# Unifying Operational Semantics with Algebraic Semantics for Instantaneous Reactions

Chengcheng Wu  Yongxin Zhao  Huibiao Zhu

Shanghai Key Laboratory of Trustworthy Computing
Software Engineering Institute, East China Normal University

UTP 2012, 27-28 August, 2012

# Outline

# Outline

# Background

1. **Real-time systems (RTS):**
   (a) RTS are widely used in many areas.
   (b) Great challenges in modeling, designing, analyzing and verifying RTS
   (c) Methods in RTS research: Finite Automata, Timed Automata, Process Algebra, Esterel, etc
2. **Related Work:**
   (a) Esterel is a synchronous language with many great processing methods.
   (b) Inspired by the Esterel language, we have proposed a signal calculus (I-Calculus).

# Contribution

(1) **Operational Semantics**

- Investigated the semantics for instantaneous reactions from an operational perspective

(2) **Unifying the Operational semantics with the algebraic semantics**

- The soundness of algebraic semantics
- The relative completeness of algebraic semantics with respect to the operational semantics.

# Outline

# I-Calculus: Event

- **Signal:** basic communication and synchronization method.
  - Three status: *presence*$(+)$, *absence*$(-)$ and *unknown*$(0)$
  - The order of status: $+ \geq 0$ and $- \geq 0$
- **Event:** $e : S \rightarrow B$.
  - Describe the status of signals we are observing
- **Definition (Compatible):**

  Event $e_1$ and $e_2$ are compatible on the signal name set $S$ if they agree with the status of all signals, i.e.,
  $\forall s \in S \bullet e_1(s) = e_2(s) \vee (s, 0) \in e_1 \vee (s, 0) \in e_2$.

  We denote it by compatible$(e_1, e_2)$.
- **Pre-order of Events**

  We say event $e_1$ is better than event $e_2$ if $\forall s \in S \bullet e_1(s) \geq e_2(s)$.
  We denote this by $e_1 \geq e_2$.

**Event Guard:** $g ::= \epsilon \mid \emptyset \mid s^+ \mid s^- \mid g \cdot g \mid g + g \mid \overline{g}.$

**Table 1. The Meaning of Event Guards**

$$[\![\epsilon]\!] =_{df} \mathbb{E} \quad [\![\emptyset]\!] =_{df} \emptyset \quad [\![s^+]\!] =_{df} \{e \mid (s,+) \in e \wedge e \in \mathbb{E}\}$$

$$[\![s^-]\!] =_{df} \{e \mid (s,-) \in e \wedge e \in \mathbb{E}\} \quad [\![g_1 + g_2]\!] =_{df} [\![g_1]\!] \cup [\![g_2]\!]$$

$$[\![g_1 \cdot g_2]\!] =_{df} \{e \mid e \in [\![g_1]\!] \wedge e \in [\![g_2]\!]\}$$

$$[\![\overline{g}]\!] =_{df} \{e \mid \forall f \in [\![g]\!] \bullet \neg \mathsf{compatible}(e,f)\}$$

## I-Calculus: Syntax

$$I ::= !s \mid I\!I \mid \bot \mid g\&I \mid I\backslash s \mid I \parallel I$$

- $!s$ is an atomic action emitting signal $s$.
- $I\!I$ is a skip reaction and $\bot$ is a chaos reaction.
- In $g\&I$, $I$ will be only executed when guard $g$ is triggered.
- $I\backslash s$ hides the actions on $s$ inside $I$.

**Example:** Let $I = s_2^+\&!s_1 \parallel (s_1^+ \cdot s_2^+)\&!s_3 \parallel s_1^-\&\bot$.

**Case 1:** If the given an input event is $e = \{(s_2, +)\}$, then ...

**Case 2:** If the given input event is $e = \{(s_1, -)\}$, $I$ will fall into chaos.

# Outline

# Operational Semantics: Configurations

- **Transition:**

  $C \longrightarrow C'$

- **Configuration:**

  $\langle I, e \rangle$ is a configuration.

- **Stable Configuration:**

  $\langle I, e \rangle^s_{stable}$ is stable in the status of signal $s$
  if for all $e' \geq e$, $\quad \langle I, e' \rangle \longrightarrow_* \langle I', e'' \rangle$
  $\quad \Longrightarrow \quad e(s) = e'(s) = e''(s)$

- **Two Special Configurations:**

  $\langle \mathit{ll}, e \rangle_{term}$ and $\langle \perp, e \rangle_{chaos}$.

# Operational Semantics: Primitives and Guarded Reactions

- **Primitives:**

$$\langle !s, e\rangle \longrightarrow \langle \bot, e\rangle, \text{ where } (s, -) \in e.$$

$$\langle !s, e\rangle \longrightarrow \langle \mathit{II}, e'\rangle, \text{ where } (s, -) \notin e \text{ and } e' = e \oplus (s, +).$$

- **Guarded Reactions:**

$$\langle g \& I, e\rangle \longrightarrow \langle I, e\rangle, \text{ if } e \in [\![g]\!]$$

$$\langle g \& I, e\rangle \longrightarrow \langle \mathit{II}, e\rangle, \text{ if } e \in [\![\overline{g}]\!]$$

# Operational Semantics: Parallel Reactions

- **Basic Parallels:**

$$\frac{\langle l_1, e\rangle_{term}}{\langle l_1 || l_2, e\rangle \longrightarrow \langle l_2, e\rangle}$$

$$\frac{\langle l_1, e\rangle_{chaos}}{\langle l_1 || l_2, e\rangle \longrightarrow \langle \bot, e\rangle_{chaos}}$$

- **Parallels:**

$$\frac{\langle l_1, e\rangle \longrightarrow \langle l_1', e'\rangle}{\langle l_1 || l_2, e\rangle \longrightarrow \langle l_1' || l_2, e'\rangle}$$

# Operational Semantics: Concealment

**Concealment Rules:**

$$\frac{\langle I, e\rangle \longrightarrow \langle \bot, e\rangle_{chaos}}{\langle I\backslash s, e\rangle \longrightarrow \langle \bot, e\rangle_{chaos}},$$

$$\frac{\langle I, e\rangle \longrightarrow \langle I', e'\rangle^{s}_{stable}}{\langle I\backslash s, e\rangle \longrightarrow \langle I[\emptyset/s^{-}, \epsilon/s^{+}, \mathit{II}/!s], e\rangle}, \text{ when } (s,+) \in e'$$

$$\frac{\langle I, e\rangle \longrightarrow \langle I', e'\rangle^{s}_{stable}}{\langle I\backslash s, e\rangle \longrightarrow \langle I[\emptyset/s^{+}, \epsilon/s^{-}], e'\rangle}, \text{ when } (s,+) \notin e'$$

$$\frac{\langle I, e\rangle \longrightarrow \langle I', e'\rangle}{\langle I\backslash s, e\rangle \longrightarrow \langle I'\backslash s, e'\rangle}, \text{ when } (s,+) \notin e'.$$

- The second transition rule describes the action of emitting a local signal by the inner reaction.
- The third transition rule defines the opposite situation when the action of emitting the local signal does not exist.

  In order to be invisible to the outside, we make the replacement $I[\emptyset/s^{+}, \epsilon/s^{-}]$.

# Operational Semantics: Example

**Example 1:**

Let $l_1 = (t^+ \& !s \parallel s^+ \& !k) \backslash s$ and $e = \{(t, +)\}$.

$$\begin{aligned} \langle l_1, e \rangle &\longrightarrow \langle (!s \parallel s^+ \& !k) \backslash s,\ \{(t, +)\} \rangle \\ &\longrightarrow \langle !k,\ \{(t, +)\} \rangle \\ &\longrightarrow \langle \mathit{ll},\ \{(k, +), (t, +)\} \rangle_{term} \end{aligned}$$

# Outline

# Algebraic Laws (1)

- **Definition:**

  The equivalence of two reactions is denoted by $I_1 =_O I_2$. The equivalence means that for any $e$ we have

$$\langle I_1, e\rangle \longrightarrow_* \langle I\!I, e'\rangle_{term} \iff \langle I_2, e\rangle \longrightarrow_* \langle I\!I, e'\rangle_{term},$$

$$\langle I_1, e\rangle \longrightarrow_* \langle \bot, e_1\rangle_{chaos} \iff \langle I_2, e\rangle \longrightarrow_* \langle \bot, e_2\rangle_{chaos}$$

- **Basic laws:**

**Equiv-1** $I =_O I$ (*reflexivity*)

**Equiv-2** $I_1 =_O I_2 \iff I_2 =_O I_1$ (*commutativity*)

**Equiv-3** $\exists I_2 \bullet I_1 =_O I_2 \wedge I_2 =_O I_3 \iff I_1 =_O I_3$ (*transitivity*)

# Algebraic Laws(2)

- **Laws for Parallel**

  **Par-1** $I_1 \parallel I_2 =_O I_2 \parallel I_1$

  **Par-2** $(I_1 \parallel I_2) \parallel I_3 =_O I_1 \parallel (I_2 \parallel I_3)$

  **Par-3** $I \parallel I =_O I$

  **Par-4** $\perp \parallel I =_O \perp$

  **Par-5** $\mathit{II} \parallel I =_O \mathit{II}$

- **Laws for Guarded Reactions**

  **Guard-1** $g_1 \& (g_2 \& I) =_O (g_1 \cdot g_2) \& I$

  **Guard-2** $g_1 \& I \parallel g_2 \& I =_O (g_1 + g_2) \& I$

  **Guard-3** $g \& (I_1 \parallel I_2) =_O g \& I_1 \parallel g \& I_2$

  **Guard-4** $\emptyset \& I =_O \mathit{II}$

  **Guard-5** $\epsilon \& I =_O I$

  **Guard-6** $g \& \mathit{II} =_O \mathit{II}$

# Algebraic Laws(3)

- **Laws for Concealment**

  **Conc-1** $(I\backslash s)\backslash t \;=_O\; (I\backslash t)\backslash s$

  **Conc-2** $(I_1 \parallel I_2)\backslash s \;=_O\; (I_1\backslash s) \parallel I_2$, provided that $s \notin I_2$

  **Conc-3** $(g\&I)\backslash s \;=_O\; g\&(I\backslash s)$, provided that $s \notin g$

  **Conc-4** $(g\&!s \parallel I)\backslash s \;=_O\; I[g/s^+, \overline{g}/s^-]$,
  provided that $s \notin g \wedge s \notin ems(I)$

- **Laws for Primitive Commands**

  **Prim-1** $s^-\&!s \;=_O\; s^-\&\bot$

  **Prim-2** $s^+\&!s \;=_O\; s^+\&\mathit{II}$

- **Dependency Law:**

  **Depend-law** $g\&!s \parallel s^+\&I \;=_O\; g\&!s \parallel (s^+ + g)\&I$

# Algebraic Laws: Proof (1)

All the laws listed can be proved, we just give an example.

Proof of law $g_1 \& (g_2 \& I) =_O (g_1 \cdot g_2) \& I$

(1) For any $e$, if we have the transition

$$\langle g_1 \& (g_2 \& I), e \rangle \longrightarrow_* \langle \mathit{II}, e' \rangle_{term}$$

if all guards for $I$ can be fired, we can find an intermediate state $\langle I, e \rangle$ that

$$\langle g_1 \& (g_2 \& I), e \rangle \longrightarrow_* \langle I, e \rangle \longrightarrow_* \langle \mathit{II}, e' \rangle_{term},$$

where $e \in [\![g_1]\!]$ and $e \in [\![g_2]\!]$ from which we have $e \in [\![g_1 \cdot g_2]\!]$. So for the second reaction, we have

$$\langle (g_1 \cdot g_2) \& I, e \rangle \longrightarrow_* \langle I, e \rangle \text{ and } \langle I, e \rangle \longrightarrow_* \langle \mathit{II}, e' \rangle_{term}.$$

# Algebraic Laws: Proof (2)

(1) (continued)

If the negation of the guards for $I$ can be fired, we can find that $e = e'$ and either $e \in [\![\overline{g_1}]\!]$ or $e \in [\![\overline{g_2}]\!]$ which implies that $e \in [\![\overline{g_1 \cdot g_2}]\!]$, then we have

$$\langle (g_1 \cdot g_2)\&I, e\rangle \longrightarrow \langle \phi\&I, e\rangle \longrightarrow \langle II, e\rangle_{term}$$

Then we have proved that for any $e$,

$$\langle g_1\&(g_2\&I), e\rangle \longrightarrow_* \langle II, e'\rangle_{term} \Longrightarrow \langle (g_1 \cdot g_2)\&I, e\rangle \longrightarrow_* \langle II, e'\rangle_{term}.$$

(2) The proof of the other side is just similar.

# Soundness of the Algebraic Laws

After all laws have been established in our framework of operational semantics, we can claim the soundness of algebraic semantics.

**Theorem 1 (Soundness)**

If two reactions is algebraically equivalent, they are also equivalent with the respect to the operational semantics.

$$I_1 = I_2 \Longrightarrow I_1 =_O I_2$$

# Outline

# The Relative Completeness (1)

**Aim:**

We come to prove that reactions which are equivalent from the operational perspective should be algebraically equivalent.

**Normal Form (Motivation):**

The equivalence of two reactions depends on the equivalence of their normal forms.

**Definition (Normal Form):**

The reaction $||_{m\in M} g_m \& !s_m \;||\; h \& \bot$ is a normal form for I-calculus if it satisfies the two conditions below, where the index set $M$ is finite and all signals $s_i (i \in M)$ are different.

1. $\forall m, n \in M, g \bullet (g \cdot s_n^+ \geq g_m \Rightarrow g \cdot g_n \geq g_m) \wedge (g \cdot s_n^+ \geq h \Rightarrow g \cdot g_n \geq h)$.
2. $\forall m \in M, g_m \cdot s_m^- \geq h \geq g_m$.

# The Relative Completeness (2)

**Example:**

$$NF = (s_1^- + s_2^+ + s_3^+)\&!s_1 \,||\, (s_1^- + s_2^+ \cdot s_3^-)\&!s_2 \,||\, (s_1^- + s_2^+)\&!s_3 \,||\, (s_1^- + s_2^+ \cdot s_3^-)\&\bot$$

**Definition (Equivalence of Normal Form)**

$$NF_1 = NF_2 \textit{ iff } h \equiv h' \textit{ and } \forall i \in M \bullet g_i \equiv g'_i,$$
$$\textit{where } NF_1 = ||_{m \in M} g_m \&!s_m \,||\, h\&\bot$$
$$\textit{and } NF_2 = ||_{m \in M} g'_m \&!s_m \,||\, h'\&\bot \textit{ are normal forms.}$$

**Theorem 2:** All instantaneous reactions can be reduced into normal forms.

**Corollary 1:** $I_1 = I_2$ *iff* $NF_1 = NF_2$, where $NF_1$ *and* $NF_2$ are the normal forms of reaction $I_1$ and $I_2$ respectively.

# The Relative Completeness (3)

**Lemma 1**

$I_1 =_O I_2 \Longrightarrow NF_1 = NF_2$ where $NF_1$ and $NF_2$ are the normal form of reaction $I_1$ and $I_2$ respectively.

Based on lemma 1, we can obtain the relative completeness of algebraic semantics.

**Theorem 3 (Relative Completeness)**

If two reactions are equivalent from the operational perspective, they are also algebraically equivalent.

$$I_1 =_O I_2 \Longrightarrow I_1 = I_2$$

**Theorem 4**

Two reactions are equivalent from the operational perspective if and only if they are algebraically equivalent.

$$I_1 =_O I_2 \Longleftrightarrow I_1 = I_2$$

# The Soundness and the Relative Completeness: Example

**Example.** Here are two differently written reactions.

$$
\begin{aligned}
I_1 &= (s_1^- \&!t \parallel t^+ \&!s_2)\backslash t \parallel s_2^+ \&!s_3 \parallel s_3^+ \&!s_1 \\
I_2 &= (s_1^- + s_2^+ + s_3^+)\&!s_1 \parallel (s_1^- + s_2^+ \cdot s_3^-)\&!s_2 \\
&\quad \parallel (s_1^- + s_2^+)\&!s_3 \parallel (s_1^- + s_2^+ \cdot s_3^-)\&\bot
\end{aligned}
$$

From the definition of normal form, we obtain that $I_2$ is a normal form. And from the algebraic laws, we can reduce the first reaction $I_1$ to $I_2$.

$$
\begin{aligned}
I_1 &= (s_1^- \&!t \parallel t^+ \&!s_2)\backslash t \parallel s_2^+ \&!s_3 \parallel s_3^+ \&!s_1 && \{depend - law\} \\
&= (s_1^- \&!t \parallel (s_1^- + t^+)\&!s_2)\backslash t \parallel s_2^+ \&!s_3 \parallel s_3^+ \&!s_1 && \{conc - 4\} \\
&= s_1^- \&!s_2 \parallel s_2^+ \&!s_3 \parallel s_3^+ \&!s_1 && \{depend - 1\} \\
&= s_1^- \&!s_2 \parallel (s_1^- + s_2^+)\&!s_3 \parallel s_3^+ \&!s_1 && \{depend - 2\} \\
&= (s_1^-)\&!s_2 \parallel (s_1^- + s_2^+)\&!s_3 \parallel (s_1^- + s_2^+ + s_3^+)\&!s_1 && \{guard - 2, 3, 4\} \\
&= (s_1^-)\&!s_2 \parallel (s_1^- + s_2^+)\&!s_3 \parallel (s_1^- + s_2^+ + s_3^+)\&!s_1 \\
&\quad \parallel (s_1^- + s_2^+ \cdot s_3^-)\&\bot && \{guard - 2\} \\
&= (s_1^- + s_2^+ + s_3^+)\&!s_1 \parallel (s_1^- + s_2^+ \cdot s_3^-)\&!s_2 \\
&\quad \parallel (s_1^- + s_2^+)\&!s_3 \parallel (s_1^- + s_2^+ \cdot s_3^-)\&\bot \\
&= I_2
\end{aligned}
$$

# Outline

# Conclusion and Future Work

## 1. Conclusion:

- We have investigated the semantics for instantaneous reactions from an operational perspective.
- We have investigated the linking theory of operational semantics and algebraic semantics for instantaneous reactions

  -**Soundness.** All the algebraic laws can be established in terms of the operational semantics, i.e

  -**Relative Completeness.** Reactions which are equivalent from the operational perspective can be reduced to the same normal form

## 2. Future Work:

- In the future, we will take sequential reaction, time-delayed reactions and more features into our consideration to complete the operational semantics for the instantaneous calculus.

**Thank you very much!**