Année 2019-2020

# Proposition de sujet de stage M2

MODÈLES MÉCANIQUES FORMELS POUR L'ALGORITHMIQUE DISTRIBUÉE, COMPORTEMENTS PROBABILISTES


LIEUX : LIRIS
Bât Nautibus, Université Claude Bernard Lyon 1
69100 Villeurbanne

et LIP6
Sorbonne Universités
4 place Jussieu,
75005 Paris

PERSONNES ENCADRANT LE STAGE :

| | Pierre Courtieu, | Xavier Urbain, | Sébastien Tixeuil |
|---|---|---|---|
| Tél. : | 01 40 27 24 13, | 04 27 46 57 07, | 01 44 27 87 62 |

Email : pierre.courtieu@cnam.fr, xavier.urbain@univ-lyon1.fr, sebastien.tixeuil@lip6.fr


## CONTEXTE ET OBJECTIFS SCIENTIFIQUES

*Ce stage se place dans le contexte du projet ANR SAPPORO (2020-2024) dont sont partenaires l'université Lyon-1, Sorbonne Université, le CNAM Paris et le Tokyo Institute of Technology (Japon).*
https://liris.cnrs.fr/recherche/safe-adaptive-and-provable-protocols-oblivious-robots-operation

L'algorithmique distribuée fait partie des domaines où le raisonnement informel n'est pas une option, en particulier lorsque des erreurs dites byzantines peuvent survenir. Elle est également caractérisée par une grande diversité de modèles dont les modulations subtiles impliquent des propriétés radicalement différentes. On considère dans ce travail les « réseaux de robots » : nuages d'entités *autonomes* devant accomplir une tâche *en coopération*. Dans ce cadre émergent, les modèles sont distingués par les capacités des robots, la topologie de l'espace dans lequel ils évoluent, le degré de synchronisme (modélisé par les propriétés du démon d'activation), les caractéristiques des erreurs pouvant survenir, etc.

On s'intéresse à l'obtention, à l'aide de l'assistant à la preuve Coq, de garanties mécaniques formelles de propriétés de certains protocoles distribués [7]. Un modèle Coq [1] pour les réseaux de robots récemment présenté capture assez naturellement de nombreuses variantes de ces réseaux, notamment en ce qui concerne la topologie ou les propriétés des démons. Ce modèle est bien sûr à l'ordre supérieur et s'appuie sur des types coinductifs. Il permet de démontrer en Coq à la fois des propriétés positives : le programme embarqué dans chacun des robots permet de réaliser la tâche *quelle que soit* la configuration de départ [6, 4] comme des propriétés négatives : il *n'existe aucun* programme embarqué permettant de réaliser la tâche [5, 2].

Le stage aborde les aspects *probabilistes* pouvant intervenir dans le comportement des robots. Un algorithme randomisé est en effet bien pratique pour briser des symmétries rendant inopérants des protocoles complètement déterministes ; une bonne illustration en est donnée par exemple dans un récent article de Yamauchi & Yamashita [8].

Il consiste en l'étude, d'une part, et l'introduction au sein du framework formel, d'autre part, des composantes probabilistes.
*Une étude de cas* intéressante pourrait concerner l'extension de solutions actuelles ASYNC de scattering (Lechine2019) (qui requiert de la randomisation) à une complexité polynomiale en moyenne.

Une bibliothèque Coq telle `alea` [1, 3] pourra être utile pour la mécanisation formelle.

## CONTEXT AND SCIENTIFIC GOALS

Distributed computing is one of the domains where informal reasoning is not an option, in particular when Byzantine failures are involved. What characterises also Distributed Computing is its diversity of models subtle modifications of which induce radical change in the system behaviour. We consider Robot Networks, that is swarms of *autonomous* mobile entities that have to accomplish some task in *cooperation*. In this emerging framework, models can be distinguished by the capabilities of robots, the

1. http://pactole.lri.fr

topology of the considered space, the level of synchrony (that is the properties of a demon), the type of the failures likely to occur, etc.

We are interested in obtaining formal and moreover mechanical guarantees of properties for certain protocols, using the Coq proof assistant. A Coq framework[1] for robot networks recently proposed can express quite a few variants of models for such networks, in particular regarding topology or demon properties. This framework is higher order and based on coinductive types. It allows to prove in Coq positive results (the task will be fulfilled using the algorithm embedded in all robots *for all* initial configuration) [6, 4] as well as negative results (*there cannot be any* embedded algorithm that will work for this task for all initial configuration) [5, 2].

As a matter of fact, *randomised algorithms* are most convenient to handle situations where symmetricity makes any deterministic protocol useless. See for instance the recent article by Yamauchi & Yamashita [8].

An objective of this proposal is to extend the formal framework so as to express and allow one to work on robot behaviours that are *probabilistic*.
An interesting case study would be to extend the current ASYNC solutions (Lechine2019) to scattering (which inherently requires randomisation) to a polynomial expected complexity.

The Coq library `alea` [1, 3] could be an interesting starting point to this goal.

COMPÉTENCES :

— Assistant à la preuve Coq,
— Algorithmique distribuée.

# Références


[1] Philippe Audebaud and Christine Paulin-Mohring. Proofs of Randomized Algorithms in Coq. *Science of Computer Programming*, 74(8) :568–589, 2009.

[2] Cédric Auger, Zohir Bouzid, Pierre Courtieu, Sébastien Tixeuil, and Xavier Urbain. Certified Impossibility Results for Byzantine-Tolerant Mobile Robots. In Teruo Higashino, Yoshiaki Katayama, Toshimitsu Masuzawa, Maria Potop-Butucaru, and Masafumi Yamashita, editors, *Stabilization, Safety, and Security of Distributed Systems - 15th International Symposium (SSS 2013)*, volume 8255 of *Lecture Notes in Computer Science*, pages 178–186, Osaka, Japan, November 2013. Springer-Verlag.

[3] David Baelde, Pierre Courtieu, David Gross-Amblard, and Christine Paulin. Towards provably robust watermarking. In *ITP*, 2012.

[4] Thibaut Balabonski, Amélie Delga, Lionel Rieg, Sébastien Tixeuil, and Xavier Urbain. Synchronous gathering without multiplicity detection : A certified algorithm. *Theory of Computing Systems*, 2018. https://doi.org/10.1007/s00224-017-9828-z.

[5] Pierre Courtieu, Lionel Rieg, Sébastien Tixeuil, and Xavier Urbain. Impossibility of Gathering, a Certification. *Information Processing Letters*, 115 :447–452, 2015.

[6] Pierre Courtieu, Lionel Rieg, Sébastien Tixeuil, and Xavier Urbain. Certified universal gathering algorithm in $\mathbb{R}^2$ for oblivious mobile robots. In Cyril Gavoille and David Ilcinkas, editors, *Distributed Computing - 30th International Symposium, (DISC 2016)*, volume 9888 of *Lecture Notes in Computer Science*, Paris, France, September 2016. Springer-Verlag.

[7] Maria Potop-Butucaru, Nathalie Sznajder, Sébastien Tixeuil, and Xavier Urbain. Formal methods for mobile robots. In Paola Flocchini, Giuseppe Prencipe, and Nicola Santoro, editors, *Distributed Computing by Mobile Entities*, volume 11340 of *Lecture Notes in Computer Science, Theoretical Computer Science and General Issues*, pages 278–313. Springer Nature, 2019.

[8] Yukiko Yamauchi and Masafumi Yamashita. Randomized Pattern Formation Algorithm for Asynchronous Oblivious Mobile Robots. In Fabian Kuhn, editor, *Distributed Computing - 28th International Symposium, (DISC 2014)*, volume 8784 of *Lecture Notes in Computer Science*, pages 137–151, Austin, USA, October 2014. Springer-Verlag.