

Generalized Craig Interpolation for Stochastic Satisfiability Modulo Theories Problems*

Ahmed Mahdi and Martin Fränzle

Carl von Ossietzky Universität,
Ammerländer Heerstrae 114-118, 26111 Oldenburg, Germany
{mahdi|fraenzle}@informatik.uni-oldenburg.de

Abstract

Craig interpolation [Cra57] is used in solving *bounded model checking* (BMC) SAT and SMT problems [McM03, McM05]. In 2012, Teige et al. [TF12] succeeded to compute interpolants for stochastic boolean satisfiability problems; i.e., SSAT [Pap85]. That was achieved by defining sound and complete resolution calculus for SSAT [TF10], and computing the Craig interpolation for $A \wedge B \wedge \neg S_{A,B}$, where $\neg S_{A,B}$ represents a conflict clause of $A \wedge B$. Consequently, one can obtain two interpolants for the formula $\Phi : A \wedge B$, where one interpolates A , and the second one interpolates B . As a result of that, an approach to solve efficiently stochastic bounded model checker problems, e.g., MDPs, was addressed by using SSAT interpolation¹ [TF12, Tei12].

In this work we present a notion of *Craig Interpolation* for the stochastic modulo theories framework; i.e., SSMT. An SSMT formula consists of free and quantified variables where the latter variables are bound to discrete domains by *existential* or *randomized* quantifiers. In the case of a randomized variable, the variable can be assigned to one of its domain values with a certain probability, where the summation of all probabilities of the same variable has to be one. The significance of SSMT comes from the fact that one can encode probabilistic hybrid automata problems as SSMT formulae [FHT08, Tei12].

Our approach to compute the Craig interpolation for SSMT is as follows: we assume that arithmetic constraints can be relaxed as simple bounds by using *interval constraint propagation* (ICP) [BMH94] as implemented in iSAT tool [TF08]. After that, we define a *sound and relatively-complete*² resolution calculus for SSMT formula as done in case of SSAT, such that if a conflict clause is derived with a certain probability, then the latter probability is a safe upper bound of the real satisfaction probability of the SSMT formula [TF10]. Then we extend Púdlak's rules [Pud97] in a way such that simple bounds are treated as literals and if a conflict clause is derived, then we get a generalized Craig interpolation for the whole formula $A \wedge B \wedge \neg S_{A,B}$.

Finally, we adapt BMC to the probabilistic case, i.e., PBMC by encoding a *step-bounded reachability* problem as an SSMT formula, where a generalized Craig interpolation is used to compute an upper bound of the maximum probability of reaching the target states.

References

- [BMH94] Frédéric Benhamou, David A. McAllester, and Pascal Van Hentenryck. Clp(intervals) revisited. In Maurice Bruynooghe, editor, *ILPS*, pages 124–138. MIT Press, 1994.
- [Cra57] William Craig. Three uses of the herbrand-gentzen theorem in relating model theory and proof theory. *J. Symb. Log.*, 22(3):269–285, 1957.

*This work was supported by the German Research Council (DFG) as part of the Transregional Collaborative Research Center SFB/TR 14 AVACS (<http://www.avacs.org>).

¹It was called a “Generalized Craig Interpolation”, as it covers SSAT and SAT problems.

²Relatively-complete; as it depends on ICP where the latter is not always complete.

- [FHT08] Martin Fränzle, Holger Hermanns, and Tino Teige. Stochastic satisfiability modulo theory: A novel technique for the analysis of probabilistic hybrid systems. In Magnus Egerstedt and Bud Mishra, editors, *HSCC*, volume 4981 of *Lecture Notes in Computer Science*, pages 172–186. Springer, 2008.
- [McM03] Kenneth L. McMillan. Interpolation and sat-based model checking. In Warren A. Hunt Jr. and Fabio Somenzi, editors, *CAV*, volume 2725 of *Lecture Notes in Computer Science*, pages 1–13. Springer, 2003.
- [McM05] Kenneth L. McMillan. An interpolating theorem prover. *Theor. Comput. Sci.*, 345(1):101–121, 2005.
- [Pap85] Christos H. Papadimitriou. Games against nature. *J. Comput. Syst. Sci.*, 31(2):288–301, 1985.
- [Pud97] Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symb. Log.*, 62(3):981–998, 1997.
- [Tei12] Tino Teige. *Stochastic Satisfiability Modulo Theories: A Symbolic Technique for the Analysis of Probabilistic Hybrid Systems*. PhD thesis, Fakultät II Informatik, Wirtschafts- und Rechtswissenschaften, Department für Informatik, Germany, Oldenburg, Escherweg.2 26122, August 2012.
- [TF08] Tino Teige and Martin Fränzle. Stochastic satisfiability modulo theories for non-linear arithmetic. In Laurent Perron and Michael A. Trick, editors, *CPAIOR*, volume 5015 of *Lecture Notes in Computer Science*, pages 248–262. Springer, 2008.
- [TF10] Tino Teige and Martin Fränzle. Resolution for stochastic boolean satisfiability. In Christian G. Fermüller and Andrei Voronkov, editors, *LPAR (Yogyakarta)*, volume 6397 of *Lecture Notes in Computer Science*, pages 625–639. Springer, 2010.
- [TF12] Tino Teige and Martin Fränzle. Generalized craig interpolation. *Logical Methods in Computer Science*, 8(2), 2012.