Proving preprocessing for Satisfiability Modulo Theories

Topic

Computer Science, Logic, Automated and interactive theorem proving, Satisfiability Modulo Theories, Verification

Institution

Inria, Loria, Université de Lorraine

Location

Nancy, France

Team/Project

VériDis

Supervision

Jasmin Blanchette, Jasmin.Blanchette@inria.fr
Pascal Fontaine, Pascal.Fontaine@loria.fr

Background

Many applications, for instance in the context of verification (and notably for critical systems in transportation, energy,...), rely on checking the satisfiability of logic formulas. Satisfiability Modulo Theories (SMT) solvers handle large formulas in expressive languages with uninterpreted symbols and interpreted operators (e.g. arithmetic or data structure operators). These tools are built using a cooperation of a SAT solver to handle the Boolean structure of the formula, and one or more theory reasoners to tackle the atoms and their language. SMT solvers are sizable and complex softwares implementing intricate algorithms, and they are error prone: it regularly happens, for instance in SMT competitions, that tools exhibit soundness errors. In a context where high confidence is a topmost requirement, this is unacceptable.

Objectives

A solution to the above issue is to require from solvers to provide a detailed certificate (or proof), and recheck this certificate. These certificates can also be used to exchange proofs and distribute checking tasks to different solvers according to their strength. Whereas the theory and practice of proof production for SAT solving and most theory reasoners is quite well understood, SMT solver also rely on many processing steps, like conjunctive normal form transformation, Skolemization, and rewriting. And certificate production for these aspects is still not mature.

We propose to study these preprocessing steps, theoretically and practically. First, the Intern will study the proof production for logically equivalent local rewritings (e.g. $x + 0$ being rewritten as x). The student will design a flexible proof-producing framework for these and study its complexity. We also suggest to evaluate practically the framework with a prototype (using the veriT SMT solver), and

proof reconstruction within the Isabelle or Coq proof assistant. Other kinds of formula processing, e.g. global logically equivalent rewriting steps (e.g. $x = 0 \wedge \varphi(x)$ rewritten as $\varphi(0)$) and other processing will be studied next.

This internship is an ideal opportunity to familiarize oneself with SMT solvers and proof assistants and to get acquainted with the exciting research taking place in the VeriDis team in Nancy. The VeriDis team will also organize the prestigious Interactive Theorem Proving conference in August 2016. This work will likely be part of a publication at an international workshop or conference (e.g., SMT, PxTP, IJCAR or Interactive Theorem Proving).

The subject of this internship will be adjusted according to the interests of the student.

Références bibliographiques

- Pascal Fontaine, Jean-Yves Marion, Stephan Merz, Leonor Prensa Nieto and Alwen Tiu. Expressiveness + Automation + Soundness: Towards Combining SMT Solvers and Interactive Proof Assistants. In Holger Hermanns and Jens Palsberg, editors, *In Proc. Tools and Algorithm for the Construction and Analysis of Systems (TACAS)*, volume 3920 of LNCS, pages 167–181. Springer-Verlag, 2006.

- Thomas Bouton, Diego Caminha B. de Oliveira, David Déharbe and Pascal Fontaine. veriT: an open, trustable and efficient SMT-solver. In Renate A. Schmidt, editor, *In Proc. Conference on Automated Deduction (CADE)*, volume 5663 of LNCS, pages 151–156. Springer-Verlag, 2009.

- Clark Barrett, Roberto Sebastiani, Sanjit A. Seshia and Cesare Tinelli, Satisfiability Modulo Theories. In Armin Biere, Marijn J. H. Heule, Hans van Maaren and Toby Walsh, editors. Chapter 26 of the Handbook of Satisfiability, pages 825–885. Volume 185 of Frontiers in Artificial Intelligence and Applications. IOS Press 2009.

Requirements

Knowledge in and deep interest for logic. Some acquaintance with either automated or interactive theorem proving is a plus. Knowledge of French is not required.