Research Internship

Comparing Models of Computation in the Presence of Byzantine Faults

Topic profile

distributed computing

theory/math

Tags

#distributed computing

#models of computation

#task solvablity

Supervision

Thomas Nowak (webpage)

Professor at ENS Paris-Saclay

Dhrubajyoti Ghosh (webpage)

PhD Student at ENS Paris-Saclay

Context

Distributed computing has been studied through a variety of models that differ in communication primitives, synchrony assumptions and fault types. A natural question is how these models compare in their computational power. Specifically, we use the solvability of decision tasks [1] as a metric to understand the computational power of a model. This is valuable when two models are equivalent and one offers a simpler setting for analysis and verification. Message passing models with asynchronous communication are realistic but many algorithms for solving tasks in these models rely on constructing a virtual "round" structure, thus boiling down the problem to synchronous message passing models. However, it is not clear whether this approach can always be used to solve tasks in asynchronous models. Many Byzantine Fault Tolerance (BFT) and blockchain protocols rely on such reductions, which highlights the need to examine their limits.

What we are looking for

Students with a background in computer science or mathematics and an interest in theoretical distributed computing.

Research

As a starting point, we look at the Asynchronous Message Passing model with up to f benign faults, AMP_f, where processes fail by crashing. The virtual round construction technique in AMP_f leads us to consider the Heard-Of model with up to f message omissions, HO_f. Recent work by the team [2] has demonstrated the conditions under which AMP_f and HO_f are equivalent and separated, thus showing when the virtual round construction approach can and cannot be used in AMP_f.

As a natural next step, we now move on from benign faults to Byzantine faults where processes can lie to each other. It has been studied whether a basic round structure building approach can always be used to solve tasks in the asynchronous model with Byzantine faults [3]. Our goal is to study whether even more complex round structure building approaches are always general or not.

References

[1] Herlihy, Kozlov, Rajsbaum. *Distributed Computing Through Combinatorial Topology*.

[2] Attiya, Castañeda, Ghosh, Nowak. *arXiv*, URL.

[3] Attiya, Flam, Welch. *arXiv*, URL.

The team

You will be part of an interdisciplinary research team at ENS Paris-Saclay near Paris, working on different aspects of distributed computing, synthetic biology, circuit design and artificial intelligence.

You are interested or would like to join us?

Please send us your questions or, in case you would like to apply, a short statement of interest and a CV, to Thomas Nowak (thomas@thomasnowak.net) and Dhrubajyoti Ghosh (dghosh@lmf.cnrs.fr).