Distributed local strategies in broadcast networks

Nathalie Bertrand
Inria Rennes, France

joint work with Paulin Fournier and Arnaud Sangnier

CDPS, August 2016, Singapore

Motivation

Verification of networks of processes of unbounded size

Why considering such networks?

- Distributed algorithms (*mutual exclusion, leader election,...*)
- Telecommunication protocols (*routing,...*)
- Algorithms for ad-hoc networks
- Biological systems
- ...

Crowd networks

All the processes have the same behavior

They form a **crowd** [Esparza, STACS'14]

More precisely:

- Every process follows a same given protocol
- Processes can communicate, by either
  - Message passing
  - Shared variables
  - Rendez-vous communications
  - **Broadcast communications**
  - **Multi-diffusion (selective broadcasts)**

Question:
Is a goal reachable in some network with N processes ?

This talk

Decidability and complexity of reachability problems in parameterized networks

Features:

- Simple protocols with broadcast communication
- Simple reachability questions
- **Taking into account some *locality* assumptions**

Outline

Outline

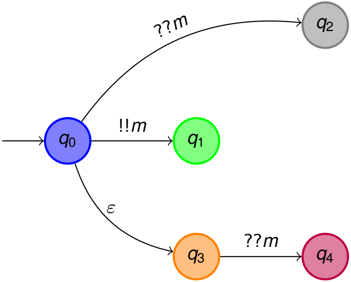
1. Networks of reconfigurable broadcast protocols
2. Restricting to local strategies
3. Conclusion

A model for reconfigurable broadcast networks

Main characteristics [Delzanno *et al.* CONCUR'10]

- No creation/deletion of nodes
- Each node executes the same finite state process
- Broadcast of the messages to the neighbors
- Communication topology evolves non-deterministically

Reconfigurable Broadcast Networks: syntax



A protocol

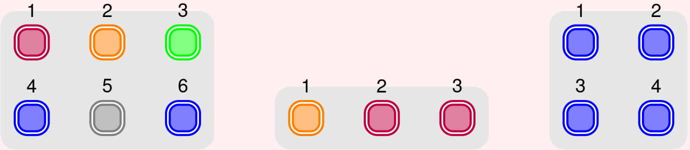
Finite state automaton. Transitions labelled with:

1. broadcast of messages - $!!m$
2. reception of messages - $??m$
3. internal actions - ε

A protocol defines a reconfigurable broadcast network

Configurations

A configuration is a vector of arbitrary size



- **Initial configurations**: **all** vertices labelled with the initial state
- *Notation :* lab(γ) *for all the labels present in* γ

Remarks:

- Size of configurations is not bounded

$\Rightarrow$ **Broadcast networks are infinite state systems**

Reconfigurable Broadcast Networks: semantics

Transition system associated with *P*

- $\mathcal{C}$: set of configurations
- $\mathcal{C}_0$: set of initial configurations
- $\rightarrow: \mathcal{C} \times \mathcal{C}$: transition relation
  - Choice a of process
  - Choice of a neighbor set
  - Execution of an action

Reconfigurable Broadcast Networks: semantics

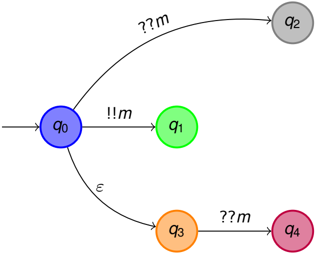
Transition system associated with P

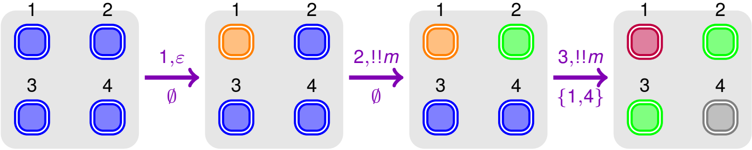
- $\mathcal{C}$: set of configurations
- $\mathcal{C}_0$: set of initial configurations
- $\rightarrow : \mathcal{C} \times \mathcal{C}$: transition relation
  - Choice a of process
  - Choice of a neighbor set
  - Execution of an action

Characteristics

- The number of vertices does not change
- Two kinds of transitions
  1. **local actions** - one process performs an internal action ε
  2. **broadcast** - one process emits a message with !!*m*, all its neighbors that can receive it with ??*m* must receive it

Reconfigurable Broadcast Networks: an example





Parameterized reachability

Parameter: Number of processes

Control State Reachability (REACH)

Input: A protocol and a control state q;

Output: Does there exist $\gamma \in \mathcal{C}_0$ and $\gamma' \in \mathcal{C}$ s.t. $\gamma \rightarrow^* \gamma'$ and $q \in \mathsf{lab}(\gamma')$?

Parameterized reachability

Parameter: Number of processes

Control State Reachability (REACH)

Input: A protocol and a control state q;

Output: Does there exist $\gamma \in \mathcal{C}_0$ and $\gamma' \in \mathcal{C}$ s.t. $\gamma \rightarrow^* \gamma'$ and $q \in \text{lab}(\gamma')$?

Remarks:

- Infinite number of possible initial configurations
- Reachability of a given configuration γ' is easy, since **the number of processes is fixed**

Parameterized reachability

Parameter: Number of processes

Control State Reachability (REACH)

Input: A protocol and a control state q;

Output: Does there exist $\gamma \in \mathcal{C}_0$ and $\gamma' \in \mathcal{C}$ s.t. $\gamma \to^* \gamma'$ and $q \in \mathrm{lab}(\gamma')$?

Remarks:

- Infinite number of possible initial configurations
- Reachability of a given configuration γ' is easy, since **the number of processes is fixed**

Theorem [Delzanno et al. FSTTCS'12]

REACH is PTIME-complete for reconfigurable broadcast networks

Outline

Local strategies

Processes do not really behave the same!

- They all follow the same protocol P, yet...
- ... if the protocol is non-deterministic, each process can take a different choice!

Local strategies

Processes do not really behave the same!

- They all follow the same protocol P, yet...
- ... if the protocol is non-deterministic, each process can take a different choice!

Local strategies dictate processes what to do given their (local) past

Two processes with same past behave similarly

Local strategy $\sigma = (\sigma_a, \sigma_r)$

- σ_a : Path(P) $\mapsto (Q \times (\{!!m\} \cup \{\varepsilon\}) \times Q)$ active actions
- σ_r : Path(P) $\times \Sigma \mapsto (Q \times \{??m\} \times Q)$ receptions

Reachability question under local strategies

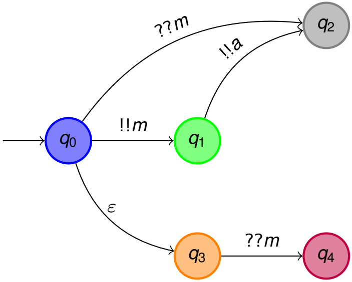
An execution respects a local strategy iff each process chooses transitions as given by the strategy

Control State Reachability (REACH[L])

Input: A protocol and a control state $q \in Q$;

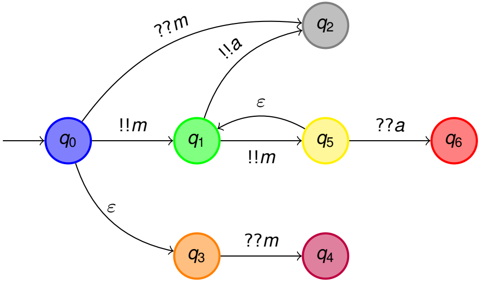
Output: Does there exist $\gamma \in \mathcal{C}_0$ and $\gamma' \in \mathcal{C}$ and a local strategy σ s.t. $\gamma \to^* \gamma'$ respects σ and $q \in \mathsf{lab}(\gamma')$?

Local strategies on an example



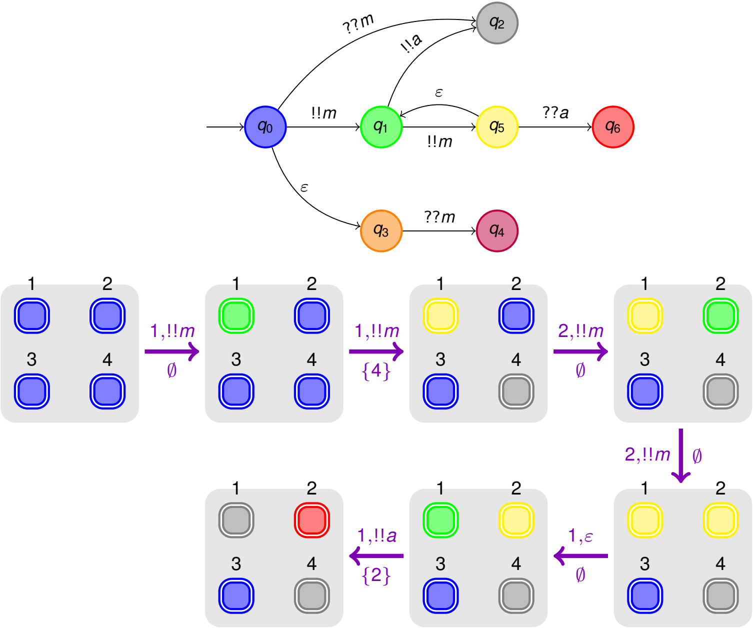
- There is no local strategy to reach q_4
  - from q_0, either all processes move to q_1, or they all move to q_3

Local strategies on an example

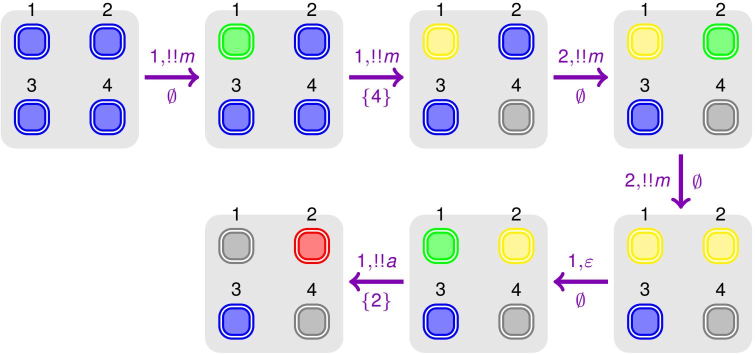


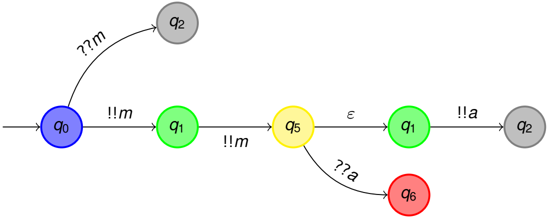
- There is no local strategy to reach q_4
  - from q_0, either all processes move to q_1, or they all move to q_3
- There exists a local strategy to reach q_6

Local executions on an example



Local executions on an example



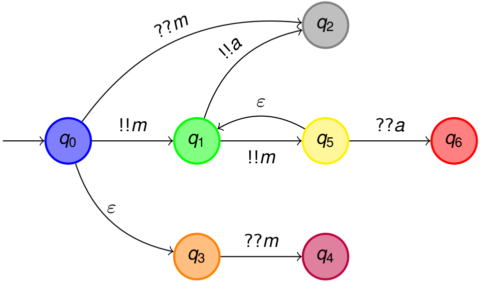


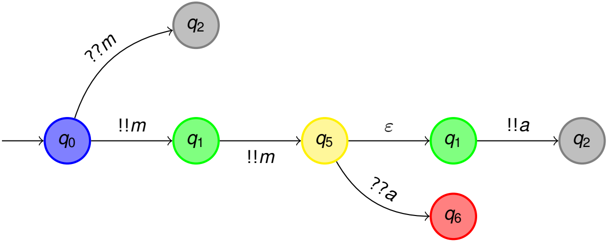
Strategy patterns for reconfigurable networks

Local strategies can be represented by trees

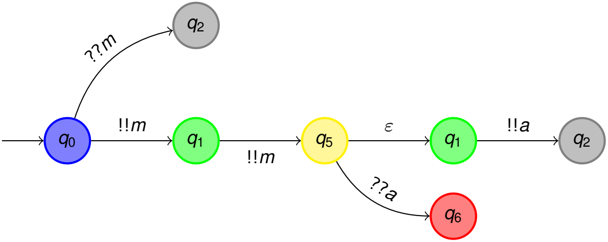
- Each path in the tree is a path in the unfolded protocol
- From each node in the tree:
  - **At most one outgoing edge is labelled by an active action (broadcast or internal action)**
  - **At most one outgoing edge labelled $??m$ per message m**
- Strategy patterns are underspecified local strategies: they may represent several local strategies

Example of strategy patterns





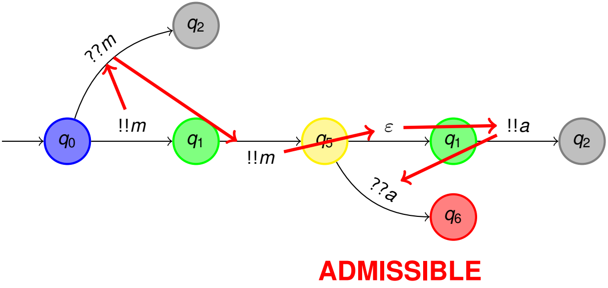
Admissible strategy patterns



An admissible strategy pattern

- A strategy pattern

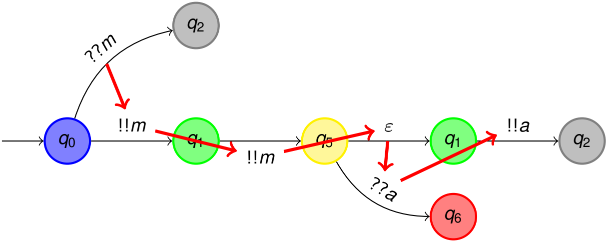
Admissible strategy patterns



An admissible strategy pattern

- A strategy pattern **+ a total order on the edges s.t.**
  - The order in the tree is satisfied
  - Each ??m is preceded by some !!m

Admissible strategy patterns

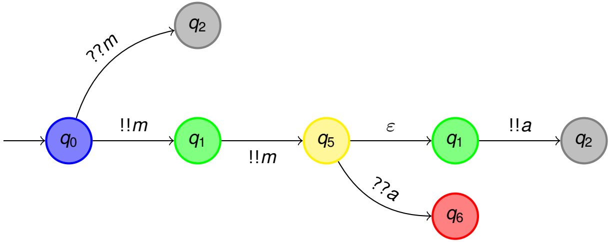


NOT ADMISSIBLE

An admissible strategy pattern

- A strategy pattern **+ a total order on the edges s.t.**
  - The order in the tree is satisfied
  - Each ??m is preceded by some !!m

Admissible strategy patterns



An admissible strategy pattern

- A strategy pattern **+ a total order on the edges s.t.**
  - The order in the tree is satisfied
  - Each ??*m* is preceded by some !!*m*

Checking whether there exists an order such that the strategy pattern is admissible can be done in polynomial time

Solving REACH[L]

How to use strategy patterns ?

Soundness and correctness

A state is reachable in Reconfigurable Networks under a local strategy iff there is an admissible strategy pattern containing it.

Solving REACH[L]

How to use strategy patterns ?

Soundness and correctness

A state is reachable in Reconfigurable Networks under a local strategy iff there is an admissible strategy pattern containing it.

Minimization

If there exists an admissible strategy pattern containing q, then there exists one of polynomial size.

Solving REACH[L]

How to use strategy patterns ?

Soundness and correctness

A state is reachable in Reconfigurable Networks under a local strategy iff there is an admissible strategy pattern containing it.

Minimization

If there exists an admissible strategy pattern containing q, then there exists one of polynomial size.

Theorem

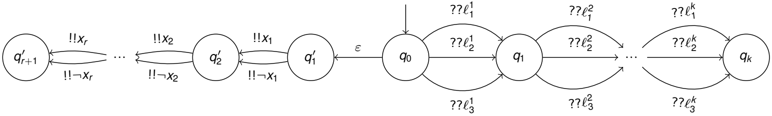
REACH[L] is in NP for Reconfigurable Broadcast Networks.

NP-hardness

- Reduction from 3SAT
- 3SAT formula $\bigwedge_{i \in [1..k]} \ell_1^i \vee \ell_2^i \vee \ell_3^i$ over the variables $\{x_1, \ldots, x_r\}$

NP-hardness

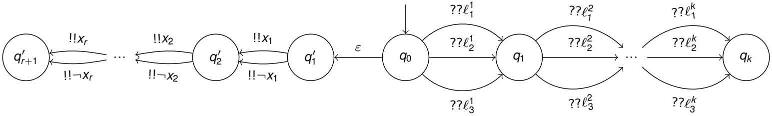
- Reduction from 3SAT
- 3SAT formula $\bigwedge_{i \in [1..k]} \ell_1^i \vee \ell_2^i \vee \ell_3^i$ over the variables $\{x_1, \ldots, x_r\}$



- Locality $\implies$ Uniform choice for x_i or $\neg x_i$
- Local strategy $\equiv$ Valuation
- q_k reachable iff formula satisfiable

NP-hardness

- Reduction from 3SAT
- 3SAT formula $\bigwedge_{i\in[1..k]} \ell_1^i \vee \ell_2^i \vee \ell_3^i$ over the variables $\{x_1, \ldots, x_r\}$



- Locality $\implies$ Uniform choice for x_i or $\neg x_i$
- Local strategy $\equiv$ Valuation
- q_k reachable iff formula satisfiable

Theorem

REACH[L] is NP-complete in Reconfigurable Broadcast Networks.

Convergence Problem

Target State Convergence (TARGET)

Input: A protocol and a set of control states T;

Output: Does there exist $\gamma \in \mathcal{C}_0$ and $\gamma' \in \mathcal{C}$ s.t. $\gamma \rightarrow^* \gamma'$ and lab(γ') $\subseteq T$?

Theorem

TARGET[L] is NP-complete in Reconfigurable Broadcast Networks.

Idea of the proof:

- Again based on strategy patterns
- Refine the notion of admissibility: the order must ensure one can 'empty' nodes towards the target set
- Still polynomial size admissible trees

Fully connected networks

Clique topology

Every broadcast necessarily reaches all participants.

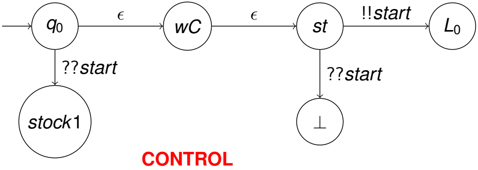
Theorem

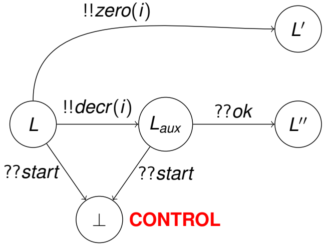
REACH[L] and TARGET[L] are undecidable in Clique Networks.

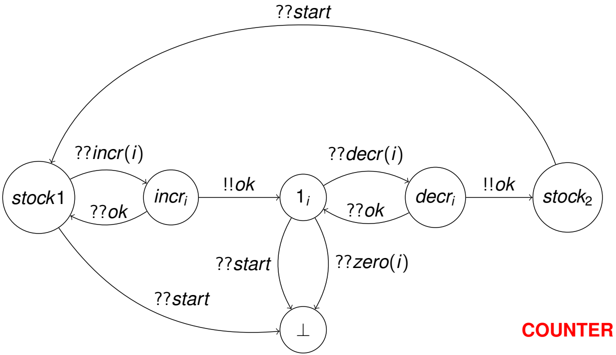
Idea of the proof:

- Encode the behavior of a Minsky machine
- For TARGET[L], as for TARGET in Clique Networks
- For REACH[L]:
  - Simulate the same run twice
  - Locality forces to do the same simulation
  - The second run can use at most as many processes for the counters as in the first run
  - Clique topology guarantees increment/decrement by 1 only

Undecidability of REACH[L] in Clique Networks







How to regain decidability?

A complete protocol

- From every state, at least one edge is labelled with an active action (internal or broadcast)
- From every state, for each message *m*, some edge is labelled with ??*m*

Property of complete protocols in clique networks: at each broadcast, all processes change their past

Theorem

REACH[L] in Clique Networks of complete protocols is decidable.

Idea of the proof:

- Abstraction: Represent processes with the same past by a single process
- Well-structured transition system

Outline

Conclusion

Local strategies in reconfigurable broadcast networks

Adding locality assumption

- all processes behave the same
- reachability and convergence are NP-complete
- technical tool: strategy patterns
- polynomial cutoff on the number of processes needed
- undecidability for clique topology
  (unless restricting to complete protocols)