Internship proposal

Comparison of orientation techniques for axioms

Keywords: Logic, automated theorem proving, rewriting, deduction modulo theory.

Context

Proofs are rarely built without context: mathematical theorems are proved for instance in set theory, or in arithmetic; program correctness may use pointer arithmetic or the theories associated to the data structures of the program (chained lists, arrays, etc.); theories can also model characteristics of encryption functions to prove security properties.

When these theories are presented as sets of axioms, automated theorem provers often struggle to find proofs, because the proof search space becomes too large. Deduction modulo theory [1] is a framework that tries to circumvent this by presenting theories as computations, more precisely as rewriting rules. Experimental results have shown that when presenting (by hand) some theories as rewriting rules, proof search is indeed improved [2, 3]. However, the question remains, given an axiomatic presentation of a theory, how to orient it as a set of rewriting rules.

Subject

Several techniques have been proposed to orient axioms into rewriting rules. Some of them are proved to be complete, meaning that deduction modulo the resulting rewriting system proves the same as the original theory. Others are merely heuristics based on the shape of formulas.

At least three automated theorem provers support deduction modulo theory, namely iProver-Modulo, Zipperposition and ArchSAT.

The goal of this internship is to experimentally assess the usefulness of the orientation techniques by testing them on various benchmarks using the three tools mentioned above. Depending on the interest of the intern, new orientation techniques could be searched for.

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.
Note that the LSV will be closed from August 1st on.

References

[1] Gilles Dowek, Thérèse Hardin, and Claude Kirchner. Theorem proving modulo. *Journal of Automated Reasoning*, 31(1):33–72, 2003.

[2] Guillaume Burel. Experimenting with deduction modulo. In Viorica Sofronie-Stokkermans and Nikolaj Bjørner, editors, *CADE*, volume 6803 of *LNCS*, pages 162–176. Springer, 2011.

[3] Guillaume Bury *et al.* Automated deduction in the B set theory using typed proof search and deduction modulo. In Ansgar Fehnker *et al.*, editors, *LPAR*, volume 35 of *EPiC Series in Computing*, pages 42–58. EasyChair, 2015.