Formalized algebraic numbers: construction and first-order theory

Cyril Cohen

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

November 20, 2012

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\text{Garfield is a cat} \quad \text{all cats have four legs}}{\text{Garfield has four legs}}$$

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\text{Garfield is a cat} \quad \text{all cats have four legs}}{\text{Garfield has four legs}}$$

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\text{Garfield is a cat} \qquad \text{for all } x \text{ which is a cat, } x \text{ has four legs}}{\text{Garfield has four legs}}$$

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\text{Garfield is a cat} \qquad \text{for all } x \text{ which is a cat, } x \text{ has four legs}}{\text{Garfield has four legs}}$$

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\text{Garfield} : \text{cat} \qquad \text{for all } x : \text{cat},\ x \text{ has four legs}}{\text{Garfield has four legs}}$$

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\begin{array}{l}\text{Garfield} : \text{cat} \\ \text{for all } x : \text{cat},\ x \text{ has four legs}\end{array}}{\text{Garfield has four legs}}$$

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\text{Garfield} : \text{cat} \qquad \forall x : \text{cat},\ x \text{ has four legs}}{\text{Garfield has four legs}}$$

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\text{Garfield} : \text{cat} \qquad \forall x : \text{cat},\ x \text{ has four legs}}{\text{Garfield has four legs}}$$

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\begin{array}{l}\mathsf{Garfield} : \mathsf{cat} \\ \forall x : \mathsf{cat},\ P(x)\end{array}}{P(\mathsf{Garfield})}$$

Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

E.g.

$$\frac{\begin{array}{l}\text{Garfield} : \text{cat} \\ \forall x : \text{cat},\ P(x)\end{array}}{P(\text{Garfield})}$$

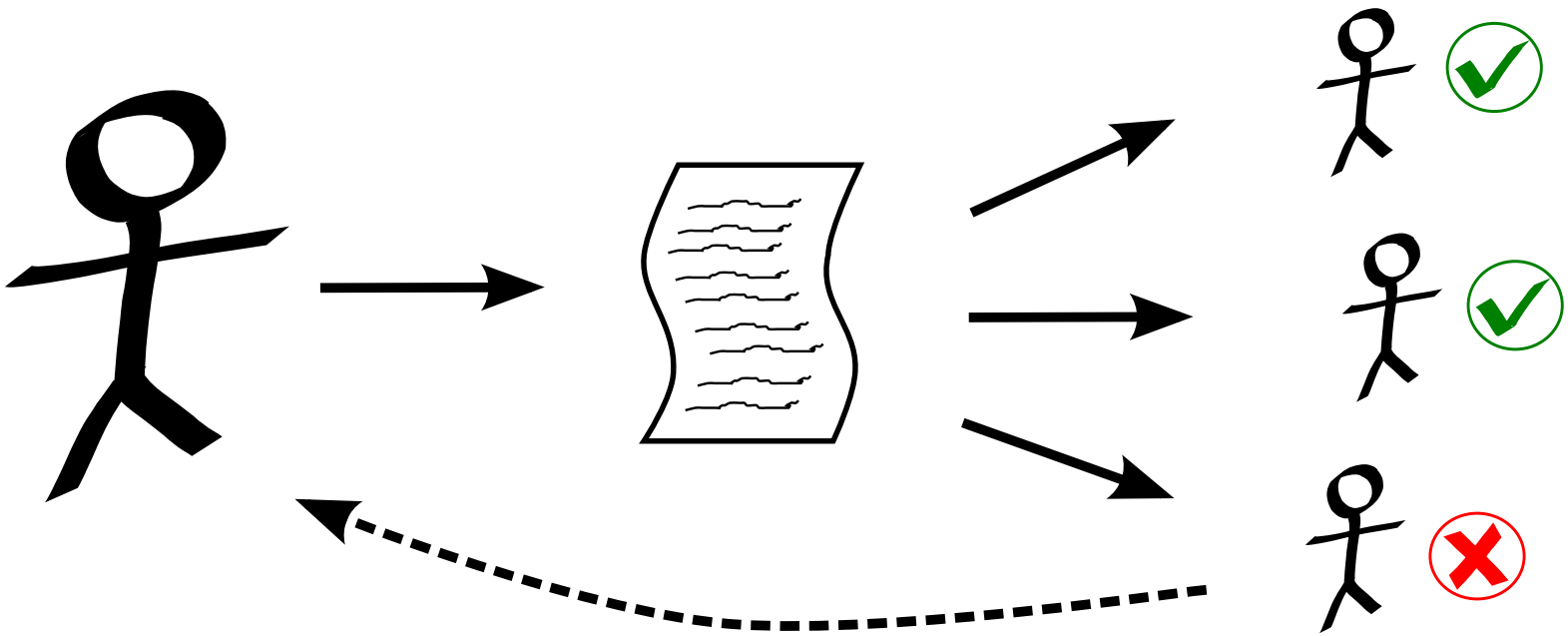
Formalization of mathematics

Mathematics is a game: mathematicians must follow "rules" to convince their colleagues.

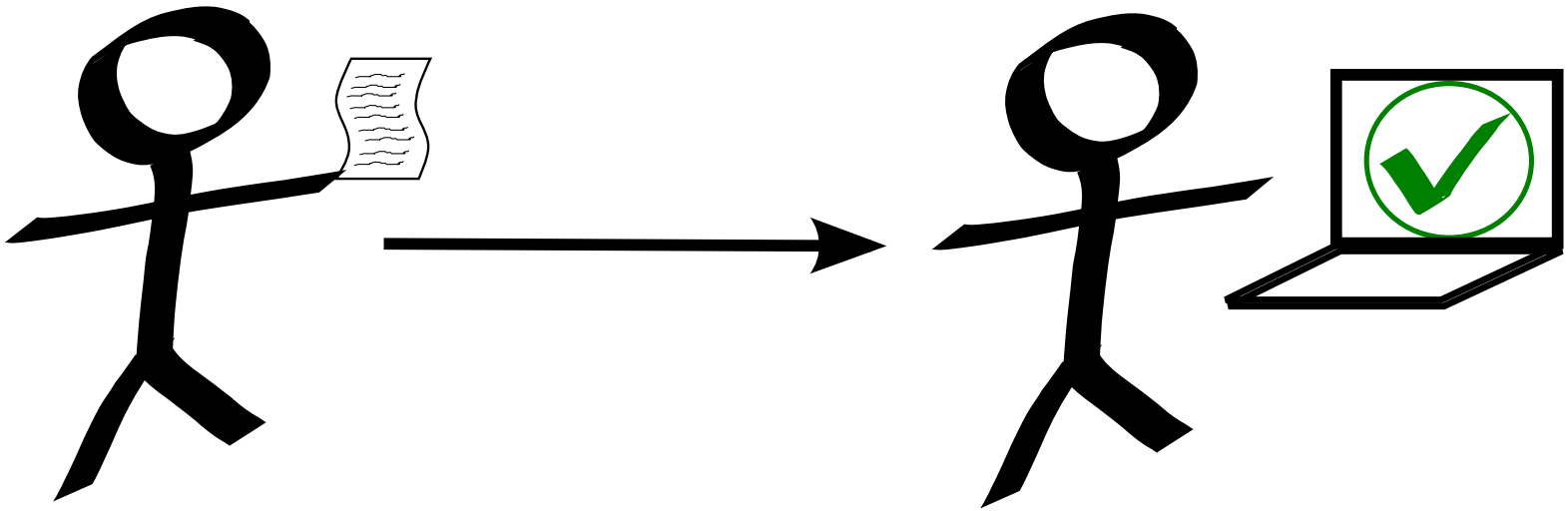
E.g.

$$\frac{t : T \qquad \forall x : T, P(x)}{P(t)}$$

Paper proof



Computer checked proof



Feit-Thompson Theorem

Statement

Finite groups of odd order are solvable

- First proof: Feit and Thompson (1962)

Feit-Thompson Theorem

Statement

Finite groups of odd order are solvable

- First proof: Feit and Thompson (1962)
- Revised:

  Bender and Glauberman (1995)
  Peterfalvi (2000)

Feit-Thompson Theorem

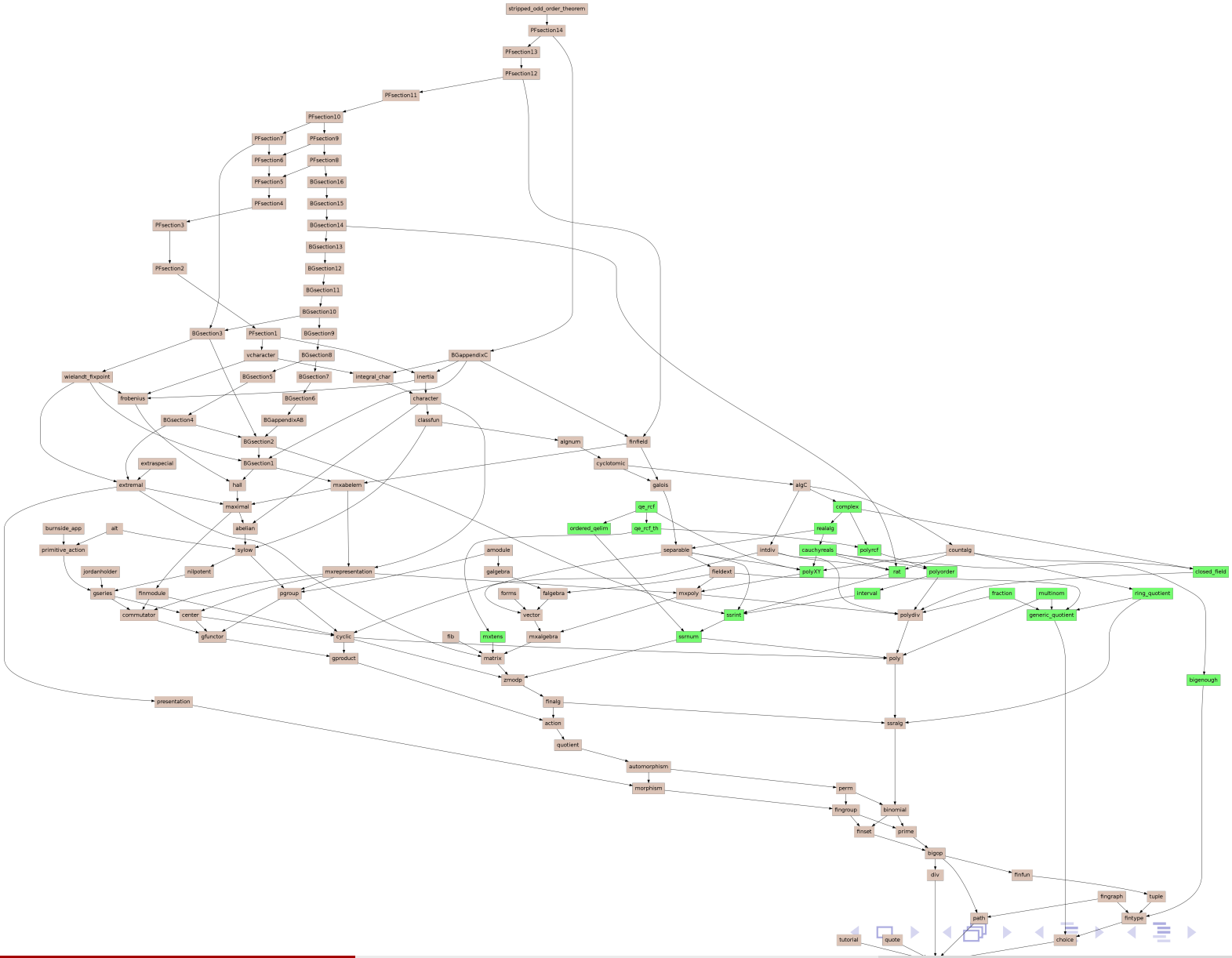
Statement

Finite groups of odd order are solvable

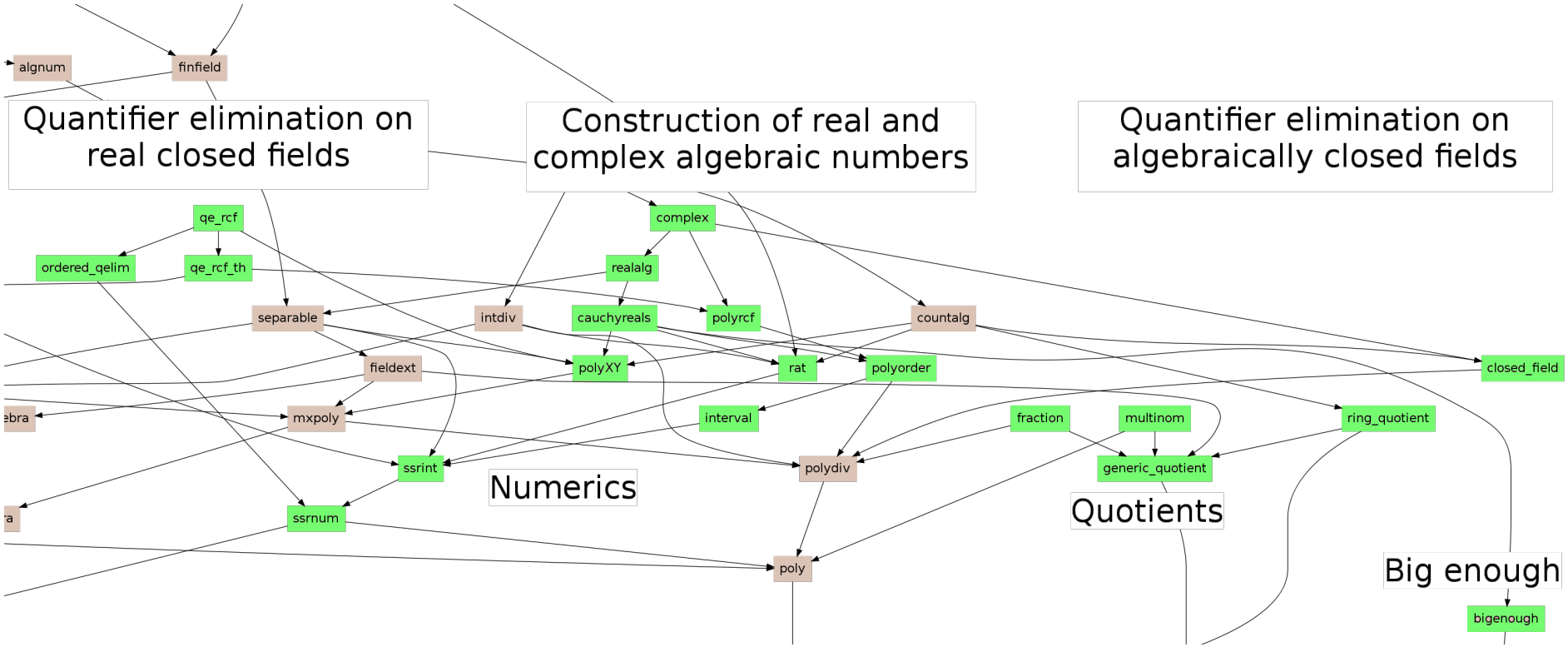
- First proof: Feit and Thompson (1962)
- Revised:

  Bender and Glauberman (1995)
  Peterfalvi (2000)
- Computer checked: Mathematical Components (September 2012)

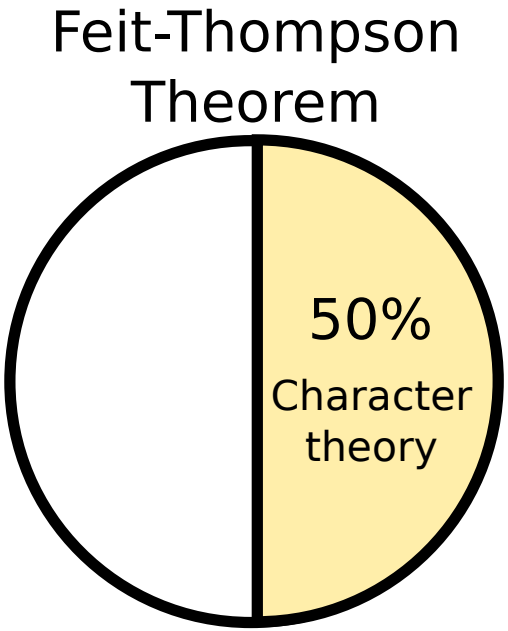
Mathematical Components project files



My contributions to the project



Complex numbers in Feit-Thompson Theorem



$$\chi_g : \mathbb{C}$$

$$\|\chi_g\| : \mathbb{R}$$

$$\|\chi_g\| > \frac{8}{15} > \frac{1}{2}$$

Outline

reals

complex := reals $[i]$

$\Leftrightarrow$ FTA

Outline

algebraic reals

algebraic complex := algebraic reals $[i]$

$\Leftrightarrow$ FTA (Gauss, Laplace, Derksen, CC and Coquand)

Outline

algebraic reals

algebraic complex := algebraic reals $[i]$

$\Leftrightarrow$ FTA (Gauss, Laplace, Derksen, CC and Coquand)

- Factoring the theory of structures with order and norm
- Construction of real algebraic numbers
- The first-order theory of real and algebraic numbers is decidable (through quantifier elimination).

Outline

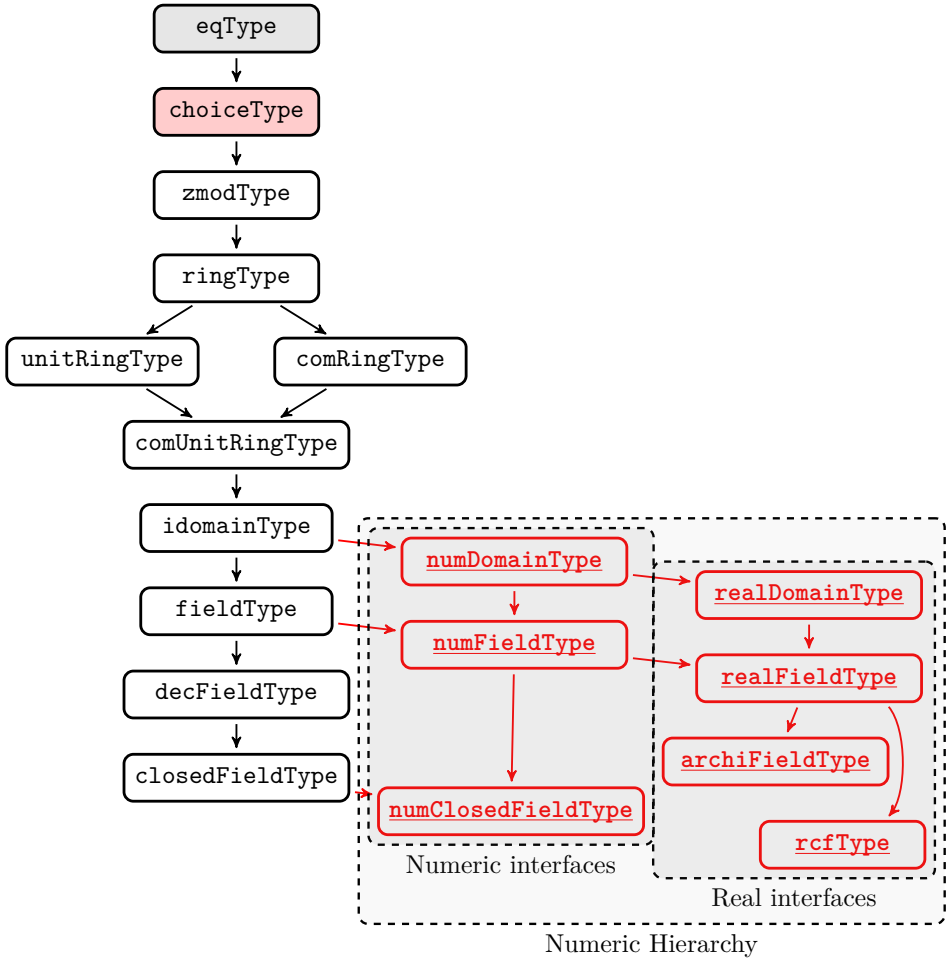
algebraic reals

algebraic complex := algebraic reals $[i]$

$\Leftrightarrow$ FTA (Gauss, Laplace, Derksen, CC and Coquand)

- Factoring the theory of structures with order and norm
- Construction of real algebraic numbers
- The first-order theory of real and algebraic numbers is decidable (through quantifier elimination).

Interfaces


eqType
choiceType
zmodType
ringType
unitRingType
comRingType
comUnitRingType
idomainType
fieldType
decFieldType
closedFieldType
numDomainType
numFieldType
numClosedFieldType
realDomainType
realFieldType
archiFieldType
rcfType
Numeric interfaces
Real interfaces
Numeric Hierarchy

Why these interfaces ?

Goal:

- Factor and organize the theory of numbers from $\mathbb{Z}$ to algebraic numbers.
- Deal with the partial order complex algebraic numbers.

How?

Why these interfaces ?

Goal:

- Factor and organize the theory of numbers from $\mathbb{Z}$ to algebraic numbers.
- Deal with the partial order complex algebraic numbers.

How?

- Reuse the packed class methodolgy (Garillot et al.)
- Based on the norm, not only $\leq$.
- Instances: integers, rationals, real and algebraic numbers.

Outline

algebraic reals

algebraic complex := algebraic reals $[i]$

$\Leftrightarrow$ FTA (Gauss, Laplace, Derksen, CC and Coquand)

- Factoring the theory of structures with order and norm
- Construction of real algebraic numbers
- The first-order theory of real and algebraic numbers is decidable (through quantifier elimination).

What are algebraic numbers?

(Complex) algebraic numbers are

- the **complex** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Real *algebraic numbers* are:

the **real** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Examples:

What are algebraic numbers?

(Complex) algebraic numbers are

- the **complex** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Real *algebraic numbers* are:

the **real** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Examples:

What are algebraic numbers?

(Complex) algebraic numbers are

- the **complex** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Real *algebraic numbers* are:

the **real** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Examples:

- $43, \frac{1}{3}, \sqrt{2}, \sqrt[5]{21}$ are real algebraic numbers

What are algebraic numbers?

(Complex) algebraic numbers are

- the **complex** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Real *algebraic numbers* are:

the **real** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Examples:

- $43, \frac{1}{3}, \sqrt{2}, \sqrt[5]{21}$ are real algebraic numbers
- $i, \sqrt{2} + i\sqrt{5}$ are algebraic

What are algebraic numbers?

(Complex) algebraic numbers are

- the **complex** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Real *algebraic numbers* are:

the **real** *roots of polynomials* with coefficients in $\mathbb{Q}$.

Examples:

- $43, \frac{1}{3}, \sqrt{2}, \sqrt[5]{21}$ are real algebraic numbers
- $i, \sqrt{2} + i\sqrt{5}$ are algebraic
- π and e are not algebraic

Representations of real algebraic numbers

$x \in \mathbb{R}, P \in \mathbb{Q}[X]$

- ✓ operations (reconstruction of polynomial using resultant)
- ✗ countable type

$P \in \mathbb{Q}[X], [a, b]$

- ✗ operations
- ✓ countable type

Construction of real algebraic numbers

Goal:

- A countable type,
- Decidability of atoms ($=$ and $\leq$),
- RCF (intermediate value theorem for polynomials).

How?

Construction of real algebraic numbers

Goal:

- A countable type,
- Decidability of atoms ($=$ and $\leq$),
- RCF (intermediate value theorem for polynomials).

How?

- Both representations
- A formalization of Cauchy reals
- A quotient of type

Construction of real algebraic numbers

Goal:

- A countable type,
- Decidability of atoms ($=$ and $\leq$),
- RCF (intermediate value theorem for polynomials).

How?

- Both representations
- A formalization of Cauchy reals
- A quotient of type

References: C.C., ITP 2012

Cauchy reals

Definition

$$(x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \quad \text{and} \quad \mu_x : \mathbb{Q} \to \mathbb{N}$$

$$\text{such that} \quad \forall \varepsilon > 0, \forall i,\ j \geq \mu_x(\varepsilon), |x_i - x_j| \leq \varepsilon$$

- Formalized just what was needed
- Some $\varepsilon - \delta$ reasoning to formalize

Cauchy reals

Definition

$$(x_n)_{n\in\mathbb{N}} \in \mathbb{Q}^{\mathbb{N}} \quad \text{and} \quad \mu_x : \mathbb{Q} \to \mathbb{N}$$

$$\text{such that} \quad \forall \varepsilon > 0, \forall i,\ j \geq \mu_x(\varepsilon), |x_i - x_j| \leq \varepsilon$$

- Formalized just what was needed
- Some $\varepsilon - N$ reasoning to formalize

Big enough

Example

$$\text{if } x_n \to a \text{ and } y_n \to b, \text{ then } x_n y_n \to ab$$

Suppose $x_n \to a$ and $y_n \to b$.
Let ε be a positive rational. Show

$$|x_n y_n - ab| \leq \varepsilon$$

Big enough

Example

$$\text{if } x_n \to a \text{ and } y_n \to b, \text{ then } x_n y_n \to ab$$

Suppose $x_n \to a$ and $y_n \to b$.
Let ε be a positive rational. Show

$$|x_n y_n - x_n b| + |x_n b - ab| \leq \varepsilon$$

Big enough

Example

$$\text{if } x_n \to a \text{ and } y_n \to b, \text{ then } x_n y_n \to ab$$

Suppose $x_n \to a$ and $y_n \to b$.
Let ε be a positive rational. Show

$$|x_n||y_n - b| + |x_n - a||b| \leq \varepsilon$$

Big enough

Example

$$\text{if } x_n \to a \text{ and } y_n \to b, \text{ then } x_n y_n \to ab$$

Suppose $x_n \to a$ and $y_n \to b$.
Let ε be a positive rational. Show

$$(1 + |a|)|y_n - b| + |x_n - a|(1 + |b|) \leq \varepsilon$$

because

$$|x_n - a| \leq 1$$

Big enough

Example

$$\text{if } x_n \to a \text{ and } y_n \to b, \text{ then } x_n y_n \to ab$$

Suppose $x_n \to a$ and $y_n \to b$.
Let ε be a positive rational. Show

$$|y_n - b| \leq \frac{\varepsilon}{2(1+|a|)} \quad \text{and} \quad |x_n - a| \leq \frac{\varepsilon}{2(1+|b|)}$$

Big enough

Goal:

- Do like in paper proofs.

How?

Usage:

Big enough

Goal:

- Do like in paper proofs.

How?

- Infer the *n a posteriori*.
- Based on Coq existential variables.

Usage:

Big enough

Goal:

- Do like in paper proofs.

How?

- Infer the *n a posteriori*.
- Based on Coq existential variables.

Usage:

- More than 100 occurences in 3163 lines of code.

Quotient types

$$\mathrm{Type}/\equiv \longrightarrow \mathrm{Type}$$

Difficult problem in Constructive TT (Hoffman, Chicli at al., Courtieu).

$\Rightarrow$ We are interested in a particular case.

Particular case for quotienting

Conditions:

- Decidable equivalence.
- Countable type.

Consequence: possibility to select a unique element in each equivalence class.

Theory of quotient types

- Inference.
- Preservation of the ring structure while quotienting by an ideal.

Outline

algebraic reals

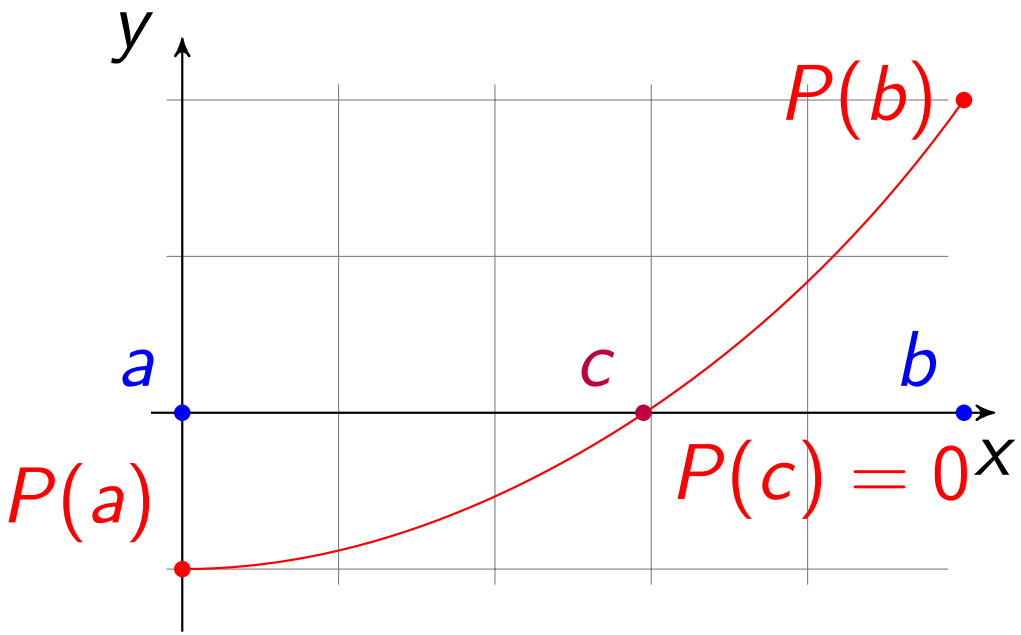
algebraic complex := algebraic reals $[i]$

$\Leftrightarrow$ FTA (Gauss, Laplace, Derksen, CC and Coquand)

- Factoring the theory of structures with order and norm
- Construction of real algebraic numbers
- The first-order theory of real and algebraic numbers is decidable (through quantifier elimination).

Definition of Real Closed Field

Field + order + intermediate value property for polynomials

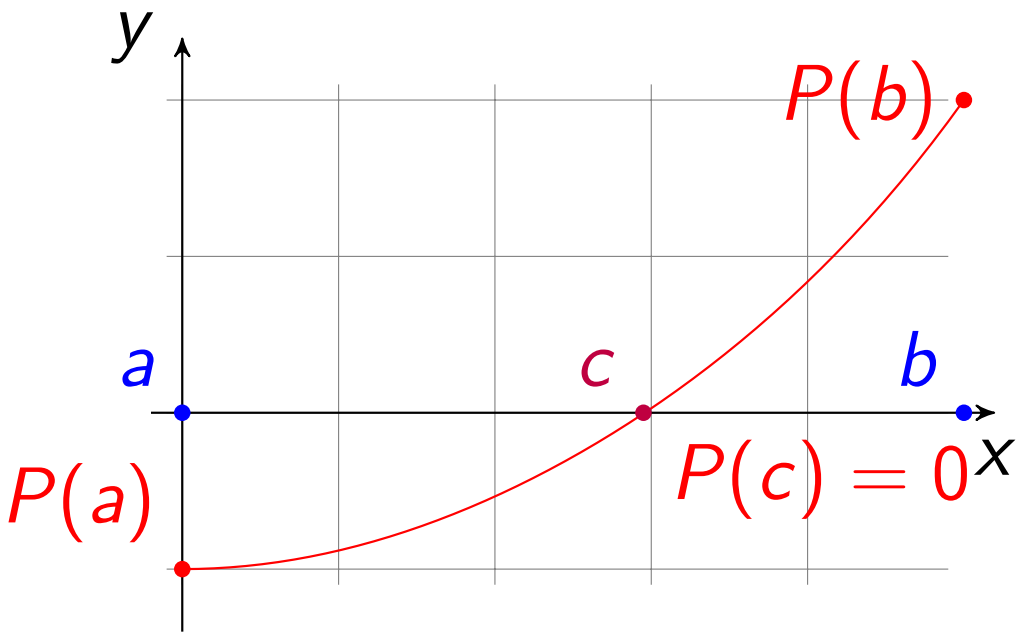


Real algebraic numbers form a real closed field

Real algebraic numbers **implement** the interface of real closed field

Definition of Real Closed Field

Field + order + intermediate value property for polynomials



Real algebraic numbers form a real closed field

Real algebraic numbers **implement** the interface of real closed field

The theory of Real Closed Fields

- Rolle, MVT, ...
- Infrastructure for intervals (membership, inclusion, splitting, ...)
- Neighborhoods

Classical reasoning on Real Closed Fields

- Decidability of the atoms ($=$ and $\leq$)

$\Rightarrow$ Decidability of simple formulas

Classical reasoning on Real Closed Fields

- Decidability of the atoms ($=$ and $\leq$)

$\Rightarrow$ Decidability of simple formulas

- In the litterature, case reasoning on arbitrary formula. e.g. $\exists x, P(x) = 0$.

$\Rightarrow$ Classical reasoning

Classical reasoning on Real Closed Fields

- Decidability of the atoms ($=$ and $\leq$)

$\Rightarrow$ Decidability of simple formulas

- In the litterature, case reasoning on arbitrary formula. e.g. $\exists x, P(x) = 0$.

$\Rightarrow$ Classical reasoning

- Unless we can decide the validity of formulas

Quantifier elimination on real closed fields

Tarski (1948)

The first-order theory of real closed fields enjoys quantifier elimination.

Consequences:

- We can decide whether first-order formulas are valid.
- We can perform case analysis on quantifier formulas.

An example

```
R : rcfType
a : R
b : R
c : R
...
=======================
exists x, a * x ^ 2 + b * x + c = 0
```

An example

```
R : rcfType
a : R
b : R
c : R
...
======================
exists x, a * x ^ 2 + b * x + c = 0
```

- Prove the conclusion

An example

```
R : rcfType
a : R
b : R
c : R
...
======================
exists x, a * x ^ 2 + b * x + c = 0
```

- Prove the conclusion
- Provide the witness for `x`

An example

```
R : rcfType
a : R
b : R
c : R
...
=======================
exists x, a * x ^ 2 + b * x + c = 0
```

- Prove the conclusion
- Eliminate the quantifier

An example (continued)

```
R : rcfType
a : R
b : R
c : R
...
======================
0 <= b ^ 2 - 4 * a * c
```

On Quantifier Elimination in Coq

Goal:

- Case reasoning on first-order formulas for ACF and RCF.

How?

- Deep embedding of first-order logic for RCF and ACF.
- Implement QE procedures and their formal proof.

References: CC and Mahboubi (Calculemus 2010, LMCS 2012).

Conclusion

New infrastructures in Mathematical Components:

- Interface design (Numerics)
- Tools to mechanize tasks (Big enough, intervals, quotients)

Conclusion

New infrastructures in Mathematical Components:

- Interface design (Numerics)
- Tools to mechanize tasks (Big enough, intervals, quotients)

With good infrastructure, fast formalizations:

- Construction of real algebraic numbers (2 weeks)
- Formalization of FTA (2 days)
- Programming and certification of QE on ACF and RCF

Conclusion

New infrastructures in Mathematical Components:

- Interface design (Numerics)
- Tools to mechanize tasks (Big enough, intervals, quotients)

With good infrastructure, fast formalizations:

- Construction of real algebraic numbers (2 weeks)
- Formalization of FTA (2 days)
- Programming and certification of QE on ACF and RCF

Good integration of the tools and the formalizations in the proof of Feit-Thompson Theorem.

Perspectives

- Generalize big enough numbers.
- Providing efficient implementations. Efficient algorithm are proved using naive ones.

$\Rightarrow$ application to fast real algebraic numbers

- An algebraic hierarchy based on types which admit uniqueness of identity proofs.
- Certifying the Cylindrical Algebraic Decomposition.

The end

Thank you for your attention.