Program Verification: Lecture 14

José Meseguer

Computer Science Department
University of Illinois at Urbana-Champaign

Provable Theorems and Theorems of an Equational Theory (Σ, E)

For $\Sigma = ((S, \leq), G)$ and order-sorted signature, define the set of Σ-equations in the obvious way (where X has a countably infinite set X_s of variables for each sort $s \in S$):

$$\Sigma.Eq = \{u = v \mid \exists s, s' \in S.\ u \in T_\Sigma(X)_s \wedge v \in T_\Sigma(X)_{s'} \wedge [s] = [s']\}.$$

Given any set of Σ-equations $E \subseteq \Sigma.Eq$, define the set of its provable theorems as:

$$PThm(E) = \{u = v \in \Sigma.Eq \mid u =_E v\}.$$

Likewise, for any $E \subseteq \Sigma.Eq$, define the set of its theorems as:

$$Thm(E) = \{u = v \in \Sigma.Eq \mid \forall \mathbb{A} \in \mathbf{Alg}_{(\Sigma,E)},\ \mathbb{A} \models u = v\}.$$

The Soundness and Completeness Theorems show that we have:

$$PThm(E) = Thm(E).$$

Inductive Theorems of an Equational Theory (Σ, E)

Given any Σ-algebra $\mathbb{A}$, define its set of theorems as:

$$Thm(\mathbb{A}) = \{u = v \in \Sigma.Eq \mid \mathbb{A} \models u = v\}.$$

Then, given an equational theory (Σ, E) define its set of inductive theorems $IndThm(\Sigma, E)$ by the set-theoretic equality:

$$IndThm(\Sigma, E) =_{def} Thm(\mathbb{T}_{\Sigma/E}).$$

In particular, when a functional module $\texttt{fmod}(\Sigma, E \cup B)\texttt{endfm}$ is (ground) confluent, terminating and sufficiently complete w.r.t. constructors Ω, since $\mathbb{T}_{\Sigma/E \cup B} \cong \mathbb{C}_{\Sigma,E/B}$, and by Ex.12.2 we know that $Thm(\mathbb{T}_{\Sigma/E}) = Thm(\mathbb{C}_{\Sigma,E/B})$, in this case $IndThm(\Sigma, E)$ are the equational properties satisfied by the equational program $\texttt{fmod}(\Sigma, E \cup B)\texttt{endfm}$. Thus, the notion of inductive theorem is a crucial concept in program verification.

Inductive Theorems of an Equational Theory (Σ, E) (II)

By definition, given a Σ-equation $u = v$, we write $E \models_{ind} u = v$, or $(\Sigma, E) \models_{ind} u = v$, and say that $u = v$ is an inductive theorem or an inductive consequence of E iff $(u = v) \in \mathit{IndThm}(\Sigma, E)$.

But since $\mathit{IndThm}(\Sigma, E) = \mathit{Thm}(\mathbb{T}_{\Sigma/E})$ and $\mathbb{T}_{\Sigma/E} \models E$, we have an inclusion $\mathit{Thm}(E) \subseteq \mathit{IndThm}(\Sigma, E)$, and therefore an implication:

$$E \models u = v \quad \Rightarrow \quad E \models_{ind} u = v$$

In general, however, the converse implication does not hold: there are theories (Σ, E) and Σ-equations $u = v$ such that $\mathbb{T}_{\Sigma/E} \models u = v$ but $E \not\models u = v$, so that, by Soundness and Completeness, $E \not\vdash u = v$. Let us see some examples.

Can have $\mathbb{T}_{\Sigma/E} \models u = v$ but $E \not\vdash u = v$

Consider the unsorted signature $\Sigma = \{0, s, \_ + \_\}$ with $E = \{x + 0 = x, x + s(y) = s(x + y)\}$. We have already proved that $\vec{E}$ is confluent and terminating. It is well-known and easy to prove (it will be done in a later lecture) that $+_{\mathbb{C}_{\Sigma,E/B}}$ is associative and commutative. Therefore, $\mathbb{T}_{\Sigma/E} \models x + y = y + x$, and $\mathbb{T}_{\Sigma/E} \models (x + y) + x = x + (y + z)$. However,

$$E \not\vdash x + y = y + x \quad \textit{and} \quad E \not\vdash (x + y) + z = x + (y + z)$$

since, by the Church-Rosser Theorem, $x + y =_E y + x$ iff $(x + y)!_{\vec{E}} = (y + x)!_{\vec{E}}$, and $(x + y) + z =_E x + (y + z)$ iff $((x + y) + z)!_{\vec{E}} = (x + (y + z))!_{\vec{E}}$. But, those canonical forms are all different, because the terms involved, $x + y$, $y + x$, $(x + y) + z$ and $x + (y + z)$ are all in $\vec{E}$-canonical form: no $\vec{E}$ rules apply to them.

Characterizing the Inductive Theorems of $(\Sigma, E \cup B)$

Can we say something about when $(u = v) \in \mathit{IndThm}(\Sigma, E \cup B)$?

Theorem (Characterization of Inductive Theorems):

1. $(u = v) \in \mathit{IndThm}(\Sigma, E \cup B)$ iff
   $\forall \theta \in [X \to T_\Sigma], E \cup B \vdash u\theta = v\theta$, where $X = \mathit{vars}(u) \cup \mathit{vars}(v)$.

2. If rules $\vec{E}$ are sort-decreasing, ground confluent, terminating and sufficiently complete w.r.t. Ω modulo B,

   $$(u = v) \in \mathit{IndThm}(\Sigma, E \cup B) \quad \Leftrightarrow \quad \forall \rho \in [X \to T_\Omega], E \cup B \vdash u\rho = v\rho.$$

Proof Hints: (1) follows from $\mathbb{T}_{\Sigma/E\cup B} \models u = v$, since any assignment $a \in [X \to T_{\Sigma/E}]$ is of the form $a = \theta; [\_]_{E\cup B}$ for some $\theta \in [X \to T_\Sigma]$. The proof of (2) is a variant of that of (1) using the (ground) Church-Rosser Theorem modulo B, sufficient completeness and the isomorphism $\mathbb{T}_{\Sigma/E\cup B} \cong \mathbb{C}_{\Sigma/\vec{E},B}$.

Inductive Theorems do not Change the Initial Algebra

Theorem (Lemma Internalization Theorem 1) Let (Σ, E) be an equational theory and G a set of Σ-equations such that $(\Sigma, E) \models_{ind} G$. Then, $\mathbb{T}_{\Sigma/E} = \mathbb{T}_{\Sigma/E \cup G}$.

Proof: Since $\mathbb{T}_{\Sigma/E \cup G} \models E$ we have a unique Σ-homomorphism $h : \mathbb{T}_{\Sigma/E} \to \mathbb{T}_{\Sigma/E \cup G}$. And since $\mathbb{T}_{\Sigma/E} \models E \cup G$, we also have a unique Σ-homomorphism $g : \mathbb{T}_{\Sigma/E \cup G} \to \mathbb{T}_{\Sigma/E}$. But then, the initiality of $\mathbb{T}_{\Sigma/E}$ forces $h; g = id_{\mathbb{T}_{\Sigma/E}}$, and the initiality of $\mathbb{T}_{\Sigma/E \cup G}$ forces $g; h = id_{\mathbb{T}_{\Sigma/E \cup G}}$. Therefore, we have an isomorphism: $\mathbb{T}_{\Sigma/E} \cong \mathbb{T}_{\Sigma/E \cup G}$. We will be done of we prove the following lemma:

Lemma Let E, E' be two sets of Σ-equations such that $\mathbb{T}_{\Sigma/E} \cong \mathbb{T}_{\Sigma/E'}$. Then, $\mathbb{T}_{\Sigma/E} = \mathbb{T}_{\Sigma/E'}$.

Inductive Theorems do not Change the Initial Algebra (II)

Proof of the Lemma: $\mathbb{T}_{\Sigma/E}$ and $\mathbb{T}_{\Sigma/E'}$ are uniquely determined by the respective ground equality relations $=_E \cap T_\Sigma^2$ and $=_{E'} \cap T_\Sigma^2$. We just need to show $(=_E \cap T_\Sigma^2) = (=_{E'} \cap T_\Sigma^2)$. Since we have a Σ-isomorphism $h : \mathbb{T}_{\Sigma/E} \to \mathbb{T}_{\Sigma/E'}$, and unique Σ-homomorphisms $[\_]_E : \mathbb{T}_\Sigma \to \mathbb{T}_{\Sigma/E}$, and $[\_]_{E'} : \mathbb{T}_\Sigma \to \mathbb{T}_{\Sigma/E}$, the initiality of $\mathbb{T}_\Sigma$ forces $[\_]_E ; h = [\_]_{E'}$, i.e., $h_s([t]_E) = [t]_{E'}$ for each $t \in T_{\Sigma,s}$, $s \in S$. Let $t \in T_{\Sigma,s}$ and $t' \in T_{\Sigma,s'}$ with $t =_E t'$. Then $[s] = [s']$ and, by h order-sorted Σ-homomorphism and $[t]_E = [t']_E$, we must have $h_s([t]_E) = h_{s'}([t']_E)$, which forces:

$$h_s([t]_E) = [t]_{E'} = [t']_{E'} = h_{s'}([t']_E)$$

giving us the containment $(=_E \cap T_\Sigma^2) \subseteq (=_{E'} \cap T_\Sigma^2)$. Using the inverse isomorphism h^{-1} we likewise get $(=_{E'} \cap T_\Sigma^2) \subseteq (=_E \cap T_\Sigma^2)$, giving us $(=_E \cap T_\Sigma^2) = (=_{E'} \cap T_\Sigma^2)$, as desired. q.e.d. q.e.d.

Equivalence of Equational Theories

Call two equational theories (Σ, E) and (Σ, E') equivalent, denoted $(\Sigma, E) \equiv (\Sigma, E')$ iff (by definition) $E \vdash E'$ and $E' \vdash E$.

Ex.14.1 Prove: (i) $(\Sigma, E) \vdash E' \Rightarrow (=_{E'}) \subseteq (=_E) \wedge (=_E) = (=_{E \cup E'})$,

(ii) $(\Sigma, E) \equiv (\Sigma, E') \;\Leftrightarrow\; (=_E) = (=_{E'}) \;\Leftrightarrow\; \mathbf{Alg}_{(\Sigma,E)} = \mathbf{Alg}_{(\Sigma,E')}$.

For example, the sets of equations $E = \{x \cdot (y \cdot z) = (x \cdot y) \cdot z, x \cdot 1 = x = 1 \cdot x, x \cdot x^{-1} = 1, 1 = x^{-1} \cdot x\}$, and $E' = \{(x \cdot y) \cdot z = x \cdot (y \cdot z), 1 \cdot x = x, x \cdot 1 = x, x \cdot x^{-1} = 1, x^{-1} \cdot x = 1, 1^{-1} = 1, (x^{-1})^{-1} = x, (x \cdot y)^{-1} = y^{-1} \cdot x^{-1}, x \cdot (x^{-1} \cdot y) = y, x^{-1} \cdot (x \cdot y) = y\}$ define equivalent theories $(\Sigma, E) \equiv (\Sigma, E')$ for the theory of groups. But E' is much better, because $\vec{E}'$ is confluent and terminating. Therefore, by the Church-Rosser Theorem we can decide whether any Σ-equality $u = v$ is a theorem of group theory by checking whether $u!_{\vec{E}'} = v!_{\vec{E}'}$.

Inductive Equivalence of Equational Theories

Call two equational theories (Σ, E) and (Σ, E') inductively equivalent, denoted $(\Sigma, E) \equiv_{ind} (\Sigma, E')$ iff (by definition) $(\Sigma, E) \models_{ind} E'$ and $(\Sigma, E') \models_{ind} E$.

Ex.14.2 Prove:

$(i)(\Sigma, E) \models_{ind} E' \Rightarrow (=_{E'} \cap T_\Sigma^2) \subseteq (=_E \cap T_\Sigma^2) \wedge (=_E \cap T_\Sigma^2) = (=_{E \cup E'} \cap T_\Sigma^2)$

(ii) $(\Sigma, E) \equiv_{ind} (\Sigma, E') \;\Leftrightarrow\; (=_E \cap T_\Sigma^2) = (=_{E'} \cap T_\Sigma^2) \;\Leftrightarrow\; \mathbb{T}_{\Sigma/E} = \mathbb{T}_{\Sigma/E'}$.

Ex.14.1 and **Ex**.14.2 give us $(\Sigma, E) \equiv (\Sigma, E') \Rightarrow (\Sigma, E) \equiv_{ind} (\Sigma, E')$. But in general $(\Sigma, E) \equiv_{ind} (\Sigma, E')$ does not imply $(\Sigma, E) \equiv (\Sigma, E')$.

For example, in pg. 5 we saw that for $\Sigma = \{0, s, \_ + \_\}$ and $E = \{x + 0 = x, x + s(y) = s(x + y)\}$, $\mathbb{T}_{\Sigma/E} \models x + y = y + x$. Thus, by the Lemma Internalization Theorem 1 and **Ex**.14.2 we have $(\Sigma, E) \equiv_{ind} (\Sigma, E \cup \{x + y = y + x\})$. But we saw in pg. 5 that $E \not\vdash x + y = y + x$, and therefore $(\Sigma, E) \not\equiv (\Sigma, E \cup \{x + y = y + x\})$.

Semantic Equivalence of Equational Programs

In Program Verification a fundamental question is:

> When are two different programs semantically equivalent?

The most obvious answer for admissible equational programs `fmod` (Σ, E) `endfm` and `fmod` (Σ, E') `endfm` is:

> When they compute the same recursive functions,

which mathematically just means: when $\mathbb{C}_{\Sigma/\vec{E}} = \mathbb{C}_{\Sigma/\vec{E}'}$.

For example, we shall prove that for $\Sigma = \{0, s, \_+\_\}$, $E = \{x + 0 = x, x + s(y) = s(x + y)\}$ and $E' = \{0 + x = x, s(x) + y = s(x + y)\}$, `fmod` (Σ, E) `endfm` and `fmod` (Σ, E') `endfm` are equivalent equational programs: both compute the addition function on natural numbers $+_{\mathbb{N}}$.

Let us give a more precise definition.

Admissible and Comparable programs

Call `fmod` $(\Sigma, E \cup B)$ `endfm` admissible iff (i) Σ is B-preregular, with non-empty sorts, (ii) $\vec{E}$ is sort-decreasing, and ground confluent and terminating modulo B, and (iii) it is sufficiently complete w.r.t. a constructor subsignature Ω.

Call $(\Sigma, E \cup B)$ satisfying (i)–(ii) ground convergent modulo B.

Given a constructor subsignature $\Omega \subseteq \Sigma$, let Ω^+ denote the signature that extends Ω by adding all non-constructor operator typings that are subsort-overloaded with some operator in Ω. Call two admissible equational programs `fmod` $(\Sigma, E \cup B)$ `endfm` and `fmod` $(\Sigma, E' \cup B')$ `endfm`, both with constructors Ω, comparable iff: (i) $E = E_0 \uplus E_{\Omega^+}$ and $E' = E'_0 \uplus E_{\Omega^+}$, with E_{Ω^+} Ω^+-equations, and each rule in $\vec{E}_0 \cup \vec{E'}_0$ is of the form $f(u_1, \ldots, u_n) \to v$, with f in $\Sigma \setminus \Omega^+$, and (ii) $B = B_0 \uplus B_{\Omega^+}$ and $B' = B'_0 \uplus B_{\Omega^+}$, with B_{Ω^+} $A \vee C \vee U$ Ω^+-axioms, and $B_0 \cup B'_0$ $A \vee C$ $(\Sigma \setminus \Omega^+)$-axioms.

Semantic Equivalence of Equational Programs (II)

Two admissible and comparable programs `fmod` $(\Sigma, E \cup B)$ `endfm` and `fmod` $(\Sigma, E' \cup B')$ `endfm` are called semantically equivalent, denoted `fmod` $(\Sigma, E \cup B)$ `endfm` $\equiv_{sem}$ `fmod` $(\Sigma, E' \cup B')$ `endfm` iff $\mathbb{C}_{\Sigma/\vec{E},B} = \mathbb{C}_{\Sigma/\vec{E}',B'}$.

Since the axioms in $B_0 \cup B_0'$ are $A \vee C$ $(\Sigma \setminus \Omega^+)$-axioms, for any $u, v \in T_{\Omega^+}$, $u =_B v$ (resp. $u =_{B'} v$) forces $u =_{B_{\Omega^+}} v$. Therefore, the unique Σ-homomorphisms $[\_!_{\vec{E}/B}]_B : \mathbb{T}_\Sigma \to \mathbb{C}_{\Sigma/\vec{E},B}$ and $[\_!_{\vec{E}'/B'}]_{B'} : \mathbb{T}_\Sigma \to \mathbb{C}_{\Sigma/\vec{E}',B'}$ can be described more precisely as $[\_!_{\vec{E}/B}]_{B_{\Omega^+}} : \mathbb{T}_\Sigma \to \mathbb{C}_{\Sigma/\vec{E},B}$ and $[\_!_{\vec{E}'/B'}]_{B_{\Omega^+}} : \mathbb{T}_\Sigma \to \mathbb{C}_{\Sigma/\vec{E}',B'}$.

Ex.14.3. Prove that for admissible and comparable `fmod` $(\Sigma, E \cup B)$ `endfm` and `fmod` $(\Sigma, E' \cup B')$ `endfm`, `fmod` $(\Sigma, E \cup B)$ `endfm` $\equiv_{sem}$ `fmod` $(\Sigma, E' \cup B')$ `endfm` iff $\forall t \in T_\Sigma$, $t!_{\vec{E}/B} =_{B_{\Omega^+}} t!_{\vec{E}'/B'}$. I.e., if Maude's `red` command gives the same result for both modulo B_{Ω^+}.

Semantic Equivalence of Equational Programs (III)

Note that $\mathbb{C}_{\Sigma/\vec{E},B} = \mathbb{C}_{\Sigma/\vec{E'},B'}$ and the Lemma in pg. 2 force $\mathbb{T}_{\Sigma/E\cup B} = \mathbb{T}_{\Sigma/E'\cup B'}$. Therefore, by **Ex**.14.2, `fmod` $(\Sigma, E \cup B)$ `endfm` $\equiv_{sem}$ `fmod` $(\Sigma, E' \cup B')$ `endfm` implies $(\Sigma, E \cup B) \equiv_{ind} (\Sigma, E' \cup B')$. But the converse implication does not hold in general.

For example, for $\Sigma = \{a, b, c\}$, $E = \{a = b\}$, and $E' = \{b = a\}$, of course $(\Sigma, E) \equiv (\Sigma, E')$ and therefore $(\Sigma, E) \equiv_{ind} (\Sigma, E')$; but although $\vec{E}$ and $\vec{E'}$ are both convergent, they have different constructors $\Omega = \{b, c\}$ and $\Omega' = \{a, c\}$, so that $\mathbb{C}_{\Sigma/\vec{E}} \neq \mathbb{C}_{\Sigma/\vec{E'}}$. Therefore, `fmod` $(\Sigma, E \cup B)$ `endfm` $\not\equiv_{sem}$ `fmod` $(\Sigma, E' \cup B')$ `endfm`.

Theorem (Program Equivalence Theorem) For admissible and comparable `fmod` $(\Sigma, E \cup B)$ `endfm` and `fmod` $(\Sigma, E' \cup B')$ `endfm`, `fmod` $(\Sigma, E \cup B)$ `endfm` $\equiv_{sem}$ `fmod` $(\Sigma, E' \cup B')$ `endfm` iff $(\Sigma, E \cup B) \models_{ind} (E'_0 \setminus E_0) \cup (B' \setminus B)$.

Semantic Equivalence of Equational Programs (IV)

Proof: To see ($\Rightarrow$), note that sematic equivalence forces $\mathbb{T}_{\Sigma/E \cup B} = \mathbb{T}_{\Sigma/E' \cup B'}$, which forces $(\Sigma, E \cup B) \models_{ind} (E'_0 \setminus E_0) \cup (B' \setminus B)$.

To prove the ($\Leftarrow$) implication, by **Ex**.14.3. we just need to show that $\forall t \in T_\Sigma$, $t!_{\vec{E}/B} =_{B_{\Omega+}} t!_{\vec{E'}/B'}$. But note that $(\Sigma, E \cup B) \models_{ind} (E'_0 \setminus E_0) \cup (B' \setminus B)$ forces $(\Sigma, E \cup B) \models_{ind} E' \cup B'$, and by **Ex**.14.2.$(i)$ this then forces $t!_{\vec{E}/B} =_{E \cup B} t!_{\vec{E'}/B'}$, which by the Church-Rosser property then forces $t!_{\vec{E}/B} =_{B_{\Omega+}} (t!_{\vec{E'}/B'})!_{\vec{E}/B}$. But note that, by sufficient completeness, $t!_{\vec{E'}/B'}$ is an Ω-term, and since $\vec{E} = \vec{E}_0 \uplus \vec{E}_{\Omega+}$, this means that no rule in $\vec{E}_0$ can apply to $t!_{\vec{E'}/B'}$, and since $\vec{E}_{\Omega+} \subseteq \vec{E'}$, no rule in $\vec{E}_{\Omega+}$ can apply to $t!_{\vec{E'}/B'}$ either. This forces $(t!_{\vec{E'}/B'})!_{\vec{E}/B} = t!_{\vec{E'}/B'}$, yielding $t!_{\vec{E}/B} =_{B_{\Omega+}} t!_{\vec{E'}/B'}$, as desired. q.e.d.

Internalizing Lemmas in Equational Programs

Theorem (Lemma Internalization Theorem 2) Let `fmod` $(\Sigma, E \cup B)$ **`endfm`** be an admissible program with constructors Ω satisfying the extra requirements on E and B allowing it to be comparable to other programs, and let G be a finite set of Σ-equations such that $(\Sigma, E \cup B) \models_{ind} G$. If the equations G can be oriented (left-to right or right to left) as sort-decreasing rules $\vec{G'}$ of the form $f(u_1, \ldots, u_n) \to w$ with f in $\Sigma \setminus \Omega^+$ and so that rules $\vec{E} \cup \vec{G'}$ are terminating modulo B, then `fmod` $(\Sigma, E \cup G' \cup B)$ `endfm` (with G and G' differing only in orientation) is admissible and `fmod` $(\Sigma, E \cup B)$ `endfm` $\equiv_{sem}$ `fmod` $(\Sigma, E \cup G' \cup B)$ `endfm`.

Proof: We will be done if we prove that $(\Sigma, E \cup G' \cup B)$ is locally ground confluent modulo B, since this makes `fmod` $(\Sigma, E \cup G' \cup B)$ `endfm` admissible and comparable with `fmod` $(\Sigma, E \cup B)$ `endfm` and, thanks to the Program Equivalence Theorem, yields

$\texttt{fmod}\ (\Sigma, E \cup B)\ \texttt{endfm} \equiv_{sem} \texttt{fmod}\ (\Sigma, E \cup G' \cup B)\ \texttt{endfm}$.

Let $t, u, v \in T_\Sigma$ be such that $u\ {}_{\vec{E}\cup\vec{G'}/B}\!\leftarrow t \rightarrow_{\vec{E}\cup\vec{G'}/B} v$. We need to show that $u \downarrow_{\vec{E}\cup\vec{G'}/B} v$. This will hold if we prove $u \downarrow_{\vec{E}/B} v$. But since $(\Sigma, E \cup B) \models_{ind} G$, **Ex**.14.2.$(i)$ forces $u =_{E\cup B} v$, which, since $\vec{E}$ is gound convergent modulo B, forces $u \downarrow_{\vec{E}/B} v$, as desired. q.e.d.

Theorem (Lemma Internalization Theorem 3) Let $\texttt{fmod}$ $(\Sigma, E \cup B)$ $\texttt{endfm}$ be an admissible program with constructors Ω satisfying the extra requirements on E and B to be comparable to other programs, and let G be a finite set of $A \vee C$ axioms for binary operators $\Sigma_0 \subseteq \Sigma \setminus \Omega^+$ general enough to declare G axioms for all operators subsort-overloaded to those in Σ_0, and making Σ $(B \cup G)$-preregular. If $(\Sigma, E \cup B) \models_{ind} G$ and the rules $\vec{E}$ are terminating modulo $B \cup G$, then $\texttt{fmod}\ (\Sigma, E \cup B \cup G)\ \texttt{endfm}$ is admissible and comparable to $\texttt{fmod}\ (\Sigma, E \cup B)\ \texttt{endfm}$, and $\texttt{fmod}\ (\Sigma, E \cup B)\ \texttt{endfm} \equiv_{sem} \texttt{fmod}\ (\Sigma, E \cup B \cup G)\ \texttt{endfm}$.

Internalizing Lemmas in Equational Programs (II)

Proof: Reasoning as in the proof of the Lemma Internalization Theorem 2, we will be done if we prove that the rules $\vec{E}$ are locally ground confluent modulo $B \cup G$. Let $t, u, v \in T_\Sigma$ be such that $u \; {}_{\vec{E}/B\cup G}\!\leftarrow t \rightarrow_{\vec{E}/B\cup G} v$. We need to show that $u \downarrow_{\vec{E}/B\cup G} v$. This will hold if we prove $u \downarrow_{\vec{E}/B} v$. But since $(\Sigma, E \cup B) \models_{ind} G$, **Ex**.14.2.$(i)$ forces $u =_{E\cup B} v$, which, since $\vec{E}$ is ground confluent modulo B, forces $u \downarrow_{\vec{E}/B} v$, as desired. q.e.d.

Exercises

Ex.14.4. Prove in detail the theorem characterizing the inductive theorems of a theory (Σ, E) stated in pg. 6 of this lecture.

Ex.14.5. Consider the equational theory (Σ, E) defined by the functional module:

```
fmod PEANO-p is
sorts NzNat Nat .   subsorts NzNat < Nat .
op 0 : -> Nat [ctor] .
op s : Nat -> NzNat [ctor] .
op p : NzNat -> Nat .
eq p(s(N:Nat)) = N:Nat .
endfm
```

which defines the predecessor function `p`. Do the following:

1. Prove that $(\Sigma, \vec{E})$ is sort-decreasing, confluent, terminating, and sufficiently complete w.r.t. $\Omega = \{0, s\}$ by either using tools in Maude's Formal Environment, or giving a hand proof.

2. Prove that $E \not\vdash s(p(y : NzNat)) = y : NzNat$.

3. Prove that $(\Sigma, E) \models_{ind} s(p(y : NzNat)) = y : NzNat$ by applying Part (2) of the theorem characterizing the inductive theorems of a theory (Σ, E) stated in pg. 6 of this lecture.