Master's thesis proposal

Automated CTL proofs in proof assistants

Context

Formal methods are more and more commonly used to ensure the correctness of industrial systems, in particular critical ones. Several techniques can be used, among which model checking, static analysis using abstract interpretation, mechanized theorem proving (automated theorem provers and proof assistants), etc. For a given system, different techniques can be used to prove the correctness of different subsystems. The question that naturally arise is whether the correctness of the subsystems implies the correctness of the whole. To show this, one needs to relate the different proof techniques together.

In the recent years, Ji [1] showed how to perform model checking proofs based on the modal logic CTL in an automated theorem prover, namely iProverModulo, with performances comparable to state-of-the-art model checkers. On the other hand, iProverModulo is able to produce proof in Dedukti format. Dedukti[1] is a universal proof checker, which is able to check proofs coming from a variety of automated provers and proof assistants. Conversely, Thiré [2] showed how to translate proof from a subset of Dedukti to various proof assistants, namely Coq, PVS, Lean, Matita and provers of the HOL family. In these proof assistants, various embedding of CTL have been developed, but they lack automation.

Subject

The goal of this internship is to study how to automate proof search of CTL formulas in proof assistants by using iProverModulo and Dedukti. First, one has to make sure that the proofs produced by iProverModulo corresponds to the fragment translatable to the proof assistants. Then, the embedding of CTL in iProverModulo, and its translation via Dedukti, should be aligned with how CTL has been defined in the various proof assistants. Finally, tactics should be developed in the proof assistant to make the whole process easy to use.

Practical informations

The internship will take place in the Laboratoire Spécification et Vérification of the ENS Paris-Saclay in Cachan. It will be supervised by Guillaume Burel, assistant professor at the Ensiie, temporarily assigned in Inria project-team Deducteam, guillaume.burel@ensiie.fr

References

[1] Kailiang Ji. CTL model checking in deduction modulo. In Amy P. Felty and Aart Middeldorp, editors, *CADE-25*, volume 9195 of *LNCS*, pages 295–310. Springer, 2015.

[2] François Thiré. Sharing a library between proof assistants: Reaching out to the HOL family. In Frédéric Blanqui and Giselle Reis, editors, *LFMTP 2018*, volume 274 of *EPTCS*, pages 57–71, 2018.

[1] `https://deducteam.github.io/`