Regular Model Checking without Transducers

Parosh Aziz Abdulla

Giorgio Delzanno

Noomene Ben Henda

Ahmed Rezine
Regular Model Checking without Transducers
This Presentation

- Basic Model
- Transition System
- Safety
- Monotonicity and Approximation
- Algorithm and Results
- Conclusion
This Presentation

· Basic Model
· Transition System
· Safety
· Monotonicity and Approximation
· Algorithm and Results
· Conclusion
Basic Model

Model Transition System Safety Monotonicity & Approximation Algorithm & Results Conclusion
Basic Model

\[
\begin{align*}
\forall & \quad \exists \\
L & \quad R
\end{align*}
\]
Transition Systems
Transitions : Local

[Diagram with colored circles and an arrow indicating transitions]
Transitions : Local

Model Transition System Safety Monotonicity & Approximation Algorithm & Results Conclusion
Transitions: Existential
Transitions : Existential

$\exists_L$
Transitions : Existential
Transitions: Existential
Transitions : Universal
Transitions: Universal
Transitions: Universal
Transitions: Universal
Transitions : Binary Communication
Transitions : Binary Communication
Transitions : Broadcast
Transitions: Broadcast
Examples

• Mutual exclusion algorithms by:
  Burns, Szymanski, Dijkstra ...

• Cache coherence protocols:
  Mesi, Illinois, Futurebus, German, ...
This Presentation

- Basic Model
- Transition System
- Safety
- Monotonicity and Approximation
- Algorithm and Results
- Conclusion
This Presentation

- Basic Model
- Transition System
- Safety
- Monotonicity and Approximation
- Algorithm and Results
- Conclusion
Safety

• Reachability of bad configurations.
Safety

- Reachability of bad configurations.

Critical Section
Safety

- Reachability of bad configurations.
Safety

- Reachability of a bad configuration.

Critical Section

Initial
Safety

- Reachability of a bad configuration.
• Reachability of a bad configuration.
Safety

• Reachability of a bad configuration.
Safety

- Reachability of a bad configuration
  - $\text{Bad} = \text{Upward Closed}$
  - represented by minimal elements
Safety
Safety

Model Transition System Safety Monotonicity & Approximation Algorithm & Results Conclusion
Safety

Model Transition System Safety Monotonicity & Approximation Algorithm & Results Conclusion

This Presentation

- Basic Model
- Transition System
- Safety
- Monotonicity and Approximation
- Algorithm and Results
- Conclusion
This Presentation

- Basic Model
- Transition System
- Safety
- Monotonicity and Approximation
- Algorithm and Results
- Conclusion
Monotonicity

\[ C_3 : \bullet \bullet \bullet \bullet \]

\[ \forall \]

\[ C_1 : \bullet \bullet \bullet \bullet \rightarrow C_2 : \bullet \bullet \bullet \bullet \]
Monotonicity

\[ C_3 : \text{ } C_1 \text{ } \rightarrow C_4 : \text{ } C_2 \]
Monotonicity
Monotonicity

Are Local Transitions Monotonic?

\[ C_1 : \text{\textbullet} \rightarrow \text{\textbullet} \rightarrow C_2 : \text{\textbullet} \]

\[ C_3 : \text{\textbullet} \rightarrow \text{\textbullet} \rightarrow \text{\textbullet} \rightarrow \text{\textbullet} \]
Monotonicity

Are Local Transitions Monotonic?

YES

\[ C_1 : \text{red} \rightarrow \text{blue} \rightarrow \text{green} \rightarrow \text{blue} \]
\[ C_2 : \text{black} \rightarrow \text{blue} \rightarrow \text{green} \rightarrow \text{blue} \]
\[ C_3 : \text{blue} \rightarrow \text{red} \rightarrow \text{green} \rightarrow \text{blue} \]
\[ C_4 : \text{blue} \rightarrow \text{green} \rightarrow \text{black} \rightarrow \text{green} \rightarrow \text{blue} \]
Monotonicity

Are Existential Transitions Monotonic?
Monotonicity

Are Existential Transitions Monotonic?

\[
\exists R \begin{cases} \quad C_3 : & \bullet \quad \bullet \quad \bullet \\ \quad C_1 : & \bullet \quad \bullet \quad \bullet \\
\quad C_2 : & \bullet \quad \bullet \\
\quad C_4 : & \bullet \quad \bullet \quad \bullet \\
\end{cases}
\]

\[
\forall \quad \forall
\]

YES
Are Universal Transitions Monotonic?
Monotonicity

Are Universal Transitions Monotonic?

\[ \forall_R \]

\[ C_2 : \quad C_3 : \quad C_4 : \quad C_1 : \]

\[ \text{NO} \]
Approximation

Downward approximation of Universal Transitions
Approximation

Downward approximation of Universal Transitions
Approximation

Downward approximation of Universal Transitions

$C_1: \forall R \in \mathbb{N} \times \mathbb{N}$
Approximation

Downward approximation of Universal Transitions

∀ R

C₁ : 

C₃ :
Approximation

Downward approximation of Universal Transitions

$\forall_R$
Are Downward Approximations of Universal Transitions Monotonic?
Approximation

Are Downward Approximations of Universal Transitions Monotonic?

YES

∀ₗₐₜ₉₅ₛ : 3ₗₐₜ₉₅₄

∀ₗₐ₅₃ : 1ₗₐ₅₃

∀ₗₐ₉₃ : 2ₗₐ₉₃

∀ₗₐ₉₄ : 4ₗₐ₉₄
This Presentation

- Basic Model
- Transition System
- Safety
- Monotonicity and Approximation
- Algorithm and Results
- Conclusion
This Presentation

- Basic Model
- Transition System
- Safety
- Monotonicity and Approximation
- Algorithm and Results
- Conclusion
Algorithm
Algorithm

Finite !!

Pre

Finite !!
Algorithm

\[\preceq\]

Model Transition System Safety Monotonicity & Approximation Algorithm & Results Conclusion
Algorithm
Algorithm
Algorithm
Algorithm
Algorithm

\[ Model\ Transition\ System\ Safety\ Monotonicity&Approximation\ Algorithm&Results\ Conclusion \]
Algorithm
Algorithm

Well Quasi Ordering:

“For each infinite sequence $a_0, a_1, \ldots$ there exists $i < j$ such that $a_i \leq a_j$”
Well Quasi Ordering:

“No infinite sequence of upward closed”
Algorithm
## Results

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>#iter</th>
<th>#constr</th>
<th>T (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bakery</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Bakery*</td>
<td>2</td>
<td>2</td>
<td>4</td>
</tr>
<tr>
<td>Burns</td>
<td>14</td>
<td>71</td>
<td>230</td>
</tr>
<tr>
<td>Burns*</td>
<td>9</td>
<td>21</td>
<td>32</td>
</tr>
<tr>
<td>Java M-lock</td>
<td>5</td>
<td>24</td>
<td>30</td>
</tr>
<tr>
<td>Java M-lock*</td>
<td>5</td>
<td>17</td>
<td>30</td>
</tr>
<tr>
<td>Dijkstra</td>
<td>13</td>
<td>150</td>
<td>1700</td>
</tr>
<tr>
<td>Dijkstra*</td>
<td>8</td>
<td>57</td>
<td>168</td>
</tr>
<tr>
<td>Szymanski</td>
<td>17</td>
<td>334</td>
<td>3880</td>
</tr>
<tr>
<td>Szymanski*</td>
<td>17</td>
<td>334</td>
<td>4080</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>#iter</th>
<th>#constr</th>
<th>t (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Synapse</td>
<td>3</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>Berkley</td>
<td>2</td>
<td>6</td>
<td>8</td>
</tr>
<tr>
<td>Mesi</td>
<td>3</td>
<td>8</td>
<td>8</td>
</tr>
<tr>
<td>Moeisi</td>
<td>1</td>
<td>12</td>
<td>12</td>
</tr>
<tr>
<td>Dec Firefly</td>
<td>3</td>
<td>11</td>
<td>16</td>
</tr>
<tr>
<td>Xerox P.D</td>
<td>3</td>
<td>20</td>
<td>52</td>
</tr>
<tr>
<td>Illinois</td>
<td>5</td>
<td>33</td>
<td>80</td>
</tr>
<tr>
<td>Futurebus</td>
<td>7</td>
<td>153</td>
<td>300</td>
</tr>
<tr>
<td>German</td>
<td>44</td>
<td>14475</td>
<td>3h45mn</td>
</tr>
</tbody>
</table>

### Mutual Exclusion Algorithms

### Cache Coherence Protocols
Conclusion

- A framework which can handle, e.g.
  - mutual exclusion and
  - cache coherence.
- Better performance than specialized tools
- Some of the examples are verified for the first time completely automatically (German, Java-Metalock)
- Can be extended to systems where the processes operate on unbounded variables (paper at CAV 2007)
- Simpler machinery compared to regular model checking (no transducers)
- Ongoing extensions to trees, graphs ...