6.3a Implicit Induction (Part 1)

Donnerstag, 14. Januar 2016 12:30

up to now:

Given a set of equations $\mathcal{E}$, two terms s, t check whether $\mathcal{E} \models s \equiv t$ holds.

This means: is $s \equiv t$ true in all models of $\mathcal{E}$ (i.e., does $A \models \mathcal{E}$ imply $A \models s \equiv t$ for all algebras A)?

But: in prog. verification, we are not interested in all models, but only in certain specific models of $\mathcal{E}$.

Ex. 6.31 plus-equations (slide)

We want to verify the following statement about our plus-equations $\mathcal{E}$:

$$\underbrace{plus(X, succ(Y))}_{s} \equiv \underbrace{succ(plus(X, Y))}_{t}$$

$\mathcal{R}$ is a convergent TRS that is equivalent to $\mathcal{E}$:

$$s =_{\mathcal{E}} t \quad \text{iff} \quad s\downarrow_{\mathcal{R}} = t\downarrow_{\mathcal{R}}$$

Here: s and t are already in normal form

$\rightsquigarrow \quad s \neq_{\mathcal{E}} t.$

Problem: "$s =_{\mathcal{E}} t$" requires that $s \equiv t$ is true in all models. But in prog. verif., we are only interested

in a model like $\mathcal{A} = (\mathbb{N}, \alpha)$ where

$\alpha_0 = 0$

$\alpha_{succ}(n) = n+1$

$\alpha_{plus}(n,m) = n+m$.

Here, we have $\mathcal{A} \models \mathcal{E}$ and $\mathcal{A} \models s \equiv t$

But $\mathcal{E}$ also has models $\mathcal{B}$ where $\mathcal{B} \models \mathcal{E}$, $\mathcal{B} \not\models s \equiv t$:
Such models typically contain elements in their domain that do not correspond to any ground term.
E.g.: $\mathcal{B} = (\mathbb{N} \cup \{\square, \triangle\}, \alpha')$ with

$\alpha'_0 = 0$

$\alpha'_{succ}(n) = \begin{cases} n+1, & \text{if } n \in \mathbb{N} \\ \triangle, & \text{if } n \in \{\square, \triangle\} \end{cases}$

$\alpha'_{plus}(n,m) = \begin{cases} n+m, & \text{if both } n,m \in \mathbb{N} \\ n, & \text{if } n \in \{\square, \triangle\} \\ m, & \text{if } n=0,\ m \in \{\square, \triangle\} \\ \triangle, & \text{if } n>0,\ m \in \{\square, \triangle\} \end{cases}$

We have $\mathcal{B} \models \mathcal{E}$:

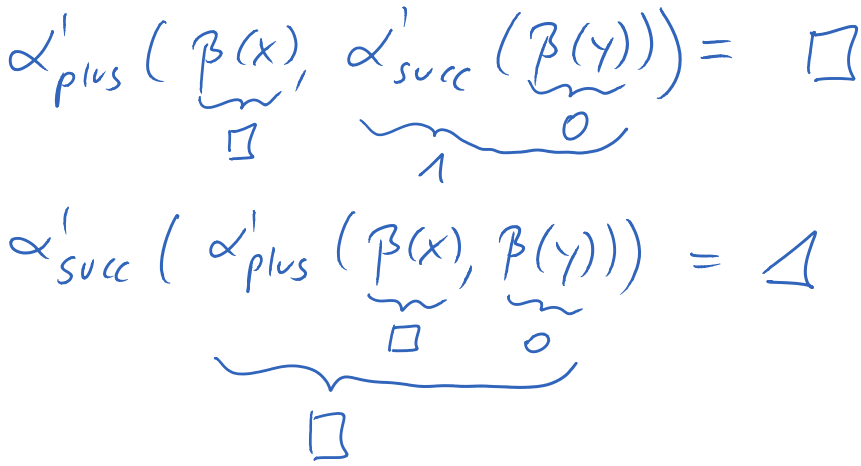
$\mathcal{B} \models plus(0, y) \equiv y$, since for any var. assignment β we have

$\alpha'_{plus}(\underbrace{\alpha'_0}_{0}, \beta(y)) = \beta(y)$ ✓

$\mathcal{B} \models plus(succ(x), y) \equiv succ(plus(x,y))$, ...

But $\mathcal{B} \not\models plus(x, succ(y)) \equiv succ(plus(x,y))$

To see this, let $\beta(x) = \square$, $\beta(y) = 0$.



So instead of validity in all models, we should check if $s \equiv t$ holds if one instantiates their variables with ground terms like 0, $succ(0)$, $succ(succ(0))$, ...

In other words, we want to know whether a statement about a program holds for all possible data objects.

Solution: define a new notion of tmt/validity which only considers instantiations of variables by ground terms.

Variable now stands for "all natural numbers, lists, ..." not for "all elements of the domain of an algebra".

Def 632 (Inductive Validity)

Let $\mathcal{E}$ be a set of equations over Σ and $\mathcal{V}$, let $s, t \in T(\Sigma, \mathcal{V})$.

The equation $s \equiv t$ is inductively valid for $\mathcal{E}$ (denoted $\mathcal{E} \models_I s \equiv t$) iff

$\mathcal{E} \vdash s\sigma \equiv t\sigma$ for all substitutions σ where

$\sigma(x) \in \mathcal{T}(\Sigma)$ for all $x \in \mathcal{V}(s) \cup \mathcal{V}(t)$.

Ex. 633

If $\mathcal{E}$ are the plus equations, then

$\mathcal{E} \not\vdash \underbrace{plus(x, succ(y))}_{s} \equiv \underbrace{succ(plus(x,y))}_{t}$ but

$\mathcal{E} \vdash_I \quad s \quad \equiv \quad t$

This can be shown by induction.

We have to show that for all ground terms t_1, t_2, we have:

$\mathcal{E} \vdash plus(t_1, succ(t_2)) \equiv succ(plus(t_1, t_2))$

let $\mathcal{R}$ again be the convergent TRS that is equivalent to $\mathcal{E}$.

We have to show

$$plus(t_1, succ(t_2)) \downarrow_{\mathcal{R}} \quad succ(plus(t_1, t_2)).$$

Since plus is "completely defined" in $\mathcal{R}$, we can first rewrite t_1, t_2 until they dont contain plus anymore.

Thus, it suffices to show

$$plus(succ^n(0), succ^{m+1}(0)) \downarrow_{\mathcal{R}} succ(plus(succ^n(0), succ^m(0)))$$

This is easy to prove by induction on n.

Goal: Prove $\mathcal{E} \vdash_I s \equiv t$ automatically

One could try to perform an induction proof on all possible ground terms.

Problems for automation: find suitable suitable induction variables

induction relations, ...

Alternative approach: do not perform induction explicitly, but re-use (a slight variant of) the completion algorithm. Here, the induction is only performed implicitly.

Surprising observation: $\mathcal{E} \vdash_I s \equiv t$ iff

adding $s \equiv t$ to $\mathcal{E}$ does not result in an "inconsistent" set of equations.

↑ the set is considered inconsistent if one can now prove equations $u \equiv v$ between ground terms that did not hold before

Thm 6.3.4 (Proof by Consistency)

$\mathcal{E} \vdash_I s \equiv t$ iff for all ground terms u, v:

$$\mathcal{E} \not\vdash u \equiv v \text{ implies } \mathcal{E} \cup \{s \equiv t\} \not\vdash u \equiv v.$$

Proof: "⇒": Let $\mathcal{E} \vdash_I s \equiv t$, let $\mathcal{E} \cup \{s \equiv t\} \vdash u \equiv v$.

We have to show that $\mathcal{E} \vdash u \equiv v$.

By Birkhoff's Thm (Thm 3.1.14), we have:

$$u = u_0 \underset{\mathcal{E} \cup \{s \equiv t\}}{\hookleftarrow} u_1 \underset{\mathcal{E} \cup \{s \equiv t\}}{\hookleftarrow} \dots \underset{\mathcal{E} \cup \{s \equiv t\}}{\hookleftarrow} u_n = v$$

Let δ be a substitution that instantiates all variables of $u_0, \dots, u_n$ by arbitrary ground terms. Then stability of $\underset{\mathcal{E} \cup \{s \equiv t\}}{\hookleftarrow}$ implies:

$\mathcal{E} \cup \{s \equiv t\}$ implies:

$u = u\delta = u_0\delta \hookrightarrow_{\mathcal{E} \cup \{s \equiv t\}} u_1\delta \hookrightarrow_{\mathcal{E} \cup \{s \equiv t\}} \dots \hookrightarrow_{\mathcal{E} \cup \{s \equiv t\}} u_n\delta = v\delta = v$

Since all $u_i\delta$ are ground terms, this derivation could also be done with $\hookrightarrow_{\mathcal{E} \cup \{s\sigma \equiv t\sigma \mid \sigma \text{ ground substitution}\}}$.

By Birkhoff's Thm., this means

$\mathcal{E} \cup \{s\sigma \equiv t\sigma \mid \sigma \text{ ground subst.}\} \models u \equiv v$,

i.e. every model of $\mathcal{E} \cup \{s\sigma \equiv t\sigma \mid \dots\}$ is also a model of $u \equiv v$.

Since $\mathcal{E} \vDash_I s \equiv t$, every model of $\mathcal{E}$ is also a model of $\{s\sigma \equiv t\sigma \mid \sigma \text{ gr. subst}\}$.

$\curvearrowright \quad \mathcal{E} \models u \equiv v$.

"$\Leftarrow$": Prerequisite: $\mathcal{E} \cup \{s \equiv t\} \models u \equiv v$ implies $\mathcal{E} \models u \equiv v$.

Clearly: $\mathcal{E} \cup \{s \equiv t\} \vDash s\sigma \equiv t\sigma$ for all ground subst. σ

$\curvearrowright \quad \mathcal{E} \vDash s\sigma \equiv t\sigma$ — " —

Prereq.

$\curvearrowright \quad \mathcal{E} \vDash_I s \equiv t$

TES

To use this theorem for automated proofs, we would have to inspect all possible ground terms u, v where $\mathcal{E} \nvDash u \equiv v$ and check whether $\mathcal{E} \cup \{s \equiv t\} \nvDash u \equiv v$.

Problematic, since there are infinitely many such ground

terms u, v.

The next observation shows:

- We use a convergent TRS $\mathcal{R}$ that is equivalent to $\mathcal{E}$.
- Instead of all ground terms u, v with $\mathcal{E} \not\models u \approx v$, we only have to inspect all ground normal forms q_1, q_2 of $\mathcal{R}$ where $q_1 \neq q_2$.

Ground normal forms:

$$NF(\mathcal{R}) = \{ q\downarrow_{\mathcal{R}} \mid q \in \mathcal{T}(\Sigma) \}.$$

For the plus-TRS $\mathcal{R}$:

$$NF(\mathcal{R}) = \{ 0, succ(0), succ^2(0), \dots \} \quad (\hat{=} \mathbb{N})$$

So to prove $\mathcal{E} \models_I plus(x, succ(y)) \approx succ(plus(x,y))$, we can now check whether there are $q_1, q_2 \in NF(\mathcal{R})$ with $q_1 \neq q_2$ such that $\mathcal{E} \cup \{plus(x, succ(y)) \approx succ(plus(x,y))\} \models q_1 \approx q_2$.

Thm 6.3.5 (Proof by Consistency with convergent TRSs)

Let $\mathcal{R}$ be a convergent TRS that is equivalent to $\mathcal{E}$.

$\mathcal{E} \models_I s \approx t$ iff for all $q_1, q_2 \in NF(\mathcal{R})$, $q_1 \neq q_2$ implies $\mathcal{E} \cup \{s \approx t\} \not\models q_1 \approx q_2$.

Proof: "$\Rightarrow$": Let $\mathcal{E} \models_I s \approx t$, let $q_1, q_2 \in NF(\mathcal{R})$ with $\mathcal{E} \cup \{s \approx t\} \models q_1 \approx q_2$ where $q_1 \neq q_2$.

By Thm 6.3.4: $\mathcal{E} \models q_1 \approx q_2$

Since $\mathcal{R}$ is convergent and equivalent to $\mathcal{E}$: $q_1 \downarrow_{\mathcal{R}} q_2$

As q_1, q_2 are normal forms, this implies $q_1 = q_2$. ↯

"$\Leftarrow$": We assume $\mathcal{E} \not\vdash_I s \equiv t$

By Thm 6.3.4., there exist ground terms u, v such that

$\mathcal{E} \not\vdash u \equiv v$ and $\mathcal{E} \cup \{s \equiv t\} \vdash u \equiv v$.

Let $q_1 = u\downarrow_{\mathcal{R}}$, $q_2 = v\downarrow_{\mathcal{R}}$. We must have $q_1 \neq q_2$, because otherwise the equivalence of $\mathcal{R}$ and $\mathcal{E}$ would imply $\mathcal{E} \vdash u \equiv v$.

Moreover:

$\mathcal{E} \cup \{s \equiv t\} \vdash q_1 \equiv u \equiv v \equiv q_2$ ↯ to the pre-requisite