On hierarchical symbol elimination and applications

Viorica Sofronie-Stokkermans

University Koblenz-Landau, Koblenz, Germany
sofronie@uni-koblenz.de

Many problems in computer science can be reduced to checking satisfiability of ground formulae w.r.t. a theory – which can be a standard theory (for instance linear arithmetic) or a complex theory (for instance the extension of a base theory $\mathcal{T}_0$ with additional function symbols axiomatized by a set $\mathcal{K}$ of formulae, or a combination of theories). Existing SMT solvers are used for checking satisfiability of ground formulae w.r.t. increasingly complex theories; the output can sometimes be "unknown" if incomplete methods are used, or termination cannot be guaranteed.

Local theory extensions. In previous work [8] we studied *local theory extensions*, i.e. extensions $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ of a base theory $\mathcal{T}_0$ (over a signature Σ_0) with additional function symbols in a signature Σ_1, whose properties can be axiomatised using a set $\mathcal{K}$ of $\Sigma_0 \cup \Sigma_1$-clauses, with the property that for every set G of ground $\Sigma_0 \cup \Sigma_1 \cup C$-clauses (where C is a new set of constants), G is unsatisfiable w.r.t. $\mathcal{T}_0 \cup \mathcal{K}$ if and only if G is already unsatisfiable w.r.t. $\mathcal{T}_0 \cup \mathcal{K}[G]$, where $\mathcal{K}[G]$ is the set of all instances of $\mathcal{K}$ in which all terms starting with a function symbol in Σ_1 are ground subterms occurring in $\mathcal{K}$ or G. In subsequent work [2, 4] we extended this notion to the notion of Ψ-local extension, where Ψ is a closure operator on ground terms. Ψ-local theories extensions can be seen as theory extensions $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ with complete ground instantiation, such that all the "extension" terms in the set of ground instances sufficient for completeness are obtained from the ground terms occurring in $\mathcal{K}$ or G, using the closure operator Ψ. In [4] we identified conditions under which the combination of two local extensions of a theory $\mathcal{T}_0$ is again a local extension of $\mathcal{T}_0$ and extended such results also to Ψ-locality. If the closure operator Ψ associates with every *finite* set of ground terms T a *finite* set $\Psi(T)$ of ground terms and $\mathcal{K}$ is finite, then *hierarchical reasoning* is possible in Ψ-local theory extensions – i.e. testing satisfiability of a set of clauses G w.r.t. the extension $\mathcal{T}_0 \cup \mathcal{K}$ can be reduced to checking the satisfiability w.r.t. $\mathcal{T}_0$ of a set of clauses G_0. If in addition $|\Psi(T)| \leq f(|T|)$, where f is a computable function, then the size of G_0 can be estimated using the function f. If for every set G of ground clauses the set G_0 of clauses obtained this way is always guaranteed to belong to a decidable fragment of $\mathcal{T}_0$, then satisfiability of ground clauses w.r.t. $\mathcal{T}_0 \cup \mathcal{K}$ is decidable. The method for hierarchical reasoning in local theory extensions was implemented in H-PILoT [3].

However, more interesting is to go beyond yes/no answers. In verification it might for instance be interesting to consider parametric systems and infer constraints on parameters (which can be values or functions) which guarantee that certain properties of the systems are met.

Symbol elimination in local theory extensions. For solving such problems, in [9, 10] we proposed a property-directed symbol elimination method and analyzed its properties. We devised a hierarchical method for symbol elimination in extensions of a theory $\mathcal{T}_0$ which allows quantifier elimination, which given as input:

(i) a theory extension $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ with set of extension functions Σ_1 satisfying a finite set of universally quantified clauses $\mathcal{K}$;

(ii) a subset of function symbols $\Sigma_{\mathsf{par}} \subseteq \Sigma_1$ considered to be parameters;

(iii) a set G of ground $\Sigma^C = \Sigma_0 \cup \Sigma_1 \cup C$-clauses (where C is a new set of constants);

(iv) a set T of ground Σ^C-terms (containing all subterms of G starting with a function symbol in Σ_1);

performs a hierarchical reduction, uses quantifier elimination in $\mathcal{T}_0$ to eliminate all extension function symbols in Σ_1 which are not in Σ_{par}, and constructs a universally quantified $\Sigma_0 \cup \Sigma_{\mathsf{par}}$-formula Γ with the property that $\mathcal{T}_0 \cup \mathcal{K} \cup \Gamma \cup G$ is unsatisfiable. (If $\mathcal{T}_0$ does not allow quantifier elimination, but has a model completion $\mathcal{T}_0^*$ which does, quantifier elimination in $\mathcal{T}_0^*$ can be used instead.) The method has been implemented in SEH-PILoT [5], an extension of H-PILoT.

We proved that if (i) $\mathcal{T}_0$ allows quantifier elimination, (ii) $\mathcal{T}_0 \subseteq \mathcal{T}_0 \cup \mathcal{K}$ is a local theory extension (with an additional property) and (iii) T is the set of all ground terms of $\mathcal{K}$ or G starting with an extension function in Σ_1, then the formula Γ obtained with the method above is the weakest universal formula with the property that $\mathcal{T}_0 \cup \mathcal{K} \cup \Gamma \cup G$ is unsatisfiable.

Applications. We used this method for symbol elimination in various areas:

- for ground interpolation in theory extensions [9, 10];
- in the verification of (parametric) systems: (i) for generating constraints on parameters describing additional conditions under which certain safety properties are guaranteed to be inductive invariants [11]; and (ii) for iteratively strengthening certain safety properties to obtain inductive invariants of a system [6];
- in problems arising from wireless research theory [7]. There, we combined general second-order symbol elimination (which we used for eliminating existentially quantified predicates) with property-directed symbol elimination (which we used for obtaining conditions on "parameters" under which formulae are satisfiable or second-order entailment holds). For second-order quantifier elimination we used a form of hierarchical ordered resolution; for symbol elimination we used the hierarchical method mentioned above.

We would like to better understand the links between our results and a form of symbol elimination studied in relationship with uniform interpolation in [1] and subsequent papers.

References

[1] D. Calvanese, S. Ghilardi, A. Gianola, M. Montali, A. Rivkin: Model completeness, uniform interpolants and superposition calculus. J. Autom. Reason. 65(7): 941-969 (2021)

[2] C. Ihlemann, S. Jacobs, V. Sofronie-Stokkermans: On local reasoning in verification. In: C.R. Ramakrishnan, J. Rehof (eds.), Proc. TACAS'08. LNCS 4963, 265-281. Springer (2008)

[3] C. Ihlemann, V. Sofronie-Stokkermans: System description: H-PILoT. In: R.A. Schmidt (ed.) Proc. CADE-22. LNAI 5663, 131-139. Springer (2009)

[4] C. Ihlemann, V. Sofronie-Stokkermans: On hierarchical reasoning in combinations of theories. In: J. Giesl, R. Hähnle (eds.) Proc. IJCAR 2010, LNAI 6173, 30-45. Springer (2010)

[5] P. Marohn, V. Sofronie-Stokkermans: SEH-PILoT: A system for property-directed symbol elimination - Work in Progress (Short Paper). SOQE@KR 2021: 75-82, CEUR Workshop Proc. 3009.

[6] D. Peuter, V. Sofronie-Stokkermans: On invariant synthesis for parametric systems. In P. Fontaine (ed.) Proc. CADE-27, LNCS 11716, 385-405. Springer, 2019.

[7] D. Peuter, V. Sofronie-Stokkermans: Symbol elimination and applications to parametric entailment problems. In B. Konev, G. Reger (eds.), FroCoS 2021, LNCS 12941, 43-62. Springer, 2021.

[8] V. Sofronie-Stokkermans: Hierarchic reasoning in local theory extensions. In: R. Nieuwenhuis (ed.), Proc. CADE-20, LNAI 3632, 219-234. Springer (2005)

[9] V. Sofronie-Stokkermans: On interpolation and symbol elimination in theory extensions. In: N. Olivetti, A. Tiwari (eds.) Proc. IJCAR 2016. LNCS (LNAI) 9706, 273-289. Springer (2016)

[10] V. Sofronie-Stokkermans: On interpolation and symbol elimination in theory extensions. Logical Methods Comput. Sci.14(3), 1-41 (2018)

[11] V. Sofronie-Stokkermans: Parametric systems: Verification and synthesis. Fundam.Informaticae, 173(2-3):91-138, 2020.