Verification of hybrid synchronous/asynchronous systems

Simon Bliudze (simon.bliudze@inria.fr)

The main goal of this project is to propose hybrid verification techniques for systems combining synchronous and asynchronous interaction mechanisms for concurrent component-based systems.

Context

BIP [2, 4] is a framework for component-based design of correct-by-construction software and embedded systems. Components are modelled as finite state machines (FSM). In order to provide an abstraction level that would allow reasoning about the parallel behaviour of concurrent components, only the relevant actions are explicitly represented by transitions of these state machines. Interaction and priority models, collectively called *glue*, specify the set of allowed atomic synchronisations among the concurrent components of the system.

JavaBIP [5] is a Java-based implementation of BIP, initially developed at EPFL. This implementation relies on the so-called *BIP Specification* classes that are associated to software components to provide an FSM representation of their relevant behaviour. Essentially, BIP Specifications represent an extended interface for such components, which provides information on when operations can be performed, extending the usual notion of interface, which only specifies what operations exist.

In addition to atomic synchronisation, which is the only interaction mechanism provided by BIP, JavaBIP provides a flexible mechanism for asynchronous message passing inspired by the one used in the Actor model [1]. In a recent study, we have proposed an extended notion of connectors that allows combining such synchronous and asynchronous interaction using flexible and expressive structured patterns.

Project goals

The main goal of the project is propose hybrid verification approaches for essential properties such as *deadlock freedom*. Indeed, dedicated techniques exist for the verification of both synchronous, e.g. [3], and asynchronous systems, e.g. [6] systems. Verification of hybrid synchronous/asynchronous systems can be carried out by encoding one of the interaction mechanisms into the other. However, such encodings tend to significantly increase the system complexity, thereby adversly affecting verification performance. The question to address is, therefore, whether it is possible to decompose the verification problem into synchronous

and asynchronous "parts" so as to verify each with the corresponding tool and combine the results.

Benefits

You will learn the principles of rigorous system design based on formal operational semantics and get an in-depth understanding of BIP, a state-of-the-art component-based framework. Successful internship can lead to a research publication.

Required skills

Good analytical skills will definitely be required. The candidate must have good understanding of Labelled Transition Systems and Finite State Automata.

Location

The internship will be carried out in the Spirals project team at Inria Lille – Nord Europe under supervision by Simon Bliudze.

Contact and application

For additional information and to apply please send an e-mail to Simon Bliudze (in English or French) with the subject "Hybrid verification internship".

References

1. Gul Agha: Actors: A Model of Concurrent Computation in Distributed Systems. Doctoral thesis, MIT (1985) [PDF]
2. Ananda Basu, Saddek Bensalem, Marius Bozga, Jacques Combaz, Mohamad Jaber, Thanh-Hung Nguyen, and Joseph Sifakis: Rigorous component-based system design using the BIP framework. *IEEE Software* **28**(3):41–48 (2011) [Website | PDF]
3. Saddek Bensalem, Marius Bozga, Thanh-Hung Nguyen, and Joseph Sifakis. DFinder: a tool for compositional deadlock detection and verification. *Computer Aided Verification*, LNCS, vol. **5643**:614–619, Springer (2009). [Website | PDF]
4. Simon Bliudze and Joseph Sifakis. The Algebra of Connectors — Structuring interaction in BIP. In *Proceedings of the 7th ACM & IEEE International Conference on Embedded Software*, EMSOFT 2007, pages 11–20, Salzburg, Austria, October 2007. ACM SigBED. [PDF]

5. Simon Bliudze, Anastasia Mavridou, Radoslaw Szymanek, and Alina Zolotukhina. Exogenous coordination of concurrent software components with JavaBIP. *Software: Practice and Experience*, **47**(11):1801–1836, November 2017. [PDF]

6. Marjan Sirjani, Ali Movaghar, Amin Shali, and Frank S. de Boer. Modeling and Verification of Reactive Systems using Rebeca. *Fundamenta Informaticae*, **63**:1–26, IOS Press (2004) [PDF]