Local State Space Construction for Compositional Verification of Concurrent Systems

Hao Zheng

Department of Computer Science and Engineering
University of South Florida
Introduction

- **Scope**: model checking of finite state concurrent systems.
  - Asynchronous.
  - Communication via *shared variables*.
  - Applications: communication protocols, multi-thread programs,
Introduction

- Scope: model checking of finite state concurrent systems.
  - Asynchronous.
  - Communication via *shared variables*.
  - Applications: communication protocols, multi-thread programs,
- To present a local state space construction approach.
  - As a key part of a methodology for scalable model checking of finite state concurrent systems.
  - To addressing state explosion due to the interleavings of concurrent executions.
  - For local safety verification.
  - To helping partial order reduction to be more effective in global state space.
Overview of the Methodology

Parallel composition of communicating processes

\[ M_1 \parallel \ldots \parallel M_n \models \varphi \]
Overview of the Methodology

Parallel composition of communicating processes

\[ M_1 \parallel \ldots \parallel M_n \models \varphi \]

\[
\text{Local State Space} \\
\text{Construction & Verification}
\]
Overview of the Methodology

Parallel composition of communicating processes

\[ M_1 \parallel \ldots \parallel M_n \models \varphi \]

Local State Space
Construction & Verification

Local state transition models

\[ G_1, \ldots, G_n \]

Is \( \varphi \) verified?

Terminate

Yes

Behavioral Analysis
Transition Dependence Relation

Global State Space Search
with Partial Order Reduction
Overview of the Methodology

Parallel composition of communicating processes

\[ M_1 \parallel \ldots \parallel M_n \models \varphi \]

Local State Space Construction & Verification

Local state transition models

\[ G_1, \ldots, G_n \]

Is \( \varphi \) verified?
Overview of the Methodology

Parallel composition of communicating processes

\[ M_1 \parallel \ldots \parallel M_n \models \varphi \]

Local State Space Construction & Verification

Local state transition models

\[ G_1, \ldots, G_n \]

Is \( \varphi \) verified?

Terminate

Yes
Overview of the Methodology

Parallel composition of communicating processes

\[ M_1 \parallel \ldots \parallel M_n \models \varphi \]

Local State Space Construction & Verification

Local state transition models

\[ G_1, \ldots, G_n \]

Is \( \varphi \) verified?

Yes

Terminate

No

Behavioral Analysis

Transition Dependence Relation

Global State Space Search with Partial Order Reduction
Overview of the Methodology

Parallel composition of communicating processes

\[ M_1 \parallel \ldots \parallel M_n \models \varphi \]

Local State Space Construction & Verification

Local state transition models

\[ G_1, \ldots, G_n \]

Terminate

Is \( \varphi \) verified?

Behavioral Analysis

Transition Dependence Relation

Global State Space Search with Partial Order Reduction
Outline

• Background
• Local state space construction: previous work
  • The thread-modular approach
• Local state space construction: an improvement
  • Synchronized local state space search
• Experimental results
• Discussions and conclusions
Background
$M_1 = (V_1, q_0, A_1)$;

$V_1 = \{l_1, x, z\}$;
$q_0 = (l_1 = 0, x = 0, z = 0)$;
$A_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$;

where

$\alpha_1 = (l_1 = 0 \land x > 0,\n z := x + 1; l_1 := 1)$;
$\alpha_2 = (l_1 = 1,\n x := 0; l_1 := 2)$;
$\alpha_3 = (l_1 = 2 \land x > 0,\n z := z \ast x; l_1 := 3)$;
$\alpha_4 = (l_1 = 3,\n x := 0; z := 0; l_1 := 0)$;

$M_2 = (V_2, p_0, A_2)$;

$V_2 = \{l_2, x, y\}$;
$p_0 = (l_2 = 0, x = 0, y = 0)$;
$A_2 = \{\beta_1, \beta_2\}$;

where

$\beta_1 = (l_2 = 0 \land y = 0, \n x := 2; l_2 := 1)$;
$\beta_2 = (l_2 = 1 \land x = 0, \n y := 1; l_2 := 0)$

$M_3 = (V_3, s_0, A_3)$;

$V_3 = \{l_3, x, y\}$;
$s_0 = (l_3 = 0, x = 0, y = 0)$;
$A_3 = \{\gamma_1, \gamma_2\}$;

where

$\gamma_1 = (l_3 = 0 \land y = 1, \n x := 3; l_3 := 1)$;
$\gamma_2 = (l_3 = 1 \land x = 0, \n y := 0; l_3 := 0)$
Processes

\[
M_1 = (V_1, q_0, A_1);
\]

\[
V_1 = \{l_1, x, z\};
\]

\[
q_0 = (l_1 = 0, x = 0, z = 0);
\]

\[
A_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\};
\]

where

\[
\alpha_1 = (l_1 = 0 \land x > 0, z := x + 1; l_1 := 1);
\]

\[
\alpha_2 = (l_1 = 1, x := 0; l_1 := 2);
\]

\[
\alpha_3 = (l_1 = 2 \land x > 0, z := z * x; l_1 := 3);
\]

\[
\alpha_4 = (l_1 = 3, x := 0; z := 0; l_1 := 0);
\]

\[
M_2 = (V_2, p_0, A_2);
\]

\[
V_2 = \{l_2, x, y\};
\]

\[
p_0 = (l_2 = 0, x = 0, y = 0);
\]

\[
A_2 = \{\beta_1, \beta_2\};
\]

where

\[
\beta_1 = (l_2 = 0 \land y = 0, x := 2; l_2 := 1);
\]

\[
\beta_2 = (l_2 = 1 \land x = 0, y := 1; l_2 := 0);
\]

\[
M_3 = (V_3, s_0, A_3);
\]

\[
V_3 = \{l_3, x, y\};
\]

\[
s_0 = (l_3 = 0, x = 0, y = 0);
\]

\[
A_3 = \{\gamma_1, \gamma_2\};
\]

where

\[
\gamma_1 = (l_3 = 0 \land y = 1, x := 3; l_3 := 1);
\]

\[
\gamma_2 = (l_3 = 1 \land x = 0, y := 0; l_3 := 0);
\]
**High Level Description: A Simple Example**

\( M_1 = (V_1, q_0, A_1); \)

\( V_1 = \{l_1, x, z\}; \)
\( q_0 = (l_1 = 0, x = 0, z = 0); \)
\( A_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}; \)

where

\( \alpha_1 = (l_1 = 0 \land x > 0, \quad z := x + 1; l_1 := 1); \)
\( \alpha_2 = (l_1 = 1, \quad x := 0; l_1 := 2); \)
\( \alpha_3 = (l_1 = 2 \land x > 0, \quad z := z \ast x; l_1 := 3); \)
\( \alpha_4 = (l_1 = 3, \quad x := 0; z := 0; l_1 := 0); \)

\[ M_2 = (V_2, p_0, A_2); \]
\[ V_2 = \{l_2, x, y\}; \]
\[ p_0 = (l_2 = 0, x = 0, y = 0); \]
\[ A_2 = \{\beta_1, \beta_2\}; \]

where

\( \beta_1 = (l_2 = 0 \land y = 0, \quad x := 2; l_2 := 1); \)
\( \beta_2 = (l_2 = 1 \land x = 0, \quad y := 1; l_2 := 0) \)

\[ M_3 = (V_3, s_0, A_3); \]
\[ V_3 = \{l_3, x, y\}; \]
\[ s_0 = (l_3 = 0, x = 0, y = 0); \]
\[ A_3 = \{\gamma_1, \gamma_2\}; \]

where

\( \gamma_1 = (l_3 = 0 \land y = 1, \quad x := 3; l_3 := 1); \)
\( \gamma_2 = (l_3 = 1 \land x = 0, \quad y := 0; l_3 := 0) \)
High Level Description: A Simple Example

\[ M_1 = (V_1, q_0, A_1); \]
\[ V_1 = \{l_1, x, z\}; \]
\[ q_0 = (l_1 = 0, x = 0, z = 0); \]
\[ A_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}; \]

where

\[ \alpha_1 = (l_1 = 0 \land x > 0, \]
\[ z := x + 1; l_1 := 1); \]
\[ \alpha_2 = (l_1 = 1, \]
\[ x := 0; l_1 := 2); \]
\[ \alpha_3 = (l_1 = 2 \land x > 0, \]
\[ z := z \cdot x; l_1 := 3); \]
\[ \alpha_4 = (l_1 = 3, \]
\[ x := 0; z := 0; l_1 := 0); \]
\[ M_2 = (V_2, p_0, A_2); \]
\[ V_2 = \{l_2, x, y\}; \]
\[ p_0 = (l_2 = 0, x = 0, y = 0); \]
\[ A_2 = \{\beta_1, \beta_2\}; \]

where

\[ \beta_1 = (l_2 = 0 \land y = 0, \]
\[ x := 2; l_2 := 1); \]
\[ \beta_2 = (l_2 = 1 \land x = 0, \]
\[ y := 1; l_2 := 0) \]
\[ M_3 = (V_3, s_0, A_3); \]
\[ V_3 = \{l_3, x, y\}; \]
\[ s_0 = (l_3 = 0, x = 0, y = 0); \]
\[ A_3 = \{\gamma_1, \gamma_2\}; \]

where

\[ \gamma_1 = (l_3 = 0 \land y = 1, \]
\[ x := 3; l_3 := 1); \]
\[ \gamma_2 = (l_3 = 1 \land x = 0, \]
\[ y := 0; l_3 := 0) \]
High Level Description: A Simple Example

\[ M_1 = (V_1, q_0, A_1); \]
\[ V_1 = \{l_1, x, z\}; \]
\[ q_0 = (l_1 = 0, x = 0, z = 0); \]
\[ A_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}; \]
where
\[ \alpha_1 = (l_1 = 0 \land x > 0, \]
\[ z := x + 1; l_1 := 1); \]
\[ \alpha_2 = (l_1 = 1, \]
\[ x := 0; l_1 := 2); \]
\[ \alpha_3 = (l_1 = 2 \land x > 0, \]
\[ z := z \ast x; l_1 := 3); \]
\[ \alpha_4 = (l_1 = 3, \]
\[ x := 0; z := 0; l_1 := 0); \]

\[ M_2 = (V_2, p_0, A_2); \]
\[ V_2 = \{l_2, x, y\}; \]
\[ p_0 = (l_2 = 0, x = 0, y = 0); \]
\[ A_2 = \{\beta_1, \beta_2\}; \]
where
\[ \beta_1 = (l_2 = 0 \land y = 0, \]
\[ x := 2; l_2 := 1); \]
\[ \beta_2 = (l_2 = 1 \land x = 0, \]
\[ y := 1; l_2 := 0) \]

\[ M_3 = (V_3, s_0, A_3); \]
\[ V_3 = \{l_3, x, y\}; \]
\[ s_0 = (l_3 = 0, x = 0, y = 0); \]
\[ A_3 = \{\gamma_1, \gamma_2\}; \]
where
\[ \gamma_1 = (l_3 = 0 \land y = 1, \]
\[ x := 3; l_3 := 1); \]
\[ \gamma_2 = (l_3 = 1 \land x = 0, \]
\[ y := 0; l_3 := 0) \]
$M_1 = (V_1, q_0, A_1)$;  

$V_1 = \{l_1, x, z\}$;  
$q_0 = (l_1 = 0, x = 0, z = 0)$;  
$A_1 = \{\alpha_1, \alpha_2, \alpha_3, \alpha_4\}$;  

where  
  
$\alpha_1 = (l_1 = 0 \land x > 0, \\
z := x + 1; l_1 := 1)$;  
$\alpha_2 = (l_1 = 1, \\
x := 0; l_1 := 2)$;  
$\alpha_3 = (l_1 = 2 \land x > 0, \\
z := z \ast x; l_1 := 3)$;  
$\alpha_4 = (l_1 = 3, \\
x := 0; z := 0; l_1 := 0)$;  

\[ M_2 = (V_2, p_0, A_2); \]
\[ V_2 = \{l_2, x, y\}; \]
\[ p_0 = (l_2 = 0, x = 0, y = 0); \]
\[ A_2 = \{\beta_1, \beta_2\}; \]

where  
  
$\beta_1 = (l_2 = 0 \land y = 0, \\
x := 2; l_2 := 1)$;  
$\beta_2 = (l_2 = 1 \land x = 0, \\
y := 1; l_2 := 0)$  

\[ M_3 = (V_3, s_0, A_3); \]
\[ V_3 = \{l_3, x, y\}; \]
\[ s_0 = (l_3 = 0, x = 0, y = 0); \]
\[ A_3 = \{\gamma_1, \gamma_2\}; \]

where  
  
$\gamma_1 = (l_3 = 0 \land y = 1, \\
x := 3; l_3 := 1)$;  
$\gamma_2 = (l_3 = 1 \land x = 0, \\
y := 0; l_3 := 0)$
State Graphs

$G_1$

$q_0 \xrightarrow{\alpha_1} q_1 \xrightarrow{\alpha_2} q_2 \xrightarrow{\alpha_3} q_3 \xrightarrow{\alpha_4} q_4 \xrightarrow{\alpha_1} q_5$

$G_2$

$p_0 \xrightarrow{\alpha_2} p_1 \xrightarrow{\alpha_2} p_2 \xrightarrow{\alpha_4} p_3 \xrightarrow{\gamma_1} p_4 \xrightarrow{\gamma_2} p_5$

$G_3$

$s_0 \xrightarrow{\alpha_2} s_1 \xrightarrow{\alpha_2} s_2 \xrightarrow{\alpha_4} s_3 \xrightarrow{\gamma_1} s_4 \xrightarrow{\gamma_2} s_5$
State Graphs

Local transitions

Local State Space Construction for Compositional Verification of Concurrent Systems

H. Zheng (CSE USF)
State Graphs

\[ G_1 \]

\( q_0 \)
\( \beta_1 \)
\( q_1 \)
\( \alpha_1 \)
\( q_2 \)
\( \alpha_2 \)
\( q_3 \)
\( \gamma_1 \)
\( q_4 \)
\( \alpha_3 \)
\( q_5 \)

\[ G_2 \]

\( p_0 \)
\( \beta_1 \)
\( p_1 \)
\( \alpha_2 \)
\( p_2 \)
\( \beta_2 \)
\( p_3 \)
\( \gamma_1 \)
\( p_4 \)
\( \alpha_4 \)
\( p_5 \)

\[ G_3 \]

\( s_0 \)
\( \beta_1 \)
\( s_1 \)
\( \alpha_2 \)
\( s_2 \)
\( \beta_2 \)
\( s_3 \)
\( \gamma_1 \)
\( s_4 \)
\( \alpha_4 \)
\( s_5 \)

External transitions

H. Zheng (CSE USF)
Local State Space Construction for Composi
Local State Graph Construction

The Thread Modular Model Checking Approach

Parallel composition of communicating processes

\[ M_1 \parallel \ldots \parallel M_n \models \varphi \]

Local State Space Construction & Verification

Local state graphs

\[ G_1, \ldots, G_n \]
Thread Modular Model Checking (TMMC)

- Each process is verified locally with a derived environment capturing all possible interactions with its neighbors.
- For each process, its environment is derived from the guarantees of its neighbors.
- The guarantee of a process $P$ is a set of state transitions on the shared variables resulting from executions of process $P$.

∀ Process $P_i$, fix its env. $E_i = \emptyset$

∀ Process $P_i$, compute its guarantee $g_i$ wrt $E_i$

∃ $g_i$ st $g_i$ is extended? No → Terminate.

Yes

∀ Process $P_i$, update its env. $E_i = \bigcup_{i \neq j} g_j$
TMMC: Illustration

\[ G_1 \ [l_1, x, z] \]
\[ G_2 \ [l_2, x, y] \]
\[ G_3 \ [l_3, x, y] \]

0, 0, 0

0, 0, 0

0, 0, 0
TMMCC: Illustration

\[
G_1 \ [l_1, x, z] \\
0, 0, 0
\]

\[
G_2 \ [l_2, x, y] \\
0, 0, 0 \\
\beta_1 \\
1, 2, 0
\]

\[
G_3 \ [l_3, x, y] \\
0, 0, 0
\]
TMMC: Illustration

\[ G_1 \ [l_1, x, z] \]

\[ G_2 \ [l_2, x, y] \]

\[ G_3 \ [l_3, x, y] \]
TMMCC: Illustration

\[ G_1 \left[ l_1, x, z \right] \]

\[ G_2 \left[ l_2, x, y \right] \]

\[ G_3 \left[ l_3, x, y \right] \]
TMMCC: Illustration

$G_1 [l_1, x, z]$

$G_2 [l_2, x, y]$

$G_3 [l_3, x, y]$
TMMC: Weakness

\( G_1 \) \([l_1, x, z]\)

\( G_2 \) \([l_2, x, y]\)

\( G_3 \) \([l_3, x, y]\)

\( G_1 \) [\( l_1, x, z \)]

\( G_2 \) [\( l_2, x, y \)]

\( G_3 \) [\( l_3, x, y \)]
Improved Local State Graph Construction

The Synchronized Local State Space Search Approach

Parallel composition of communicating processes

\[ M_1 \parallel \ldots \parallel M_n \models \varphi \]

Local State Space Construction & Verification

Local state graphs

\[ G_1, \ldots, G_n \]
Local State Space Search ($LS^3$)

- Construct local state graphs by searching joint state space of communicating processes.
  - Extend the local SGs resulting from interactions among processes.
  - Avoiding adding external transitions in wrong states.

**Algorithm**

∀ Process $P_i$, initialize $G_i$ with $init_i$

∀ Processes $P_i$ and $P_j$, search their joint state space $G_{ij}$

Extend $G_i$ and $G_j$ wrt $G_{ij}$

∃ Process $P_i$ st $G_i$ extended with new transitions?

No

Terminate.
Local State Space Construction for Compositional Verification of Concurrent Systems

$LS^3$: Illustration

localSearch()

$G_1$

$G_2$

$G_3$

$M_1, M_2$

$q_0$

$p_0$

$s_0$
$LS^3$: Illustration

localSearch()

$M_1, M_2$

$q_0, p_0$

$q_1, p_1$

$q_2, p_1$

$q_3, p_2$

$q_3, p_3$

$G_1$

$q_0$

$G_2$

$p_0$

$G_3$

$s_0$
$LS^3$: Illustration

localSearch()

$M_1, M_2$

$q_0, p_0$

$q_1, p_1$

$q_2, p_1$

$q_3, p_2$

$q_3, p_3$

$G_1$

$q_0$

$q_1$

$q_2$

$q_3$

$G_2$

$p_0$

$p_1$

$p_2$

$p_3$

$G_3$

$s_0$
Local Search

\[ \text{localSearch()} \]

\[ M_2, M_3 \]
$LS^3$: Illustration

localSearch()

$M_2, M_3$

$p_0, s_0$

$p_1, s_1$

$G_1$

$q_0$

$q_1$

$q_2$

$q_3$

$G_2$

$p_0$

$p_1$

$p_2$

$p_3$

$G_3$

$s_0$
$LS^3$: Illustration

localSearch()

$M_2, M_3$

$p_0, s_0$

$p_1, s_1$

$G_1$

$q_0$

$q_1$

$q_2$

$q_3$

$G_2$

$p_0$

$p_1$

$p_2$

$p_3$

$G_3$

$s_0$

$s_1$
$LS^3$: Illustration

localSearch()

$M_1, M_3$

$G_1$

$q_0$

$q_1$

$q_2$

$q_3$

$G_2$

$p_0$

$p_1$

$p_2$

$p_3$

$G_3$

$s_0$

$s_1$
Illustration

\( localSearch() \)

\( M_1, M_3 \)

\( q_0, s_0 \)

\( q_1, s_1 \)

\( q_2, s_1 \)

\( q_3, s_2 \)

\( G_1 \)

\( q_0 \)

\( q_1 \)

\( q_2 \)

\( q_3 \)

\( G_2 \)

\( p_0 \)

\( p_1 \)

\( p_2 \)

\( p_3 \)

\( G_3 \)

\( s_0 \)

\( s_1 \)
**$LS^3$: Illustration**

```
localSearch()

$M_1, M_3$

$q_0, s_0$

$q_1, s_1$

$q_2, s_1$

$q_3, s_2$

$G_1$

$q_0$

$q_1$

$q_2$

$q_3$

$G_2$

$p_0$

$p_1$

$p_2$

$p_3$

$G_3$

$s_0$

$s_1$

$s_2$
```
$LS^3$: Illustration: Final Results

$G_1$

- $q_0$ with transitions $\beta_1$ to $q_1$
- $q_1$ with transition $\alpha_1$ to $q_2$
- $q_2$ with transition $\alpha_2$ to $q_3$
- $q_3$ with transition $\gamma_1$ to $q_4$
- $q_4$ with transition $\alpha_3$ to $q_5$

$G_2$

- $q_0$ with transition $\beta_1$ to $p_1$
- $p_1$ with transition $\alpha_2$ to $p_2$
- $p_2$ with transition $\beta_2$ to $p_3$
- $p_3$ with transition $\gamma_1$ to $p_4$
- $p_4$ with transition $\alpha_4$ to $p_5$

$G_3$

- $s_0$ with transition $\beta_1$ to $s_1$
- $s_1$ with transition $\alpha_2$ to $s_2$
- $s_2$ with transition $\beta_2$ to $s_3$
- $s_3$ with transition $\gamma_1$ to $s_4$
- $s_4$ with transition $\alpha_4$ to $s_5$

H. Zheng (CSE USF) Local State Space Construction for Composi
Experiment 1

- Experimented on small examples to show that $LS^3$ is capable of avoiding extra states added into local SGs.

<table>
<thead>
<tr>
<th></th>
<th>phil</th>
<th>peterson.3</th>
<th>syzmanski.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mono</td>
<td>(9, 9, 9, 9)</td>
<td>(2627, 2421, 2745)</td>
<td>(4311, 4415, 4383, 4352)</td>
</tr>
<tr>
<td>TMMC</td>
<td>(16, 16, 16, 16)</td>
<td>(2997, 2952, 2952)</td>
<td>(5875, 6125, 6250, 6375)</td>
</tr>
<tr>
<td>$LS^3$</td>
<td>(9, 9, 9, 9)</td>
<td>(2627, 2421, 2745)</td>
<td>(5201, 5453, 5598, 5755)</td>
</tr>
</tbody>
</table>

**Mono**: construct local SGs while searching the global state space of the whole system.

- A special case of $LS^3$ applied to all processes.
- Used as the baseline to compare the results from TMMC and $LS^3$. 
Experiment 1

- Experimented on small examples to show that $LS^3$ is capable of avoiding extra states added into local SGs.

<table>
<thead>
<tr>
<th></th>
<th>phil</th>
<th>peterson.3</th>
<th>syzmanski.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mono</td>
<td>(9, 9, 9, 9)</td>
<td>(2627, 2421, 2745)</td>
<td>(4311, 4415, 4383, 4352)</td>
</tr>
<tr>
<td>TMMC</td>
<td>(16, 16, 16, 16)</td>
<td>(2997, 2952, 2952)</td>
<td>(5875, 6125, 6250, 6375)</td>
</tr>
<tr>
<td>$LS^3$</td>
<td>(9, 9, 9, 9)</td>
<td>(2627, 2421, 2745)</td>
<td>(5201, 5453, 5598, 5755)</td>
</tr>
</tbody>
</table>

**Mono**: construct local SGs while searching the global state space of the whole system.
- A special case of $LS^3$ applied to all processes.
- Used as the baseline to compare the results from TMMC and $LS^3$. 
Experiment 1

- Experimented on small examples to show that $LS^3$ is capable of avoiding extra states added into local SGs.

<table>
<thead>
<tr>
<th></th>
<th>phil</th>
<th>peterson.3</th>
<th>syzmanski.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mono</td>
<td>(9, 9, 9, 9)</td>
<td>(2627, 2421, 2745)</td>
<td>(4311, 4415, 4383, 4352)</td>
</tr>
<tr>
<td>TMMC</td>
<td>(16, 16, 16, 16)</td>
<td>(2997, 2952, 2952)</td>
<td>(5875, 6125, 6250, 6375)</td>
</tr>
<tr>
<td>$LS^3$</td>
<td>(9, 9, 9, 9)</td>
<td>(2627, 2421, 2745)</td>
<td>(5201, 5453, 5598, 5755)</td>
</tr>
</tbody>
</table>

**Mono**: construct local SGs while searching the global state space of the whole system.

- A special case of $LS^3$ applied to all processes.
- Used as the baseline to compare the results from TMMC and $LS^3$. 
## Experiment 2

<table>
<thead>
<tr>
<th>Method</th>
<th>State counts of local state graphs</th>
</tr>
</thead>
<tbody>
<tr>
<td>brp</td>
<td>(5600*, 2226*, 351694*, 295*, 84, 30)</td>
</tr>
<tr>
<td>iprotocol</td>
<td>(19, 1256*, 53, 18104*, 110627*, 283444*)</td>
</tr>
<tr>
<td>lamport</td>
<td>(9344*, 9344*, 9344*, 9344*, 9344*)</td>
</tr>
<tr>
<td>lann</td>
<td>(250, 250, 250, 250, 566, 560, 561, 412)</td>
</tr>
<tr>
<td>peterson.4</td>
<td>(124535*, 104922*, 104088*, 103319*)</td>
</tr>
<tr>
<td>syzmanski.5</td>
<td>(35000*, 36250*, 36875*, 37500*, 38125*)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Method</th>
<th>Time</th>
<th>Mem</th>
<th>State counts of local state graphs</th>
</tr>
</thead>
<tbody>
<tr>
<td>TMMC</td>
<td>2.7</td>
<td>174</td>
<td>(5600*, 2226*, 351694*, 295*, 84, 30)</td>
</tr>
<tr>
<td>LS$^3$</td>
<td>9.8</td>
<td>214</td>
<td>(1368, 1496, 25091, 77, 35, 14)</td>
</tr>
<tr>
<td>TMMC</td>
<td>8.8</td>
<td>408</td>
<td>(19, 230, 29, 2647, 3656, 23747)</td>
</tr>
<tr>
<td>LS$^3$</td>
<td>10.1</td>
<td>68</td>
<td>(8800, 8800, 8800, 8800, 8800)</td>
</tr>
<tr>
<td>TMMC</td>
<td>15.9</td>
<td>106</td>
<td>(9344*, 9344*, 9344*, 9344*, 9344*)</td>
</tr>
<tr>
<td>LS$^3$</td>
<td>24.8</td>
<td>143</td>
<td>(8800, 8800, 8800, 8800, 8800)</td>
</tr>
<tr>
<td>TMMC</td>
<td>1.3</td>
<td>15</td>
<td>(250, 250, 250, 250, 566, 560, 561, 412)</td>
</tr>
<tr>
<td>LS$^3$</td>
<td>4.3</td>
<td>33</td>
<td>(250, 248, 248, 248, 566, 554, 555, 408)</td>
</tr>
<tr>
<td>TMMC</td>
<td>TO</td>
<td>–</td>
<td>(124535*, 104922*, 104088*, 103319*)</td>
</tr>
<tr>
<td>LS$^3$</td>
<td>10.9</td>
<td>88.5</td>
<td>(13573, 12993, 12869, 12801)</td>
</tr>
<tr>
<td>TMMC</td>
<td>59.4</td>
<td>198</td>
<td>(35000*, 36250*, 36875*, 37500*, 38125*)</td>
</tr>
<tr>
<td>LS$^3$</td>
<td>59.1</td>
<td>211</td>
<td>(30684*, 31934*, 32659*, 33444*, 34265*)</td>
</tr>
</tbody>
</table>
Discussions & Conclusions

- Presented an improved local state space construction method $LS^3$.
  - A key part of a methodology to address the state explosion problem due to interleavings of concurrent executions.
- $LS^3$ can produce local SGs with less unreachable states.
- $LS^3$ may incur noticeable time/mem. overhead.
  - Need to balance between size & accuracy of local SGs and cost of time & memory.
- Good target applications are loosely coupled systems.

Future work:
- Improve the $LS^3$ method further.
- Combine TMMC and $LS^3$ for their advantages.
Discussions & Conclusions

- Presented an improved local state space construction method $LS^3$.
  - A key part of a methodology to address the state explosion problem due to interleavings of concurrent executions.
- $LS^3$ can produce local SGs with less unreachable states.
- $LS^3$ may incur noticeable time/mem. overhead.
  - Need to balance between size & accuracy of local SGs and cost of time & memory.
- Good target applications are loosely coupled systems.
- Future work:
  - Improve the $LS^3$ method further.
  - Combine TMMC and $LS^3$ for their advantages.
Thank you

and

Questions?