x \mapsto t\} \circ \sigma) = y\sigma$ for every variable y.
Therefore, for any equation $u =^? v$ in E, we have $u\sigma = v\sigma$ iff
$u\{x \mapsto t\}\sigma = v\{x \mapsto t\}\sigma$.

(ii) and (iii) follow by induction from (i).

Unification

Lemma:

$\Rightarrow_U$ is Noetherian.

Proof:

A variable x is called solved, if it occurs exactly once in E, namely on the lhs of some $x =^? t$.

Let φ map every E to a triple $(n_1, n_2, n_3) \in \mathbb{N} \times \mathbb{N} \times \mathbb{N}$ where

n_1 is the number of non-solved variables in E,

n_2 is the size of E (i.e., $\sum_{s=^? t \in E}(|s| + |t|)$),

n_3 is the number of equations $t =^? x$ in E.

Then $E \Rightarrow_U E'$ implies $\varphi(E) >_{lex} \varphi(E')$.

Unification

Lemma:

If E is irreducible w.r.t. $\Rightarrow_U$, then it is $\bot$ or in solved form.

Proof:

If E is neither $\bot$ nor in solved form, then it contains

$x_i =^? u_i$, $x_j =^? u_j$ with $x_i = x_j$ $\Rightarrow$ apply Eliminate

or $x_i =^? u_i$ with $x_i \in \mathrm{Var}(u_i)$ $\Rightarrow$ apply Occurs-Check

or $x_i =^? u_i$ with $x_i \in \mathrm{Var}(u_j)$ and $i \neq j$ $\Rightarrow$ apply Eliminate

or $f(\dots) = f(\dots)$ $\Rightarrow$ apply Decompose

or $f(\dots) = g(\dots)$ $\Rightarrow$ apply Clash

or $f(\dots) = x$ $\Rightarrow$ apply Orient.

Unification

Theorem:

E is unifiable if and only if there exists a most general unifier $\text{mgu}(E) = \sigma$ of E, such that σ is idempotent and $dom(\sigma) \cup codom(\sigma) \subseteq \text{Var}(E)$.

Proof:

"if": trivial.

"only if": Compute an arbitrary normal form of E using $\Rightarrow_U$.
By the previous lemmas, it is in solved form and represents an idempotent mgu σ of E.
Since none of the inference rules introduces new variables, $dom(\sigma) \cup codom(\sigma) \subseteq \text{Var}(E)$.

Unification

Problem: exponential growth of terms possible:

Consider the unification problem
$\{x_1 =^? f(x_0, x_0),\ x_2 =^? f(x_1, x_1),\ \dots, x_n =^? f(x_{n-1}, x_{n-1})\}$

Alternatively: Consider the unification problem $\{s_n =^? t_n\}$,

$$\text{where } s_n = f(x_1, \qquad f(x_2, \qquad f(\dots, x_n \qquad\qquad) \dots)),$$
$$t_n = f(f(x_0, x_0), f(f(x_1, x_1), f(\dots, f(x_{n-1}, x_{n-1}))\dots)).$$

Unification

Solution:

Use sharing to avoid duplication:
DAGs instead of trees; every variable occurs only once.

Replace intermediate occurs-checks by a single acyclicity test at the end.

Theorem (Paterson, Wegman):
A most-general unifier can be computed in linear time.

Critical Pairs

Let $l_i \to r_i$ $(i = 1, 2)$ be two rewrite rules in a TRS R whose variables have been renamed such that $\mathrm{Var}(\{l_1, r_1\}) \cup \mathrm{Var}(\{l_2, r_2\}) = \emptyset$.

Let $p \in \mathrm{Pos}(l_1)$ be a position such that l_1/p is not a variable and σ is an mgu of l_1/p and l_2.

Then $r_1\sigma \leftarrow l_1\sigma \to (l_1\sigma)[r_2\sigma]_p$.

$\langle r_1\sigma, (l_1\sigma)[r_2\sigma]_p \rangle$ is called a critical pair of R.

The critical pair is joinable (or: converges), if $r_1\sigma \downarrow_R (l_1\sigma)[r_2\sigma]_p$.

Critical Pairs

Theorem ("Critical Pair Theorem"):
A TRS R is locally confluent if and only if all its critical pairs are joinable.

Proof:
"only if": obvious, since joinability of a critical pair is a special case of local confluence.

Critical Pairs

Proof:

"if": Suppose s rewrites to t_1 and t_2 using rewrite rules $l_i \rightarrow r_i \in R$ at positions $p_i \in \text{Pos}(s)$, where $i = 1, 2$.
Without loss of generality, we can assume that the two rules are variable disjoint, hence $s/p_i = l_i\theta$ and $t_i = s[r_i\theta]_{p_i}$.

We distinguish between two cases: Either p_1 and p_2 are in disjoint subtrees ($p_1 \parallel p_2$), or one is a prefix of the other (w.o.l.o.g., $p_1 \leq p_2$).

Critical Pairs

Case 1: $p_1 \,||\, p_2$.

Then $s = s[l_1\theta]_{p_1}[l_2\theta]_{p_2}$,
and therefore $t_1 = s[r_1\theta]_{p_1}[l_2\theta]_{p_2}$ and $t_2 = s[l_1\theta]_{p_1}[r_2\theta]_{p_2}$.

Let $t_0 = s[r_1\theta]_{p_1}[r_2\theta]_{p_2}$.
Then clearly $t_1 \longrightarrow_R t_0$ using $l_2 \longrightarrow r_2$ and $t_2 \longrightarrow_R t_0$ using $l_1 \longrightarrow r_1$.

Critical Pairs

Case 2: $p_1 \le p_2$.

Case 2.1: $p_2 = p_1\, q_1\, q_2$, where l_1/q_1 is some variable x.

In other words, the second rewrite step takes place at or below a variable in the first rule. Suppose that x occurs m times in l_1 and n times in r_1 (where $m \geq 1$ and $n \geq 0$).

Then $t_1 \rightarrow_R^* t_0$ by applying $l_2 \rightarrow r_2$ at all positions $p_1\, q'\, q_2$, where q' is a position of x in r_1.

Conversely, $t_2 \rightarrow_R^* t_0$ by applying $l_2 \rightarrow r_2$ at all positions $p_1\, q\, q_2$, where q is a position of x in l_1 different from q_1, and by applying $l_1 \rightarrow r_1$ at p_1 with the substitution θ', where $\theta' = \theta[x \mapsto (x\theta)[r_2\theta]_{q_2}]$.

Critical Pairs

Case 2.2: $p_2 = p_1\,p$, where p is a non-variable position of l_1.

Then $s/p_2 = l_2\theta$ and $s/p_2 = (s/p_1)/p = (l_1\theta)/p = (l_1/p)\theta$, so θ is a unifier of l_2 and l_1/p.

Let σ be the mgu of l_2 and l_1/p, then $\theta = \sigma \circ \rho$ and $\langle r_1\sigma, (l_1\sigma)[r_2\sigma]_p\rangle$ is a critical pair.

By assumption, it is joinable, so $r_1\sigma \rightarrow^*_R v \leftarrow^*_R (l_1\sigma)[r_2\sigma]_p$.

Consequently, $t_1 = s[r_1\theta]_{p_1} = s[r_1\sigma\rho]_{p_1} \rightarrow^*_R s[v\rho]_{p_1}$ and $t_2 = s[r_2\theta]_{p_2} = s[(l_1\theta)[r_2\theta]_p]_{p_1} \rightarrow^*_R s[(l_1\sigma\rho)[r_2\sigma\rho]_p]_{p_1} \rightarrow^*_R s[v\rho]_{p_1}$.

This completes the proof of the Critical Pair Theorem.

Critical Pairs

Note: Critical pairs between a rule and (a renamed variant of) itself must be considered – except if the overlap is at the root (i.e., $p = \varepsilon$).

Critical Pairs

Corollary:

A terminating TRS R is confluent if and only if all its critical pairs are joinable.

Proof:

By Newman's Lemma and the Critical Pair Theorem.

Critical Pairs

Corollary:

For a finite terminating TRS, confluence is decidable.

Proof:

For every pair of rules and every non-variable position in the first rule there is at most one critical pair $\langle u_1, u_2 \rangle$.

Reduce every u_i to some normal form u_i'. If $u_1' = u_2'$ for every critical pair, then R is confluent, otherwise there is some non-confluent situation $u_1' \leftarrow_R^* u_1 \leftarrow_R s \rightarrow_R u_2 \rightarrow_R^* u_2'$.