Improved On-The-Fly Livelock Detection with $\text{DFS}_{\text{FIFO}}$

Alfons Laarman

Joint with David Faragó
(Karlsruhe Institute of Technology)

May 14th, 2013

NFM, Moffett Field, CA, USA
Dealing with State Space Explosion

Problem
State Explosion in LTL Model Checking

Viable solutions:

- Parallelization
- Partial-Order/Confluence Reduction
- Specialization on subclasses of LTL (Livelocks, Weak LTL)
1. Introduction

2. LTL

3. Parallelism

4. Partial-Order Reduction

5. DFS\textsubscript{FIFO}

6. Conclusion
LTL Model Checking

\[ M : \]

\[ TS : \]

\[ \{\} \]

\[ \{} \]

\[ \{\} \]

\[ \{a\} \]
LTL Model Checking

\[ M \models \varphi \]

LTL formula, e.g.:

\[ \varphi = \Box (a \Rightarrow \Diamond b) \]

\[ M : \]

\[ TS : \]

\[ \{\} \rightarrow \{\} \]

\[ \{\} \rightarrow \{\} \]

\[ \{a\} \rightarrow \{\} \]
LTL Model Checking

\[ \mathcal{M} \models \varphi \iff \mathcal{L} (\mathcal{T} S) \subseteq \mathcal{L} (A\varphi) \]

LTL formula, e.g.:

\[ \varphi = \Box (a \Rightarrow \Diamond b) \]

\[ A\varphi \text{ (Büchi): } \neg a, b \]
LTL Model Checking

\( \mathcal{M} \models \varphi \)

\( \mathcal{L}(\mathcal{T}S) \subseteq \mathcal{L}(A\varphi) \)

\( \mathcal{L}(\mathcal{T}S) \cap \mathcal{L}(A\neg\varphi) = \emptyset \)

LTL formula, e.g.:

\( \varphi = \Box(a \Rightarrow \Diamond b) \)

\( A\varphi \) (Büchi):

\( \neg a, b \)
LTL Model Checking

\[ \mathcal{M} \models \varphi \]
\[ \L(\mathcal{T}S) \subseteq \L(A_\varphi) \]
\[ \L(\mathcal{T}S) \cap \L(A_{\neg \varphi}) = \emptyset \]
\[ \mathcal{T}S \otimes A_{\neg \varphi} \]
contains no accepting cycle

LTL formula, e.g.:
\[ \varphi = \square(a \Rightarrow \Diamond b) \]

A_\varphi (Büchi):
\[ \neg a, b \]

TS:

\[ \begin{align*}
\{\} & \rightarrow \{\} \\
\{\} & \rightarrow \{\} \\
\{\} & \rightarrow \{a\} \\
\end{align*} \]
LTL Model Checking

\[ M \models \varphi \]

\[ L(TS) \subseteq L(A_\varphi) \]

\[ L(TS) \cap L(A_{\neg \varphi}) = \emptyset \]

\[ TS \otimes A_{\neg \varphi} \]

contains no accepting cycle

LTL formula, e.g.:

\[ \varphi = \Box(a \Rightarrow \Diamond b) \]

\[ A_\varphi \text{ (Büchi)} : \]

\[ \neg a, b \]
**LTL Model Checking**

\[ \mathcal{M} \models \varphi \]

\[ \mathcal{L}(TS) \subseteq \mathcal{L}(A\varphi) \]

\[ \mathcal{L}(TS) \cap \mathcal{L}(A\neg\varphi) = \emptyset \]

\[ TS \otimes A\neg\varphi \]

contains no accepting cycle

**LTL formula, e.g.:**

\[ \varphi = \Box(a \Rightarrow \Diamond b) \]

\[ A\varphi \text{ (Büchi):} \]

\[ \neg a, b \]

\[ 2^{2C} \times 2^{2^{|AP|}} \]
Nested Depth-First Search

Algorithm

- Two DFS searches
- Linear \((2N)\) in size of the cross product
- DFS order (hard to parallelize)
Simple idea: \textit{P independent, randomized} NDFS instances (swarm)
\textit{Store states in lockless hash/tree table [FMCAD 2010/SPIN 2011]}

- More on the fly (bug hunting)
- No speedup for full verification
CNDFS for Parallel LTL Model Checking

Simple idea: \( P \) independent, randomized NDFS instances (swarm)
Store states in lockless hash/tree table [FMCAD 2010/SPIN 2011]

+ More on the fly (bug hunting)
— No speedup for full verification

Better idea: Store information in graph to prune work:
Multi-core NDFS \( \rightarrow \) CNDFS [ATVA 2011/2012]
Simple idea: *P independent, randomized* NDFS instances (swarm)
Store states in lockless hash/tree table [FMCAD 2010/SPIN 2011]

+ More on the fly (bug hunting)
— No speedup for full verification

Better idea: Store information in graph to prune work:
Multi-core NDFS → CNDFS [ATVA 2011/2012]
Simple idea: \( P \) independent, randomized NDFS instances (swarm).
Store states in lockless hash/tree table [FMCAD 2010/SPIN 2011]

+ More on the fly (bug hunting)

— No speedup for full verification

Better idea: Store information in graph to prune work:
Multi-core NDFS \( \rightarrow \) CNDFS [ATVA 2011/2012]

Worst case complexity: \( N \times P \), but in practice close to \( N \)
LTL property: □◊ progress

<table>
<thead>
<tr>
<th></th>
<th>SPIN NDFS</th>
<th>LTSmin CNDFS</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1 core</td>
<td>48 cores</td>
</tr>
<tr>
<td>leaderₜ</td>
<td>1390</td>
<td>926</td>
</tr>
<tr>
<td>garp</td>
<td>2050</td>
<td>1061</td>
</tr>
<tr>
<td>i-prot</td>
<td>103</td>
<td>76</td>
</tr>
</tbody>
</table>
LTL property: □◊progress

<table>
<thead>
<tr>
<th></th>
<th>SPIN</th>
<th>LTSmin</th>
<th>CNDFS</th>
</tr>
</thead>
<tbody>
<tr>
<td>leaderₜ</td>
<td>1390</td>
<td>926</td>
<td>51</td>
</tr>
<tr>
<td>garp</td>
<td>2050</td>
<td>1061</td>
<td>59</td>
</tr>
<tr>
<td>i-prot</td>
<td>103</td>
<td>76</td>
<td>4</td>
</tr>
</tbody>
</table>
Partial-Order Reduction

TS :
Partial-Order Reduction

\[ \mathcal{T}S: \]

\[ \text{deadlock} \]

\[ \mathcal{T}S: \]
Partial-Order Reduction

\[ \mathcal{T}S : \]

\[ \mathcal{T}S : \]

\[ \mathcal{T}S : \]

\[ \mathcal{T}S : \]

\[ \text{deadlock} \]

\[ +\text{cycle} \]
Partial-Order Reduction

$\mathcal{T}S$:

deadlock

$\downarrow$ +cycle

$\mathcal{T}S$:

+visibility

$\mathcal{T}S$:

$\mathcal{T}S$:
Partial-Order Reduction for (C)NDFS

- stack proviso for NDFS
Partial-Order Reduction for (C)NDFS

- stack proviso for NDFS
- CNDFS has incomplete stacks \(\Rightarrow\) No POR
Partial-Order Reduction for (C)NDFS

- Stack proviso for NDFS
- CNDFS has incomplete stacks $\Rightarrow$ No POR

Other solutions to solve the problem of parallelism & POR: OWCTY + Topological Sort Proviso [Barnat et al. 2010]
Specializing on Livelock Detection

Livlock LTL property: □◊P

Livlocks are important properties, they are used for:

- $\frac{1}{3}$ of all the BEEM models
- $\frac{1}{2}$ of the models in the Promela Database
  (http://www.albertolluch.com/research/promelamodels)
Specializing on Livelock Detection

Livlock LTL property: $\Box \Diamond P$

Livlocks are important properties, they are used for:

- $\frac{1}{3}$ of all the BEEM models
- $\frac{1}{2}$ of the models in the Promela Database
  (http://www.albertolluch.com/research/promelamodels)
- Progress detection DFS [Holzmann et al. 1996]
- $\text{DFS}_{\text{FIFO}}$ with Partial-Order Reduction [Farago et al. 2009]
Livelock LTL property: $\square\Diamond P$

Livelocks are important properties, they are used for:

- $\frac{1}{3}$ of all the BEEM models
- $\frac{1}{2}$ of the models in the Promela Database
  ([http://www.albertolluch.com/research/promelamodels](http://www.albertolluch.com/research/promelamodels))
- Progress detection DFS [Holzmann et al. 1996]
- $\text{DFS}_{\text{FIFO}}$ with Partial-Order Reduction [Farago et al. 2009]
DFS_FIFO for Livelock Detection
DFS\textsubscript{FIFO} for Livelock Detection

DFS

BFS

DFS

BFS
DFS_FIFO for Livelock Detection

DFS FIFO for Livelock Detection
Improved On-The-Fly Livelock Detection with DFS_{FIFO}

May 14th, 2013
Expected outcome:

- $\text{DFS}_{\text{FIFO}}$ makes single pass over state space (unlike NDFS)
- $|T|S| \leq \frac{1}{2} |C|$

Up to 4 times as fast as NDFS
Expected outcome:

- $\text{DFS}_{\text{FIFO}}$ makes single pass over state space (unlike NDFS)
- $|TS| \leq \frac{1}{2}|C|$

Up to 4 times as fast as NDFS

<table>
<thead>
<tr>
<th></th>
<th>LTSmin (sec)</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>$\text{DFS}_{\text{FIFO}}$</td>
<td>NDFS</td>
</tr>
<tr>
<td>garp</td>
<td>591.2</td>
<td>969.2</td>
</tr>
<tr>
<td>i-prot</td>
<td>41.4</td>
<td>70.6</td>
</tr>
<tr>
<td>leader$_t$</td>
<td>233.2</td>
<td>753.6</td>
</tr>
</tbody>
</table>
Cycle proviso

- progress cycle $\Rightarrow$ visibility proviso
- non-progress cycle $\Rightarrow$ report counter example

No additional stack proviso required!
DFS_FIFO and Partial-Order Reduction

Cycle proviso

- progress cycle ⇒ visibility proviso
- non-progress cycle ⇒ report counter example

No additional stack proviso required!

<table>
<thead>
<tr>
<th>Model</th>
<th>States</th>
<th>LTSmin (POR)</th>
<th>SPIN (POR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>DFS_FIFO</td>
<td>NDFS</td>
<td>NDFS</td>
</tr>
<tr>
<td>garg</td>
<td>72,318,749</td>
<td>2.2%</td>
<td>32.6%</td>
</tr>
<tr>
<td>i-protocol</td>
<td>20,052,267</td>
<td>31.8%</td>
<td>32.0%</td>
</tr>
<tr>
<td>leaderₜ</td>
<td>89,771,572</td>
<td>0.5%</td>
<td>0.5%</td>
</tr>
</tbody>
</table>
Cycle proviso

- progress cycle $\Rightarrow$ visibility proviso
- non-progress cycle $\Rightarrow$ report counter example

No additional stack proviso required!

<table>
<thead>
<tr>
<th>Model</th>
<th>States</th>
<th>LTSmin (POR)</th>
<th>SPIN (POR)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>DFS\textsubscript{FIFO}</td>
<td>NDFS</td>
</tr>
<tr>
<td>garp</td>
<td>72,318,749</td>
<td>2.2%</td>
<td>32.6%</td>
</tr>
<tr>
<td>i-protocol</td>
<td>20,052,267</td>
<td>31.8%</td>
<td>32.0%</td>
</tr>
<tr>
<td>leader\textsubscript{t}</td>
<td>89,771,572</td>
<td>0.5%</td>
<td>0.5%</td>
</tr>
</tbody>
</table>

LTSmin uses the stubborn set method [SPIN 2013]
Parallel DFS\textsubscript{FIFO}
Parallel DFS\textsubscript{FIFO}
Parallel DFS\textsubscript{FIFO} Experiments

**cndfs**
- garp
- giop2.nomig
- i-protocol2
- leader5

**dfs fifo**
- garp
- giop2.nomig
- i-protocol2
- leader5
Parallel \text{DFS}_{\text{FIFO}} \text{ Experiments}

\text{No cycle proviso} \Rightarrow \text{Parallelism + POR!}
Parallel LTL with Partial Order Reduction

\( \text{DFS}_{\text{FIFO}} \) vs OWCTY & Topological Sort Proviso
[Baranat et al 2010]
Parallel LTL with Partial Order Reduction

**DFS\textsubscript{FIFO} vs OWCTY & Topological Sort Proviso**

[Barnat et al 2010]

| N | Alg.   | $|\mathcal{R}|$ | $|\mathcal{T}|$ | $T_1$  | $T_{48}$ | $U$  | $|\mathcal{R}_{\text{por}}|$ | $|\mathcal{T}_{\text{por}}|$ | $T_{1_{\text{por}}}$ | $T_{48_{\text{por}}}$ | $U_{\text{por}}$ |
|---|-------|----------|----------|--------|---------|------|----------------|----------------|----------------|----------------|----------------|
| 9 | cndfs | 3.6E7    | 2.3E8    | 502.6  | 12.0    | 41.8 | 27.9%         | 0.1%           | 211.8          | n/a            | n/a            |
| 9 | pdfs\textsubscript{fifo} | 3.6E7    | 2.3E8    | 583.6  | 14.3    | 40.8 | 1.5%          | 0.0%           | 12.9           | 3.6            | 3.5            |
| 9 | owcty | 3.6E7    | 2.3E8    | 498.7  | 51.9    | 9.6  | 12.6%         | 0.0%           | 578.4          | 35.7           | 16.2           |
| 10 | cndfs | 2.4E8    | 1.7E9    | 30'    | 90.7    | 30'  | 19.3%         | 5.4%           | 1102.7         | n/a            | n/a            |
| 10 | pdfs\textsubscript{fifo} | 2.4E8    | 1.7E9    | 30'    | 109.3   | 30'  | 0.7%          | 0.1%           | 35.0           | 2.5            | 14.0           |
| 10 | owcty | 2.4E8    | 1.7E9    | 30'    | 663.1   | 30'  | 8.7%          | 2.2%           | 156.3          | 30'            | 30'            |
| 11 | pdfs\textsubscript{fifo} | 30'      | 30'      | 30'    | 30'     | 30'  | 5.1E6         | 7.1E6          | 109.8          | 5.3            | 20.7           |
| 11 | owcty | 30'      | 30'      | 30'    | 30'     | 30'  | 9.3E7         | 1.7E8          | 1036.5         | 30'            | 30'            |
| 12 | pdfs\textsubscript{fifo} | 30'      | 30'      | 30'    | 30'     | 30'  | 1.6E7         | 2.2E7          | 369.1          | 11.2           | 33.0           |
| 13 | pdfs\textsubscript{fifo} | 30'      | 30'      | 30'    | 30'     | 30'  | 6.6E7         | 9.2E7          | 1640.5         | 38.1           | 43.0           |
| 14 | pdfs\textsubscript{fifo} | 30'      | 30'      | 30'    | 30'     | 30'  | 2.0E8         | 2.9E8          | 120.3          | 30'            | 30'            |
| 15 | pdfs\textsubscript{fifo} | 30'      | 30'      | 30'    | 30'     | 30'  | 8.4E8         | 1.2E9          | 527.5          | 30'            | 30'            |
Conclusions

By specializing for livelocks with $\text{DFS}_{\text{FIFO}}$, we

- improved partial-order reduction
- improved the efficiency of parallelization by 100%
- allow efficient combination of POR and parallelism
Conclusions

By specializing for livelocks with DFS\textsubscript{FIFO}, we

- improved partial-order reduction
- improved the efficiency of parallelization by 100%
- allow efficient combination of POR and parallelism

Future work

- use testers to support more LTL properties [Valmari CAV ’93]
Conclusions

By specializing for livelocks with $\text{DFS}_{\text{FIFO}}$, we

- improved partial-order reduction
- improved the efficiency of parallelization by 100%
- allow efficient combination of POR and parallelism

Future work

- use testers to support more LTL properties [Valmari CAV ’93]

Other mentioned works

1. Boosting Multi-Core Reachability Performance with Shared Hash Tables – FMCAD’10
2. Parallel Recursive State Compression for Free – SPIN’11
3. Multi-Core Nested Depth-First Search – ATVA’11
4. Improved Multi-Core Nested Depth-First Search – ATVA’12
5. SpinS: Extending LTSmin with Promela through SpinJa – PDMC’12