A Monadic Approach to Certified Exact Real Arithmetic

Russell O'Connor

Radboud University Nijmegen

TYPES / TFP 2006

April 19, 2006

Certified Real Arithmetic

- Arbitrary precision real number computation
- We have fast complex libraries
  - MPFR
- We have slow certified implementations
  - C-CoRN
- We want to find the sweet spot of easy to certify fast enough real arithemetic.

Certified Reals Arithmetic

- Why certified?
  - Toward certified computer algebra
    - Certified calculator
  - Disproof of Merten’s conjecture
    - Requires approximating roots of zeta function
  - Kepler conjecture
    - 99% certain it is correct
    - We are going to make that 100%.

Completion

- Let X be a “metric space”.
- Define $C(X)$ the metric space of regular functions.

$$C(X) \stackrel{\text{def}}{=} \{ f : \mathbb{Q}^+ \Rightarrow X \mid \forall \varepsilon_1 \varepsilon_2, \overline{B}_{\varepsilon_1 + \varepsilon_2} (f(\varepsilon_1), f(\varepsilon_2)) \}$$

Completion

- Let X be a "metric space".
- Define $C(X)$ the metric space of regular functions.

$$C(X) \stackrel{\text{def}}{=} \{ f : \mathbb{Q}^{+} \Rightarrow X \mid \forall \varepsilon_1 \varepsilon_2, \overline{B}_{\varepsilon_1 + \varepsilon_2}(f(\varepsilon_1), f(\varepsilon_2)) \}$$

- C is a monad.
  - $X \hookrightarrow C(X)$
  - $C(C(X)) \rightarrow C(X)$
  - $(X \rightarrow Y) \Rightarrow (C(X) \rightarrow C(Y))$

Uniform Continuity

- Suppose
  - X is a nice metric space.
  - $f : X \to Y$ is uniformly continuous with modulus μ.
  - $x : \mathbb{Q}^+ \Rightarrow X$ is a regular function.

Uniform Continuity

- Suppose
  - X is a nice metric space.
  - $f : X \to Y$ is uniformly continuous with modulus μ.
  - $x : \mathbb{Q}^{+} \Rightarrow X$ is a regular function.
- Then
  - $f \circ x \circ \mu : \mathbb{Q}^{+} \Rightarrow Y$ is a regular function.

Uniform Continuity

- Suppose
  - X is a nice metric space.
  - $f : X \to Y$ is uniformly continuous with modulus μ.
  - $x : \mathbb{Q}^+ \Rightarrow X$ is a regular function.
- Then
  - $f \circ x \circ \mu : \mathbb{Q}^+ \Rightarrow Y$ is a regular function.
- This yields the map operation of type

$(X \to Y) \Rightarrow (C(X) \to C(Y))$.

Uniformly Continuous Functions

- $\mathbb{Q}$ is nice.
- Uniformly continuous functions, $\mathbb{Q} \to \mathbb{Q}$:
  - $\lambda x.\ \text{-}x$
  - $\lambda x.\ |x|$
  - $\lambda x.\ c + x$
  - $\lambda x.\ cx$
    - $\lambda\varepsilon.\ c^{-1}\varepsilon$ is a modulus of continuity
- All these lift to $C(\mathbb{Q}) \to C(\mathbb{Q})$.

Uniformly Continuous, Curried Functions

- $X \to \mathbb{Q}$ is a metric space.
  - Using the ∞-norm.
- More uniformly continuous functions, $\mathbb{Q} \to ([a, b] \to \mathbb{Q})$:
  - $\lambda x.\, \lambda y.\, x + y$
  - $\lambda x.\, \lambda y.\, xy$
- All these lift to $C(\mathbb{Q}) \to C([a, b] \to \mathbb{Q})$.
  - Isomorphic to $C(\mathbb{Q}) \to C([a, b]) \to C(\mathbb{Q})$.

Reciprocal

- Let $x : C(\mathbb{Q})$ and $x \# 0$.
- Consider $0 < a < x$ where $a : \mathbb{Q}$.
- Consider the domain $[a, \infty) \cap \mathbb{Q}$.

Reciprocal

- Let $x : C(\mathbb{Q})$ and $x \# 0$.
- Consider $0 < a < x$ where $a : \mathbb{Q}$.
- Consider the domain $[a, \infty) \cap \mathbb{Q}$.
- $\lambda y.\ (\max(a, y))^{-1}$ is uniformly continuous with modulus $\lambda\varepsilon.\ \varepsilon a^2$.
- Map x over this uniformly continuous function.

Calculus

- Taylor series!

$$\cos(a) = \sum_{i=0}^{\infty} \frac{(-1)^i a^{2i}}{(2i)!}$$

- Alternating sums easily make regular functions.
  - $\cos_{\mathbb{Q}} : \mathbb{Q} \to C(\mathbb{Q})$
  - $\mathrm{bind}\ \cos_{\mathbb{Q}} : C(\mathbb{Q}) \to C(\mathbb{Q})$

Range Reduction - exp

$$\exp(x) = \frac{1}{\exp(-x)}$$

Range Reduction - $\ln$

$$\ln(x) = -\ln\left(\frac{1}{x}\right)$$

Range Reduction - exp

$$\exp(x) = \exp^2\left(\frac{x}{2}\right)$$

Range Reduction - cos

$$\cos(x) = 1 - 2\sin^2\left(\frac{x}{2}\right)$$

Range Reduction - $\sin$

$$\sin(x) = 3\sin\left(\frac{x}{3}\right) - 4\sin^3\left(\frac{x}{3}\right)$$

Range Reduction - $\ln$

$$\ln(x) = \ln\left(\frac{x}{2^n}\right) + n\ln(2)$$

Range Reduction - $\ln$

$$\ln(x) = \ln\left(\frac{3}{4}x\right) + \ln\left(\frac{4}{3}\right)$$

Range Reduction - arctan

$$\arctan(x) = -\arctan(-x)$$

Range Reduction - arctan

$$0 \leq x \Rightarrow \arctan(x) = \frac{\pi}{2} - \arctan\left(\frac{1}{x}\right)$$

Range Reduction - arctan

$$0 \leq x \Rightarrow \arctan(x) = \frac{\pi}{4} + \arctan\left(\frac{x-1}{x+1}\right)$$

π

$$\pi = 48 \arctan\left(\frac{1}{38}\right) + 80 \arctan\left(\frac{1}{57}\right) + 28 \arctan\left(\frac{1}{239}\right) + 96 \arctan\left(\frac{1}{268}\right)$$

Compression

- $[a - \varepsilon, a + \varepsilon]$ contains a unique smallest rational.
- Let $\mathrm{approx}_{\varepsilon}(a)$ be that rational.
- Let $x : C(\mathbb{Q})$.
- $\lambda\varepsilon.\ \mathrm{approx}_{\varepsilon/2}(x(\varepsilon/2)) : C(\mathbb{Q})$

  is equivalent to x but “smaller”.

Correctness

- What does it mean to be correct?
  - Could prove properties of these functions.
  - Could prove equivalence to a reference standard.
- C-CoRN
  - Provides a reference implementation of real numbers in Coq.
- Formalize this theory in your favourite system!

Speed

- Is this fast enough?
- What is fast enough?
- Hales's proof of the Kepler conjecture provides a "test suite".
- Haskell prototype: Few Digits
  - Entered in the "Many Digits" competition
    - Did not finish last!

Other Representations

$$C(X) \quad \{f : \underbrace{\boxed{\mathbb{Q}^+}}_{\text{Gauge}} \Rightarrow \underbrace{\boxed{X}}_{\text{Base}} \mid \forall \varepsilon_1 \varepsilon_2, \overline{B}_{\varepsilon_1+\varepsilon_2}(f(\varepsilon_1), f(\varepsilon_2))\}$$

$$\{2^n \mid n : \mathbb{Z}\} \qquad \{a 2^b \mid a, b : \mathbb{Z}\}$$

$$\{\varphi^n \mid n : \mathbb{Z}\} \qquad \mathbb{Z}[\varphi]$$

Other Work

- Use the type $\mathbb{Q} + C(\mathbb{Q})$
  - Run rational operations when it is known to be rational
    - Sometimes rational operations are slower
- Have functions return an interval
  - Return a point the the result is known to be precise

More Information

- Google “Few Digits”
  - http://r6.ca/FewDigits/
- Upcoming paper in Mathematical Structures in Computer Science.