3.1b Deduction of Equations (Part 2)

Dienstag, 27. Oktober 2015 09:00

Now we can mimick $\equiv_\mathcal{E}$ in a purely syntactical way. One only has to take the equations in $\mathcal{E}$ and add stability, monotonicity, reflexivity, symmetry, and transitivity.

<u>Def 3.1.11</u> (Rewrite Relation, Proof Relation, Derivation)

For a set of equations $\mathcal{E}$, the corresponding <u>rewrite relation</u> $\rightarrow_\mathcal{E} \subseteq \mathcal{T}(\Sigma, \mathcal{V}) \times \mathcal{T}(\Sigma, \mathcal{V})$ is defined as follows:

$$s \rightarrow_\mathcal{E} t \quad \text{iff} \quad s|_\pi = t_1\sigma \quad \text{and} \quad t = s[t_2\sigma]_\pi$$

for some $t_1 \equiv t_2 \in \mathcal{E}$, some $\sigma \in SUB(\Sigma, \mathcal{V})$, some $\pi \in Occ(s)$

The relation $\leftrightarrow_\mathcal{E}^*$ is the <u>proof relation</u> of $\mathcal{E}$.

We say that an equation $s \equiv t$ can be <u>derived from $\mathcal{E}$</u> ("$\mathcal{E} \vdash s \equiv t$") iff $s \leftrightarrow_\mathcal{E}^* t$.

Goal: Find out whether $s \equiv_\mathcal{E} t$, i.e., whether $\mathcal{E} \models s \equiv t$.

This is a semantical question, since one has to check whether all models $\mathcal{A}$ of $\mathcal{E}$ also satisfy $s \equiv t$.

$\Rightarrow$ difficult to automate

Solution: Check instead whether $s \leftrightarrow_\mathcal{E}^* t$, i.e., whether $\mathcal{E} \vdash s \equiv t$.

This is a syntactical question:
One has to find a derivation

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

This is enough, because

$$s \equiv_\mathcal{E} t \qquad \text{iff} \qquad s \leftrightarrow_\mathcal{E}^* t$$

(this will be proved in Birkhoff's Theorem, Thm 3.1.14).

Ex. 3.1.12 $\mathcal{E}$ = plus-equations

Goal: Find out whether

$$plus(succ(succ(\mathcal{O})), x) \longleftrightarrow^*_{\mathcal{E}} plus(succ(\mathcal{O}), succ(x))\ \checkmark$$

This can be done automatically (one has to check whether left- or right-hand sides of equations match subterms). Requires search, because one does not know which equation of $\mathcal{E}$ should be applied in which direction.

To show that $\equiv_{\mathcal{E}}$ and $\longleftrightarrow^*_{\mathcal{E}}$ are the same, we first prove that the 5 properties (stability, monotonicity, reflexivity, symmetry, transitivity) of $\equiv_{\mathcal{E}}$ also hold for $\longleftrightarrow^*_{\mathcal{E}}$.

Lemma 3.1.13 ($\longleftrightarrow^*_{\mathcal{E}}$ is a stable + monotonic equivalence relation)

For any set of equations $\mathcal{E}$, $\rightarrow_{\mathcal{E}}$ and $\longleftrightarrow^*_{\mathcal{E}}$ are stable and monotonic. Moreover, $\longleftrightarrow^*_{\mathcal{E}}$ is an equivalence relation.

Proof:

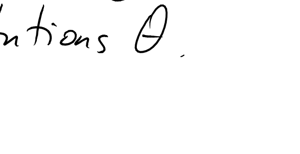
$\rightarrow_{\mathcal{E}}$ is stable, i.e.: show that $s \rightarrow_{\mathcal{E}} t$ implies
$s\theta \rightarrow_{\mathcal{E}} t\theta$
for all substitutions θ.

$s \rightarrow_{\mathcal{E}} t$

$\leadsto$ $s|_\pi = t_1\sigma$, $t = s[t_2\sigma]_\pi$ for some $\pi \in Occ(s)$, subst. σ,
$t_1 \equiv t_2 \in \mathcal{E}$

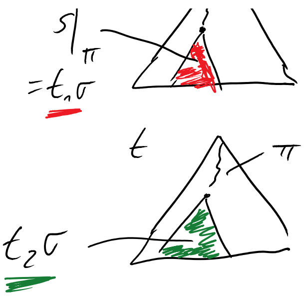
Goal: Show that $s\theta \rightarrow_{\mathcal{E}} t\theta$.

$s\theta|_\pi = s|_\pi\theta = t_1\underbrace{\sigma\theta}$



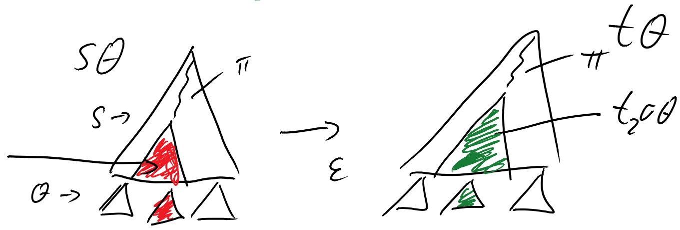
$$s\theta|_\pi = s|_\pi \theta = t_1 \underbrace{\sigma\theta}_{\sigma'}$$

σ' is the composition of the substitutions σ and θ (first apply σ, then θ).



$s\theta \to_\mathcal{E}$ $s\theta[t_2 \underbrace{\sigma'}_{\sigma\theta}]_\pi =$ $s\theta[t_2\sigma\theta]_\pi =$ $s[t_2\sigma]_\pi\theta =$ $t\;\theta$.

$s\theta|_\pi =$ $s|_\pi\theta =$ $t_1\sigma\theta$



In a similar way, one can show that $\to_\mathcal{E}$ is closed under contexts (monotonic).

To show that $\overset{*}{\leftrightarrow}_\mathcal{E}$ is stable and monotonic, one can use induction on the length of the derivation. $\boxed{\mathcal{E}}$

Now we can show the main theorem that states that the semantical relation $\equiv_\mathcal{E}$ and the syntactical relation $\overset{*}{\leftrightarrow}_\mathcal{E}$ are the same.

<u>Thm 3.1.15</u> (Birkhoff's Theorem)

Let $\mathcal{E}$ be a set of equations. Then the relations $\equiv_\mathcal{E}$ and $\overset{*}{\leftrightarrow}_\mathcal{E}$ are the same. In other words:
$\mathcal{E} \models s \equiv t$ iff $\mathcal{E} \vdash s \equiv t$.

<u>Proof</u>

<u>"$\Leftarrow$" Soundness</u> show that $s \overset{*}{\leftrightarrow}_\mathcal{E} t$ implies $s \equiv_\mathcal{E} t$

First, we show that $s \leftrightarrow_\mathcal{E} t$ implies $s \equiv_\mathcal{E} t$.

$s \leftrightarrow_{\mathcal{E}} t$

$\rightsquigarrow$ there is a $t_1 \equiv t_2$ or $t_2 \equiv t_1$ in $\mathcal{E}$ such that

$s|_\pi = t_1\sigma$, $t = s[t_2\sigma]_\pi$ for some π, σ

We have $t_1 \equiv_{\mathcal{E}} t_2$ by symmetry of $\equiv_{\mathcal{E}}$ (Lemma 3.1.10)

$\rightsquigarrow$ $t_1\sigma \equiv_{\mathcal{E}} t_2\sigma$ by stability of $\equiv_{\mathcal{E}}$ (Lemma 3.1.4(d))

$\rightsquigarrow$ $s[t_1\sigma]_\pi \equiv_{\mathcal{E}} s[t_2\sigma]_\pi$ by monotonicity of $\equiv_{\mathcal{E}}$ (Lemma 3.1.8(b))

$\rightsquigarrow$ $s \equiv_{\mathcal{E}} t$

Now we show that $s \leftrightarrow^*_{\mathcal{E}} t$ implies $s \equiv_{\mathcal{E}} t$:

Let $s \leftrightarrow^n_{\mathcal{E}} t$ for $n \in \mathbb{N}$. We use induction on n.

Ind. Base: $n = 0$

$s \leftrightarrow^0_{\mathcal{E}} t$

$\rightsquigarrow$ $s = t$

$\rightsquigarrow$ $s \equiv_{\mathcal{E}} t$ by reflexivity of $\equiv_{\mathcal{E}}$ (Lemma 3.1.10)

Ind. Step $n > 0$

$s = s_0 \leftrightarrow_{\mathcal{E}} s_1 \leftrightarrow_{\mathcal{E}} s_2 \leftrightarrow_{\mathcal{E}} \dots \leftrightarrow_{\mathcal{E}} s_{n-1} \leftrightarrow_{\mathcal{E}} s_n = t$

By the induction hypothesis:

$s \leftrightarrow^{n-1}_{\mathcal{E}} s_{n-1}$ implies $s \equiv_{\mathcal{E}} s_{n-1}$

By the claim above

$s_{n-1} \leftrightarrow_{\mathcal{E}} t$ implies $s_{n-1} \equiv_{\mathcal{E}} t$

$\Big\}$ $s \equiv_{\mathcal{E}} t$ by transitivity of $\equiv_{\mathcal{E}}$ (Lemma 3.1.10)

"$\Rightarrow$" Completeness: show that $s \equiv_{\mathcal{E}} t$ implies $s \leftrightarrow^*_{\mathcal{E}} t$

$s \equiv_{\mathcal{E}} t$ means that $\mathcal{A} \models \mathcal{E}$ implies $\mathcal{A} \models s \equiv t$

Idea of the proof:

(A)

- Construct a specific $A=(\mathcal{A},\alpha)$ and a specific variable assignment β such that for $I=(\mathcal{A},\alpha,\beta)$ we have

$$I \models s \equiv t \quad \text{iff} \quad s \leftrightarrow^*_{\mathcal{E}} t$$

(B)
- Then show that $A \models \mathcal{E}$.
- This proves the desired claim:

$$s \equiv_{\mathcal{E}} t$$
$$\curvearrowright A \models s \equiv t \quad (\text{since } A \models \mathcal{E})$$
$$\curvearrowright I \models s \equiv t \quad (\text{since } I \text{ results from } A \text{ by adding the variable assignment } \beta)$$
$$\curvearrowright s \leftrightarrow^*_{\mathcal{E}} t$$

(A) Define $I=(\mathcal{A},\alpha,\beta)$ such that
$I \models s \equiv t$ iff $s \leftrightarrow^*_{\mathcal{E}} t$.

First idea: interpret every term "as itself",
i.e., choose an interpretation where
$I(t)=t$ for any term t

Then: $\mathcal{A} = \mathcal{T}(\Sigma,\mathcal{V})$

$\alpha_f = f$ for any $f \in \Sigma$

$\beta(x) = x$ for any $x \in \mathcal{V}$

Now indeed $I(t)=t$ for all terms.

But this is not yet what we want.
If $s \leftrightarrow^*_{\mathcal{E}} t$, then we want $I(s)=I(t)$.
Solution: I should not map every term to itself,
but it should map every term to its equivalence
class wrt. $\leftrightarrow^*_{\mathcal{E}}$, i.e.: $I(t) = [t]$.

For any equivalence relation, the <u>equivalence class</u> of an object t is the set of all objects that are equivalent to t:

$$[t]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}} = \{ s \mid s \overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}} t \}$$

(e.g.: $[\mathcal{O}]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}} = \{ \mathcal{O}, plus(\mathcal{O},\mathcal{O}), plus(plus(\mathcal{O},\mathcal{O}),\mathcal{O}), \ldots \}$)

The <u>quotient set</u> $\mathcal{T}(\Sigma,\mathcal{V})/_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}$ is the set of all equivalence classes, i.e.: $\mathcal{T}(\Sigma,\mathcal{V})/_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}} = \{ [t]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}} \mid t \in \mathcal{T}(\Sigma,\mathcal{V}) \}$.

e.g.: $\mathcal{T}(\Sigma,\mathcal{V})/_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}} = \{ [\mathcal{O}]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}, [succ(\mathcal{O})]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}, \ldots, [x]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}, [y]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}, [plus(x,y)]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}, \ldots \}$)

Now we want to define an interpretation I which interprets every term t as its equivalence class $[t]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}$.

Then: $I \models s \equiv t$ iff $I(s) = I(t)$

iff $[s]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}} = [t]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}$

iff $s \overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}} t$.

$I = (\mathcal{A}, \alpha, \beta)$ with

- $\mathcal{A} = \mathcal{T}(\Sigma,\mathcal{V})/_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}$
- α_f: We want $I(f(t_1,\ldots,t_n)) = \alpha_f(\underbrace{I(t_1)}_{[t_1]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}},\ldots,\underbrace{I(t_n)}_{[t_n]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}})$

$$\overset{!}{=} [f(t_1,\ldots,t_n)]_{\overset{*}{\underset{\mathcal{E}}{\longleftrightarrow}}}.$$

$$\doteq [f(t_1,\dots,t_n)]_{\overset{*}{\leftrightarrow}_\mathcal{E}}.$$

Thus: $\alpha_f([t_1]_{\overset{*}{\leftrightarrow}_\mathcal{E}},\dots,[t_n]_{\overset{*}{\leftrightarrow}_\mathcal{E}}) = [f(t_1,\dots,t_n)]_{\overset{*}{\leftrightarrow}_\mathcal{E}}.$

- β: We want $\underbrace{I(x)}_{\beta(x)} = [x]_{\overset{*}{\leftrightarrow}_\mathcal{E}}.$

Thus: $\beta(x) = [x]_{\overset{*}{\leftrightarrow}_\mathcal{E}}$ for all $x \in \mathcal{V}$.

Now indeed: $I(t) = [t]_{\overset{*}{\leftrightarrow}_\mathcal{E}}$ (can be shown by structural induction).

$\rightsquigarrow$ (A) solved.

Next we solve (B):
We have to show that $\overbrace{(\mathcal{T}(\Sigma,\mathcal{V})/_{\overset{*}{\leftrightarrow}_\mathcal{E}}, \alpha)}^{A} \models \mathcal{E}$.
Let $u \equiv v \in \mathcal{E}$.
We have to show $A \models u \equiv v$.
Let φ be a variable assignment, let $\mathcal{J} = (\mathcal{T}(\Sigma,\mathcal{V})/_{\overset{*}{\leftrightarrow}_\mathcal{E}}, \alpha, \varphi)$:
we have to show $\mathcal{J} \models u \equiv v$, i.e., $\mathcal{J}(u) = \mathcal{J}(v)$.
For any variable x, let s_x be a term from the equivalence class $\varphi(x)$. In other words: $\varphi(x) = [s_x]_{\overset{*}{\leftrightarrow}_\mathcal{E}}$.
Let σ be the substitution with $x\sigma = s_x$ for all variables occurring in $\mathcal{E}$.
Then: $\mathcal{J}(x) = \varphi(x) = [s_x]_{\overset{*}{\leftrightarrow}_\mathcal{E}} = [x\sigma]_{\overset{*}{\leftrightarrow}_\mathcal{E}}.$
By structural induction, one can show that for all terms t, we have

$$\mathcal{J}(t) = [t\sigma]_{\overset{*}{\leftrightarrow}_\mathcal{E}}.$$

Now one can show that for any $u \equiv v \in \mathcal{E}$, we have
$\mathcal{J}(u) = \mathcal{J}(v)$:

$u \equiv v \quad \in \mathcal{E}$

$\curvearrowright \quad u \overset{*}{\longleftrightarrow}_{\mathcal{E}} v$

$\curvearrowright \quad u\sigma \overset{*}{\longleftrightarrow}_{\mathcal{E}} v\sigma \quad$ (since $\overset{*}{\longleftrightarrow}_{\mathcal{E}}$ is stable, Lemma 3.1.13)

$\curvearrowright \quad [u\sigma]_{\overset{*}{\longleftrightarrow}_{\mathcal{E}}} = [v\sigma]_{\overset{*}{\longleftrightarrow}_{\mathcal{E}}}$

$\curvearrowright \quad \mathcal{J}(u) = \mathcal{J}(v)$

This implies $\mathcal{A} \models u \equiv v$ and finishes the proof of (B).

$\boxtimes$

By Birkhoff's Theorem we can now try to solve the word problem automatically.

<u>Ex. 3.1.15</u>

$\mathcal{E}$ = set of the 3 group axioms

Goal: Solve the word problem $i(i(n)) \equiv_{\mathcal{E}} n$.

By Birkhoff's Thm., this is equivalent to $i(i(n)) \overset{*}{\longleftrightarrow}_{\mathcal{E}} n$

In general: To prove $s \overset{*}{\longleftrightarrow}_{\mathcal{E}} t$ automatically, one can construct a search tree:

where $s_1, s_2, \dots$ are all terms that are reachable from s in one step with $\longleftrightarrow_{\mathcal{E}}$

Then we check if t occurs in this tree.

If yes, then $s \overset{*}{\longleftrightarrow}_{\mathcal{E}} t$ and therefore $s \equiv_{\mathcal{E}} t$.

If no, then $s \overset{*}{\not\longleftrightarrow}_{\mathcal{E}} t$ and therefore $s \not\equiv_{\mathcal{E}} t$.

<u>Problems:</u>

- Paths could be infinitely long (depth could be infinite)

- Node could have infinitely many children
  (This happens if $\mathcal{E}$ contains equations $u \equiv v$ with $\mathcal{V}(u) \neq \mathcal{V}(v)$)
  (breadth could be infinite)

The word problem for equations is not decidable, but semi-decidable:

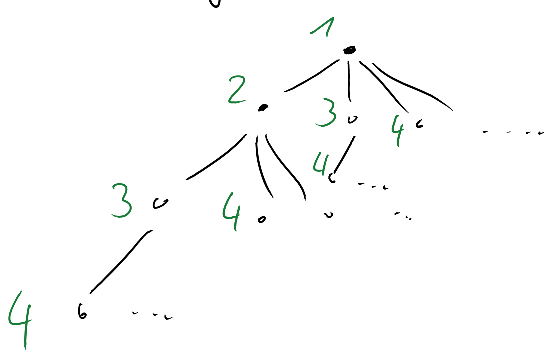
Given a set of equations $\mathcal{E}$ and $s \equiv t$:

if $s \equiv_{\mathcal{E}} t$: procedure terminates with "yes"

if $s \not\equiv_{\mathcal{E}} t$: procedure might not terminate (or say "no")

Semi-Decision Procedure:

- build up the search tree starting with s
- stop as soon as one reaches t
- if $\mathcal{V}(t_1) = \mathcal{V}(t_2)$ for all $t_1 \equiv t_2 \in \mathcal{E}$, then one can build up the tree with breadth-first search
- otherwise, one has to construct the tree "by diagonalization" to ensure that eventually one reaches every node of the tree:



2 main drawbacks

- search not goal directed: if $s \leftrightarrow^*_{\mathcal{E}} t$ holds, it will take very long to find the proof
- not useful to disprove equations: if $s \leftrightarrow^*_{\mathcal{E}} t$ doesn't hold,

then the procedure usually doesn't terminate.

<u>Therefore</u>: • Identify classes of $\mathcal{E}$ where $=_{\mathcal{E}}$ is decidable.

• Develop more efficient procedures for these cases.