May and Must Abstractions for Markov Decision Processes
Anvesh Komuravelli, David Henriques, Fei He and Edmund Clarke

Methodology

Safety and Liveness
\[ \psi \equiv \neg \varphi \lor (X\varphi) \lor (XW\varphi) \]
\[ \psi' \equiv \varphi \land (X\varphi') \lor (XW\varphi') \]

Simulation
MDP \( M \) simulates \( H \) if there is \( \mathcal{R} \subseteq S \times S' \) s.t.
- \( s' \in \mathcal{R}(s) \) \( \iff \) \( s \in \mathcal{R}(s') \)
- \( \mu(s') = \mu_\mathcal{R}(s) \) \( \forall s \)

Preservation Theorem
Let \( \mathcal{M} \) simulate \( H \). If \( \mathcal{M} \models \varphi \) then \( \mathcal{M} \models \varphi \).
If \( \mathcal{M} \not\models \varphi \), then \( \mathcal{M} \not\models \varphi \).

May Abstractions
Consider a partition \( \mathcal{P} \) of \( S \).
- states of the abstraction are elements of \( \mathcal{P} \)
- for each transition in \( \mathcal{M} \), its lifting is in \( \mathcal{M} \)

Must Abstractions
Consider a partition \( \mathcal{P} \) of \( S \).
- states of the abstraction are elements of \( \mathcal{P} \)
- transitions in the abstraction are the common parts of liftings of distributions among concrete states in each partition class

Abstraction Refinement Loop
1. Initial partition is the trivial partition \( \mathcal{P} \).
2. If \( \text{May-ref} \) return true;
3. If \( \neg(\text{Must-ref}) \) return false;
4. Pick a refinement method;
5. Refine \( \mathcal{P} \) according to 4;
6. Goto 2;
This is guaranteed to stop because eventually the partition becomes the diagonal relation.

Results

<table>
<thead>
<tr>
<th>Model</th>
<th>Property</th>
<th>Concrete Model (# states)</th>
<th>Game-based (# states)</th>
<th>May/Must (if May/Must states)</th>
<th>Game-based (s)</th>
<th>May/Must (s)</th>
<th>Game-based (f lters)</th>
<th>May/Must (f lters)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zeroconf</td>
<td>Reachability</td>
<td>1065569</td>
<td>966</td>
<td>1808</td>
<td>525</td>
<td>3391</td>
<td>127</td>
<td>245</td>
</tr>
<tr>
<td>Zeroconf</td>
<td>Safety</td>
<td>26121</td>
<td>-</td>
<td>940</td>
<td>-</td>
<td>50</td>
<td>-</td>
<td>205</td>
</tr>
<tr>
<td>Wlan</td>
<td>Reachability</td>
<td>28480</td>
<td>258</td>
<td>525</td>
<td>5.5</td>
<td>7</td>
<td>70</td>
<td>179</td>
</tr>
<tr>
<td>GridWorld</td>
<td>Nested Safety</td>
<td>10201</td>
<td>-</td>
<td>431</td>
<td>-</td>
<td>13</td>
<td>-</td>
<td>86</td>
</tr>
<tr>
<td>Non-det GridWorld</td>
<td>Nested Safety</td>
<td>15555</td>
<td>-</td>
<td>2011</td>
<td>-</td>
<td>1518</td>
<td>-</td>
<td>434</td>
</tr>
</tbody>
</table>

References