Statistical Model Checking as Feedback Control

Anna Lukina, MSc
Vienna University of Technology
Supervisor: Radu Grosu
Co-supervisor: Ezio Bartocci
Analysis of CPS: Challenges

State-space explosion:
- Open, physical part, uncertain and distributed

Model is generally not known:
- Basic laws of physical part (or controller) only partially available

Current-state is generally not known:
- Output is a function of only a subset of the state variables

How to steer towards rare events (RE) is a challenge:
- Relation between RE and the CPS behavior is not known
Outline

- Learning
- State Estimation
- Control
- Future
Model Checking as Feedback Control

Controller (imp. splitting)

Estimator (imp. sampling)

CP System (hidden MM)

Anna Lukina
Statistical Model Checking of Cyber-Physical Systems
Learning a DTMC: Input

Trace(s): 1, 1, 2, 3, 1, 2, 2, 2, 3, 3, 1, 2, 3, 3, 3, ...

Unknown model:

assume DTMC

<table>
<thead>
<tr>
<th>$T_H$</th>
<th>$X_1$</th>
<th>$X_2$</th>
<th>$X_3$</th>
<th>$X_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1$</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
</tr>
<tr>
<td>$X_2$</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
</tr>
<tr>
<td>$X_3$</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
<td></td>
</tr>
<tr>
<td>$X_4$</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$O_H$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$X_2$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$X_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>$X_4$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Learning a DTMC: Output

Learned model

<table>
<thead>
<tr>
<th>$T_H$</th>
<th>$X_1$</th>
<th>$x_2$</th>
<th>$x_3$</th>
<th>$x_4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1$</td>
<td>0.5</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0.51</td>
<td>0</td>
<td>0.49</td>
<td>0</td>
</tr>
<tr>
<td>$X_3$</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
<td>0.5</td>
</tr>
<tr>
<td>$x_4$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>$O_H$</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>$X_1$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_2$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$x_3$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>$x_4$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
</tbody>
</table>
Learning a DTMC: Input

Trace(s): 1, 1, 2, 3, 1, 2, 2, 2, 3, 3, 1, 2, 3, 3, 3, ...

Unknown model:

<table>
<thead>
<tr>
<th>( T_H )</th>
<th>( x_1 )</th>
<th>( x_2 )</th>
<th>( x_3 )</th>
<th>( x_4 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_1 )</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
</tr>
<tr>
<td>( x_2 )</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
</tr>
<tr>
<td>( x_3 )</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
</tr>
<tr>
<td>( x_4 )</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
<td>0.25</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>( O_H )</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
</tr>
</thead>
<tbody>
<tr>
<td>( x_1 )</td>
<td>0.5</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>( x_2 )</td>
<td>0</td>
<td>0.5</td>
<td>0.5</td>
<td>0</td>
</tr>
<tr>
<td>( x_3 )</td>
<td>0</td>
<td>0</td>
<td>0.5</td>
<td>0.5</td>
</tr>
<tr>
<td>( x_4 )</td>
<td>0.5</td>
<td>0</td>
<td>0</td>
<td>0.5</td>
</tr>
</tbody>
</table>
Learning a DTMC: Output

Learned model

Initial $O_H$ big impact!

$T_H$ | $X_1$ | $X_2$ | $X_3$ | $X_4$
---|---|---|---|---
$X_1$ | 0.84 | 0.16 | 0 | 0
$X_2$ | 0.50 | 0 | 0.24 | 0.26
$X_3$ | 0 | 0 | 0.52 | 0.48
$X_4$ | 0 | 0 | 0.52 | 0.48

$O_H$ | 1 | 2 | 3 | 4
---|---|---|---|---
$X_1$ | 0.67 | 0.33 | 0 | 0
$X_2$ | 0 | 0 | 1 | 0
$X_3$ | 0 | 0 | 0 | 1
$X_4$ | 0 | 0 | 0 | 1
Discrete-time Markov Chain

Learning curve with Matlab HMM Toolbox
State Estimation (IS)

**Given**

- \( P(X_{t+1} \mid X_t) = T_H, P(X_1) \)
- \( P(y_t \mid X_t) = O_H \)
- trace \( y_{1,t+1} = y_1, \ldots, y_{t+1} \)

**Compute** \( P(X_{t+1} \mid y_{1:t+1}) \)
State Estimation (IS)

Initial distribution of the particles

\begin{align*}
\text{State 1:} & \quad P(a) = 0.2, \quad P(b) = 0.8 \\
\text{State 2:} & \quad P(c) = 1.0 \\
\text{State 3:} & \quad P(a) = 0.6, \quad P(b) = 0.4 \\
\text{State 4:} & \quad P(d) = 1.0 \\
\text{State 5:} & \quad P(a) = 10^{-6}, \quad P(b) = 10^{-6}
\end{align*}
Simulate the CPS

P(a) = 0.2
P(b) = 0.8
X₁

P(c) = 1.0
X₂

P(a) = 0.6
P(b) = 0.4
X₃

P(d) = 1.0
X₄

P(a) = 10^{-6}
P(b) = 1 \cdot 10^{-6}
X₅

P(a) = 0.6
P(b) = 0.4
X₃

P(c) = 1.0
X₂

P(a) = 0.2
P(b) = 0.8
X₁

P(d) = 1.0
X₄

P(a) = 10^{-6}
P(b) = 1 \cdot 10^{-6}
X₅

P(a) = 0.6
P(b) = 0.4
X₃

P(d) = 1.0
X₄

P(a) = 10^{-6}
P(b) = 1 \cdot 10^{-6}
X₅
State Estimation (IS)

New configuration of the particles

P(a) = 0.2
P(b) = 0.8
\( X_1 \)

P(c) = 1.0
\( X_2 \)

P(a) = 0.6
P(b) = 0.4
\( X_3 \)

P(d) = 1.0
\( X_4 \)

P(a) = 10^{-6}
P(b) = 1 \times 10^{-6}
\( X_5 \)

P(a) = 0.6
P(b) = 0.4

P(a) = 1.0

P(a) = 10^{-6}
P(b) = 1 \times 10^{-6}
Observe ‘a’ and resample the particles

\[ P(a) = 0.2 \]
\[ P(b) = 0.8 \]
\[ x_1 \]

\[ P(a) = 0.6 \]
\[ P(b) = 0.4 \]
\[ x_2 \]

\[ P(a) = 0.6 \]
\[ P(b) = 0.4 \]
\[ x_3 \]

\[ P(d) = 1.0 \]
\[ x_4 \]

\[ P(a) = 10^{-6} \]
\[ P(b) = 1 \times 10^{-6} \]
\[ x_5 \]
Property Decomposition

A nested sequence of temporal logic properties:
\[ \varphi_0 \iff \varphi_1 \iff \varphi_2 \ldots \iff \varphi_n = \varphi \]

A set of increasing levels:
\[ 0 = \ell_0 < \ell_1 < \ell_2 < \ldots < \ell_n = T \]
- Reaching a level implies having reached all the lower levels:
  \[ P(\ell \geq \ell_i) = P(\ell \geq \ell_i \mid \ell \geq \ell_{i-1})P(\ell \geq \ell_{i-1}), \quad P(\ell \geq \ell_0) = 1, \quad \gamma = P(\ell \geq \ell_n) \]
- The shorter trace satisfying more intermediate properties is given a higher score

The probability of the rare event:
\[ \gamma = \prod_{i=0}^{n} P(\ell \geq \ell_i \mid \ell \geq \ell_{i-1}) \]
- Levels are chosen such that to minimize the relative variance of the final estimate
Adaptive Levels for Control (ISp)

Check the property of reaching state N within N-1 transitions

\[ T_H = \begin{bmatrix}
1 - p & p & 0 & \ldots & 0 \\
1 - p & 0 & p & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 - p & \ldots & \ldots & p & 0 \\
\vdots & \vdots & \vdots & \ldots & \ldots 
\end{bmatrix} \]

\[ O_H = \begin{bmatrix}
1 & 0 & 0 & \ldots & 0 \\
0 & 1 & 0 & \ldots & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
0 & \ldots & \ldots & 1 & 0 \\
\vdots & \vdots & \vdots & \ldots & \ldots 
\end{bmatrix} \]
Adaptive Levels for Control (ISp)

Simulation with 10 particles for checking the property of reaching state 25
Controller (imp. splitting)

CP System

Estimator (imp. sampling)

Model Checking as Feedback Control

Anna Lukina

Statistical Model Checking of Cyber-Physical Systems
Model Checking as Feedback Control

Controller (imp. splitting)

action: s

CP System

output: a

Estimator (imp. sampling)

a: 4/5   b: 1/5

a: 1/5   b: 4/5

a: 1/5   b: 4/5

1/2

1/2

1/2

1

T

T₁

Anna Lukina

Statistical Model Checking of Cyber-Physical Systems
Model Checking as Feedback Control

Controller (imp. splitting)

Estimator (imp. sampling)

CP System

action: s

output: a

Anna Lukina

Statistical Model Checking of Cyber-Physical Systems
Model Checking as Feedback Control

Controller (imp. splitting)

Estimator (imp. sampling)

CP System

state: 1

action: s

output: a

1

2

3

1

2

3

1/2 1/2

a: 4/5
b: 1/5

a: 1/5
b: 4/5

a: 1/5
b: 4/5

T

T1

Anna Lukina

Statistical Model Checking of Cyber-Physical Systems
Model Checking as Feedback Control

Controller (imp. splitting)

CP System

Estimator (imp. sampling)

Annotation: a: 4/5, b: 1/5

Output: ab

State: 1
Model Checking as Feedback Control

Controller (imp. splitting)

Estimator (imp. sampling)

CP System

state: 1

action: s

output: ab

a: 4/5
b: 1/5

a: 1/5
b: 4/5

a: 1/5
b: 4/5

1/2
1/2
1/2
1/2
Model Checking as Feedback Control

Controller (imp. splitting)

Estimator (imp. sampling)

CP System

State: 12

Action: s

Output: ab

a: 4/5  
b: 1/5

a: 1/5  
b: 4/5

a: 1/5  
b: 4/5

T

T

T1

Anna Lukina

Statistical Model Checking of Cyber-Physical Systems
Model Checking as Feedback Control

Controller (imp. splitting)

action: sp

state: 12

Estimator (imp. sampling)

output: ab

CP System

Anna Lukina
Statistical Model Checking of Cyber-Physical Systems
Model Checking as Feedback Control

Controller (imp. splitting)

Estimator (imp. sampling)

CP System

state

action

output

1

2

3

1/2

1/2

1/2

1

a: 4/5
b: 1/5

a: 1/5
b: 4/5

a: 1/5
b: 4/5

Anna Lukina

Statistical Model Checking of Cyber-Physical Systems
Model Checking as Feedback Control

Controller (imp. splitting) → CP System → Estimator (imp. sampling)

- State transition:
  - From 1 → 2 with probability 2/10
  - From 1 → 3
  - From 2 → 3 with probability 1/2
  - From 3 → 1 with probability 1/2

- Action:
  - From 2 to 1 with probability 4/5
  - From 2 to 3 with probability 1/5
  - From 3 to 2 with probability 4/5
  - From 3 to 1 with probability 1/5

- Output:
  - From 1 to 2
  - From 2 to 3
  - From 3 to 1

- Time:
  - $T_1$
  - $T$

Anna Lukina
Statistical Model Checking of Cyber-Physical Systems
Model Checking as Feedback Control

Controller (imp. splitting)

Estimator (imp. sampling)

CP System

Anna Lukina

Statistical Model Checking of Cyber-Physical Systems
Future Research

- Testing on real case studies of CPS
- Efficient scoring for importance splitting
- Optimal derivation of the levels for importance splitting
- Importance sampling gives the beliefs and not actual states
- Optimal control from the belief-states
Thank you!