Symmetry Reduction and Heuristic Search for Error Detection in Model Checking

Workshop on Model Checking and Artificial Intelligence
10. August 2003

Alberto Lluch Lafuente? - Tilman Mehler?
lafuente@informatik.uni-freiburg.de

Institut für Informatik, Albert-Ludwigs-Universität Freiburg, Germany
Introduction

- Model checking as debugging tool.
- Counterexamples are used to fix errors.
- Main Drawbacks:
  - State Explosion Problem.
  - Long counterexamples difficult to understand.
- Heuristic search can:
  - Accelerate search for errors.
  - Obtain short counterexamples.
- Heuristic search successful only if combined with other techniques: partial order reduction, symmetry reduction.
Model Checking Framework

- Asynchronous concurrent system.
- $n$ identical processes $P_0..P_n$.
- System’s state space: LTS $T = \langle S, s_0, \rightarrow, L \rangle$
  - $S$: set of states
  - $s_0 \in S$ is the initial state
  - $\rightarrow \subseteq S \times S$: transition relation
  - $L : S \rightarrow 2^{AP}$ labeling function.
- Verification of safety property.
- Bug finding phase: errors are common
- Explicit-state model checking.
Symmetry Reduction

- Symmetries can be exploited to reduce the state space.
- Some properties are invariant under the symmetry.
- System remains behaviorally equivalent under symmetry permutations.
- Types of symmetries: rotational, full, mirror, etc.
- Detecting symmetries is difficult.
- Practical approaches: symmetric data types with restricted operations.
- Our assumption: correct symmetry is given.
Definitions

- Symmetry relation \( \sim \) on \( S \).
- \( s_1, s_2 \in S \) symmetric iff \( s_1 \sim s_2 \).
- \( s_1 \rightarrow s'_1, s_2 \rightarrow s'_2 \) are symmetric iff \( s_1 \sim s_2 \) and \( s'_1 \sim s'_2 \).
- \( AP \) invariant under \( \sim \) iff \( s_1, \sim s_2 \sim L(s_1) = L(s_2) \).
- \( T_{/\sim} = \langle S_{/\sim}, [s_0], \Rightarrow, L_{/\sim} \rangle \)
  - \([s]\): orbit or equivalence class of \( s \).
  - \([s_1] \Rightarrow [s'_1]\) if \( s_2 \rightarrow s'_2 \in \Rightarrow \) such that \( s_2 \in [s_1] \) and \( s'_2 \in [s'_1] \).
- If \( AP \) invariant under \( \sim \), \( L_{/\sim}([s]) = L(s') \) for some \( s' \in [s] \).
Orbit Problem

- $T_{\sim}$ analyzed by exploring a *representative* part of $T$.
- Orbit problem: $s \sim s'$?
- Use representative states for $[s]: \text{rep} : S \rightarrow S$.
- $\text{rep}$ canonical if $s \sim s' \in S \Leftrightarrow \text{rep}(s) = \text{rep}(s')$.
  - Lead to optimal reductions.
  - Computation can be time-expensive.
- Non unique representatives: normalizing functions
  - Lead to sub-optimal reductions.
  - Less computation time.
Reachability and Bisimulation Equivalence

- A symmetry relation $\sim$ preserves reachability:
  - if $s_1 \sim s'_1$ and $s_1 \sim s_2$ and $\exists s'_2 \mid s'_2 \sim s'_1$ then $s_2 \sim s'_2$.
  - $s_1 \sim s'_1$ and $s_2 \sim s'_2$ are symmetric paths.

- A bisimulation relation $\sim$ preserves safety properties:
  - If $s_1 \sim s'_1$ error path then every symmetric path is error path.
  - Safety verification reduced to reachability.
  - If $e$ error state, then every state in $[e]$ is error state.
Heuristic Search in Model Checking

- Safety error detection reduced to reachability.
- Drawbacks: long counterexamples, large exploration.
- Alternative: Heuristic search.
- LTS as (weighted) state transition graph.
- Heuristics guide the search to:
  - Accelerate the search.
  - Provide minimal counterexamples.
- Our approach:
  1. Best-First to find an error quickly.
  2. A* to find minimal counterexample.
From system state $s = (pc_0, \ldots, pc_n, v_0, \ldots)$ to system state $s' = (pc'_0, \ldots, pc'_n, v'_0, \ldots)$ each $P_i$ must progress from $pc_i$ to $pc'_i$. 

$M = P_1 | \cdots | P_n$
FSM Distance Heuristic (2)

- The minimal number of system transitions from $s$ to $s'$ is less or equal to the sum of the minimal distances from $pc_i$ to $pc'_i$ in each $P_i$.
- FSM Distance is a lower bound to the distance to $s'$.
- A* is able to deliver the minimal path to $s'$.
- FSM distance is computed in $O(n)$.
  - Pre-computing the distances in $P_i$ in $O(|P_i|^3)$.
  - In practice: $|P_i| << |M|$, since $|M|$ is $O(|P_1| \cdot \ldots \cdot |P_n|)$. 
Symmetry reduction and Heuristic Search

- Algorithm: straightforward combination.
- Symmetric paths have the same length.
- Symmetric paths have the same cost if symmetric transitions have the same cost.
- Heuristic $h$ is symmetric if $s \sim s' \rightarrow h(s) = h(s')$.
- Experiments with Best-first search
  - Combination better than one technique in isolation.
  - Symmetry reduction depends on kind of permutation.
  - Heuristic reduction depends on heuristic accuracy.
Searching for an orbit

Problem: find minimal path to error state $e$.

“$e$ never reached” not always invariant under $\sim$, but

$e$ violates $f$ and $f$ invariant under $\sim$.

“[$e$] never reached” invariant under $\sim$.

Find minimal path to $e =$

Find minimal path to [$e$]: $s_0 \sim e', e' \in [e]$.

Obtain symmetric path $s_0 \sim e$.

How to check $[s] = [e]$?

rep canonical: $[s] = [e]$ iff $\text{rep}(s) = \text{rep}(e)$

rep normalizing: store $[e]$ and make query.
Distance to an orbit (1)

- \( F D^e \) lower bound for the distance to \( e \) in \( T \).
- \( F D^e \) **not** lower bound for the distance to \([e]\) in \( T/\sim\).

Minimal (symmetric) paths from:
- \( s' \) to \( e \) \( \equiv [s]to[e] \)
- \( s \) to \( e' \) \( \equiv [s]to[e] \)

Minimal (symmetric) paths from:
- \( s \) to \( e \)
- \( s' \) to \( e' \)
Distance to an orbit (2)

- Given $h^e$ that estimates distance from $s$ to $e$ in $T$.
- $h_{/\sim}^{[e]}(s) = \min_{e' \in [e]} \{ h^{e'}(s) \}$.
- If $h^e$ is admissible, then $h_{/\sim}^{[e]}$ is admissible.
- If $h^e$ is monotone, then $h_{/\sim}^{[e]}$ is monotone.
- Time complexity of $h_{/\sim}^{[e]} = T(h^e) \times [e]$.
  - With rotational pid symmetries $|[e]|$ is $O(n)$ :)
  - With full pid symmetries $|[e]|$ is $O(n!)$ :(
Implementations of $FD^{[e]}_\sim$

- Alternative 1
  - Store states of $[e]$ with distinct pid permutations in table $\{e\}$
  - Time complexity $O(n \times |\{e\}|)$.
  - $|\{e\}|$ is 1 if not pid permutations applied.

- Alternative 2 (current work)
  - Reduce to Minimum Weight Assignment Problem.
  - Time complexity $O(n^3)$.

- Alternative 2 better if $O(||[e]||) > n^2$
## Experiments: Rotational

### Leader election

<table>
<thead>
<tr>
<th></th>
<th>n</th>
<th>8</th>
<th>9</th>
<th>10</th>
</tr>
</thead>
<tbody>
<tr>
<td>$FD^e$</td>
<td>states</td>
<td>2,106</td>
<td>2,641</td>
<td>3,117</td>
</tr>
<tr>
<td></td>
<td>time</td>
<td>1.6</td>
<td>2.5</td>
<td>3.6</td>
</tr>
<tr>
<td>$FD^{[e]}_{/\sim}$</td>
<td>s</td>
<td>2,106</td>
<td>2,641</td>
<td>3,117</td>
</tr>
<tr>
<td></td>
<td>time(l1)</td>
<td>1.6</td>
<td>2.5</td>
<td>3.6</td>
</tr>
<tr>
<td></td>
<td>time(l2)</td>
<td>2.7</td>
<td>4.4</td>
<td>6.5</td>
</tr>
<tr>
<td>BFS</td>
<td>states</td>
<td>188,514</td>
<td>632,389</td>
<td>o.m.</td>
</tr>
<tr>
<td></td>
<td>time</td>
<td>9:38.7</td>
<td>43:46</td>
<td>o.m.</td>
</tr>
<tr>
<td>ADFS</td>
<td>states</td>
<td>o.m.</td>
<td>o.m.</td>
<td>o.m.</td>
</tr>
<tr>
<td></td>
<td>time</td>
<td>o.m.</td>
<td>o.m.</td>
<td>o.m.</td>
</tr>
</tbody>
</table>
### Experiments: Peterson

<table>
<thead>
<tr>
<th></th>
<th>n=6</th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>n</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>$FD^e$</td>
<td>states</td>
<td>6,292</td>
<td>34,268</td>
<td>241,370</td>
</tr>
<tr>
<td></td>
<td>time</td>
<td>2.8</td>
<td>22.7</td>
<td>8:07</td>
</tr>
<tr>
<td>$FD_{/\sim}^{[e]}$</td>
<td>states</td>
<td>5,134</td>
<td>39,885</td>
<td>455,634</td>
</tr>
<tr>
<td></td>
<td>time(I1)</td>
<td>4.5</td>
<td>49.8</td>
<td>50:52</td>
</tr>
<tr>
<td></td>
<td>time(I2)</td>
<td>4.67</td>
<td>1:0.1</td>
<td>30:20</td>
</tr>
</tbody>
</table>

For $n=6$:

<table>
<thead>
<tr>
<th></th>
<th>$FD^e$</th>
<th>$FD_{/\sim}^{[e]}$</th>
<th>$FD_{/\sim}^{[e]}$</th>
</tr>
</thead>
<tbody>
<tr>
<td>average time</td>
<td>$4.170e^{-6}$</td>
<td>$1.322e^{-3}$</td>
<td>$2.432e^{-4}$</td>
</tr>
</tbody>
</table>

Symmetry Reduction and Heuristic Search for Error Detection in Model Checking – p.17/?
## Experiments: Database

<table>
<thead>
<tr>
<th></th>
<th>n</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>FD$^e$</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>states</td>
<td></td>
<td>190</td>
<td>689</td>
<td>1,225</td>
</tr>
<tr>
<td>time</td>
<td></td>
<td>0.4</td>
<td>7.9</td>
<td>1:48</td>
</tr>
<tr>
<td><strong>FD$^{[\varepsilon]}_{/\sim}$</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s</td>
<td></td>
<td>343</td>
<td>499</td>
<td>1,524</td>
</tr>
<tr>
<td>time(I1)</td>
<td></td>
<td>0.7</td>
<td>7.4</td>
<td>2:44</td>
</tr>
<tr>
<td>time(I2)</td>
<td></td>
<td>1.0</td>
<td>8.4</td>
<td>2:59</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th><strong>FD$^e$</strong></th>
<th><strong>FD$^{[\varepsilon]}_{1/\sim}$</strong></th>
<th><strong>FD$^{[\varepsilon]}_{2/\sim}$</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Database (n=8)</td>
<td>$2.514e^{-6}$</td>
<td>$2.580e^{-4}$</td>
<td>$5.242e^{-4}$</td>
</tr>
</tbody>
</table>
### Experiments: Database (non cyclic)

<table>
<thead>
<tr>
<th></th>
<th>$n=6$</th>
<th>$n=7$</th>
<th>$n=8$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$FD^e$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>states</td>
<td>398</td>
<td>391</td>
<td>1,978</td>
</tr>
<tr>
<td>time</td>
<td>1.4</td>
<td>9.5</td>
<td>6:47</td>
</tr>
<tr>
<td>$FD^{[e]}_\sim$</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>s</td>
<td>38</td>
<td>48</td>
<td>59</td>
</tr>
<tr>
<td>time(l1)</td>
<td>0.2</td>
<td>1.3</td>
<td>12.1</td>
</tr>
<tr>
<td>time(l2)</td>
<td>0.3</td>
<td>1.5</td>
<td>12.5</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>$FD^e$</th>
<th>$FD^{[e]}_1\sim$</th>
<th>$FD^{[e]}_2\sim$</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database ($n=8$)</td>
<td>$2.514e^{-6}$</td>
<td>$2.580e^{-4}$</td>
<td>$5.242e^{-4}$</td>
</tr>
</tbody>
</table>
Symmetry reduction and Heuristic search compatible.
- Orthogonal combination.

Finding minimal counterexample is important.
- More efficient with canonical representatives.
- Admissible heuristic $F D^{[e]}_{\sim}$: two implementations.
- Heuristic search outperforms blind search

Current and Future Work: Experiments with Partial Order Reduction, Heuristic Search and Abstraction.