Diagnosis, Synthesis and Analysis of Probabilistic Models

Tingting Han

University of Twente, The Netherlands

September 25, 2009
What do I do?
What do I do?

Mom

Fixing computers
What do I do?

Mom

Programming
What do I do?

A college mate

Mom

Applied mathematics, Formal methods
What do I do?

A college mate

Mom
What do I do?

A college mate

Mom

Correctness!
What do I do?

A college mate

Mom
What do I do?

A college mate

Mom

There should be no collisions!

- requirements
- formal-world
- system
- real-world
- Modeling
- system model
- up to $10^7$ states
- □ ¬collision
- property specification
- Model Checking
- satisfied
- violated
- Counterexample

Model checking

Han (University of Twente)
Diagnosis, Synthesis & Analysis of Probabilistic Model
Sept. 25, 2009
What do I do?

A college mate

Mom
What do I do?

A researcher in a workshop

A college mate

Mom

add Probability!
What do I do?

A researcher in a workshop

A college mate

Mom

add Probability! ⇒ probabilistic model checking
What do I do?

Boss

A researcher in a workshop

A college mate

Mom
Analysis
### Specifications

<table>
<thead>
<tr>
<th></th>
<th>branching-time</th>
<th>linear-time</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>logic</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>automata</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>untimed</td>
<td>real-time</td>
<td>untimed</td>
</tr>
<tr>
<td></td>
<td>real-time</td>
<td></td>
</tr>
</tbody>
</table>
How to model check CTMC against?

For CTMC model:

<table>
<thead>
<tr>
<th>Logic</th>
<th>Branching-time</th>
<th>Linear-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automata</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Untimed</td>
<td>Real-time</td>
<td>Untimed</td>
</tr>
</tbody>
</table>
How to model check CTMC against linear real-time specification?

For CTMC model:

<table>
<thead>
<tr>
<th></th>
<th>branching-time</th>
<th>linear-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>logic</td>
<td>😊</td>
<td>😊</td>
</tr>
<tr>
<td>automata</td>
<td></td>
<td></td>
</tr>
<tr>
<td>untimed</td>
<td>real-time</td>
<td>untimed</td>
</tr>
</tbody>
</table>
How to model check CTMC against linear real-time specification?

For CTMC model:

<table>
<thead>
<tr>
<th></th>
<th>branching-time</th>
<th>linear-time</th>
</tr>
</thead>
<tbody>
<tr>
<td>logic</td>
<td>☺</td>
<td>☺</td>
</tr>
<tr>
<td>automata</td>
<td></td>
<td>☺</td>
</tr>
<tr>
<td>untimed</td>
<td>real-time</td>
<td>untimed</td>
</tr>
<tr>
<td>real-time</td>
<td></td>
<td>real-time</td>
</tr>
</tbody>
</table>

CTMC \(\Rightarrow\) probabilistic model checking \(\Leftarrow\) deterministic timed automata
Diagnosis
Diagnosis

What’s wrong with your model?
What’s wrong with your model?

- **model**
- **specification**

Probabilistic model checking

- **satisfied**
- **violated**

no counter-examples
Diagnosis

What’s wrong with your model?

- model
- specification
- probabilistic model checking
- satisfied
- violated
- no counter-examples
Diagnosis

What’s wrong with your model?

- Define a counterexample

What has been done?
Diagnosis

What’s wrong with your model?

What has been done?

– Define a counterexample
– Design algorithms

discrete-time Markov chain $\mathcal{M}$

$P_{\leq p}(\text{property})$

probabilistic model checking

satisfied

violated

Paths | Prob.
--- | ---
$\sigma_1$ | $\Pr(\sigma_1)$
$\sigma_2$ | $\Pr(\sigma_2)$
$\sigma_3$ | $\Pr(\sigma_3)$
... | ...

$\sum_i \Pr(\sigma_i) > p$
Diagnosis

What’s wrong with your model?

Compact representation

Before: After:

What has been done?

– Define a counterexample
– Design algorithms

– Compact representation
What’s wrong with your model?

What has been done?
- Define a counterexample
- Compact representation
- Design algorithms
- Generalization

Diagnosis, Synthesis & Analysis of Probabilistic Models
Synthesis
Synthesis

What parameter values can make the model “safe”?
What parameter values can make the model “safe”?

\( \text{trains}[\text{speed} = ?, \text{length} = ?] \) satisfies \( P > 0.9999 \)\((\text{no collision})\)
What parameter values can make the model “safe”?

\( \text{trains}[speed = ?, \ length = ?] \) satisfies \( \mathcal{P}_{>0.9999}(\text{no collision}) \)
What parameter values can make the model “safe”? 

\[ \text{trains}[\text{speed} = ?, \text{length} = ?] \] satisfies \( P_{>0.9999}(\text{no collision}) \)

Parameter synthesis is much harder than model checking!