Quantified Bounded Model Checking for Rectangular Hybrid Automata

Luan Nguyen1, Djordje Maksimovic2, Taylor T. Johnson1, Andreas Veneris2
1University of Texas at Arlington, Arlington, TX USA, 2University of Toronto, Ontario, Canada

Overview

- QBMC: a quantified bounded model checking (BMC) for Rectangular Hybrid Automata (RHA)
  - encodes the BMC problem for RHA in a quantified form
  - performs QBMC by querying the Z3 SMT solver via its Python API and uses its quantifier-handling procedures [1]
  - implemented as a module within HyST [2]

Illustrative Example

$x := 3$
start
x ≥ 2.5

| Bad States: $P = V_i(x) \quad (\text{Loc}_1 = \text{Loc}_2 \rightarrow x \geq 2.5)$ |
|---|---|---|---|
| $a_1 = 0, b_1 = 1, a_2 = 0, b_2 = 2$ |

<table>
<thead>
<tr>
<th>Tools</th>
<th>$k \leq 4$</th>
<th>$k \leq 8$</th>
<th>$k \leq 16$</th>
</tr>
</thead>
<tbody>
<tr>
<td>QBMC</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$9^2$</td>
<td>3.7</td>
<td>52.2</td>
<td>5.1</td>
</tr>
<tr>
<td>$9^3$</td>
<td>15.5</td>
<td>65.6</td>
<td>31.3</td>
</tr>
<tr>
<td>$9^4$</td>
<td>256.1</td>
<td>702.8</td>
<td>1062.1</td>
</tr>
<tr>
<td>HyComp</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$9^2$</td>
<td>0.8</td>
<td>121.9</td>
<td>1.33</td>
</tr>
<tr>
<td>$9^3$</td>
<td>2.7</td>
<td>307.9</td>
<td>12.81</td>
</tr>
<tr>
<td>$9^4$</td>
<td>63.9</td>
<td>2655.4</td>
<td>N/A</td>
</tr>
</tbody>
</table>

Fischer mutual exclusion protocol
Discrete locations: $4^N$
Discrete state-spaces: $(N + 1)(4N)^N$

Lynch-Shavit mutual exclusion protocol
Discrete locations: $9^N$
Discrete state-spaces: $(N + 1)(9N)^N$

Algorithm

Quantified free BMC for Hybrid Automata

$\Phi(k) \triangleq I(V_0) \land \bigwedge_{i=0}^{k-1} T_i(V, V') \land (V_{i+1}^k = P(V_i))$

$\Omega(k) \triangleq \exists V_0, V_1, ..., V_k, \forall t \quad \exists V' \mid I(V_0) \land T(V, V') \land \bigwedge_{i=1}^{k-1} t_{i+1} \rightarrow (V = V_i) \land (V' = V_{i+1}) \land (V_{i+1}^k = P(V_i))$

$\delta$: the real time elapse in the trajectories

$t = \{t_1, t_2, ..., t_{10 \times g \times k}\}$: index each iteration of the BMC of hybrid automata $H$

QBMC examples are available online at: [http://www.verivital.com/hyst/cfv2015.zip](http://www.verivital.com/hyst/cfv2015.zip)

Conclusion

- present a new SMT-based verification technique that encodes the BMC problem for RHA in a quantified form, which also subsumes this encoding for timed automata
- present preliminary experimental results included such as Fischer and Lynch-Shavit mutual exclusion, and compare to dReach and HyComp
- In future, we will investigate more general classes of hybrid automata

References