Proposition de sujet de stage M2

FORMAL MECHANICAL MODELS FOR DISTRIBUTED COMPUTING – LUMINOUS ROBOTS

LOCATIONS:	LIRIS	and possibly	D2S
	Bât Nautibus, Université Claude Bernard Lyon 1		Tokyo Institute of Technology
	69100 Villeurbanne		Tokyo, Japon

PERSONNES ENCADRANT LE STAGE :

Pierre Courtieu,	Xavier Urbain,	Xavier Défago
Tél. : 01 40 27 24 13,	04 27 46 57 07,	
Email : pierre.courtieu@cnam.fr	xavier.urbain@univ-lyon1.fr,	defago@c.titech.ac.jp

CONTEXT AND SCIENTIFIC GOALS

This work takes place within the ANR project SAPPORO (2020-2024) involving Université Lyon-1, Sorbonne Université, CNAM Paris (France), and Tokyo Institute of Technology (Japan).

https://sapporo.liris.cnrs.fr

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[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) [4, 2] as well as negative results (*there cannot be any* embedded algorithm that will work for this task for all initial configuration) [3, 1].

This internship focuses on autonomous robots with lights, in Euclidean spaces, and in particular on the validation, within Pactole, of a Model-Cheking abstraction recently proposed by Defago et al.

Model checkers are indeed relatively safe tools in the sense that when a model checkers takes a formula and answers "YES" one can be reasonably sure that there is a model for this formula. Howevern it is much more difficult to be certain that the formula that has been given is a correct abstraction of the initial problem one wants to solve. The argument is usually a pen and paper proof in a scientific publication, that is: checked by human beings who can leave a few subtle errors.

RECOMMENDED PREVIOUS KNOWLEDGE:

- Formal proof, Proof assitants (Coq),
- Distributed Computing.

References

[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] 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.

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

[4] 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.