# Construction of real algebraic numbers in Coq

**Cyril Cohen**

INRIA Saclay – Île-de-France
LIX École Polytechnique
INRIA Microsoft Research Joint Centre
cohen@crans.org

November 28, 2011

# Why formalise real algebraic numbers ?

- Subset of real numbers with decidable equality
- Countable
- Instance of real closed field
- Useful in the formalisation of Feit-Thompson theorem (Mathematical Components project)

# What are real algebraic numbers ?

Real algebraic numbers are real roots of polynomials with coefficients in $\mathbb{Q}$.

# What do we want to know about it ?

- Comparison (equality, ordering)
- Arithmetic operations and their properties (ordered field)
- Intermediate value theorem for polynomials

# “Top-down” approach

- start with a notion of real numbers
- restrict it to roots of polynomials with coefficients in $\mathbb{Q}$

# Cauchy reals

Representation :

- a sequence $(x_n)_{n \in \mathbb{N}}$
- a convergence modulus $m : \mathbb{Q} \to \mathbb{N}$
  such that : $\forall \varepsilon\ i\ j,\ m(\varepsilon) < i, j \to |x_i - x_j| < \varepsilon$

# the theory of Cauchy reals

- Definition of the equality $\equiv$ (not decidable)

$$\bar{x} \equiv \bar{y} \quad \Longleftrightarrow \quad |x_n - y_n| \underset{n\infty}{\longrightarrow} 0$$

- Setoid property of Cauchy reals
- Definition and morphism property of arithmetic operations
- Property of operations (basically field properties)

# "Top-down" representation of algebraics

The type `algcreal` of algebraic Cauchy reals is given by:

- a Cauchy real $\bar{x}$
- a polynomial $P \in \mathbb{Q}[X]$ such that $P(\bar{x}) \equiv 0$

# Properties of algebraic Cauchy reals

- Comparison is now decidable (thanks to the additional information given by the polynomial)
- We can define all the operations using the ones on Cauchy reals (and constructing the appropriate polynomials)

# Issues with this representation

The setoid of algebraic Cauchy reals represents the set of real algebraic numbers.
But:

- No (direct) evidence that the underlining "set" is countable
- No evidence that we can get a datatype which elements represent distinct algebraic numbers.

# “Bottom-up” representation

A pair of:

- a polynomial of $\mathbb{Q}[X]$
- some way to select a precise root (interval, approximation, ...)

# Our selection method

The type `algdom` representing the "algebraic numbers domain" is definied by a pair:

- polynomial $P \in \mathbb{Q}[X]$
- interval $[c - r, c + r]$ such that $P$ is monotone and change sign

# Equivalence of representations

We build :

- `to_algcreal: algdom -> algcreal`
- `to_algdom: algcreal -> algdom`

Such that

```
forall x, to_algcreal (to_algdom x) == x
```

# Porting operations to the "algebraic numbers domain"

Operations on `algdom` are derived from `algcreal`:

```
eq_algdom x y := (eq_algcreal
    (to_algcreal x)(to_algcreal y))

add_algdom x y := to_algdom (add_algcreal
    (to_algcreal x)(to_algcreal y))
```

# Quotient of `algdom`

`eq_algdom` is a decidable equivalence on a countable type

# Quotient of `algdom`

`eq_algdom` is a decidable equivalence on a countable type

$\Rightarrow$ We can take the effective quotient type of `algdom` by this equivalence.

# Quotient of `algdom`

`eq_algdom` is a decidable equivalence on a countable type

$\Rightarrow$ We can take the effective quotient type of `algdom` by this equivalence.

$\Rightarrow$ This defines the type `realalg` of exact algebraic numbers

# Structure of `realalg`

Transfer operations from `algdom` to `realalg`

Transfer their properies (derived from `algcreal`)

# Structure of `realalg`

Transfer operations from `algdom` to `realalg`

Transfer their properies (derived from `algcreal`)

$\Rightarrow$ `realalg` has a structure of real closed field with decidable comparison

# Practical use

- This structure is not designed for efficient computation.
- Its aim is to make constructive proofs:
  - to implement the real closed field interface
  - to help certifying an efficient implementation

# Conclusion

We used:

- One representation for computation: `algcreal`
- One representation to hold data: `algdom`

Future work:

- Complex algebraic numbers (extension with $i$)