The pervasive use of computers in mathematics and engineering has led to an increased demand for reliability in the implementation of algorithms in computer algebra systems. However, while computer algebra systems like Matlab and Mathematica are widely used, the implementations of the algorithms are often not carefully specified or documented. By using a proof assistant to represent both the algorithms and the proofs of the mathematical theorems stating their specification, the correctness of the implementations can be formally verified.

This thesis studies an approach, based on refinements, for formally verifying efficient programs and data structures in the interactive theorem prover Coq. It also describes the formalization of many mathematical results and notions from constructive algebra. This involves implementing libraries of formalized mathematics that can be used to reason about algorithms from computer algebra. This way the gap between computer algebra systems and interactive theorem provers can be decreased, increasing both the reliability of the implemented algorithms and the computational capabilities of proof assistants.

UNIVERSITY OF
GOTHENBURG

ISBN 978-91-982237-0-5

Anders Mörtberg

Formalizing Refinements and Constructive Algebra in Type Theory

2014

UNIVERSITY OF GOTHENBURG

Formalizing Refinements and Constructive Algebra in Type Theory

Anders Mörtberg

Ph.D. thesis

Department of Computer Science and Engineering
Chalmers University of Technology & University of Gothenburg

Gothenburg, Sweden 2014

IT Faculty