Verifying Robustness of Distributed Systems against Weak Consistency Models

Supervisors:

Ahmed Bouajjani, Professor, Univ. Paris Diderot and Institut Universitaire de France.
https://www.irif.fr/~abou/

Constantin Enea, Maître de Conférences (Associate Professor), Univ. Paris Diderot.
https://www.irif.fr/~cenea/

Laboratory:
IRIF (Institut de Recherche en Informatique Fondamentale) https://www.irif.fr/en/index

Contact information:
Address: Univ. Paris Diderot, Bâtiment Sophie Germain, 8 place Aurélie Nemours, 75013 Paris.
Email: {abou, cenea}@irif.fr *Phone:* +33 (0) 1 5727 9264/41

1 Description of the project

1.1 General context

The modern society is based on the development of automated services that allow frequent and fast access, transformation, and storage of data. These services must be reliable and performant in the same time, which is a real challenge. Such services are insured by applications running over large scale networks. These applications use distributed implementations of abstract data structures allowing to manipulate data through abstract operations such as add, remove, increment, decrement, et). In fact, in order to ensure the availability and low latency, data are duplicated in several remote sites. Operations are executed locally, and updates are propagated to other sites through the network. Therefore, updates are in general not visible to all sites in the same time, and when they become visible, they are not necessarily visible to them in the same order. This leads to complex consistency issues that makes extremely hard to reason about the behaviours of such distributed data structures, and about the functional correctness of their clients (i.e., the applications using them).

Several correctness criteria of libraries implementing distributed data structures have been defined. These correctness criteria correspond to different levels of consistency guaranteed by these libraries to their clients. In fact, it can be shown that in the distributed setting, strong consistency (where all duplicas are always consistent) cannot be ensured in general, and only weaker consistency criteria, where duplicas are allowed to diverge momentarily under some conditions, can be guaranteed. Therefore, two important questions can be considered:

- Given a library implementing an abstract data structure, is this implementation robust against changes in the assumptions about the underlying execution platform, which means that the set of visible behaviours of this data structure is insensitive to degradations of the guarantees of the network (such as message reordering, message losses, etc.).
- Given the implementation of an application that is using an abstract data structure, is the functional correction of this application robust against relaxations of the consistency model guaranteed by the used libraries of distributed data structures.

1.2 Goal

The goal of this project is to investigate the decidability and the complexity of the two problems defined above for typical correctness criteria. An approach to tackle these problems is to investigate first their reduction to state reachability problems, and then, to determine conditions under which these state reachability problems can be solved.

1.3 Bibliography

The topic of this project is related to work on verifying correctness criteria for distributed data structure, as well as on work on verifying robustness against weak memory models (adopted in modern muti-processors).

- Ahmed Bouajjani, Roland Meyer, Eike Moehlmann. *Deciding Robustness against Total Store Ordering.* In 38th International Colloquium on Automata, Languages and Programming (ICALP'11), 2011.
- Ahmed Bouajjani, Egor Derevenetc, Roland Meyer. *Checking and Enforcing Robustness against TSO.* In 22nd European Symposium on Programming (ESOP'13), 2013.
- Ahmed Bouajjani, Constantin Enea, Jad Hamza. *Verifying eventual consistency of optimistic replication systems.* In 41st ACM SIGPLAN Symposium on Principles of Programming Languages (POPL'14), 2014.
- Ahmed Bouajjani, Constantin Enea, Rachid Guerraoui, Jad Hamza. *On Verifying Causal Consistency.* In 44th ACM SIGPLAN Symposium on Principles of Programming Languages (POPL'17), 2017.

1.4 Background

A solid background in theoretical aspects of computer science is required. Candidates must have or be ready to develop skills in topics such as formal verification, concurrency, automata, algorithms, complexity, computability.