Logical Foundations of Self-Adapting Distributed Systems

Radu IOSIF (VERIMAG, Grenoble)
mailto:Radu.Iosif@univ-grenoble-alpes.fr
https://nts.imag.fr/index.php/Radu_Iosif

1 Context, goal and challenges

Applications of distributed systems are omnipresent, allowing to share resources and coordinate activities between geographically distributed parties. Furthermore, they increase the resilience of systems through fault tolerance, availability, and recovery mechanisms. Designing, understanding, and validating distributed systems is challenging because of the huge number of interactions between components, some potentially leading to unpredictable scenarios. Ensuring the correctness of distributed systems is not yet mature — to cite Lamport[1]:

> *[Concurrent] algorithms can be quite subtle and hard to get right, their correctness proofs require a degree of precision and rigor unknown to most mathematicians (and many computer scientists).*

Reconfiguration is inherent to modern distributed computing. Processes can be created or removed due to internal faults, redistribution of resources, workload or traffic changes. Moreover, the shape of the communication network may change. Cloud computing, IoT and edge computing vitally relly on such features.

Self-adapting systems initiate and carry out reconfiguration sequences automatically, in order to avoid expensive or even mission-critical downtimes, required by manual reconfiguration. The verification techniques developped in this thesis will be designed with such dynamic reconfiguration aspects in mind.

2 Methodology and workplan

The successful candidate will develop logics and automated reasoning techniques that enable writing formal proofs of correctness of self-adapting distributed systems. A promising approach is using logics that describe the shape of a network (i.e., the interconnection of processes via communication channels) and how this shape changes with time. Recent work of the hosting group at VERIMAG considers a variant of *Separation Logic*[2] equipped with a special connective that decomposes a structure into sub-structures with disjoint interpretations of the relations from the signature. This logic has been used to write Hoare-style proofs of correctness of dynamic reconfiguration programs[3] and check absence of concurrency errors in infinite sets of configurations[4]. Preliminary steps in understanding the connections of Separation Logic with more standard formalisms, such as Monadic Second Order Logic[5] or Hyperedge-replacement Graph Grammars[6] have also been undertaken[7].

Particular attention will be devoted to the implementation of practical verification tools based on automated theorem proving and model checking based on the logics developped in this thesis. To this end, the candidate is expected to work on implementation and prototyping, in addition to theoretical research.

3 Funding and application

The thesis will be carried out under a 3-year contract funded by the University of Grenoble Alpes. Applications should be posted to the ADUM website https://adum.fr/ and evaluated by a selection jury. The application process is described at https://edmstii.univ-grenoble-alpes.fr/. Please contact mailto:Radu.Iosif@univ-grenoble-alpes.fr for further assistance.

[1] L. Lamport. How to write a 21st century proof. *Journal of Fixed Point Theory and Applications*, 11(1):43–63, 2012.

[2] https://en.wikipedia.org/wiki/Separation_logic

[3] E. Ahrens, M. Bozga, R. Iosif, and J.-P. Katoen. Reasoning about distributed reconfigurable systems. *Proc. ACM Program. Lang.*, 6(OOPSLA2), 2022. https://dl.acm.org/doi/abs/10.1145/3563293

[4] M. Bozga, R. Iosif, and J. Sifakis. Verification of component-based systems with recursive architectures. *Theor. Comput. Sci.*, 940(Part):146–175, 2023. https://www.sciencedirect.com/science/article/abs/pii/S0304397522006181

[5] https://en.wikipedia.org/wiki/Monadic_second-order_logic

[6] https://www.researchgate.net/publication/215991881_Hyperedge_replacement_graph_grammars

[7] R. Iosif and F. Zuleger. On the Expressiveness of a Logic of Separated Relations. https://arxiv.org/abs/2208.01520