The PD-KIND algorithm in the Golem CHC solver

author: Štěpán Henrych | supervisor: doc. RNDr. Jan Kofroň, Ph.D.

Background

Software verification ensures program correctness in safety-critical systems. Key approaches include interactive theorem proving, static analysis, and automated **model checking** – which exhaustively verifies safety properties like "no bad states are reachable".

Constrained Horn Clauses (CHCs) encode verification tasks as logical constraints, separating system behavior (transition models) from property checking.

Golem is a solver, that solves CHC satisfiability problems and generates validity witnesses: inductive invariants (SAFE) or counterexamples (UNSAFE) using 6 different model checking algorithms.

PDKind is another such algorithm, which combines IC3's reachability analysis with k-induction, replacing single-step induction with multi-step reasoning. This hybrid approach enhances proof strength for complex systems where traditional IC3 fails.

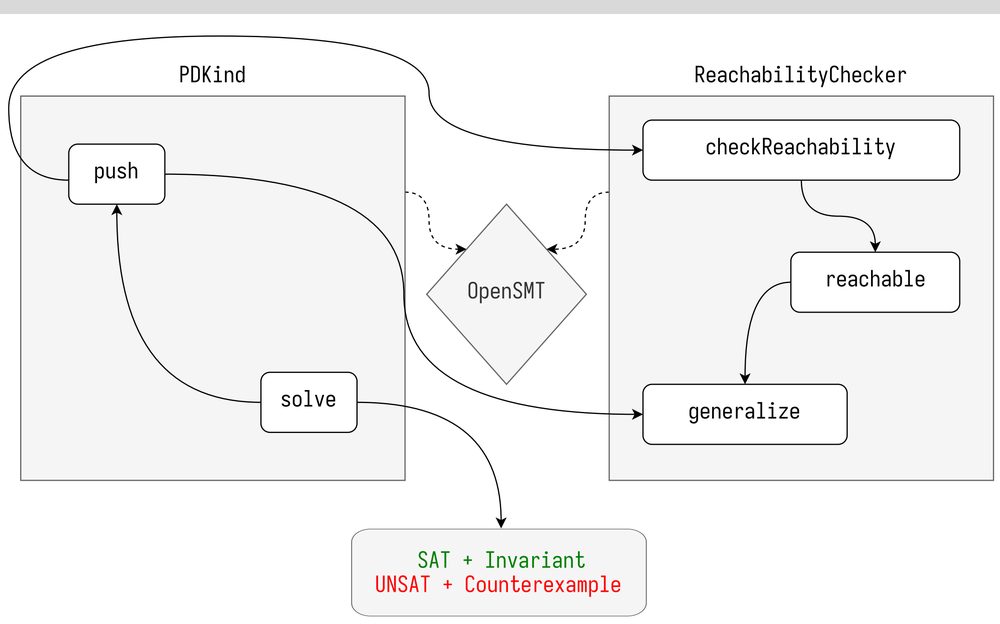
Goals

- Analyze PDKind's algorithm and design its integration into Golem.
- Implement PDKind as a new engine in the Golem framework.
- Extend the engine to generate validity witnesses (SAFE/UNSAFE).
- Evaluate performance against existing engines on a set of benchmarks.
- Verify witness correctness using Golem's internal validator.

Technologies

- **Programming Language:** `C++17`
- **Solver Framework:** `Golem`
- **SMT Backend:** `OpenSMT`

Architecture of the PDKind engine



Architecture Details

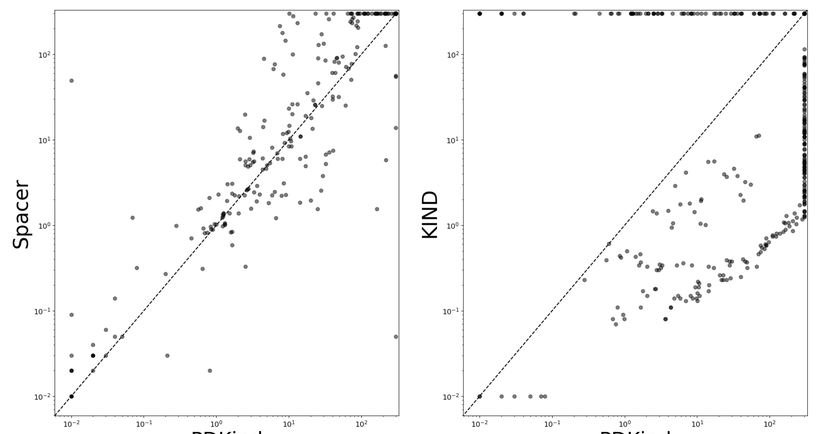
The PDKind engine is composed of two tightly connected modules:

- **PDKind Core:** Orchestrates the verification workflow, handling the main algorithmic steps (*push*, *solve*).
- **Reachability Checker:** Responsible for generalization, reachability analysis, and k-induction (*generalize*, *reachable*, *checkReachability*).

Both modules communicate with the **OpenSMT** solver, which provides satisfiability checking and interpolation. The architecture enables efficient invariant generation and supports witness validation for both SAFE and UNSAFE results.

Experiments

Time comparison of SAT results:



Result table:

Result	**PDKind**	Spacer	KIND
SAT	**242**	214	260
UNSAT	**68**	70	84
TIMEOUT	**188**	214	154

Conclusion

PDKind was integrated into the Golem solver as a new engine combining IC3-style reachability with k-induction. The implementation supports generation and validation of inductive invariants and counterexamples.

Experimental results show that PDKind performs competitively with existing engines. It excels on SAT benchmarks, solving problems that KIND and Spacer cannot, thanks to its ability to strengthen safety properties that are not immediately k-inductive. While KIND is faster when the property is already k-inductive, and Spacer is slightly better on UNSAT cases, PDKind's unique approach makes it a valuable and complementary addition to Golem's engine portfolio.

Overall, PDKind is reliable on both satisfiable and unsatisfiable problems and promising as a complete solver. Future work will focus on improving performance for harder UNSAT cases.

https://github.com/stepanhen/PDKIND-thesis
https://github.com/stepanhen/golem