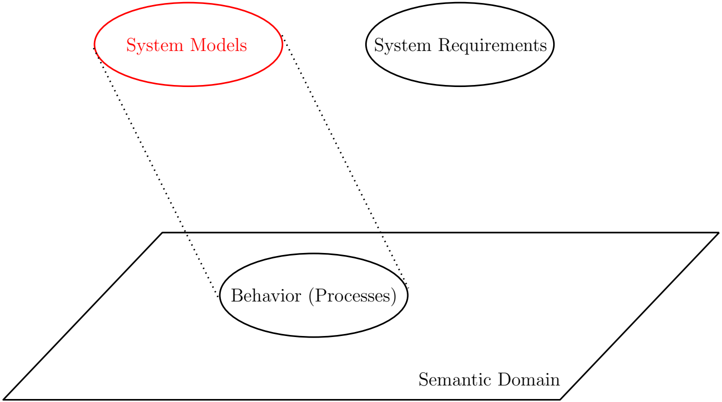
System Validation: Describing (Multi-)actions

Mohammad Mousavi and Jeroen Keiren

HALMSTAD UNIVERSITY

Open Universiteit

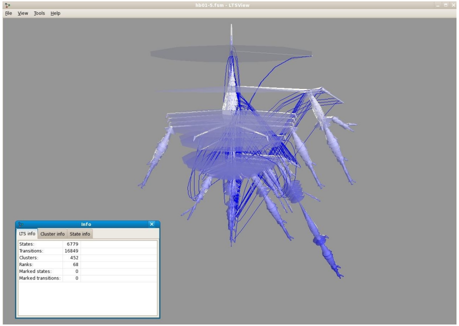
General Overview



From Processes to Their Algebra

Motivation

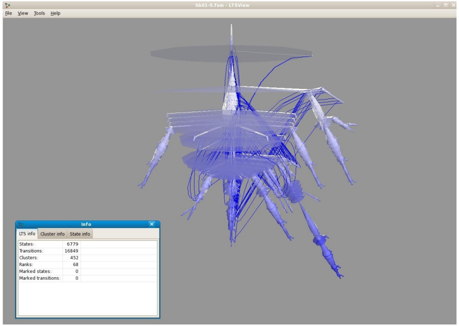
- Graphical representation is monstrously big



From Processes to Their Algebra

Motivation

- Graphical representation is monstrously big
- Manipulating and analyzing the graphical representation is virtually impossible



From Processes to Their Algebra

Motivation

- Graphical representation is monstrously big
- Manipulating and analyzing the graphical representation is virtually impossible

Solution

Use a compact textual presentation and algebraic rules for manipulating them

Actions

- Atomic building blocks of processes
- May represent:
  - internal activities
  - sending messages
  - receiving messages
  - the result of a synchronization
- May take parameters, typically denoted by $a(d)$ of any Abstract Data Type

Actions
Examples

- `act rcv_coin: Euro;`
  $rcv\_coin(one\_euro)$

Actions
Examples

- `act rcv_coin: Euro;`
  rcv_coin(one_euro)
- `act snd_number,rcv_number: Nat;`
  snd_number(1)

Actions
Examples

- `act rcv_coin: Euro;`
  rcv_coin(one_euro)
- `act snd_number,rcv_number: Nat;`
  snd_number(1)
- `act ack_number: Bool # Nat;`
  ack_number(true, 42)

Actions
Examples

- `act rcv_coin: Euro;`
  rcv_coin(*one_euro*)
- `act snd_number,rcv_number: Nat;`
  snd_number(*1*)
- `act ack_number: Bool # Nat;`
  ack_number(*true*, *42*)

Note
Actions are not functions or procedures, in the programming languages' sense

Multi-Actions

- A number of actions happening at the same time
  $receive(d) \mid send(d)$

Multi-Actions

- A number of actions happening at the same time
  $\mathit{receive}(d) \mid \mathit{send}(d)$
- Types of multi-actions:

Multi-Actions

- A number of actions happening at the same time
  $receive(d) \mid send(d)$
- Types of multi-actions:
  - τ internal (invisible) action

Multi-Actions

- A number of actions happening at the same time
  $\mathit{receive}(d) \mid \mathit{send}(d)$
- Types of multi-actions:
  - τ internal (invisible) action
  - a unparameterised action

Multi-Actions

- A number of actions happening at the same time
  $\mathit{receive}(d) \mid \mathit{send}(d)$
- Types of multi-actions:
  - τ internal (invisible) action
  - a unparameterised action
  - $a(\vec{d})$ action with parameters

Multi-Actions

- A number of actions happening at the same time
  $\mathit{receive}(d) \mid \mathit{send}(d)$
- Types of multi-actions:
  - τ internal (invisible) action
  - a unparameterised action
  - $a(\vec{d})$ action with parameters
  - $\alpha \mid \beta$ composite multi-action consisting of α and β

Basic Axioms for Multi-Actions

Axioms for multi-actions used in reasoning about processes

MA1	$\alpha \mid \beta = \beta \mid \alpha$
MA2	$(\alpha \mid \beta) \mid \gamma = \alpha \mid (\beta \mid \gamma)$
MA3	$\alpha \mid \tau = \alpha$

Example

$\mathit{receive}(d) \mid \mathit{send}(d) = \mathit{send}(d) \mid \mathit{receive}(d) \mid \tau$ by MA1 and MA3

Reasoning about multi-actions

Modelling of communication requires reasoning rules for multi-actions.

Reasoning about multi-actions

Modelling of communication requires reasoning rules for multi-actions.

Example

If *send* | *receive* communicate to *comm* we need rules to do transformation

Reasoning about multi-actions

Modelling of communication requires reasoning rules for multi-actions.

Example

If *send* | *receive* communicate to *comm* we need rules to do transformation

Auxiliary operators:

- Removal of multi-actions $\alpha \setminus \beta$

Reasoning about multi-actions

Modelling of communication requires reasoning rules for multi-actions.

Example

If *send* | *receive* communicate to *comm* we need rules to do transformation

Auxiliary operators:

- Removal of multi-actions $\alpha \setminus \beta$
- Inclusion between multi-action $\alpha \sqsubseteq \beta$

Reasoning about multi-actions

Modelling of communication requires reasoning rules for multi-actions.

Example

If *send* $|$ *receive* communicate to *comm* we need rules to do transformation

Auxiliary operators:

- Removal of multi-actions $\alpha \setminus \beta$
- Inclusion between multi-action $\alpha \sqsubseteq \beta$
- Stripping data off $\underline{\alpha}$

Axioms for Removal of Multi-Actions $\alpha \setminus \beta$

MD1	$\tau \setminus \alpha = \tau$
MD2	$\alpha \setminus \tau = \alpha$
MD3	$\alpha \setminus (\beta \,\vert\, \gamma) = (\alpha \setminus \beta) \setminus \gamma$
MD4	$(a(d) \,\vert\, \alpha) \setminus a(d) = \alpha$
MD5	$(a(d) \,\vert\, \alpha) \setminus b(e) = a(d) \,\vert (\alpha \setminus b(e)) \quad$ if $a \not\equiv b$ or $d \not\approx e$

Example

- $(send(d)|error|receive(d)) \setminus (send(d)|receive(d)) = error$
- $a \setminus a = \tau$

Axioms for Inclusion of Multi-Actions $\alpha \sqsubseteq \beta$

MS1	$\tau \sqsubseteq \alpha = \mathit{true}$
MS2	$a \sqsubseteq \tau = \mathit{false}$
MS3	$a(d) \mid \alpha \sqsubseteq a(d) \mid \beta = \alpha \sqsubseteq \beta$
MS4	$a(d) \mid \alpha \sqsubseteq b(e) \mid \beta = a(d) \mid (\alpha \setminus b(e)) \sqsubseteq \beta \quad \text{if } a \not\equiv b \text{ or } d \not\approx e$

Example

- $a(1) \sqsubseteq a(1)|b(2) = \mathit{true}$
- $a(1) \sqsubseteq b(2) = \mathit{false}$

MAN1	$\underline{\tau} = \tau$
MAN2	$\underline{a(d)} = a$
MAN3	$\underline{\alpha \mid \beta} = \underline{\alpha} \mid \underline{\beta}$

Example

$$\underline{ack\_number(true, 42) \mid error} \overset{MAN3}{=} \underline{ack\_number(true, 42)} \mid \underline{error}$$

$$\overset{MAN2}{=} ack\_number \mid error$$

Example

Show using the axioms that $(b \mid a(d)) \setminus a(d) = b$

$$(b \mid a(d)) \setminus a(d)$$

Example

Show using the axioms that $(b \,|\, a(d)) \setminus a(d) = b$

$$(b \,|\, a(d)) \setminus a(d)$$

MA1 $\quad \alpha \,|\, \beta = \beta \,|\, \alpha$

Example

Show using the axioms that $(b \mid a(d)) \setminus a(d) = b$

$$(b \mid a(d)) \setminus a(d) \stackrel{MA1}{=} (a(d) \mid b) \setminus a(d)$$

MA1 $\quad \alpha \mid \beta = \beta \mid \alpha$

Example

Show using the axioms that $(b \mid a(d)) \setminus a(d) = b$

$$(b \mid a(d)) \setminus a(d) \overset{MA1}{=} (a(d) \mid b) \setminus a(d)$$

MD4 $\quad (a(d) \mid \alpha) \setminus a(d) = \alpha$

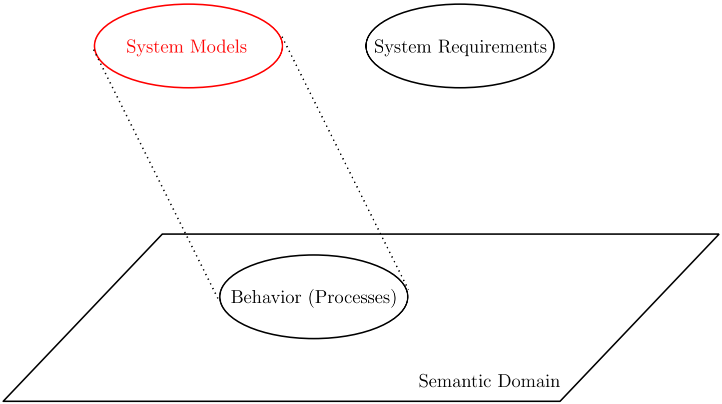
Example

Show using the axioms that $(b \mid a(d)) \setminus a(d) = b$

$$(b \mid a(d)) \setminus a(d) \overset{MA1}{=} (a(d) \mid b) \setminus a(d)$$
$$\overset{MD4}{=} b$$

MD4 $\quad (a(d) \mid \alpha) \setminus a(d) = \alpha$

General Overview



Thank you very much.