Some Issues and Challenges when Testing from Symbolic and Timed Specifications

Julien Schmaltz

Institute for Computing and Information Sciences
Radboud University Nijmegen
The Netherlands
julien@cs.ru.nl
Context

- Model-Based Testing
- Black-box
- Based on Labeled Transition Systems (LTS)
- Formal conformance relation (\textit{ioco} and variations)
- Automatic
- European Project Training and Research On Testing (TAROT)
  - Postdoc in Nijmegen since March 2007
  - Joint work with Jan Tretmans
  - Previous experience with theorem proving and hardware
Realistic Safety-Critical Systems deal with both:
  - Symbolic Models
    - Several data types
    - Operations on constants and variables
  - Timed Models
    - Timed events and actions
    - Timing requirements

There are formal testing techniques for each one of them, but none for both.
**Objective**

- Global objective: combine testing techniques for timed and symbolic systems
- Today: discuss “problems” ... Issues and Challenges!
Outline

1. The ioco theory and its variations
   - The original ioco theory
   - Symbolic ioco
   - Timed ioco

2. Timed and Symbolic Models
   - Flow between symbolic and timed models
   - Symbolic Timed Automata: Syntax and Semantics
   - Quiescence
Input Output Labeled Transition System (IOLTS) model of the supplier.
Input Output Conformance: the \textit{ioco} theory

- Specification models are IOLTS
- Implementation models are input-enabled IOLTS
- Implementation $Imp$ is \textit{ioco}-conforming to Specification $Spec$ if
  - Every output produced by $Imp$ can also be produced by $Spec$
  - If $Imp$ does not produce any output, so does $Spec$ (quiescence)

Definition (The \textit{ioco} conformance relation)

Let $Spec$ be an IOLTS, $Imp$ be an input enabled IOLTS, and let consider a set of traces $\mathcal{F}$:

$$Imp \ ioco_{\mathcal{F}} \ Spec \equiv \forall \sigma \in \mathcal{F}, \ \text{out}(i_0 \ \text{after} \ \sigma) \subseteq \text{out}(s_0 \ \text{after} \ \sigma)$$
Quiescence

Definition (Quiescence)

A state is quiescent if there is no output or no \( \tau \)-transition.
Symbolic Extensions

Different definitions have been proposed:

- Legall (Transition Systems)
- Frantzen (Transition Systems)
- Gottlieb (Constraint Solving)
- Hierons (Extended FSM)
- ...

They all face similar issues:

- Calculations about guards
- Satisfiability of guards
- Symbolic execution/reachability
- Choosing pertinent data in test cases
- Quiescence
- ...

Julien Schmaltz
Issues when Testing from Symbolic and Timed Specifications
Symbolic Extensions: sioco by Frantzen

Different definitions have been proposed:

- Legall (Transition Systems)
- Frantzen (Transition Systems)
- Gottlieb (Constraint Solving)
- Hierons (Extended FSM)
- ... 

They all face similar issues:

- Calculations about guards
- Satisfiability of guards
- Symbolic execution/reachability
- Choosing pertinent data in test cases
- Quiescence
- ...
Example: Symbolic specification of our supplier

Interaction variables: prod, quant, ref

Location variables: rp, q, r

<table>
<thead>
<tr>
<th>!cancel</th>
</tr>
</thead>
<tbody>
<tr>
<td>!confirm</td>
</tr>
</tbody>
</table>

\[
\begin{align*}
\text{rq} \langle \text{prod}, \text{quant} \rangle \\
\text{rp} := \text{prod}, \ q := \text{quant} \\
\text{loq} \langle \text{ref}, \text{prod}, \text{quant} \rangle \\
[\text{prod} = \text{rp} \land \text{quant} < q] \\
\ r := \text{ref} \\
\text{ord} \langle \text{ref} \rangle \\
[r = \text{ref}] \\
\end{align*}
\]
Example: Symbolic specification of our supplier

Interaction variables: \( \text{prod}, \text{quant}, \text{ref} \)

Location variables: \( \text{rp}, \text{q}, \text{r} \)

Gates

\[
\begin{align*}
\text{!cancel} & \quad \text{!confirm} \\
\text{?rq} & \quad \text{!oq} \\
\text{rp} := \text{prod}, \text{q} := \text{quant} & \\
\text{r} := \text{ref} & \\
\text{[prod} = \text{rp} \land \text{quant} < \text{q]} & \\
\text{[r} = \text{ref}] & \\
\end{align*}
\]
Example: Symbolic specification of our supplier

Interaction variables: \( \text{prod}, \text{quant}, \text{ref} \)

Location variables: \( \text{rp}, \text{q}, \text{r} \)

Updates:

\[
\text{rp} := \text{prod}, \text{q} := \text{quant} \\
\text{r} := \text{ref} \\
\text{ord} \langle \text{ref} \rangle \\
\text{rq} \langle \text{prod}, \text{quant} \rangle \\
\text{oq} \langle \text{ref}, \text{prod}, \text{quant} \rangle \\
\text{cancel} \\
\text{confirm}
\]

\[ [\text{prod} = \text{rp} \land \text{quant} < \text{q}] \]

Julien Schmaltz

Issues when Testing from Symbolic and Timed Specifications
Example: Symbolic specification of our supplier

Interaction variables:
- prod
- quant
- ref

Location variables:
- rp
- q
- r

Keys:
- !cancel
- !confirm

Interaction:
- ?rq⟨prod, quant⟩
- !oq⟨ref, prod, quant⟩

Constraints:
- [prod = rp ∧ quant < q]
- r := ref
- r := ref

Location variables: rp, q, r
Interaction variables: prod, quant, ref
Symbolic Quiescence

Depends on the existence of proper interaction variables to enable transition, which depends on the values of previous interaction variables.

\[
\begin{align*}
?rq\langle prod, quant \rangle \\
\text{rp} := prod, q := quant \\
!oq\langle ref, prod, quant \rangle \\
[prod = rp \land quant < q] \\
r := ref \\
!confirm \\
?ord\langle ref \rangle \\
[r = ref]
\end{align*}
\]
Symbolic Quiescence

Depends on the existence of proper interaction variables to enable transition, which depends on the values of previous interaction variables.

\[
\begin{align*}
?rq\langle prod, 0\rangle \\
r p := prod, q := 0
\end{align*}
\]

\[
\begin{align*}
!q\langle ref, prod, quant\rangle \\
[prod = rp \land quant < q] \\
r := ref
\end{align*}
\]

\[
\begin{align*}
!ord\langle ref\rangle \\
[r = ref]
\end{align*}
\]
Symbolic Quiescence

Depends on the existence of proper interaction variables to enable transition, which depends on the values of previous interaction variables.

\[ \prod = rp \land \text{quant} < 0 \]

\[ \text{unsat. over } \mathbb{N} \]

?rq(\prod, 0)
\[ rp := \prod, q := 0 \]

!cancel

!confirm

\[ \text{ord}(\text{ref}) \]
\[ [r = \text{ref}] \]

\[ \text{confirm}(\text{ref}, \prod, \text{quant}) \]
\[ [\prod = rp \land \text{quant} < 0] \]
\[ r := \text{ref} \]

Julien Schmaltz

Issues when Testing from Symbolic and Timed Specifications
Symbolic Quiescence

Depends on the existence of proper interaction variables to enable transition, which depends on the values of previous interaction variables.

\[
\neg (\exists prod, quant : prod = rp \land quant < q)
\]

\[
\delta \\
\begin{array}{l}
 rp := prod, q := 0 \\
\end{array}
\]

\[
\tau
\]

![Diagram of symbolic quiescence with interaction actions and variables](image)
Variations of \textit{tioco}

Active research domain:

- Bohnenkamp \textit{et al.}, T-TorX (TA)
- Larsen \textit{et al.}, TRON (based on UPPAAL) (TA)
- Krichen \textit{et al.}, TTG (TA)
- Brandon Briones \textit{et al.} (TTS)
- ... 

Common challenges:

- Quiescence
- Practical Implementations
- Timed Automata (\textit{e.g.} urgency)
- ...
Urgency in Timed Automata

According to TA semantics, transitions *must* or *may* be taken. There are two main possibilities to express urgency:

- **Deadlines/Urgency Predicates**
  - Conceptually nicer
  - No timed deadlock
  - Non-convex zones

- **Location invariants**
  - Efficient implementations
  - Less restrictive
  - Potential timed deadlock

- **Issue**
  - Urgency and Quiescence
Urgency in Timed Automata: Examples

“the system \textit{may} output an \(x\) within 5 time units, or no output is ever produced”

“the system \textit{must} output an \(x\) within 5 time units”

“the system \textit{may} output an \(x\) (after 5 time units) at any time, or never produce an output”
Urgency and Quiescence

\( Spec \): possible to delay \(!x\) forever
\( Imp \): never produce an output

Case 1: \( Imp \) is conformed to \( Spec \)
- Theory \textit{rtio\textsubscript{o}c} from Krichen \textit{et al.}
  (extented with quiescence)
- Issue: compatibility with the original \textit{i\textsubscript{o}c}o theory

Case 2: \( Imp \) is not conformed to \( Spec \)
- \( Spec \) and \( Imp \) as LTS, agreement with \textit{i\textsubscript{o}c}o
- Theory \textit{tio\textsubscript{o}c} of Brandan-Briones \textit{et al.}
- Issue: output \textit{must} be produced
Quiescence: Definitions

Definition (Timed Quiescence *a la ioco*)
A state is quiescent iff there is no enabled output or $\tau$-transition, now and in the future.

Definition (Timed Quiescence (T-TorX))
A state is quiescent iff there is no state reachable by $\tau$-steps or by delaying, where a transition with an output label is enabled.
Quiescence: Definitions and their Consequences

Definition (Timed Quiescence a la ioco)

A state is quiescent iff there is no enabled output or \( \tau \)-transition, now and in the future.

Example

\[
\delta \\
[c > 10] \\
!x \\
\leq 10 \\
?b \\
\tau \\
\delta \\
\]
Quiescence: Definitions and their Consequences

**Definition (Timed Quiescence (T-TorX))**

A state is quiescent iff there is no state reachable by $\tau$-steps or by delaying, where a transition with an output label is enabled.

**Example**

\[
\begin{align*}
\delta & \quad [c > 10] & \quad \delta & \quad \delta \\
\delta & \quad \delta & \quad \delta & \quad \delta \\
!x & \quad c \leq 10 & \quad ?b & \quad \tau
\end{align*}
\]
Outline

1. The \textit{ioco} theory and its variations
   - The original \textit{ioco} theory
   - Symbolic \textit{ioco}
   - Timed \textit{ioco}

2. Timed and Symbolic Models
   - Flow between symbolic and timed models
   - Symbolic Timed Automata: Syntax and Semantics
   - Quiescence
Combining Data and Time

- **Timed Automata**
  - Clocks: *continuous* variables
  - Clock constraints
  - Clock invariants

- **Symbolic Transition Systems**
  - *Discrete* variables
    - Interaction variables associated with labels
    - Location variables
  - Symbolic guards
Interaction between time and data: restrictions

We should restrict the following cases:

Interaction between clock and location variables:

\[
!a \ [q \leq \sqrt{c}]
\]

Clocks guarded by interaction variables:

\[
!a \langle i \rangle \ c \leq i
\]

But, we should allow:

Using integer loc. var. in clock guards and invariants:

\[
!a \ c \leq v_1
\]

Storing/Sending time stamps of events:

\[
!a \ v := c
\]
Symbolic Timed Automata: Syntax

\[ g\langle i \rangle \kappa \rho \theta \lambda \]

\[ I \rightarrow I' \]
Symbolic Timed Automata: Syntax

Gate $g$
Interaction Variables $\bar{i}$
Interaction with environment

Ex: $\text{?msg}\langle m, n \rangle$
Symbolic Timed Automata: Syntax

Key $\kappa$
First order formula over interaction and location variables

Ex: $[m == \text{start} \land n == 1]$
Symbolic Timed Automata: Syntax

Update $\rho$
Assign first order terms over inter., loc. and clock variables to loc. variables

Ex: $v_1 := n + v_2$ or $v_1 := n + c$
Symbolic Timed Automata: Syntax

Ex: $v_1 \leq v_2 \rightarrow c \leq v_3, \{c\}$
Symbolic Timed Automata: Semantics

Semantics is given by a Timed Transition System:

- States are triple composed of a location, valuations for the location and clock variables
- Transitions enabled if the clock guard, the key, and the destination invariant are satisfied
- A location must be left if its invariant is not satisfied, time can pass otherwise

Input/Ouput: \( G = G_I \cup G_U \)
- \( G_I \) are input gates,
- \( G_U \) are output gates
The \textit{ioco} theory and its variations

Timed and Symbolic Models

Symbolic Timed Automata: Syntax and Semantics

Quiescence

\begin{verbatim}

\texttt{stioco supplier}

\texttt{r} := \texttt{ref} \[ r = \texttt{ref} \]

\texttt{!cancel} \langle \texttt{ref} \rangle

\texttt{!oq} \langle \texttt{ref}, \texttt{prod}, \texttt{quant} \rangle

[ \texttt{prod} = \texttt{rp} \land \texttt{quant} < \texttt{q} ]

\texttt{r} := \texttt{ref}

[ \texttt{c} < 10 ], \{ \texttt{c} \}

[ \texttt{c} < 1 \}, \{ \texttt{c} \}

\texttt{!confirm} \[ \texttt{c} < 5 \]

\texttt{rp} := \texttt{prod}, \texttt{q} := \texttt{quant}

\{ \texttt{c} \}

\texttt{?rq} \langle \texttt{prod}, \texttt{quant} \rangle

\texttt{?ord} \langle \texttt{ref} \rangle

[ \texttt{r} = \texttt{ref} ]

[ \texttt{c} < 15 ]

\{ \texttt{c} \}
\end{verbatim}

Julien Schmaltz

Issues when Testing from Symbolic and Timed Specifications
Quiescence for STIOA

Two possibilities
- Symbolic quiescence
- “Timed” quiescence

Definition (Quiescence for STIOA)
A system is quiescent if it is symbolic quiescent or timed quiescent.
Quiescence for STIOA: Symbolic Quiescence

Quiescence if keys are unsatisfiable

\[ \neg (\exists prod, quant : prod = rp \land quant < q) \]

\[ \delta \]

\[ \neg \]

[\prod = \text{rp} \land \text{quant} < q]\]

\[ \text{rq}(\text{prod, quant}) \]

\[ \text{rp} := \text{prod}, \text{q} := \text{quant} \]

\{c\}

\[ \text{cancel} \]

\{c\}

\[ [c < 5] \]

\[ \tau \]

\[ [c < 10], \{c\} \]

\[ [c < 15] \]

\{c\}

\[ \text{confirm} \]

\[ \text{rq}(\text{ref, prod, quant}) \]

\[ \text{rq}(\text{ref}) \]

\[ [r = \text{ref}] \]

\[ [c < 15] \]

\{c\}

Julien Schmaltz

Issues when Testing from Symbolic and Timed Specifications
The \textit{ioco} theory and its variations

Timed and Symbolic Models

Flow between symbolic and timed models

Symbolic Timed Automata: Syntax and Semantics

Quiescence

Quiescence for STIOA: Timed Quiescence

Quiescence if keys are unsatisfiable or if clock guards are false
Conclusion

- Identified challenges/issues
  - Urgency
  - Quiescence
  - ...

- Definition for Timed and Symbolic Models
  - Symbolic Timed Input Output Automata

- Future Work
  - Define a testing theory for STIOA
  - Algorithms/Implementation
There are many issues and challenges ... find solutions!
Further Reading