Symbolic verification of real-time design patterns

This proposal focuses on the extension of the theory of BIP design patterns (called "architectures") to the real-time domain.

Context

In our previous paper [1], we have defined the notion of architectures—design patterns for the BIP component-based framework.

An architecture is as an operator A that, applied to a set of components $\mathcal{B}$, builds a composite component $A(\mathcal{B})$ meeting a characteristic property Φ. Composability is based on an associative, commutative and idempotent architecture composition operator $\oplus$. Both the notion of architectures and the composition operator $\oplus$ are formally defined within the context of the BIP framework.

The main result is that if two architectures A_1 and A_2 enforce respectively safety properties (intuitively: *"something bad will never happen"*) Φ_1 and Φ_2, the composed architecture $A_1 \oplus A_2$ enforces the property $\Phi_1 \wedge \Phi_2$, that is both properties are preserved by architecture composition. We have, furthermore, defined the notion of *non-interference* and proved that, if two architectures are mutually non-interfering, their composition also preserves liveness properties (intuitively: *"something good will eventually happen"*).

During a previous ENS L3 internship, Waïss Azizian has extended these results to the real-time domain (relying on timed automata as the behavioural model). However, checking non-interference of real-time architectures turned out to be a computationally expensive task.

The project objectives

The goal of this project is to propose and implement abstractions and symbolic methods allowing efficient non-interference verification, e.g. using Satisfiability Modulo Theories (SMT) solvers.

Location

The internship will be carried out in the Spirals project team at Inria Lille – Nord Europe.

Contact and application

For additional information and to apply please send me an e-mail (in English or French) with the subject “Real-time design patterns internship”.

Reference

1. Paul Attie, Eduard Baranov, Simon Bliudze, Mohamad Jaber, and Joseph Sifakis. A general framework for architecture composability. Formal Aspects of Computing, 18(2):207–231, April 2016. Open access. [DOI]