Verifying Programs on Relaxed Memory Models  
with focus on x86-TSO  
Alexander Linden  
Institut Montefiore, Université de Liège, Belgium

The problem

Ensuring that concurrent programs remain correct when moved to multi-core processors implementing relaxed memory models (x86-TSO).

Fig: x86-TSO model

The approach: state space exploration and memory fence insertion

Start with a program that is correct (with respect to a safety property) under SC (the standard memory model).

Verify that the safety property still holds when the program is moved to a relaxed memory model and correct it as needed.

Procedure:
1. Explore the state space of the program, modelling the store buffers.
2. When violations of safety properties are found:
   - detect a problematic relaxation;
   - avoid it by inserting a memory fence into the program;
   - repeat this procedure until the safety property is satisfied.

The features of the approach

- allows the verification of cyclic programs by modelling the store buffers by automata.

Example: Unbounded buffer content (x,1)(y,1)(x,1)(y,1) ... (x,1)(y,1) is represented by the finite automaton

\[ (x,1) \rightarrow (y,1) \rightarrow (x,1) \]

- limits the size of the state space by using partial-order reduction techniques (POR):
  - persistent sets,
  - sleep sets.

The results

A verification tool that
- can handle cyclic programs,
- is compatible with POR,
- produces a correct program.

Future work:
- extend to other memory models,
- optimize use of POR.

Experiments:

<table>
<thead>
<tr>
<th>Mutual Exclusion</th>
<th>Algorithms</th>
<th>without err. correction</th>
<th>with error correction</th>
</tr>
</thead>
<tbody>
<tr>
<td>Program</td>
<td>entry</td>
<td>#P</td>
<td>#St</td>
</tr>
<tr>
<td>Dekker</td>
<td>single</td>
<td>2</td>
<td>118</td>
</tr>
<tr>
<td>Dekker</td>
<td>repeated</td>
<td>2</td>
<td>5468</td>
</tr>
<tr>
<td>Peterson</td>
<td>single</td>
<td>2</td>
<td>108</td>
</tr>
<tr>
<td>Peterson</td>
<td>repeated</td>
<td>2</td>
<td>400</td>
</tr>
<tr>
<td>Gen. Pet.</td>
<td>single</td>
<td>3</td>
<td>15476</td>
</tr>
<tr>
<td>Bakery</td>
<td>single</td>
<td>2</td>
<td>775</td>
</tr>
</tbody>
</table>

http://www.montefiore.ulg.ac.be  
linden@montefiore.ulg.ac.be