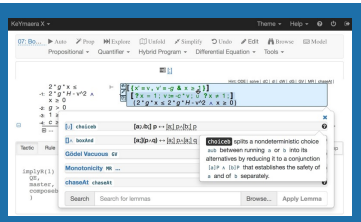

Replay of SMT Proof in KeYmaera X

Ismail Patel, Dr. Stefan Mitsch

DePaul University College of Computing and Digital Media

ABSTRACT

The KeYmaera X theorem prover is an automated and interactive theorem prover for cyber-physical systems (CPS). One subtask in CPS proofs is reasoning over Boolean formulas, which are currently implemented in KeYmaera X with a poorly performing naive exhaustive exploration of the search space. This task is historically well-understood in the SAT/SMT community and highly efficient automated solvers exist. Duplicating such solver implementations inside a theorem prover is a waste of research resources; the alternative of exporting problems and simply trusting an external solver is equally unsatisfactory because it prevents us from producing a complete human-inspectable proof of a CPS in a single axiomatic system.

This project proposes to interact with an automated proof-producing solver (Z3) by replaying and checking external proofs within the axiomatic system of KeYmaera X. The promise of the project is combining the best of both worlds: the optimized performance of an external solver and the trust of a proof expressed in a single axiomatic system. The following references are base readings for how Z3 produces proofs and related attempts to integrate it with other theorem provers.

INTRODUCTION

This paper presents a novel proof replay framework integrating the automated theorem-prover Z3 with the cyber-physical system (CPS) verification tool KeYmaera X. By implementing proof replay functionality, we aim to harness the computational efficiency of Z3 and the trustworthiness of KeYmaera X's axiomatic system, offering an efficient yet robust solution for CPS verification. The proposed approach reads external proofs from Z3, processes them, and checks them within KeYmaera X, providing a unique pathway to reliable automated CPS proofs.

BACKGROUND

Proofs in Z3

Z3 is an SMT (Satisfiability Modulo Theories) solver that produces proofs of logical statements involving arithmetic, arrays, and other data structures. We specifically target the proof-producing capabilities of Z3, leveraging its support for proof generation in the SMT-LIB format. By analyzing Z3's proof output, we extract and interpret logical constructs required to replay these proofs within another verification system

Core Proofs in KeYmaera X

KeYmaera X is a deductive verification tool for CPS, relying on differential dynamic logic (dL) to reason about the continuous and discrete changes in such systems. Proofs in KeYmaera X are structured as derivations within its axiomatic system, emphasizing soundness in safety-critical applications. KeYmaera X, however, lacks the performance of Z3 in proof generation, which our proof replay method addresses by enabling the use of Z3's proofs within KeYmaera X.

Tactics in KeYmaera X

KeYmaera X employs tactics—automated strategies that apply specific proof rules to achieve proof goals. This modular design allows for complex proofs to be broken down into repeatable steps, promoting consistency and scalability. Our approach builds on this by creating compatible tactics to process Z3-derived proofs, bridging the gap between Z3's proof logic and KeYmaera X's proof strategies.

PROOF REPLAY

Proof replay in this context involves translating the proof structure from Z3's format into constructs compatible with KeYmaera X. This requires:

Parsing Z3 Proofs: Our system begins by reading proof data from Z3 in SMT-LIB format, focusing on expressions and logical operators that align with KeYmaera X's logic.

Constructing KeYmaera X Proof Tactics: For each Z3 proof step, a corresponding KeYmaera X tactic is generated, preserving logical equivalence.

Verification in KeYmaera X: Once parsed and converted, the proof is checked within KeYmaera X to ensure each tactic correctly leads to the stated proof goal.

METHODS

The implementation of this proof replay functionality required developing several key components:

Proof Data Structures: Custom classes were created to process Z3 proofs by mapping each logical element to constructs compatible with KeYmaera X. These structures allow for accurate interpretation and replay of proofs within the KeYmaera X environment.

Translation Functions: A core set of translation functions was written to interpret logical expressions, such as AND, OR, NOT, and IMPLIES, from Z3's syntax into KeYmaera X's.

Replay Architecture: A software architecture was set up to support proof translation, tactic generation, and verification within KeYmaera X. This system iterates through the steps of each Z3 proof, generating tactics and applying them step-by-step, facilitating real-time proof replay and verification within KeYmaera X.

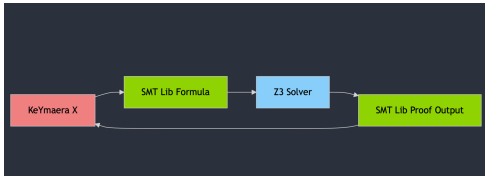

Figure 1: Flow of Z3 Proof Reader. KeYmaera X takes an expression e.g P&Q -> P. Converts the expression to an SMT Lib Formula. The formula is passed to Z3 which outs a proof in SMT Lib format. That output is then replayed in KeYmaera X.

```
Run with -debug for more details.
(set-option :produce-proofs true)
(declare-fun _p_P () Bool)
(declare-fun _p_Q () Bool)
(assert (not (=> (and _p_P _p_Q) _p_P)))
(check-sat)
```

Figure 2: Expression Converted to SMT Lib Formula

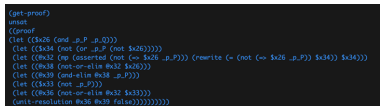

Figure 3: Z3 output of formula

RESULTS

This is project is a work in progress. The current case that is being worked on is a simple expression P&Q -> P. We are replaying this proof with the assumption that there will be an overlap between other general cases.

DISCUSSIONS / CONCLUSIONS

In conclusion, this project demonstrates the potential of combining KeYmaera X's formal rigor with Z3's computational efficiency to advance CPS verification by leveraging external proof-producing solvers in a way that maintains verifiable integrity. Rather than duplicating solver efforts or relying on opaque external results, this approach facilitates a seamless replay of Z3's proof outputs directly within KeYmaera X, aiming for transparent, human-inspectable proofs within a single, cohesive axiomatic framework. Although this work remains in progress, it sets a promising foundation for efficiently incorporating external proofs in CPS verification, aiming ultimately to expand KeYmaera X's capabilities to handle complex proofs and advanced tactics reliably and trustworthily.

KeYmaera X	Z3
Identity (id): $\frac{*}{p \vdash p}$	Asserted: $\frac{*}{\{p\} \vdash p}$
Modus Ponens (MP): $\frac{*}{p_1, p_1 \rightarrow p_2 \vdash p_2}$	Modus Ponens (MP): $\frac{\Gamma_1 \vdash p_1 \quad \Gamma_2 \vdash p_1 \rightarrow p_2}{\Gamma_1 \cup \Gamma_2 \vdash p_2}$

Table 1: Corresponding Proof Rules in KeYmaera X and Z3

Figure 4: In progress conversion of figure 3 to map to KeYmaera X's proof rules.

FUTURE DIRECTIONS

- Generalize from propositional logic to first-order logic of real arithmetic

SOURCES AND ACKNOWLEDGEMENTS

S. Böhme, "Proof Reconstruction for Z3 in Isabelle/HOL," in *Proceedings of the 7th International Workshop on Satisfiability Modulo Theories (SMT '09)*, 2009.

Thank you Dr. Stefan Mitsch