Internship subject (Master 2 or Master 1)

Refinement for open automata

Main advisor: Rabéa Ameur-Boulifa

Co-advisors: Ludovic Henrio and Eric Madelaine

Place: Eurecom – Sophia Antipolis
or
Laboratoire de l'Informatique du Parallélisme (LIP) – École Normale Supérieure de Lyon

Context

Establishing equivalences or refinement relations between programs or system is crucial for verifying correctness of programs, by establishing that one implementation is the refinement of a specification.

In the previous years, we have studied theoretical foundations for open systems and our formalism, called open automata, is able to represent operators of composition of processes, represented as hierarchically composed automata with holes and parameters. Our long term goal is to develop a methodology combining symbolic operational semantic and bisimulation equivalences with deductive reasoning on the data part, and in practice combining bisimulation algorithms with SMT solvers to get automatic procedures proving equational properties of these open systems. In the last years, we designed a weak bisimulation theory for open automata and a translation from a specification language that we used, called pNets, to open automata [4, 2, 3].

Among the properties of our formalisms, we are interested in compositionality: If two systems are proven equivalent they will be undistinguishable by their context, and they will also be undistinguishable when their holes are filled with equivalent systems. The article [4] is illustrated with a transport protocol running example; it shows the characteristics of our formalism and our bisimulation relations.

Objectives

The main objective of the internship is to study refinement theory for open automata. Our purpose is to define a refinement relation between the symbolic models allowing refinement verification for a class of open systems.

The internship will start with a study of the semantics of a simple language called value passing CCS. The first objective of this internship is to design a semantics value passing CCS in terms of open automata. Especially, we will be able to extend the semantics by taking into account the semantics of operators for composing CCS processes.

After this preliminary step, the next objective will be to design a refinement theory for open automata. We will make sure that this relation is specified in a constructive manner, so that an algorithm could be derived from the specification in the future [1]. The relationship between refinement and automata composition should also play a major role in this definition.

The next steps in the internship will rely on these two initial works; they will consist in addressing some of the following (independent) objectives:

- Express and prove compositionality properties for the refinement relation over open automata.
- Study formally the behaviour of CCS operators wrt refinement.
- Compare this theory with the state of the art of the refinement semantics.
- Design the algorithm that checks refinement between two open automata.

References

[1] Françoise Bellegarde, Celina Charlet and Olga Kouchnarenko: How to Compute the Refinement Relation for Parameterized Systems. 1st ACM & IEEE International Conference on Formal Methods and Models for Co-Design (MEMOCODE 2003), 24-26 June 2003, Mont Saint-Michel, France. DOI: 10.1109/MEMCOD.2003.1210095

[2] Henrio, L., Madelaine, E., Zhang, M.: 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

[3] Hou, Z., Madelaine, E.: Symbolic Bisimulation for Open and Parameterized Systems. In: PEPM 2020 - ACM SIGPLAN Workshop on Partial Evaluation and Program Manipulation, New-Orleans, United States (January 2020). https://hal.inria.fr/hal-02406098

[4] Rabéa Ameur-Boulifa and Ludovic Henrio and Eric Madelaine: Compositional equivalences based on Open pNets. arXiv 2007.10770 (2020). https://arxiv.org/abs/2007.10770