

**Proposition de sujet de stage M2**

MODÈLES FORMELS POUR LES ESSAIS DE ROBOTS, ESPACES

LIEU : LRI/PCRI et Cédric, CNAM & ENSIIE  
Bât 650, Université Paris Sud 292 rue Saint-Martin  
91405 Orsay Cedex France 75003 Paris

PERSONNES ENCADRANT LE STAGE :

Xavier Urbain, Pierre Courtieu, Sébastien Tixeuil  
Tél. : 01 69 36 73 38, 01 40 27 24 13, 01 44 27 87 62  
Email : xavier.urban@ensiie.fr, pierre.courtieu@cnam.fr,  
sebastien.tixeuil@lip6.fr

CONTEXTE ET OBJECTIFS SCIENTIFIQUES

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. Un modèle Coq<sup>1</sup> 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 [2], comme des propriétés négatives : *il n'existe aucun* programme embarqué permettant de réaliser la tâche [3, 1].

Le stage consiste à étendre le modèle formel à d'autres topologies (des réseaux discrets par exemple, anneaux, etc.) et des dimensions supérieures afin de proposer un cadre apte à établir des résultats nouveaux notamment pour l'exploration et les tâches d'élection d'un chef ou de formation de motifs géométriques. Ces deux problèmes ont été montrés équivalents (au sens où il existe un algorithme pour résoudre l'un des problèmes si on dispose en entrée de la solution de l'autre problème, et vice-versa) sous des hypothèses système particulières. L'extension de cette équivalence à un modèle moins contraint est un problème ouvert intéressant.

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 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<sup>1</sup> 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) [2] as well as negative results (*there cannot be any* embedded algorithm that will work for this task for all initial configuration) [3, 1].

---

1. <http://pactole.lri.fr>

An objective of this proposal is to extend this framework to some particular topologies (discrete spaces, and higher dimensions) so as to propose a framework in which some new results could be formally established, in particular regarding exploration, the election of a leader, or the formation of geometrical patterns. Those two problems have been shown equivalent (meaning that there is an algorithm that solves one of them if one has as an input a solution for the other one) under some particular assumptions. Extending this equivalence to less constrained models is an interesting open problem.

COMPÉTENCES :

— Assistant à la preuve Coq.

## Références

- [1] 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.
- [2] Pierre Courtieu, Lionel Rieg, Sébastien Tixeuil, and Xavier Urbain. A Certified Universal Gathering Algorithm for Oblivious Mobile Robots. *CoRR*, abs/1506.01603, 2015.
- [3] Pierre Courtieu, Lionel Rieg, Sébastien Tixeuil, and Xavier Urbain. Impossibility of Gathering, a Certification. *Information Processing Letters*, 115 :447–452, 2015.