Contributions to the verification and control of timed and probabilistic models

Nathalie Bertrand

Inria Rennes

Habilitation defense - November 16th 2015

Formal verification of software systems

Software systems are everywhere.
Bugs are everywhere.
Formal verification should be everywhere!

static analysis analysis of the source code of a program in a static manner, *i.e.* without executing it

theorem proving automated proofs of mathematical statements through logical reasoning using deduction rules

model based testing generation of a set of testing scenarios, given a model of the system

model checking certification that a mathematical representation of the system satisfies a model of its specification

Formal verification of software systems

Software systems are everywhere.
Bugs are everywhere.
Formal verification should be everywhere!

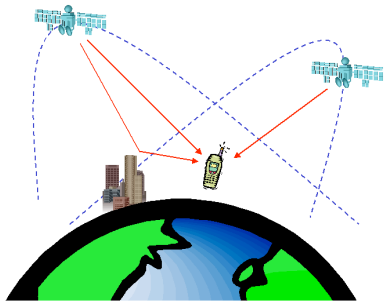
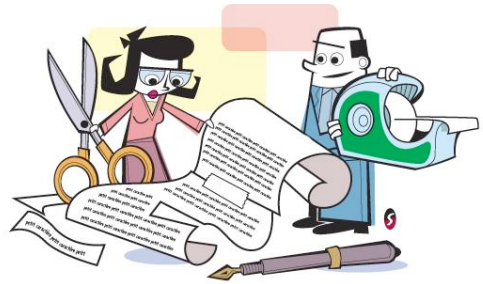
static analysis analysis of the source code of a program in a static manner, *i.e.* without executing it

theorem proving automated proofs of mathematical statements through logical reasoning using deduction rules

model based testing generation of a set of testing scenarios, given a model of the system

model checking certification that a mathematical representation of the system satisfies a model of its specification

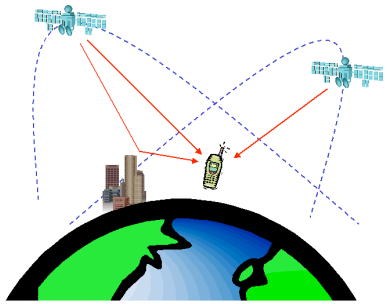
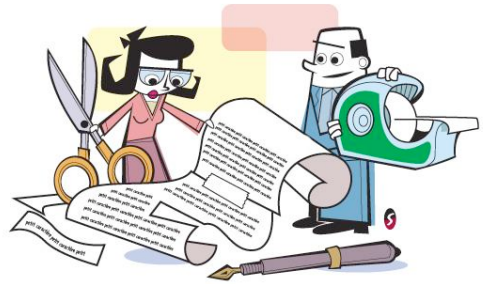
Principles of model checking

Does  satisfy  ?

system

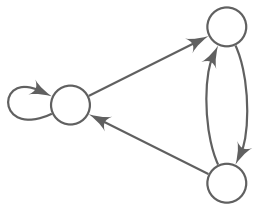
specification

Principles of model checking

Does  satisfy  ?

system

specification

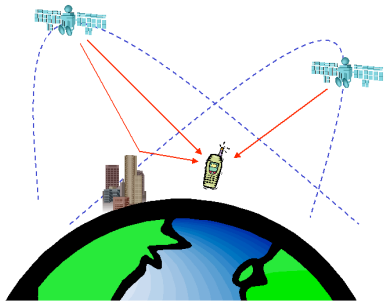
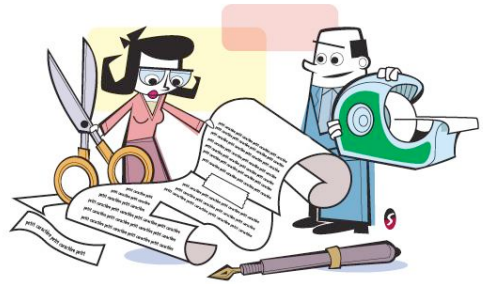


φ

model

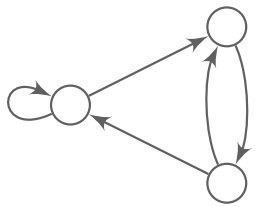
formula

Principles of model checking

Does  satisfy  ?

system

specification



model

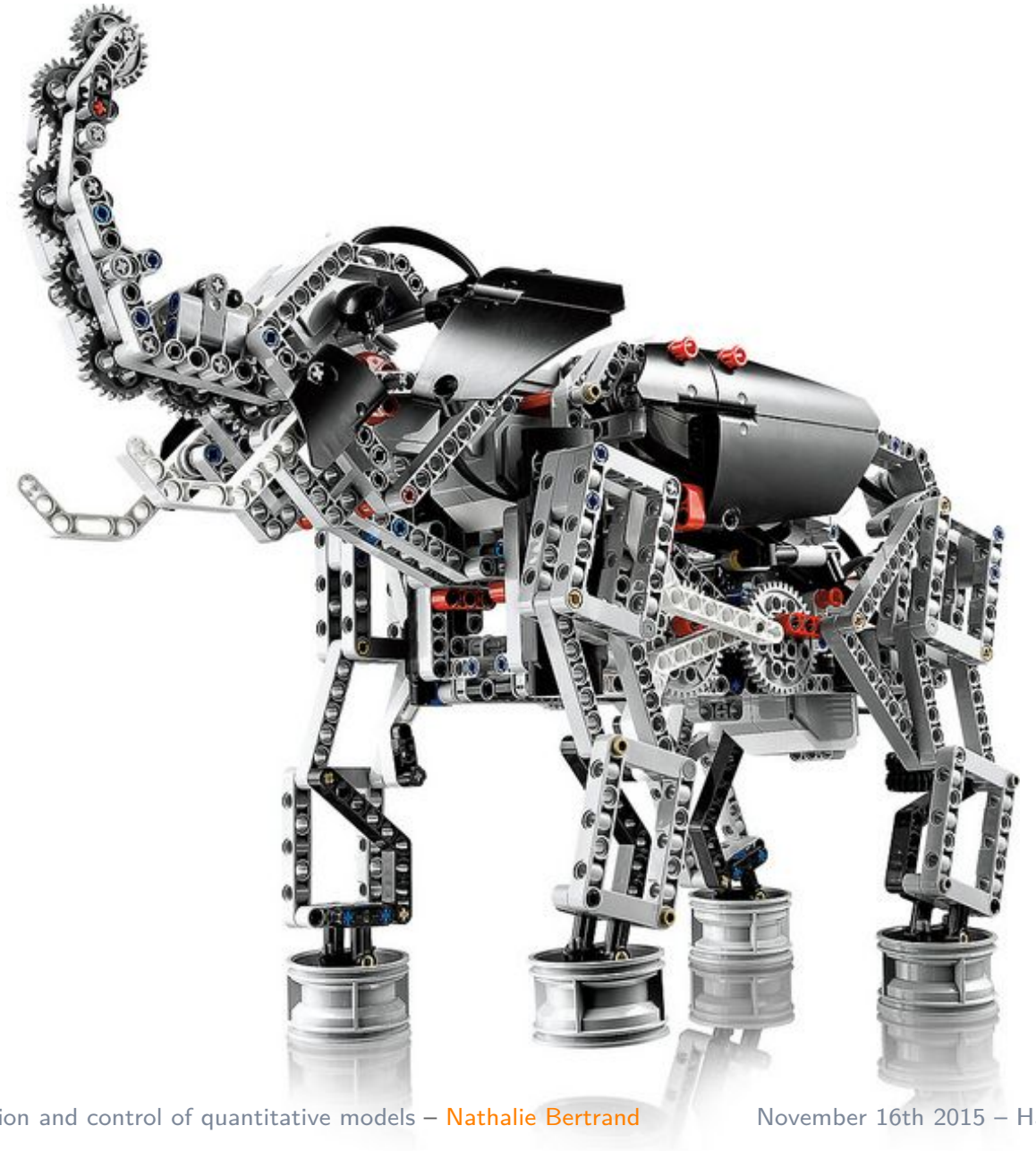
$\models$

model checker

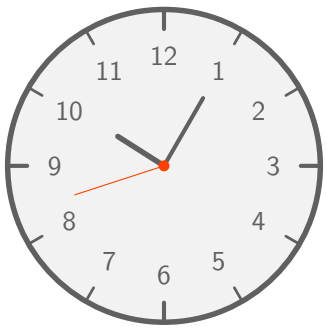
φ

formula

?



Rich models for complex systems

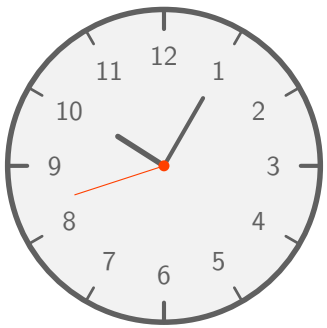


timing constraints

delays, timeouts

real-time systems

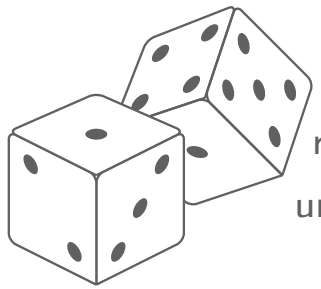
Rich models for complex systems



delays, timeouts

real-time systems

timing constraints

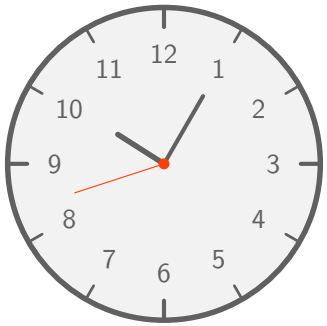


randomized algorithms

unpredictable behaviours

probabilities

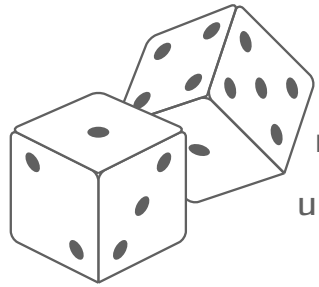
Rich models for complex systems



delays, timeouts

real-time systems

timing constraints



randomized algorithms

unpredictable behaviours

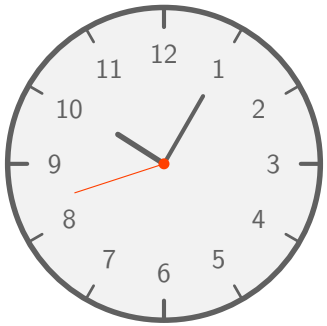
probabilities

large systems

security concerns

partial observation

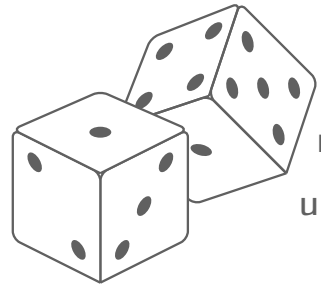
Rich models for complex systems



delays, timeouts

real-time systems

timing constraints



randomized algorithms

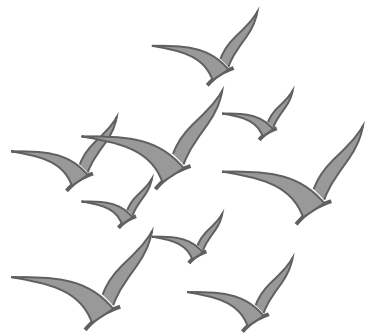
unpredictable behaviours

probabilities

large systems

security concerns

partial observation

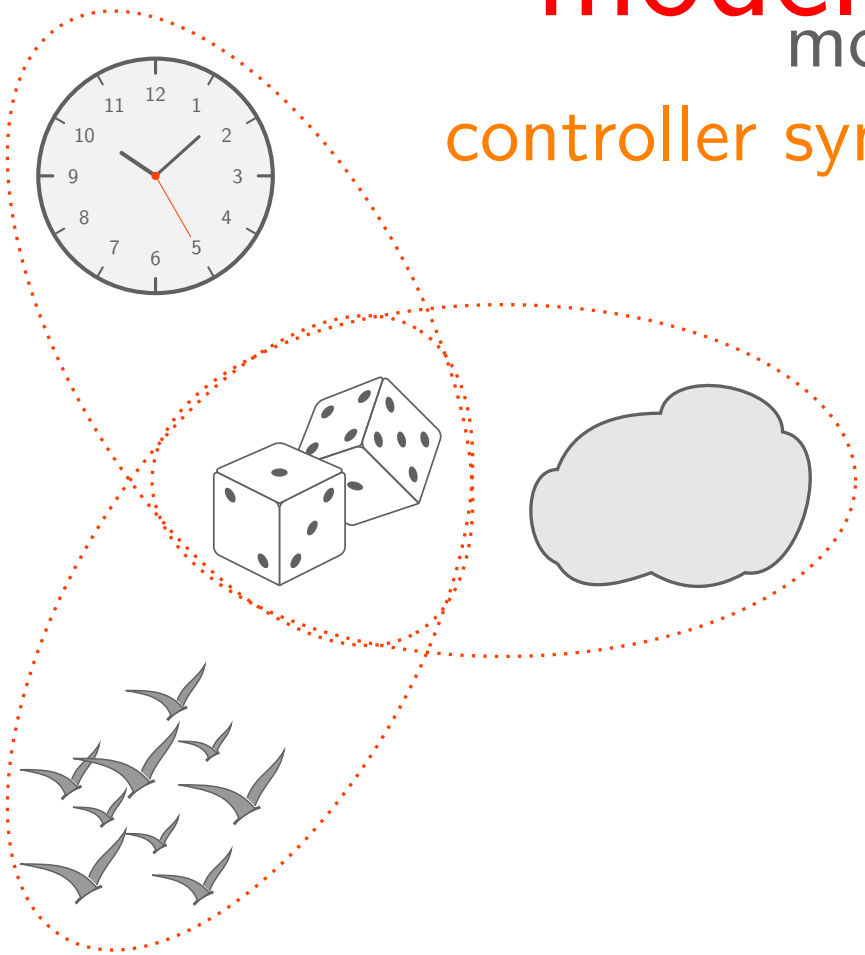


unknown value

generic systems

parameters

Contributions in a nutshell



model-based testing

model checking

monitoring issues

controller synthesis

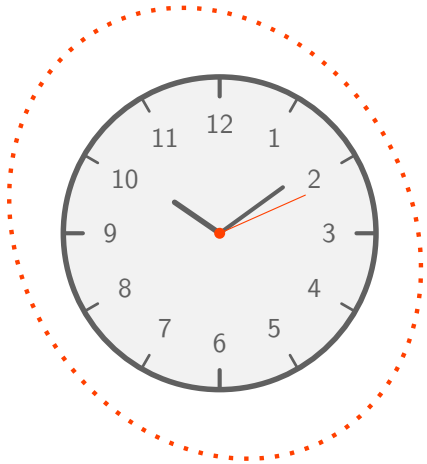
decidability

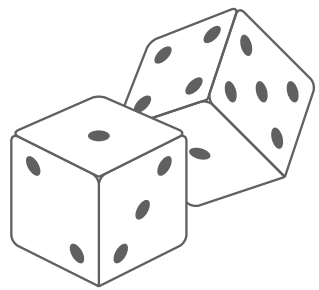
complexity

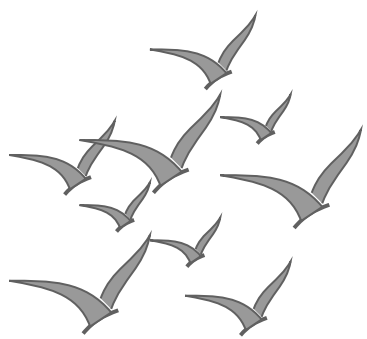
algorithms

Outline

1. **timed automata**

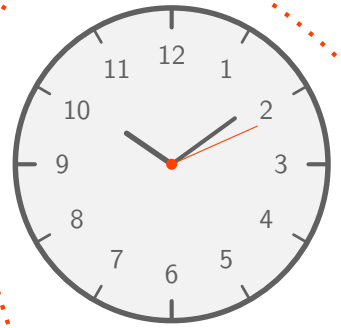




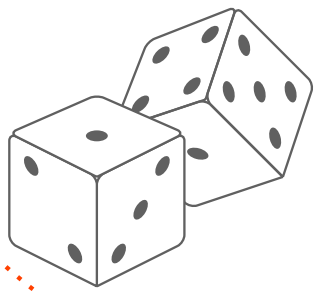


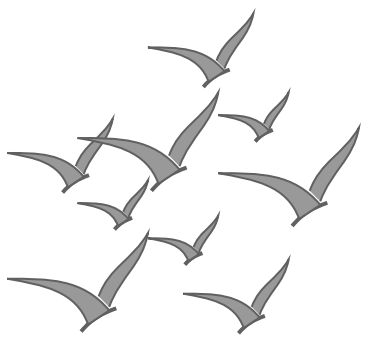
Outline

1. **timed automata**



2. **stochastic timed automata**



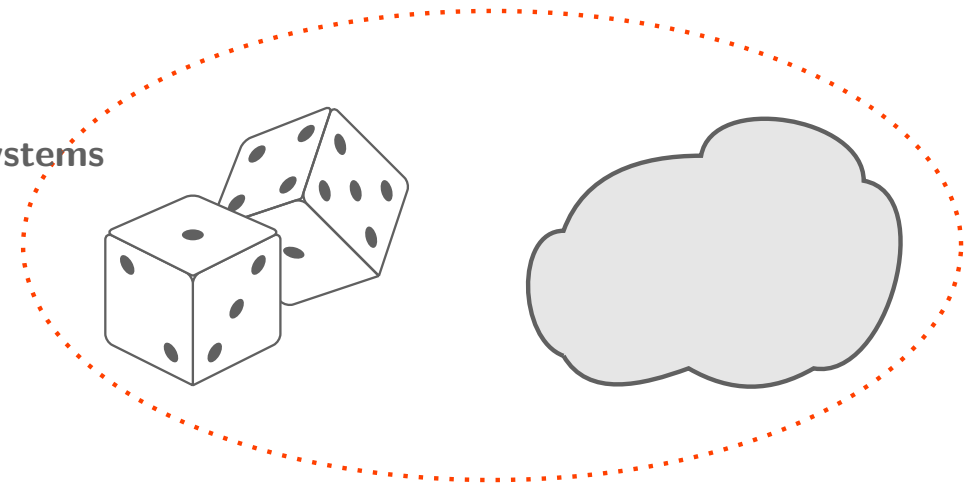


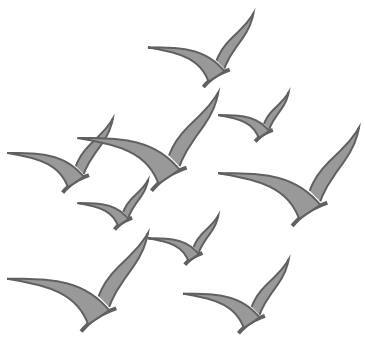
Outline

❶ **timed automata**

❷ **stochastic timed automata**

❸ **partially observable probabilistic systems**



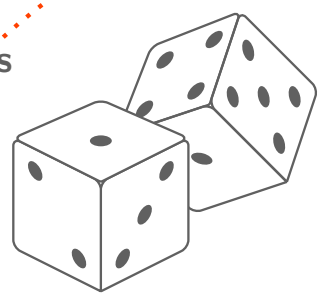


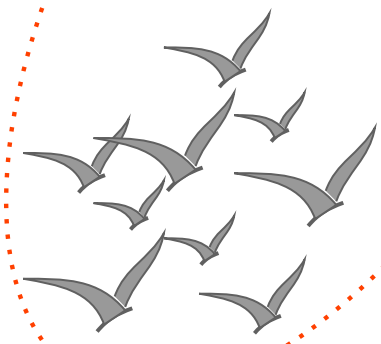
Outline

1. **timed automata**

2. **stochastic timed automata**

3. **partially observable probabilistic systems**

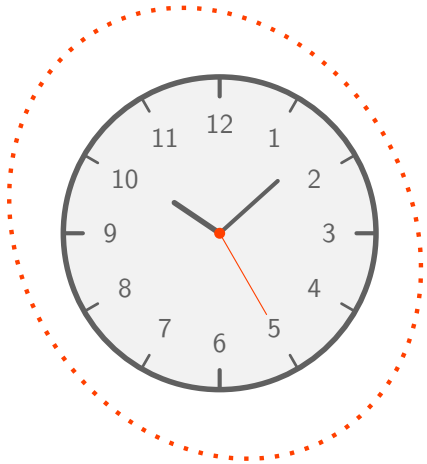


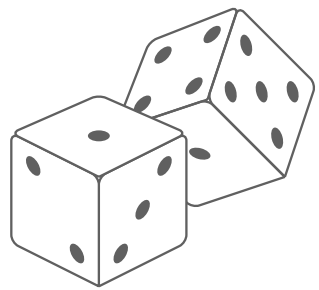


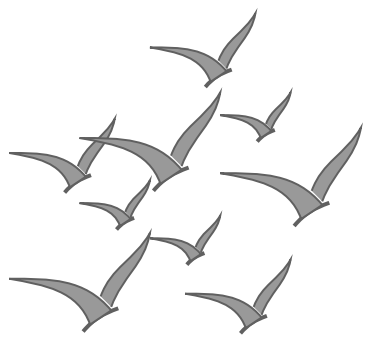
4. **parameterized probabilistic networks**

Outline

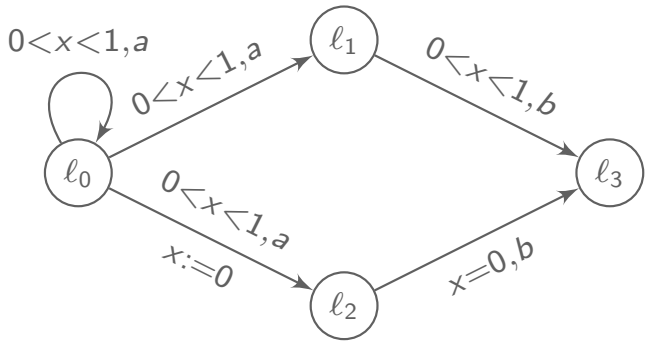
1. **timed automata**





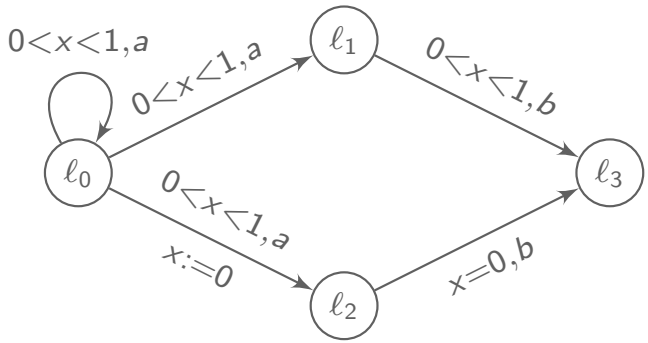


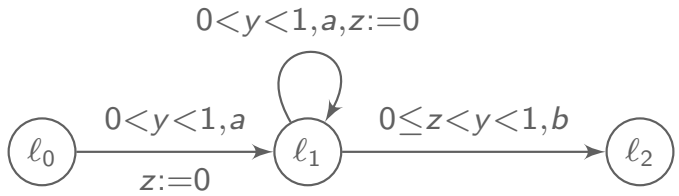
Determinizing timed automata



$(a,.5)(b,.5)$ read on two paths

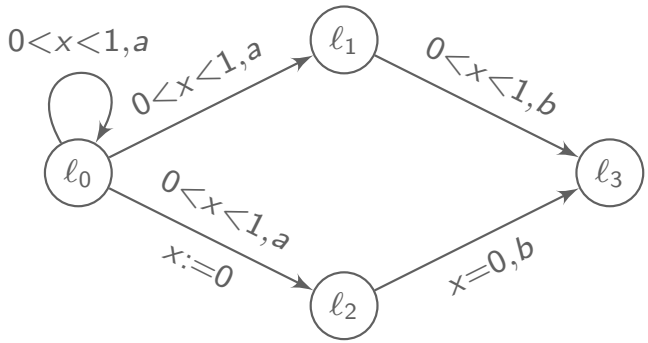
Determinizing timed automata

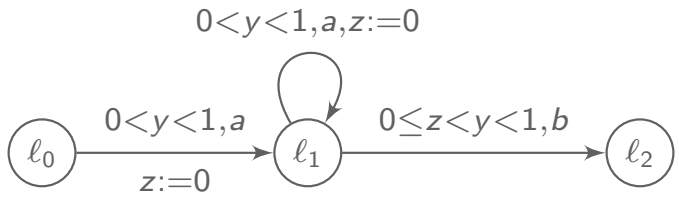




$(a,.5)(b,.5)$ read on two paths

Determinizing timed automata



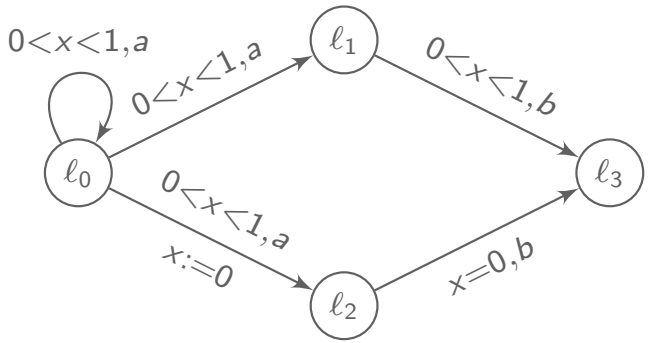


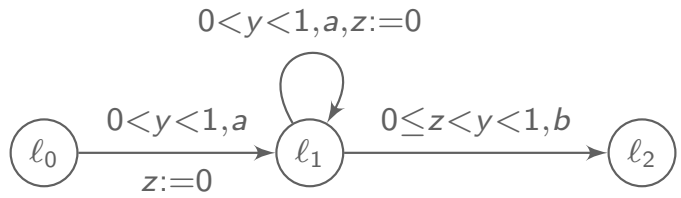
$(a,.5)(b,.5)$ read on two paths

Motivations for determinization

simpler model, easy complementation, offline monitor synthesis

Determinizing timed automata





$(a,.5)(b,.5)$ read on two paths

Motivations for determinization

simpler model, easy complementation, offline monitor synthesis

Hard problem for timed automata

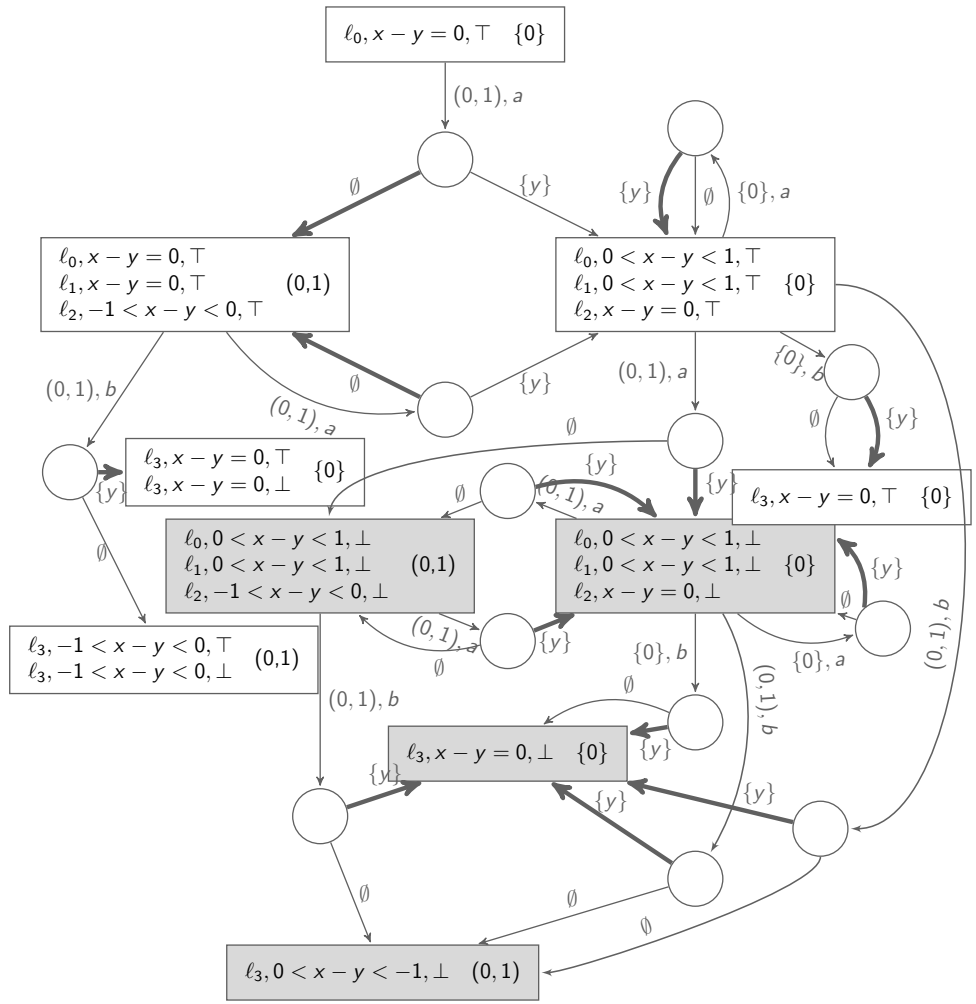
- determinization unfeasible in general
- determinizability undecidable

[AD94] Alur and Dill, *A theory of timed automata*. TCS, 1994.
[Tri06] Tripakis, *Folk theorems on the determinization and minimization of timed automata*, IPL, 2006.
[Fin06] Finkel, *Undecidable problems about timed automata*, Formats'06.

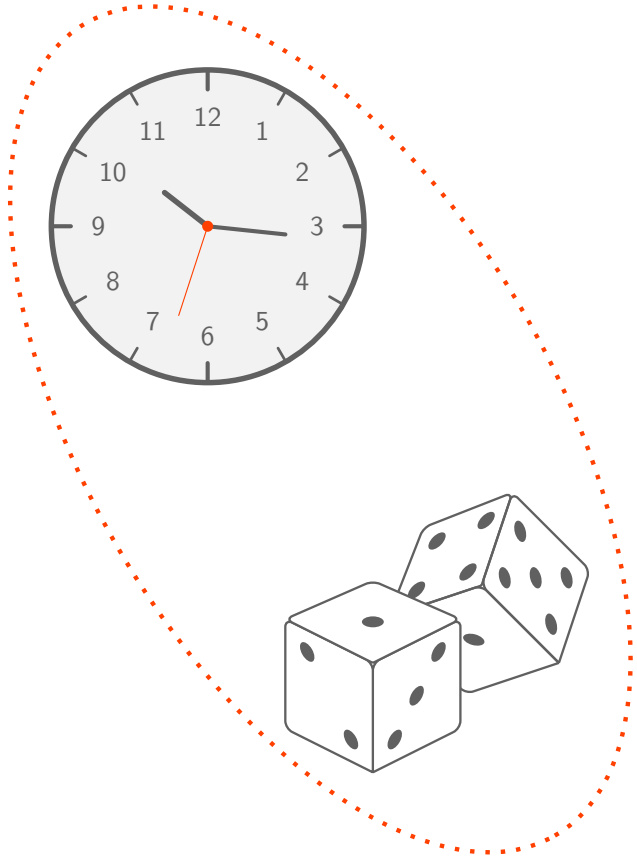
Game-based over-approximation algorithm

[FoSSaCS'11, FMSD'15]
w. Jéron, Krichen, Stainer
Amélie Stainer's PhD thesis

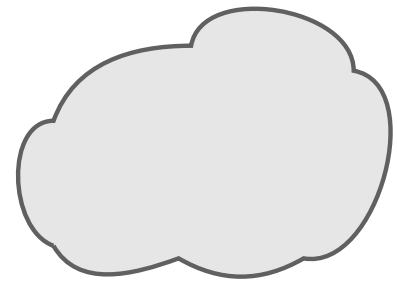
- exact determinization or over-approximation
- subsumes exact determinization procedure w. Baier, Bouyer and Brihaye [ICALP'09]
- no complexity overhead
- application to offline test generation w. Jéron, Krichen and Stainer [TACAS'11, LMCS'12]

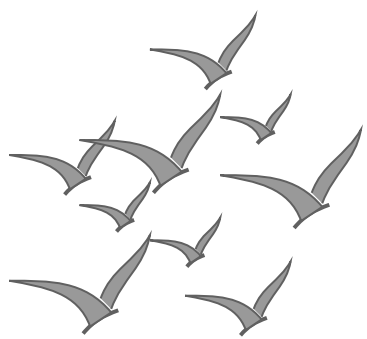


Outline

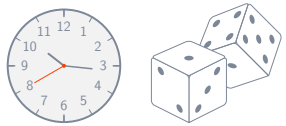


❷ **stochastic timed automata**





Mixing time and probabilities



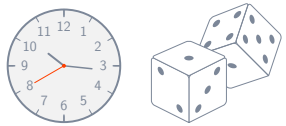
Two complementary views

1. probabilistic model and real-time property
   model: CTMC; property: CSL, CSL^{TA}, or timed automata
2. probabilistic & timed model
   stochastic Petri nets, probabilistic timed automata,
   probabilistic real-time systems

[BHHK03] Baier *et al.*, *Model checking algorithms for continuous-time Markov chains*. IEEE TSE, 2003.
[DHS09] Donatelli, Haddad and Sproston, *Model checking timed and stochastic properties with CSL^{TA}*, IEEE TSE, 2009.

[KNSS02] Kwiatkowska *et al.*, *Automatic verification of real-time systems with discrete probability distributions*, TCS, 2002.
[ACD91] Alur, Courcoubetis and Dill, *Model-checking for probabilistic real-time systems*, ICALP'91.

Mixing time and probabilities



Two complementary views

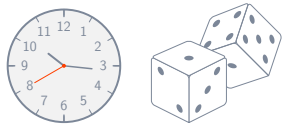
1. probabilistic model and real-time property
   model: CTMC; property: CSL, CSL^{TA}, or timed automata
2. probabilistic & timed model
   stochastic Petri nets, probabilistic timed automata,
   probabilistic real-time systems

Stochastic timed automata: timed automata with random delays

[BHHK03] Baier *et al.*, *Model checking algorithms for continuous-time Markov chains*. IEEE TSE, 2003.
[DHS09] Donatelli, Haddad and Sproston, *Model checking timed and stochastic properties with CSL^{TA}*, IEEE TSE, 2009.

[KNSS02] Kwiatkowska *et al.*, *Automatic verification of real-time systems with discrete probability distributions*, TCS, 2002.
[ACD91] Alur, Courcoubetis and Dill, *Model-checking for probabilistic real-time systems*, ICALP'91.

Mixing time and probabilities



Two complementary views

1. probabilistic model and real-time property
   model: CTMC; property: CSL, CSL^{TA}, or timed automata
2. probabilistic & timed model
   stochastic Petri nets, probabilistic timed automata,
   probabilistic real-time systems

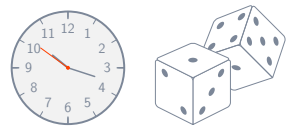
Stochastic timed automata: timed automata with random delays

- probabilistic choice between events — extends CTMC
- non-deterministic choice between events — extends CTMDP

[BHHK03] Baier *et al.*, *Model checking algorithms for continuous-time Markov chains*. IEEE TSE, 2003.
[DHS09] Donatelli, Haddad and Sproston, *Model checking timed and stochastic properties with CSL^{TA}*, IEEE TSE, 2009.

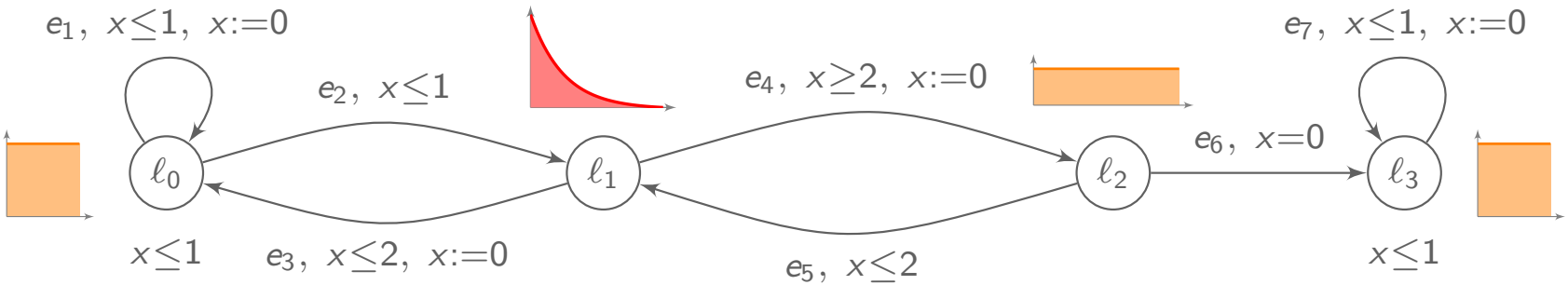
[KNSS02] Kwiatkowska *et al.*, *Automatic verification of real-time systems with discrete probability distributions*, TCS, 2002.
[ACD91] Alur, Courcoubetis and Dill, *Model-checking for probabilistic real-time systems*, ICALP'91.

Model checking STA



[FSTTCS'07, LICS'08, QEST'08, QEST'13, LMCS'14]

w. Baier, Bouyer, Brihaye, et al.



almost-sure satisfaction: $\mathbb{P}(\Box\neg\ell_3) = 1$

pruned region Markov chain abstraction

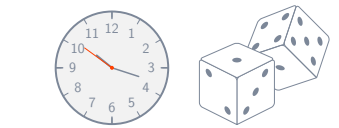
correct for restricted classes of STA

quantitative analysis: $\mathbb{P}(\Diamond^{\leq 4}\ell_2) \approx 0.248$

refined Markov chain with memoryless regions

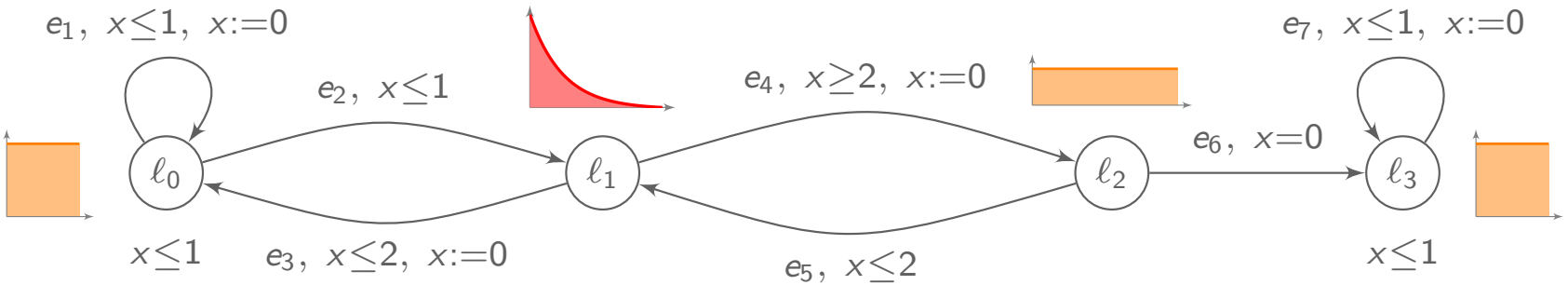
correct for even more restricted classes of STA

Model checking STA



[FSTTCS'07, LICS'08, QEST'08, QEST'13, LMCS'14]

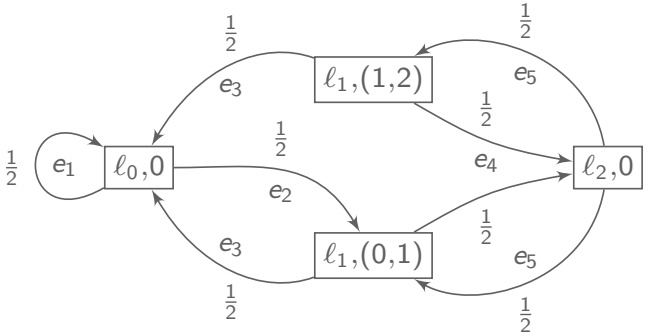
w. Baier, Bouyer, Brihaye, et al.



almost-sure satisfaction: $\mathbb{P}(\Box\neg\ell_3) = 1$

pruned region Markov chain abstraction

correct for restricted classes of STA



quantitative analysis: $\mathbb{P}(\Diamond^{\leq 4}\ell_2) \approx 0.248$

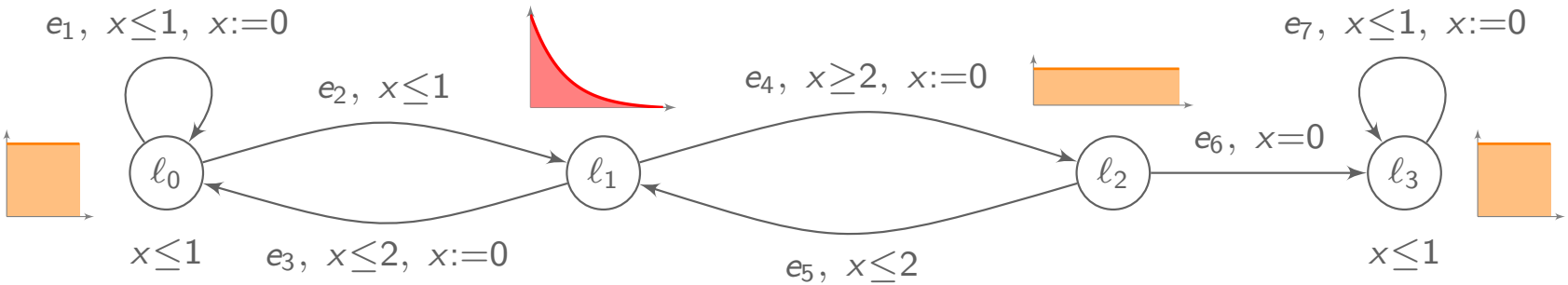
refined Markov chain with memoryless regions

correct for even more restricted classes of STA

Model checking STA

[FSTTCS'07, LICS'08, QEST'08, QEST'13, LMCS'14]

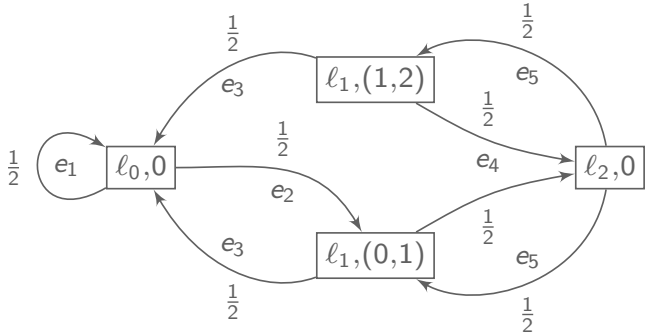
w. Baier, Bouyer, Brihaye, et al.



almost-sure satisfaction: $\mathbb{P}(\Box\neg\ell_3) = 1$

pruned region Markov chain abstraction

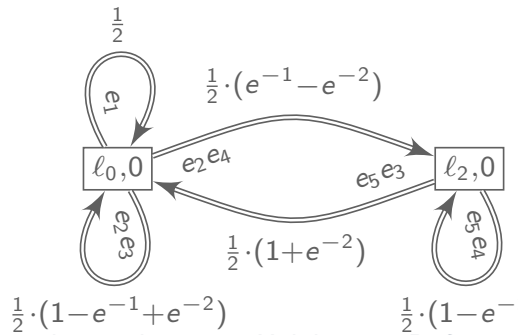
correct for restricted classes of STA



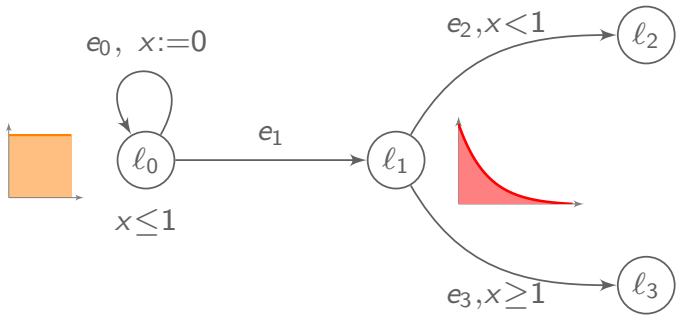
quantitative analysis: $\mathbb{P}(\Diamond^{\leq 4}\ell_2) \approx 0.248$

refined Markov chain with memoryless regions

correct for even more restricted classes of STA



Controlling STA



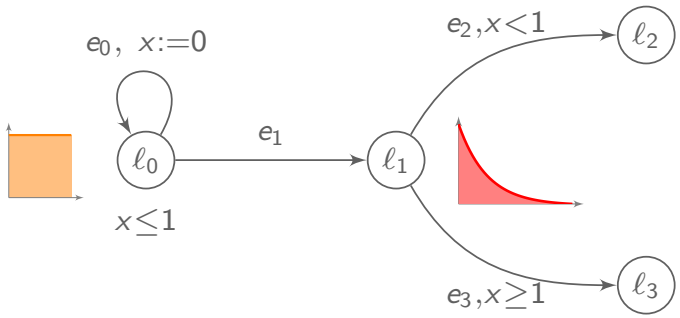
[Formats'12, QEST'14]
w. Brihaye, Genest, Schewe

no optimal scheduler to maximize probability to reach ℓ_3

- existence of optimal scheduler for time-bounded reachability
  $\sup_\sigma \mathbb{P}_\sigma(\Diamond^{\leq 3.2}\ell_3)$ is attained by a memoryless deterministic scheduler

- decidability of limit-sure time-unbounded reachability
  whether $\sup_\sigma \mathbb{P}_\sigma(\Diamond\ell_3) = 1$ is decidable in PTIME

Controlling STA



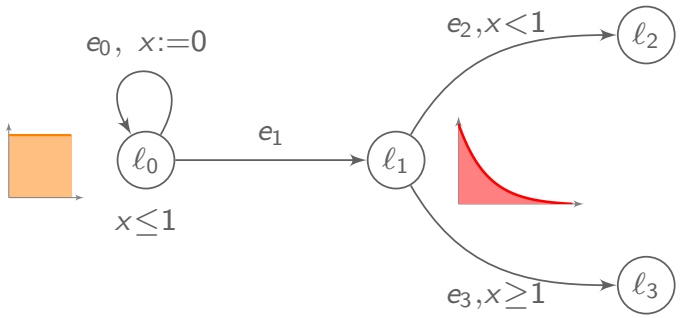
[Formats'12, QEST'14]
w. Brihaye, Genest, Schewe

no optimal scheduler to maximize probability to reach ℓ_3

- existence of optimal scheduler for time-bounded reachability
  $\sup_\sigma \mathbb{P}_\sigma(\Diamond^{\leq 3.2}\ell_3)$ is attained by a memoryless deterministic scheduler

- decidability of limit-sure time-unbounded reachability
  whether $\sup_\sigma \mathbb{P}_\sigma(\Diamond\ell_3) = 1$ is decidable in PTIME

Controlling STA

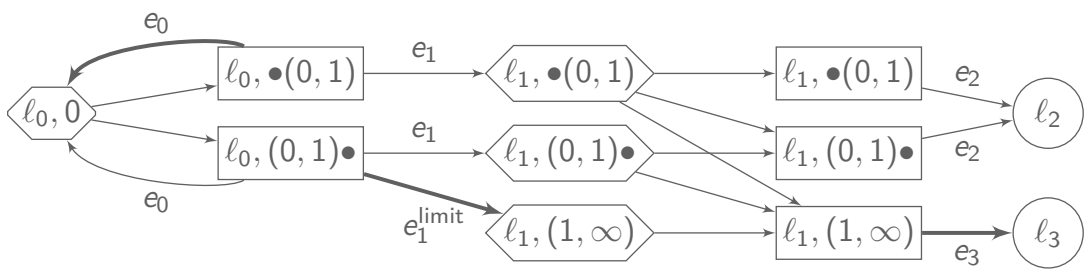


[Formats'12, QEST'14]
w. Brihaye, Genest, Schewe

no optimal scheduler to maximize probability to reach ℓ_3

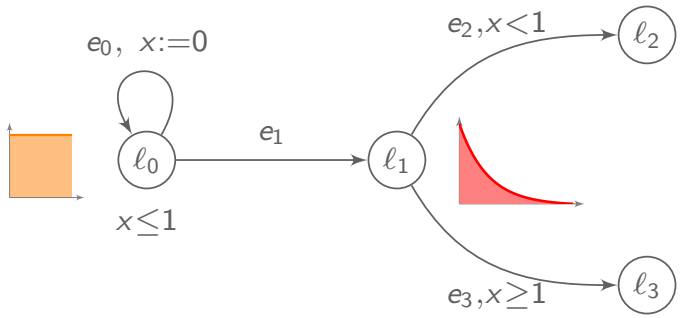
- existence of optimal scheduler for time-bounded reachability
  $\sup_\sigma \mathbb{P}_\sigma(\Diamond^{\leq 3.2}\ell_3)$ is attained by a memoryless deterministic scheduler

- decidability of limit-sure time-unbounded reachability
  whether $\sup_\sigma \mathbb{P}_\sigma(\Diamond\ell_3) = 1$ is decidable in PTIME

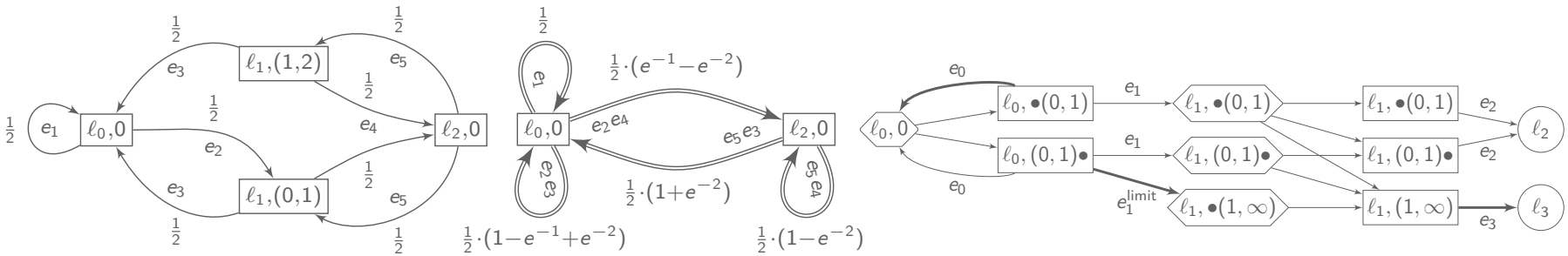


Stochastic timed automata: summary

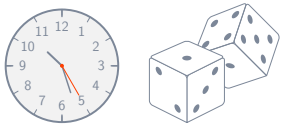
- timed automata with random delays



- refinements of the region abstraction to decide various model checking and control problems (for restricted classes)



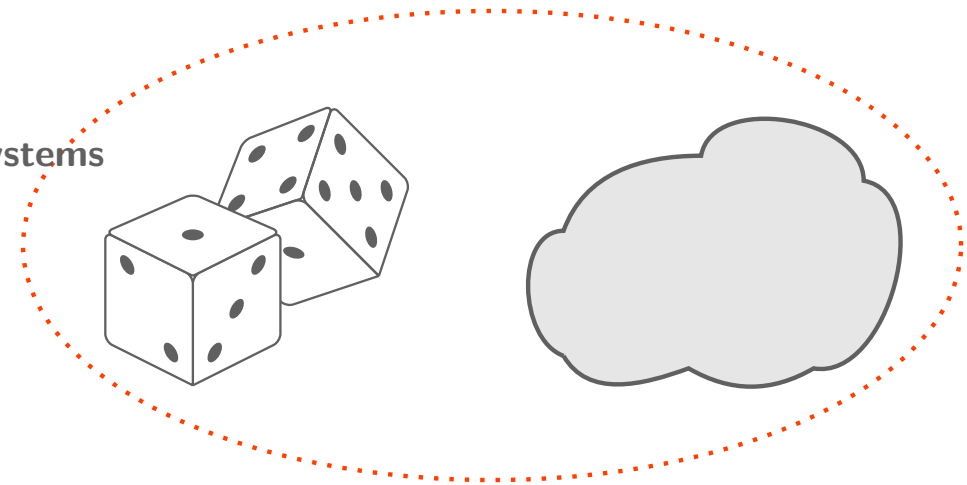
Stochastic timed automata: perspectives

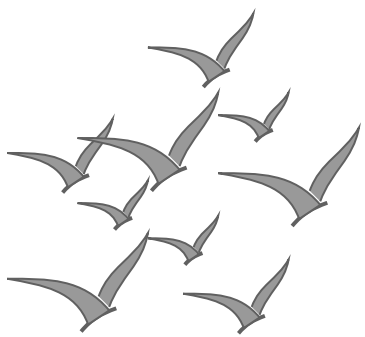


- an intriguing open question
  - decidability of almost-sure model checking for general STA?
- controlling STA for qualitative objectives
  - Büchi condition positively already harder than limit-sure reachability
- controlling *reactive* STA for quantitative objectives
  - approximation scheme based on finite attractor property?

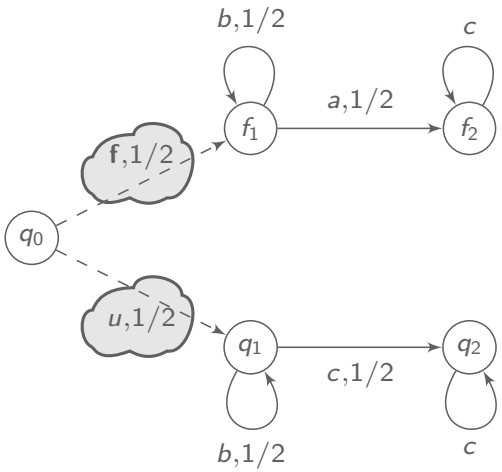
Outline

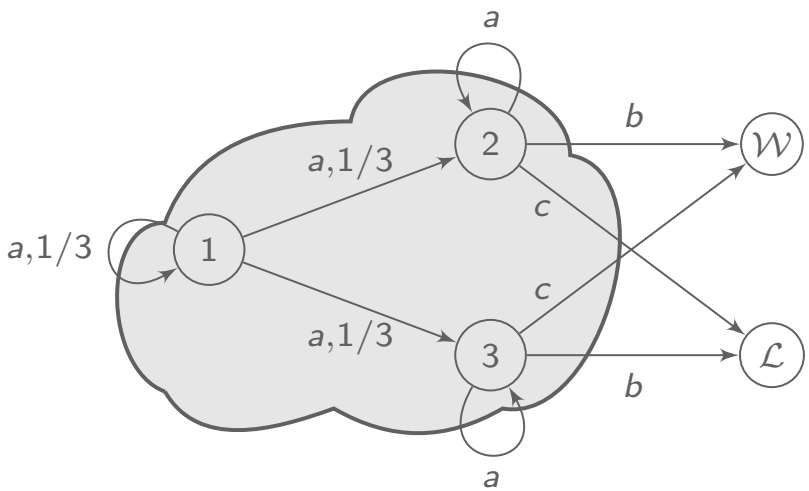
❸ **partially observable probabilistic systems**





Partially observable probabilistic systems

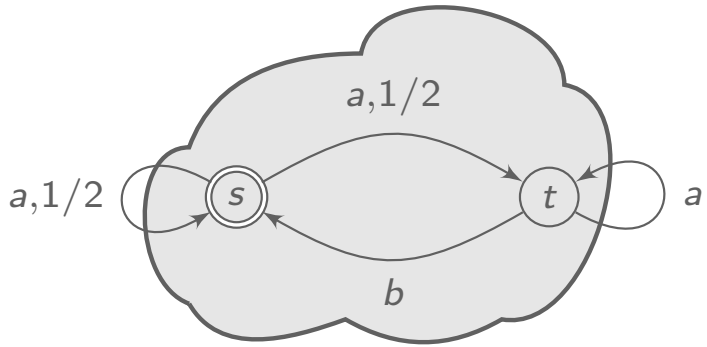




- monitoring issues: fault diagnosis
- control problems: probability optimization for a given objective
- language-theory: languages defined by probabilistic automata

[Rab63] Rabin, *Probabilistic automata*. I&C, 1963.
[Ast65] Aström, *Optimal control of Markov decision processes with incomplete state estimation*, JMAA, 1965.
[Paz71] Paz, *Introduction to probabilistic automata*, Academic Press, 1971.
[TT05] Thorsley and Teneketzis, *Diagnosability of stochastic discrete-event systems*, IEEE TAC, 2005.

Probabilistic Büchi automata



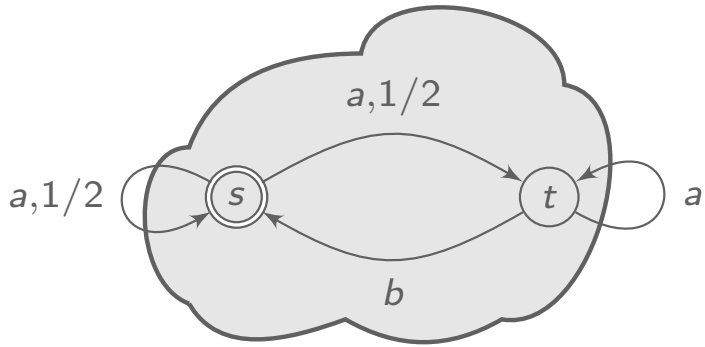
[FoSSaCS'08, JACM'12]
w. Baier, Größer

probabilistic acceptors for ω-languages

$$\mathcal{L}(\mathcal{A}) = \{w \in \Sigma^\omega \mid \mathbb{P}(w \text{ accepted}) > 0\}$$

- language depends on probability values
- closure under complement
- undecidability of emptiness

Probabilistic Büchi automata



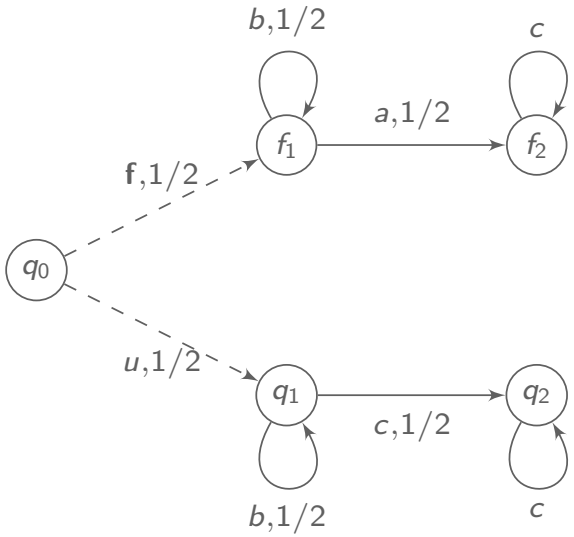
[FoSSaCS'08, JACM'12]
w. Baier, Größer

probabilistic acceptors for ω-languages

$$\mathcal{L}(\mathcal{A}) = \{w \in \Sigma^\omega \mid \mathbb{P}(w \text{ accepted}) > 0\}$$

- language depends on probability values
- closure under complement
- undecidability of emptiness

Fault diagnosis in probabilistic systems



[FoSSaCS'14, FSTTCS'14]
w. Haddad et al.
Engel Lefaucheux's PhD thesis

Objective: given observation, determine whether a fault **f** occurred

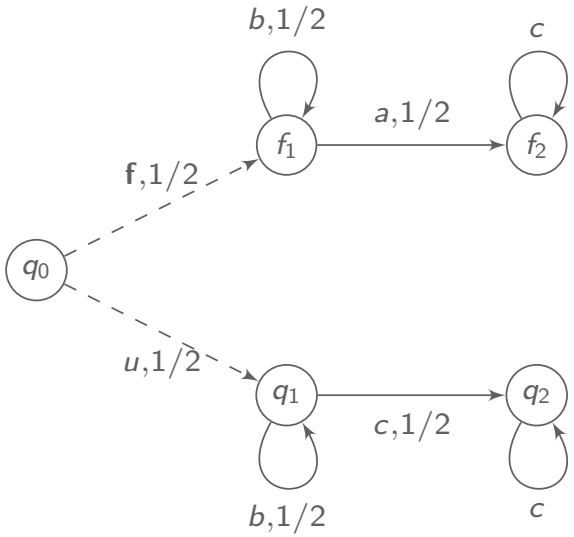
Probabilistic diagnosis: almost-sure detection of faults

- semantical study of relevant diagnosability notions
- diagnosability is PSPACE-complete

Active probabilistic diagnosis: control the system so that it is diagnosable

- active diagnosability is EXPTIME-complete
- undecidable if correct runs must have positive probability

Fault diagnosis in probabilistic systems



[FoSSaCS'14, FSTTCS'14]
w. Haddad et al.
Engel Lefaucheux's PhD thesis

Objective: given observation, determine whether a fault **f** occurred

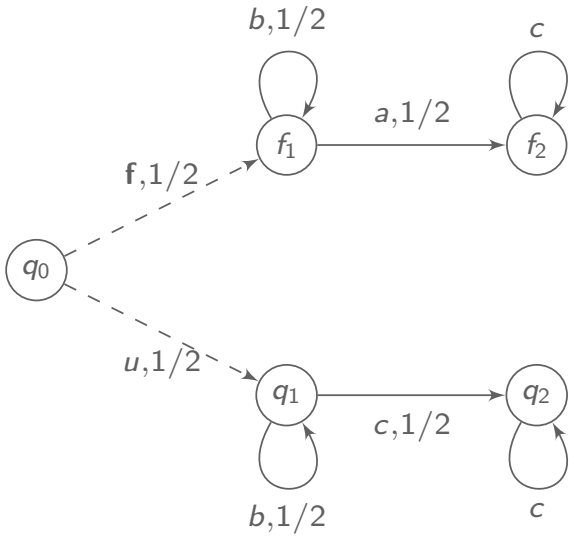
Probabilistic diagnosis: almost-sure detection of faults

- semantical study of relevant diagnosability notions
- diagnosability is PSPACE-complete

Active probabilistic diagnosis: control the system so that it is diagnosable

- active diagnosability is EXPTIME-complete
- undecidable if correct runs must have positive probability

Fault diagnosis in probabilistic systems



[FoSSaCS'14, FSTTCS'14]
w. Haddad et al.
Engel Lefaucheux's PhD thesis

Objective: given observation, determine whether a fault **f** occurred

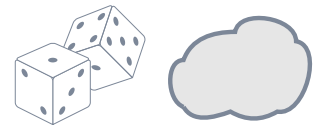
Probabilistic diagnosis: almost-sure detection of faults

- semantical study of relevant diagnosability notions
- diagnosability is PSPACE-complete

Active probabilistic diagnosis: control the system so that it is diagnosable

- active diagnosability is EXPTIME-complete
- undecidable if correct runs must have positive probability

Partial observation & probabilities: summary



Probabilistic Büchi automata

- language properties, undecidability of emptiness problem

Fault diagnosis for stochastic systems

- passive and active diagnosis

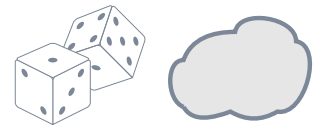
Partially observable MDP [FSTTCS'11] w. Genest

- cost optimization for almost-sure reachability

Stochastic games with signals [LICS'09] w. Genest and Gimbert

- qualitative determinacy for almost-sure reachability, safety or Büchi
- resolution and optimal strategy synthesis 2EXPTIME-complete
- memory requirements: from none to doubly exponential

Partial observation & probabilities: summary



Probabilistic Büchi automata

- language properties, undecidability of emptiness problem

Fault diagnosis for stochastic systems

- passive and active diagnosis

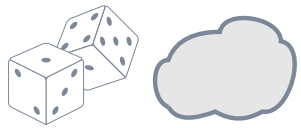
Partially observable MDP [FSTTCS'11] w. Genest

- cost optimization for almost-sure reachability

Stochastic games with signals [LICS'09] w. Genest and Gimbert

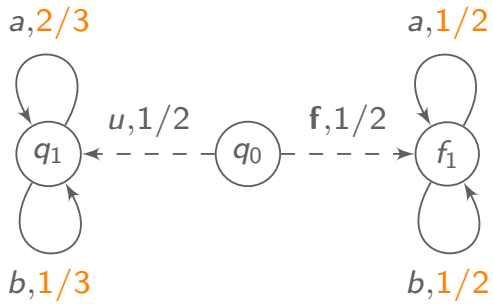
- qualitative determinacy for almost-sure reachability, safety or Büchi
- resolution and optimal strategy synthesis 2EXPTIME-complete
- memory requirements: from none to doubly exponential

Partial observation & probabilities: perspectives



Fault diagnosis: towards more quantitative questions

- accurate approximate diagnosability
- spatial optimization - sensor minimization
- temporal optimization - observation times minimization

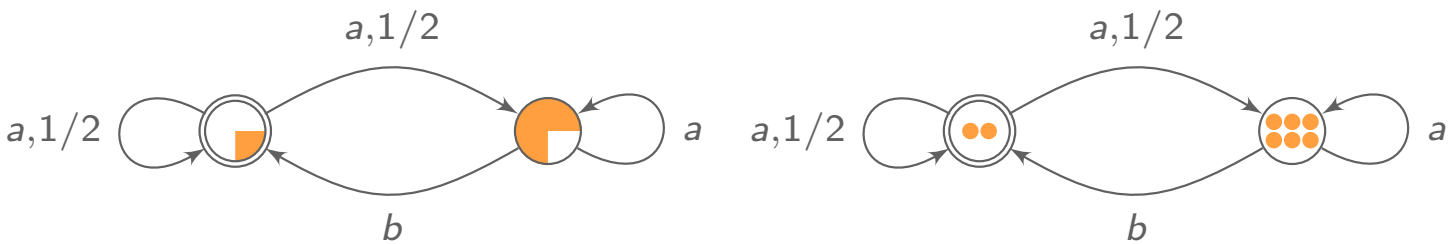


Partial observation *vs* no observation

- any difference from a decidability point of view?

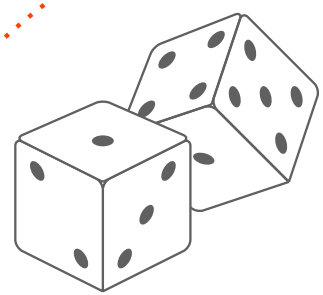
Alternative semantics for probabilistic automata

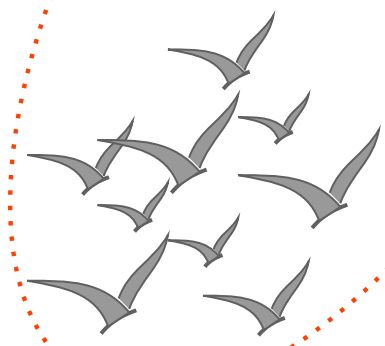
- continuous distributions approximated by large discrete sets



- link with parameterized verification

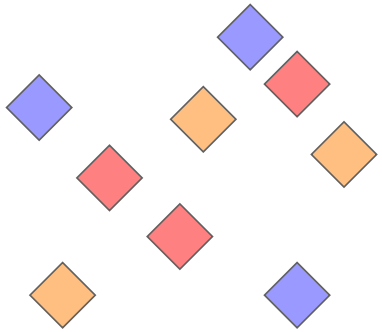
Outline

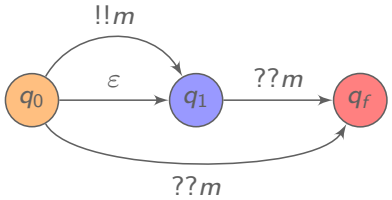




❹ **parameterized probabilistic networks**

Networks of many identical processes



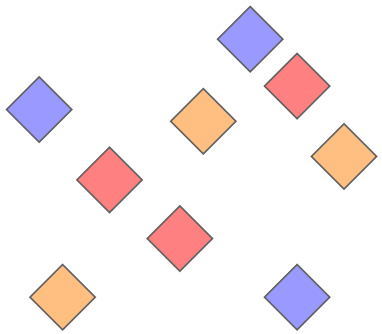


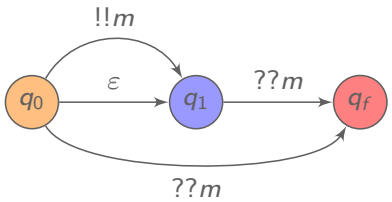
unknown number of nodes
all running same code
broadcast communications

Parameterized verification does the network satisfy its specification independently of the number of nodes?

[GS92] German and Sistla, *Reasoning about systems with many processes*, JACM 1992.
[EFM99] Esparza, Finkel and Mayr, *On the verification of broadcast protocols*, LICS'99.
[DSZ10] Delzanno, Sangnier and Zavaterro, *Parameterized verification of ad hoc networks*. CONCUR'00.
[Esp14] Esparza, *Keeping a crowd safe: on the complexity of parameterized verification*. STACS'14.

Networks of many identical processes





unknown number of nodes
all running same code
broadcast communications

Parameterized verification does the network satisfy its specification independently of the number of nodes?

Need for probabilities

- symmetry breaker in protocols

  random backoff time between retransmissions
- abstraction of unpredictable behaviour

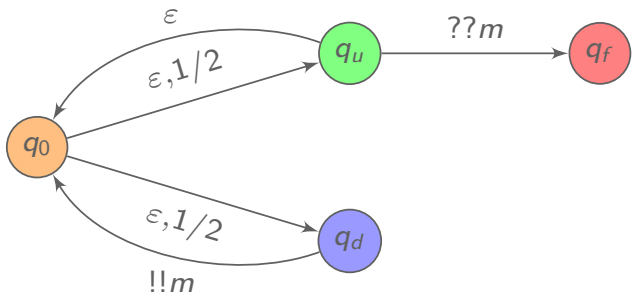
  message losses or node breakdowns

Challenge

parameter + non-determinism + probabilities

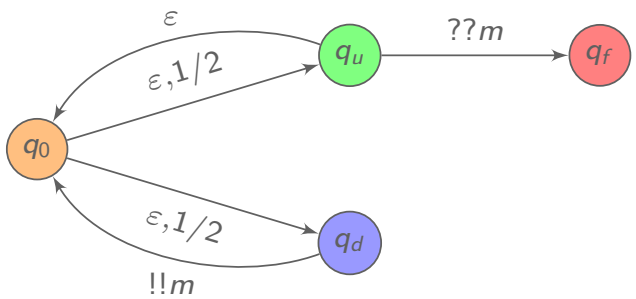
[GS92] German and Sistla, *Reasoning about systems with many processes*, JACM 1992.
[EFM99] Esparza, Finkel and Mayr, *On the verification of broadcast protocols*, LICS'99.
[DSZ10] Delzanno, Sangnier and Zavaterro, *Parameterized verification of ad hoc networks*. CONCUR'00.
[Esp14] Esparza, *Keeping a crowd safe: on the complexity of parameterized verification*. STACS'14.

Probabilistic broadcast networks



unknown number of nodes
identical MDP
broadcast communications

Probabilistic broadcast networks



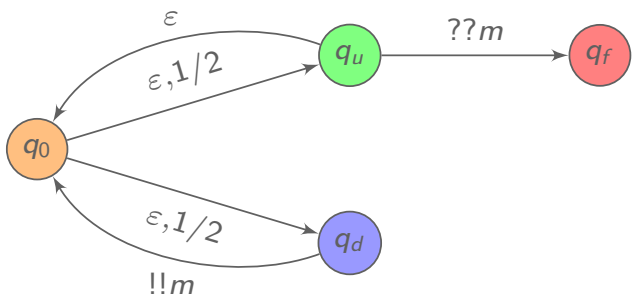
unknown number of nodes
identical MDP
broadcast communications

Scheduler chooses
active node, action, set of receivers, reception transitions

Qualitative parameterized verification

do there exist an initial configuration and a scheduler such that almost-surely a property holds?

Probabilistic broadcast networks



unknown number of nodes
identical MDP
broadcast communications

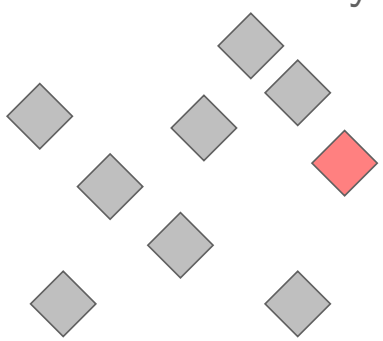
Scheduler chooses
active node, action, set of receivers, reception transitions

Qualitative parameterized verification

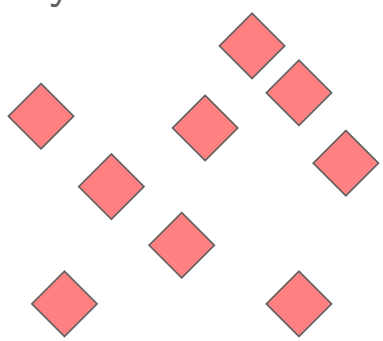
do there exist an initial configuration and a scheduler such that almost-surely a property holds?

Properties

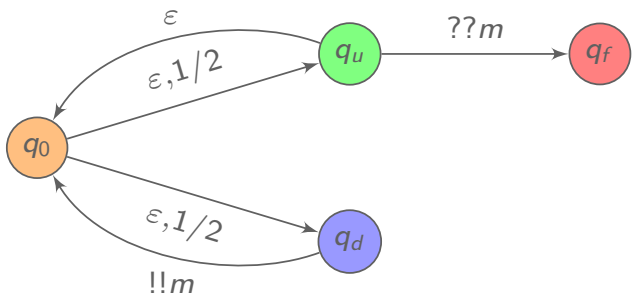
state reachability



synchronization

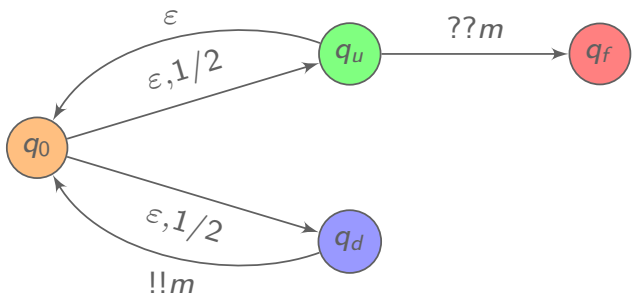


Qualitative parameterized verification



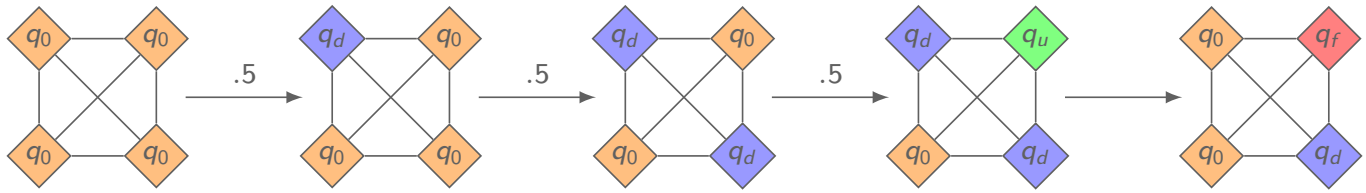
[FSTTCS'13, FoSSaCC'14]
w. Fournier, Sangnier
Paulin Fournier's PhD thesis

Qualitative parameterized verification



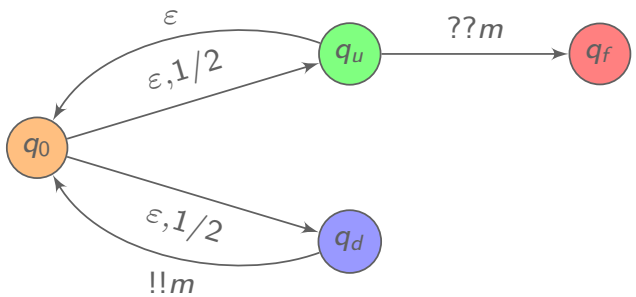
[FSTTCS'13, FoSSaCC'14]
w. Fournier, Sangnier
Paulin Fournier's PhD thesis

- fixed size clique networks



qualitative reachability and synchronization pbs mostly undecidable

Qualitative parameterized verification

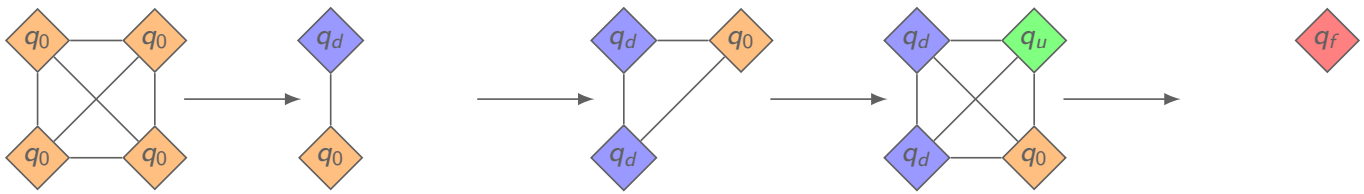


[FSTTCS'13, FoSSaCC'14]
w. Fournier, Sangnier
Paulin Fournier's PhD thesis

- fixed size clique networks

qualitative reachability and synchronization pbs mostly undecidable

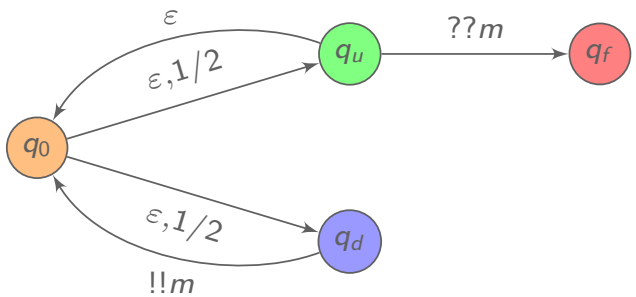
- dynamic clique networks



qualitative reachability and synchronization pbs decidable and NPR

finite attractor in probabilistic well-structured transition system

Qualitative parameterized verification



[FSTTCS'13, FoSSaCC'14]
w. Fournier, Sangnier
Paulin Fournier's PhD thesis

- fixed size clique networks

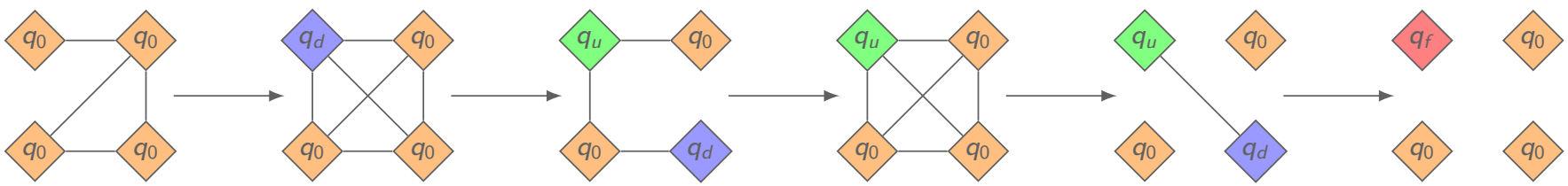
qualitative reachability and synchronization pbs mostly undecidable

- dynamic clique networks

qualitative reachability and synchronization pbs decidable and NPR

finite attractor in probabilistic well-structured transition system

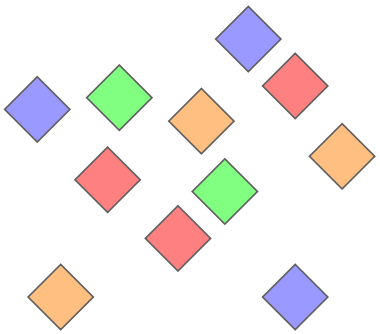
- fixed size reconfigurable networks

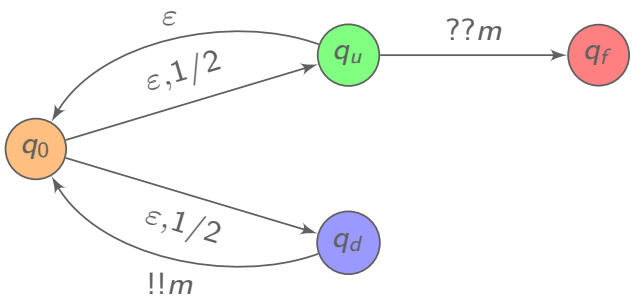


qualitative reachability pbs decidable, from PTIME to co-NP-complete

involved cases reduce to parity condition in game networks

Probabilistic networks: summary

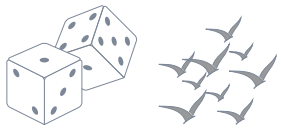




- networks of many identical probabilistic processes
- selective broadcast communications

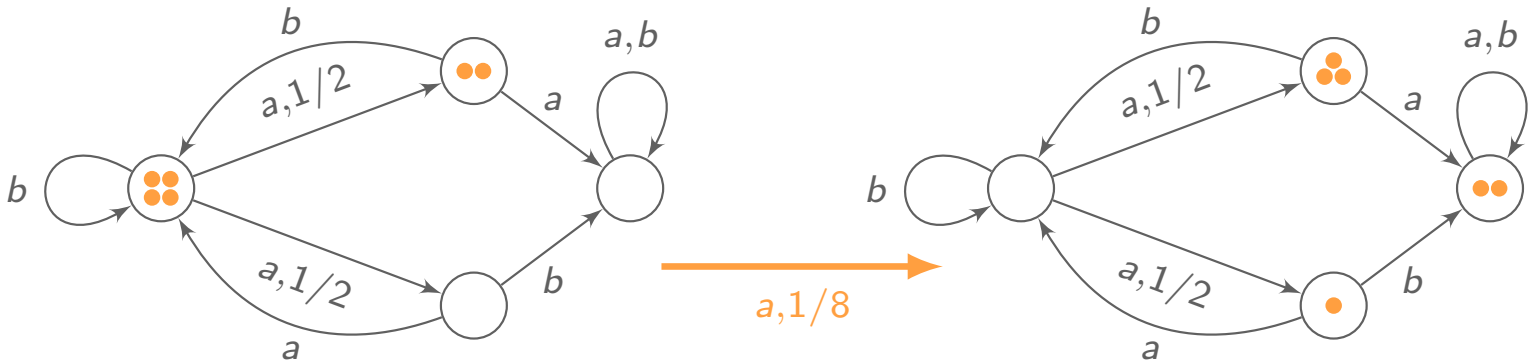
- decidability and complexity of
  qualitative parameterized reachability and synchronization problems

Probabilistic networks: perspectives



- probabilistic broadcast networks
  - quantitative analysis
  - richer properties, proportions

- uniform control of many identical MDP
  - no communication
  - same control policy for every MDP

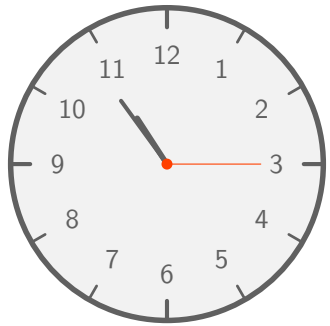


- distributed protocols
  - synthesis of correct-by-design protocols

Summary of contributions

❶ **timed automata**

game-based determinization



❷ **stochastic timed automata**

almost sure model checking

& quantitative analysis for subclasses

control issues for reachability objectives

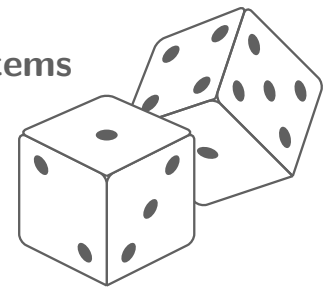
❸ **partially observable probabilistic systems**

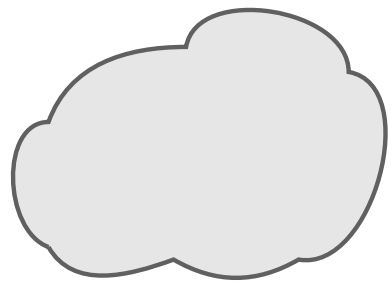
probabilistic Büchi automata

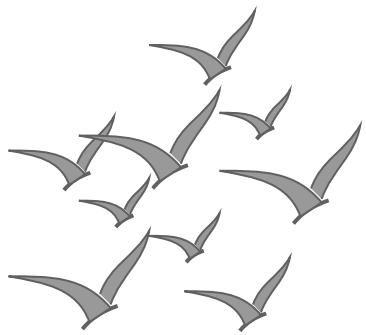
cost optimization in partially observable MDP

determinacy and complexity of stochastic games

passive and active probabilistic fault diagnosis







❹ **parameterized probabilistic networks**

qualitative reachability and synchronization

General perspectives

formal verification of
quantitative systems

General perspectives

More formal verification of
more quantitative systems

General perspectives

More formal verification of
more quantitative systems

more theory

- partial observation *vs* no observation
- qualitative model checking of general STA

more quantitative analysis

- controlling reactive STA for quantitative objectives
- quantified diagnosis and tradeoffs
- quantitative parameterized verification questions

more applications

- systems biology: uniform control of identical MDP
- distributed algo: synthesis of correct-by-design protocols
- security analysis: partial observation & probabilities