Parametrized verification of networks with many identical probabilistic processes

Paulin Fournier

ENS Cachan Antenne de Bretagne
Université de Rennes 1

December 5, 2012

Advisor : Nathalie Bertrand
Thierry Jeron

Team : Vertecs, INRIA

Parameterized Verification

Problems

- Models with an unknown parameter (*e.g.* size, probability)
- Standard verification for each instances of the parameter impossible

Parameterized Verification

Problems

- Models with an unknown parameter (*e.g.* size, probability)
- Standard verification for each instances of the parameter impossible

Solution: Parameterized verification

Verification for all the range of the parameter at once

Parameterized Verification

Problems

- Models with an unknown parameter (*e.g.* size, probability)
- Standard verification for each instances of the parameter impossible

Solution: Parameterized verification

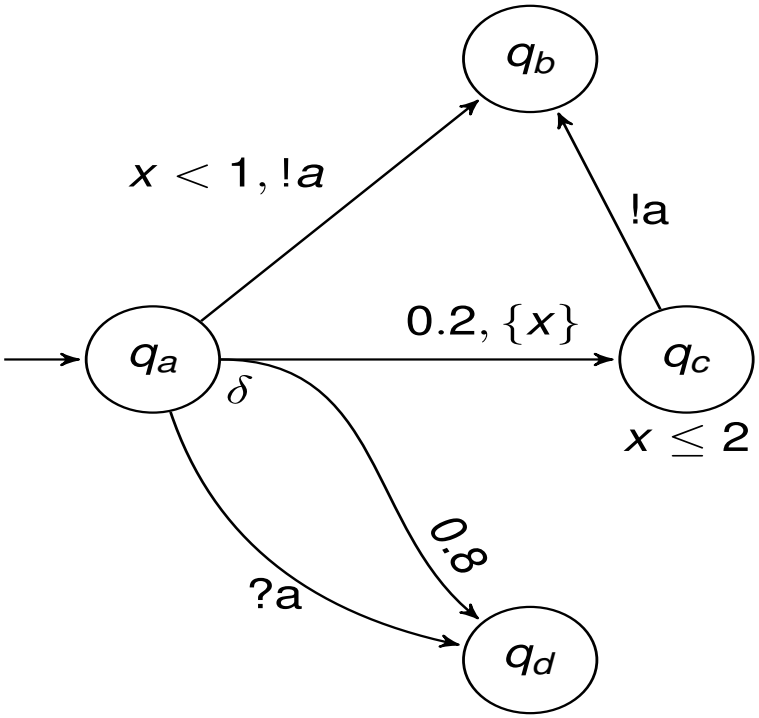
Verification for all the range of the parameter at once

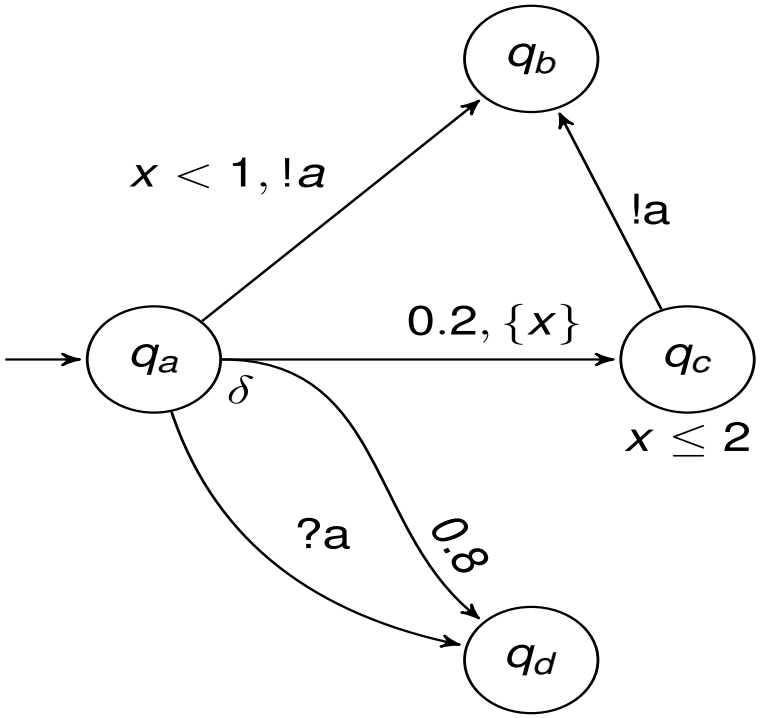
Our work

- Model: Probabilistic Timed Protocol
- Parameter: Number of processes
- Applications: Wireless sensor networks, Peer to peer, ...

The model: Probabilistic timed protocol

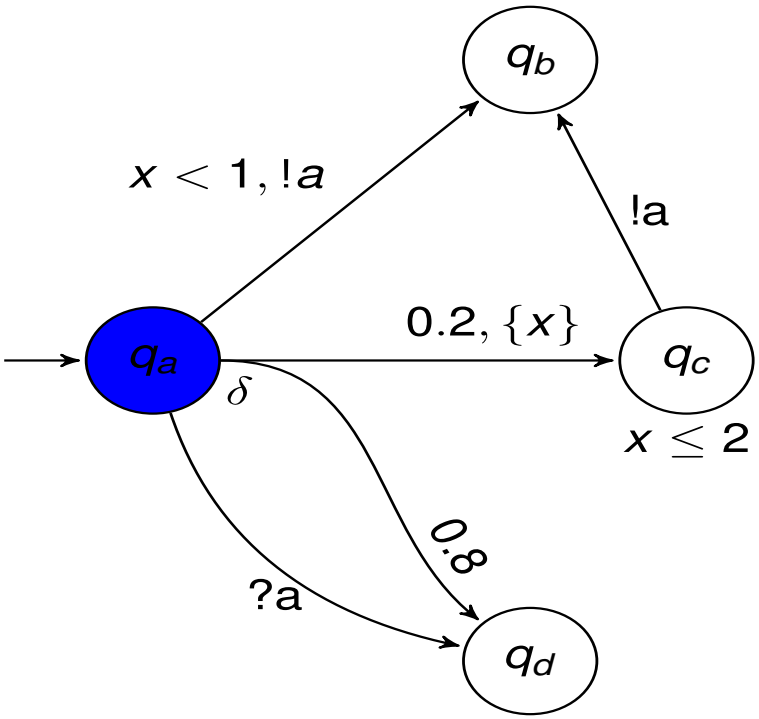
N identical processes in a **clique**.

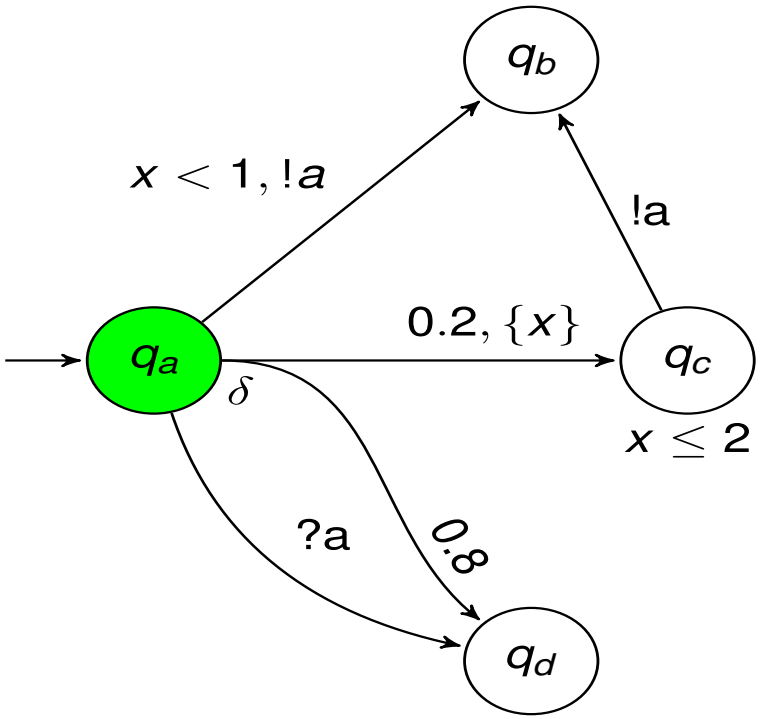




The model: Probabilistic timed protocol

N identical processes in a **clique**.



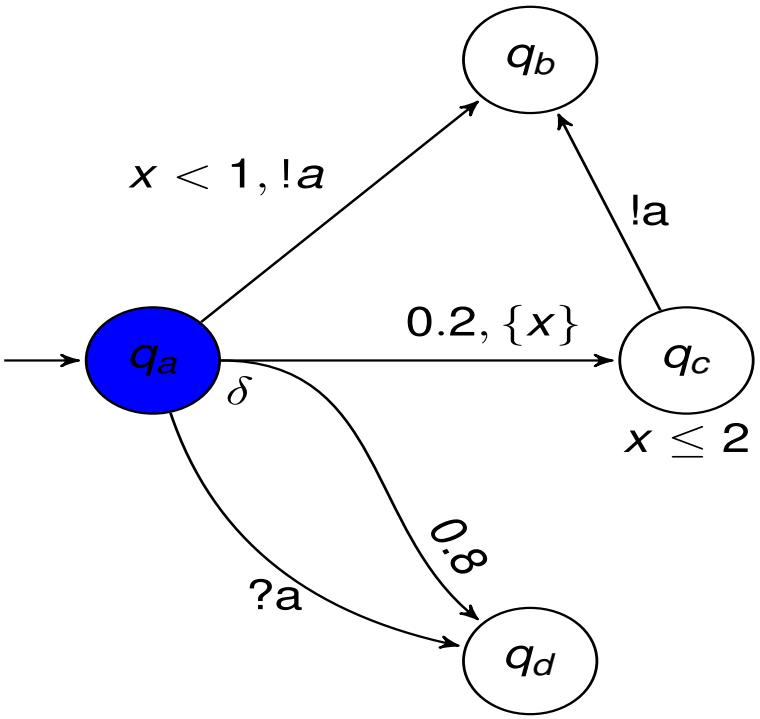


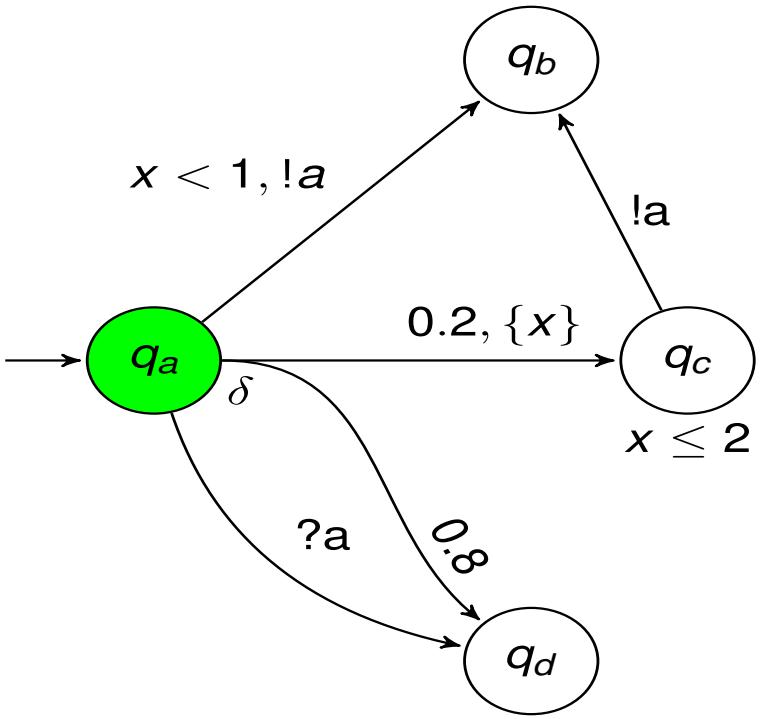
q_a 0

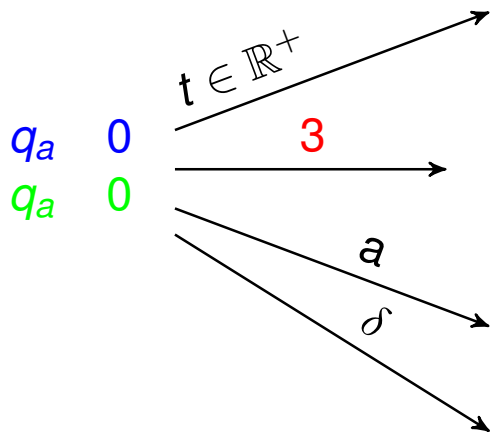
q_a 0

The model: Probabilistic timed protocol

N identical processes in a **clique**.

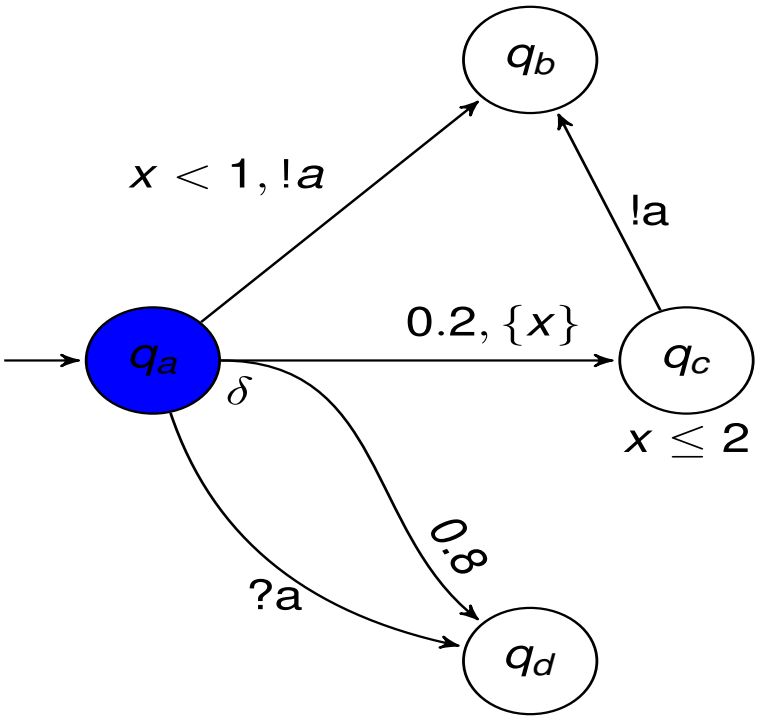


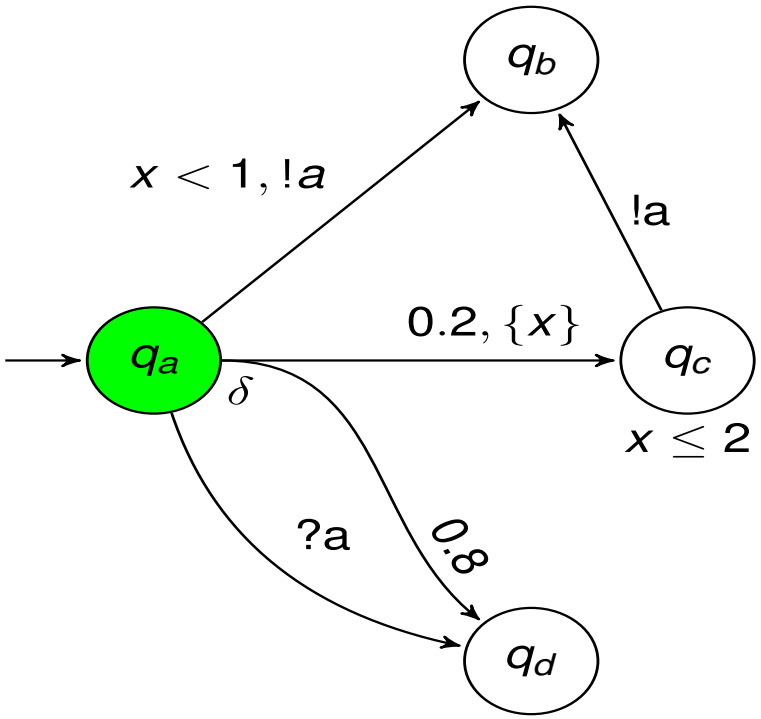


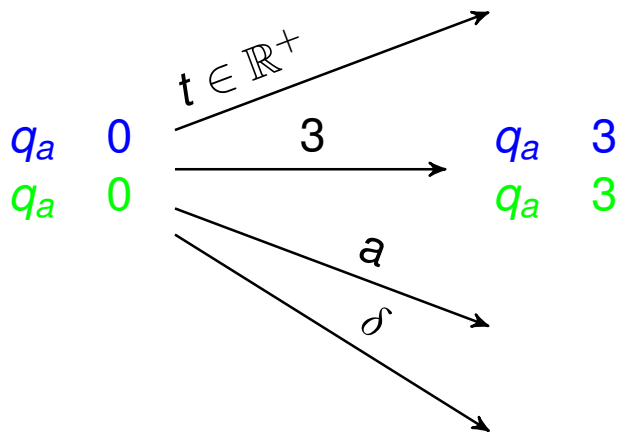


The model: Probabilistic timed protocol

N identical processes in a **clique**.

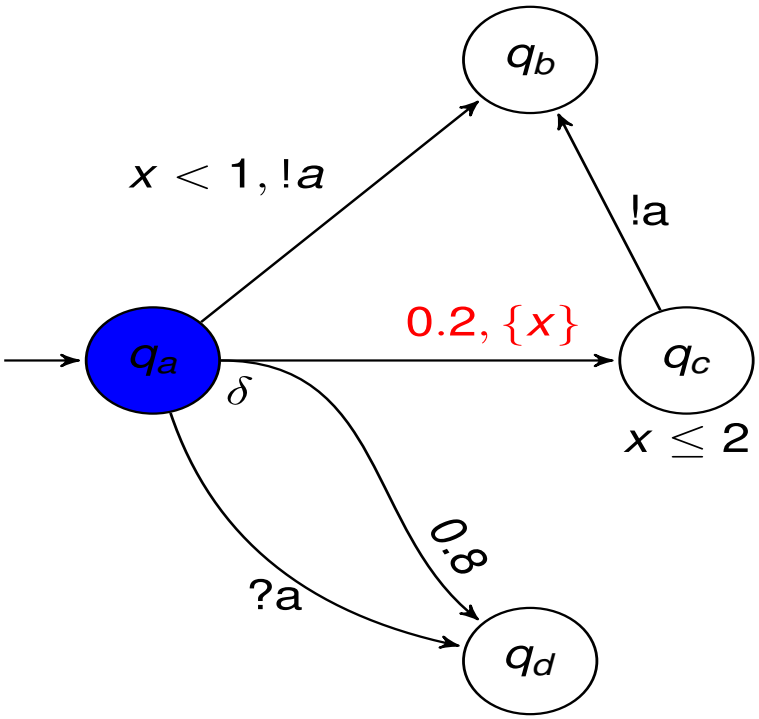


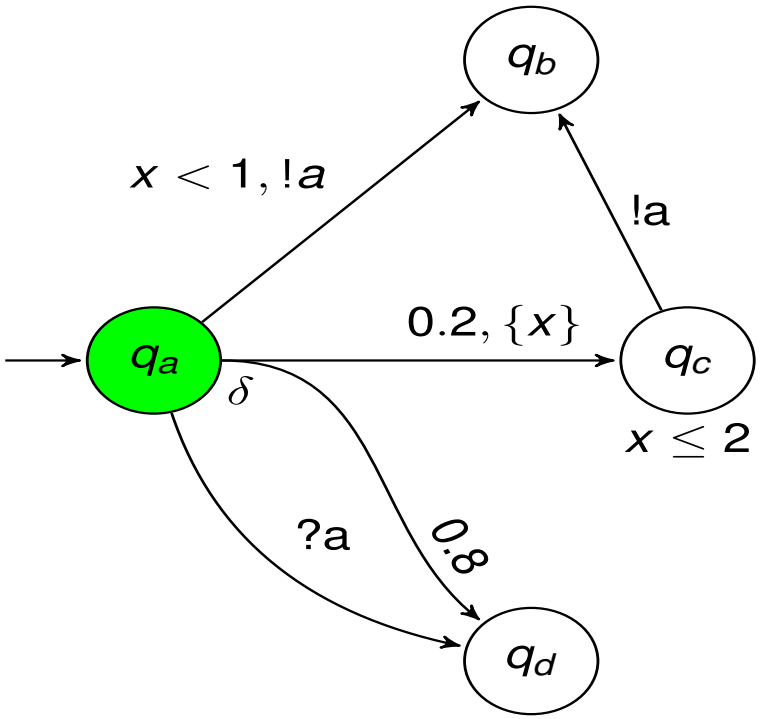


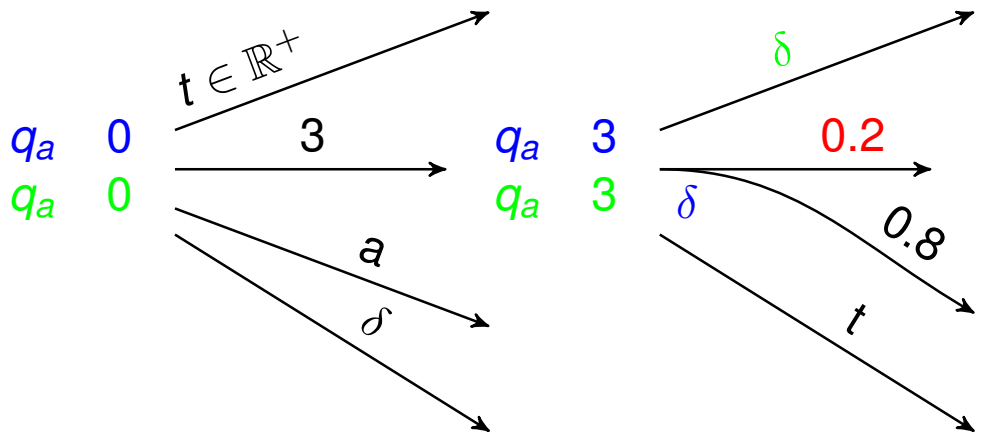


The model: Probabilistic timed protocol

N identical processes in a **clique**.

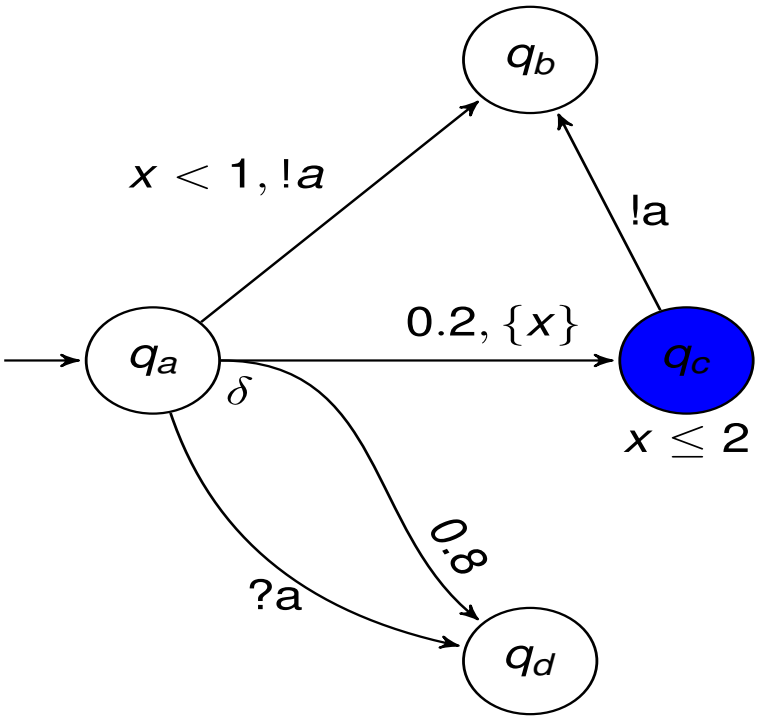


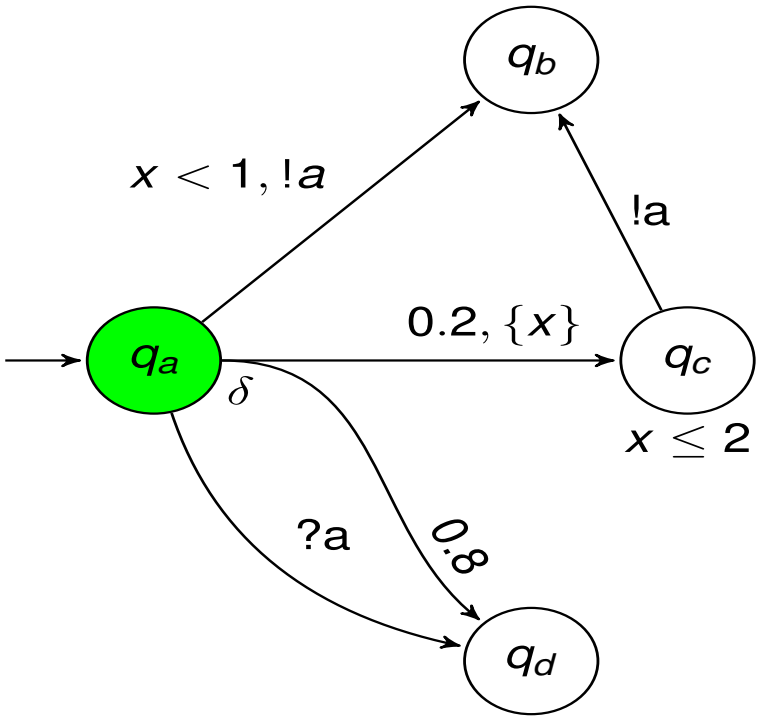


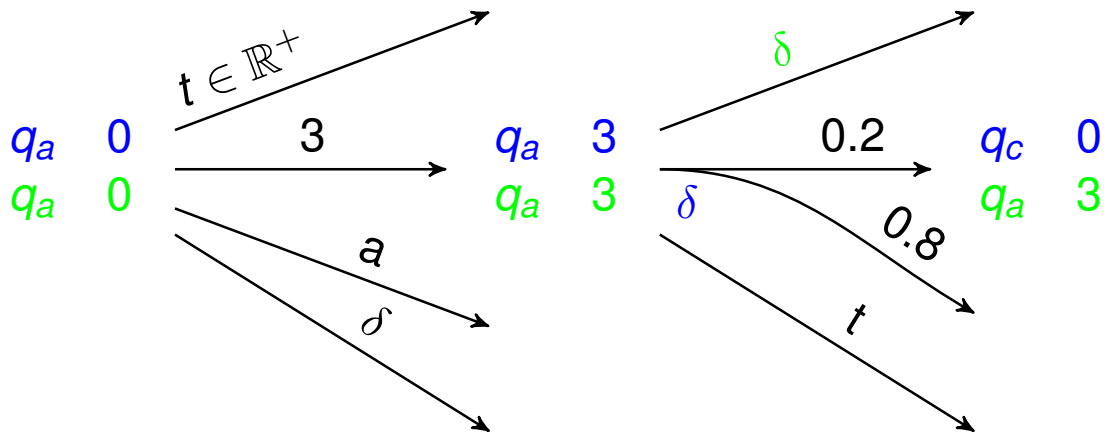


The model: Probabilistic timed protocol

N identical processes in a **clique**.

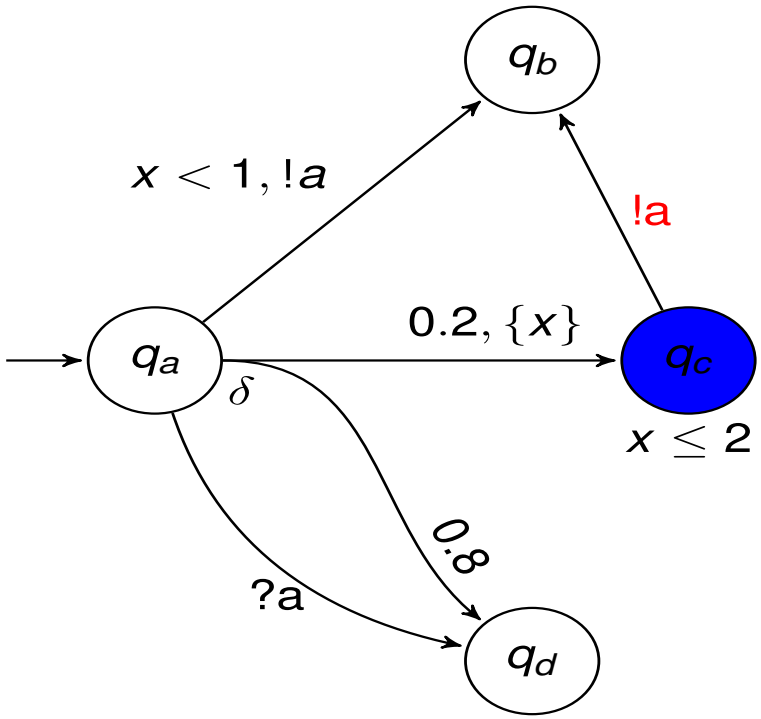


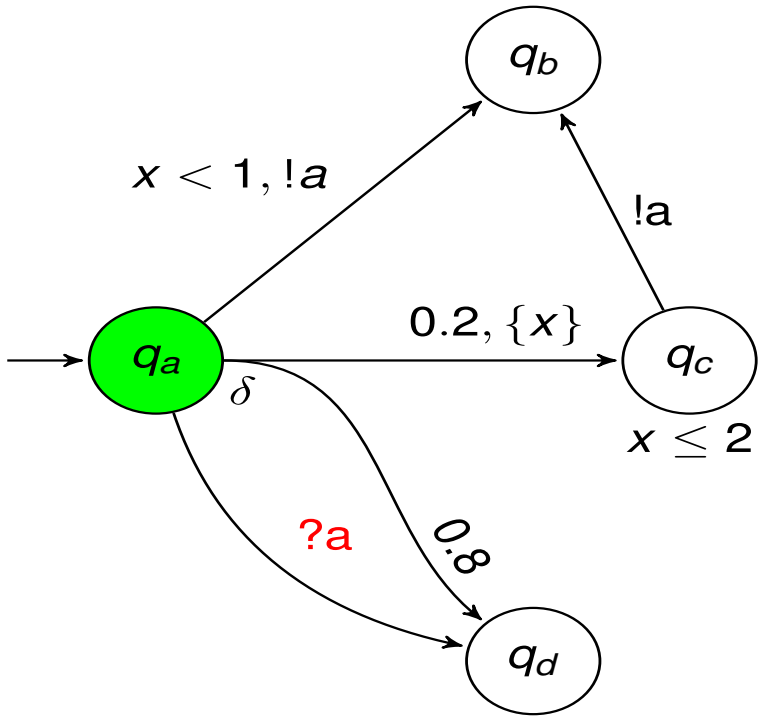


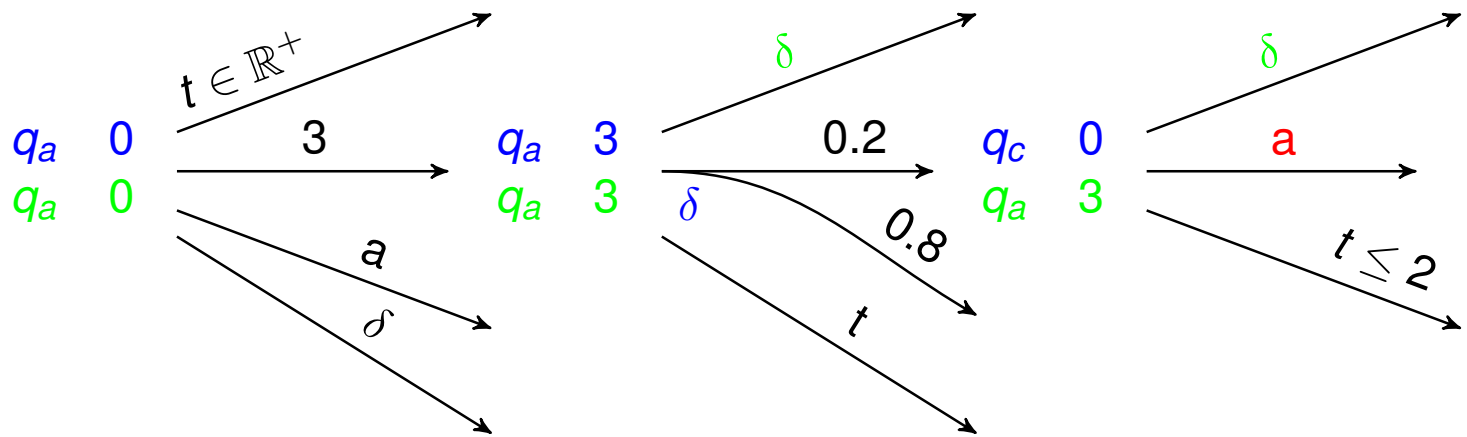


The model: Probabilistic timed protocol

N identical processes in a **clique**.

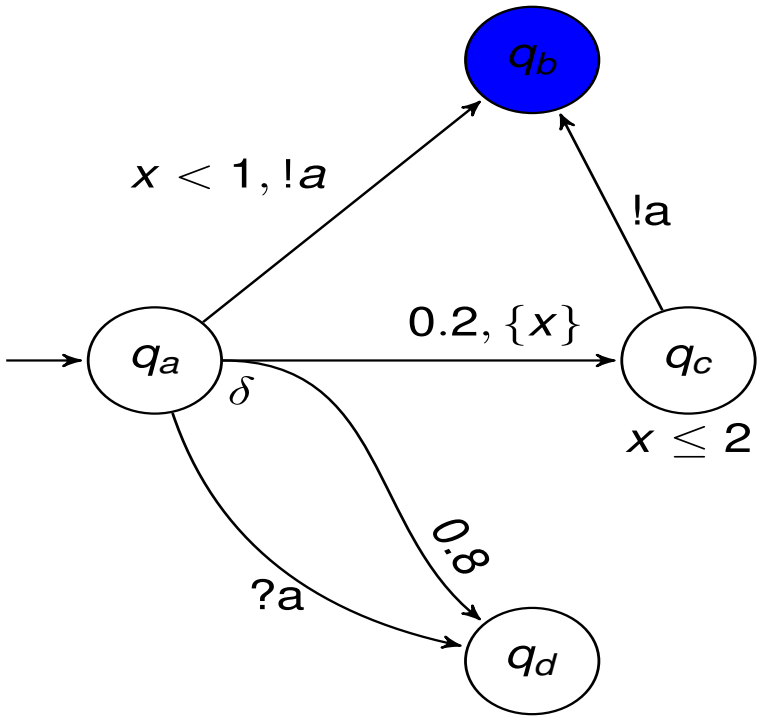


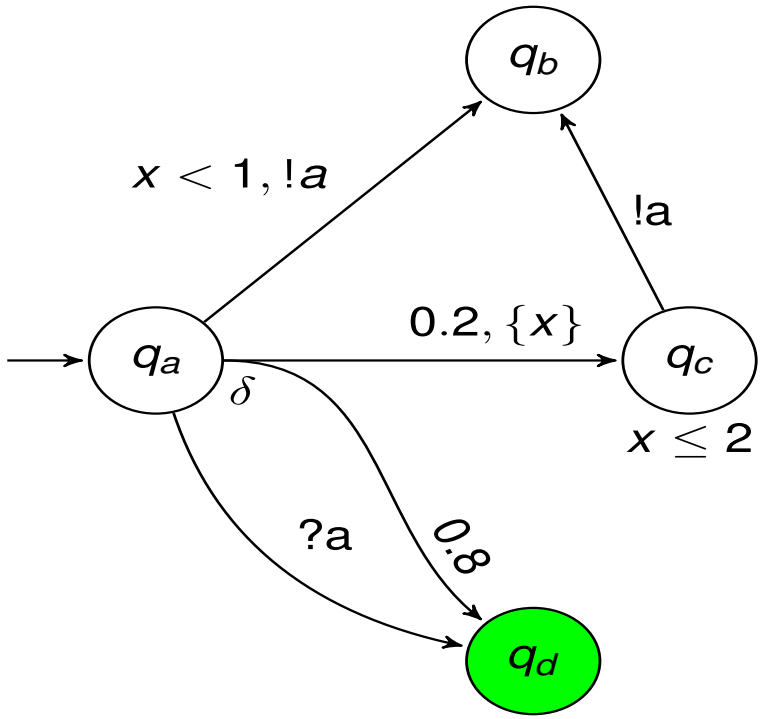


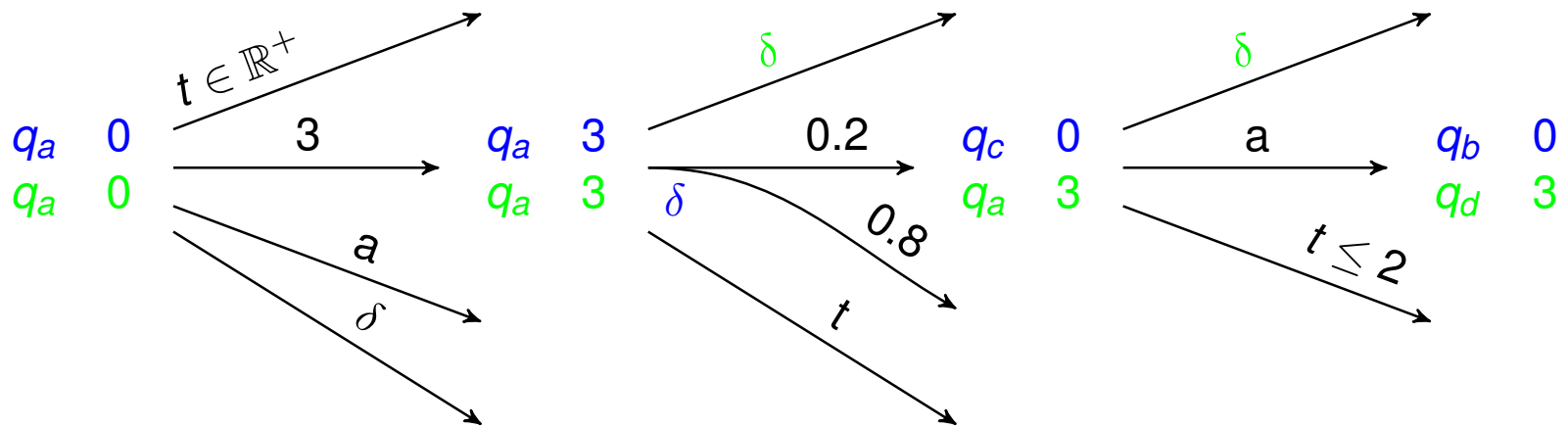


The model: Probabilistic timed protocol

N identical processes in a **clique**.

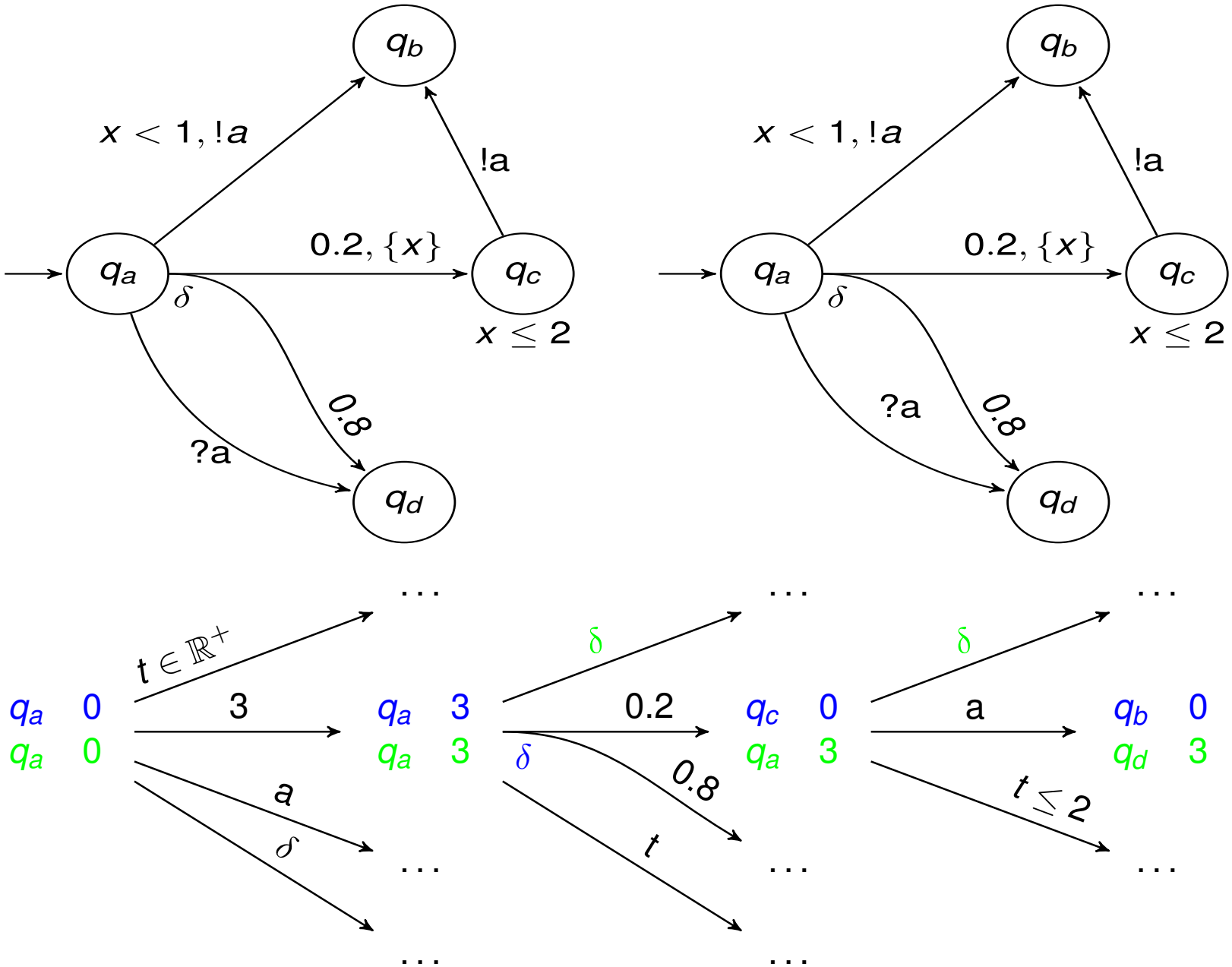






The model: Probabilistic timed protocol

N identical processes in a **clique**.



Problems studied: $\text{REACH}_{opt}^{\sim b}$

Input: A probabilistic protocol $\mathcal{P}$, and a control state $q_f \in Q$.
Question: Does there exists $N \in \mathbb{N}_{>0}$ with

$$\mathbb{P}_{opt}(\mathcal{P}^N \models \diamond q_f) \sim b?$$

$opt \in \{\min, \max\}$, $b \in \{0, 1\}$ and $\sim \in \{<, =, >\}$

Problems studied: $\text{REACH}^{\sim b}_{opt}$

Input: A probabilistic protocol $\mathcal{P}$, and a control state $q_f \in Q$.
Question: Does there exists $N \in \mathbb{N}_{>0}$ with

$$\mathbb{P}_{opt}(\mathcal{P}^N \models \diamond q_f) \sim b?$$

Notes

- $\text{REACH}^{=1}_{max}$: reach good state with friendly adversary
- $\text{REACH}^{=1}_{min}$: reach for all adversary
- $\text{REACH}^{>0}_{max}$: negative answer: avoid for all adversary

---

$opt \in \{\min, \max\}$, $b \in \{0, 1\}$ and $\sim \in \{<, =, >\}$

Undecidability with fix topology

Undecidability with fix topology

Reduction of existence of bounded path in 2 counter machine (Undecidable [Minsky 67])

Two counter machine instructions

- i : $x++$ goto i'
- i : if $x = 0$ goto i' else $x--$ goto i"

Undecidability with fix topology

Reduction of existence of bounded path in 2 counter machine (Undecidable [Minsky 67])

Two counter machine instructions

- i : $x++$ goto i'
- i : if $x = 0$ goto i' else $x--$ goto i"

Idea of the proof (adapted from [Abdulla, Henda, Mayr 07])

- Model counters value by number of processes in a state

Undecidability with fix topology

Reduction of existence of bounded path in 2 counter machine (Undecidable [Minsky 67])

Two counter machine instructions

- i : $x++$ goto i'
- i : if $x = 0$ goto i' else $x--$ goto i"

Idea of the proof (adapted from [Abdulla, Henda, Mayr 07])

- Model counters value by number of processes in a state
- Model zero test by probabilistic choice

Undecidability with fix topology

Reduction of existence of bounded path in 2 counter machine (Undecidable [Minsky 67])

Two counter machine instructions

- i : $x++$ goto i'
- i : if $x = 0$ goto i' else $x--$ goto i"

Idea of the proof (adapted from [Abdulla, Henda, Mayr 07])

- Model counters value by number of processes in a state
- Model zero test by probabilistic choice
- Infinite (false) zero tests

Undecidability with fix topology

Reduction of existence of bounded path in 2 counter machine (Undecidable [Minsky 67])

Two counter machine instructions

- i : $x++$ goto i'
- i : if $x = 0$ goto i' else $x--$ goto i"

Idea of the proof (adapted from [Abdulla, Henda, Mayr 07])

- Model counters value by number of processes in a state
- Model zero test by probabilistic choice
- Infinite (false) zero tests
- $P_{min}(\Diamond error) = 1 \Leftrightarrow$ existence of bounded path

Mobil topology: Decidability

Mobil topology: Decidability

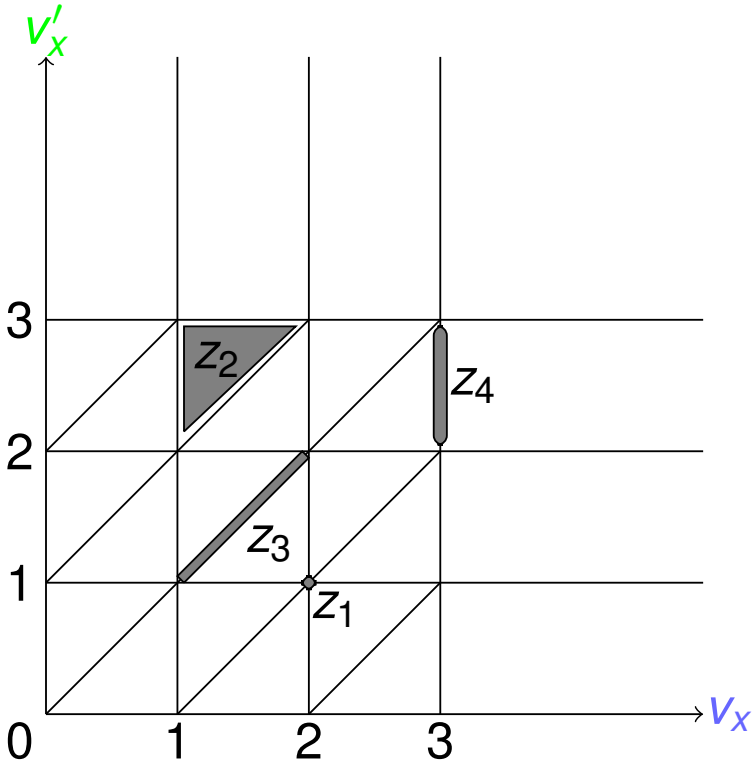
Clique of probabilistic timed protocol with:

Deletion rate λ:
Each process have probability λ to be lost after each action and each time unit.
Models: crash, out of range, out of power, ...

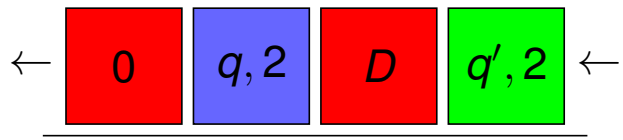
Creation rate μ:
Creation of *n* processes with probability $\mu^n(1-\mu)$.
Models: maintenance, new comer, ...

Reduction of regions to channel contents

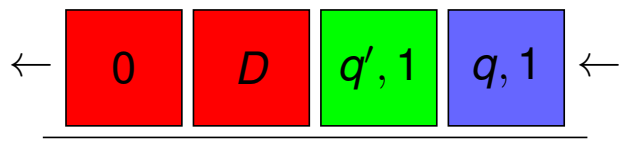
$\mathcal{P} : (q, x)$ and $\mathcal{P} : (q', x)$



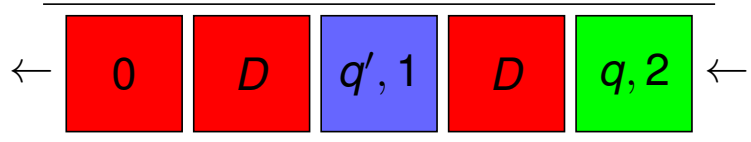
z_4: $v_x = 2 < v'_x < 3$



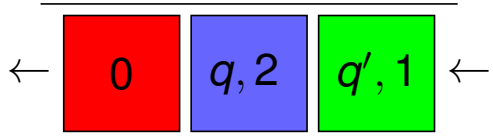
z_3: $1 < v_x = v'_x < 2$



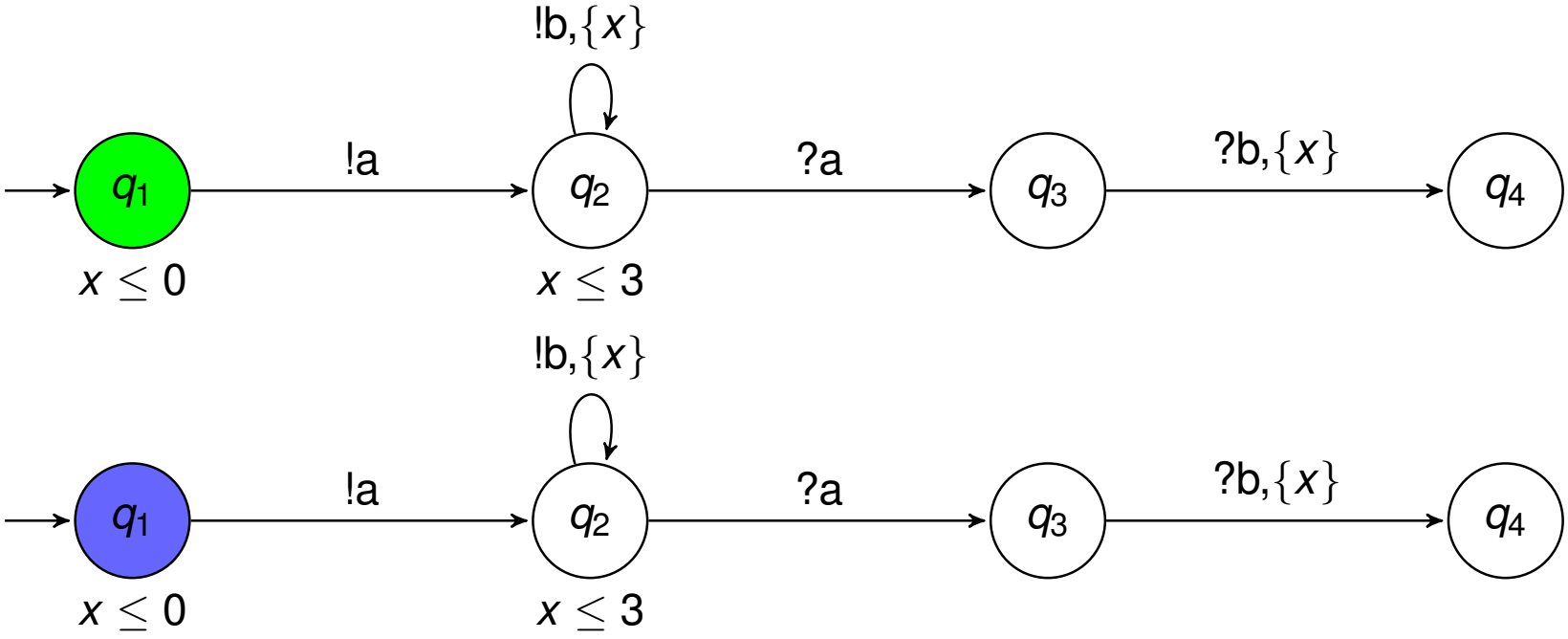
z_2: $1 < v_x < 2 < v'_x < 3, \{v_x\} < \{v'_x\}$

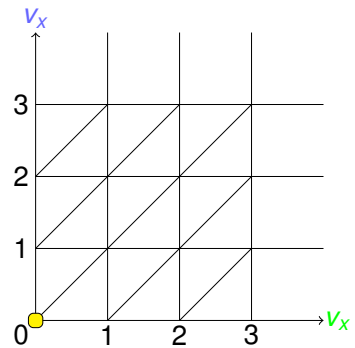


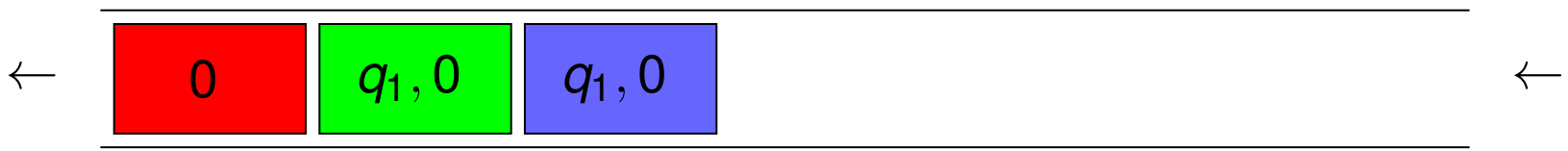
z_1: $v_x = 2, v'_x = 1$



Simulation

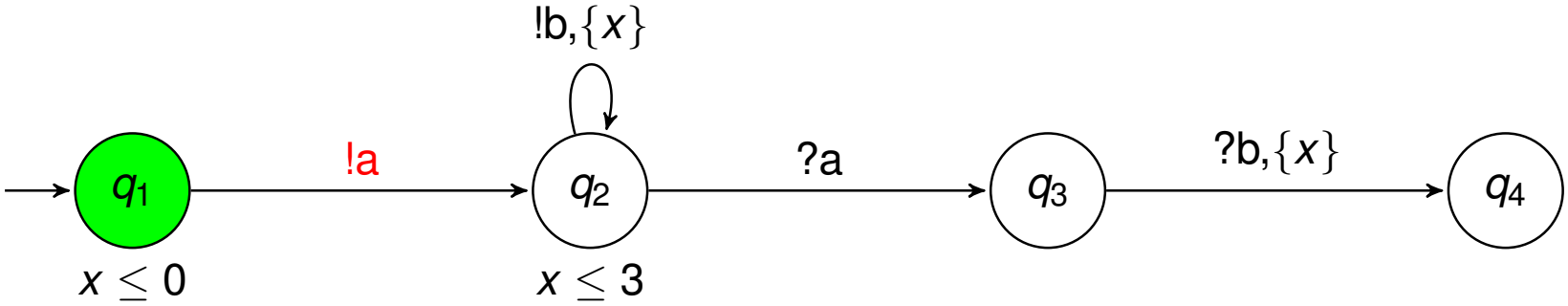


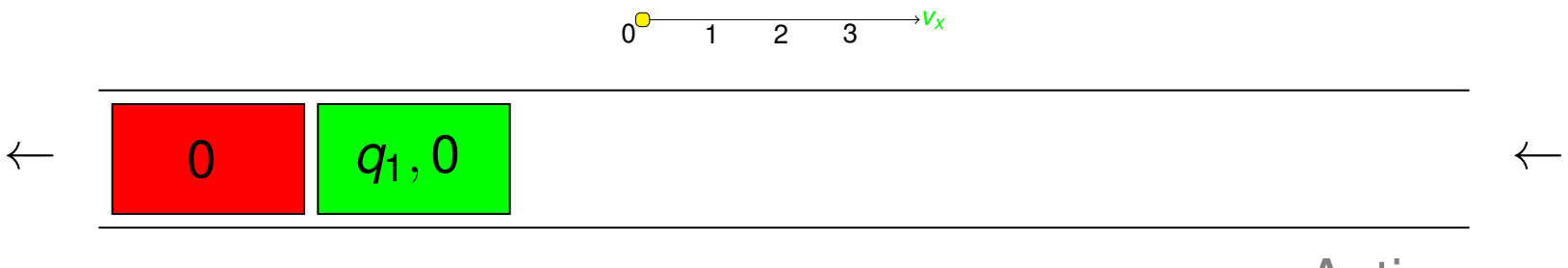




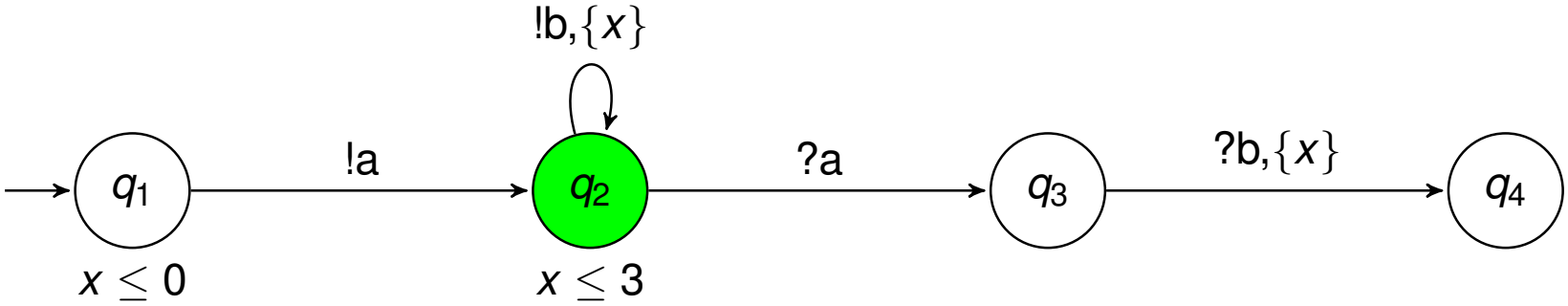
Loss

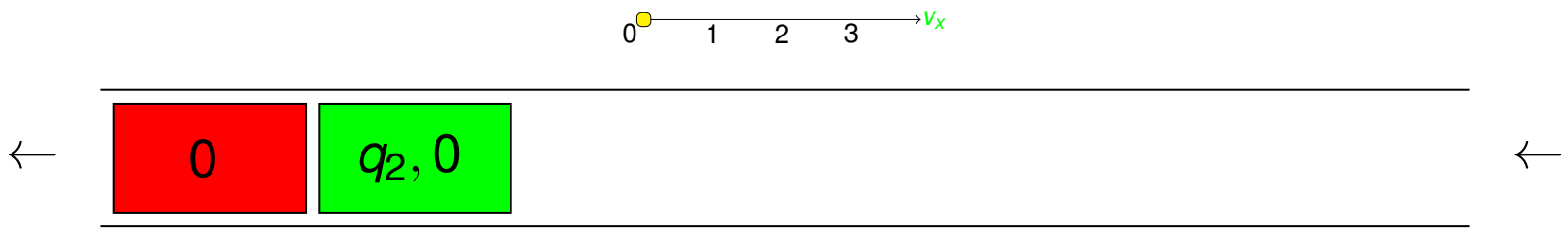
Simulation





Simulation

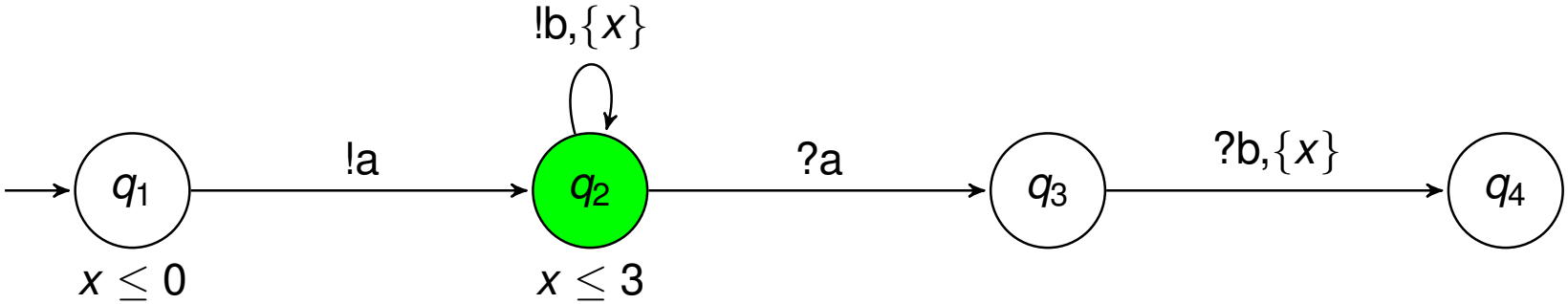


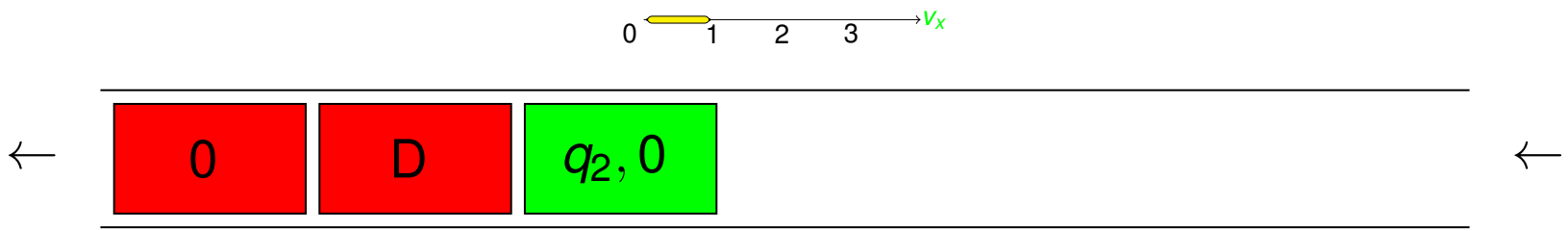


Action a

Time elapsing

Simulation

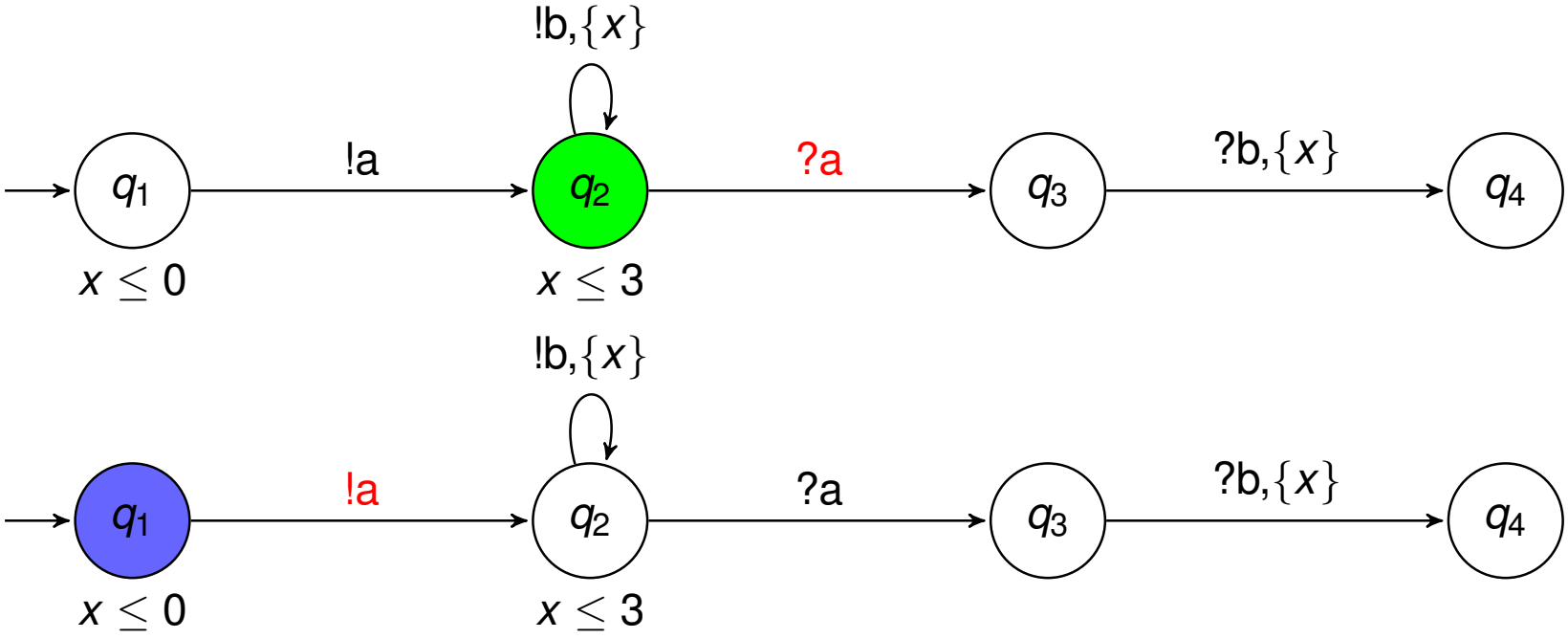


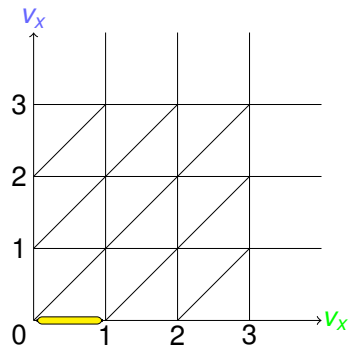


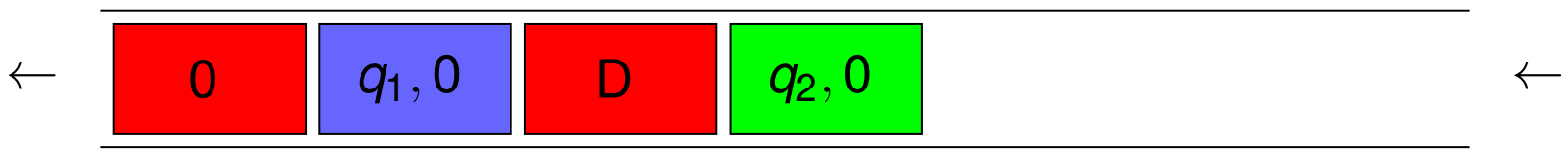
Time elapsing

Maintenance/creation

Simulation



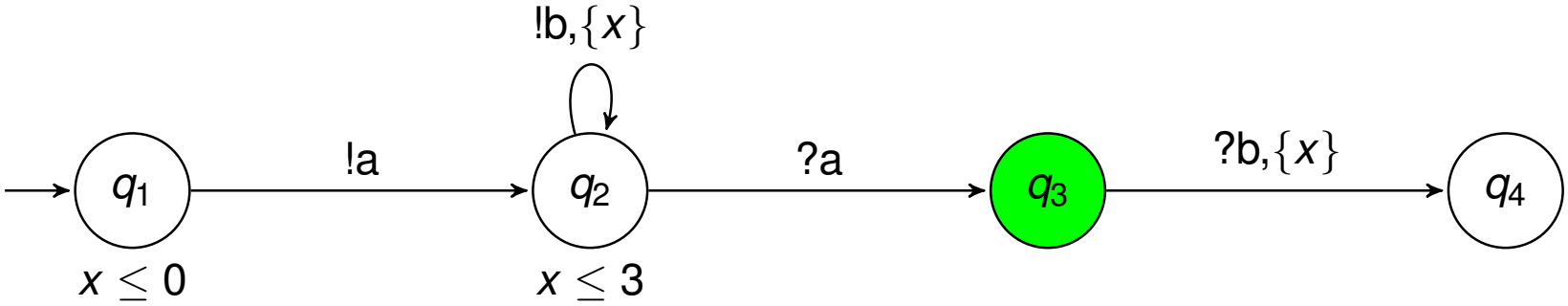


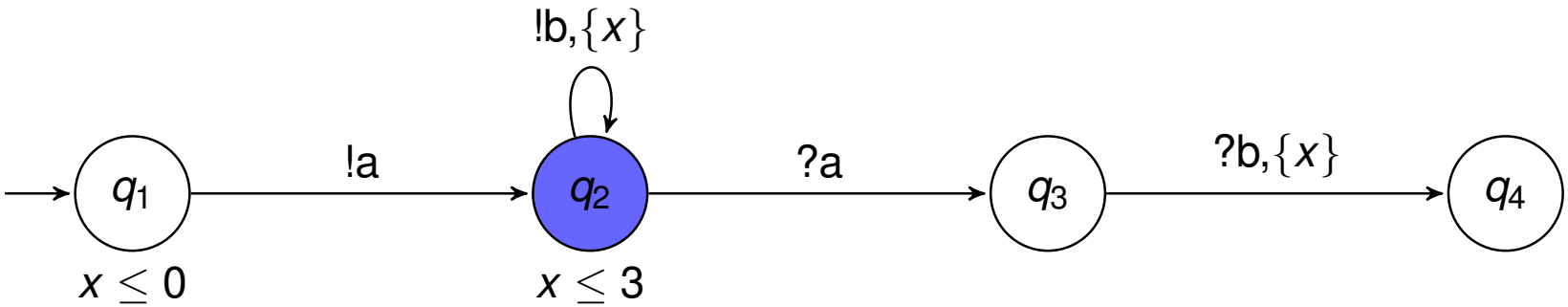


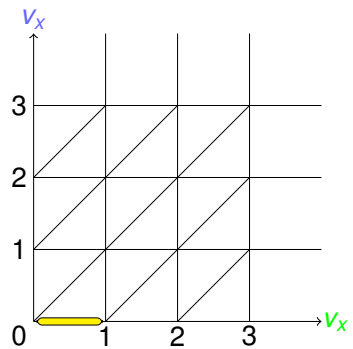
Maintenance/creation

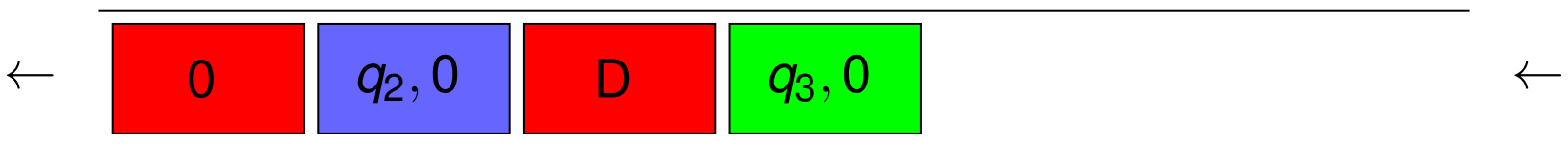
Action a

Simulation





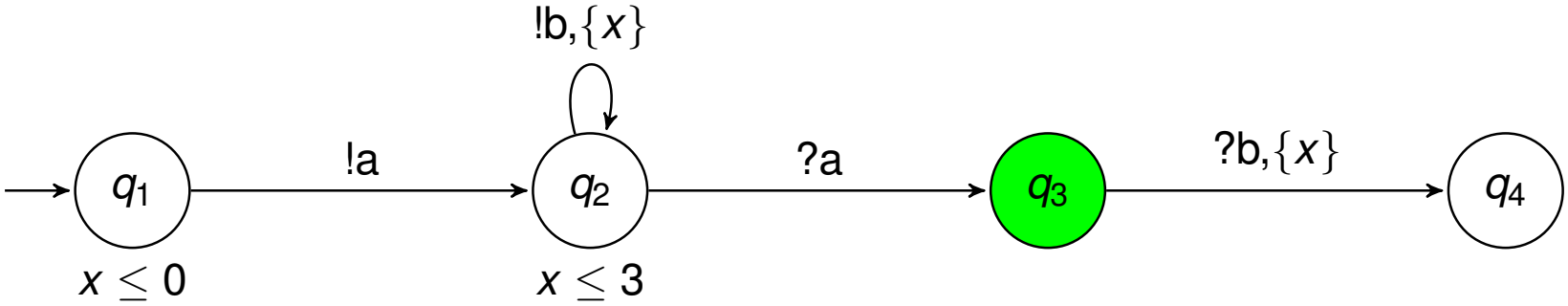


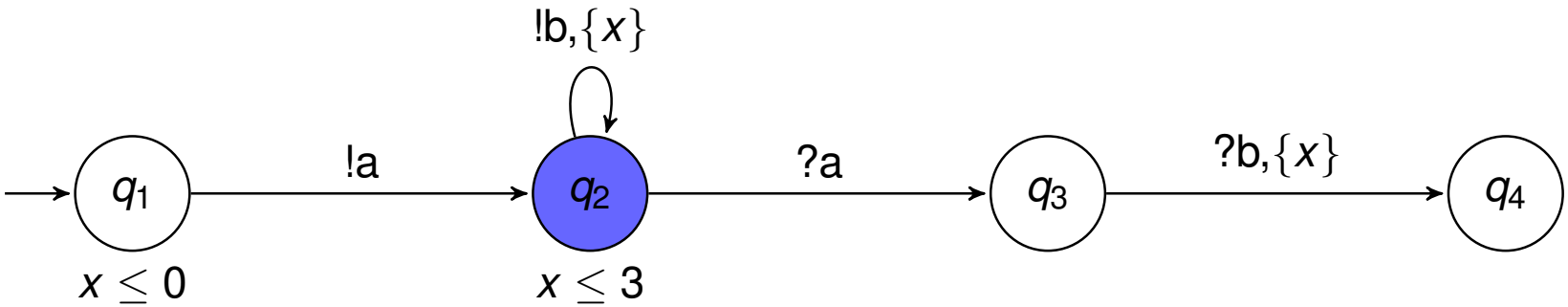


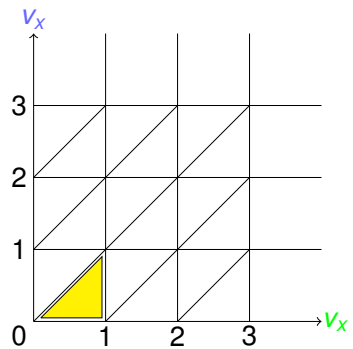
Action a

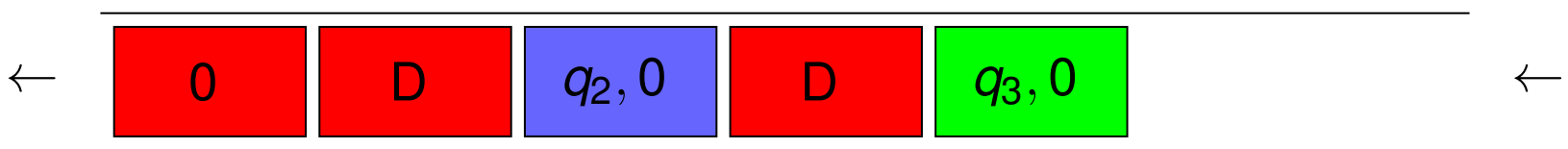
Time elapsing

Simulation





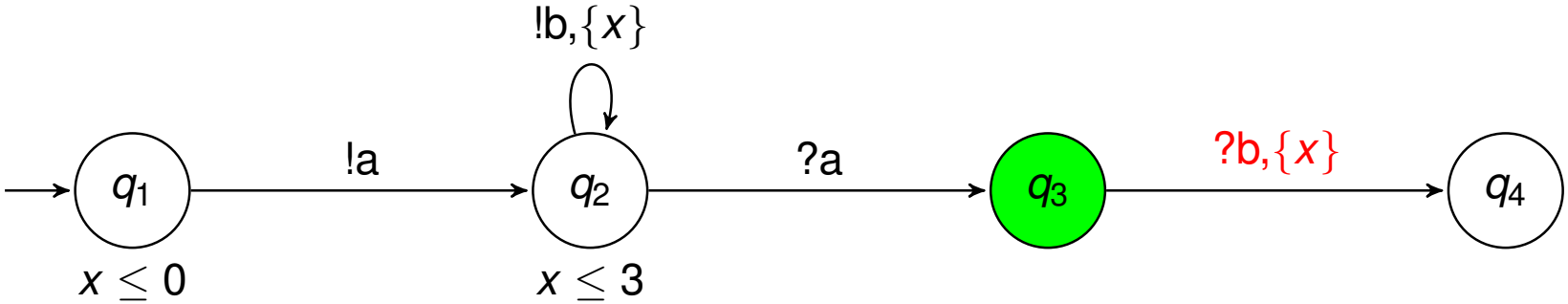


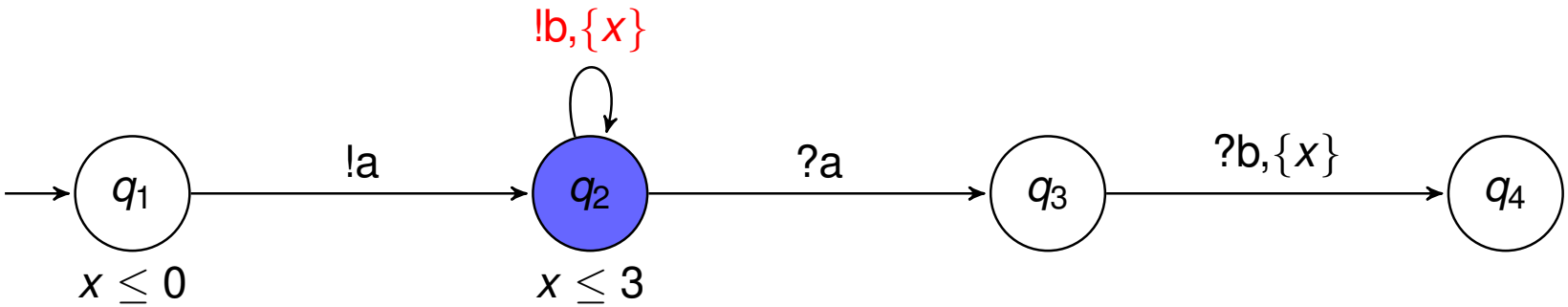


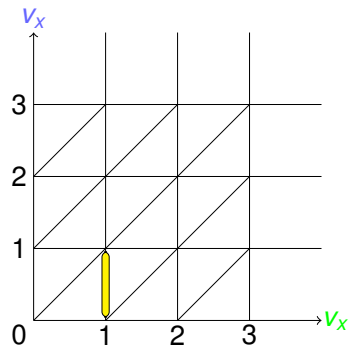
Time elapsing

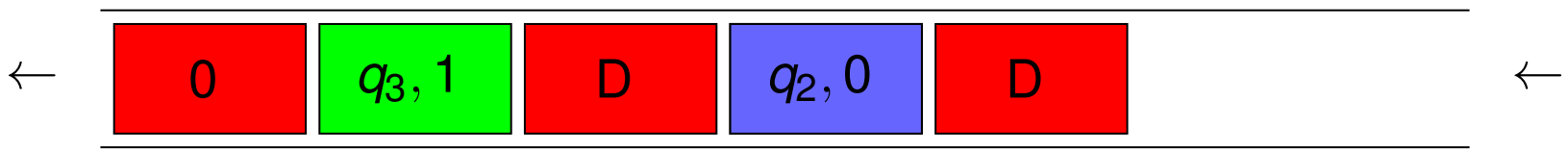
Time elapsing

Simulation





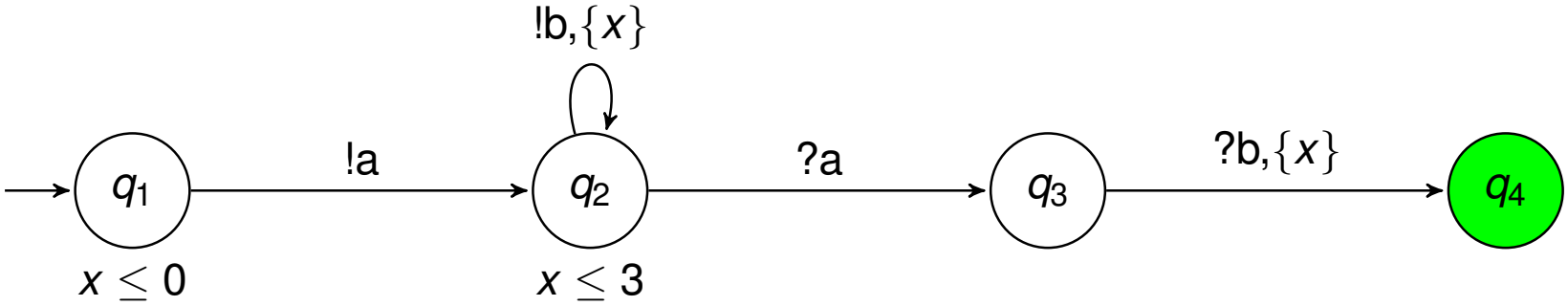


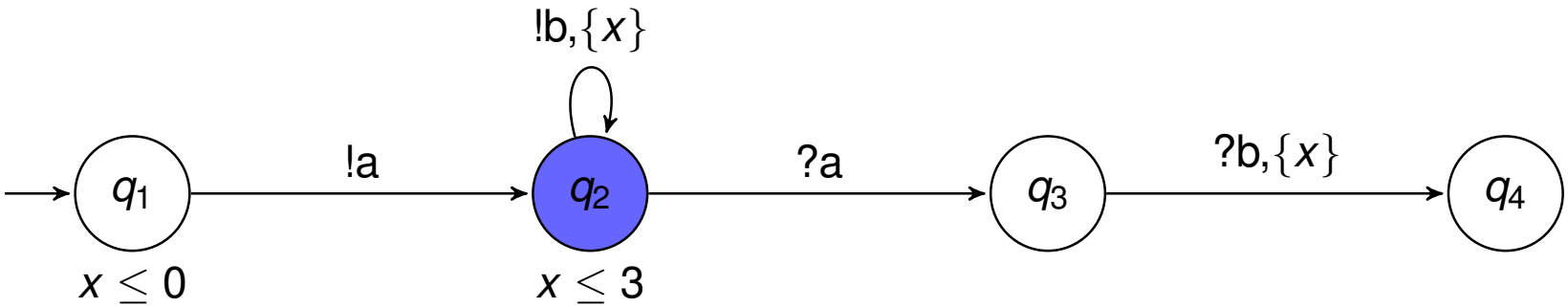


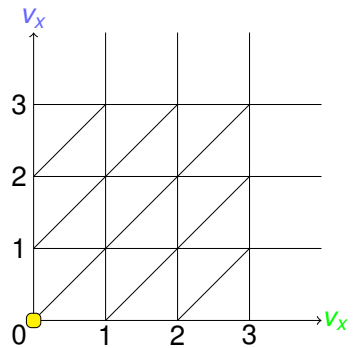
Time elapsing

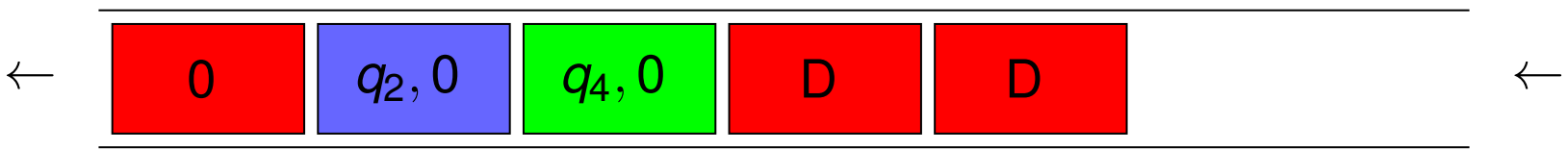
Action b

Simulation





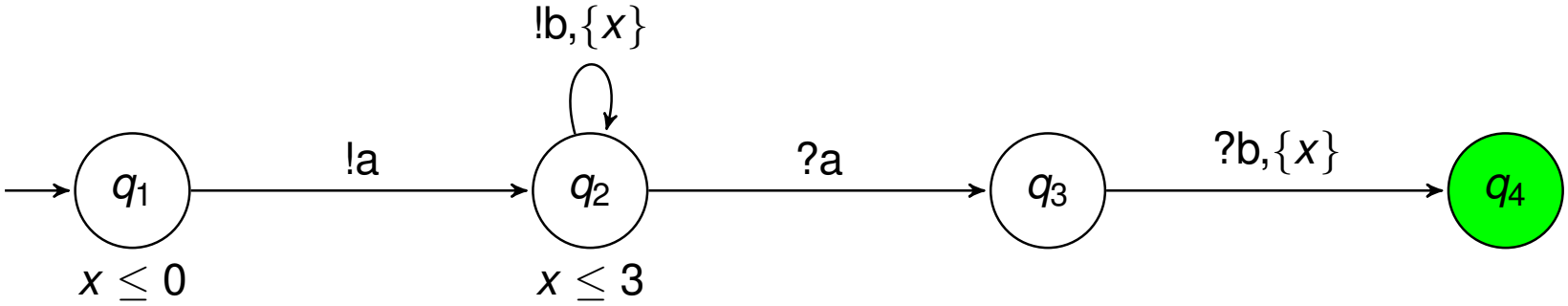


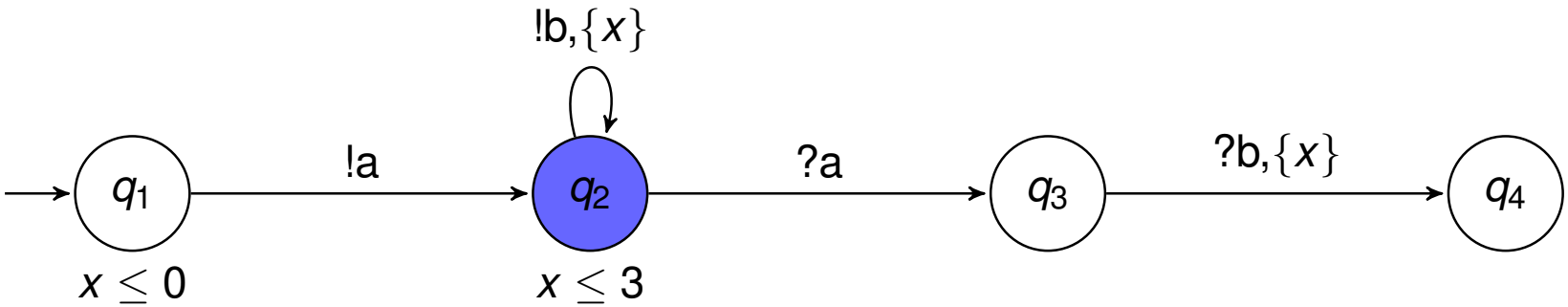


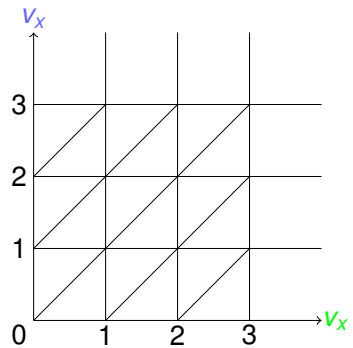
Action b

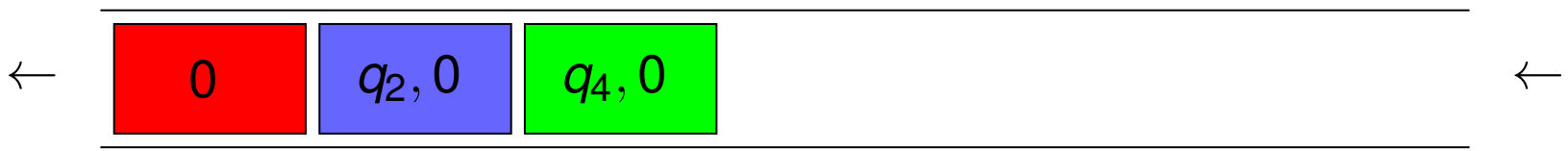
Remove useless messages

Simulation









Remove useless messages

Conclusion

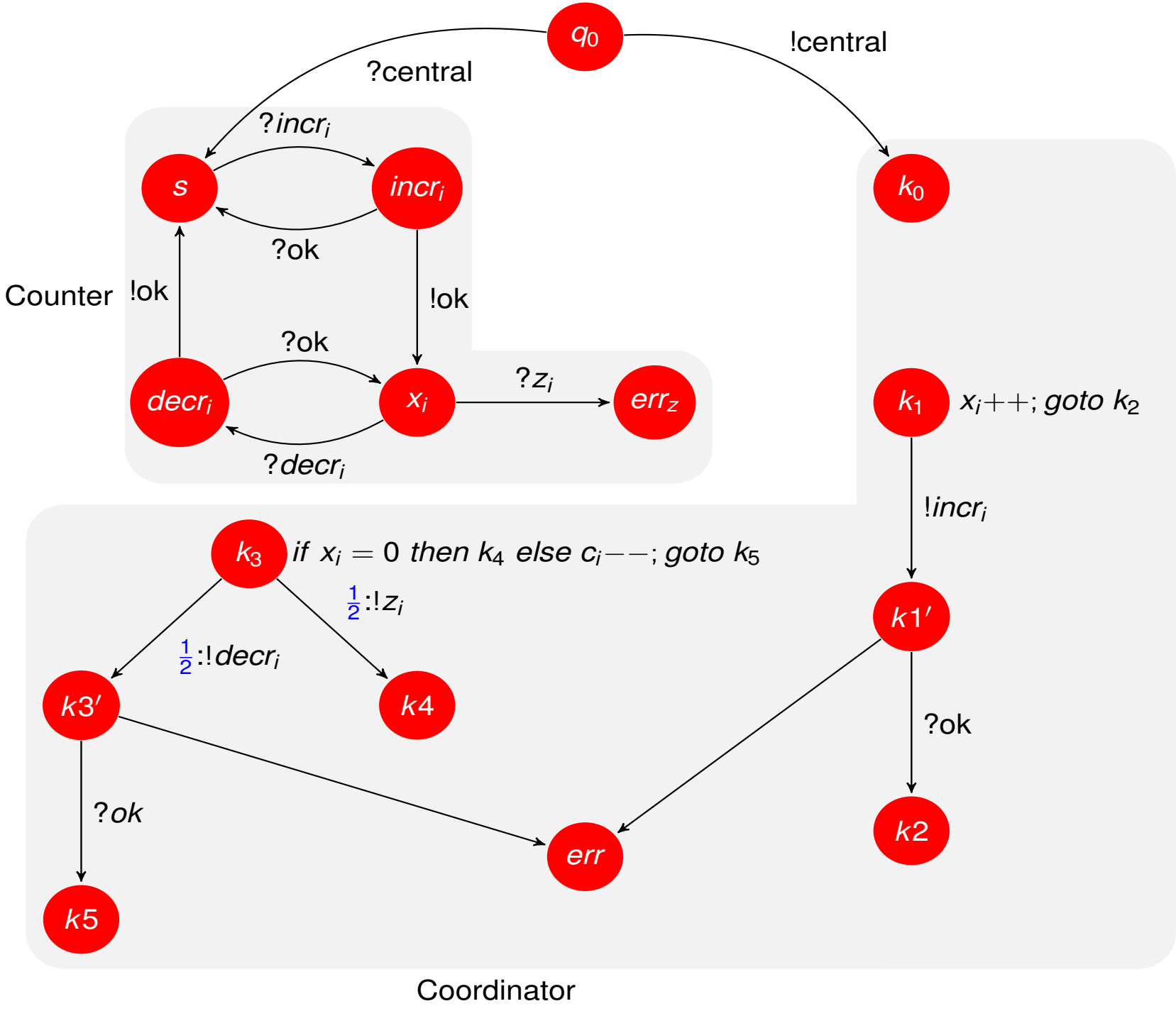
Parametric verification is :

- Verifying for all parameter at once
- Undecidable for fix topology
- Decidable for Mobile topology

			$\text{REACH}^{>0}_{max}$	$\text{REACH}^{=1}_{max}$	$\text{REACH}^{=1}_{min}$	$\text{REACH}^{<1}_{min}$
Static			[ADRST11]	U	U	U
mobil	timed	1	D	D	D	D
		≥ 2	[ADM04]	U	U	U

Future works

- Quantitative properties
- $P_{min}(\phi) = f(N) \pm \epsilon$
- Topologies properties
- Synthesis of parameter


q_0
?central
!central
?$incr_i$
s
$incr_i$
?ok
Counter
!ok
!ok
?ok
$decr_i$
x_i
?z_i
err_z
?$decr_i$
k_0
k_1
$x_i{+}{+}$; goto k_2
!$incr_i$
k_3
if $x_i = 0$ then k_4 else $c_i{-}{-}$; goto k_5
$\frac{1}{2}$:!z_i
$\frac{1}{2}$:!$decr_i$
$k3'$
$k4$
$k1'$
?ok
?ok
err
$k2$
$k5$
Coordinator

Bibliography I

Parosh Aziz Abdulla, Giorgio Delzanno, Othmane Rezine, Arnaud Sangnier, and Riccardo Traverso.

On the verification of timed ad hoc networks.

In *FORMATS*, pages 256–270, 2011.

Parosh Aziz Abdulla, Johann Deneux, and Pritha Mahata.

Multi-clock timed networks.

In *LICS*, pages 345–354, 2004.

Parosh Aziz Abdulla, Noomene Ben Henda, and Richard Mayr.

Decisive markov chains.

Logical Methods in Computer Science, 3(4), 2007.

Parosh Aziz Abdulla and Bengt Jonsson.

Model checking of systems with many identical timed processes.

Theor. Comput. Sci., 290(1):241–264, 2003.

Bibliography II

Christel Baier, Nathalie Bertrand, and Ph. Schnoebelen.

A note on the attractor-property of infinite-state markov chains.

Inf. Process. Lett., 97(2):58–63, 2006.

Nathalie Bertrand.

Modèles stochastiques pour les pertes de messages dans les protocoles asynchrones et techniques de vérification automatique, 2006.

Tomás Brázdil and Antonín Kucera.

Computing the expected accumulated reward and gain for a subclass of infinite markov chains.

In *FSTTCS*, pages 372–383, 2005.

Giorgio Delzanno, Arnaud Sangnier, and Gianluigi Zavattaro.

Parameterized verification of ad hoc networks.

In *CONCUR*, pages 313–327, 2010.

Bibliography III

Giorgio Delzanno, Arnaud Sangnier, and Gianluigi Zavattaro.

On the power of cliques in the parameterized verification of ad hoc networks.

In *FOSSACS*, pages 441–455, 2011.

Giorgio Delzanno, Arnaud Sangnier, and Gianluigi Zavattaro.

Parameterized verification of safety properties in ad hoc network protocols.

In *PACO*, pages 56–65, 2011.

Matthias Fruth.

Probabilistic model checking of contention resolution in the ieee 802.15.4 low-rate wireless personal area network protocol.

In *ISoLA*, pages 290–297, 2006.

Bibliography IV

Hafedh Zayani, Kamel Barkaoui, and Rahma Ben Ayed.

Probabilistic verification and evaluation of backoff procedure of the wsn eco-mac protocol.

CoRR, abs/1005.2050, 2010.