

Doctoral Thesis Report

Martin Blicha

Effective Automated Software Verification: A Multilayered Approach

Summary The thesis develops a set of foundational techniques as well as tools for symbolic model checking. Two notable foundational insights are introduced and evaluated in the thesis: The first insight is that interpolants created by Farkas lemma can often be decomposed with favorable effect. The second insight is to infer transition invariants by iterative squaring. They enable short certificates for long counter-examples. Both techniques are evaluated in the Golem Horn clause solver. Finally the thesis introduces a cooperative parallelization approach for property directed K induction. The chapters cover material that was published in several conferences: TACAS, VMCAI, FMCAD, SAS and a journal.

Structure The thesis provides introduction and preliminary notions in chapters 1 and 2, which allow the thesis to be read as a self-contained entity. The first main result on decomposing Farkas interpolants is presented in Chapter 3. Chapter 4 describes the transition power abstraction, Chapter 5 the Golem Horn Solver, and Chapter 6 the cooperative parallelization approach for property directed K-induction.

Text The technical writing is very good. It is precise and appears free of technical errors. The content is self-contained and examples are provided in suitable places to make the material accessible. A typo that triggers some confusion is the following: Algorithm 4.5 on page 65 describes a function called `IsReachable`. I believe it should be `IsReachableLt`. Likewise Algorithm 4.4 describes `IsReachableEq`.

Contents Let me start by appraising the two notable foundational contributions.

Farkas lemma plays a central role in extracting interpolants for linear arithmetic. It exploits that an infeasible set of inequalities can be certified by a vector of non-negative coefficients, such that the sum of inequalities when multiplied by the coefficients add up to a tight and infeasible inequality. All variables are eliminated from the resulting inequality. For interpolation, it means that the subset of non-zero coefficients to rows with A-local variables produce an inequality where these variables have been eliminated. The single inequality is an interpolant with respect to the constraints containing the B-local variables. The insight is that the single inequality can sometimes be decomposed into a stronger set of multiple inequalities. Multiple inequalities may capture useful properties that are not captured by a single inequality.

The chapter on *Split Transition Power Abstractions* introduces a new method for symbolic model checking. In a nutshell it develops a version of iterative squaring that exploits interpolation and quantifier projection (it is shown that model based projection is more useful than full quantifier elimination when refining counter-

examples) to minimize representations of transition invariants. In addition, the chapter presents a K-induction variant. I would call it 2^K induction for the purpose of the report. The K-induction variant is non-trivial because in contrast to linear K-induction the version using iterative squaring could introduce a large number of equivalent sub-formulas. The insight used to control the representation of 2^K unfolding is that sequences of size equal to 2^{K-1} have one representation, sequences of size less than 2^{K-1} are defined recursively as a combination of sequences of length 2^{K-2} and strictly less than 2^{K-2} .

The two foundational contributions are notable. They are fundamental algorithms that address central issues in symbolic model checking. I believe these results stand out and are of lasting value for symbolic model checking. The question of decomposing interpolants is useful in different settings. Possible follow-on research topics include decomposing interpolants over other theories, or decomposing formulas into monadic or near monadic forms. The insight of using interpolation based and model-based projection methods for iterative squaring is sophisticated and the way it is pursued in the thesis is exemplar: it addresses what to me appears to be the main questions on how to turn the basic idea into an effective tool. It relates to Savich's method for establishing PSPACE membership, but there it is a theoretical tool. Iterative squaring was proposed for symbolic model checking with BDDs, but does not offer any space advantages: the size of the BDDs for a transitive closure will be the same regardless of how it is computed.

Golem is a symbolic solver for Constrained Horn clauses (CHC). It integrates the methods established in the other chapters and contains a portfolio of algorithms for symbolic model checking. It allows experiments with other algorithms, such as SPACER, in a setting where the same underlying solver for SMT constraints are used. It participated in recent competitions for CHC solvers and placed at the top. It allows evaluating the split transition abstractions on both synthetic benchmarks and set of programs extracted from model checking evaluations.

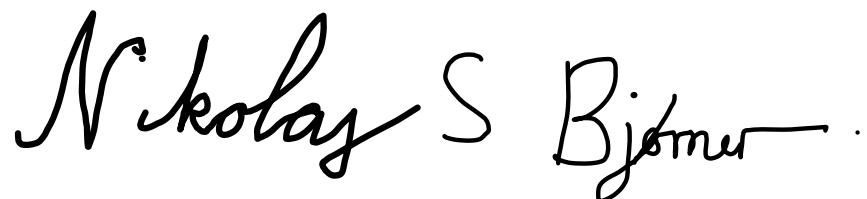
Parallel DP-KIND is an implementation of property directed K-induction within the FiRE/ICE parallel framework supporting. It is built on top of an open source K induction tool, Sally and uses OpenSMT for interpolation queries.

The two tool and experimental contributions are non-trivial both in terms of what is required to make them work and their evaluation relative to state of the art. They represent stellar empirical contributions. The engineering efforts required for these contributions is very significant. It is well above and beyond the stage of prototyping or scripting experiments, a level that is already adequate for establishing empirical feedback.

Concluding Remarks The thesis of high technical quality: It both covers a substantial number of already peer reviewed works by the author from top conferences. It contains several creative ideas that integrate non-trivial insights, and

it includes empirical evaluation of the developed algorithms available, not only in a reproducible format, but generally available for experimentation and evaluation, including in model checking competitions. The thesis therefore clearly meets the standard requirements for a dissertation thesis in computer science and should be accepted. The thesis is excellent.

Sincerely,

A handwritten signature in black ink that reads "Nikolaj S Bjørner". The signature is written in a cursive style with a horizontal line at the end.

March 3rd, 2023

Nikolaj Bjørner
Partner Researcher
Microsoft Research, Redmond
Phone: (425)-4350112
Email: nbjorner@microsoft.com
Web: <http://research.microsoft.com/~nbjorner>