Available online at www.sciencedirect.com
SCIENCE DIRECT®
Electronic Notes in Theoretical Computer Science
ELSEVIER Electronic Notes in Theoretical Computer Science 125 (2005) 25–36
www.elsevier.com/locate/entcs

TSAT++: an Open Platform for Satisfiability Modulo Theories [1]

Alessandro Armando Claudio Castellini Enrico Giunchiglia
Massimo Idini Marco Maratea

MRG-DIST
University of Genova
Genova, Italy

Abstract

This paper describes TSAT++, an open platform which realizes the *lazy SAT-based approach* to Satisfiability Modulo Theories (SMT). SMT is the problem of determining satisfiability of a propositional combination of T-literals, where T is a first-order theory for which a satisfiability procedure for a set of ground atoms is known. TSAT++ enjoys a modular design in which an enumerator and a theory-specific satisfiability checker cooperate in order to solve SMT. Modularity allows both different enumerators, and satisfiability checkers for different theories (or combinations of theories), to be plugged in, as far as they comply to a simple and well-defined interface. A number of optimization techniques are also implemented in TSAT++, which are independent of the modules used (and of the corresponding theory). Some experimental results are presented, showing that TSAT++, instantiated for *Separation Logic*, is competitive with, or faster than, state-of-the-art solvers for that very logic.

Keywords: Boolean Satisfiability, Ground Decision Procedures, Separation Logic, Hardware Verification, Formal Methods

1 Introduction

Satisfiability Modulo Theories (SMT, see [15]) is the problem of determining satisfiability of a propositional combination of T-literals, where T is a simple

[1] We thank Ofer Strichman and Gilles Audemard for valuable suggestions about their solvers. This work is partially supported by COFIN and FIRB projects, and also by MIUR (Italian Ministry of Education, University and Research) under the project RoboCare – A Multi-Agent System with Intelligent Fixed and Mobile Robotic Components.
Email: {armando,drwho,enrico,idini,marco}@mrg.dist.unige.it

doi:10.1016/j.entcs.2004.06.065

first-order theory of practical interest, such as, e.g., the theory of arrays, of lists, full linear arithmetic (real and integer) and Separation Logic [17]. By the term "simple" we mean that the theory must have a known satisfiability procedure for a conjunctive set of ground atoms. A number of systems and techniques for SMT have been recently presented (e.g., [4,17,8]), showing that the problem is of great interest. In fact, the behavior of complex infinite-state systems (e.g., real-time hardware and programs) can be rigorously specified in SMT, and automated reasoning can be used to solve the related problems. In other words SMT seems an interesting compromise between expressivity and tractability.

One of the most promising approaches to SMT is the so-called *lazy SAT-based approach* [1,2,8]. The idea is that of managing the search for a model via an efficient machine for Boolean Satisfiability (SAT), e.g., the Davis-Logemann-Loveland algorithm (see, e.g., the seminal paper [7]), and delegating first-order reasoning to an ad-hoc satisfiability procedure for the theory T [2].

As long as this de-coupling is handled smartly, this approach benefits from

(i) the possibility of re-using, for the search, most of the technology and skill achieved in years of research on SAT;

(ii) the possibility to upgrade the T-satisfiability procedure, improving performance and/or extending the range of theories tackled with reasonable effort.

As far as we understand, while great attention has so far been devoted to the theoretical and practical issues of combining decision procedures for various theories, little or no care has been put in building a *practical*, *open* architecture, in which SAT reasoners and satisfiability procedures can be smoothly combined, while retaining good performance. (An attempt is represented by the forthcoming [10].)

Therefore, in this paper we propose a schema for realizing the approach, which modularly combines an enumerator and a satisfiability checker. These two modules take care, in turn, of the search and the first-order reasoning required. Their combination is realized via C++ abstract classes. The system we have built along these lines, TSAT++, is an *open platform* for SMT, in which any such modules can be plugged, as far as they comply with the interfaces defined by the classes.

We also show that a number of optimization techniques, both borrowed from the AI and Formal Methods literature and new, can be smoothly imple-

[2] really, just a satisfiability procedure for a conjunctive set of T-atoms is required here; but we will keep the term for the sake of simplicity.