Types for Proofs, Computers and Mathematics

Yves Bertot

INRIA Sophia Antipolis
2004 route des Lucioles, BP 93
06902 Sophia Antipolis CEDEX

May 13, 2003

1 Introduction

Type theory and formalized Mathematics

A guided tour of formalized Mathematics from the types community

– Introspection

– Numbers

– Algebra

– Geometry

– Analysis

Introspection

– Studies of basic models of computation : combinatory logic, typed and untyped λ-calculus, process-algebra, π-calculus, the Calculus of Constructions,

– Algorithms of formal reasoning : unification, satisfiability, ordered binary decision diagrams (BDD),

– Computer systems : protocols, temporal logic, (Büchi) automata, hardware,

– Programming languages, functional and imperative cores, Java, bytecode verification, compiler correctness,

– Sorting, sorting, sorting. . .

3 Numbers

Numbers

- Natural numbers,
  - primality tests, combinatorics, RSA encryption and decryption *Minho, Nijmegen, Sophia*,
- Integers,
  - unbounded binary representation of numbers,
  - decision procedures: Omega (linear inequalities), Ring (polynomial equalities), *Lannion, Paris*,
  - Efficient implementation of algorithms : square root, division. (from GMP), *Sophia, Nancy*.

Real numbers

- One presentation based on 18 axioms characterizing a complete archimedian field,
- Decision procedures : Field (fractional equalities), Fourier (linear inequalities),
- Most basic functions `sin, cos, ...` formalized *Rocquencourt*,
- The three gap theorem, the Bertrand conjecture, the intermediate value theorem. . . *L'Aquila, Paris, Rocquencourt, Sophia*,
- Floating point arithmetics: the IEEE 754 standard, floating point expansions, *Sophia, Lyon*.

Constructive real numbers

The *CCorN* repository, *Nijmegen*,

– Foundations of type theory make it possible to distinguish between constructive and non-constructive mathematics,

– Constructive real numbers as Cauchy sequences : apartness is primitive, equality is defined as a negation, *Edinburgh*, *Nijmegen*, *Udine*,

– Constructive proof of the fundamental theorems of Algebra and analysis, *Nijmegen*

– Rational numbers: representation drawn from Euclid's GCD algorithm and continued fractions, *Nijmegen*, *Sophia*.

Algebra

- Category theory, *Rocquencourt*, *Tokyo*,
- Schemes, sheaves, algebraic geometry (formalization or Hartshorne's book), *Sophia*, *Nice*,
- Universal algebra, *Nijmegen*,
- Commutative algebra (groups, rings, fields), *Sophia*,
- linear algebra (vector spaces, matrices), *Sophia*.

Polynomials

- the free algebra of polynomials, *Sophia*,
- Karatsuba multiplication, *Sophia*,
- Fast Fourier Transform, *Nijmegen*, *Sophia*,
- Recursive descriptions of polynomials, *Sophia*, *Chalmers*,
- Irreductibility of polynomials on finite fields, *Sophia*,
- Gröbner bases : Buchberger's algorithm and Dickson's lemma *Chalmers*, *Sophia*.

Type-theory provers of symbolic systems

- Computer Algebra systems:
  - Coq-Maple collaboration, *Chalmers*, *Paris*,
  - Coq-Gap collaboration, *Nijmegen*,
  - FOC : developing a certified computer algebra library, *Paris*,
- Rewriting:

`Coq-Elan`, *Lannion*, *Nancy*.

Geometry

- Understanding axioms for geometry, *Sophia*, *Strasbourg*, *Helsinki*,
- High-school geometry : lines, circles, angles, planes in the 3D space, *Sophia*,
- Convex hull algorithms in the plane, *Sophia*,
- Modelers and surface topology, *Strasbourg*.

10 Other fields

Other fields

- Formal topology : Hahn-Banach, Heine-Borel, *Padova*, *Chalmers*.
- And probably a few others.