Master Thesis Proposal

Interpolation in First Order Logic with Equality

Bernhard Mallinger

Advisor: Ass.Prof. Stefan Hetzl

March 14, 2014

1 Motivation and problem statement

After decades of continued research, the area of software verification still lacks effective methods for reasoning about real world programs, which is necessary to prove vital safety or liveness properties. The emergence of symbolic model checking and bounded model checking constitute considerable advances. Here, the set of reachable states of a program are described by means of abstraction, i.e. automatically derived predicates overapproximate them. However for actually finding suitable abstractions, sophisticated methods are required.

Furthermore, in dealing with programs with loops with an a priori unknown number of iterations, it is necessary to infer loop invariants in order to be able to give a meaningful guarantee of the state of the program afterwards. Finding such an invariant still is a highly non-trivial problem.

In recent years, the approach of applying Craig interpolation to solve both of these problems enjoyed increasing popularity, especially after successful applications for instance in [McM03] for use in abstraction or [Wei10] for use in loop invariant generation.

The Interpolation theorem is a long known basic result of mathematical logic. Interpolants lay bare certain logical relations between formulas or sets of formulas in a concise way. This process is fully analytic in the sense that interpolants can efficiently be calculated from proofs of the relations of the formulas. Leveraging the tremendous progress of automatic deduction systems in the last decades, obtaining the required proofs is feasible.

For practical applicability, often relatively weak formalisms such as propositional logic or equational logic with uninterpreted function symbols are studied. While considerable

research has been conducted and is still ongoing in these areas, unrestricted first order logic with equality has received relatively little attention.

2 Aim of the work

This thesis aims at giving comprehensive account of existing techniques and results with respect to interpolation in full first order logic with equality. This includes different proofs of interpolation results with a focus on constructive proofs which give rise to concrete and implementation-ready algorithms for finding interpolants. These algorithms, as listed in § 4.1, will be presented, analysed and compared.

Dependant on the respective findings, improvements or extensions of these algorithms will be investigated. More concretely, developing an efficient interpolation algorithm for LK and extending existing approaches without equality to include equality are among the central research interests.

Non-constructive methods, especially of a model theoretic nature, will be treated in order to form a theoretical baseline and to give a broader picture. In this spirit, further corollaries and also applications of the interpolation theorem will be presented.

3 Methodology and approach

As the problem at hand is a well-defined mathematical task, standard mathematical methodology applies.

Determined by the results in the investigations, implementations of the algorithms are deemed scientifically valuable but most likely beyond the scope of this thesis.

4 State of the art

Current research and application is rooted in the fundamental result by Craig ([Cra57a]), here given in a formulation suitable for resolution calculus[1]:

Theorem 1 (Interpolation)**.** Let A and B be first-order sentences such that $A \wedge B$ is refutable. Then there exists an interpolant I such that

1. $A \supset I$ is valid
2. $I \wedge B$ is unsatisfiable
3. the non-logical symbols of I are only those that appear in both A and B.

This basic result has been proven in different formalisms using different syntactic methods (cf. e.g. [Cra57a]; [Tak87]; [Kra97]; [Pud97]), but also via semantic, model theoretic means

[1] Also known as *reverse interpolation*

(cf. e.g. [Sho67, section 5.2]; [CK90, theorem 2.2.20]). To this end, the interpolation theorem can be seen as a corollary Robinson's joint consistency theorem, but even more, latter can also be proven from the former. This suggest a close relation between one the one hand the proof-theoretic and on the other hand the model-theoretic view.

Another major corollary of the interpolation theorem is given by Beth in form of the definability theorem, which shows that the notions of implicit and explicit definability coincide. In shallow terms, an implicit definitions refers to a definition by usage in a formula, whereas an explicit definition gives a definition in terms of another formula. The non-trivial direction of this theorem states that implicit definitions can be converted into explicit ones and can be proved by using the an interpolant as explicit definition.

4.1 Interpolation algorithms

Constructive proofs of the interpolation theorem directly give rise to algorithms for computing interpolants. For instance in [Tak87, theorem 6.6], the well known Maehara lemma is used in the proof, which forms an efficient procedure for extracting interpolants from first-order LK proofs, but does not consider equality and function symbols. It is unknown to the author whether the approach can be generalized to handle equality.

[Hua95] describes an algorithm for extracting interpolants from proofs from first order resolution calculus with equality. In a two stage approach, an initially constructed relational interpolant is later stripped of non-common constant and function symbols by overbinding them. [Pud97] and [Kra97] independently propose similar approaches, whereas both are restricted to propositional logic.

In [BL11], also a two step approach is proposed for first order logic without equality. The interesting difference to [Hua95] lies in the proof method: While in the latter the overbinding in the second stage only works for the kind of interpolants which have been constructed in the first stage of this very algorithm, the method of [BL11] argues about correctness of the overbinding based directly on the properties of relational interpolants. This works for any interpolant and is therefore a more flexible and powerful approach.

Another noteworthy and in fact one of the first interpolation algorithms of practical interest was introduced in [McM03], where it was also embedded in a model checking procedure.

5 Relevance to the curriculum of Computational Intelligence

Logic as core machinery of computer science is featured prominently in the curriculum of Computational Intelligence, first and foremost in the mandatory module "Logic and Computability" as well as the module "Logic, Mathematics, and Theoretical Computer Science", but also as essential theoretic foundations of other modules.

The logic used in this thesis, first-order logic with equality, clearly is among the most common and useful ones; the interpolation theorem is hereby a celebrated result. As argued in § 1, advancements in this field have direct consequences for the area of formal verification, which is also featured in the curriculum.

The following courses possess the most direct relation to the topic of this thesis:

- Formal Methods in Computer Science
- Proof Theory 1
- Logic and Computability
- Advanced Mathematical Logic

References

[BJ13] Maria Paola Bonacina and Moa Johansson. On interpolation in automated theorem proving. Technical Report 86/2012, Dipartimento di Informatica, Università degli Studi di Verona, 2013. Submitted to journal August 2013.

[BL11] M. Baaz and A. Leitsch. *Methods of Cut-Elimination.* Trends in Logic. Springer, 2011.

[CK90] C.C. Chang and H.J. Keisler. *Model Theory.* Studies in Logic and the Foundations of Mathematics. Elsevier Science, 1990.

[Cra57a] William Craig. Linear Reasoning. A New Form of the Herbrand-Gentzen Theorem. *The Journal of Symbolic Logic*, 22(3):250–268, September 1957.

[Cra57b] William Craig. Three uses of the herbrand-gentzen theorem in relating model theory and proof theory. *The Journal of Symbolic Logic*, 22(3):269–285, September 1957.

[Hua95] Guoxiang Huang. Constructing craig interpolation formulas. In *Proceedings of the First Annual International Conference on Computing and Combinatorics*, COCOON '95, pages 181–190, London, UK, UK, 1995. Springer-Verlag.

[Kra97] Jan Krajíček. Interpolation theorems, lower bounds for proof systems, and independence results for bounded arithmetic. *Journal of Symbolic Logic*, pages 457–486, 1997.

[McM03] Kenneth L. McMillan. Interpolation and sat-based model checking. In Jr. Hunt, Warren A. and Fabio Somenzi, editors, *Computer Aided Verification*, volume 2725

of *Lecture Notes in Computer Science*, pages 1–13. Springer Berlin Heidelberg, 2003.

[Pud97] Pavel Pudlák. Lower bounds for resolution and cutting plane proofs and monotone computations. *J. Symb. Log.*, 62(3):981–998, 1997.

[Sho67] J.R. Shoenfield. *Mathematical logic*. Addison-Wesley series in logic. Addison-Wesley Pub. Co., 1967.

[Tak87] G. Takeuti. *Proof Theory*. Studies in logic and the foundations of mathematics. North-Holland, 1987.

[Wei10] Georg Weissenbacher. *Program Analysis with Interpolants*. PhD thesis, 2010.