Proof systems based on restricted Boolean circuits

Florent Capelli
Université de Lille

04/02/2019

Abstract

In this internship, we propose to look at proof systems based on syntactically restricted circuits. We are mainly interested in designing proof systems for #SAT, the problem of counting the number of satisfying assignments of a CNF formula, that is, we want to design a system such that if we are given a CNF formula F with k satisfying assignments, one can write a proof P that can be checked in polynomial time in the size of P that F has indeed k satisfying assignments. We propose to use restricted Boolean circuits arising in the field of Knowledge Compilation as proofs so that P is such a restricted circuit representing all solutions of F and so that one can both check that P represents F and count the number of satisfying assignments of P in polynomial time in the size of the circuit.

Given a CNF formula, that is, an instance of the well-known NP-complete problem SAT, one can easily be convinced that it is satisfiable by being given a satisfying assignment of the variables that one can check independently in polynomial time. However, when the instance is not satisfiable, it is much harder to convince someone of this fact. A well-known way of doing so is by writing a proof of unsatisfiability by explaining how one can apply satisfiability preserving transformations of the formula until a trivially unsatisfiable formula is reached, typically, a formula containing the empty clause. Such a mechanism is usually refered to as a *propositional proof system*. While one cannot except to always find a proof of unsatisfiability that is of polynomial size in the size of the input formula, the key feature of a proof system is that a proof can be checked in polynomial time in the *size of the proof* (Cook and Reckhow 1979).

Many such proof systems have been proposed in theory. In practice, to ensure the correctness of their output, modern SAT solvers are expected to always output a proof of unsatisfiability whenever it is necessary, the proof usually being written using a variation of a proof system known as *resolution* (Robinson 1965). See (Nordström 2015) for an introduction on the subject of proof complexity and its relation with practical SAT Solvers.

While many proof systems have been proposed and studied for proving the unsatisfiability of a CNF formula, few have been proposed to prove stronger properties on the input CNF such as proving that a CNF formula has at least or at most k satisfying assignments . In this internship, we propose to study the design of proof systems for this problem, that is, we want to construct a proof system such that if we are given a CNF formula F with k satisfying assignments, one can write a proof P in this system that can be checked in polynomial time in the size of P that F has indeed k satisfying assignments.

We propose to use restricted Boolean circuits as proofs so that P is such a restricted circuit representing all solutions of F and so that one can both check that P represents F and count the number of satisfying assignments of P in polynomial time in the size of the circuit. The Boolean circuits arising in the field of Knowledge Compilation, a field studying among others how one can transform a CNF formula into an efficient data structures allowing to solve quickly many hard problems on CNF formula such as counting or enumerating its satisfying assignments. See (Darwiche and Marquis 2002) for a survey. If time allows, the student may implement his system inside an existing #SAT solver such as D4 so that

it not only returns the number of satisfying assignments of a formula but also a verifiable proof of this fact.

Required skills

While they will be appreciated, we do not except any prior knowledge on proof complexity or knowledge compilation from the student and the internship will start with a bibliographical work on these subjects. The student is expected to have some skills in writing mathematical proofs . Skills in software development are not compulsory but welcome as it would be very interesting to observe how proof systems for #SAT behave in practice.

Details on the internship environment

The student will be working under the supervision of Florent Capelli (florent.capelli@univ-lille.fr) in the Inria Team LINKS depending both on Inria Lille and on CRIStAL laboratory in the Université de Lille.

References

Cook, Stephen A, and Robert A Reckhow. 1979. "The Relative Efficiency of Propositional Proof Systems." *The Journal of Symbolic Logic* 44 (1). Cambridge University Press: 36–50.

Darwiche, Adnan, and Pierre Marquis. 2002. "A Knowledge Compilation Map." *Journal of Artificial Intelligence Research* 17: 229–64.

Nordström, Jakob. 2015. "On the Interplay Between Proof Complexity and Sat Solving." *ACM SIGLOG News* 2 (3). ACM: 19–44.

Robinson, J. A. 1965. "A Machine-Oriented Logic Based on the Resolution Principle." *J. ACM* 12 (1). New York, NY, USA: ACM: 23–41. doi:10.1145/321250.321253.