3.2b Congruence Closure (Part 2)

Dienstag, 3. November 2015 08:30

<u>Solution</u>: Do not compute all equations $\mathcal{E}_i$, but only those that are "potentially useful" to check whether the desired equation $s \equiv t$ is entailed by $\mathcal{E}$.

<u>Crucial Observation</u>: To check whether $s \equiv t$ follows from $\mathcal{E}$, one only needs equations between terms that already occur as subterms in $\mathcal{E}$ or s or t.
Thus, instead of $\mathcal{E}_i$ one only computes those equations of $\mathcal{E}_i$ that only concern those subterms.

<u>Def 328</u> (Subterms for Congruence Closure)
For any term s, we define $Subterms(s) = \{ s|_\pi \mid \pi \in Occ(s) \}$.
For a set of equations $\mathcal{E}$, we define

$$Subterms(\mathcal{E}) = \bigcup_{s \equiv t \in \mathcal{E}} Subterms(s) \cup Subterms(t).$$

Clearly, $Subterms(s)$ is finite for every term s.
Similarly, if $\mathcal{E}$ is finite, then $Subterms(\mathcal{E})$ is also finite.
To check whether $s \equiv_{\mathcal{E}} t$ holds one only has to consider $CC(\mathcal{E}) \cap (\mathcal{S} \times \mathcal{S})$, where

$$\mathcal{S} = Subterms(\mathcal{E}) \cup Subterms(s) \cup Subterms(t)$$

<u>Def 329</u> (Congruence Closure w.r.t. a Set of Terms)
Let $\mathcal{E}$ be a set of ground identities over Σ, let $s, t \in \mathcal{T}(\Sigma)$.

Let $S = \text{Subterms}(\mathcal{E}) \cup \text{Subterms}(s) \cup \text{Subterms}(t)$.
Then we define:

- $\mathcal{E}_0^S = (\mathcal{E} \cup R) \cap (S \times S)$
- $\mathcal{E}_{i+1}^S = (\mathcal{E}_i^S \cup S(\mathcal{E}_i^S) \cup T(\mathcal{E}_i^S) \cup C(\mathcal{E}_i^S)) \cap (S \times S)$

Then $CC^S(\mathcal{E}) = \bigcup_{i \in \mathbb{N}} \mathcal{E}_i^S$ is the congruence closure of $\mathcal{E}$ w.r.t. S

Ex 3.2.10.

In $\mathcal{E}_1^S$, we no longer have $g(i) \equiv g(j)$, because $g(i) \notin S$ (and $g(j) \notin S$).

In $\mathcal{E}_1$, 10 equations were added due to congruence.

In $\mathcal{E}_1^S$, only 2 equations are —— " ——.

Since S is finite, the iteration $\mathcal{E}_0^S, \mathcal{E}_1^S, \ldots$ cannot continue infinitely long. $\Rightarrow$ $CC^S(\mathcal{E})$ is reached after finitely many steps.

Lemma 3.2.11. ($CC^S(\mathcal{E})$ is reached in finitely many steps)

Let $\mathcal{E}$ be a set of ground identities, let $s, t \in \mathcal{T}(\Sigma)$, let $S = \text{Subterms}(\mathcal{E}) \cup \text{Subterms}(s) \cup \text{Subterms}(t)$. Then there exists an $i \in \mathbb{N}$ such that $\mathcal{E}_i^S = \mathcal{E}_{i+1}^S$.
This implies $CC^S(\mathcal{E}) = \mathcal{E}_i^S$.

Proof: We clearly have $\mathcal{E}_i^S \subseteq \mathcal{E}_{i+1}^S$ for all $i \in \mathbb{N}$.
Since $\mathcal{E}_i^S \subseteq S \times S$ for all $i \in \mathbb{N}$ and $S \times S$ is finite, there must be some $i \in \mathbb{N}$ with $\mathcal{E}_i^S = \mathcal{E}_{i+1}^S$.
Thus, $\mathcal{E}_i^S = \mathcal{E}_j^S$ for all $j > i$.

Hence, $\mathcal{E}_i^S = \bigcup_{j \in \mathbb{N}} \mathcal{E}_j^S = CC^S(\mathcal{E})$. ☒

We now show that

$$s \equiv_{\mathcal{E}} t \quad \text{iff} \quad s \equiv t \in CC^S(\mathcal{E}).$$

Then we obtain a <u>decision procedure</u> for the word problem of $\mathcal{E}$:

1. Compute $CC^S(\mathcal{E})$ (terminates by Lemma 3.2.11)
2. If $s \equiv t \in CC^S(\mathcal{E})$ then return "yes", else return "no".

To prove completeness, we again use Birkhoff's Theorem.

<u>Thm 3.2.12</u> (Congruence Closure w.r.t. S is Sound + Complete)

Let $\mathcal{E}$ be a set of ground identities over Σ, let $s, t \in \mathcal{T}(\Sigma)$, let $S \supseteq \text{Subterms}(\mathcal{E}) \cup \text{Subterms}(s) \cup \text{Subterms}(t)$. Then we have $s \equiv_{\mathcal{E}} t$ iff $s \equiv t \in CC^S(\mathcal{E})$.

<u>Proof</u>: <u>"$\Leftarrow$" (Soundness)</u>

Since $CC^S(\mathcal{E}) \subseteq CC(\mathcal{E})$, this follows from the soundness of $CC(\mathcal{E})$ (Thm. 3.2.7).

<u>"$\Rightarrow$" (Completeness)</u>

$$s \equiv_{\mathcal{E}} t \quad \underset{\substack{\text{Birkhoff's Thm} \\ \text{(Thm 3.1.14)}}}{\curvearrowright} \quad s \overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}} t.$$

Therefore, it suffices to show:

$s \xleftrightarrow{n}_{\mathcal{E}} t$ implies $s \equiv t \in CC^S(\mathcal{E})$

for all $n \in \mathbb{N}$.

Proof by induction on n.

Ind Base: $n = 0$

$s \xleftrightarrow{0}_{\mathcal{E}} t$ means $s = t$. This is contained in

$$R \cap (S \times S) \subseteq \mathcal{E}_0^S \subseteq CC^S(\mathcal{E}).$$

Ind Step: $n > 0$

$s = s_0 \longleftrightarrow_{\mathcal{E}} s_1 \longleftrightarrow_{\mathcal{E}} s_2 \longleftrightarrow_{\mathcal{E}} \dots \longleftrightarrow s_n = t$

Case 1: there is a k with $1 \leq k < n$ where the k-th rewrite step is applied on top position,

i.e.: $s_k = u$, $s_{k+1} = v$ for some $u \equiv v$ or $v \equiv u \in \mathcal{E}$

$$\left.\begin{array}{l} s = s_0 \longleftrightarrow_{\mathcal{E}} s_1 \longleftrightarrow_{\mathcal{E}} \dots \longleftrightarrow_{\mathcal{E}} s_k = u \\ v = s_{k+1} \longleftrightarrow_{\mathcal{E}} \dots \longleftrightarrow_{\mathcal{E}} s_n = t \end{array}\right\} \text{Both these rewrite sequences have a length} < n$$

We can apply the induction hypothesis, because

$$S \supseteq \text{Subterms}(\mathcal{E}) \cup \text{Subterms}(s) \cup \underbrace{\text{Subterms}(u)}_{\subseteq \text{Subterms}(\mathcal{E})}$$

and $S \supseteq \text{Subterms}(\mathcal{E}) \cup \underbrace{\text{Subterms}(v)}_{\subseteq \text{Subterms}(\mathcal{E})} \cup \text{Subterms}(t)$

By the ind. hyp: $s \equiv u$, $v \equiv t \in CC^S(\mathcal{E})$

Moreover $u \equiv v \in \mathcal{E}_1^S \subseteq CC^S(\mathcal{E})$

Since $CC^S(\mathcal{E})$ is closed under transitivity, we obtain

$$s \equiv t \in CC^S(\mathcal{E}).$$

Case 2: In $s \xleftrightarrow{n}_{\mathcal{E}} t$, no equation from $\mathcal{E}$ is applied on top position.
Let $\pi_1, \dots, \pi_k \in Occ(s)$ be the top positions of s where equations are applied in the rewrite sequence $s \xleftrightarrow{n}_{\mathcal{E}} t$, where $\pi_i \perp \pi_j$ for all $i \neq j$.

Thus: $s = s[p_1]_{\pi_1} \dots [p_k]_{\pi_k}$, $t = s[q_1]_{\pi_1} \dots [q_k]_{\pi_k}$
where $p_i \xleftrightarrow{*}_{\mathcal{E}} q_i$ for all $1 \leq i \leq k$.

Each of these rewrite sequences has at most length n and during the sequence, an equation is applied on top position.
As in Case 1, this implies $p_i \equiv q_i \in CC^S(\mathcal{E})$.
Since $CC^S(\mathcal{E})$ is closed under contexts for terms from S, we obtain $s \equiv t \in CC^S(\mathcal{E})$.

$\boxed{\checkmark}$

Ex 3.2.13 In our example, $CC^S(\mathcal{E})$ can be used to decide whether $s \equiv_{\mathcal{E}} t$ holds.

Corollary 3.2.14 (Decidability of Word Problem for Ground Identities)
Let $\mathcal{E}$ be a finite set of ground identities. Then $s \equiv_{\mathcal{E}} t$ can be decided in polynomial time for any $s, t \in \mathcal{T}(\Sigma)$.

This does not work for general equations (with variables)
E.g.: $\mathcal{E} = \{f(f(x)) \equiv g(x)\}$, $s = f(g(a))$, $t = g(f(a))$
Does $s \equiv_{\mathcal{E}} t$ hold? Yes:

$$s = f(g(a)) \leftarrow_{\mathcal{E}} f(f(f(a))) \rightarrow_{\mathcal{E}} g(f(a)) = t$$

$$s = f(g(a)) \leftarrow_{\mathcal{E}} \underline{f(f(f(a)))} \rightarrow_{\mathcal{E}} g(f(a)) = t$$

Here, one has to use a term that is not contained in $Subterms(\mathcal{E}) \cup Subterms(s) \cup Subterms(t)$.

Improve the decision procedure for word problem for ground identities: Do not include all equations in $\mathcal{E}_0^S, \mathcal{E}_1^S, \ldots$ but use a representation by <u>equivalence classes</u>.

- Let $\Rightarrow_{\mathcal{E}}$ be the relation with $s \Rightarrow_{\mathcal{E}} t$ iff $s \equiv t \in \mathcal{E}$.
- let $Eq(\mathcal{E})$ be the set of all equations that follow from $\mathcal{E}$ by reflexivity, symmetry, and transitivity:

$$Eq(\mathcal{E}) = \{ s \equiv t \mid s \Leftrightarrow_{\mathcal{E}}^* t \}$$

- Now we use a slightly different iteration:

$$\mathcal{E}_0^{S'} = Eq(\mathcal{E}) \cap (S \times S)$$

$$\mathcal{E}_{i+1}^{S'} = Eq(\mathcal{E}_i^{S'} \cup C(\mathcal{E}_i^{S'})) \cap (S \times S)$$

Idea: repeated alternation of
- equivalence
- congruence

Clearly: $CC^S(\mathcal{E}) = \bigcup_{i \in \mathbb{N}} \mathcal{E}_i^{S'}$

Advantage: $\Rightarrow_{\mathcal{E}_i^{S'}}$ is an equivalence relation. Therefore, it can be represented by its equivalence classes, i.e., by the quotient set

$$S_i = S/_{\Rightarrow_{\mathcal{E}_i^{S'}}} = \{ [s]_{\Rightarrow_{\mathcal{E}_i^{S'}}} \mid s \in S \}$$

This results in the following algorithm:

Algorithm CONGRUENCE_CLOSURE$(\mathcal{E}, s, t)$

Input: finite set of ground identities $\mathcal{E}$, ground terms s, t

Output: "true" if $s \equiv_{\mathcal{E}} t$ and "false" otherwise

1. Let $S = Subterms(\mathcal{E}) \cup Subterms(s) \cup Subterms(t)$

Equivalence
2. Let $L = \{\{u,v\} \mid u \equiv v \in \mathcal{E}\} \cup \{\{u\} \mid u \in S\}$

3. Unite all sets $M_1, M_2 \in L$ with $M_1 \cap M_2 \neq \emptyset$.

Congruence
4. Let $K = L \cup \{\{f(u_1,\dots,u_n), f(v_1,\dots,v_n)\} \mid f \in \Sigma,$ there exist $M_i \in L$ such that $u_i, v_i \in M_i,$ $f(u_1,\dots,u_n), f(v_1,\dots,v_n) \in S\}$

Equivalence
5. Unite all sets $M_1, M_2 \in K$ with $M_1 \cap M_2 \neq \emptyset$.

6. If $K \neq L$ then let $L = K$ and go back to step 4.

7. Otherwise: if there is an $M \in L$ with $s \in M$ and $t \in M$ then return "true", else return "false".

Thm 3.2.15

The algorithm CONGRUENCE_CLOSURE terminates and is correct.