ObsGraph: a Tool for Modular Verification of Inter-enterprise Business Processes

Hanen OCHI
Kais KLAI

LIPN – MeFoSyLoMa - Juin 2012
Abstraction and Verification of Inter-enterprise Business Processes (IEBP)
Motivation
Motivation
Motivation

Abstraction
Motivation

Abstraction

Composition
Related work

Model checking approaches:

Explicit approaches:

\textit{Abstraction}: States are represented by the graph’s nodes
Related work

Model checking approaches:

Explicit approaches:
*Abstraction*: States are represented by the graph’s nodes

Symbolic approaches:
*Abstraction*: States are represented by BDD techniques
Related work

Model checking approaches:

Explicit approaches:
*Abstraction*: States are represented by the graph’s nodes

Symbolic approaches:
*Abstraction*: States are represented by BDD techniques

Hybrid approaches:
*Abstraction*: Graph’s nodes representing a set of states are encoded using BDD techniques + the graph is represented explicitly
Verification of IEBP: Explicit approaches

- **Operating Guideline**
  - Abstraction used on SOA for services
  - Annotated automata
  - Verification of constraints represented as nodes’ annotations

- **Communication graph**
  - Abstraction used for web services
  - A bi-part graph: visible nodes + hidden nodes
  - Verification of graph’s paths
Hybrid approaches:

- **Symbolic Observation Graph SOG**
  - ✔ Abstraction of the reachability graph
  - ✔ Model checking
  - ✔ Events occurring in the formula: *Obs*
  - ✔ Events not occurring in the formula: *UnObs*
  - ✔ Structure :
Hybrid approaches:

- **Symbolic Observation Graph SOG**
  - Abstraction of the reachability graph
  - Model checking
  - Events occurring in the formula: *Obs*
  - Events not occurring in the formula: *UnObs*
  - Structure:
Hybrid approaches:

- **Symbolic Observation Graph SOG**
  - Abstraction of the reachability graph
  - Model checking
  - Events occurring in the formula: Obs
  - Events not occurring in the formula: UnObs
  - Structure:

```
<table>
<thead>
<tr>
<th>t0</th>
<th>t1</th>
<th>t2</th>
<th>t3</th>
<th>t4</th>
<th>t5</th>
</tr>
</thead>
<tbody>
<tr>
<td>a1</td>
<td>a2</td>
<td>a3</td>
<td>a4</td>
<td>a5</td>
<td>a6</td>
</tr>
</tbody>
</table>
```

Zoom on the aggregate $a_2$
Hybrid approaches:

- **Symbolic Observation Graph SOG**
  - ✔ Abstraction of the reachability graph
  - ✔ Model checking
  - ✔ Events occurring in the formula: *Obs*
  - ✔ Events not occurring in the formula: *UnObs*
  - ✔ Structure:
    - **Node**: Set of states linked by *unobserved* actions
Hybrid approaches:

- **Symbolic Observation Graph SOG**
  - Abstraction of the reachability graph
  - Model checking
  - Events occurring in the formula: *Obs*
  - Events not occurring in the formula: *UnObs*
  - Structure:
    - Node: Set of states linked by *unobserved* actions
    - Edges: Labeled by *observed* actions
Abstraction

- **New version of Symbolic Observation Graph (SOG) for a workflow:**

  ✓ Observation of only collaborative actions

  ✓ Adding \{term\} : additional virtual observed action for proper termination
    \((\text{Act}=\text{Obs} \cup \text{UnObs} \cup \{\text{term}\})\)

  ✓ Terminal circuit ⇔ deadlock state

  ✓ Observed behavior : \(\lambda\)

  \(\Rightarrow\) Nodes : Aggregates \(<S, \lambda>\)
Abstraction

• Comportement Observé <λ>

Définitions

1. $\lambda_T : T \rightarrow 2^{\text{Obs}}$

   $\lambda_T(s) = (\text{Enable}(\text{Sat}(s)) \cap \text{Obs}) \cup \{\text{term}\}$ si $F \cap \text{Sat}(s) \neq \emptyset$

   $(\text{Enable}(\text{Sat}(s)) \cap \text{Obs}) \cup \{\text{term}\}$ sinon

2. $\lambda_T : 2 \rightarrow 2^{\text{Obs}}$

   $\lambda_T(S) = \{\lambda_T(m) | m \in S\}$

3. $\lambda_{\text{min}} : 2 \rightarrow 2^{2^{\text{Obs}}}$

   $\lambda_{\text{min}}(S) = \{X \in \lambda_T(S) | \nexists Y \in \lambda_T(S) : Y \subset (X \setminus \{\text{term}\})\}$
Observed behavior
Observed behavior

\[ \lambda = \{ \{ t_1 \}, \{ t_2 \}, \{ t_3 \}, \{ t_1, t_2 \}, \{ t_1, t_2, t_3 \}, \emptyset \} \]
Observed behavior

\[ \lambda = \{\{t_1\}, \{t_2\}, \{t_3\}, \{t_1, t_2\}, \{t_1, t_2, t_3\}, \emptyset\} \]
Observed behavior

\[ \lambda = \{ \{ t_1 \}, \{ t_2 \}, \{ t_3 \}, \{ t_1, t_2 \}, \{ t_1, t_2, t_3 \}, \{ \emptyset \} \} \]

\[ \Rightarrow \lambda = \{ \{ t_1 \}, \{ t_2 \}, \{ t_3 \}, \{ \emptyset \} \} \]
Observed behavior

\[ \lambda = \{\{t_1\}, \{t_2\}, \{t_3\}, \{t_1, t_2\}, \{t_1, t_2, t_3\}, \emptyset\} \]

\[ \Rightarrow \lambda = \{\{t_1\}, \{t_2\}, \{t_3\}, \emptyset\} \]

**Theorem**: Deadlock freeness

A SOG \( G \) is said to be deadlock free \( \Leftrightarrow \not\exists \ a \in G \mid \emptyset \in a.\lambda \)
• **Theorem**: Deadlock freeness
  
  A SOG $G$ is said to be deadlock free $\iff \not\exists a \in G \mid \emptyset \in a.\lambda$

• **Proposition** :

  Let $WF$ a BP and let $G$ the associated SOG
  
  $WF$ has a deadlock state $\iff \exists a \in G \mid \emptyset \in a.\lambda$
Example (SOGs)

Reachability graph: 21 nodes + 22 edges

Reachability graph: 26 nodes + 66 edges

SOG of contractor

\[ \lambda = \{s_{\text{order}}\} \]
\[ \lambda = \{p_{\text{cost}}\} \]
\[ \lambda = \{c_{\text{spec}}\} \]
\[ \lambda = \{h_{\text{prod}}\} \]
\[ \lambda = \{\text{term}\} \]

SOG of subcontractor

\[ \lambda = \{r_{\text{order}}\} \]
\[ \lambda = \{p_{\text{spec}}, c_{\text{cost}}\} \]
\[ \lambda = \{c_{\text{cost}}\} \]
\[ \lambda = \{\text{ship}\} \]

MeFoSyLoMa
• Locally $a = \langle S, \lambda \rangle$
Composition of SOGs

- Locally $a = \langle S, \lambda \rangle$

For composition $a = \langle \lambda \rangle$
Composition of SOGs

• Locally $a = \langle S, \lambda \rangle$
  
  For composition $a = \langle \lambda \rangle$

• Synchronized product of two (or more) SOGs:
  Compute the observed behavior of $a = a_1 \times a_2$
Composition of SOGs

- Locally $a = <S, \lambda>$
- For composition
  - $a = <\lambda>$

- Synchronized product of two (or more) SOGs:
  - Compute the observed behavior of $a = a_1 \times a_2$

\[ \lambda_1 = \{\{t_1\}, \{t_3\}\} \]
\[ \lambda_2 = \{\{t_3\}\} \]
Composition of SOGs

- Locally $a = <S, \lambda>$

- Synchronized product of two (or more) SOGs:
  Compute the observed behavior of $a = a_1 \times a_2$

\[ \lambda_1 = \{\{t_1\}, \{t_3\}\} \]

\[ \lambda_2 = \{\{t_3\}\} \]

\[ \lambda = \{\emptyset, \{t_3\}\} \]
Composition of SOGs

• Locally $a = \langle S, \lambda \rangle$
  
  For composition $a = \langle \lambda \rangle$

• Synchronized product of two (or more) SOGs:
  Compute the observed behavior of $a = a_1 \times a_2$

\[
\lambda_1 = \{t_1\}, \{t_3\}\]

\[
\lambda_2 = \{t_3\}\]

\[
\lambda = \emptyset, \{t_3\}\]

Theorem:

*The composition of two SOGs $(G_1, \text{Obs}_1)$ and $(G_2, \text{Obs}_2)$ is a SOG $(G, \text{Obs}_1 \cup \text{Obs}_2)$*
Composition

SOG of contractor

\[ \lambda = \{s_{\text{order}}\} \]

\[ A'_0 \rightarrow s_{\text{order}} \]

\[ \lambda = \{p_{\text{cost}}\} \]

\[ A'_1 \rightarrow p_{\text{cost}} \]

\[ \lambda = \{c_{\text{spec}}\} \]

\[ A'_2 \rightarrow c_{\text{spec}} \]

\[ \lambda = \{h_{\text{prod}}\} \]

\[ A'_3 \rightarrow h_{\text{prod}} \]

\[ \lambda = \{\text{term}\} \]

\[ A'_4 \]

SOG of subcontractor

\[ \lambda = \{r_{\text{order}}\} \]

\[ A_0 \rightarrow s_{\text{order}} \]

\[ \lambda = \{p_{\text{spec}}, \{c_{\text{cost}}\}\} \]

\[ A_1 \rightarrow p_{\text{spec}} \]

\[ \lambda = \{c_{\text{cost}}\} \]

\[ A_2 \rightarrow c_{\text{cost}} \]

\[ \lambda = \{p_{\text{spec}}\} \]

\[ A_3 \rightarrow p_{\text{spec}} \]

\[ \lambda = \{c_{\text{cost}}\} \]

\[ A_4 \rightarrow c_{\text{cost}} \]

\[ \lambda = \{\text{ship}\} \]

\[ A_5 \rightarrow \text{ship} \]

\[ \lambda = \{\text{ship}\} \]

\[ A_6 \rightarrow \text{ship} \]

\[ \lambda = \{\text{term}\} \]
Composition

Reachability graph: 99 nodes + 320 edges

Synchronized product

MeFoSyLoMa
Reachability graph: 99 nodes + 320 edges

**Composition**

\[
\begin{align*}
A'_0A_0 & : \lambda = \{\text{order}\} \\
A'_1A'_1 & : \lambda = \{\text{spec}, \emptyset\} \\
A'_2A_3 & : \lambda = \{\text{cost}\} \\
A'_3A_5 & : \lambda = \{\text{prodcut}\} \\
A'_4A_6 & : \lambda = \{\text{term}\} \quad \text{Synchronized product}
\end{align*}
\]
Application on web services

✓ Web service: \(<(P, T, F, W), m_0, I, O, \Omega)>\n
• Definition (Soundness): \(N=<(P, T, F, W), m_0, I, O, \Omega>\) is sound if:
  ✓ option to complete: \(\forall m \in R(N^*, m_0), \exists m_f \in \Omega \text{ s.t. } m_f \in R(N^*, m_0)\)
  ✓ proper completion: if \(\exists m \in R(N^*, m_0) \text{ and } m_f \in \Omega \text{ s.t. } m > m_f\) then \(m = m_f\);
  ✓ no dead transitions: \(\forall t \in T, \exists m \in R(N^*, m_0) \text{ s.t. } m \rightarrow t;\)

• Soundness on SOG: \(G=<(A, Act, \rightarrow a_0, \Omega'), m_0, I, O, \Omega>\) is sound if:
  ✓ option to complete: \(\forall a \in A, \emptyset \notin a.\lambda \land \exists a_f \in \Omega' \text{ s.t. } a_f \in R(a)\)
  ✓ proper completion: if \(\exists a \in A, m \in a.S, \text{ m}_f \in \Omega' \text{ s.t. } m > m_f\) then \(m = m_f\);
  ✓ no dead transitions: \(\cup_{a \in A} \text{Enable}(a.S):T;\)
Application on web services

• Checking Soundness on the composition of SOGs:

Let $N_1$ and $N_2$ be two oWF-nets locally sound and let $G_1$ and $G_2$ be the corresponding SOGs respectively. $N_1 \oplus N_2$ is sound iff:

- none $\exists$ a aggregate in $G_1 \oplus G_2$ s.t $\emptyset \in a \lambda$

AND

- $\forall t \in \text{Obs}_1 \cup \text{Obs}_2$, $\exists a, a'$ two aggregates in $G_1 \oplus G_2$ s.t. $a \rightarrow_t a'$. 

MeFoSyLoMa
Implementation

- Workflow Model
  - Associated SOG + Verification on the fly
  - Synchronized product of SOGs + Verification on the fly

- SOG
  - Verification on the fly
  - Synchronized product of SOGs + Verification on the fly

MeFoSyLoMa
### Experimental results

<table>
<thead>
<tr>
<th>Model</th>
<th>Places</th>
<th>Trans</th>
<th>Obs</th>
<th>RG States</th>
<th>RG Edges</th>
<th>OG States</th>
<th>OG Edges</th>
<th>Time(s)</th>
<th>SOG States</th>
<th>SOG Edges</th>
<th>SOG Time(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>18</td>
<td>11</td>
<td>4</td>
<td>26</td>
<td>66</td>
<td>12</td>
<td>20</td>
<td>&lt;1</td>
<td>5</td>
<td>4</td>
<td>&lt;1</td>
</tr>
<tr>
<td>SC</td>
<td>15</td>
<td>9</td>
<td>4</td>
<td>11</td>
<td>11</td>
<td>9</td>
<td>11</td>
<td>&lt;1</td>
<td>7</td>
<td>7</td>
<td>&lt;1</td>
</tr>
<tr>
<td>OS</td>
<td>15</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>17</td>
<td>&lt;1</td>
<td>10</td>
<td>10</td>
<td>&lt;1</td>
</tr>
<tr>
<td>R</td>
<td>38</td>
<td>33</td>
<td>17</td>
<td>28</td>
<td>33</td>
<td>369</td>
<td>14 (E^2)</td>
<td>&lt;1</td>
<td>17</td>
<td>17</td>
<td>&lt;1</td>
</tr>
<tr>
<td>Ph5</td>
<td>36</td>
<td>16</td>
<td>10</td>
<td>417</td>
<td>10 (E^2)</td>
<td>14 (E^2)</td>
<td>34 (E^2)</td>
<td>16</td>
<td>297</td>
<td>721</td>
<td>8</td>
</tr>
<tr>
<td>Ph6</td>
<td>43</td>
<td>19</td>
<td>12</td>
<td>14 (E^2)</td>
<td>46 (E^2)</td>
<td>61 (E^2)</td>
<td>17 (E^3)</td>
<td>245</td>
<td>991</td>
<td>28 (E^2)</td>
<td>42</td>
</tr>
<tr>
<td>Ph7</td>
<td>50</td>
<td>22</td>
<td>14</td>
<td>52 (E^2)</td>
<td>19 (E^3)</td>
<td>26 (E^2)</td>
<td>88 (E^3)</td>
<td>42 (E^2)</td>
<td>33 (E^2)</td>
<td>11 (E^3)</td>
<td>162</td>
</tr>
<tr>
<td>Ph10</td>
<td>71</td>
<td>31</td>
<td>20</td>
<td>23 (E^5)</td>
<td>23 (E^4)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>12 (E^4)</td>
<td>58 (E^4)</td>
<td>15 (E^2)</td>
</tr>
<tr>
<td>2xPh5</td>
<td>71</td>
<td>31</td>
<td>4</td>
<td>23 (E^5)</td>
<td>23 (E^4)</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>21</td>
<td>50</td>
<td>15</td>
</tr>
</tbody>
</table>

**Table:** Experimental results: OG vs. SOG

- **RG:** Reachability Graph
- **OG:** Operating Guideline
- **SOG:** Symbolic Observation Graph
## Experimental results

<table>
<thead>
<tr>
<th>Model</th>
<th>Places</th>
<th>Trans</th>
<th>Obs</th>
<th>RG (States</th>
<th>Edges</th>
<th>OG (States</th>
<th>Edges</th>
<th>Time(s)</th>
<th>SOG (States</th>
<th>Edges</th>
<th>Time(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>18</td>
<td>11</td>
<td>4</td>
<td>26</td>
<td>66</td>
<td>12</td>
<td>20</td>
<td>&lt;1</td>
<td>5</td>
<td>4</td>
<td>&lt;1</td>
</tr>
<tr>
<td>SC</td>
<td>15</td>
<td>9</td>
<td>4</td>
<td>11</td>
<td>11</td>
<td>9</td>
<td>11</td>
<td>&lt;1</td>
<td>7</td>
<td>7</td>
<td>&lt;1</td>
</tr>
<tr>
<td>OS</td>
<td>15</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>17</td>
<td>&lt;1</td>
<td>10</td>
<td>10</td>
<td>&lt;1</td>
</tr>
<tr>
<td>R</td>
<td>38</td>
<td>33</td>
<td>17</td>
<td>28</td>
<td>33</td>
<td>369</td>
<td>14 E²</td>
<td>&lt;1</td>
<td>17</td>
<td>17</td>
<td>&lt;1</td>
</tr>
<tr>
<td>Ph5</td>
<td>36</td>
<td>16</td>
<td>10</td>
<td>417</td>
<td>10 E²</td>
<td>14 E²</td>
<td>34 E²</td>
<td>16</td>
<td>297</td>
<td>721</td>
<td>8</td>
</tr>
<tr>
<td>Ph6</td>
<td>43</td>
<td>19</td>
<td>12</td>
<td>14 E²</td>
<td>46 E²</td>
<td>61 E²</td>
<td>17 E³</td>
<td>245</td>
<td>991</td>
<td>28 E²</td>
<td>42</td>
</tr>
<tr>
<td>Ph7</td>
<td>50</td>
<td>22</td>
<td>14</td>
<td>52 E²</td>
<td>19 E³</td>
<td>26 E²</td>
<td>88 E³</td>
<td>42 E²</td>
<td>33 E²</td>
<td>11 E³</td>
<td>162</td>
</tr>
<tr>
<td>Ph10</td>
<td>71</td>
<td>31</td>
<td>20</td>
<td>23 E⁵</td>
<td>23 E⁴</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>12 E⁴</td>
<td>58 E⁴</td>
<td>15 E²</td>
</tr>
<tr>
<td>2xPh5</td>
<td>71</td>
<td>31</td>
<td>4</td>
<td>23 E⁵</td>
<td>23 E⁴</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>21</td>
<td>50</td>
<td>15</td>
</tr>
</tbody>
</table>

**Table:** Experimental results: OG vs. SOG

- **RG:** Reachability Graph
- **OG:** Operating Guideline
- **SOG:** Symbolic Observation Graph
## Experimental results

<table>
<thead>
<tr>
<th>Model</th>
<th>Places</th>
<th>Trans</th>
<th>Obs</th>
<th>RG States</th>
<th>RG Edges</th>
<th>OG States</th>
<th>OG Edges</th>
<th>Time(s)</th>
<th>SOG States</th>
<th>SOG Edges</th>
<th>Time(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>C</td>
<td>18</td>
<td>11</td>
<td>4</td>
<td>26</td>
<td>66</td>
<td>12</td>
<td>20</td>
<td>&lt;1</td>
<td>5</td>
<td>4</td>
<td>&lt;1</td>
</tr>
<tr>
<td>SC</td>
<td>15</td>
<td>9</td>
<td>4</td>
<td>11</td>
<td>11</td>
<td>9</td>
<td>11</td>
<td>&lt;1</td>
<td>7</td>
<td>7</td>
<td>&lt;1</td>
</tr>
<tr>
<td>OS</td>
<td>15</td>
<td>8</td>
<td>8</td>
<td>10</td>
<td>10</td>
<td>12</td>
<td>17</td>
<td>&lt;1</td>
<td>10</td>
<td>10</td>
<td>&lt;1</td>
</tr>
<tr>
<td>R</td>
<td>38</td>
<td>33</td>
<td>17</td>
<td>28</td>
<td>33</td>
<td>369</td>
<td>14 E^2</td>
<td>&lt;1</td>
<td>17</td>
<td>17</td>
<td>&lt;1</td>
</tr>
<tr>
<td>Ph5</td>
<td>36</td>
<td>16</td>
<td>10</td>
<td>417</td>
<td>10 E^2</td>
<td>14 E^2</td>
<td>34 E^2</td>
<td>16</td>
<td>297</td>
<td>721</td>
<td>8</td>
</tr>
<tr>
<td>Ph6</td>
<td>43</td>
<td>19</td>
<td>12</td>
<td>14 E^2</td>
<td>46 E^2</td>
<td>61 E^2</td>
<td>17 E^3</td>
<td>245</td>
<td>991</td>
<td>28 E^2</td>
<td>42</td>
</tr>
<tr>
<td>Ph7</td>
<td>50</td>
<td>22</td>
<td>14</td>
<td>52 E^2</td>
<td>19 E^3</td>
<td>26 E^2</td>
<td>88 E^3</td>
<td>42 E^2</td>
<td>33 E^2</td>
<td>11 E^3</td>
<td>162</td>
</tr>
<tr>
<td>Ph10</td>
<td>71</td>
<td>31</td>
<td>20</td>
<td>23 E^5</td>
<td>23 E^4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>12 E^4</td>
<td>58 E^4</td>
<td>15 E^2</td>
</tr>
<tr>
<td>2xPh5</td>
<td>71</td>
<td>31</td>
<td>4</td>
<td>23 E^5</td>
<td>23 E^4</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>21</td>
<td>50</td>
<td>15</td>
</tr>
</tbody>
</table>

**Table:** Experimental results: OG vs. SOG

- **RG:** Reachability Graph
- **OG:** Operating Guideline
- **SOG:** Symbolic Observation Graph

MeFoSyLoMa
Conclusion

- Study of some approaches for abstraction workflows
- New version of the graph of symbolic observation adapted to workflow
- Checking for deadlock freeness

-CosyVerif:
  ✓ Online shared tools integration platform.
  ✓ Integration of ObsGraphTool:
    Local Verification on workflow models
    Modular verification for composition of workflows

Demo
Further work

• **Modeling, Abstraction and Verification of Inter-Enterprise Processes**
  
  - Consider different types of properties
  
  - Consider shared resources
  
  - Consider time explicitly
Further work

- Consider different types of properties
  - Specific properties: Expressed with temporal logic (LTL, CTL ..)

- Consider shared resources

- Consider time explicitly
Further work

• **Modeling, Abstraction and Verification of Inter-Enterprise Processes**

  - Consider different types of properties
    - Specific properties: Expressed with temporal logic (LTL, CTL ..)
  
  - Consider shared resources

  - Consider time explicitly
    - Model: e.g. timed Petri nets
    - Properties: e.g. TCTL
Bibliographie


Thank you for your attention