Unfoldings of Networks of Timed Automata

Franck Cassez    Thomas Chatain    Claude Jard
Patricia Bouyer  Serge Haddad     Pierre-Alain Reynier

Rennes, December 3, 2008
Unfoldings [McMillan ’93]

- First defined for Petri nets
- Then extended to other true concurrency models [Esparza, Römer ’99]
- Compact representation of the executions
- Explicit representation of concurrency
- Avoid computation of interleavings
- Model-checking, diagnosis, asynchronous circuits
- Optimization: adequate orders [Esparza, Römer, Vogler ’02]
Timed Automata [Alur, Dill ’94]

- \( \langle L, l_0, \Sigma, X, T, \text{Inv} \rangle \)

- Transitions \( t \overset{\text{def}}{=} \langle l, g, a, R, l' \rangle \), with
  - source: \( l \overset{\text{def}}{=} \alpha(t) \in L \)
  - target: \( l' \overset{\text{def}}{=} \beta(t) \in L \)
  - guard: \( g \overset{\text{def}}{=} \gamma(t) \)
  - label: \( a \overset{\text{def}}{=} \lambda(t) \in \Sigma \)
  - resetted clocks: \( R \overset{\text{def}}{=} \rho(t) \subseteq X \)

```
 l_1
 ◯--------------
 |              |
 |              |
 v              v
 l_2
 ◯--------------
 |              |
 |              |
 v              v
  x \geq 3       x := 0
```

```
 l_1
 ◯--------------
 |              |
 |              |
 v              v
  x \leq 1       d
```

```
 l_2
 ◯--------------
 |              |
 |              |
 v              v
  b
```

Timed Automata: Semantics

State $\langle l, dor, \theta \rangle$

- location: $l \in L$
- current date: $\theta \in \mathbb{R}$
- date of latest reset for every clock: $\forall x \in X \quad dor(x) \leq \theta$

The transition $t$ can occur at date $\theta' \geq \theta$ from state $\langle l, dor, \theta \rangle$, if:

- the invariant of $l$ is satisfied until date $\theta'$:
  $\theta' - dor \models Inv(l)$
- $l = \alpha(t)$
- the guard of $t$ is satisfied at date $\theta'$: $\theta' - dor \models \gamma(t)$
Example of Timed Automaton

date: $\theta = 0$

dor$(x) = 0$

$l_1 \quad x \leq 1$

$l_2 \quad x := 0$

$b \quad x \geq 3$
Example of Timed Automaton

\[ l_1 x \leq 1 \]

\[ l_2 \]

\[ a \]

\[ d \]

\[ x := 0 \]

\[ b \]

\[ x \geq 3 \]

\( (a, 0.7) \)

date: \( \theta = 0.7 \)

dor(\( x \)) = 0
Example of Timed Automaton

\[
\begin{align*}
&l_1 & & x \leq 1 \\
&\text{a} & & d \\
&l_2 & & x := 0 \\
&\text{b} & & x \geq 3
\end{align*}
\]

\[
\text{date: } \theta = 3 \\
\text{dor}(x) = 0
\]

(a, 0.7), (b, 3)
Example of Timed Automaton

\[ \text{date: } \theta = 3.5 \]
\[ \text{dor}(x) = 0 \]

\[(a, 0.7), (b, 3), (b, 3.5)\]
Example of Timed Automaton

\[(a, 0.7), (b, 3), (b, 3.5), (d, 4)\]

date: \(\theta = 4\)

dor(\(x\)) = 4
Example of Timed Automaton

\[ \text{date: } \theta = 5 \]
\[ \text{dor}(x) = 4 \]

\[
\begin{align*}
\text{l}_1 & \quad x \leq 1 \\
\text{l}_2 & \quad x \geq 3 \\
\end{align*}
\]

\[
\text{\textcolor{blue}{(a, 0.7), (b, 3), (b, 3.5), (d, 4), (a, 5)}}
\]
Networks of Timed Automata

- synchronization by shared labels
- local clocks

\[
\begin{align*}
\theta &= 0 \\
dor(x) &= 0 \\
dor(y) &= 0 \\

l_1 \quad &x \leq 1 \\
& a \\
& d \\
& x := 0 \\
l_2 \quad & x \geq 3 \\
& b \\

l_3 \quad & y \leq 2 \\
& c \\
& y := 0 \\
l_4 \quad & y := 0 \\
& d
\end{align*}
\]
Networks of Timed Automata

- synchronization by shared labels
- local clocks

\[ l_1 \quad x \leq 1 \]
\[ l_2 \quad x := 0 \]
\[ l_3 \quad y := 0 \]
\[ l_4 \quad y \leq 2 \]

(a, 0.7)

\[ \theta = 0.7 \]
\[ dor(x) = 0 \]
\[ dor(y) = 0 \]
Networks of Timed Automata

- synchronization by shared labels
- local clocks

\[
\begin{align*}
\theta &= 3 \\
dor(x) &= 0 \\
dor(y) &= 0
\end{align*}
\]

\[
\begin{align*}
&l_1: x \leq 1 \\
&a: x := 0 \\
&\downarrow d \\
&l_2: x \geq 3 \\
&\downarrow b \\
&\downarrow \text{transition}
\end{align*}
\]

\[
\begin{align*}
l_3: & \\
&\downarrow c \\
&y := 0 \\
&\downarrow d \\
l_4: & y \leq 2 \\
&\downarrow y := 0
\end{align*}
\]

\[(a, 0.7), (b, 3)\]
Networks of Timed Automata

- synchronization by shared labels
- local clocks

\( l_1 \): \( x \leq 1 \)
\( l_2 \): \( x \geq 3 \)
\( l_3 \): \( y \leq 2 \)
\( l_4 \): \( y := 0 \)

Date: \( \theta = 4 \)
\( dor(x) = 0 \)
\( dor(y) = 4 \)

\( (a, 0.7), (b, 3), (c, 4) \)
Networks of Timed Automata

- synchronization by shared labels
- local clocks

\( l_1 \)
\( x \leq 1 \)
\( l_2 \)
\( x \geq 3 \)
\( l_3 \)
\( y \leq 2 \)
\( l_4 \)
\( y \geq 0 \)

(a, 0.7), (b, 3), (c, 4), (d, 4)

date: \( \theta = 4 \)
dor(x) = 4
dor(y) = 4
Networks of Timed Automata

- synchronization by shared labels
- local clocks

\( l_1 \)  
\( x \leq 1 \)  
\( a \)  
\( x := 0 \)  
\( l_2 \)  
\( x \geq 3 \)  
\( b \)  

\( l_3 \)  
\( dor(x) = 4 \)  
\( dor(y) = 4 \)  
\( l_4 \)  
\( y := 0 \)  
\( y \leq 2 \)  
\( d \)  
\( y := 0 \)  

\( (a, 0.7), (b, 3), (c, 4), (d, 4), (a, 5) \)
Networks of Timed Automata

- synchronization by shared labels
- local clocks

\[
\begin{align*}
\theta &= 6 \\
dor(x) &= 6 \\
dor(y) &= 6
\end{align*}
\]

\[
\begin{align*}
l_1 &\quad x \leq 1 \\
l_2 &\quad x := 0 \\
l_3 &\quad y := 0 \\
l_4 &\quad y \leq 2
\end{align*}
\]

\[
\begin{align*}
(a, 0.7), (b, 3), (c, 4), (d, 4), (a, 5), (d, 6)
\end{align*}
\]
Networks of Timed Automata

- synchronization by shared labels
- local clocks

\[ \theta = 7 \]
\[ \text{dor}(x) = 6 \]
\[ \text{dor}(y) = 6 \]

\[ x \leq 1 \]
\[ x := 0 \]
\[ x \geq 3 \]

\[ y \leq 2 \]
\[ y := 0 \]

\[ (a, 0.7), (b, 3), (c, 4), (d, 4), (a, 5), (d, 6), (a, 7) \]
Processes of Networks of *Untimed* Automata

![Diagram of Processes](image)
Processes of Networks of *Untimed* Automata

\[ l_1 \rightarrow a \rightarrow l_2 \rightarrow b \rightarrow l_1 \]
\[ l_3 \rightarrow c \rightarrow l_4 \rightarrow d \rightarrow l_3 \]
\[ l_1 \rightarrow a \downarrow \]
\[ l_2 \rightarrow a \rightarrow l_1 \]
\[ l_3 \rightarrow a \rightarrow l_2 \]

\( a \)
Processes of Networks of *Untimed* Automata

\[ l_1 \rightarrow a \rightarrow d \rightarrow l_2 \rightarrow b \]

\[ l_3 \rightarrow c \rightarrow l_4 \rightarrow d \]

\[ l_1 \rightarrow a \rightarrow l_2 \]

\[ l_3 \rightarrow c \rightarrow l_4 \]
Processes of Networks of *Untimed* Automata

\[ \text{Diagram of processes} \]

\[ a, c, d \]
Processes of Networks of *Untimed* Automata

\[ a, c, d, a \]
Processes of Networks of *Untimed* Automata
Unfoldings of Networks of *Untimed* Automata
Processes of NTA

\((a, 0.7), (c, 4), (d, 4), (a, 5)\)

\[l_1 \quad x \leq 1\]
\[l_2 \quad a \quad d \quad x := 0\]
\[l_2 \quad b \quad x \geq 3\]

\[l_3 \quad c \quad y := 0\]
\[l_4 \quad d \quad y := 0\]
\[l_4 \quad y \leq 2\]
Processes of NTA

\[(a, 0.7), (c, 4), (d, 4), (a, 5)\]

Other dates are possible with the same structure
Symbolic Processes of NTA

\((a, \theta_1), (c, \theta_2), (d, \theta_3), (a, \theta_4)\)

Other dates are possible with the same structure → parameters
Symbolic Processes of NTA: Symbolic constraints

- induced by
  - guards
  - invariants
  - causality
- convex union of zones [Ben Salah, Bozga, Maler, '06]
- analog of [Aura, Lilius, '00] for NTA

\[
\begin{align*}
\theta_1 & \leq 1 \\
\theta_3 - \theta_2 & \leq 2 \\
\theta_4 - \theta_3 & \leq 1 \\
\theta_1 & \leq \theta_3 \\
\theta_2 & \leq \theta_3 \\
\theta_3 & \leq \theta_4 \\
\theta_4 - \theta_3 & \leq 2
\end{align*}
\]
Difficulties with Time in Unfoldings

- In untimed nets, feasibility of an event is a local property.
- In NTA, it depends on the context.
- In simple case (no invariants), it is still a local property.
How to simulate a NTA without using clocks, but with as much concurrency as possible?

- Look for local conditions to play a transition.
- Executions must respect the usual semantics.
- Notion of partial state $L$: for each automaton, either $\langle l_i, dor_i, \theta_i \rangle$ or $\bullet$.

\[
\begin{align*}
  dor(x) &= \ ? \\
  dor(y) &= 0 \\
  l_1 \xrightarrow{a} l_2 & \quad x \leq 1 \\
  l_2 \xrightarrow{b} l_3 & \quad b \\
  l_2 \xrightarrow{d} l_4 & \quad x := 0 \\
  l_3 \xrightarrow{c} l_4 & \quad c \\
  l_4 \xrightarrow{d} l_3 & \quad y := 0 \\
  l_4 \xrightarrow{\bullet} l_4 & \quad y \leq 2 \\
  l_4 \xrightarrow{\bullet} l_4 & \quad y := 0 \\
\end{align*}
\]
Concurrent Operational Semantics for NTA

How to simulate a NTA without using clocks, but with as much concurrency as possible?

- Look for local conditions to play a transition.
- Executions must respect the usual semantics.
- Notion of partial state $L$: for each automaton, either $\langle l_i, dor_i, \theta_i \rangle$ or $\bullet$.

\[
dor(x) = 0 \quad \text{dor}(y) = ?
\]

\[
l_1 \xrightarrow{a} x \leq 1 \quad l_3 \xrightarrow{c} y \leq 2
\]

\[
l_2 \xrightarrow{d} x := 0
\]

\[
x \geq 3
\]

\[
l_4 \xrightarrow{d} y := 0
\]
Concurrent Operational Semantics for NTA

How to simulate a NTA without using clocks, but with as much concurrency as possible?

- Look for local conditions to play a transition.
- Executions must respect the usual semantics.
- Notion of partial state $L$: for each automaton, either $\langle l_i, dor_i, \theta_i \rangle$ or $\cdot$.

\[
\begin{align*}
  dor(x) &= 0 \\
  x &\leq 1 \\
  x &:= 0 \\
  b &\rightarrow x \geq 3 \\
  l_1 &\xrightarrow{a} l_2 \\
  l_2 &\xrightarrow{d} l_1 \\
  l_2 &\xrightarrow{c} l_3 \\
  l_3 &\xrightarrow{b} l_2 \\
  l_4 &\xrightarrow{d} l_4 \\
  y &\leq 2 \\
  y &:= 0
\end{align*}
\]
Concurrent Operational Semantics for NTA

How to simulate a NTA without using clocks, but with as much concurrency as possible?

- Look for local conditions to play a transition.
- Executions must respect the usual semantics.
- Notion of partial state $L$: for each automaton, either $\langle l_i, dor_i, \theta_i \rangle$ or $\bullet$.

\[
\begin{align*}
dor(x) &= 0 \\
l_1 &\xrightarrow{a} l_2, x \leq 1 \\
l_2 &\xrightarrow{b} l_1, x \geq 3 \\
l_3 &\xrightarrow{c} l_4, y \leq 2 \\
l_4 &\xrightarrow{d} l_3, y := 0
\end{align*}
\]
To take $t$ at $\theta$ from $L$, we want:

for all context $S$ of $L$, $t$ can occur at $\theta$ from $L \cup S$.

We have:

$t$ can occur at $\theta$ from $L \cup S$

if

\{ the automata concerned by $t$ agree
\}

no invariant in $L \cup S$ expires before $\theta$
Local Conditions to Take Transitions

To take \( t \) at \( \theta \) from \( L \), we want:

for all context \( S \) of \( L \), \( t \) can occur at \( \theta \) from \( L \cup S \).

We have:

\( t \) can occur at \( \theta \) from \( L \cup S \)

if

\[
\begin{cases}
\text{the automata concerned by } t \text{ agree} \\
L \text{ is stable in } S \text{ until } \theta
\end{cases}
\]
Local Stability Condition

Intuition

\[ LSC(L, \theta) \implies \]

for all context \( S \) of \( L \), \( L \) is stable in \( S \) until \( \theta \).

Completeness
Global states are stable until the date where one of their invariants expires.
Several choices to define $LSC(L, \theta)$:

- **trivial choice:** $L$ is a global state.
- **BHR:** $L$ involves all the automata that have invariants.
- **more generic:** $L$ contains enough information to check that no automaton of $L$ may be forced to synchronize earlier than $\theta$ with another automaton.
A proposition for $LSC(L, \theta)$

Definition: $LSC(L, \theta)$ holds iff

$L$ contains enough information to check that no automaton of $L$ may be forced to synchronize earlier than $\theta$ with another automaton:

$$
\begin{align*}
\forall i \in J_L \quad \theta - dor_i \models Inv_i(l_i) \\
\forall t \in \text{Sync} \\
I_t \cap J_L \neq \emptyset & \implies \begin{cases}
I_t \subseteq J_L \\
\forall \exists i \in I_t \cap J_L \quad l_i \neq \alpha_i(t_i) \\
\forall \exists i \in I_t \cap J_L \quad \theta - dor_i \not\models \gamma_i(t_i) \\
\forall \forall i \in I_t \setminus J_L \quad Inv(\alpha_i(t_i)) \equiv \text{true}
\end{cases}
\end{align*}
$$

where

- $I_t$ is the set of automata involved in transition $t$;
- $J_L$ is the set of automata whose state is defined in the partial state $L$. 
Symbolic Unfoldings of NTA

- In symbolic unfoldings: keep track of all the partial state \( L \) (not only the part that participates in \( t \)) → use read arcs.

- Any configuration (process) of the unfolding maps (by removing the read arcs) to a pre-process (i.e. a prefix of a process) of the NTA.

- Use only minimal sets \( L \) to increase concurrency.
Conclusion

- concurrent operational semantics for NTA
- parameterized local stability condition
- solve constraints on the dates of the events
- study of the form of the constraints
  → finite complete prefix of the unfolding
- if there is no urgency, the unfolding is simply the superimposition of the processes