3.1a Deduction of Equations (Part 1)

Donnerstag, 22. Oktober 2015 12:30

3. Term Rewriting and Deduction of Equations

Goal: find methods to solve the word problem $s \equiv_E t$ automatically.

3.1.: first method for solving the word problem
(not yet efficient/applicable in practice, but first step)

3.2: practical method for the special case where
E contains no variables (congruence closure)

3.3: practical method for the general case (term rewriting)

3.1. Deduction of Equations

Goal: check whether $E \models s \equiv t$ holds

Difficult, because "$\models$" is defined semantically
(i.e., we have to check all possible (infinitely many)
algebras)

Solution: Find a syntactical way which corresponds to the
semantics, i.e., find a calculus (suitable for
automation) which checks $s \equiv_E t$.

To this end: We need 2 techniques to modify/manipulate terms:
substitutions + subterm replacements

Def 3.1.1 (Substitutions, Matching)

A mapping $\sigma : \mathcal{V} \to \mathcal{T}(\Sigma, \mathcal{V})$ is a substitution iff
$\sigma(x) \neq x$ only holds for finitely many variables.

$SUB(\Sigma, \mathcal{V})$ is the set of all substitutions over Σ and $\mathcal{V}$.

The identity substitution $id \in SUB(\Sigma, \mathcal{V})$ is: $id(x) = x$ for all $x \in \mathcal{V}$.

$DOM(\sigma) = \{ x \in \mathcal{V} \mid \sigma(x) \neq x \}$ is the domain of the subst. σ.

Since DOM is finite, σ can be represented as the set

$$\{ x/\sigma(x) \mid x \in DOM(\sigma) \}.$$

Ex 3.12 $\sigma = \{ x/plus(x,y),\ y/0,\ z/succ(z) \}$ $\rightsquigarrow$ $DOM(\sigma) = \{x, y, z\}$

Then: $\sigma(x) = plus(x,y)$

$\sigma(u) = u$

$\sigma(plus(x,y)) = plus(\sigma(x), \sigma(y))$

$= plus(plus(x,y), 0)$

Def 3.11 (cont.)

Substitutions can be extended to terms: $\sigma : \mathcal{T}(\Sigma, \mathcal{V}) \to \mathcal{T}(\Sigma, \mathcal{V})$ as follows: $\sigma(f(t_1, \ldots, t_n)) = f(\sigma(t_1), \ldots, \sigma(t_n))$.

We say that a term s matches a term t iff there exists a substitution σ such that $\sigma(s) = t$. Then σ is called matcher of s and t.

Ex 3.12 (cont.)

$plus(x,y)$ matches $plus(plus(x,y), 0)$, because

$\sigma(plus(x,y)) = plus(plus(x,y), 0)$

for $\sigma = \{ x/plus(x,y), y/0 \}$.

For $x^* = x_1 \ldots x_n \in \mathcal{V}^*$ with $x_i \neq x_j$ for $i \neq j$ and $t^* = t_1 \ldots t_n \in \mathcal{T}(\Sigma, \mathcal{V})^*$,

we often write $\{ x^*/t^* \}$ instead of $\{ x_1/t_1, \ldots, x_n/t_n \}$.

Moreover, we often write $t\sigma$ instead of $\sigma(t)$.

We say that a subst. σ is a ground substitution iff $x\sigma \in \mathcal{T}(\Sigma)$ for all $x \in DOM(\sigma)$.

E.g.: $\sigma = \{ X/\sigma,\ Y/succ(\sigma) \}$ is a ground subst.

$X\sigma = \sigma$, $Z\sigma = Z$

If $s \equiv t$ is satisfied by an algebra, then $s\sigma \equiv t\sigma$ is also satisfied by this algebra.
Similarly, $s \equiv_\varepsilon t$ implies $s\sigma \equiv_\varepsilon t\sigma$.
Thus: the relation $\equiv_\varepsilon$ is "stable" (or "closed under substitutions").

Def 3.1.3 (Stability)
A relation $\rightarrow$ on terms ($\rightarrow \subseteq T(\Sigma, \mathcal{V}) \times T(\Sigma, \mathcal{V})$) is stable (or "closed under substitutions") iff we have the following for all terms t_1, t_2 and all substitutions σ:

$$t_1 \rightarrow t_2 \quad \text{implies} \quad t_1\sigma \rightarrow t_2\sigma$$

Our goal now is to prove that $\equiv_\varepsilon$ is stable.
To this end: show the connection between
Variable assignments β (semantical) and
substitutions σ (syntactical).

To prove statements about terms (and about other inductively defined data structures):

Structural Induction

For terms: We want to prove a statement $\varphi(t)$ for all terms t.

Induction Base: Prove $\varphi(X)$ for all variables $X \in \mathcal{V}$.

Induction Step: Prove $\varphi(f(t_1, \ldots, t_n))$.

As induction hypothesis, one can use that $\varphi(t_1), \ldots, \varphi(t_n)$ holds.

Lemma 3.1.4 ($\equiv_\mathcal{E}$ stable)

Let $\mathcal{I} = (\mathcal{A}, \alpha, \beta)$ be an interpretation, let $s, t \in T(\Sigma, \mathcal{V})$, let $\sigma \in SUB(\Sigma, \mathcal{V})$, let $\mathcal{I}' = (\mathcal{A}, \alpha, \beta')$ with $\beta'(x) = \mathcal{I}(x\sigma)$.

(a) $\mathcal{I}(t\sigma) = \mathcal{I}'(t)$ for all $t \in T(\Sigma, \mathcal{V})$
(b) $\mathcal{I} \models s\sigma \equiv t\sigma$ iff $\mathcal{I}' \models s \equiv t$

} Substitution Lemma

(c) For all algebras A, we have:
$A \models s \equiv t$ implies $A \models s\sigma \equiv t\sigma$

(d) For all sets of equations $\mathcal{E}$, we have
$s \equiv_\mathcal{E} t$ implies $s\sigma \equiv_\mathcal{E} t\sigma$

Goal: Mimick the semantical relation $\equiv_\mathcal{E}$ in a syntactical.

Examples to illustrate Lemma 3.1.4

$\mathcal{I} = (\mathbb{N}, \alpha, \beta)$ with
$\alpha_{succ}(n) = n+1$
$\alpha_{plus}(n,m) = n+m$
$\beta(x) = 5$
$\beta(y) = 3$

$\mathcal{I}' = (\mathbb{N}, \alpha, \beta')$
$\beta'(x) = \mathcal{I}(x\sigma) = \mathcal{I}(s(x)) = 6$

(a) $t = plus(x,x)$, $\sigma = \{x / succ(x)\}$

$\mathcal{I}(t\sigma) = \mathcal{I}(plus(succ(x), succ(x))) = 12$
($succ(x)$: 6, $succ(x)$: 5)

$\mathcal{I}'(t) = \mathcal{I}'(plus(x,x)) = 12$
(x: 6)

(b) $\mathcal{I} \models \underbrace{s^6(x)}_{12}\sigma \equiv \underbrace{plus(x,x)}_{12}\sigma$

$\mathcal{I}' \models s^6(x) \equiv plus(x,x)$

(c) $A \models plus(x, 0) \equiv x$ implies
$A \models plus(succ(x), 0) \equiv succ(x)$

(d) $plus(x,0) \equiv_\varepsilon x$ implies
$plus(succ(x), 0) \equiv_\varepsilon succ(x)$

Proof of Lemma 3.1.4

(a) We prove the following statement $\varphi(t)$ for all terms t:

For all $\mathcal{I}, \mathcal{I}', \sigma$ as above: $\mathcal{I}(t\sigma) = \mathcal{I}'(t)$

We use structural induction on terms.

Ind. Base: Here, t is a variable $x \in \mathcal{V}$.

$\mathcal{I}(x\sigma) = \beta'(x) = \mathcal{I}'(x)$ ✓

Ind. Step: Here, t has the form $f(t_1, \dots, t_n)$.

$\mathcal{I}(f(t_1, \dots, t_n)\sigma)$
$= \mathcal{I}(f(t_1\sigma, \dots, t_n\sigma))$
$= \alpha_f(\underbrace{\mathcal{I}(t_1\sigma)}, \dots, \underbrace{\mathcal{I}(t_n\sigma)})$
$= \alpha_f(\mathcal{I}'(t_1), \dots, \mathcal{I}'(t_n))$ by the ind. hypothesis
$= \mathcal{I}'(f(t_1, \dots, t_n))$

(b) $\mathcal{I} \models s\sigma \equiv t\sigma$
iff $\underbrace{\mathcal{I}(s\sigma)} = \underbrace{\mathcal{I}(t\sigma)}$
iff $\mathcal{I}'(s) = \mathcal{I}'(t)$ by (a)
iff $\mathcal{I}' \models s \equiv t$

(c) Let $A \models s \equiv t$.
To show: $A \models s\sigma \equiv t\sigma$
Let $A = (\mathcal{A}, \alpha)$.
For any $\mathcal{I} = (\mathcal{A}, \alpha, \beta)$, we therefore have to show:

$\mathcal{I} \models s\sigma \equiv t\sigma$

Let $\mathcal{I}' = (\mathcal{A}, \alpha, \beta')$ with $\beta'(x) = \mathcal{I}(x\sigma)$ for all $x \in \mathcal{V}$.

Since $\mathcal{I}'$ results from the algebra $\mathcal{A}$ by adding a var. assignment,

$\mathcal{A} \models s \equiv t$ implies $\mathcal{I}' \models s \equiv t$.

By (b): $\mathcal{I} \models s\sigma \equiv t\sigma$.

(d) Let $s \equiv_{\mathcal{E}} t$, i.e., $\mathcal{E} \models s \equiv t$.

So for any algebra $\mathcal{A}$ with $\mathcal{A} \models \mathcal{E}$, we have $\mathcal{A} \models s \equiv t$.

By (c), we also have $\mathcal{A} \models s\sigma \equiv t\sigma$.

Hence: $s\sigma \equiv_{\mathcal{E}} t\sigma$

First Syntactic concept: Substitution $\Rightarrow$ $\equiv_{\mathcal{E}}$ is closed under substitutions (stable)

Second syntactic concept: positions $\Rightarrow$ $\equiv_{\mathcal{E}}$ is closed under contexts (monotonic)

Def 3.15 (Positions)

For a term t, let $Occ(t)$ be the set of all positions of t. Here, $Occ(t)$ is the smallest subset of $\mathbb{N}^*$ with:

- $\varepsilon \in Occ(t)$ (empty position / top position)
- $i\pi \in Occ(t)$, if $t = f(t_1, \ldots, t_n)$, $1 \leq i \leq n$, and $\pi \in Occ(t_i)$.

For a term t with $\pi \in Occ(t)$, $t|_\pi$ is the subterm of t at the position π, which is defined as follows:

- $t|_\varepsilon = t$

follows:

- $t|_\varepsilon = t$
- $f(t_1,\dots,t_n)\,|_{i\pi} = t_i|_\pi$

Ex. 3.16 $t = plus(succ(plus(0, succ(0))), succ(0))$

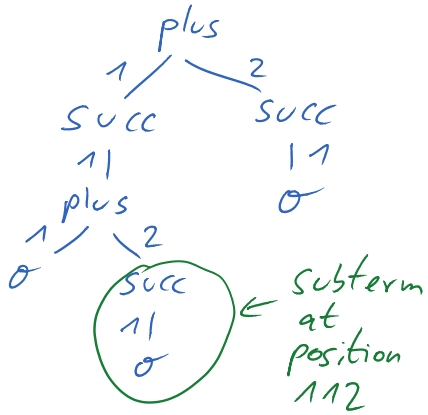
$t|_\varepsilon = t$

$t|_1 = succ(plus(0, succ(0)))$

$t|_2 = succ(0)$

$t|_{11} = plus(0, succ(0))$

$t|_{112} = succ(0)$



$t[times(0,0)]_{112} = plus(succ(plus(0, times(0,0))), succ(0))$

$112 >_{IN^*} 11 >_{IN^*} 1 >_{IN^*} \varepsilon$. $112 \perp 111$

Def 3.15 (cont.)

For a term t and a $\pi \in Occ(t)$, let $t[r]_\pi$ be the term that results from replacing $t|_\pi$ by the term r:

- $t[r]_\varepsilon = r$
- $f(t_1,\dots,t_n)[r]_{i\pi} = f(t_1,\dots,t_i[r]_\pi,\dots,t_n)$

For $\pi_1, \pi_2 \in Occ(t)$, we say that π_1 is below π_2 ($\pi_1 >_{IN^*} \pi_2$) iff π_2 is a proper prefix of π_1 (i.e.: $\pi_1 = \pi_2\pi$ for some $\pi \in \mathbb{N}^+$, i.e. $\pi \neq \varepsilon$).

We say that π_1 and π_2 are independent ("$\pi_1 \perp \pi_2$") iff neither $\pi_1 >_{IN^*} \pi_2$ nor $\pi_2 >_{IN^*} \pi_1$ nor $\pi_1 = \pi_2$.

We know: $\equiv_\varepsilon$ is closed under substitutions

Now we show: $\equiv_\varepsilon$ is closed under contexts (monotonic)

Def 3.1.7 (Monotonic)
A relation $\rightarrow$ on terms is monotonic iff the following holds for all terms t_1, t_2, q and all $\pi \in Occ(q)$:

$t_1 \rightarrow t_2$ implies $q[t_1]_\pi \rightarrow q[t_2]_\pi$

E.g.: if $plus(x,0) \rightarrow x$
then $succ(plus(x,0)) \rightarrow succ(x)$

Lemma 3.1.8 ($\equiv_\mathcal{E}$ is monotonic)
Let s,t,q be terms, let $\pi \in Occ(q)$. Then we have:
(a) for all algebras A, we have:
if $A \models s \equiv t$, then $A \models q[s]_\pi \equiv q[t]_\pi$.
(b) for all sets of equations $\mathcal{E}$, we have:
if $s \equiv_\mathcal{E} t$, then $q[s]_\pi \equiv_\mathcal{E} q[t]_\pi$
(i.e.: $\equiv_\mathcal{E}$ is monotonic)

Proof: (a) We have to prove the following statement $\varphi(\pi)$ for all positions π:
"For all algebras A, all terms s,t,q with $\pi \in Occ(q)$, we have: $A \models s \equiv t$ implies $A \models q[s]_\pi \equiv q[t]_\pi$."
We prove this statement by structural induction on the position π.
Ind. Base: $\pi = \varepsilon$
We know $A \models s \equiv t$.
To prove: $A \models \underbrace{q[s]_\varepsilon}_{s} \equiv \underbrace{q[t]_\varepsilon}_{t}$ ✓
Ind. Step: $\pi = i\pi'$
Since $i\pi' \in Occ(q)$, q has the form $f(q_1, \ldots, q_i, \ldots, q_n)$.
We know: $A \models s \equiv t$

To prove: $\mathcal{A} \models q[s]_{i\pi'} \equiv q[t]_{i\pi'}$,

i.e., $\mathcal{A} \models f(q_1,..,q_n)[s]_{i\pi'} \equiv f(q_1,..,q_n)[t]_{i\pi'}$

$\mathcal{A} \models f(q_1,..,q_i[s]_{\pi'},..,q_n) \equiv f(q_1,..,q_i[t]_{\pi'},..,q_n)$

Let $\mathcal{A} = (\mathcal{A}, \alpha)$. For every interpretation $\mathcal{I} = (\mathcal{A}, \alpha, \beta)$, we have to show

$\mathcal{I} \models f(q_1,..,q_i[s]_{\pi'},..,q_n) \equiv f(q_1,..,q_i[t]_{\pi'},..,q_n)$,

i.e., $\alpha_f(\mathcal{I}(q_1),..,\mathcal{I}(q_i[s]_{\pi'}),..) = \alpha_f(\mathcal{I}(q_1),..,\mathcal{I}(q_i[t]_{\pi'}),..)$

It suffices to show that

$\mathcal{I}(q_i[s]_{\pi'}) = \mathcal{I}(q_i[t]_{\pi'})$. (*)

The induction hypothesis implies:

"For all $\mathcal{A}, s, t, q'$: $\mathcal{A} \models s \equiv t$ implies $\mathcal{A} \models q'[s]_{\pi'} \equiv q'[t]_{\pi'}$"

By choosing q' to be q_i, we know that

$\mathcal{A} \models s \equiv t$ implies $\mathcal{A} \models q_i[s]_{\pi'} \equiv q_i[t]_{\pi'}$

Hence: $\mathcal{I} \models q_i[s]_{\pi'} \equiv q_i[t]_{\pi'}$, i.e., (*) holds.

(b) $s \equiv_\mathcal{E} t$ means that

$\mathcal{A} \models \mathcal{E}$ implies $\mathcal{A} \models s \equiv t$.

This implies $\mathcal{A} \models q[s]_\pi \equiv q[t]_\pi$, by (a) ∎

2 syntactical properties of $\equiv_\mathcal{E}$:

- stable ($s \equiv_\mathcal{E} t \rightsquigarrow s\sigma \equiv_\mathcal{E} t\sigma$)
- monotonic ($s \equiv_\mathcal{E} t \rightsquigarrow q[s]_\pi \equiv_\mathcal{E} q[t]_\pi$)

Word Problem: $s \equiv_\mathcal{E} t$

Def 3.19 (Equivalence Relation, Congruence Relation)

Let M be a set, let $\rightarrow$ be a relation on M

($\to \subseteq M \times M$). Then the relation $\to$ is called

- reflexive iff $t \to t$ holds for all $t \in M$ (e.g. $\geq_{IN}$, $\trianglerighteq$)
- symmetric iff $t_1 \to t_2$ implies $t_2 \to t_1$ for all $t_1, t_2 \in M$ (e.g. $=_{IN}$)
- transitivity iff $t_1 \to t_2$ and $t_2 \to t_3$ implies $t_1 \to t_3$ for all $t_1, t_2, t_3 \in M$ (e.g. $\geq_{IN}$, $>_{IN}$, $\trianglerighteq$)
- an equivalence relation iff $\to$ is reflexive, symmetric, and transitive (e.g. $=_{IN}$)

For a relation $\to$,

- $\to^=$ is the reflexive closure of $\to$, where $\to^=$ is the smallest relation that contains $\to$ and is reflexive, i.e. it is the smallest relation such that
  - if $t_1 \to t_2$, then $t_1 \to^= t_2$ for all $t_1, t_2 \in M$
  - $t \to^= t$ for all $t \in M$
- $\to^+$ is the transitive closure of $\to$, where $\to^+$ is the smallest relation that contains $\to$ and is transitive, i.e.: $t_1 \to^+ t_2$ iff there exist $s_0, \ldots, s_n$ with $n > 0$ such that:
$$t_1 = s_0 \to s_1 \to \ldots \to s_n = t_2$$
- $\to^*$ is the transitive-reflexive closure of $\to$, where: $t_1 \to^* t_2$ iff there exist $s_0, \ldots, s_n$ with $n \geq 0$ such that $t_1 = s_0 \to s_1 \to \ldots \to s_n = t_2$.
- $\leftrightarrow$ is the symmetric closure of $\to$, where $t_1 \leftrightarrow t_2$ iff $t_1 \to t_2$ or $t_2 \to t_1$
- $\leftrightarrow^*$ is the transitive-reflexive-symmetric closure, i.e., the smallest equivalence relation that contains

$\rightarrow$,

A relation $\rightarrow$ (on terms) is a <u>congruence relation</u> iff it is an equivalence relation and $\rightarrow$ is monotonic.

We write $t_1 \rightarrow^{*} t_2$ for $t_1 = s_0 \rightarrow s_1 \rightarrow \ldots \rightarrow s_n = t_2$.

—

We already know that $\equiv_E$ is stable and monotonic. The following lemma states that $\equiv_E$ is also reflexive, symmetric, and transitive.

<u>Lemma 3.1.10</u> ($\equiv_E$ is an equivalence relation)
Let E be a set of equations. Then $\equiv_E$ is an equivalence and a congruence relation.

<u>Proof</u>: clear, because $\equiv_E$ is a form of equality.

E.g.: $A \models t \equiv t$ holds for any algebra A, therefore it also holds for any model A of E. $\sim t \equiv_E t$ ∎