On-the-fly Abstractions of Formulas in Proofs Mixing First-Order Reasoning and Temporal Logic

General information

Supervisor	Stephan Merz
Adress	Inria Nancy – Grand Est, Villers-lès-Nancy
Phone	+33 3 54 95 84 78
Email	stephan.merz@loria.fr

Context

The TLA$^+$ Proof System TLAPS [1] is an interactive proof assistant for reasoning about TLA$^+$ specifications. The TLA$^+$ language [3] is mainly intended for specifying distributed algorithms at a high level of abstraction. It is based on mathematical set theory for describing the data structures manipulated by an algorithm, and on the Temporal Logic of Actions, a variant of linear-time temporal logic, for describing the executions of a system. Consequently, TLA$^+$ proofs mix reasoning about set theory, expressed in first-order logic, and in temporal logic, and TLAPS includes automatic back-end provers for both logics.

However, first-order logic provers do not support the operators of temporal logic. Conversely, the decision procedure for propositional temporal logic included with TLAPS does not understand variables, terms, and quantifiers of first-order logic. The combination of both logics therefore relies on a technique called *coalescing* [2], which corresponds to the introduction of fresh symbols representing subformulas that the back-end prover does not support.

Internship subject

The current implementation of coalescing in TLAPS works adequately for introducing fresh atomic propositions that represent first-order formulas appearing in the scope of operators of temporal logic; it suffices for proving safety properties of specifications. Coalescing temporal subformulas of first-order logic is more delicate: such sub-formulas may contain occurrences of bound variables that should remain visible so that the first-order prover can instantiate them. For example, the two formulas

$$\exists x \in S : \Box\Diamond(x = z) \qquad \text{and} \qquad \forall y \in S : \Box\Diamond(y = z)$$

(where z is a variable of temporal logic) should be coalesced to $\exists x \in S : F(x)$ and $\forall y \in S : F(y)$, respectively, for some fresh predicate symbol F. The situation is more delicate in the presence of schematic operator symbols that are available in TLA$^+$. Moreover, one may want to integrate some laws of logic such as symmetry of equality or distributivity of $\forall$ and $\Box$ into the coalescing procedure to augment its reasoning

power. The current implementation of coalescing in TLAPS computes a conservative approximation that often requires the user to introduce abstractions manually, making first-order temporal logic reasoning more tedious than it would have to be.

The objective of this internship is first to provide more solid bases for coalescing by considering its semantics, based on the treatment in [2]. Secondly, a more complete coalescing algorithm should be described and proved correct in this semantic framework. Based on the interests of the student and the time frame, this algorithm could be prototypically implemented and validated within TLAPS.

The student working on this subject should be interested in mathematical logic and be well acquainted with the semantics of first-order logic. Prior knowledge of second-order or temporal logic would be a plus but is not required. No experience with proof assistants is necessary: during the internship the student will be able to gain some insight into the use of TLAPS. For the (optional) implementation aspects, familiarity with functional programming and OCaml in particular is required.

Work environment

The internship will take place in Nancy within the VeriDis team of Inria Nancy – Grand Est, a stimulating international research group that is common to Inria, CNRS, University of Lorraine, and the Max-Planck Institute for Informatics in Saarbrücken, and is located at LORIA on the science campus of Nancy. The city of Nancy is a lively university town of intermediate size (about 300,000 inhabitants) in the North-East of France. It offers affordable housing and is home to a rich cultural life and historic treasures, in particular from the 18th and the early 20th century.

References

[1] Denis Cousineau, Damien Doligez, Leslie Lamport, Stephan Merz, Daniel Ricketts, Hernán Vanzetto. TLA$^+$ Proofs. 18th Intl. Symp. Formal Methods (FM). Springer LNCS 7436, pp. 147-154. Paris, France, 2012.

[2] Damien Doligez, Jael Kriener, Leslie Lamport, Tomer Libal, Stephan Merz. Coalescing: Syntactic Abstraction for Reasoning in First-Order Modal Logics. Intl. Wsh. Automated Reasoning in Quantified Non-Classical Logics. Vienna, Austria, 2014. `http://arxiv.org/abs/1409.3819`.

[3] Leslie Lamport. Specifying Systems. Addison Wesley (Boston, Mass.), 2002. `http://lamport.azurewebsites.net/tla/tla.html`.