Formal Techniques for Software Engineering: Equivalence Axiomatizations

Rocco De Nicola

IMT Institute for Advanced Studies, Lucca
rocco.denicola@imtlucca.it

June 2013

Lesson 11

Equivalence Checking

Checking whether the process graphs of two basic process terms are equivalent is hard:

Equivalence Checking

- LTS have have to be computed
- Their equivalence has to be proved

Equational Characterization

- Equational axiomatisation permit avoiding the computation of process graphs and bisimulation relations altogether and can be used in automated reasoning
- Axioms permit a deeper understanding of the impact and the "meaning" of equivalences.

Properties of an Axiomatization

Soundness and Completeness

We are after an equational theory $E_{CCS} \vdash P = Q$ of CCS terms that

- is sound for strong bisimilarity:
  if $E_{CCS} \vdash P \ = \ Q$ holds for CCS processes P and Q, then $P \sim Q$;
- is complete for strong bisimilarity:
  if $P \sim Q$ holds for CCS processes P and Q, then $E_{CCS} \vdash P \ = \ Q$;

We have that:

- Soundness ensures that if terms are proved equal by the axioms, then they are in the same bisimulation equivalence class,
- Completeness ensures that bisimilar terms can always be equated by taking advantage of the equational reasoning.

We are after a similar result for weak bisimilarity ($\approx$).

Signatures and Terms

Signatures

- A signature Σ consists of a finite set of function symbols (or operators) $F, \; G, \; \dots$, where each function symbol F has arity $ar(F)$, the number of arguments.
- A function symbol $a, \; b, \; c, \; \dots$ of arity 0 is called a constant.

Terms over a signature Σ

- Assume the presence of a countably infinite set of variables $X, \; Y, \; Z \; \dots$ disjoint from the signature. The set of open terms s, t, u, ... over Σ is denoted by $T(\Sigma)$ and is the least set satisfying:
  1. each variable is in $T(\Sigma)$;
  2. if $F \in \Sigma$ and $t_1, ..., t_{ar(F)} \in T(\Sigma)$, then $F(t_1, ..., t_{ar(F)}) \in T(\Sigma)$
- A term is closed if it does not contain variables. The set of closed terms is denoted by $CT(\Sigma)$.

Signatures and Terms

Signatures

- A signature Σ consists of a finite set of function symbols (or operators) $F,\ G,\ \ldots$, where each function symbol F has arity $ar(F)$, the number of arguments.
- A function symbol $a,\ b,\ c,\ \ldots$ of arity 0 is called a constant.

Terms over a signature Σ

- Assume the presence of a countably infinite set of variables $X,\ Y,\ Z\ \ldots$ disjoint from the signature. The set of open terms s, t, u, ... over Σ is denoted by $T(\Sigma)$ and is the least set satisfying:
  1. each variable is in $T(\Sigma)$;
  2. if $F \in \Sigma$ and $t_1, \ldots, t_{ar(F)} \in T(\Sigma)$, then $F(t_1, \ldots, t_{ar(F)}) \in T(\Sigma)$
- A term is closed if it does not contain variables. The set of closed terms is denoted by $CT(\Sigma)$.

Substitutions and Axioms

Substitution over a signature Σ

- A substitution is a mapping $\sigma : Var \rightarrow T(\Sigma)$ from variables to open terms.
- A substitution σ is closed if $\sigma(X) \in CT(\Sigma)$ for all variables X.
- The application of a substitution σ to a term t is written $\sigma(t)$ and denotes the term obtained by the concurrent replacement of all variables X in t by $\sigma(X)$.

Axioms over Σ

- An axiom is an (universally quantified) equality assertion of the form $s = t$, with $s, t \in T(\Sigma)$.
- An axiomatisation E is a finite set of axioms.

Substitutions and Axioms

Substitution over a signature Σ

- A substitution is a mapping $\sigma : Var \to T(\Sigma)$ from variables to open terms.
- A substitution σ is closed if $\sigma(X) \in CT(\Sigma)$ for all variables X.
- The application of a substitution σ to a term t is written $\sigma(t)$ and denotes the term obtained by the concurrent replacement of all variables X in t by $\sigma(X)$.

Axioms over Σ

- An axiom is an (universally quantified) equality assertion of the form $s = t$, with $s, t \in T(\Sigma)$.
- An axiomatisation E is a finite set of axioms.

Equational Logic

Axiomatisations

An axiomatisation E induces a (least) equality relation $=_E$ on $T(\Sigma)$ s.t.:

- Relation $=_E$ contains all equalities in E.
- $=_E$ is closed under reflexivity, symmetry, and transitivity.
- $=_E$ is closed under contexts and substitutions.

Inference Rules

(Axioms) $$\frac{(s = t) \in E}{\sigma(s) =_E \sigma(t)}$$

(Reflexivity) $$\frac{}{t =_E t}$$

(Transitivity) $$\frac{t_1 =_E t_2 \quad t_2 =_E t_3}{t_1 =_E t_3}$$

(Symmetry) $$\frac{t_1 =_E t_2}{t_2 =_E t_1}$$

(Substitutivity) $$\frac{t_1 =_E t_1' \quad \cdots \quad t_k =_E t_k'}{F(t_1, \ldots, t_k) =_E F(t_1', \ldots, t_k')} \quad ar(F) = k$$

Axioms for Basic CCS (nil, prefix, sum)

$Base_{AX}$

$$
\begin{array}{lrcl}
\text{(A1)} & X + Y & = & Y + X \\
\text{(A2)} & X + (Y + Z) & = & (X + Y) + Z \\
\text{(A3)} & X + nil & = & X \\
\text{(A4)} & X + X & = & X
\end{array}
$$

- We shall write $=$ instead of $=_{Base_{AX}}$
- The variables X, Y, and Z in the axioms range over the collection of CCS terms.
- The equality relation on basic process terms induced by the set $Base_{AX}$ is obtained by taking the set of closed substitution instances of axioms in $Base_{AX}$ and closing it under equivalence and contexts.

Equational Reasoning

An Equational Proof

$$\begin{aligned} a.(b.nil + nil) + (a.nil + a.b.nil) &= a.b.nil + (a.nil + a.b.nil) && \text{(A3)} \\ &= a.b.nil + (a.b.nil + a.nil) && \text{(A1)} \\ &= (a.b.nil + a.b.nil) + a.nil && \text{(A2)} \\ &= a.b.nil + a.nil && \text{(A4)} \end{aligned}$$

This proof establishes that:

$$a.(b.nil + nil) + (a.nil + a.b.nil) = a.b.nil + a.nil$$

in four steps where each step represents an "application" of an axiom to a subterm to produce a new term using the inference rules seen before.
Thus we can write:

$$Base_{AX} \vdash a.(b.nil + nil) + (a.nil + a.b.nil) = a.b.nil + a.nil$$

Axioms for Static Operators

Restriction - Res_{AX}

$$
\begin{array}{lrcl}
\text{(Res1)} & nil\backslash L & = & nil \\
\text{(Res2)} & (\alpha.p)\backslash L & = & \begin{cases} nil & \text{if } \alpha, \overline{\alpha} \in L \\ \alpha.(p\backslash L) & \text{otherwise} \end{cases} \\
\text{(Res3)} & (p+q)\backslash L & = & p\backslash L + q\backslash L
\end{array}
$$

Relabelling - Rel_{AX}

$$
\begin{array}{lrcl}
\text{(Rel1)} & nil[f] & = & nil \\
\text{(Rel2)} & (\alpha.p)[f] & = & f(\alpha).(p[f]) \\
\text{(Rel3)} & (p+q)[f] & = & p[f] + q[f]
\end{array}
$$

Axioms for Parallel Composition

Expansion Theorem: - Exp_{AX}

$$(Exp)\left(\sum_{i\in I}\mu_i.p_i\right)\big|\left(\sum_{j\in J}\mu'_j.q_j\right) \;=\; \sum_{i\in I}\mu_i.\left(p_i \mid \sum_{j\in J}\mu'_j.q_j\right) + \sum_{j\in J}\mu'_j.\left(\left(\sum_{i\in I}\mu_i.p_i\right) \mid q_j\right) + \sum_{\{(i,j)\,\mid\,\overline{\mu}_i=\mu'_j\}}\tau.(p_i \mid q_j)$$

Example

$$p \triangleq \alpha.\,p' + \beta.\,p'' \qquad q \stackrel{def}{=} \overline{\alpha}.\,q' + \gamma.\,q'' \qquad r \stackrel{def}{=} (p \mid q)\backslash\alpha$$

$$Base_{AX} \cup Res_{AX} \cup Exp_{AX} \vdash r = \beta.\,(p'' \mid q)\,\backslash\alpha + \gamma.\,(p \mid q'')\,\backslash\alpha + \tau.\,(p' \mid q')\,\backslash\alpha$$

If processes p', p'', q', q'' are known, we can continue till we get a term with only prefixes and sums.

Soundness and Completeness (for finite CCS)

Soundness of the Axiomatisation

$$Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \vdash p = q \qquad \textit{implies} \qquad p \sim q$$

Proof.

We need to prove:

1. Soundness of the axioms, i.e. we need to prove that A1-A4, Res1-Res3, Rel1-Rel3 and Exp are sound (= can be replaced by $\sim$)
2. Inference rules are sound; this amounts to saying that
   - $\sim$ is an equivalence relation
   - $\sim$ is a congruence for all CCS operators

□

Soundness and Completeness (for finite CCS)

Completeness of the Axiomatization

$p \sim q$ *implies* $Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \vdash p = q.$

Standard form

A process $p \in \mathcal{P}_{CCS}$ is in standard form (s.f.) if p has the form

$$\sum_{i=1}^{m} \mu_i . p_i$$

where each p_i is itself in standard form.

Lemma

Given any finite CCS process p there exists a process p' in s.f. such that

$$Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \vdash p = p'$$

Completeness Proof

Theorem

$p \sim q$ implies $Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \vdash p = q$.

Proof

We can assume that $p \sim q$ and that p e q are in s.f.:

$$p \equiv \sum_{i=1}^{m} \mu_i.p_i \qquad \text{and} \qquad q \equiv \sum_{j=1}^{n} \mu_j.q_j$$

and proceed by induction on the max depth (k) of p and q.

- $k = 0$, then both p and q are *nil* and by (Reflexivity) $nil = nil$.
- If $k > 0$, then at least one of p and q is different from *nil*. Assume that $p \neq nil$ and that $\mu.p'$ is a summand of p, then we have $p \xrightarrow{\mu} p'$ and since $p \sim q$, we have $\exists q' : q \xrightarrow{\mu} q'$ with $p' \sim q'$. Being q in s.f. we have that $\mu.q'$ is a summand of q. Now, p' e q' are in s.f. and their max depth is less than k, thus by induction we know that $p' = q'$. Thus, each summand of p is a summand of q; similarly we can prove the converse. The thesis follows then by relying on (A4) to eliminate duplicated summands.

Completeness Proof

Theorem

$p \sim q$ implies $Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \vdash p = q$.

Proof

We can assume that $p \sim q$ and that p e q are in s.f.:

$$p \equiv \sum_{i=1}^{m} \mu_i.p_i \qquad \text{and} \qquad q \equiv \sum_{j=1}^{n} \mu_j.q_j$$

and proceed by induction on the max depth (k) of p and q.

- $k = 0$, then both p and q are *nil* and by (Reflexivity) $nil = nil$.
- If $k > 0$, then at least one of p and q is different from *nil*. Assume that $p \neq nil$ and that $\mu.p'$ is a summand of p, then we have $p \xrightarrow{\mu} p'$ and since $p \sim q$, we have $\exists q' : q \xrightarrow{\mu} q'$ with $p' \sim q'$. Being q in s.f. we have that $\mu.q'$ is a summand of q. Now, p' e q' are in s.f. and their max depth is less than k, thus by induction we know that $p' = q'$. Thus, each summand of p is a summand of q; similarly we can prove the converse. The thesis follows then by relying on (A4) to eliminate duplicated summands.

Dealing with Weak Bisimilarity

Weak bisimilarity is not a congruence!

Equational reasoning is closed under contexts and substitutions, but $\approx$ is not! Indeed, $\approx$ is not a congruence for summation.

Main idea

We can still take the largest congruence $\approx^c$ contained in $\approx$:

- $\approx^c$ must be a congruence
- $\approx^c$ must be a weak bisimulation (i.e., $\approx^c \subseteq \approx$)
- Any other congruence $\mathcal{R}$ that enjoys the same properties must be included in $\approx^c$.

Notice that the identity relation (Id) and strong bisimilarity ($\sim$) are congruences and they are included in $\approx$, but they are too strong to satisfy our needs.

Dealing with Weak Bisimilarity

Weak bisimilarity is not a congruence!

Equational reasoning is closed under contexts and substitutions, but $\approx$ is not! Indeed, $\approx$ is not a congruence for summation.

Main idea

We can still take the largest congruence $\approx^c$ contained in $\approx$:

- $\approx^c$ must be a congruence
- $\approx^c$ must be a weak bisimulation (i.e., $\approx^c \subseteq \approx$)
- Any other congruence $\mathcal{R}$ that enjoys the same properties must be included in $\approx^c$.

Notice that the identity relation (Id) and strong bisimilarity ($\sim$) are congruences and they are included in $\approx$, but they are too strong to satisfy our needs.

(Weak) Observational Congruence

Observational Congruence

Two CCS processes p and q are observationally congruent, written $p \cong q$ if for any $\mu \in Act$:

- if $p \xrightarrow{\mu} p'$ then $q \stackrel{\mu}{\Longrightarrow} q'$ for some q' such that $p' \approx q'$;
- if $q \xrightarrow{\mu} q'$ then $p \stackrel{\mu}{\Longrightarrow} p'$ for some p' such that $p' \approx q'$.

Notice that:

- $\cong$ is not defined recursively
- $\stackrel{\mu}{\Longrightarrow}$ is used instead of $\stackrel{\hat{\mu}}{\Longrightarrow}$ (for the first bisimulation step)
- $\sim \subseteq \cong \subseteq \approx$
- $\cong$ is an equivalence (because $\approx$ is)
- It can be proved that $\cong$ is preserved by all contexts

Hennessy' Lemma: $p \approx q$ iff $p \cong q$ or $\tau.p \cong q$ or $p \cong \tau.q$

(Weak) Observational Congruence

Observational Congruence

Two CCS processes p and q are observationally congruent, written $p \cong q$ if for any $\mu \in Act$:

- if $p \xrightarrow{\mu} p'$ then $q \stackrel{\mu}{\Longrightarrow} q'$ for some q' such that $p' \approx q'$;
- if $q \xrightarrow{\mu} q'$ then $p \stackrel{\mu}{\Longrightarrow} p'$ for some p' such that $p' \approx q'$.

Notice that:

- $\cong$ is not defined recursively
- $\stackrel{\mu}{\Longrightarrow}$ is used instead of $\stackrel{\hat{\mu}}{\Longrightarrow}$ (for the first bisimulation step)
- $\sim \subseteq \cong \subseteq \approx$
- $\cong$ is an equivalence (because $\approx$ is)
- It can be proved that $\cong$ is preserved by all contexts

Hennessy' Lemma: $p \approx q$ iff $p \cong q$ or $\tau.p \cong q$ or $p \cong \tau.q$

(Weak) Observational Congruence

Observational Congruence

Two CCS processes p and q are observationally congruent, written $p \cong q$ if for any $\mu \in Act$:

- if $p \xrightarrow{\mu} p'$ then $q \stackrel{\mu}{\Longrightarrow} q'$ for some q' such that $p' \approx q'$;
- if $q \xrightarrow{\mu} q'$ then $p \stackrel{\mu}{\Longrightarrow} p'$ for some p' such that $p' \approx q'$.

Notice that:

- $\cong$ is not defined recursively
- $\stackrel{\mu}{\Longrightarrow}$ is used instead of $\stackrel{\hat{\mu}}{\Longrightarrow}$ (for the first bisimulation step)
- $\sim \subseteq \cong \subseteq \approx$
- $\cong$ is an equivalence (because $\approx$ is)
- It can be proved that $\cong$ is preserved by all contexts

Hennessy' Lemma: $p \approx q$ iff $p \cong q$ or $\tau.p \cong q$ or $p \cong \tau.q$

(Weak) Observational Congruence

Observational Congruence

Two CCS processes p and q are observationally congruent, written $p \cong q$ if for any $\mu \in Act$:

- if $p \xrightarrow{\mu} p'$ then $q \stackrel{\mu}{\Longrightarrow} q'$ for some q' such that $p' \approx q'$;
- if $q \xrightarrow{\mu} q'$ then $p \stackrel{\mu}{\Longrightarrow} p'$ for some p' such that $p' \approx q'$.

Notice that:

- $\cong$ is not defined recursively
- $\stackrel{\mu}{\Longrightarrow}$ is used instead of $\stackrel{\hat{\mu}}{\Longrightarrow}$ (for the first bisimulation step)
- $\sim \subseteq \cong \subseteq \approx$
- $\cong$ is an equivalence (because $\approx$ is)
- It can be proved that $\cong$ is preserved by all contexts

Hennessy' Lemma: $p \approx q$ iff $p \cong q$ or $\tau.p \cong q$ or $p \cong \tau.q$

(Weak) Observational Congruence

Observational Congruence

Two CCS processes p and q are observationally congruent, written $p \cong q$ if for any $\mu \in Act$:

- if $p \xrightarrow{\mu} p'$ then $q \overset{\mu}{\Longrightarrow} q'$ for some q' such that $p' \approx q'$;
- if $q \xrightarrow{\mu} q'$ then $p \overset{\mu}{\Longrightarrow} p'$ for some p' such that $p' \approx q'$.

Notice that:

- $\cong$ is not defined recursively
- $\overset{\mu}{\Longrightarrow}$ is used instead of $\overset{\hat{\mu}}{\Longrightarrow}$ (for the first bisimulation step)
- $\sim \subseteq \cong \subseteq \approx$
- $\cong$ is an equivalence (because $\approx$ is)
- It can be proved that $\cong$ is preserved by all contexts

Hennessy' Lemma: $p \approx q$ iff $p \cong q$ or $\tau.p \cong q$ or $p \cong \tau.q$

(Weak) Observational Congruence

Observational Congruence

Two CCS processes p and q are observationally congruent, written $p \cong q$ if for any $\mu \in Act$:

- if $p \xrightarrow{\mu} p'$ then $q \stackrel{\mu}{\Longrightarrow} q'$ for some q' such that $p' \approx q'$;
- if $q \xrightarrow{\mu} q'$ then $p \stackrel{\mu}{\Longrightarrow} p'$ for some p' such that $p' \approx q'$.

Notice that:

- $\cong$ is not defined recursively
- $\stackrel{\mu}{\Longrightarrow}$ is used instead of $\stackrel{\hat{\mu}}{\Longrightarrow}$ (for the first bisimulation step)
- $\sim \subseteq \cong \subseteq \approx$
- $\cong$ is an equivalence (because $\approx$ is)
- It can be proved that $\cong$ is preserved by all contexts

Hennessy' Lemma: $p \approx q$ iff $p \cong q$ or $\tau.p \cong q$ or $p \cong \tau.q$

(Weak) Observational Congruence

Observational Congruence

Two CCS processes p and q are observationally congruent, written $p \cong q$ if for any $\mu \in Act$:

- if $p \xrightarrow{\mu} p'$ then $q \stackrel{\mu}{\Longrightarrow} q'$ for some q' such that $p' \approx q'$;
- if $q \xrightarrow{\mu} q'$ then $p \stackrel{\mu}{\Longrightarrow} p'$ for some p' such that $p' \approx q'$.

Notice that:

- $\cong$ is not defined recursively
- $\stackrel{\mu}{\Longrightarrow}$ is used instead of $\stackrel{\hat{\mu}}{\Longrightarrow}$ (for the first bisimulation step)
- $\sim \subseteq \cong \subseteq \approx$
- $\cong$ is an equivalence (because $\approx$ is)
- It can be proved that $\cong$ is preserved by all contexts

Hennessy' Lemma: $p \approx q$ iff $p \cong q$ or $\tau.p \cong q$ or $p \cong \tau.q$

Axioms for Weak Bisimilarity

All the axioms for $\sim$ continue to hold for $\cong$

τ-Laws

$$
\begin{array}{lrcl}
(\tau 1) & \mu.\tau.p & = & \mu.p \\
(\tau 2) & p + \tau.p & = & \tau.p \\
(\tau 3) & \mu.(p + \tau.q) & = & \mu.(p + \tau.q) + \mu.q
\end{array}
$$

- $\tau 1$ can absorb τ actions that immediately follow a prefix
- $\tau 2$ can eliminate redundant alternatives
- $\tau 3$ can be used to saturate the normal form

Soundness and Completeness

Full standard form

A process $p \in \mathcal{P}_{CCS}$ is in full standard form (f.s.f.) if p has the form

$$\sum_{i=1}^{m} \mu_i . p_i$$

where each p_i is itself in full standard form and if

$$p \stackrel{\mu}{\Longrightarrow} p' \quad \text{implies} \quad p \stackrel{\mu}{\longrightarrow} p'$$

Lemma

Given any finite CCS process p there exists a process p′ in f.s.f. such that $Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \cup \tau - Laws \vdash p = p'$

Soundness and Completeness of the Axiomatization

$Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \cup \tau - Laws \vdash p = q \qquad iff \qquad p \cong q$

Soundness and Completeness (for finite CCS)

Full standard form

A process $p \in \mathcal{P}_{CCS}$ is in full standard form (f.s.f.) if p has the form

$$\sum_{i=1}^{m} \mu_i . p_i$$

where each p_i is itself in full standard form and if

$$p \stackrel{\mu}{\Longrightarrow} p' \quad \text{implies} \quad p \stackrel{\mu}{\longrightarrow} p'$$

Lemma

Given any finite CCS process p there exists a process p′ in f.s.f. such that $Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \cup \tau - Laws \vdash p = p'$

Completeness of the Axiomatization

$p \cong q \quad \textit{implies} \quad Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \cup \tau - Laws \vdash p = q.$

Saturation Lemma

Let $EQ_\tau \;=\; Base_{AX} \cup Res_{AX} \cup Rel_{AX} \cup Exp_{AX} \cup \tau - Laws$, then
if p is in standard form and $p \stackrel{\mu}{\Rightarrow} p'$, we have $EQ \vdash p = p + \mu.p'$.

Proof:

The proof goes by induction on $depth(p)$.

Since p is in s.f., if $p \stackrel{\mu}{\Rightarrow} p'$, it might be due to:

1. $\mu.p'$ is a sumand of p. The claim follows from (A4).
2. $\mu.q$ is a summand of p and
   $q \stackrel{\tau}{\Rightarrow} p'$. By induction we have that $EQ_\tau \vdash q = q + \tau.p'$, hence

$$
\begin{array}{rcll}
EQ_\tau \vdash p & = & p + \mu.q & (A4) \\
 & = & p + \mu.(q + \tau.p') & EQ_\tau \vdash q = q + \tau.p' \\
 & = & p + \mu.(q + \tau.p') + \mu.p' & (\tau 3) \\
 & = & p + \mu.q + \mu.p' & EQ_\tau \vdash q = q + \tau.p' \\
 & = & p + \mu.p' & (A4)
\end{array}
$$

%

Saturation Lemma

Proof continued:

3. $\tau.q$ is a summand of p and $q \stackrel{\mu}{\Rightarrow} p'$. By induction we have that $EQ_\tau \vdash q = q + \mu.p'$,

$$
\begin{array}{rcll}
E_4 \vdash p & = & p + \tau.q & (A4) \\
 & = & p + \tau.q + q & (\tau 2) \\
 & = & p + \tau.q + q + \mu.p' & EQ_\tau \vdash q = q + \mu.p' \\
 & = & p + \tau.q + \mu.p' & (\tau 2) \\
 & = & p + \mu.p' & (A4)
\end{array}
$$

□

Reduction to full standard form

For each p in s.f. there exists p' in f.s.f. of equal depth s.t. $EQ_\tau \vdash p = p'$.

Proof.

By induction on $depth(p)$. If $depth(p) = 0$ then $p \equiv nil$ and p is already in f.s.f.. Otherwise, for each summand $\mu.q$ of p, we can assume that q has been reduced, by means of EQ_τ, to a f.s.f., without increasing its depth. Let us now consider all pairs

$$(\mu_i, p_i),\ 1 \leq i \leq k,\ \text{s.t. } p \stackrel{\mu_i}{\Longrightarrow} p_i \text{ and } p \stackrel{\mu_i}{\not\longrightarrow} p_i$$

Each p_i has to be in f.s.f. because it is a subterm $\mu.q$ of p. By exploiting the saturation lemma, we have have:

$$EQ_\tau \vdash p = p + \mu_1.p_1 + \cdots + \mu_k.p_k$$

and the r.h.s. of the equality is a f.s.f. that has the same depth of p. □

Completeness Theorem

$p \cong q$ implica $E_\tau \vdash p = q$.

Proof.

The proof goes by induction on $depth(p) + depth(q)$.
We can assume that p and q are in f.s.f. and distinguish the two cases

- $depth(p) + depth(q) = 0$
- $depth(p) + depth(q) \neq 0$

In the former case we have $p \equiv nil \equiv q$ and the claim follows trivially. Otherwise, w.l.o.g., assume $p \neq nil$ and that $p \cong q$ and $\mu.p'$ is a summand of p. We have to show that q has a summand provably equal to $\mu.p'$. Since $p \xrightarrow{\mu} p'$ and $p \cong q$, we have that there exists q' s.t. $q \stackrel{\mu}{\Rightarrow} q'$ e $p' \approx q'$, moreover since q is in f.s.f. we have $q \xrightarrow{\mu} q'$, and $\mu.q'$ is a summand of q. Unfortunately, we cannot use induction because we only have $p' \approx q'$, and not $p' \cong q'$.

Reduction to full standard form

Proof continued

But we can exploit the fact that

$$p' \approx q' \text{ iff } 1.\ p' = q' \text{ or } 2.\ p' = \tau.q' \text{ or } 3.\ \tau.p' = q'.$$

Case 1.: Since p' e q' are in f.s.f. and their depth is smaller than that of p and q respectively, by induction it follws that $EQ_\tau \vdash p' = q'$, hence that $EQ_\tau \vdash \mu.p' = \mu.q'$.

Case 2.: We need to reduce $\tau.q'$ to a f.s.f. to apply induction. We have that there exists q'' in f.s.f. with the same depth as $\tau.q'$, hence as q, s.t. $EQ_\tau \vdash \tau.q' = q''$. Since $depth(p') + depth(q'') \leq depth(p) + depth(q)$ by induction we have $EQ_\tau \vdash p' = q''$ and thus $EQ_\tau \vdash p' = \tau.q'$ and by $(\tau 1)$ it follows $EEQ_\tau \vdash \mu.p' = \mu.q'$.

Case 3.: Is similar to Case 2..
We have thus shown that via EQ_τ each summand $\mu.p'$ di p can be reduced to a summand of q. Similarly, each summand $\mu'.q'$ ofi q an be reduced to a summand of p. Since we can use (A4) to get rid of duplicated summands we can , we can conclude that $EQ_\tau \vdash p = q$. □