5.1 Unification

Donnerstag, 3. Dezember 2015 12:00

5. Confluence of TRSs

- needed for decision procedure for the word problem
- general question: is result of computation deterministic?

5.1: Unification
- needed to check confluence
- will also be needed for completion
- many other applications in computer science (resolution in logic programming + automated reasoning, polymorphic type checking, etc.)
- in contrast to other lectures, we will introduce a more efficient algorithm

5.2 Checking confluence for terminating TRSs (decidable)

5.3 — " — non-terminating TRSs (undecidable)

5.1. Unification

Given two terms s, t. Does there exist a substitution σ such that $s\sigma = t\sigma$?

"unifier"

Ex: $g(f(x), Y) \stackrel{?}{=} g(Y, f(z))$

This unification problem is solvable.

A unifier is $\sigma = \{Y/f(z), X/z\}$.

Def 5.1.1 (Unification)
Two terms s and t are *unifiable* iff there exists a substitution σ with $s\sigma = t\sigma$. Such a substitution is a *unifier* of s and t.
A *unification problem* over Σ and $\mathcal{V}$ is a finite set
$S = \{s_1 =^? t_1, \ldots, s_n =^? t_n\}$ with $s_i, t_i \in \mathcal{T}(\Sigma, \mathcal{V})$.
A substitution σ is a *solution* or a unifier of S iff $s_i\sigma = t_i\sigma$ holds for all $1 \le i \le n$. $U(S)$ is the set of all unifiers of S.

A unification problem may have several solutions (see slide).
We prefer unifiers that are as general as possible.
σ is more general than σ' iff σ' can be obtained as a specialization of σ (i.e., $\sigma' = \sigma \circ \delta$ for some substitution δ

Composition of σ and δ, i.e., first apply σ, then δ

E.g.: $\sigma = \{X/z, Y/f(z)\}$ is more general than
$\sigma_1 = \{X/a, Y/f(a), z/a\}$, because
$\sigma_1 = \sigma \circ \underbrace{\{z/a\}}_{\delta}$. Instead of "$\sigma \circ \delta$", we often just write "$\sigma\delta$".

δ | just write "$\sigma\delta$".

In our example, σ is more general than $\sigma_1, \sigma_2, \sigma_3$.

Similarly, σ_3 is more general than $\sigma, \sigma_1, \sigma_2$.
(see slide)

Def 5.1.2. (Most general unifier)

A subst. σ is <u>more general</u> than a subst. σ' iff there exists a substitution δ with $\sigma' = \sigma \circ \delta$.

A subst. σ is a most general unifier (mgu) of a unification problem S iff $\sigma \in U(S)$ and σ is more general than any $\sigma' \in U(S)$.

Both σ and σ_3 are mgus in our example.

Lemma 5.1.3. (Uniqueness of most general substitutions)

Let σ, σ' be two substitutions. If σ is more general than σ' and σ' is more general than σ, then there exists a variable renaming δ such that $\sigma' = \sigma\delta$.

A subst. δ is a <u>variable renaming</u> iff δ is injective and
$x\delta \in \mathcal{V}$ for all $x \in \mathcal{V}$.

In our example, σ is more general than σ_3 and vice versa. Indeed: $\sigma = \sigma_3 \circ \underbrace{\{x/z,\ z/x\}}$

is a variable renaming
($\{x/z\}$ would not be injective)

Now our goal is to check whether a unification problem is solvable and to compute a mgu. One mgu is enough, because it represents <u>all</u> unifiers of the unification problem:

<u>Lemma 5.1.4</u> (Representing all unifiers)

Let S be a unification problem over Σ and $\mathcal{V}$, let σ be a mgu of S. Then we have

$$U(S) = \{\sigma \circ \delta \mid \delta \in SUB(\Sigma, \mathcal{V})\}.$$

<u>Proof</u>: "$\supseteq$": To show: $\sigma \circ \delta$ is a unifier of S.

For all $s =^? t \in S$ we have $s\sigma = t\sigma$. This implies $s\sigma\delta = t\sigma\delta$.

"$\subseteq$": Let $\sigma' \in U(S)$. Since σ is a mgu of S, there exists a δ such that $\sigma' = \sigma\delta$. ☒

Idea for unification algorithm: Transform unification problem repeatedly until it is in "solved form". From a unif. problem in solved form one can directly obtain the mgu.

<u>Def 5.1.5.</u> (Solved form of a unif. problem)

A unification problem $S = \{x_1 =^? t_1, \ldots, x_n =^? t_n\}$ is in solved form iff the x_i are pairwise different variables that do not occur in the terms $t_1, \ldots, t_n$. Then we define the substitution $\sigma_S = \{x_1/t_1, \ldots, x_n/t_n\}$.

Ex: $\{g(f(x),y) =^? g(y, f(z))\} \Longrightarrow^* \underbrace{\{x =^? z,\ y =^? f(z)\}}_{S'}$

S' is in solved form.

$\sigma_{S'} = \{x/z, y/f(z)\}$

However, $\{x =^? f(x)\}$ is not in solved form, since x also occurs on the right-hand side. This unif. problem is not solvable (occur failure).

<u>Lemma 5.1.6</u> (mgu of a unific. problem in solved form)

Let S be a unif. problem in solved form. Then σ_S is a mgu of S and for all $\sigma' \in U(S)$ we have $\sigma' = \sigma_S \circ \sigma'$.

<u>Proof</u>: Since the x_i do not occur in $t_1, \ldots, t_n$, we have

$x_i \sigma_S = t_i = t_i \sigma_S \quad \rightsquigarrow \sigma_S \in U(S)$.

Now let $\sigma' \in U(S)$. We have to show $\sigma' = \sigma_S \circ \sigma'$.

For x_i: $\quad x_i \sigma' \overset{\text{as } \sigma' \in U(S)}{=} \underbrace{t_i}_{x_i \sigma_S} \sigma' = x_i \sigma_S \sigma'$

For $x \in \mathcal{V} \setminus \{x_1, \ldots, x_n\}$: $\quad x \sigma' = \underbrace{x \sigma_S}_{x} \sigma'$

$\boxed{\text{q}}$

Now we define a transformation relation $\Longrightarrow$ in order to simplify unification problems.

<u>Def. 5.1.7.</u> (Transformation of Unification Problems)

- <u>Delete</u> $S \dot{\cup} \{t =^? t\} \Longrightarrow S$
- <u>Reduce Terms</u> $S \dot{\cup} \{f(s_1,\dots,s_n) =^? f(t_1,\dots,t_n)\} \Longrightarrow S \cup \{s_1 =^? t_1, \dots, s_n =^? t_n\}$
- <u>Exchange</u> $S \dot{\cup} \{t =^? x\} \Longrightarrow S \dot{\cup} \{x =^? t\}$, if $t \notin \mathcal{V}$
- <u>Reduce Var.</u> $S \dot{\cup} \{x =^? t\} \Longrightarrow \{u\sigma =^? v\sigma \mid u =^? v \in S\} \cup \{x =^? t\}$,
  if $\sigma = \{x/t\}$, $x \notin \mathcal{V}(t)$, $x \in \mathcal{V}(S)$

otherwise this rule would not modify the unif. problem

<u>Ex 5.1.8</u>

$\{g(\underline{f(x)}, \underline{y}) =^? g(\underline{y}, \underline{f(z)})\}$ $\Longrightarrow_{\text{Red. Term}}$

$\{f(x) =^? y,\ y =^? f(z)\}$ $\Longrightarrow_{\text{Red. Var.}}$ using $\sigma = \{y/f(z)\}$

$\{f(x) =^? f(z),\ y =^? f(z)\}$ $\Longrightarrow_{\text{Red. Term}}$

$\{x =^? z,\ y =^? f(z)\}$ ← This is in solved form.

↝ The original unif. problem is solvable and its mgu is $\{x/z,\ y/f(z)\}$.

<u>Unif. Algorithm</u> UNIFY (Martelli + Montanari, 1982):

Apply transf. rules as long as possible.

If the resulting unif. problem is in solved form, then the original unif. problem is solvable and we can read off the mgu.

If the resulting unif. problem is not in solved form, then the original problem is not solvable.

2 possible reasons why unification could fail:

occur failure $\{x =^? f(x)\}$

$\{x =^? f(y),\ y =^? f(x)\}$

clash failure $\{f(x) =^? g(x)\}$

Thm 5.1.9 (Soundness of UNIFY)

see slide

Proof: (a) Proving well-foundedness of $\Rightarrow$ is not trivial, because "Red. Var." can increase the size of a unif. problem.

A variable x is solved in a unif. problem S iff x occurs exactly once in S, on the left-hand side of an equation $x =^? t$ where $x \notin \mathcal{V}(t)$.

We map every unification problem S to a triple (n_1, n_2, n_3) where:

- n_1 = number of variables in S that are not solved
- n_2 = number of symbols in S

• n_3 = number of equations $t =^? x$ in S where $t \notin \mathcal{V}$.

Then (n_1, n_2, n_3) decreases w.r.t. $(>_{\mathbb{N}})^3_{lex}$ in each transformation step.

(b) $S \Rightarrow S' \curvearrowright U(S) = U(S')$ is obvious, except for the transformation rule "Reduce Var.".

$\{x =^? t\}$ is in solved form $\underset{\text{Lemma 5.1.6}}{\curvearrowright}$ $\sigma = \{x/t\}$ is mgu of $\{x =^? t\}$

Thus: For all unifiers θ of $\{x =^? t\}$

(i.e., for all θ with $x\theta = t\theta$)

we have $\theta = \sigma\theta$ by Lemma 5.1.6.

$\theta \in U(S \dot\cup \{x =^? t\})$ iff

$x\theta = t\theta$ and $\theta \in U(S)$ iff $\leftarrow$ since $\theta = \sigma\theta$

$x\theta = t\theta$ and $\sigma\theta \in U(S)$ iff

$x\theta = t\theta$ and $u\sigma\theta = v\sigma\theta$ for all $u =^? v \in S$ iff

$x\theta = t\theta$ and $\theta \in U(\{u\sigma =^? v\sigma \mid u =^? v \in S\})$ iff

$\theta \in U(\{u\sigma =^? v\sigma \mid u = v \in S\} \cup \{x =^? t\})$

(c) Let S be solvable and in normal form w.r.t. $\Rightarrow$.

We have to show that S only contains equations of the form $x =^? t$ where x does not occur on any right-hand side.

• S cannot contain $f(\ldots) =^? g(\ldots)$ (would not be solvable)

- S cannot contain $f(\ldots) =^? f(\ldots)$ (would not be in normal form)
- S cannot contain $t =^? x$ for $t \notin \mathcal{V}$ (— " —)
- S cannot contain $x =^? t$ for $x \in \mathcal{V}(t)$ (if $t = x$: not in norm. form; if $t \neq x$: not solvable)

$\Rightarrow$ S only contains equations of the form $x =^? t$ with $t \notin \mathcal{V}$, $x \notin \mathcal{V}(t)$.

x cannot occur anywhere else in S, because otherwise S would not be in normal form (one could appy "Reduce Var.").

$\Rightarrow$ S in solved form.

(d) Termination of UNIFY follows from (a).

Thus: UNIFY(S) computes a normal form of S, i.e. a unif. problem S' with $S \Rightarrow^* S'$, where S' is in normal form.

By (b): $U(S) = U(S')$.

If S is solvable $\rightsquigarrow U(S) = U(S') \neq \emptyset$, i.e., S' is also solvable.

$\overset{(c)}{\rightsquigarrow}$ S' is in solved form

$\rightsquigarrow$ $\sigma_{S'}$ is the mgu of S' (and thus, of S).

If S is not solvable $\rightsquigarrow U(S) = U(S') = \emptyset$

$\rightsquigarrow$ S' is not in solved form

$\leadsto$ Alg. returns "false".

<u>Corollary 5.1.10</u> (Unification Thm.)

If a unif. problem is solvable, then it has a mgu.

<u>Proof</u>: apply UNIFY

<u>Unification</u>: is there a σ such that $s\sigma = t\sigma$?

<u>Matching</u>: is there a σ such that $s\sigma = t$?

Every unification alg. can also be turned into a matching algorithm:

(a) Replace variables in t by fresh constants

(b) Apply unification

(c) Undo step (a).

<u>Algorithm MATCH (s,t)</u>

Input: 2 terms s,t

Output: A matcher σ with $s\sigma = t$ if it exists.
"False", otherwise

1. Let $\theta = \{x/c_x \mid x \in \mathcal{V}(t)\}$, where c_x are fresh constants.
2. Compute UNIFY$(\{s \stackrel{?}{=} t\theta\})$.
3. If UNIFY returns "False", then stop with "False".
4. If UNIFY returns $\{x_1/t_1, \dots, x_n/t_n\}$, then return

$\{x_1/t_1', \dots, x_n/t_n'\}$, where t_i' results from t_i by replacing the fresh constants c_x by x again.

Ex. 5.1.11 $\quad s = g(x,y) \qquad t = g(f(x), x)$

s and t are not unifiable (occur failure).

But: s matches t

$\theta = \{x/c_x\}$.

$$\text{UNIFY}(\{s \stackrel{?}{=} t\theta\}) = \text{UNIFY}(\{g(x,y) = g(f(c_x), c_x)\})$$
$$= \{x/f(c_x), \; y/c_x\}.$$

$$\text{MATCH}(s,t) = \{x/f(x), \; y/x\}.$$