Improving Live Sequence Chart to Automata Translation for Verification

Rahul Kumar & Eric Mercer
GT-VMT 2008, Budapest, Hungary
Specifications

- Bulky
- Hard to write
- Even harder to read
- Extracting correctness properties...

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Pages in Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>114</td>
</tr>
<tr>
<td>TCP</td>
<td>91</td>
</tr>
<tr>
<td>BVCI</td>
<td>60</td>
</tr>
<tr>
<td>SSH</td>
<td>38</td>
</tr>
</tbody>
</table>
Alternative: Live Sequence Charts

- Intuitive
- Formal semantics
- Inter-process behavior
- Other:
  - Interaction diagrams
  - Message Sequence Chart
  - Timing Diagrams
  - Sequence Diagrams

_Damm et. al., Brill et. al., R.I.TU-T. 120_
Example

BVCI protocol
60 pages

One Page Specification!

Bunker et. al.

SMC Lab, Brigham Young University, USA
How do we use them?

How should we do this?

Specification  System
How do we use them?

Stage I
- Specification
- Temporal Logic
- Automata for verification

Stage II
- Verification tool
- System

Result: Is System = Specification?
Live Sequence Charts

Instances/Processes
Synchronous Messages
Asynchronous Messages
Locations
Conditions
Prechart
Main chart
Temperatures
Coregions
Simultaneous regions
Previous Translation to Automata

Klose et. al.
Transformation Algorithm

- Process each state of automaton using depth first traversal
- For each state:
  - Create deterministic transition relation
  - Create total transition relation
- Proof of correctness included in paper

True (first and safety state only) for detecting all errors.

Self-loop for non-progress.

To safety state.

To successor states (progress).
Automata Transformation
Testing

- Test on symbolic model checking using NuSMV
  - Compare to previous automata approach (Klose et. al., Toben et. al.)
- Test using SPIN
  - Compare to past LSC to LTL approach (Kumar et. al.)
- Highly concurrent specification (a worst case)
  - $A_{cxm}$: Chart contains $c$ co-region with $m$ messages in each co-region
- Use puzzle solving models with messages
## Results: NuSMV

<table>
<thead>
<tr>
<th>Specification</th>
<th>Traditional Verification</th>
<th>Improved Verification</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Reachability</td>
<td>ACTL</td>
</tr>
<tr>
<td></td>
<td>States</td>
<td>Time</td>
</tr>
<tr>
<td>A3x5</td>
<td>1.02e06</td>
<td>34</td>
</tr>
<tr>
<td>A3x6</td>
<td>1.02e06</td>
<td>237</td>
</tr>
<tr>
<td>A3x7</td>
<td>879048</td>
<td>1568</td>
</tr>
</tbody>
</table>

*Time in seconds.*

2x faster!!
## Results: SPIN

<table>
<thead>
<tr>
<th>Specification</th>
<th>Model</th>
<th>Without Errors</th>
<th>With Errors</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>States</td>
<td>Memory</td>
</tr>
<tr>
<td>A7x6</td>
<td>soko</td>
<td>97500</td>
<td>17.2</td>
</tr>
<tr>
<td></td>
<td>plain</td>
<td>406</td>
<td>7.4</td>
</tr>
<tr>
<td>A8x6</td>
<td>soko</td>
<td>97500</td>
<td>18.5</td>
</tr>
<tr>
<td></td>
<td>plain</td>
<td>406</td>
<td>8.7</td>
</tr>
<tr>
<td>A9x6</td>
<td>soko</td>
<td>97500</td>
<td>20.1</td>
</tr>
<tr>
<td></td>
<td>plain</td>
<td>406</td>
<td>10.3</td>
</tr>
</tbody>
</table>

*Memory in MB, Time in seconds.*

### 5x bigger specifications!!
Conclusions

- New translation provides an automata
  - Better suited for verification
  - Performance improved
  - Eliminates need for special tools and algorithms
  - Does have to deal with standard synchronous composition

- Future work:
  - Extend translation to additional constructs of LSCs
  - Extend translation to knowledge based logics
  - Provide a tool for LSC to automata development
Questions?

Rahul Kumar (rahul@cs.byu.edu)

Eric Mercer (egm@cs.byu.edu)

Software Model Checking Laboratory
3325 TMCB
Brigham Young University
Provo, UT 84606
USA
Trends
Software Testing Today

1. Specification
2. Test Cases
3. System Implementation
4. Run Tests
5. Bug Fixes
Formal Verification

Requirements → Specification → Verification tool → Result: Is System = Specification?

System → Model → Iterate