SMT and Theory Combination Techniques

Filipe Casal

SQIG, Instituto de Telecomunicações, Lisboa

Recently, the Automated Reasoning community has turned its attention to the area of Satisfiability Modulo Theories (SMT). Shortly, SMT deals with problems that are a generalization of boolean SAT problems, in the sense that we are dealing with first-order formulas and not just propositional formulas. This generalization is natural: SAT solving techniques are extensively studied and meaningful improvements to SAT solvers are extremely hard to develop, and SMT problems arise ever more frequently in fields such as Automated Theorem Proving and Software Verification.

Concretely, an SMT solver for a generic first-order theory generally consists of a Boolean Reasoner that breaks down the formula and finds high level inconsistencies (the formula $\varphi \wedge \psi \wedge \neg\varphi$ would be automatically ruled out, independently of whether φ or ψ are satisfiable) and a Theory Solver that verifies whether the formula is in fact satisfiable in the underlying theory. Essentially, the Boolean Reasoners are formula simplification mechanisms with a SAT solver, and the Theory Solvers are the decision procedures for decidable theories (usually Presburger arithmetic, arrays or bitvectors).

Suppose now we would like to formally verify an assertion that deals with both bitvectors as well as with arithmetic. This formula contains symbols from both theories, so the respective Theory Solvers would not be able to parse this formula. Here, we would like to modularly combine the decision procedures for these theories into a decision procedure for the union of these theories. This method of combination, the Nelson-Oppen method, requires the theories to satisfy many properties.

Since Nelson and Oppen introduced this combination procedure in 1979 [3], the study of the classes of theories which decision procedures can be combined has been actively studied. In 2005, it was shown that shiny [5] and polite [4] theories could be combined with an arbitrary theory. Later, a stronger notion of polite theory was proposed, see [2], in order to overcome a subtle issue with a proof in [4]. In [1], we analyse the relationship between shiny and strongly polite theories in the one-sorted case. We show that a shiny theory with a decidable quantifier-free satisfiability problem is strongly polite and provide two different sufficient conditions for a strongly polite theory to be shiny. Based on these results, we derive a combination method for the union of a polite theory with an arbitrary theory. Joint work with João Rasga, SQIG, Instituto de Telecomunicações and Departamento de Matemática, Instituto Superior Técnico, Universidade de Lisboa.

References

1. F. Casal and J. Rasga Revisiting the Equivalence of Shininess and Politeness. In *Proceedings of the 19th International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'2013)*, volume 8312 of *LNCS*, pages 198–212, 2013.
2. D. Jovanović and C. Barrett. Polite theories revisited. In *Proceedings of the Seventeenth International Conference on Logic for Programming, Artificial Intelligence, and Reasoning (LPAR'2010)*, volume 6397 of *LNCS*, pages 402–416, 2010.
3. G. Nelson and D. C. Oppen. Simplification by cooperating decision procedures. *ACM Transactions on Programming Languages and Systems*, 1(2):245–257, 1979.
4. S. Ranise, C. Ringeissen, and C. G. Zarba. Combining data structures with nonstably infinite theories using many-sorted logic. In *Proceedings of the Fifth International Workshop on Frontiers of Combining Systems (FroCoS'2005)*, volume 3717 of *LNAI*, pages 48–64, 2005.
5. C. Tinelli and C. G. Zarba. Combining nonstably infinite theories. *Journal of Automated Reasoning*, 34(3):209–238, 2005.