Opening the Black Box: Interpolation in SMT-based Model Checking

FACULTY OF MATHEMATICS AND PHYSICS
Charles University

Martin Blicha
joint work with Antti Hyvärinen, Jan Kofroň, and Natasha Sharygina

Università della Svizzera italiana

Motivation

- Rich use of interpolants in model checking – abstractions, inductive invariants, …
- Problem
  - Traditionally, model checkers and interpolating SMT solvers developed independently
  - Usage of the interpolator: black box, one-size-fits-all approach
- Our approach
  - Tight cooperation between model checker and interpolator
  - *Flexible* interpolation framework
  - *Smart* model checker

Towards Flexible Interpolation

- Decomposition of Farkas Interpolants
  - Interpolation procedure for LRA conflicts
  - Generalization of interpolation procedure based on Farkas coefficients – flexibility in logical strength
- Blicha, Hyvärinen, Kofroň, Sharygina: *Decomposing Farkas Interpolants*. TACAS 2019.

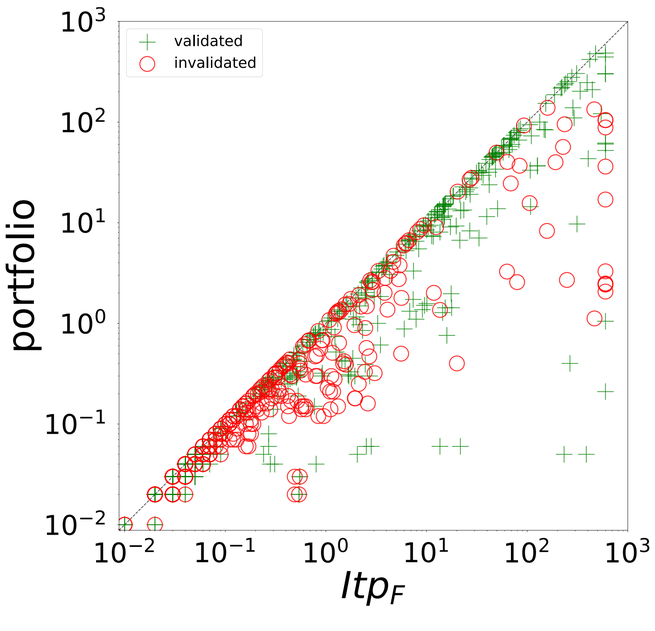
Experiments

- Sally[1] with OpenSMT[2] as interpolator
- Sally benchmark set – 1107 transition systems

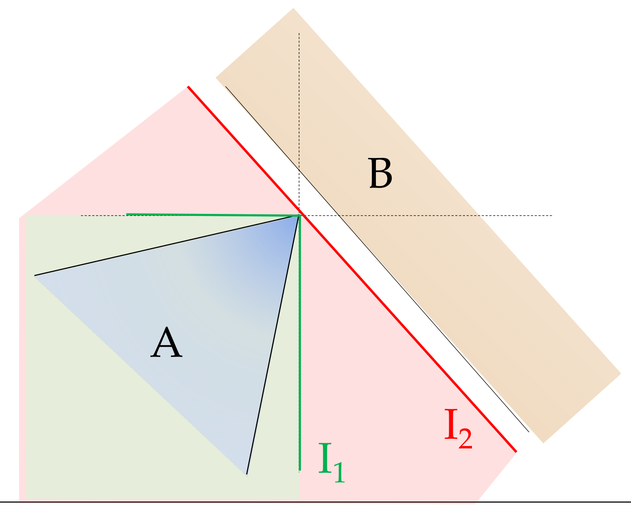
Comparison of the performance of a portfolio against only Farkas interpolation. Runtime in seconds.

Portfolio consisting of four approaches: Farkas interpolants, decomposed interpolants, and their duals.

[1] `http://sri-csl.github.io/sally`
[2] `https://github.com/usi-verification-and-security/opensmt/`



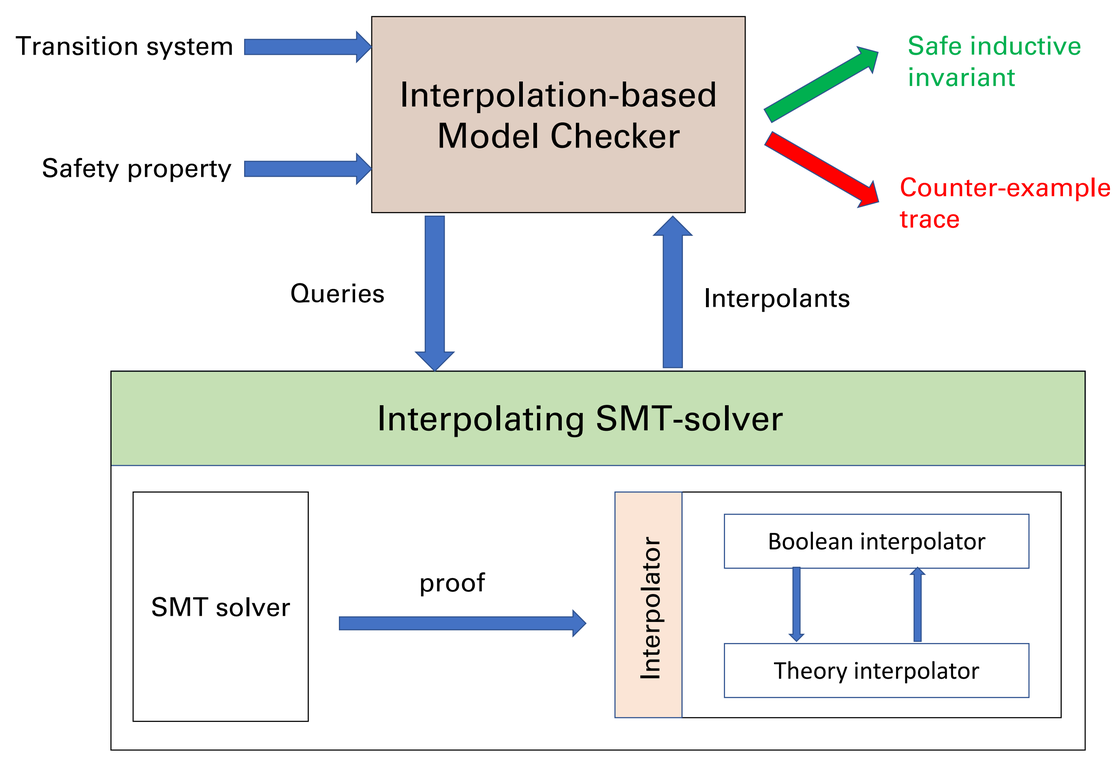
Craig Interpolation



Definition [Craig'57]:
For an unsatisfiable $A \wedge B$, interpolant is a formula I such that:

- $A \Rightarrow I$
- $B \Rightarrow \neg I$
- I contains only common symbols of A and B

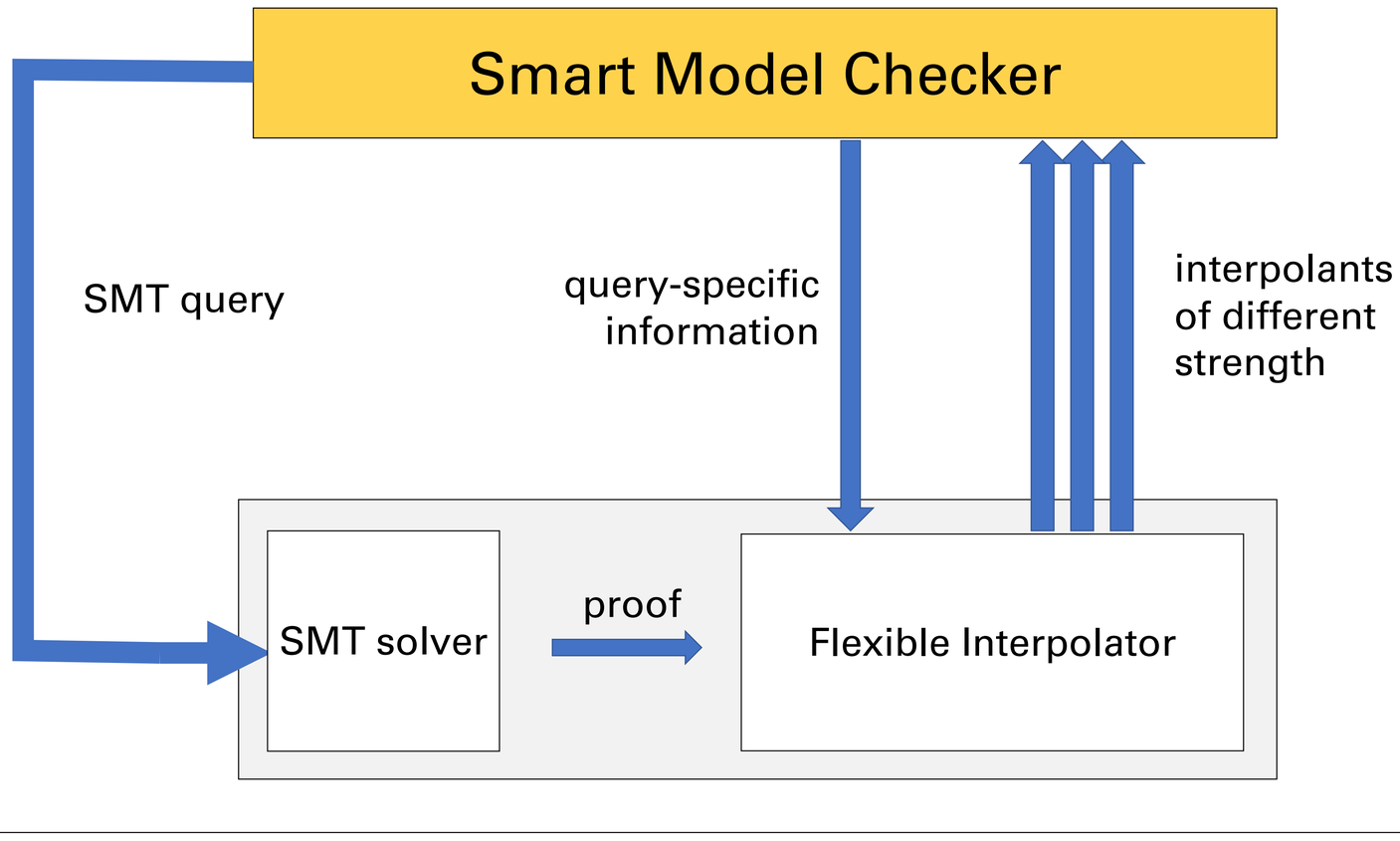
Interpolation-based Model Checking



Towards Smart Model Checker

- Utilizing flexible interpolation — In progress
  - Parallelization – different interpolation strategies
- Multiple interpolants from a single query
  - Choose one with appropriate strength — Future work
  - Delay choice until more information available

Envisioned Approach – Tight Cooperation



This work has been partially supported by Czech Science Foundation project 17-12465S and by the Swiss National Science Foundation (SNSF) grant 200020_166288