Modeling and Verification of Systems with Uncertainties

Benoît Delahaye

Habilitation defense
Science

Science is a systematic enterprise that builds and organizes knowledge in the form of testable explanations and predictions about the universe. [...]

▶ Natural sciences
Study nature

▶ Social sciences
Study society

▶ Formal sciences
Study abstract concepts

1https://en.wikipedia.org/wiki/Science
Example: Prediction of the growth of a jellyfish

What is the size after 100 days?
Theoretical Computer Science
Science of Models

Motivation

Providing theories, tools and techniques for building and analyzing models

- **Modeling**: How to build models
  - Language (formalism) – Expressivity – Abstraction – Manipulation

- **Verification**: How to analyze models
  - (Semi-)Automation – Complexity/Efficiency – Diagnosis
Introduction

Inconvenience of deterministic modeling

Choosing the value of unknown variables

- Guess?
- Experimental data?
- Mean value?
Inconvenience of deterministic modeling

Choosing the value of unknown variables

- Guess?
- Experimental data?
- Mean value?

The **deterministic** model is not representative of a family of variable systems
Modeling with uncertainties

**Deterministic** modeling requires perfect knowledge of the systems

**Uncertainties** can come from several sources
- Incomplete knowledge of the system (ex: unknown variables)
- Incomplete knowledge of the environment (ex: temperature, food)
- Abstraction: the model is too complex to be studied in its entirety
- ...
Modeling with uncertainties

**Deterministic** modeling requires perfect knowledge of the systems.

**Uncertainties** can come from several sources:
- Incomplete knowledge of the system (ex: unknown variables)
- Incomplete knowledge of the environment (ex: temperature, food)
- Abstraction: the model is too complex to be studied in its entirety
- ...

How are uncertainties accounted for?

- Non-determinism
- Probabilities
- Parameters
Modeling with uncertainties

Deterministic modeling requires perfect knowledge of the systems

Uncertainties can come from several sources

- Incomplete knowledge of the system (ex: unknown variables)
- Incomplete knowledge of the environment (ex: temperature, food)
- Abstraction: the model is too complex to be studied in its entirety
- ...

How are uncertainties accounted for?

- Non-determinism
- Probabilities
- Parameters
- Left out
Example: Jellyfish size ctd.

- **Non-determinism:** No further information
  
  ⇒ Study all potential outputs

- **Probabilities:** Imperfect information
  
  ⇒ Study the distribution of outputs

- **Parameters:** Building more information
  
  ⇒ The outcome is a function of $p$
  
  ⇒ Optimization

$size = f(\text{food})$
Verification with uncertainties

Simulation is not sufficient when there are uncertainties.

- Statistical analysis
  - Using extensive simulations
- Automated techniques
  - Formal model analysis
  - Mix with statistical analysis
  - ...

Bottleneck of formal verification

- Complexity
- Undecidability in some cases
- Size of the models
Challenges

**Modeling**
- Capturing details / characteristics
  - Enhance expressivity
  - Develop new modeling formalisms
- Dealing with the size
  - Develop abstraction techniques
  - Study composition techniques

**Verification**
- Solving problems / Answering questions
  - Characterize decidability
  - Develop verification techniques
- Dealing with the size
  - Combine abstraction and verification
  - Enhance efficiency
## Challenges

### Modeling
- Capturing details / characteristics
  - Enhance expressivity
  - Develop new modeling formalisms
- Dealing with the size
  - Develop abstraction techniques
  - Study composition techniques

### Verification
- Solving problems / Answering questions
  - Characterize decidability
  - Develop verification techniques
- Dealing with the size
  - Combine abstraction and verification
  - Enhance efficiency

---

Most of all: **Ease of use** by non-specialists
Contributions to the field 1/2

In the past 10 years, my contributions can be classified in 2 domains:

▶ Theoretical work on modeling formalisms and their verification
▶ Practical application of modeling and verification techniques to concrete case studies

Main “Theoretical” contributions

▶ Timed algebra of services – [FORTE’13], [ICTAC’14], [MSCS’18]
▶ Probabilistic Event-B – [SAC’17], [SoSyM’19]
▶ Probabilistic time Petri nets – [PETRI NETS’16]
▶ Parametric interval Markov chains + timed extension
  [SynCoP’15], [VMCAI’16], [TIME’16], [QEST’17], [TCS’18], [JLAMP’20]
Contributions to the field 2/2

Main “Practical” contributions

▶ Statistical model checking
  Several applications + Prototype tool – [ISoLA’12], [STTT’12], [STTT’15]

▶ **Parametric statistical model checking**
  Prototype tool + Application to UAV – [FORTE’19]

▶ Parameter synthesis using statistical model checking
  Application to oceanography – [MSystems’17], [Sci. Rep.’20]

▶ **Graphical event models learning and verification**
  Application to security assessment – [IEA/AIE’19]
Parametric Interval Markov Chains
using constraints

Anicet Bart, Paulin Fournier, Didier Lime, Eric Monfroy, Laure Petrucci, Charlotte Truchet
Outline

Introduction

Parametric Interval Markov Chains
  Parametric IMCs and Semantics
  Dealing with the semantics
  Constraint encodings
  Discussion

Parametric Statistical Model Checking

Perspectives
Context
Modeling and Analyzing families of Markov chains

System = Markov chain

- Probabilistic transition system
- Many existing verification techniques
Context
Modeling and Analyzing families of Markov chains

System = Markov chain

- Probabilistic transition system
- Many existing verification techniques
- What about variability?
Context

Modeling and Analyzing families of Markov chains

System = Markov chain

- Probabilistic transition system
- Many existing verification techniques
- What about variability?

Abstraction: interval Markov chain (Jonsson, Larsen - LICS’91)

- Represent families of Markov chains
- Several semantics
- Reason on all implementations at once
Motivation

Controlling variability

Robustness / Dimensioning

- Choosing the size of the intervals in order to preserve properties

Example: Coin manufacture

How precise must the balance of a coin be to ensure that the probability of having 5 heads in 10 tosses is above 0.49?

Answer: $\varepsilon \leq 0.01$
Motivation

Controlling variability

Robustness / Dimensioning

- Choosing the size of the intervals in order to preserve properties

Example: Coin manufacture

How precise must the balance of a coin be to ensure that the probability of having 5 heads in 10 tosses is above 0.49?
Answer: $\varepsilon \leq 0.01$

⇒ All the coins that respect the above specification with $\varepsilon \leq 0.01$ will satisfy the property
Challenges

**Compatibility**

Preserving the characteristics of IMCs
- Considering all semantics

**Decidability**

Being able to solve the original problem
- Compute the set of parameter values ensuring a given property

**Usefullness**

Being able to deal with “large enough” models
- Number of states/ transitions
- Number of parameters
Outline

Introduction

Parametric Interval Markov Chains

Parametric IMCs and Semantics

Background : IMCs
Parametric IMCs
Dealing with the semantics
Constraint encodings
Discussion

Parametric Statistical Model Checking

Perspectives
Interval Markov Chains (IMCs)

Semantics

Specification (IMC)
Interval Markov Chains (IMCs)

Semantics

Specification (IMC)

Implementation (MC)

“Once and for all” semantics $\models_1^o$
Interval Markov Chains (IMCs)

Semantics

**Specification (IMC)**

**Implementation (MC)**

“IMDP” semantics $\models$
Interval Markov Chains (IMCs)

Semantics

Specification (IMC)

Implementation (MC)

"At every step" semantics $\models$
Parametric Interval Markov Chains (pIMCs)

Valuating the parameters of $I$ with valuation $v$ gives an IMC $v(I)$.

Implementations are implementations of the resulting IMCs w.r.t chosen semantics.
Parametric Interval Markov Chains (pIMCs)

Valuating the parameters of $\mathcal{I}$ with valuation $v$ gives an IMC $v(\mathcal{I})$
Parametric Interval Markov Chains (pIMCs)

Valuating the parameters of $\mathcal{I}$ with valuation $v$ gives an IMC $v(\mathcal{I})$
Valuating the parameters of $\mathcal{I}$ with valuation $\nu$ gives an IMC $\nu(\mathcal{I})$

Implementations are implementations of the resulting IMCs w.r.t chosen semantics
Properties

Given pIMC $P$ and state label $\alpha$, synthesize all parameter valuations ensuring that 

Consistency

$P$ admits at least one implementation.

Existential/Universal qualitative reachability

$\exists M \models P$ s.t. $P^M(\Diamond \alpha) > 0$

$\forall M \models P$ s.t. $P^M(\Diamond \alpha) > 0$

Existential/Universal quantitative reachability

$\exists M \models P$ s.t. $P^M(\Diamond \alpha) \sim \lambda$

$\forall M \models P$ s.t. $P^M(\Diamond \alpha) \sim \lambda$
## Properties

Given pIMC $\mathcal{P}$ and state label $\alpha$, synthesize all parameter valuations ensuring that

<table>
<thead>
<tr>
<th>Consistency</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{P}$ admits at least one implementation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Existential/Universal qualitative reachability</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\exists \mathcal{M} \models \mathcal{P}$ s.t. $\mathbb{P}^\mathcal{M}(\Diamond \alpha) &gt; 0$</td>
</tr>
<tr>
<td>$\forall \mathcal{M} \models \mathcal{P}$ s.t. $\mathbb{P}^\mathcal{M}(\Diamond \alpha) &gt; 0$</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Existential/Universal quantitative reachability</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\exists \mathcal{M} \models \mathcal{P}$ s.t. $\mathbb{P}^\mathcal{M}(\Diamond \alpha) \sim \lambda$</td>
</tr>
<tr>
<td>$\forall \mathcal{M} \models \mathcal{P}$ s.t. $\mathbb{P}^\mathcal{M}(\Diamond \alpha) \sim \lambda$</td>
</tr>
</tbody>
</table>

Depends on the chosen IMC semantics
Outline

Introduction

Parametric Interval Markov Chains
  Parametric IMCs and Semantics
  Dealing with the semantics
  Constraint encodings
  Discussion

Parametric Statistical Model Checking

Perspectives
Reducing to “once-and-for-all”

**Observation**

The “once-and-for-all” semantics can be dealt with

- The implementation structure is known
- MC techniques can be adapted
Reducing to “once-and-for-all”

**Observation**

The “once-and-for-all” semantics can be dealt with

- The implementation structure is known
- MC techniques can be adapted

**Consistency:**

**Theorem**

*An IMC is consistent iff it admits an implementation with the same structure.*

So we focus on implementations respecting the structure of the IMC.
Reducing to “once-and-for-all”

Observation

The “once-and-for-all” semantics can be dealt with
- The implementation structure is known
- MC techniques can be adapted

Consistency:

Theorem

An IMC is consistent iff it admits an implementation with the same structure.

So we focus on implementations respecting the structure of the IMC.

- Extends to qualitative reachability
Quantitative reachability

Equivalence of $|=^{a}_{I}$, $|=^{d}_{I}$ and $|=^{o}_{I}$ for IMCs

**Theorem**

Let $\mathcal{I}$ be an IMC. For all MC $\mathcal{M}$ such that $\mathcal{M} |\!|=^{a}_{I} \mathcal{I}$ and all state label $\alpha$, there exist MCs $\mathcal{M}_{\leq}$ and $\mathcal{M}_{\geq}$ such that $\mathcal{M}_{\leq} |\!|=^{o}_{I} \mathcal{I}$, $\mathcal{M}_{\geq} |\!|=^{o}_{I} \mathcal{I}$ and

$$\mathbb{P}^{\mathcal{M}_{\leq}}(\Diamond \alpha) \leq \mathbb{P}^{\mathcal{M}}(\Diamond \alpha) \leq \mathbb{P}^{\mathcal{M}_{\geq}}(\Diamond \alpha)$$

Constructive proof:
Quantitative reachability

Equivalence of $\models^a_I$, $\models^d_I$ and $\models^o_I$ for IMCs

**Theorem**

Let $I$ be an IMC. For all MC $M$ such that $M \models^a_I I$ and all state label $\alpha$, there exist MCs $M_\leq$ and $M_\geq$ such that $M_\leq \models^o_I I$, $M_\geq \models^o_I I$ and

$$\mathbb{P}^{M_\leq} (\Diamond \alpha) \leq \mathbb{P}^{M} (\Diamond \alpha) \leq \mathbb{P}^{M_\geq} (\Diamond \alpha)$$

**Constructive proof:**
Quantitative reachability

Equivalence of $\models_{\mathcal{I}}, \models_{\mathcal{I}}^d$ and $\models_{\mathcal{I}}^o$ for IMCs

Theorem

Let $\mathcal{I}$ be an IMC. For all MC $\mathcal{M}$ such that $\mathcal{M} \models_{\mathcal{I}}^a \mathcal{I}$ and all state label $\alpha$, there exist MCs $\mathcal{M}_\leq$ and $\mathcal{M}_\geq$ such that $\mathcal{M}_\leq \models_{\mathcal{I}}^o \mathcal{I}$, $\mathcal{M}_\geq \models_{\mathcal{I}}^o \mathcal{I}$ and

$$\mathbb{P}^{\mathcal{M}_\leq} (\Diamond \alpha) \leq \mathbb{P}^{\mathcal{M}} (\Diamond \alpha) \leq \mathbb{P}^{\mathcal{M}_\geq} (\Diamond \alpha)$$

Constructive proof:
Quantitative reachability

Equivalence of $\models^a_I$, $\models^d_I$ and $\models^o_I$ for IMCs

Theorem

Let $\mathcal{I}$ be an IMC. For all MC $\mathcal{M}$ such that $\mathcal{M} \models^a_I \mathcal{I}$ and all state label $\alpha$, there exist MCs $\mathcal{M}_\leq$ and $\mathcal{M}_\geq$ such that $\mathcal{M}_\leq \models^o_I \mathcal{I}$, $\mathcal{M}_\geq \models^o_I \mathcal{I}$ and

$$\mathbb{P}^{\mathcal{M}_\leq}(\diamond \alpha) \leq \mathbb{P}^{\mathcal{M}}(\diamond \alpha) \leq \mathbb{P}^{\mathcal{M}_\geq}(\diamond \alpha)$$

Constructive proof:
Outline

Introduction

Parametric Interval Markov Chains
  Parametric IMCs and Semantics
  Dealing with the semantics
  Constraint encodings
  Discussion

Parametric Statistical Model Checking

Perspectives
Constraint encoding $C_{\exists c}(\mathcal{P})$

For consistency

$C_{\exists c}(\mathcal{P})$: For each state $s \in S$, Constraints are as follows:

1. $\rho_s$, if $s = s_0$
2. $\rho_s \iff \sum_{s' \in \text{Succ}(s)} \theta_{s'}^{s} = 1$
3. $\neg \rho_s \iff \sum_{s' \in \text{Pred}(s) \setminus \{s\}} \theta_{s'}^{s} = 0$, if $s \neq s_0$
4. $\neg \rho_s \iff \sum_{s' \in \text{Succ}(s)} \theta_{s'}^{s} = 0$
5. $\rho_s \Rightarrow \theta_{s'}^{s} \in P(s, s')$, for all $s' \in \text{Succ}(s)$
Constraint encoding $\mathcal{C}_{\exists c}(\mathcal{P})$

For consistency

$\mathcal{C}_{\exists c}(\mathcal{P})$: For each state $s \in S$, 
Ex. solution:

\[ p = 0.5 \]
\[ q = 0.5 \]
Consistency and Qualitative Reachability

**Theorem**

A pIMC $\mathcal{P}$ is existential consistent iff $C_{\exists c}(\mathcal{P})$ is satisfiable.

Linear in the size of $\mathcal{P}$
Consistency and Qualitative Reachability

**Theorem**

A pIMC $\mathcal{P}$ is existential consistent iff $C_{\exists c}(\mathcal{P})$ is satisfiable.

Linear in the size of $\mathcal{P}$

- Extends to qualitative reachability (Existential + Universal): $C_{\exists r}(\mathcal{P})$
Quantitative Reachability Encoding $C_{\exists \mathbf{r}}(\mathcal{P}, \alpha)$

Based on the classical construction

($S_{\top}$ as usual, $S_{\bot}$ using $C_{\exists \mathbf{r}}(\mathcal{P})$, and additional real-valued variables and constraints for reachability properties).

Theorem

$C_{\exists \mathbf{r}}(\mathcal{P}, \alpha) \cup (\pi_{s_0} \sim p)$ is satisfiable iff $\exists \mathcal{M} \models \mathcal{P}: P^\mathcal{M}(\Diamond \alpha) \sim p$

$C_{\exists \mathbf{r}}(\mathcal{P}, \alpha) \cup (\pi_{s_0} \not\sim p)$ is unsatisfiable iff $\forall \mathcal{M} \models \mathcal{P}: P^\mathcal{M}(\Diamond \alpha) \sim p$
Quantitative Reachability Encoding $\mathbf{C}_{\exists \bar{r}}(\mathcal{P}, \alpha)$

Based on the classical construction

(S$_\top$ as usual, S$_\bot$ using $\mathbf{C}_{\exists r}(\mathcal{P})$, and additional real-valued variables and constraints for reachability properties).

**Theorem**

- $\mathbf{C}_{\exists \bar{r}}(\mathcal{P}, \alpha) \cup (\pi_{s_0} \sim p))$ is satisfiable iff $\exists \mathcal{M} \models \mathcal{P}: \mathbb{P}^\mathcal{M}(\Diamond \alpha) \sim p$

- $\mathbf{C}_{\exists \bar{r}}(\mathcal{P}, \alpha) \cup (\pi_{s_0} \not\sim p))$ is unsatisfiable iff $\forall \mathcal{M} \models \mathcal{P}: \mathbb{P}^\mathcal{M}(\Diamond \alpha) \sim p$

Regardless of the chosen semantics!
Implementation

Prototype tool

Generates the CSP encodings

- QF_LRA (qualitative) / QF_NRA (quantitative) logic in SMT_LIB format
- No integer variables ⇒ Real
- Plugged in to Z3
Implementation

Prototype tool

Generates the CSP encodings

- QF_LRA (qualitative) / QF_NRA (quantitative) logic in SMT_LIB format
- No integer variables ⇒ Real
- Plugged in to Z3

<table>
<thead>
<tr>
<th>Benchmark NAND</th>
<th>pIMC</th>
<th>C_{\exists c}</th>
<th>time</th>
<th>C_{\exists r}</th>
<th>time</th>
<th>C_{\exists r}</th>
<th>time</th>
</tr>
</thead>
<tbody>
<tr>
<td>K=1; N=2</td>
<td>104</td>
<td>255</td>
<td>0.17s</td>
<td>170</td>
<td>0.19s</td>
<td>296</td>
<td>69.57s</td>
</tr>
<tr>
<td>K=1; N=3</td>
<td>252</td>
<td>621</td>
<td>0.24s</td>
<td>406</td>
<td>0.30s</td>
<td>703</td>
<td>31.69s</td>
</tr>
<tr>
<td>K=1; N=5</td>
<td>930</td>
<td>2,308</td>
<td>0.57s</td>
<td>1,378</td>
<td>0.51s</td>
<td>2,404</td>
<td>T.O.</td>
</tr>
<tr>
<td>K=1; N=10</td>
<td>7,392</td>
<td>18,611</td>
<td>9.46s</td>
<td>9,978</td>
<td>13.44s</td>
<td>17,454</td>
<td>T.O.</td>
</tr>
</tbody>
</table>
Outline

Introduction

Parametric Interval Markov Chains
  Parametric IMCs and Semantics
  Dealing with the semantics
  Constraint encodings
  Discussion

Parametric Statistical Model Checking

Perspectives
Discussion

**Summary:**
- New modeling formalism and verification technique
- Constraint encodings
- Linear size
- Prototype implementation
- Equivalence of semantics for quantitative reachability
Discussion

▶ **Summary:**
  - New modeling formalism and verification technique
  - Constraint encodings
  - Linear size
  - Prototype implementation
  - Equivalence of semantics for quantitative reachability

▶ **Perspectives:**
  - Extension of equivalence/encoding to other properties (LTL?)
  - Generation and representation of *all solutions*
  - Extension to Constraint Markov Chains
  - …
Parametric Statistical Model Checking

and application to UAV case study

Christian Attigbe, Ran Bao, Paulin Fournier, Abhignya Kamma, Didier Lime
Outline

Introduction

Parametric Interval Markov Chains

Parametric Statistical Model Checking
  Monte Carlo and pMCs
  UAV case study
  Discussion

Perspectives
Context
Verification of (parametric) probabilistic systems

Markov chain verification: well established
- Model-checking algorithms
- Goes through the whole state space
- Optimizations
Context
Verification of (parametric) probabilistic systems

Markov chain verification: well established

- Model-checking algorithms
- Goes through the whole state space
- Optimizations

- State-space explosion
- Infinite systems?
### Context

Verification of (parametric) probabilistic systems

---

#### Markov chain verification: well established

- Model-checking algorithms
- Goes through the whole state space
- Optimizations

- **State-space explosion**
- **Infinite systems?**

---

#### Parametric Markov chains verification

- Similar to Markov chains verification
- Yields rational functions of the parameters
Context
Verification of (parametric) probabilistic systems

Markov chain verification: well established
- Model-checking algorithms
- Goes through the whole state space
- Optimizations
- State-space explosion
- Infinite systems?

Parametric Markov chains verification
- Similar to Markov chains verification
- Yields rational functions of the parameters
- State-space explosion
- Infinite systems?
- Number of parameters?
Motivation
Dealing with large (infinite) probabilistic systems

Statistical model checking (SMC)
Multiple approximation techniques
- Simulation-based
- Formal guarantees

Limitations:
- Bounded linear properties only
- Purely probabilistic systems only
# Motivation
Dealing with large (infinite) probabilistic systems

## Statistical model checking (SMC)

### Multiple approximation techniques
- Simulation-based
- Formal guarantees

- Model-size independent
- Any executable model
- Infinite systems
Motivation
Dealing with large (infinite) probabilistic systems

Statistical model checking (SMC)

Multiple approximation techniques

- Simulation-based
- Formal guarantees

- Model-size independent
- Any executable model
- Infinite systems

Limitations:

- Bounded linear properties only
- Purely probabilistic systems only
What about parametric models?

1. How to simulate?
   - Guess and optimize?

2. How to give meaningful guarantees?
What about parametric models?

1. How to simulate?
   - Guess and optimize?
   - Importance sampling

2. How to give meaningful guarantees?
   - Importance sampling

We extend Statistical Model Checking (Monte Carlo) to parametric Markov chains.

▶ Based on importance sampling with symbolic outcome
▶ Output is a polynomial function of the parameters
▶ Comes with parametric confidence intervals

Prototype tool
Application to UAV case study
What about parametric models?

1. How to simulate?
   - Guess and optimize?
   - Importance sampling

2. How to give meaningful guarantees?
   ⇒ Importance sampling

⇒ We extend Statistical Model Checking (Monte Carlo) to **parametric Markov chains**
   - Based on **importance sampling** with symbolic outcome
   - Output is a polynomial function of the parameters
   - Comes with parametric confidence intervals

+ Prototype tool
+ Application to UAV case study
Outline

Introduction

Parametric Interval Markov Chains

Parametric Statistical Model Checking
  Monte Carlo and pMCs
  UAV case study
  Discussion

Perspectives
Properties

We only consider properties on bounded runs.

- **Bounded reachability**: Studying the probability of reaching a given state in less than $\ell$ steps. Written $\mathbb{P}_\mathcal{M}(\Diamond \leq \ell \cdot s)$.

- **Bounded safety**: Studying the probability of staying in a set of safe states during $\ell$ steps. Written $\mathbb{P}_\mathcal{M}(\Box = \ell \cdot E)$.

- **Expected reward**: Studying the expected value of a given reward function $r$ on runs of length $\ell$. Written $\mathbb{E}_{\mathcal{M}}^\ell(r)$.

**Remark**

**Expected reward** properties capture bounded safety and reachability.
Intuition for pMCs

Expected reward $r$

How to run simulations?
Intuition for pMCs

Expected reward $r$

How to run simulations? Use a *normalization function* $f \rightarrow M^f$
Intuition for pMCs

Expected reward $r$

How to run simulations? Use a *normalization function* $f \rightarrow \mathcal{M}^f$

Use $r'(\rho) = \frac{P_{\mathcal{M}(\rho)}}{P_{\mathcal{M}^f(\rho)}} r(\rho)$ instead of $r$
Intuition for pMCs

Expected reward $r$

How to run simulations? Use a normalization function $f \to \mathcal{M}^f$

Use $r'(\rho) = \frac{\mathbb{P}_\mathcal{M}(\rho)}{\mathbb{P}_\mathcal{M}^f(\rho)} r(\rho)$ instead of $r$

$$\mathbb{E}_\mathcal{M}(r')(v) = \mathbb{E}_\mathcal{M}^v(r)$$ for all valid parameter valuation $v$

If $\mathcal{M}^f$ and $\mathcal{M}^v$ have the same structure
Intuition for pMCs

Expected reward $r$

How to run simulations? Use a *normalization function* $f \rightarrow M^f$

Use $r'(\rho) = \frac{P_{M}(\rho)}{P_{M^f}(\rho)} r(\rho)$ instead of $r$

$$E_{M}(r')(v) = E_{M^v}(r) \text{ for all valid parameter valuation } v$$

If $M^f$ and $M^v$ have the same structure

**Bonus:** confidence interval = polynomial function of the parameters
Example

Measure the probability of reaching 4 in less than 5 steps

\[ r(\rho_i) = 1 \text{ if } \rho_i \text{ reaches } 4 \]

\[ \begin{align*}
\rho_1 &= 0 \cdot 1 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \\
\rho_2 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 3 \cdot 4 \\
\rho_3 &= 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \\
\rho_4 &= 0 \cdot 1 \cdot 0 \cdot 1 \cdot 1 \cdot 0 \\
\rho_5 &= 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \\
\rho_6 &= 0 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 4 \\
\rho_7 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2 \\
\rho_8 &= 0 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 
\end{align*} \]
Example

Measure the probability of reaching 4 in less than 5 steps

\[
\begin{align*}
\rho_1 &= 0 \cdot 1 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \quad r'(\rho_1) = 0 \\
\rho_2 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 3 \cdot 4 \quad r'(\rho_2) = 27pqt \\
\rho_3 &= 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \quad r'(\rho_3) = 0 \\
\rho_4 &= 0 \cdot 1 \cdot 0 \cdot 1 \cdot 1 \cdot 0 \quad r'(\rho_4) = 0 \\
\rho_5 &= 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \quad r'(\rho_5) = 3q \\
\rho_6 &= 0 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 4 \quad r'(\rho_6) = 27qt^2 \\
\rho_7 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2 \quad r'(\rho_7) = 0 \\
\rho_8 &= 0 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \quad r'(\rho_8) = 0
\end{align*}
\]

- \( r(\rho_i) = 1 \) if \( \rho_i \) reaches 4
Example

Measure the probability of reaching 4 in less than 5 steps

\[
\begin{align*}
\rho_1 &= 0 \cdot 1 \cdot 1 \cdot 2 \cdot 2 \cdot 2 & r'(\rho_1) &= 0 \\
\rho_2 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 3 \cdot 4 & r'(\rho_2) &= 27pqt \\
\rho_3 &= 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & r'(\rho_3) &= 0 \\
\rho_4 &= 0 \cdot 1 \cdot 0 \cdot 1 \cdot 1 \cdot 0 & r'(\rho_4) &= 0 \\
\rho_5 &= 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 4 & r'(\rho_5) &= 3q \\
\rho_6 &= 0 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 4 & r'(\rho_6) &= 27qt^2 \\
\rho_7 &= 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2 & r'(\rho_7) &= 0 \\
\rho_8 &= 0 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 & r'(\rho_8) &= 0 \\
\end{align*}
\]

\[\mathbb{E}^5_M(r') \sim 3.375pq + 0.375q + 3.375qt^2\]

- \(r(\rho_i) = 1\) if \(\rho_i\) reaches 4
- Here, \(\mathbb{E}^5_M(r') \sim 3.375pq + 0.375q + 3.375qt^2\)

For \(v(p) = v(q) = 0.25\), \(v(t) = 0.5\): \(\mathbb{E}^5_M(r')(v) \sim 0.41\) (exact: 0.261..)
Example

Measure the probability of reaching 4 in less than 5 steps

\[ \rho_1 = 0 \cdot 1 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \quad r'(\rho_1) = 0 \]

\[ \rho_2 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 3 \cdot 4 \quad r'(\rho_2) = 27pqt \]

\[ \rho_3 = 0 \cdot 3 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \quad r'(\rho_3) = 0 \]

\[ \rho_4 = 0 \cdot 1 \cdot 0 \cdot 1 \cdot 1 \cdot 0 \quad r'(\rho_4) = 0 \]

\[ \rho_5 = 0 \cdot 3 \cdot 4 \cdot 4 \cdot 4 \cdot 4 \quad r'(\rho_5) = 3q \]

\[ \rho_6 = 0 \cdot 3 \cdot 3 \cdot 3 \cdot 4 \cdot 4 \quad r'(\rho_6) = 27qt^2 \]

\[ \rho_7 = 0 \cdot 1 \cdot 0 \cdot 3 \cdot 2 \cdot 2 \quad r'(\rho_7) = 0 \]

\[ \rho_8 = 0 \cdot 1 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \quad r'(\rho_8) = 0 \]

- \( r(\rho_i) = 1 \) if \( \rho_i \) reaches 4
- Here, \( \mathbb{E}_M^5 (r') \sim 3.375pqt + 0.375q + 3.375qt^2 \)
  For \( v(p) = v(q) = 0.25, v(t) = 0.5 \): \( \mathbb{E}_M^5 (r')(v) \sim 0.41 \) (exact: 0.261..)
- With 1 000 runs:
  \( \mathbb{E}_M^5 (r') \sim 0.2801 \)
  Size of CI = 0.0296
Prototype Implementation

**MCpMC**

parametric Statistical Model Checking

- Written in Python
- input: prism model or python class
- output: parametric probability function / confidence interval
- graphical web interface (ongoing work)

^Available at https://github.com/Astlo/IMCpMC
Outline

Introduction

Parametric Interval Markov Chains

Parametric Statistical Model Checking
  Monte Carlo and pMCs
  UAV case study
  Discussion

Perspectives
Context: UAVs flying above a crowd (Entertainment)

- UAV public shows
- Concerned with safety
Context: UAVs flying above a crowd (Entertainment)

- UAV public shows
- Concerned with safety

⇒ How to ensure that the flight is safe?
Measuring safety of the crowd

Humans are safe if UAVs are far

Trajectory computation depends on position estimation

Precise position estimation ensures human safety

⇒ Focus on the probability that a UAV stays in a “safe zone”

Guaranteeing human safety
Measuring safety of the crowd

Guaranteeing human safety

- Humans are safe if UAVs are far
Measuring safety of the crowd

Humans are safe if UAVs are far

Trajectory computation depends on position estimation
Measuring safety of the crowd

 Guarant ee ing human safety

- Humans are safe if UAVs are far
- Trajectory computation depends on position estimation
- Precise position estimation ensures human safety
Measuring safety of the crowd

- Humans are safe if UAVs are far
- Trajectory computation depends on position estimation
- Precise position estimation ensures human safety

⇒ Focus on the probability that a UAV stays in a “safe zone”
Modeling UAV trajectory

- Flight plan is cut in segments
- 5 safety zones of fixed size
Modeling UAV trajectory

- Flight plan is cut in segments
- 5 safety zones of fixed size

Position estimation:

Sensor precision
Filter correction \{ Precision parameter

Diagram showing the flow of information from sensors to flight control with nodes labeled for filter, position, PID, and modulation.
Modeling UAV trajectory

- Flight plan is cut in segments
- 5 safety zones of fixed size

Position estimation:

Sensor precision
Filter correction \{ Precision parameter

For each segment

- Estimated position according to precision parameters
- Next position = function of estimated position
Resulting Models

(a) Precision on $y$
(b) Precision on $x, y$
(c) Complex flight plan
(d) Wind disturbance

- 4 models of increasing complexity
- Position = real-valued variables
- Prism (a) and Python (b,c,d) models
- Parameters = precision of Position($x,y$) + wind force
Parametric Statistical Model Checking UAV case study

Results: Probability of entering zones 4-5

<table>
<thead>
<tr>
<th>#sim</th>
<th>Model</th>
<th>#p</th>
<th>10k</th>
<th>20k</th>
<th>50k</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>V1</td>
<td>V2</td>
<td></td>
</tr>
<tr>
<td>Running time</td>
<td>(d)(np)</td>
<td>5</td>
<td>28s</td>
<td>53-54s</td>
<td>149-155s</td>
</tr>
<tr>
<td>Scenario 1</td>
<td></td>
<td></td>
<td>5.44%</td>
<td>5.61%</td>
<td>5.59%</td>
</tr>
<tr>
<td>Conf. interv.</td>
<td></td>
<td></td>
<td>±0.98%</td>
<td>±0.69%</td>
<td>±0.42%</td>
</tr>
<tr>
<td>Scenario 2</td>
<td></td>
<td></td>
<td>10.8%</td>
<td>10.8%</td>
<td>10.9%</td>
</tr>
<tr>
<td>Conf. interv.</td>
<td></td>
<td></td>
<td>±1.35%</td>
<td>±0.91%</td>
<td>±0.57%</td>
</tr>
<tr>
<td>Running time</td>
<td>(d)(p)</td>
<td>9</td>
<td>185-190s</td>
<td>311-314s</td>
<td>612-621s</td>
</tr>
<tr>
<td>Scenario 1</td>
<td></td>
<td></td>
<td>4.95%</td>
<td>5.28%</td>
<td>4.16%</td>
</tr>
<tr>
<td>Conf. interv.</td>
<td></td>
<td></td>
<td>±5.22%</td>
<td>±4.71%</td>
<td>±1.86%</td>
</tr>
<tr>
<td>Scenario 2</td>
<td></td>
<td></td>
<td>9.55%</td>
<td>10.3%</td>
<td>9.57%</td>
</tr>
<tr>
<td>Conf. interv.</td>
<td></td>
<td></td>
<td>±8.40%</td>
<td>±7.04%</td>
<td>±5.29%</td>
</tr>
</tbody>
</table>

Precision parameters PF0/1/2/3/4: 0-2m / 2-4m / 4-6m / 6-8m / 8-10m

Zone4: 8m from trajectory. Zone5: 50m from trajectory

Scenario 1
PF0/1/2/3/4 = 0.15/0.3/0.4/0.1/0.05

Scenario 2
PF0/1/2/3/4 = 0.1/0.25/0.35/0.2/0.1
Outline

Introduction

Parametric Interval Markov Chains

Parametric Statistical Model Checking
  Monte Carlo and pMCs
  UAV case study

Discussion

Perspectives
Discussion

- **Summary:**
  - Parametric Monte Carlo procedure for pMC
  - Polynomial parametric confidence interval
  - Prototype implementation
  - Application to UAV flight plan analysis
Discussion

▶ **Summary:**
  ▶ Parametric Monte Carlo procedure for pMC
  ▶ Polynomial parametric confidence interval
  ▶ Prototype implementation
  ▶ Application to UAV flight plan analysis

▶ **Perspectives:**
  ▶ Impact of the normalization function
  ▶ Improving MCpMC
  ▶ Comparison/Integration(?) to existing tools
Outline

Introduction

Parametric Interval Markov Chains

Parametric Statistical Model Checking

Perspectives
Gap between theory and practice

Remark

The modeling formalism used in the UAV case study is not (parametric/interval) Markov chains.
Gap between theory and practice

Remark

The modeling formalism used in the UAV case study is not (parametric/interval) Markov chains.

- Not suited to practical applications
  - Real valued variables
  - Complex behaviour
  - Huge model
- Model practitioners are not aware / expert of those formalisms
Gap between theory and practice

Remark

The modeling formalism used in the UAV case study is not (parametric/interval) Markov chains.

- Not suited to practical applications
  - Real valued variables
  - Complex behaviour
  - Huge model
- Model practitioners are not aware / expert of those formalisms

We need to make theory usable in practice
Gap between theory and practice

Remark

The modeling formalism used in the UAV case study is not (parametric/interval) Markov chains.

- Not suited to practical applications
  - Real valued variables
  - Complex behaviour
  - Huge model
- Model practitioners are not aware/ expert of those formalisms

We need to make theory usable in practice

- pSMC is promising (few modeling requirements)
Research axes

- Reducing model size:
  - Abstraction / Composition theories
  - Automated model learning using experimental data

- Enhancing pSMC:
  - More insightful types of parameters
  - Choice of normalization functions

- Developing a verification platform:
  - Usable by computer scientists and modelers
  - Ex: Parameterization of the jellyfish model
Research axes

Reducing model size

- Abstraction / Composition theories
- Automated model learning using experimental data
Research axes

Reducing model size
- Abstraction / Composition theories
- Automated model learning using experimental data

Enhancing pSMC
- More insightfull types of parameters
- Choice of normalization functions
Research axes

Reducing model size
- Abstraction / Composition theories
- Automated model learning using experimental data

Enhancing pSMC
- More insightfull types of parameters
- Choice of normalization functions

Developing a verification platform
- Usable by computer scientists and modelers
  Ex: Parameterisation of the jellyfish model
Thanks

- The jury
- Ph.D. students and postdocs
  Amine, Dimitri, Eva, Hadrien, Paulin
- Co-authors
- LS2N Colleagues
  Anne-Françoise, Annie, Assia, Audrey, Charlery, Christine, Claude, Damien V., Elodie, Géraldine, Gilles, Guillaume, Laura, Marion, Pascal, Samuel, Virginie, . . .
- All my friends and family
Thanks

▶ The jury
▶ Ph.D. students and postdocs
  Amine, Dimitri, Eva, Hadrien, Paulin
▶ Co-authors
▶ LS2N Colleagues
  Anne-Françoise, Annie, Assia, Audrey, Charlery, Christine, Claude, Damien V., Elodie, Géraldine, Gilles, Guillaume, Laura, Marion, Pascal, Samuel, Virginie, . . .
▶ All my friends and family

Thank you for listening!
References I


References II


