Internship subject (Master 2 or Master 1)

Model Checking for Open Automata

Advisors: Rabéa Ameur-Boulifa[(1)] and Ludovic Henrio[(2)]

Place:
(1) Télécom Paris – Sophia Antipolis
or
(2) Laboratoire de l'Informatique du Parallélisme (LIP) – ENS de Lyon

Contact: `rabea.ameur-boulifa@telecom-paris.fr` or `ludovic.henrio@ens-lyon.fr`

Context

Ensuring the reliability of systems requires rigorous verification techniques. However, as systems – particularly distributed ones – grow in size and complexity, traditional approaches such as model checking face the well-known state explosion problem, which limits their scalability.

In recent years, research has introduced the theoretical foundations of open systems and defined the formalism of Open Automata (OA) [3, 4, 5]. Open Automata (OA) offer a formalism designed to tackle this issue, combining symbolic and compositional modelling. A distinctive feature of OA is the notion of a hole, which makes it possible to explicitly describe the interactions between a system and its environment. This enables compositional verification, where system components can be verified independently before combining the results. The transitions of OA are richer than those of classical labelled transition systems (LTSs): they include guards that express relations between automaton parameters and the actions of holes, as well as assignments encoding their effects. These models have been shown to possess desirable properties, such as the preservation of behavioural equivalences (e.g., bisimulation) under composition.

Despite these advantages, OA cannot be directly verified using standard model checking techniques [1]. The existing property specification languages, mostly temporal logics such as LTL or CTL, are designed for classical LTSs and do not account for the holes or environmental dependencies that are intrinsic to OA. To fully exploit the potential of OA for verification, it is necessary to develop new property specification languages capable of expressing the interactions between system behaviour and environmental actions.

To tackle this issue, we propose developing *a new temporal logic specifically designed for OAs, allowing for more scalable and effective verification.*

Objectives

This internship aims at developing a new temporal logic tailored for Open Automata, with the following objectives:

- Designing a property specification language suitable for Open Automata
- Defining a model-checking algorithm adapted to Open Automata.
- Validating the approach through examples.

References

[1] Manna, Z., Pnueli, A.: The temporal logic of reactive and concurrent systems – Specification. Springer (1992), https://doi.org/10.1007/978-1-4612-0931-7

[2] Clarke, E.M., Grumberg, O., Peled, D.A.: Model checking. MIT Press, London, Cambridge (1999)

[3] Ludovic Henrio, Eric Madelaine, Min Zhang: A Theory for the Composition of Concurrent Processes. In Albert, E., Lanese, I., eds.: 36th International Conference on Formal Techniques for Distributed Objects, Components, and Systems (FORTE). Volume LNCS-9688 of Formal Techniques for Distributed Objects, Components, and Systems., Heraklion, Greece (June 2016) 175–194. https://hal.inria.fr/hal-01299562

[4] Rabéa Ameur-Boulifa, Ludovic Henrio, Eric Madelaine: Compositional equivalences based on Open pNets. Journal of Logical and Algebraic Methods in Programming, 2022, 131, pp.100842. ⟨hal-03894031⟩.

[5] Rabéa Ameur-Boulifa, Quentin Corradi, Ludovic Henrio, Eric Madelaine: Refinements for Open Automata. 21st International Conference on Software Engineering and Formal Methods, SEFM 2023, Eindhoven, Netherlands. pp.11-29, (Extended version) ⟨hal-04193421⟩.