Automated Analysis of Industrial Workflow-based Models

Mario Cortes-Cornax
Adrian Mos

Ajay Krishna
Gwen Salaün

The 33rd ACM/SIGAPP Symposium On Applied Computing
Pau, France
10 April, 2018
Talk Overview

I  Introduction to Mangrove
II  Verification framework
III  Behavioural verification
IV  Data-based analysis
V   Case study
Mangrove

Domain specific process modelling language

Domain-dependent and platform independent

Unifies Business process and SOA

Establishes concept mappings between domain specific concepts and process activities
Mangrove Elements: Publishing System
Automated Verification

Eclipse Designer
DSPML
XML
Mangrove

Intermediate format
XML

PIF

Behavioural verification
LNT

CADP

Data-based analysis
API

Z3

model to model transformation

SAT formula generation

model to text transformation
# Mangrove to PIF Transformation

<table>
<thead>
<tr>
<th>Event Type</th>
<th>Initial Event</th>
<th>End Event</th>
<th>XOR Split</th>
<th>OR Split</th>
<th>AND Split</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>STEP 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STEP 1</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STEP 2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STEP 2</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STEP 3</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>STEP 3</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Condition</th>
<th>(x ∧ ¬y) ∨ (¬x ∧ y)</th>
<th>x ∨ y</th>
<th>x ∧ y</th>
</tr>
</thead>
</table>

<table>
<thead>
<tr>
<th>Task</th>
<th>TASK 1</th>
<th>TASK 1</th>
<th>TASK 1</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>TASK 2</td>
<td>TASK 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TASK 3</td>
<td>TASK 3</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TASK 1</td>
<td>TASK 1</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TASK 2</td>
<td>TASK 2</td>
</tr>
<tr>
<td></td>
<td></td>
<td>TASK 3</td>
<td>TASK 3</td>
</tr>
</tbody>
</table>

II
Labelled Transition Systems (LTS)

Semantic model for LNT

Choice

Interleaving
Functional Verification

Deadlock Freedom

\[ \text{not } < \text{ true}^* > [ \text{ true } ] \text{ false} \]

Safety Properties

\[ [ \text{ true}^* . \text{ REQ0} . (\text{not REL0})^* . \text{ REQ1}] \text{ false} \]

Reachability

\[ < \text{ true}^*. \text{ PUT} . \text{true}^* . \text{ GET} > \text{ true} \]
Process Comparison

Conservative

Inclusive

Exclusive

Selective

Equivalence checking using CADP toolset
Data in Mangrove

- Data is not considered until now
- Behavioural model is an over approximation
- Possible “false-negatives” in verification
Modelling Mangrove Data

- Mangrove flows are directed by conditions
- Conditions can be modelled as satisfiability (SAT) constraints
- SAT constraints can be fed to a SAT solver to detect infeasible paths

\[(\text{exp} \geq 125 \land \text{exp} \leq 678) \land (\text{age} \geq 45 \land \text{age} \leq 90) \land (\text{exp} \geq 100) \land (\text{age} = 30)\]
Behaviour Refinement using SAT

1. PIF
2. Build SAT Constraints
3. Check SAT
4. Identify Infeasible States
5. Update PIF
6. Generate Feasible Behaviour

XML → Java → Z3 SMT Solver → Java → Java StaX → CADP
Document Processing

Model #1
Document Processing

Model #2
Labelled Transition Systems

Model #1

Model #2
Behavioural Verification

• Do the processes evolve conservatively?

  No

• Whether all rejections are notified in Model #2?

  No
Data-based Analysis

Assume, dataset is high quality i.e. $q\text{Ind} \geq 96$

$$((\text{rej} = 0 \oplus \text{rej} = 1 \oplus \text{rej} = 2) \land (q\text{Ind} \leq 75))$$  

$$((\text{rej} = 0 \oplus \text{rej} = 1 \oplus \text{rej} = 2) \land (q\text{Ind} > 75 \land q\text{Ind} < 96))$$  

$$((\text{rej} = 0 \oplus \text{rej} = 2) \land (q\text{Ind} \geq 96))$$
Data-based Analysis

Assume, dataset is high quality i.e. $q_{Ind} \geq 96$

$((rej = 0 \oplus rej = 1 \oplus rej = 2) \land (q_{Ind} \leq 75))$  UNSAT

$((rej = 0 \oplus rej = 1 \oplus rej = 2) \land (q_{Ind} > 75 \land q_{Ind} < 96))$  UNSAT

$((rej = 0 \oplus rej = 1 \oplus rej = 2) \land (q_{Ind} \geq 96))$  SAT
Concluding Remarks

**Behavioural Analysis**
- Identifies erroneous behavior
- Checks correctness of model evolution

**Data-based Analysis**
- Refines the model
- Identifies infeasible paths

**Future Work**
- Non-functional properties:
  - Execution time
  - Optimal resource allocation
Thank you!