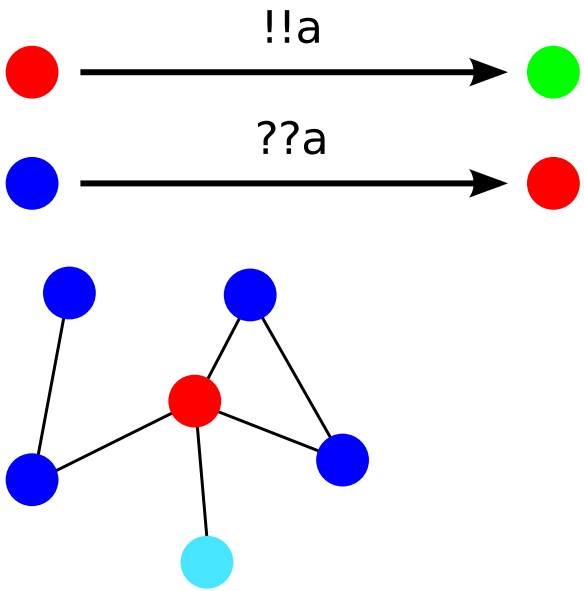
Specification and Verification of Concurrent and Distributed Systems

C.I.N.A. meeting

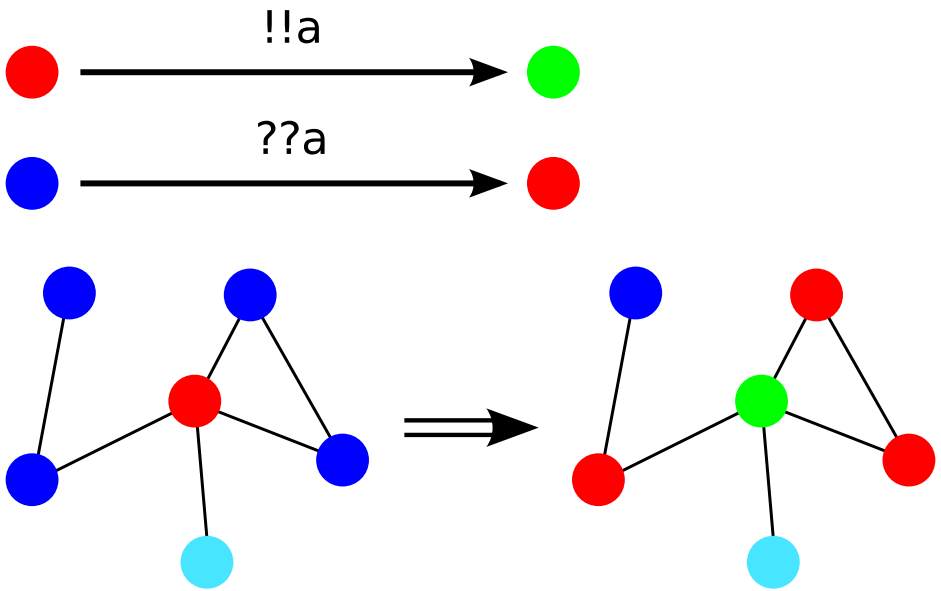
Riccardo Traverso Giorgio Delzanno

Pisa, February 5th, 2013

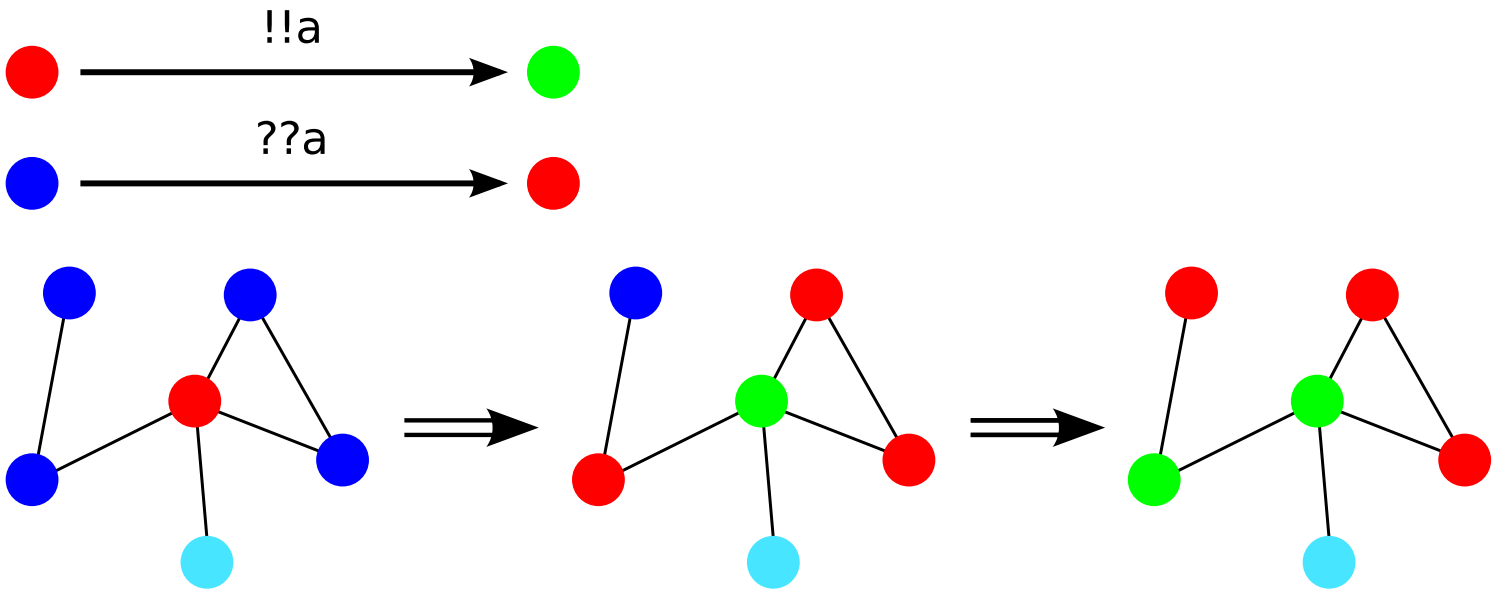
The starting point: Ad Hoc Networks (AHN)



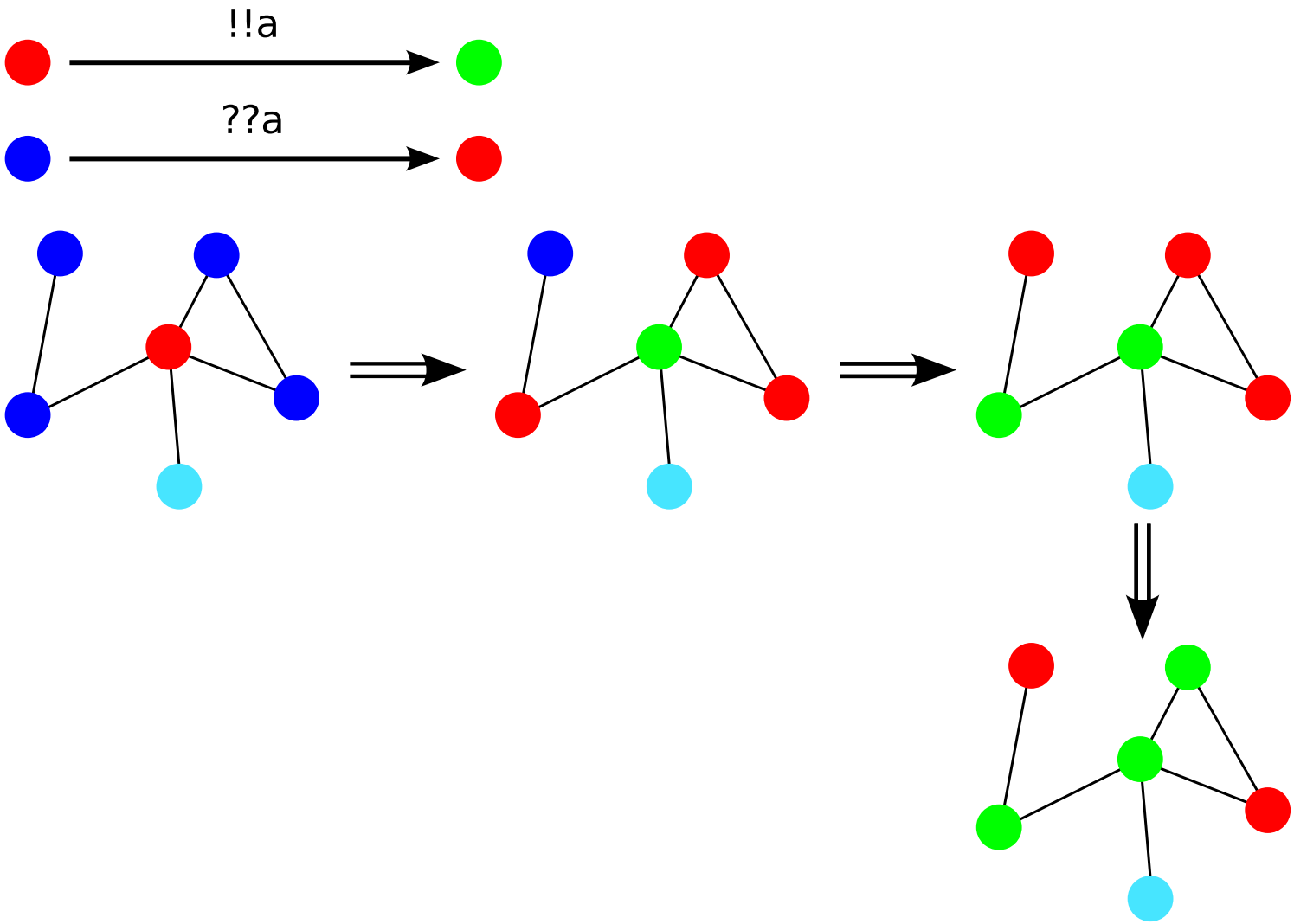
The starting point: Ad Hoc Networks (AHN)



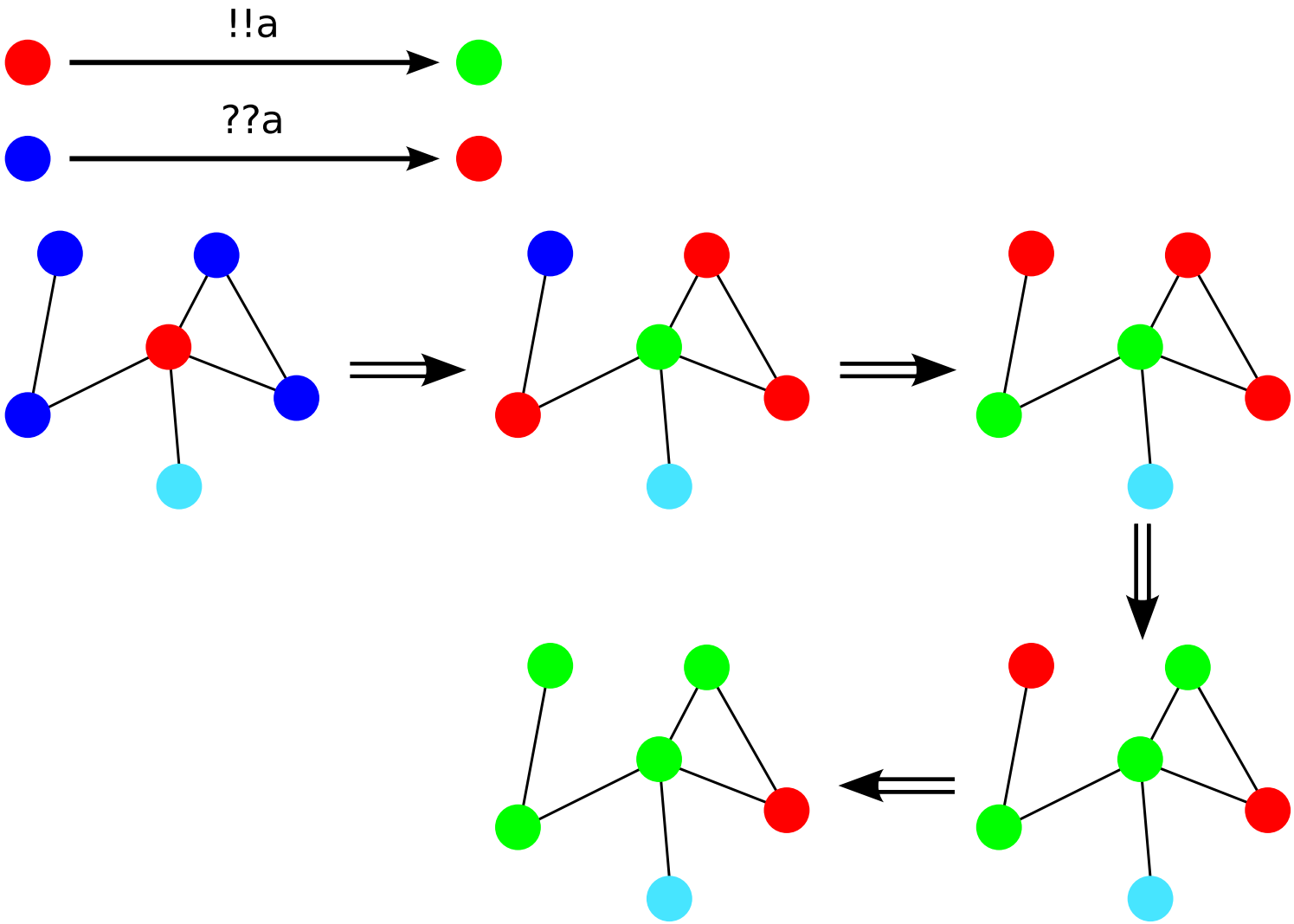
The starting point: Ad Hoc Networks (AHN)



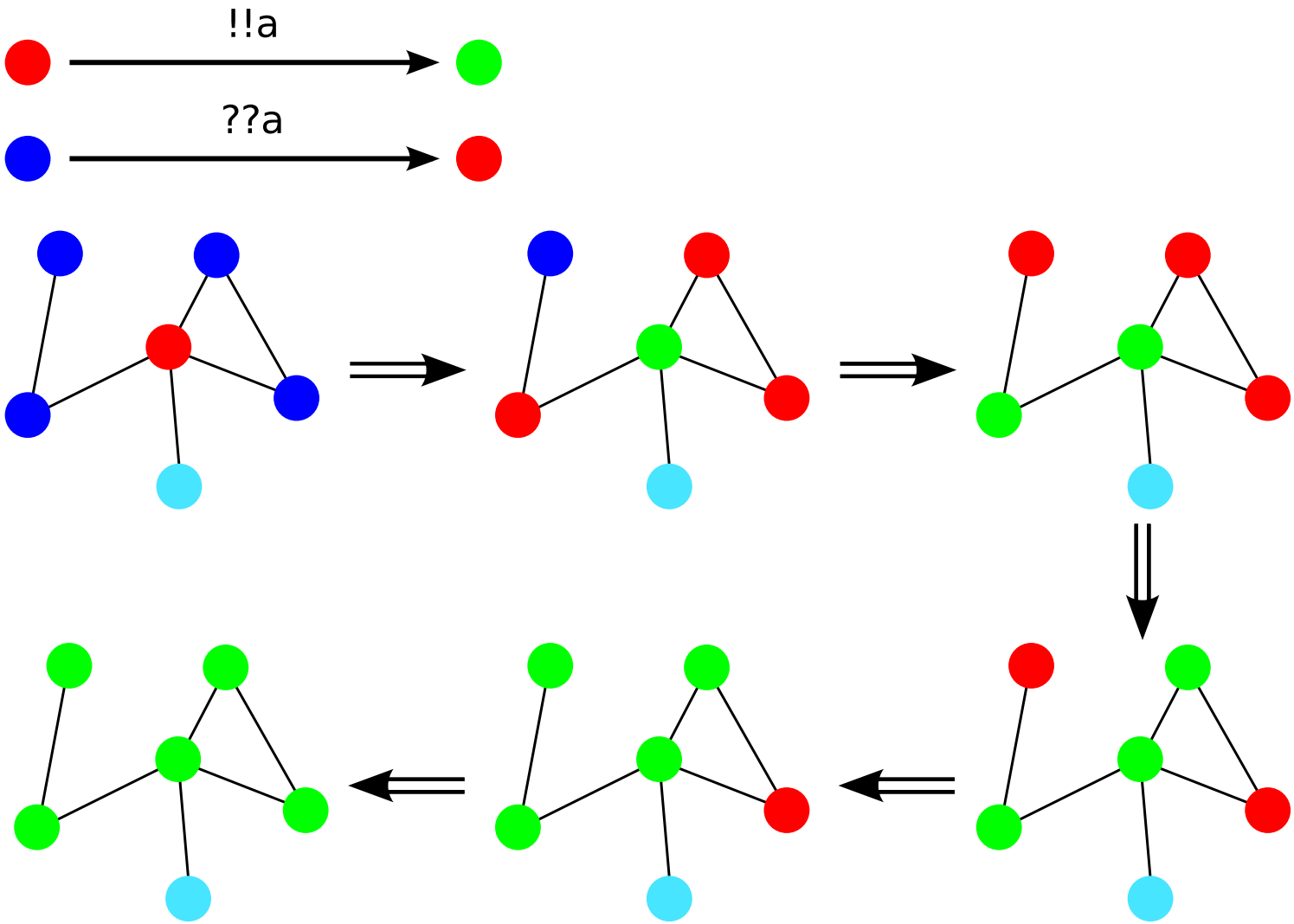
The starting point: Ad Hoc Networks (AHN)



The starting point: Ad Hoc Networks (AHN)



The starting point: Ad Hoc Networks (AHN)



Parameterized verification on AHN

Given a protocol (automaton) and its associated transition system (AHN), compute:

- reachability of a configuration with at least one process in a given state (COVER);
- reachability of a configuration with all processes in a given state (TARGET);
- existence of a computation traversing infinitely often configurations with at least one process in a given state (REPEAT-COVER).

Results on AHN problems

- Those problems are all undecidable for arbitrary graphs.
- There are some decidability results by restricting COVER to configurations in specific classes of graphs.
- By introducing mobility in the model, COVER, TARGET and REPEAT-COVER become decidable.

Aim

To investigate the interplay between richer models of distributed systems and the underlying communication topology.

- Features inspired from routing protocols for Ad Hoc Networks:
  - dynamic networks;
  - more realistic communication (synch. vs asynch, broadcast vs unicast);
  - node identifiers.
- Theoretical research: existing approaches are mostly about modelling rather than analysis.

With whom do we work?

Collaborations

Uppsala University, Program Verification Group:

- Parosh Aziz Abdulla (prof.), Faouzi Atig (PhD), Othmane Rezine (PhD student)

University Paris Diderot - Paris 7 - LIAFA:

- Arnaud Sangnier (prof.)

Università di Bologna INRIA - FOCUS Research Team:

- Gianluigi Zavattaro (prof.)

Which are the models considered?

Reconfigurable Broadcast Networks (RBN)

- Synchronous broadcast and reception of messages (like AHN).
- Random rearrangements of the network connections.

RBN: Parameterized Reachability Problem

We consider cardinality constraints (CC) on the number of processes in a given control state:

$$\varphi ::= a \leq \#q < b \mid \varphi \wedge \varphi \mid \varphi \vee \varphi \mid \neg\varphi$$

($a \in \mathbb{N}$, q is a local control state, and $b \in (\mathbb{N} \setminus \{0\}) \cup \{+\infty\}$)

- PRP: can we reach a configuration satisfying some CC φ from an initial configuration?
- No restrictions on the initial number of processes.

RBN: Results (FSTTCS12)

- PRP is PTime-complete for CC without negation and with only $\#q \geq 1$ atoms.
- For CC with $\#q \geq 1$ atoms and negation PRP is NP-complete.
- PRP is PSpace-complete for unrestricted CC.

RBN: Extension with node identifiers

- Each node in a configuration has its own identifier (unbounded data domain).
- It is a basic requirement in order to build routing tables.
- Identifiers may be:
  - exchanged with broadcast messages;
  - saved in local variables;
  - tested for equality.

RBN: Extension with node identifiers (in progress)

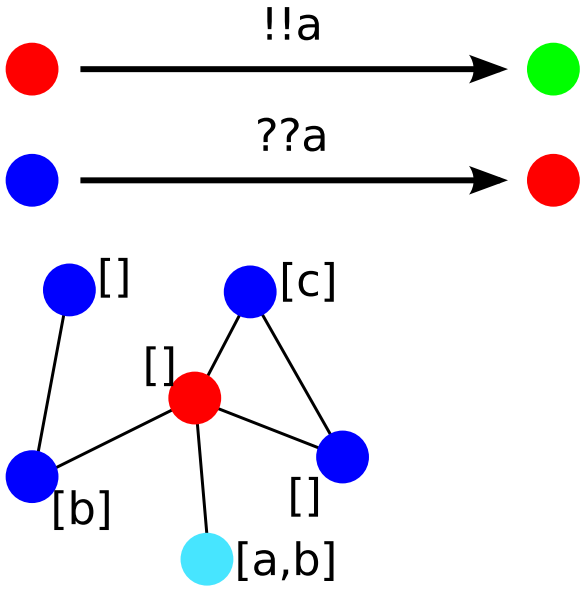
We consider COVER, without network reconfigurations (fully connected case):

- 1 RO + 1 RW locals, 1 ID per message $\Longrightarrow$ undecidability
- 1 RW local, 1 ID per message $\Longrightarrow$ decidability

And with reconfigurations:

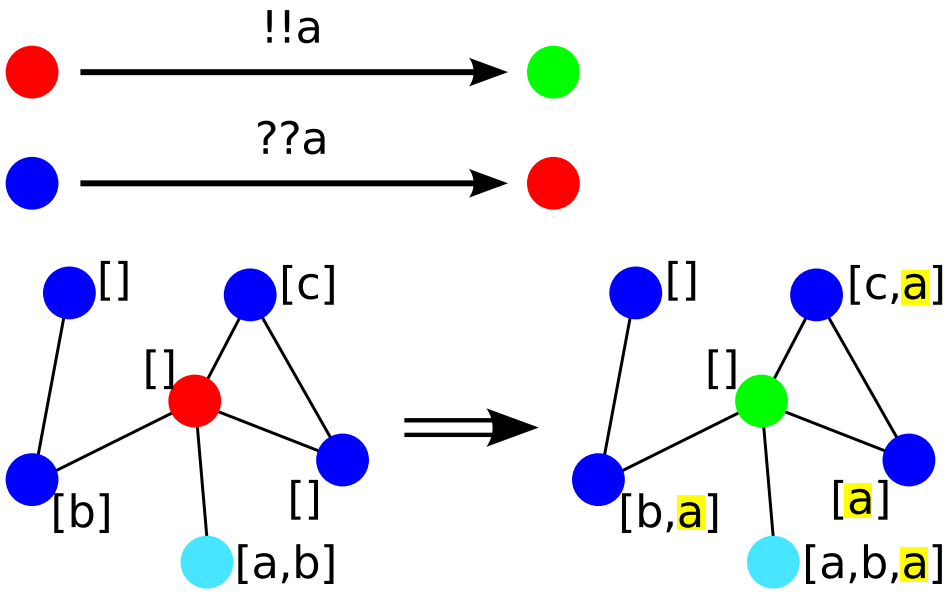
- 1 RO + 1 RW locals, 2 ID per message $\Longrightarrow$ undecidability
- 1 RO + 1 RW locals, 1 ID per message $\Longrightarrow$ decidability?

Asynchronous Broadcast Networks (ABN)



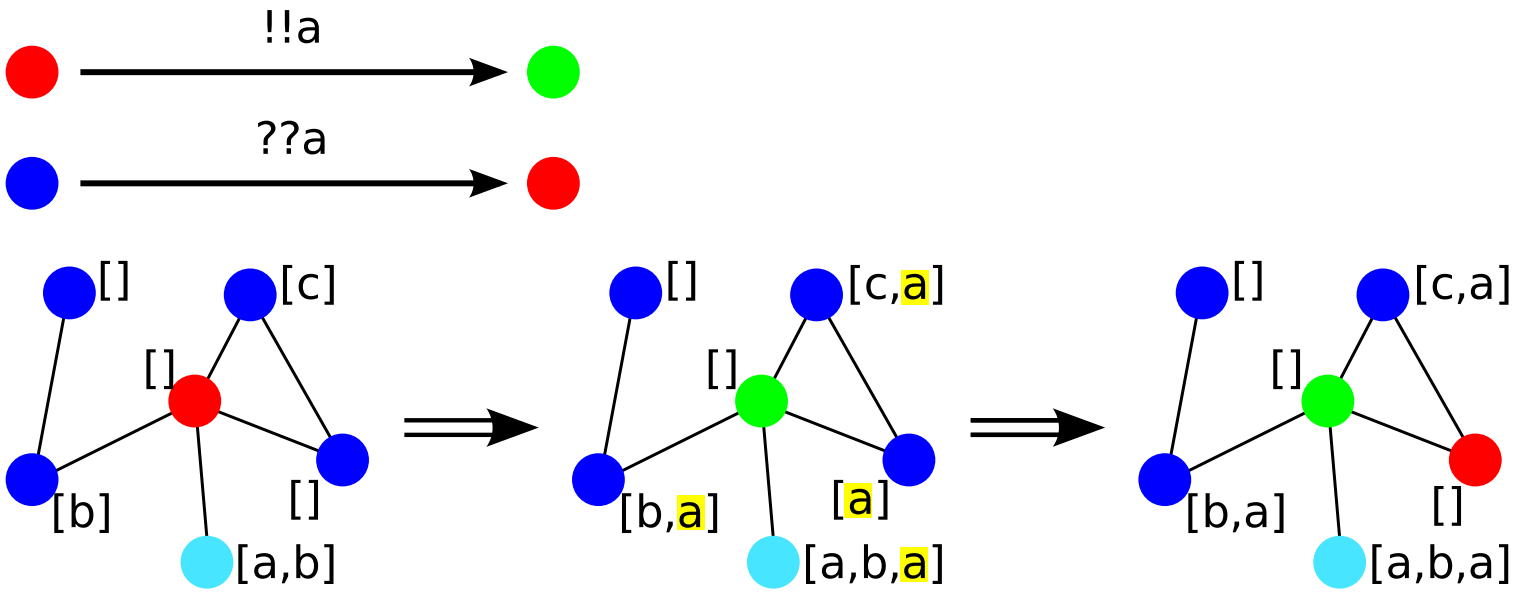
(with multisets as mailboxes)

Asynchronous Broadcast Networks (ABN)



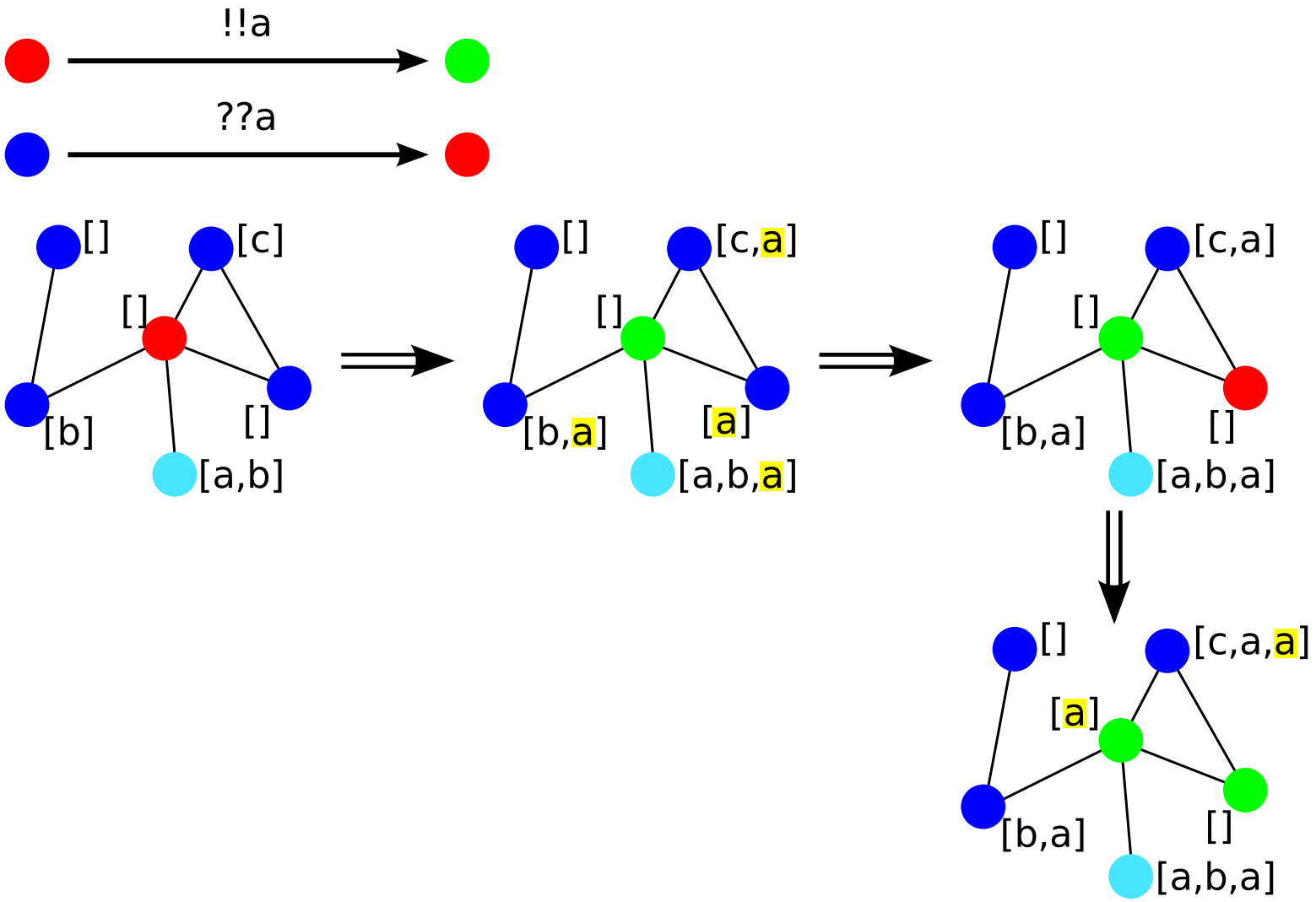
(with multisets as mailboxes)

Asynchronous Broadcast Networks (ABN)



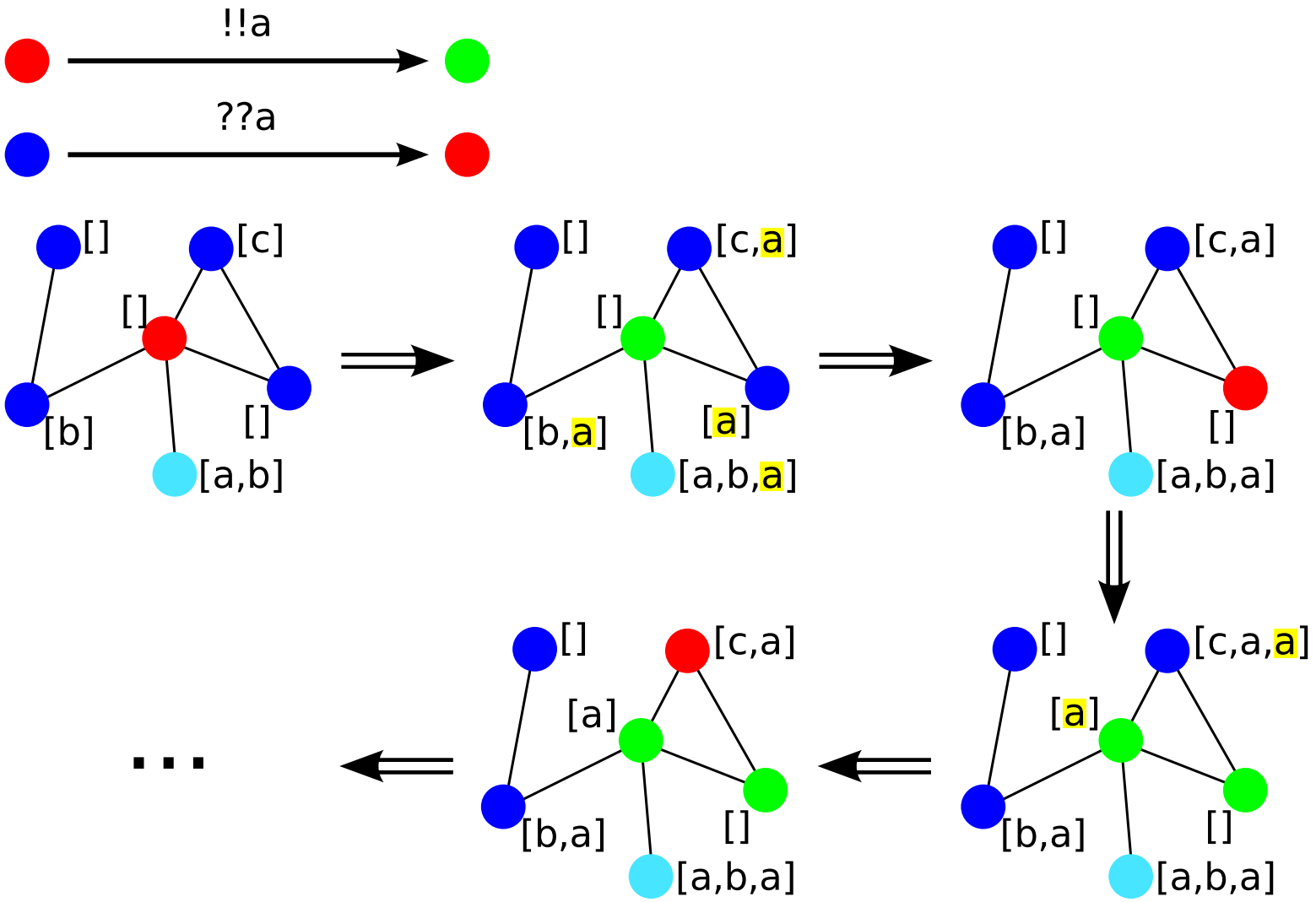
(with multisets as mailboxes)

Asynchronous Broadcast Networks (ABN)



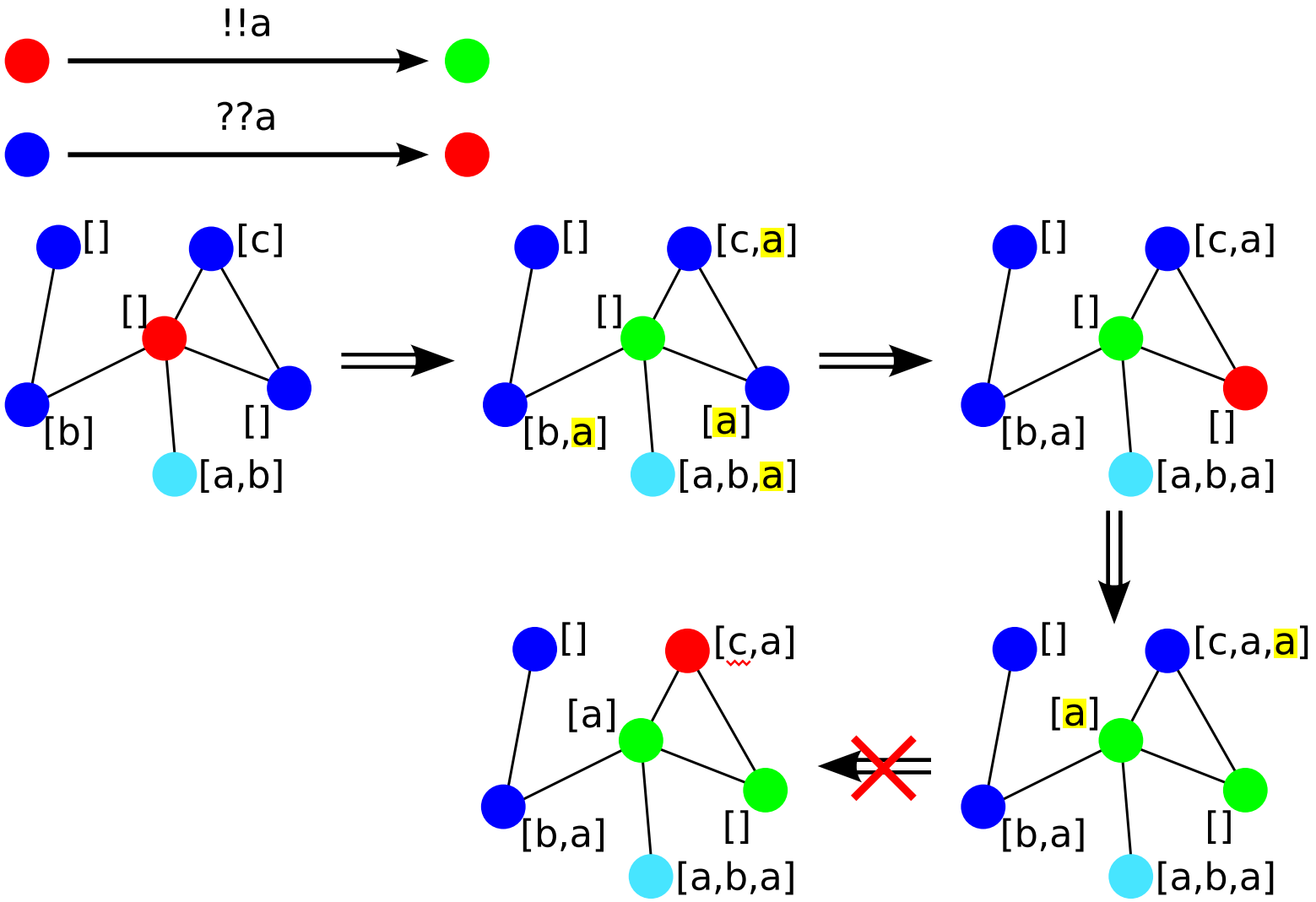
(with multisets as mailboxes)

Asynchronous Broadcast Networks (ABN)



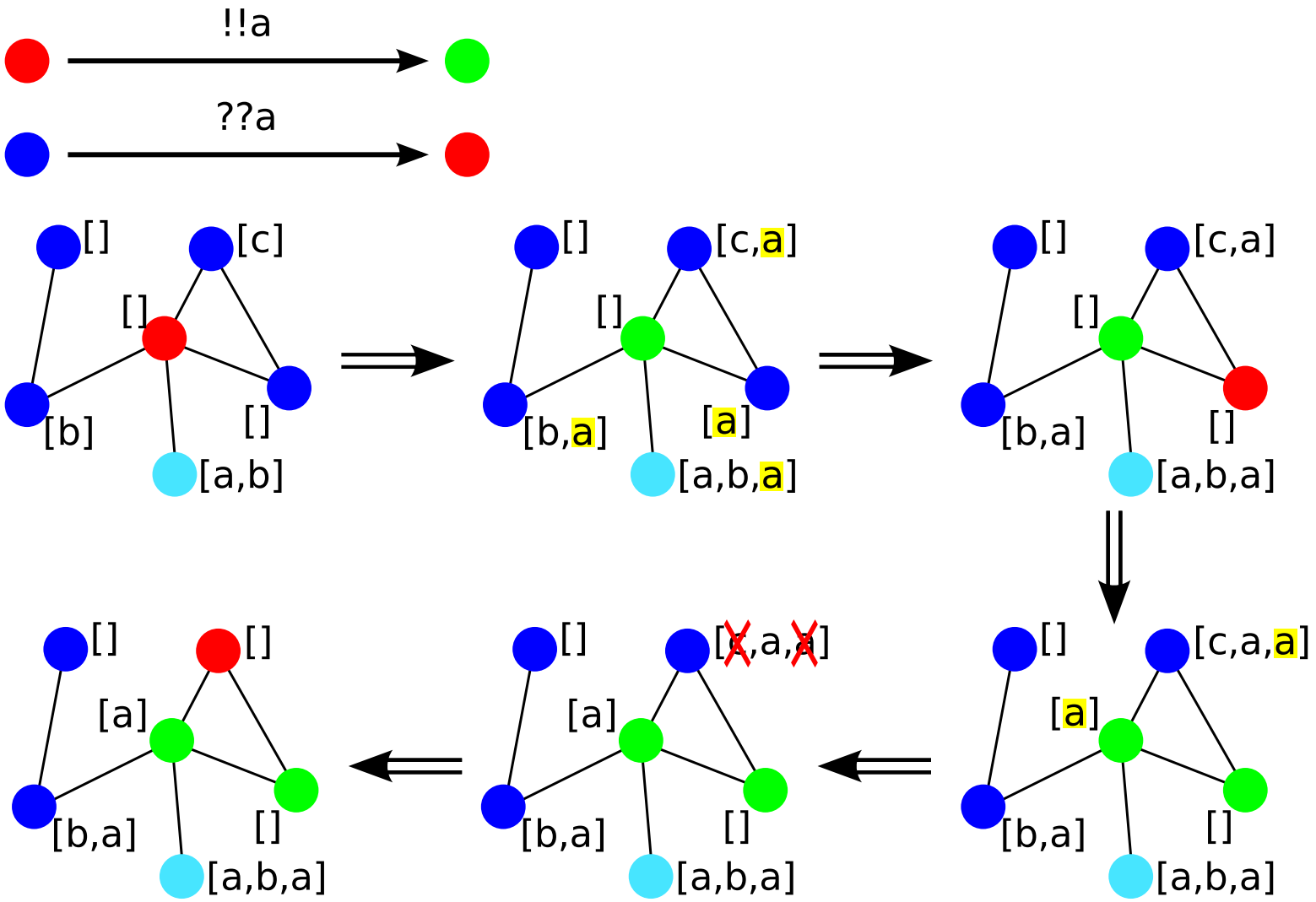
(with multisets as mailboxes)

Asynchronous Broadcast Networks (ABN)



(with FIFO queues as mailboxes)

Asynchronous Broadcast Networks (ABN)



(with lossy FIFO queues as mailboxes)

ABN: Results (ICTCS12, LATA13)

	$COVER^{\mathcal{K}}(\mathbb{M})$		$COVER(\mathbb{M})$	
	ABN	ABN_ϵ	ABN	ABN_ϵ
LFIFO	PTime	PTime	PTime	PTime
Bag	PTime	undec.	PTime	undec.
FIFO	undec.	undec.	undec.	undec.

		ABN / ABN_ϵ		
	AHN	LFIFO	Bag	FIFO
Fully connected graphs	✓	PTime	PTime/undec.	undec.
Arbitrary graphs	undec.	PTime	PTime/undec.	undec.

ABN: Extension with time (in progress)

Extensions to the model:

- Each automaton is equipped with $k \in \mathbb{N}$ local clocks.
- Each received message is associated to its current age.
- Transition guards.
- With $k = 0$, COVER should be decidable.

ABN: Extension with quantified send and receive (future)

Two new communication primitives:

- existential send ($!!_{\exists}a$);
- universal receive ($??_{\forall}a$).

COVER, by adding only $??_{\forall}a$ actions:

- in fully-connected graphs, it should be undecidable;
- uncommonly, it seems to be more difficult to be able to solve it in fully-connected graphs rather than in arbitrary graphs.

With both $!!_{\exists}a$ and $??_{\forall}a$ actions:

- for arbitrary graphs, it should be undecidable;

Thank you for your attention!