Orthogonal Extensions in SOS

MohammadReza Mousavi and Michel Reniers

Department of Computer Science,
Eindhoven University of Technology

ICALP, July 2005,
Lisbon, Portugal

Overview

→ Motivating Example

1. Definitions
2. Meta-Theorems
3. Conclusions

Minimal Process Algebra (MPA)

- δ : deadlock,
- $a.\_$: (a class of) action prefix,
- $\_ + \_$: choice

Minimal Process Algebra (MPA)

$\delta\ ,\ a.\_\ ,\ \_ + \_$

$MPA:$

$$x + y = y + x$$

$$x + (y + z) = (x + y) + z$$

$$x + x = x$$

$$x + \delta = x$$

Minimal Process Algebra (MPA)

$\delta\ ,\ a.\_\ ,\ \_ + \_$

$MPA:$

$$x + y = y + x \quad x + (y + z) = (x + y) + z$$

$$x + x = x \quad x + \delta = x$$

$MPA \vdash (\delta + a.\delta) = a.\delta \qquad MPA \vdash a.(a.\delta + a.\delta) = a.a.\delta$

MPA: Operational Model

$\delta\ ,\ a.\_\ ,\ \_+\_$

$TSS(MPA):$

(a) $\dfrac{}{a.x \xrightarrow{a} x}\ (a \in A)$

(co) $\dfrac{x \xrightarrow{a} x'}{x+y \xrightarrow{a} x'}$ **(c1)** $\dfrac{y \xrightarrow{a} y'}{x+y \xrightarrow{a} y'}$

MPA: Operational Model

$$\delta\ ,\ a.\_\ ,\ \_ + \_$$

$TSS(MPA)$:

$$\text{(a)}\ \frac{}{a.x \xrightarrow{a} x}(a \in A) \qquad \text{(co)}\ \frac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'} \qquad \text{(ci)}\ \frac{y \xrightarrow{a} y'}{x + y \xrightarrow{a} y'}$$

$$TSS(MPA) \vDash a.(\delta + a.\delta) \xrightarrow{a} \delta + a.\delta \qquad TSS(MPA) \vDash (a.\delta) + \delta \xrightarrow{a} \delta$$

MPA: Behavioral Equivalence

Symmetric relation R is a bisimulation iff for all $(p, q) \in R$:

- $\forall_{l,p'} p \xrightarrow{l} p' \Rightarrow \exists_{q'} q \xrightarrow{l} q' \;\wedge\; (p', q') \in R.$

$\underline{\leftrightarrow}$ is the largest bisimulation relation on closed terms.

MPA: Operational Meets Equational

- Soundness: $\forall_{p,q}\, p = q \Rightarrow p \underline{\leftrightarrow} q.$
- Completeness: $\forall_{p,q}\, p \underline{\leftrightarrow} q \Rightarrow p = q.$

Timed-MPA

- δ : delayable deadlock,
- $a.\_$: (a class of) delayable action prefix,
- $\_ + \_$: choice

- $\underline{\underline{\delta}}$: undelayable deadlock
- $\underline{\underline{\sigma}}.\_$: unit time delay
- $\underline{\underline{a}}.\_$: (a class of) undelayable action prefix

Timed-MPA

$$\delta,\ a.\_,\ \_ + \_,\ \underline{\underline{\delta}},\ \underline{\underline{\sigma}}.\_,\ \underline{\underline{a}}.\_$$

$$TMPA:$$

$$x + y = y + x \qquad x + (y + z) = (x + y) + z$$

$$x + x = x \qquad x \not+ \delta = \not x$$

$$\delta = \underline{\underline{\sigma}}.\delta \qquad x + \underline{\underline{\delta}} = x$$

$$(\underline{\underline{\sigma}}.x) + \underline{\underline{\sigma}}.y = \underline{\underline{\sigma}}.(x + y) \qquad a.x = (\underline{\underline{a}}.x) + \underline{\underline{\sigma}}.a.x$$

$$(a.x) + \delta = a.x$$

Timed-MPA: Operational Model

$\delta,\ a.\_,\ \_+\_,\ \underline{\underline{\delta}},\ \underline{\underline{\sigma}}.\_,\ \underline{\underline{a}}.\_$

$TSS(TMPA):$

(ua) $\dfrac{}{\underline{\underline{a}}.x \xrightarrow{a} x}$ **(td)** $\dfrac{}{\underline{\underline{\sigma}}.x \xrightarrow{1} x}$

(tc0) $\dfrac{x \xrightarrow{1} x' \quad y \xrightarrow{1} y'}{x+y \xrightarrow{1} x'+y'}$ **(tc1)** $\dfrac{x \xrightarrow{1} x' \quad y \stackrel{1}{\nrightarrow}}{x+y \xrightarrow{1} x'}$ **(tc2)** $\dfrac{y \xrightarrow{1} y' \quad x \stackrel{1}{\nrightarrow}}{x+y \xrightarrow{1} y'}$

(ta) $\dfrac{}{a.x \xrightarrow{1} a.x}$ **(d)** $\dfrac{}{\delta \xrightarrow{1} \delta}$

Nostalgia: Remembering the Untimed Past

- Is there any formal link between
  the untimed theory and the timed one?
- Can we re-use any of the untimed results (i.e., equalities)
  in the timed setting?
- If yes, can we formulate "generic re-usability criteria"
  for any such extensions?

Nomenclature (1/2)

- Signature Σ: A collection of function symbols with fixed arities (e.g., δ, $a.\_$, $\_ + \_$),
- Terms $T(\Sigma)$: Built upon function symbols and variables as expected,
- Closed terms $C(\Sigma)$: terms in $T(\Sigma)$ that do not mention any variable,

Nomenclature (2/2)

- Equational theory (Σ, E): E is a set of equations on $T(\Sigma)$.
- Trans. Sys. Spec. (TSS) (Σ, L, D): A set of deduction rules defining a transition relation with L labels on closed Σ-terms

Equational Conservativity

(E_1, Σ_1) is an equationally conservative ground-extension of (E_0, Σ_0) iff:

- the signature is extended, i.e., $\Sigma_0 \subseteq \Sigma_1$ and
- the old ground-equalities are preserved,
  i.e., for all $p, p' \in C(\Sigma_0)$, $E_0 \vdash p = p' \Leftrightarrow E_1 \vdash p = p'$.

Equational Conservativity

(E_1, Σ_1) is an equationally conservative ground-extension of (E_0, Σ_0) iff:

- the signature is extended, i.e., $\Sigma_0 \subseteq \Sigma_1$ and
- the old ground-equalities are preserved,
  i.e., for all $p, p' \in C(\Sigma_0)$, $E_0 \vdash p = p' \Leftrightarrow E_1 \vdash p = p'$.

Is timed-MPA an equationally conservative ground-extension of MPA?

Equational Conservativity

(E_1, Σ_1) is an equationally conservative ground-extension of (E_0, Σ_0) iff:

- the signature is extended, i.e., $\Sigma_0 \subseteq \Sigma_1$ and
- the old ground-equalities are preserved,
  i.e., for all $p, p' \in C(\Sigma_0)$, $E_0 \vdash p = p' \Leftrightarrow E_1 \vdash p = p'$.

Is timed-MPA an equationally conservative ground-extension of MPA?
Don't know yet!

Operational Conservativity [Fokkink&Verhoef96]

$tss_1 = (\Sigma_1, L_1, D_1)$ is an operationally conservative extension of $tss_0 = (\Sigma_0, L_0, D_0)$ iff:

- the signature, labels and rules are extended:
  $\Sigma_0 \subseteq \Sigma_1$, $L_0 \subseteq L_1$ and $D_0 \subseteq D_1$ and
- no new behavior is added to the old terms:
  for all $p \in C(\Sigma_0)$, $p' \in C(\Sigma_1)$ and $l \in L_1$, $tss_0 \vdash p \xrightarrow{l} p' \Leftrightarrow tss_1 \vdash p \xrightarrow{l} p'$.

Operational Cons. Meets Equational Cons.

Theorem.

- If tss_1 is an operationally conservative extension of tss_0 and
- E_0 and E_1 are sound and complete equational theories for tss_0 and tss_1, respectively

then E_1 is an equationally conservative (ground-)extension of E_0.

Wrapping Up (Already)?

Is (the TSS of) Timed-MPA an operationally conservative extension of MPA?

(a) $\dfrac{}{a.x \xrightarrow{a} x}(a \in A)$ (c0) $\dfrac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'}$ (c1) $\dfrac{y \xrightarrow{a} y'}{x + y \xrightarrow{a} y'}$

(ua) $\dfrac{}{\underline{\underline{a}}.x \xrightarrow{a} x}$ (td) $\dfrac{}{\underline{\underline{\sigma}}.x \xrightarrow{1} x}$

(tc0) $\dfrac{x \xrightarrow{1} x' \quad y \xrightarrow{1} y'}{x + y \xrightarrow{1} x' + y'}$ (tc1) $\dfrac{x \xrightarrow{1} x' \quad y \stackrel{1}{\not\rightarrow}}{x + y \xrightarrow{1} x'}$ (tc2) $\dfrac{y \xrightarrow{1} y' \quad x \stackrel{1}{\not\rightarrow}}{x + y \xrightarrow{1} y'}$

(ta) $\dfrac{}{a.x \xrightarrow{1} a.x}$ (d) $\dfrac{}{\delta \xrightarrow{1} \delta}$

Wrapping Up? No, Sorry.

(a) $\dfrac{}{a.x \xrightarrow{a} x}(a \in A)$ (c0) $\dfrac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'}$ (c1) $\dfrac{y \xrightarrow{a} y'}{x + y \xrightarrow{a} y'}$

(ua) $\dfrac{}{\underline{\underline{a}}.x \xrightarrow{a} x}$ (td) $\dfrac{}{\underline{\underline{\sigma}}.x \xrightarrow{1} x}$

(tc0) $\dfrac{x \xrightarrow{1} x' \quad y \xrightarrow{1} y'}{x + y \xrightarrow{1} x' + y'}$ (tc1) $\dfrac{x \xrightarrow{1} x' \quad y \overset{1}{\not\to}}{x + y \xrightarrow{1} x'}$ (tc2) $\dfrac{y \xrightarrow{1} y' \quad x \overset{1}{\not\to}}{x + y \xrightarrow{1} y'}$

(ta) $\dfrac{}{a.x \xrightarrow{1} a.x}$ (d) $\dfrac{}{\delta \xrightarrow{1} \delta}$

No: $TSS(TMPA) \vdash a.\delta \xrightarrow{1} a.\delta$ but $TSS(MPA) \vdash a.\delta \overset{1}{\not\to}$

Orthogonality

$tss_1 = (\Sigma_1, L_1, D_1)$ is an orthogonal extension of $tss_0 = (\Sigma_0, L_0, D_0)$ iff:

- the signature, labels and rules are extended:
  $\Sigma_0 \subseteq \Sigma_1$, $L_0 \subseteq L_1$ and $D_0 \subseteq D_1$ and
- old behavior is extended:
  for all $p, p' \in C(\Sigma_0)$ and $l \in L_0$, $tss_0 \vdash p \xrightarrow{l} p' \Leftrightarrow tss_1 \vdash p \xrightarrow{l} p'$ and
- behavioral equalities on old terms are preserved:
  for all $p, p' \in C(\Sigma_0)$, $tss_0 \vdash p \underline{\leftrightarrow} p' \Leftrightarrow tss_1 \vdash p \underline{\leftrightarrow} p'$.

Orthogonality Meets Equational Cons.

Theorem.

- If tss_1 is an orthogonal extension of tss_0 and
- E_0 and E_1 are sound and complete equational theories for tss_0 and tss_1, respectively

then E_1 is an equationally conservative ground-extension of E_0.

Orthogonality

$tss_1 = (\Sigma_1, L_1, D_1)$ is an orthogonal extension of $tss_0 = (\Sigma_0, L_0, D_0)$ iff:

- the signature, labels and rules are extended:
  $\Sigma_0 \subseteq \Sigma_1$, $L_0 \subseteq L_1$ and $D_0 \subseteq D_1$ and
- old behavior is extended:
  for all $p, p' \in C(\Sigma_0)$ and $l \in L_0$, $tss_0 \vdash p \xrightarrow{l} p' \Leftrightarrow tss_1 \vdash p \xrightarrow{l} p'$ and
- equalities on old terms are preserved:
  for all $p, p' \in C(\Sigma_0)$, $tss_0 \vdash p \underline{\leftrightarrow} p' \Leftrightarrow tss_1 \vdash p \underline{\leftrightarrow} p'$.

Is timed-MPA an orthogonal extension of MPA?
Don't know yet!

Granting Extensions

$tss_1 = (\Sigma_1, L_1, D_1)$ is a granting extension of $tss_0 = (\Sigma_0, L_0, D_0)$ iff:

- the signature, labels and rules are extended:
  $\Sigma_0 \subseteq \Sigma_1$, $L_0 \subseteq L_1$ and $D_0 \subseteq D_1$ and
- old behavior is extended:

  for all $p, p' \in C(\Sigma_0)$ and $l \in L_0$, $tss_0 \vdash p \xrightarrow{l} p' \Leftrightarrow tss_1 \vdash p \xrightarrow{l} p'$ and
- self-transitions with new labels are added to old terms:

  for all $p, p' \in C(\Sigma_0)$ and $l \notin L_0$, $tss_1 \vdash p \xrightarrow{l} p' \Leftrightarrow p = p'$.

Granting Extensions

$tss_1 = (\Sigma_1, L_1, D_1)$ is a granting extension of $tss_0 = (\Sigma_0, L_0, D_0)$ iff:

- the signature, labels and rules are extended:
  $\Sigma_0 \subseteq \Sigma_1$, $L_0 \subseteq L_1$ and $D_0 \subseteq D_1$ and
- old behavior is extended:

  for all $p, p' \in C(\Sigma_0)$ and $l \in L_0$, $tss_0 \vdash p \xrightarrow{l} p' \Leftrightarrow tss_1 \vdash p \xrightarrow{l} p'$ and
- self-transitions with new labels are added to old terms:

  for all $p, p' \in C(\Sigma_0)$ and $l \notin L_0$, $tss_1 \vdash p \xrightarrow{l} p' \Leftrightarrow p = p'$.

Is timed-MPA a granting extension of MPA?

Granting Extensions

Is timed-MPA a granting extension of MPA?

(a) $$\frac{}{a.x \xrightarrow{a} x}\ (a \in A)$$

(c0) $$\frac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'}$$

(c1) $$\frac{y \xrightarrow{a} y'}{x + y \xrightarrow{a} y'}$$

(ua) $$\frac{}{\underline{\underline{a}}.x \xrightarrow{a} x}$$

(td) $$\frac{}{\underline{\underline{\sigma}}.x \xrightarrow{1} x}$$

(tc0) $$\frac{x \xrightarrow{1} x' \quad y \xrightarrow{1} y'}{x + y \xrightarrow{1} x' + y'}$$

(tc1) $$\frac{x \xrightarrow{1} x' \quad y \overset{1}{\not\rightarrow}}{x + y \xrightarrow{1} x'}$$

(tc2) $$\frac{y \xrightarrow{1} y' \quad x \overset{1}{\not\rightarrow}}{x + y \xrightarrow{1} y'}$$

(ta) $$\frac{}{a.x \xrightarrow{1} a.x}$$

(d) $$\frac{}{\delta \xrightarrow{1} \delta}$$

Granting Extensions

Is timed-MPA a granting extension of MPA? Looks like!

(a) $$\frac{}{a.x \xrightarrow{a} x}(a \in A)$$

(c0) $$\frac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'}$$

(c1) $$\frac{y \xrightarrow{a} y'}{x + y \xrightarrow{a} y'}$$

(ua) $$\frac{}{\underline{\underline{a}}.x \xrightarrow{a} x}$$

(td) $$\frac{}{\underline{\underline{\sigma}}.x \xrightarrow{1} x}$$

(tc0) $$\frac{x \xrightarrow{1} x' \quad y \xrightarrow{1} y'}{x + y \xrightarrow{1} x' + y'}$$

(tc1) $$\frac{x \xrightarrow{1} x' \quad y \not\xrightarrow{1}}{x + y \xrightarrow{1} x'}$$

(tc2) $$\frac{y \xrightarrow{1} y' \quad x \not\xrightarrow{1}}{x + y \xrightarrow{1} y'}$$

(ta) $$\frac{}{a.x \xrightarrow{1} a.x}$$

(d) $$\frac{}{\delta \xrightarrow{1} \delta}$$

Some Simple Observations

- An operational conservative extension is an orthogonal extension.
- A granting extension is an orthogonal extension.

Combining Granting and Operational Conserv.

- Orthogonal extension is pre-order (i.e., reflexive and transitive) on TSS's.

- If $tss_1 \cup tss_0$ and $tss_2 \cup tss_0$ are
granting and operational conservative extensions of tss_0, respectively,
labels of tss_1 and tss_0 are disjoint and
labels of tss_1 and tss_2 are disjoint

  then $tss_2 \cup tss_1 \cup tss_0$ is an orthogonal extension of tss_0.

Operational Conservativity Criteria

Theorem (Sketch).
Consider tss_1 and tss_0. If for all deduction rules tss_1 one of the following holds:

- the source of the conclusion d mentions a function symbol not in Σ_0 or,
- a *relevant premise* of d has a label not in L_1 or a target not in $T(\Sigma_0)$,

then $tss_0 \cup tss_0$ is an operational conservative extension of tss_0

Syntactic Granting Criteria

- Mainly concern unification:

- Check whether there are enough unifiable rules that
  can cover the old syntax and,
  the non-unifiable ones should
  have a term not from the old syntax in the source of the conclusion or
  have relevant negative premises with the granting labels.

Granting Criteria

(a) $\dfrac{}{a.x \xrightarrow{a} x}(a \in A)$

(c0) $\dfrac{x \xrightarrow{a} x'}{x + y \xrightarrow{a} x'}$

(c1) $\dfrac{y \xrightarrow{a} y'}{x + y \xrightarrow{a} y'}$

(ua) $\dfrac{}{\underline{\underline{a}}.x \xrightarrow{a} x}$

(td) $\dfrac{}{\underline{\underline{\sigma}}.x \xrightarrow{1} x}$

(tc0) $\dfrac{x \xrightarrow{1} x' \quad y \xrightarrow{1} y'}{x + y \xrightarrow{1} x' + y'}$

(tc1) $\dfrac{x \xrightarrow{1} x' \quad y \not\xrightarrow{1}}{x + y \xrightarrow{1} x'}$

(tc2) $\dfrac{y \xrightarrow{1} y' \quad x \not\xrightarrow{1}}{x + y \xrightarrow{1} y'}$

(ta) $\dfrac{}{a.x \xrightarrow{1} a.x}$

(d) $\dfrac{}{\delta \xrightarrow{1} \delta}$

Unification: Towards Granting Criteria

- The set of terms generated by t is the set of $\{\sigma(t) | \sigma : \mathcal{V} \mapsto T(\Sigma)\}$
- Substitution σ is a unifier for $t \xrightarrow{l} t'$ iff $\sigma(t) = \sigma(t')$
- $t \xrightarrow{l} t'$ is unifiable if there is a unifier σ for it
- $U(t \xrightarrow{l} t')$ denotes the set of all unifiers for $t \xrightarrow{l} t'$
- for a set H of positive transition formulae,
  $U(H)$ denotes the intersection of unifiers for all $h \in H$

Granting Criteria (Simplified)

Consider $tss_0 = (\Sigma_0, L_0, D_0)$. The granting criteria for tss_0 is defined as follows.
For all deduction rules $d = \frac{H}{c}$ in D_1 one of the following holds:

- H has no negative transition formulae,
- the size of terms decreases
  from the source of conclusion to the source of all premises,
- the conclusion of d is unifiable and $U(H) \subseteq U(c)$,

and further, the conclusions of D_1 with their unifiers applied to them can generate all Σ_0 terms.

Overview

Done:

1. the basic ideas behind languages extensions;
2. suggested the concepts of ground-equational conservative and orthogonal extensions (as a way to prove g.-eq. cons. ext.),
3. presented operational conservative and granting as two extremes of orthogonality,
4. formulated syntactic criteria to capture granting extensions and ways of combining the two extremes.

To be done:

1. moving the multi-sorted settings with variable binding,
2. investigating other syntactic ways of proving orthogonality.

Overview

Further reading:

1. M.R. Mousavi, Michel A. Reniers, *Orthogonal Extensions in Structural Operational Semantics*, Technical Report CSR-05-16, Eindhoven University of Technology, 2005.
2. J.C.M. Baeten, M.R. Mousavi, Michel A. Reniers, *Timing the Untimed: Terminating Successfully while Being Conservative*, Technical Report CSR-05-21, Eindhoven University of Technology, 2005.

Overview

- ✓ Motivating Example
- ✓ Definitions
- ✓ Meta-Theorems
- ✓ Conclusion

Thank You!

Operational Conservativity Meta-Theorem

Theorem (Sketch).
Consider $tss_1 = (\Sigma_1, L_1, D_1)$ and $tss_0 = (\Sigma_0, L_0, D_0)$. If for all deduction rules d in D_1 one of the following holds:

- the source of the conclusion d mentions a function symbol not in Σ_0 or,
- a (relevant) premise of d has a label not in L_1 or a target not in $T(\Sigma_0)$,

then $(\Sigma_0 \cup \Sigma_1, L_0 \cup L_1, D_0 \cup D_1)$ is an operational conservative extension of tss_0