UNIVERSIDADE FEDERAL DE MINAS GERAIS
Instituto de Ciências Exatas
Programa de Pós-Graduação em Ciência da Computação

Tomaz Gomes Mascarenhas

Demonstrando teoremas em Lean por meio da reconstrução de provas em SMT

Belo Horizonte
2023

Tomaz Gomes Mascarenhas

Demonstrando teoremas em Lean por meio da reconstrução de provas em SMT

Versão Final

Dissertação apresentada ao Programa de Pós-Graduação em Ciência da Computação da Universidade Federal de Minas Gerais, como requisito parcial à obtenção do título de Mestre em Ciência da Computação.

Orientador: Haniel Barbosa

Belo Horizonte
2023

Tomaz Gomes Mascarenhas

Proving Lean theorems via reconstructed SMT proofs

Final Version

Thesis presented to the Graduate Program in Computer Science of the Federal University of Minas Gerais in partial fulfillment of the requirements for the degree of Master in Computer Science.

Advisor: Haniel Barbosa

Belo Horizonte
2023

[Ficha Catalográfica em formato PDF]

A ficha catalográfica será fornecida pela biblioteca. Ela deve estar em formato PDF e deve ser passada como argumento do comando `ppgccufmg` no arquivo principal `.tex`, conforme o exemplo abaixo:

```
\ppgccufmg{
      ...
      fichacatalografica={ficha.pdf}
}
```

[Folha de Aprovação em formato PDF]

A folha de aprovação deve estar em formato PDF e deve ser passada como argumento do comando `ppgccufmg` no arquivo principal `.tex`, conforme o exemplo abaixo:

```
\ppgccufmg{
     ...
     folhadeaprovacao={folha.pdf}
}
```

Dedicuum cest laborae a quelquis personatum que ajudorat a facirelo.

Acknowledgments

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

At vero eos et accusamus et iusto odio dignissimos ducimus qui blanditiis praesentium voluptatum deleniti atque corrupti quos dolores et quas molestias excepturi sint occaecati cupiditate non provident, similique sunt in culpa qui officia deserunt mollitia animi, id est laborum et dolorum fuga. Et harum quidem rerum facilis est et expedita distinctio. Nam libero tempore, cum soluta nobis est eligendi optio cumque nihil impedit quo minus id quod maxime placeat facere possimus, omnis voluptas assumenda est, omnis dolor repellendus. Temporibus autem quibusdam et aut officiis debitis aut rerum necessitatibus saepe eveniet ut et voluptates repudiandae sint et molestiae non recusandae. Itaque earum rerum hic tenetur a sapiente delectus, ut aut reiciendis voluptatibus maiores alias consequatur aut perferendis doloribus asperiores repellat.

"*Só quem sonha acordado vê o sol nascer.*"
(Unkown)

Resumo

Lorem ipsum dolor sit amet, consectetur adipisicing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Sed ut perspiciatis unde omnis iste natus error sit voluptatem accusantium doloremque laudantium, totam rem aperiam, eaque ipsa quae ab illo inventore veritatis et quasi architecto beatae vitae dicta sunt explicabo. Nemo enim ipsam voluptatem quia voluptas sit aspernatur aut odit aut fugit, sed quia consequuntur magni dolores eos qui ratione voluptatem sequi nesciunt. Neque porro quisquam est, qui dolorem ipsum quia dolor sit amet, consectetur, adipisci velit, sed quia non numquam eius modi tempora incidunt ut labore et dolore magnam aliquam quaerat voluptatem. Ut enim ad minima veniam, quis nostrum exercitationem ullam corporis suscipit laboriosam, nisi ut aliquid ex ea commodi consequatur? Quis autem vel eum iure reprehenderit qui in ea voluptate velit esse quam nihil molestiae consequatur, vel illum qui dolorem eum fugiat quo voluptas nulla pariatur?

Palavras-chave: Verificação Formal, Lean, SMT

Abstract

Despite their expressivity and robustness, interactive theorem provers (ITPs) can be quite costly to use in large-scale formalizations due to the burden of interactively proving goals. Discharging some of these goals via automatic theorem provers, such as satisfiability modulo theories (SMT) solvers, is a known way of improving the usability of ITPs. This thesis describes a novel integration between the ITP Lean 4 and the SMT solver cvc5.

Assuming an encoding of the Lean goal as an SMT problem and that cvc5 generates a proof for the encoded problem, we show how to lift this proof into a proof of the original Lean goal. This requires proving the correctness, inside Lean, of the steps taken by the solver, as well as decoding the terms in the proof into the original Lean ones. Thus Lean can accept the SMT proof as a proof of the original goal.

This tool is part of the joint project Lean-SMT, which aims to create a tactic in Lean that implements the whole pipeline, that is, from a goal in Lean, translate it into a query in SMT-Lib format, try to prove it using a SMT solver and, in case it is successful, lift the proof produced, closing the original goal in Lean (which is done by our tool). All the other steps of the pipeline are in an advanced stage of development.

Keywords: Formal Verification, Lean, SMT

List of Figures

List of Tables

Lista de Algoritmos

Contents

Chapter 1

Introduction

1.1 Context

1.2 Contributions

Chapter 2

Formal Preliminaries

2.1 Satisfiability Modulo Theories

2.2 Lean's Type Theory

2.3 Lean's Framework for Metaprogramming

Chapter 3

Certifying Reconstruction of SMT Proofs in Lean

3.1 Certified vs Certifying

3.2 Tactics

Chapter 4

Evaluation

Chapter 5

Future Work