Formal Verification of Mobile Robot Protocols

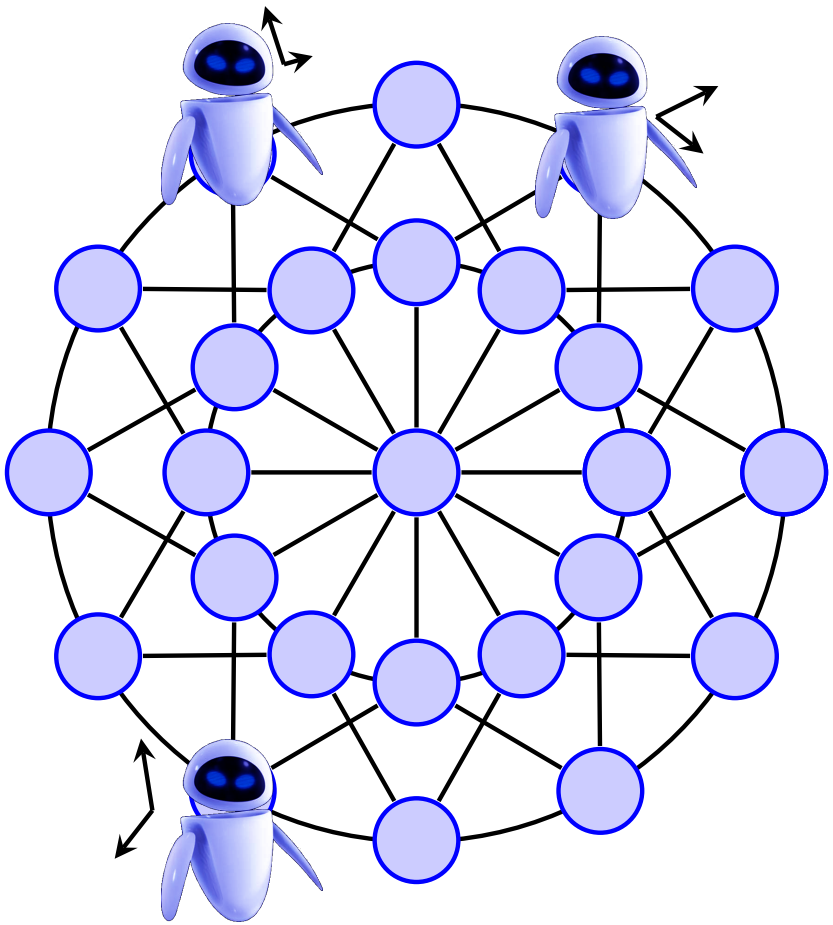
Modelling and Verifying Parallel processes

Laure Millet

Béatrice Bérard
Maria Potop-Butucaru
Yann Thierry-Mieg
Sébastien Tixeuil

5 décembre 2012

Context



A global objective :

Explore an unknown environment

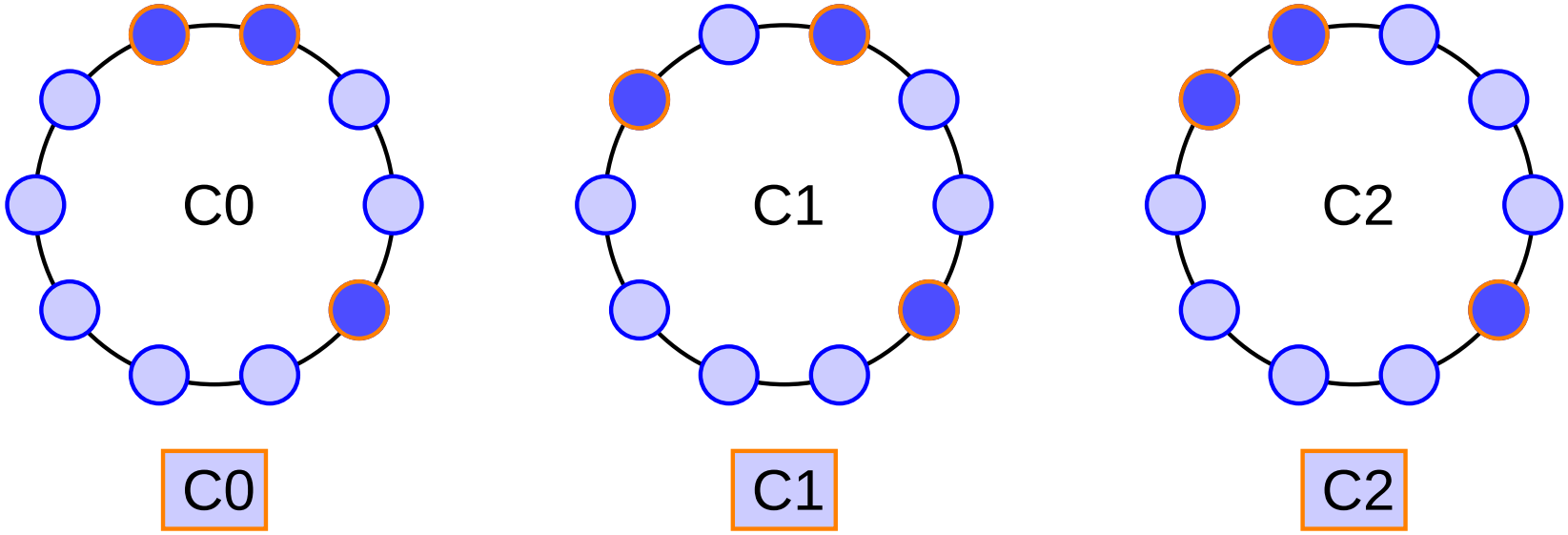
Robot Model [SY1993]

Restricted robot

Min-Algorithm :

3 robots explore a ring of size 10

Exploration phase



Problematic

Verification

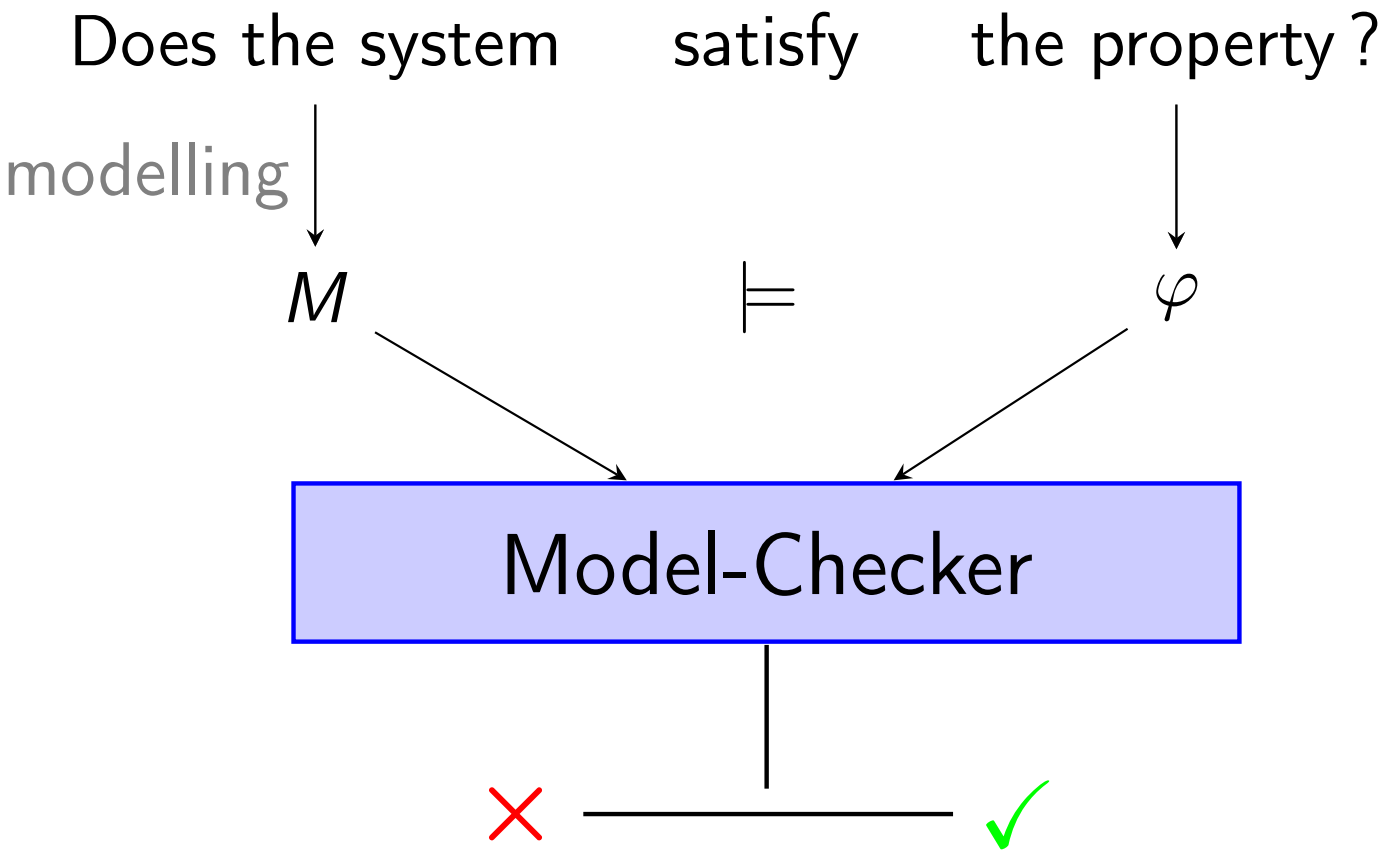
Exhaustive hand made proof

Given an algorithm, how to formally verify it ?

Two execution models

- Synchronous : SYm [SY1993]
- Asynchronous : CORDA [Prencipe2000]

Model-Checking



Modelling

System

The system is divided in sub-components :

- Robot behavior : Robots
- Execution models : Scheduler

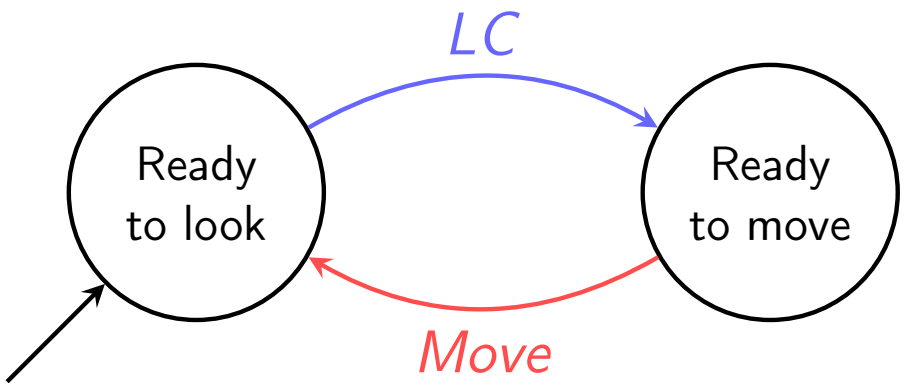
Each sub-component is modeled by a finite automaton

The system is the synchronized product of these automata

Property

Temporal logic : LTL

Robots

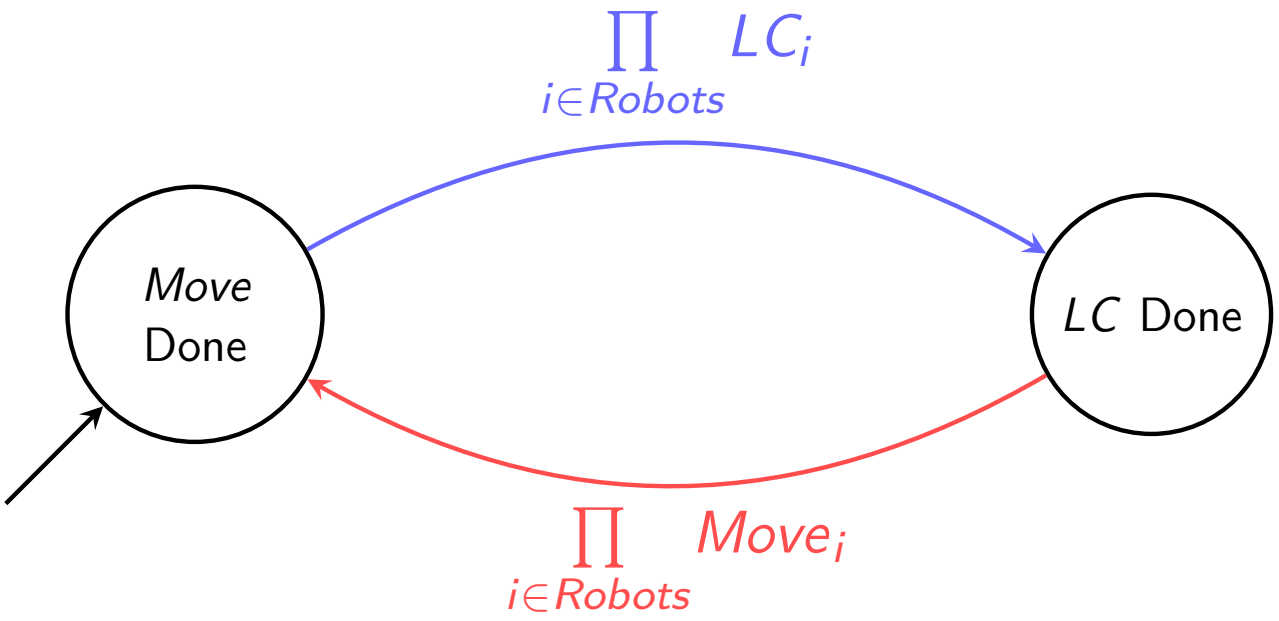


Computations and moves

- Depend on the topology
- Described by an algorithm

Scheduler

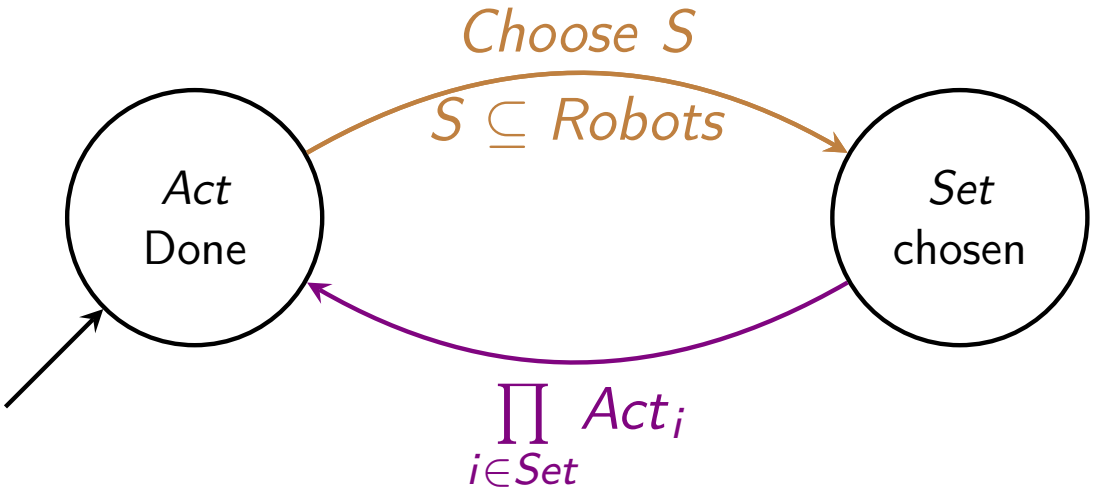
SYm : The synchronous model



All robots are synchronized

Scheduler

CORDA : The asynchronous model



Asynchronous environment :

Moves can be executed from an outdated observation

Fairness : $GF(\textit{schedule all robots})$

Model-Checking of Min-Algorithm

The Exclusive Perpetual Exploration

- Exclusivity :
  $G(\textit{no two robots on the same node nor on the same edge})$
- Perpetual Exploration : $GF(\textit{All robots explore all nodes})$

Model-Checking

For the minimal ring size : $n = 10$

States	Transitions	Model	$\models$
1 499	2 250	SYm	✓
19 745	39 363	CORDA	×

Algorithm patch and Model-Checking

Modifications

Moves made from obsolete observations

Algorithm patch and Model-Checking

Modifications

Moves made from obsolete observations

Model-Checking

n	States	Transitions	Memory (kB)	Time	$\models$
10	1.581.961	6.090.209	1.416.880	7min	✓
11	1.926.385	7.421.315	1.568.748	9min	✓
13	2.716.637	10.476.317	2.252.600	21min	✓
14	3.162.409	12.307.905	2.560.724	27min	✓
16	4.155.385	16.041.365	2.772.188	36min	✓

Conclusion and Perspectives

Conclusion

- Models generator
  - DiVinE : An LTL model-checker
  - Models : SYm and CORDA
- Verification
  - Algorithms [BMPT2010]
  - Counter-example production

Perspectives

- Algorithms Formal Verification
  - On other graph shapes
  - With probabilistic rules
- Controller Synthesis
  Find a winning strategy for the robot coalition

Bibliographie

BMPT2010 L. Blin, A. Milani, M. Potop-Butucaru, et S. Tixeuil, « Exclusive perpetual ring exploration without chirality », Distributed Computing, p. 312–327, 2010.

BBCR2010 J. Barnat, L. Brim, M. Češka, et P. Ročkai, « DiVinE : Parallel Distributed Model Checker », in Parallel and Distributed Methods in Verification, 2010.

SY1993 I. Suzuki et M. Yamashita, « Distributed anonymous mobile robots : Formation of geometric patterns », 1993.

Prencipe2000 G. Prencipe, «A new distributed model to control and coordinate a set of autonomous mobile robots : the CORDA model», 2000.