Formalizing Mathematics in ACL2

Ruben Gamboa

2023-10-24

Table of contents

Preface 3

I Introduction to ACL2 4

1 Introduction to ACL2 5

II Algebra 6

2 Polynomials 7

3 Quadratic Formula 8

References 9

Preface

The theorem prover ACL2 has been used extensively to reason about hardware and software systems. It was designed to prove theorems about functions in Common LISP, and it is among the top theorem provers in the world.

ACL2 was not, however, designed explicitly to reason about mathematics. In fact, it lacks many features that would normally be considered mandatory for mathematical reasoning, such as

- the real numbers,
- sets,
- higher-order functions, and
- strong support for quantifiers.

Nevertheless, mathematics is essential for reasoning about many software systems, e.g., number theory in cryptography or the Discrete Fourier Transform in signal processing. So many areas of mathematics have indeed been formalized in ACL2, often pushing the boundary of what is and is not formalizable in ACL2. This book collects many different mathematical proofs in ACL2, including results from number theory, algebra, and analysis. It aims to teach you, the reader, how those formalizations proceeded and how to use ACL2 to prove new mathematical facts.

The first part of the book introduces ACL2 to readers who are unfamiliar with this theorem prover. You may safely skip this part if you are already confident with ACL2. The remaining parts examine a number of different mathematical formalizations in ACL2. You may essentially read these in any order, though some depend on previously formalized results.

To learn more about ACL2 visit the ACL2 home page at https://www.cs.utexas.edu/users/moore/acl2/.

Part I

Introduction to ACL2

1 Introduction to ACL2

See Kaufmann, Manolios, and Moore (2000) for information about ACL2.

Part II

Algebra

2 Polynomials

This chapter describes how polynomials can be defined in ACL2 and some simple theorems about polynomials in general.

3 Quadratic Formula

This chapter presents a proof of the quadratic formula for polynomials with real or complex coefficients.

References

Kaufmann, M., P. Manolios, and. Moore. 2000. *Computer-Aided Reasoning: An Approach.* Kluwer Academic Press.