Conflict-Driven Reasoning in Unions of Theories

Maria Paola Bonacina

Dipartimento di Informatica, Università degli Studi di Verona
Strada Le Grazie 15, I-37134, Verona, Italy, EU
mariapaola.bonacina@univr.it

As the development of automated reasoning has brought to relative maturity multiple reasoning paradigms and tools, a general challenge is that of *interfacing*, *combining*, and *integrating* them, in *reasoning environments* that are more powerful and easier to use. Reasoning in a union $\mathcal{T}$ of theories $\mathcal{T}_1, \ldots, \mathcal{T}_n$ is a context where this challenge arises naturally, and many applications of automated reasoning require to handle a union of at least a few theories. This talk advertises a recent paradigm named CDSAT (*Conflict-Driven SATisfiability*) for *conflict-driven reasoning* in a union of theories [4].

Reasoning in a union of theories can be approached in more than one way. The *equality sharing scheme* by Nelson and Oppen, and its integration in the well-known DPLL($\mathcal{T}$) framework, combine decision procedures for $\mathcal{T}_i$-satisfiability ($1 \leq i \leq n$) into a decision procedure for $\mathcal{T}$-satisfiability. Decision procedures are combined as *black-boxes* that only exchange entailed (disjunctions of) equalities between shared variables. Superposition reasons in a union of theories by taking the union of their axiomatizations: under suitable conditions the termination of superposition is *modular*, so that termination on $\mathcal{T}_i$-satisfiability problems ($1 \leq i \leq n$) implies termination on $\mathcal{T}$-satisfiability problems [1]. *Model-based theory combination* by de Moura and Bjørner is a variant of equality sharing, where the $\mathcal{T}_i$-satisfiability procedures build candidate $\mathcal{T}_i$-models, and propagate equalities true in the current candidate $\mathcal{T}_i$-model rather than entailed. DPLL(Γ+$\mathcal{T}$) integrates superposition and DPLL($\mathcal{T}$) with model-based theory combination to handle unions mixing axiomatized and built-in theories [5].

DPLL($\mathcal{T}$) and DPLL($\Gamma+\mathcal{T}$) are built around the CDCL (*Conflict-Driven Clause Learning*) procedure for propositional satisfiability (SAT) pioneered by Marques Silva and Sakallah. CDCL builds a candidate partial model of a propositional abstraction of the formula, and applies propositional resolution only to *explain* conflicts between the model and the formula, so that the conflict explanation tells how to update the model and solve the conflict. CDCL inspired several $\mathcal{T}_i$-satisfiability procedures for fragments of arithmetic (e.g, using Fourier-Motzkin resolution only to explain conflicts in linear real arithmetic), and was generalized to first-order logic (without equality) in a theorem-proving method named SGGS (*Semantically-Guided Goal-Sensitive* reasoning) [6]. Methods that perform nontrivial inferences only to explain conflicts are called *conflict-driven*.

In DPLL($\mathcal{T}$) and DPLL($\Gamma+\mathcal{T}$) the conflict-driven reasoning is only propositional as in CDCL: conflict-driven $\mathcal{T}_i$-satisfiability procedures could be integrated only as black-boxes, so that they could not participate in the model construction on a par with CDCL. The MCSAT (*Model-Constructing SATisfiability*) framework by de Moura and Jovanović shows how to integrate CDCL and a conflict-

driven $\mathcal{T}_i$-satisfiability procedure, called *theory plugin*, so that *both* propositional and $\mathcal{T}_i$-reasoning are conflict-driven. A key idea is to abandon black-box combination: open the black-box, pull out from the $\mathcal{T}_i$-satisfiability procedure clausal inference rules that can *explain* $\mathcal{T}_i$-conflicts, and enable CDCL and the $\mathcal{T}_i$-plugin to cooperate in model construction.

CDSAT generalizes MCSAT to the multi-theory case, solving the problem of how to combine multiple $\mathcal{T}_i$-satisfiability procedures, some of which are conflict-driven and some of which are black-boxes. The theories are assumed to be equipped with theory inference systems called *theory modules*, with propositional logic viewed as one of the theories in the union. CDSAT provides a framework for the theory modules to cooperate as peers in building a candidate $\mathcal{T}$-model and explaining $\mathcal{T}$-conflicts. Thus, reasoning in a union of theories is achieved by putting together inference systems, rather than procedures or axiomatizations: of course, theory modules are abstractions of decision procedures, and inference rules may correspond to axioms. A black-box $\mathcal{T}_i$-satisfiability procedure is treated as a theory module with only one inference rule that invokes the procedure to check $\mathcal{T}_i$-satisfiability. CDSAT encompasses the previous approaches: it reduces to CDCL if propositional logic is the only theory, to equality sharing if propositional logic is absent and all $\mathcal{T}_i$-satisfiability procedures are black-boxes, to DPLL($\mathcal{T}$) if propositional logic is one of the theories and all other theories have black-box $\mathcal{T}_i$-satisfiability procedures, and to MCSAT if there are propositional logic and another theory with a conflict-driven $\mathcal{T}_i$-satisfiability procedure. Under suitable hypotheses, CDSAT is *sound*, *terminating*, and *complete*.

CDSAT opens several exciting directions for future work, including an integration, or at least an interface, between CDSAT and SGGS, or SGGS enriched with conflict-driven superposition to handle equality. Descriptions of all these approaches appear in recent surveys [2, 3] where the references can be found.

References

1. A. Armando, M. P. Bonacina, S. Ranise, and S. Schulz. New results on rewrite-based satisfiability procedures. *ACM TOCL*, 10(1):129–179, 2009.
2. M. P. Bonacina. On conflict-driven reasoning. In N. Shankar and B. Dutertre, editors, *Proc. of the 6th Workshop on Automated Formal Methods (AFM)*, volume 5 of *Kalpa Publications*, pages 31–49. EasyChair, 2018.
3. M. P. Bonacina, P. Fontaine, C. Ringeissen, and C. Tinelli. Theory combination: beyond equality sharing. In Carsten Lutz et al., editor, *Description Logic, Theory Combination, and All That: Essays Dedicated to Franz Baader*, volume 11560 of *LNAI*, pages 57–89. Springer, 2019.
4. M. P. Bonacina, S. Graham-Lengrand, and N. Shankar. Conflict-driven satisfiability for theory combination: transition system and completeness. *J. Automat. Reason.*, in press:1–31, 2019. Available at http://doi.org/10.1007/s10817-018-09510-y.
5. M. P. Bonacina, C. A. Lynch, and L. de Moura. On deciding satisfiability by theorem proving with speculative inferences. *J. Automat. Reason.*, 47(2):161–189, 2011.
6. M. P. Bonacina and D. A. Plaisted. Semantically-guided goal-sensitive reasoning: inference system and completeness. *J. Automat. Reason.*, 59(2):165–218, 2017.