Formalizing Refinements and Constructive Algebra in Type Theory

ANDERS MÖRTBERG

The defense of this thesis for the degree of Doctor of Philosophy
will be held in room **ED**, EDIT building,
Rännvägen 6B, Chalmers University of Technology,
on **Friday, Dec 12, 2014**, at **10:00**.

Discussion Leader: **Georges Gonthier**
Microsoft Research Cambridge

The thesis is available at the Department of Computer Science and Engineering, Chalmers University of Technology.

Department of Computer Science and Engineering
Chalmers University of Technology and Göteborg University
SE-412 96 Göteborg, Sweden
Telephone +46 (0)31–772 1000

UNIVERSITY OF
GOTHENBURG

Abstract

The extensive use of computers in mathematics and engineering has led to an increased demand for reliability in the implementation of algorithms in computer algebra systems. One way to increase the reliability is to formally verify that the implementations satisfy the mathematical theorems stating their specification. By implementing and specifying algorithms from computer algebra inside a proof assistant both the reliability of the implementation and the computational capabilities of the proof assistant can be increased.

This first part of the thesis presents a framework, developed in the interactive theorem prover Coq, for conveniently implementing and reasoning about program and data refinements. In this framework programs defined on rich dependent types suitable for proofs are linked to optimized implementations on simple types suitable for computation. The correctness of the optimized algorithms is established on the proof-oriented types and then automatically transported to the computation-oriented types. This method has been applied to develop a library containing multiple algorithms from computational algebra, including: Karatsuba's polynomial multiplication, Strassen's matrix multiplication and the Sasaki-Murao algorithm for computing the characteristic polynomial of matrices over commutative rings.

The second part of the thesis presents the formalization of notions from constructive algebra. Focus is on the theory of coherent and strongly discrete rings, which provides a general setting for developing linear algebra over rings instead of fields. Examples of such rings include Bézout domains, Prüfer domains and elementary divisor rings. Finitely presented modules over these rings are implemented using an abstraction layer on top of matrices. This enables us to constructively prove that the category of these modules form a suitable setting for developing homological algebra. We further show that any finitely presented module over an elementary divisor ring can be decomposed to a direct sum of a free module and cyclic modules in a unique way. This decomposition gives a decision procedure for testing if two finitely presented modules are isomorphic.

Keywords: Formalization of mathematics, refinements, constructive algebra, type theory, Coq, SSReflect.

ISBN: 978-91-982237-0-5