Toward a new formalization of real numbers

Catherine Lelay

Institute for Advanced Sciences

September 24, 2015

Toward a new formalization of real numbers in Coq using Univalent Foundations

Catherine Lelay

Institute for Advanced Sciences

September 24, 2015

What is Formal Proof?

Formal proof

A formal proof is a proof written in a language precise enough to be checked by a computer.

What is Formal Proof?

Formal proof

A formal proof is a proof written in a language precise enough to be checked by a computer.

Proof assistant

Software for writing and verifying formal proofs.
Examples: ACL2, Coq, HOL Light, Isabelle HOL, Mizar, PVS

What is Formal Proof?

Formal proof

A formal proof is a proof written in a language precise enough to be checked by a computer.

Proof assistant

Software for writing and verifying formal proofs.
Examples: ACL2, Coq, HOL Light, Isabelle HOL, Mizar, PVS

+ guaranteed result

What is Formal Proof?

Formal proof

A formal proof is a proof written in a language precise enough to be checked by a computer.

Proof assistant

Software for writing and verifying formal proofs.
Examples: ACL2, Coq, HOL Light, Isabelle HOL, Mizar, PVS

+ guaranteed result
− tedious process

What is Formal Proof?

Formal proof

A formal proof is a proof written in a language precise enough to be checked by a computer.

Proof assistant

Software for writing and verifying formal proofs.
Examples: ACL2, Coq, HOL Light, Isabelle HOL, Mizar, PVS

- \+ guaranteed result
- − tedious process

Definition of $\mathbb{R}$

Definition

The set of real numbers $\mathbb{R}$ is :

- a non-trivial abelian field
- totally ordered
- archimedean
- complete

Definition of $\mathbb{R}$

Definition

The set of real numbers $\mathbb{R}$ is :

- a non-trivial abelian field
- totally ordered
- archimedean
- complete

In proof assistants, $\mathbb{R}$ can be:

- Axiomatic (Coq standard library, PVS)
- Constructive
  - Cauchy sequences (C-CoRN/MathClasses, Isabelle/HOL)
  - Dedekind cuts (HOL4, Mizar)

Definition of $\mathbb{R}$

Definition

The set of real numbers $\mathbb{R}$ is :

- a non-trivial abelian field
- totally ordered
- archimedean
- complete

In proof assistants, $\mathbb{R}$ can be:

- Axiomatic (Coq standard library, PVS)
- Constructive
  - Cauchy sequences (C-CoRN/MathClasses, Isabelle/HOL)
  - Dedekind cuts (HOL4, Mizar)

Definition of $\mathbb{R}$

Definition

The set of real numbers $\mathbb{R}$ is :

- a non-trivial abelian field
- totally ordered
- archimedean
- complete

In proof assistants, $\mathbb{R}$ can be:

- Axiomatic (Coq standard library, PVS)
- Constructive
  - Cauchy sequences (C-CoRN/MathClasses, Isabelle/HOL)
  - Dedekind cuts (HOL4, Mizar)

Definition of $\mathbb{R}$

Definition

The set of real numbers $\mathbb{R}$ is :

- a non-trivial abelian field
- totally ordered
- archimedean
- complete

In proof assistants, $\mathbb{R}$ can be:

- Axiomatic (Coq standard library, PVS)
- Constructive
  - Cauchy sequences (C-CoRN/MathClasses, Isabelle/HOL)
  - Dedekind cuts (HOL4, Mizar)

Definition of $\mathbb{R}$

Definition

The set of real numbers $\mathbb{R}$ is :

- a non-trivial abelian field
- totally ordered
- archimedean
- complete

In proof assistants, $\mathbb{R}$ can be:

- Axiomatic (Coq standard library, PVS)
- Constructive
  - Cauchy sequences (C-CoRN/MathClasses, Isabelle/HOL)
  - Dedekind cuts (HOL4, Mizar)

Real numbers in Coq

- Reals (Coq standard library)

- C-CoRN/MathClasses

Real numbers in Coq

- Reals (Coq standard library)
  - Axioms
  - User-friendly library of real analysis about total functions (adding Coquelicot)
  - Proofs cannot be extracted as programs
- C-CoRN/MathClasses

Real numbers in Coq

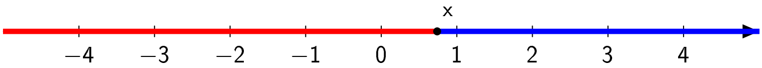
- Reals (Coq standard library)
  - Axioms
  - User-friendly library of real analysis about total functions (adding Coquelicot)
  - Proofs cannot be extracted as programs
- C-CoRN/MathClasses
  - Cauchy sequences
  - Good library of real analysis about total and partial functions
  - Not easy to use

Real numbers in Coq

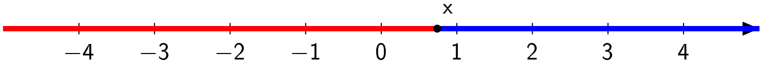
- Reals (Coq standard library)
  - Axioms
  - User-friendly library of real analysis about total functions (adding Coquelicot)
  - Proofs cannot be extracted as programs
- C-CoRN/MathClasses
  - Cauchy sequences
  - Good library of real analysis about total and partial functions
  - Not easy to use

Goal: Build a new library based on Dedekind cuts

Definition of Dedekind cuts



Definition of Dedekind cuts



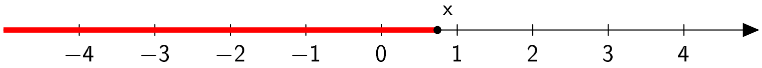
Definition (Dedekind cut)

$(L, U) \subseteq \mathbb{Q} \times \mathbb{Q}$ where :

- $\exists x \in L$, $\exists y \in U$, and $L \cap U = \varnothing$,
- $\forall x \in L, \forall y \in \mathbb{Q}, y < x \Rightarrow y \in L$,
- $\forall x \in L, \exists y \in \mathbb{Q}, x < y \wedge y \in L$,
- $\forall x \in U, \forall y \in \mathbb{Q}, x < y \Rightarrow y \in U$,
- $\forall x \in U, \exists y \in \mathbb{Q}, y < x \wedge y \in U$,
- $\forall (r, x, y) \in \mathbb{Q}^3, x < r < y \Rightarrow x \in L \vee y \in U$.

$$\mathbb{R} = \{\text{Dedekind cuts}\}$$

A second definition of Dedekind cuts



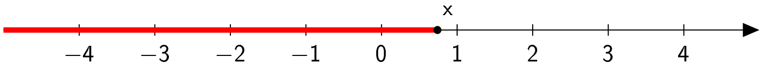
Definition (Dedekind cut)

$L \subseteq \mathbb{Q}$ where :

- $\exists x \in L$,
- $\exists M \in \mathbb{Q}, \forall x \in L, x \leq M$,
- $\forall x \in L, \forall y \in \mathbb{Q}, y < x \Rightarrow y \in L$,
- $\forall x \in L, \exists y \in \mathbb{Q}, x < y \wedge y \in L$.

$$\mathbb{R} = \{\text{Dedekind cuts}\}$$

A second definition of Dedekind cuts



Definition (Dedekind cut)

$L \subseteq \mathbb{Q}$ where :

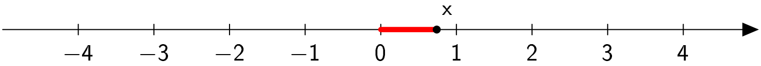
- $\exists x \in L$,
- $\exists M \in \mathbb{Q}, \forall x \in L, x \leq M$,
- $\forall x \in L, \forall y \in \mathbb{Q}, y < x \Rightarrow y \in L$,
- $\forall x \in L, \exists y \in \mathbb{Q}, x < y \wedge y \in L$.

$$\mathbb{R} = \{\text{Dedekind cuts}\}$$

$\oplus$ Easier to define

$\ominus$ Difficulties to define multiplication

A better definition of Dedekind cuts



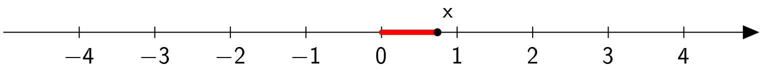
Definition (Dedekind cut)

$L \subseteq \{r \in \mathbb{Q} \mid 0 \leq r\}$ where :

- $\exists M \in \mathbb{Q}, \forall x \in L, x \leq M$,
- $\forall x \in L, \forall y \in \mathbb{Q}, 0 \leq y < x \Rightarrow y \in L$,
- $\forall x \in L, \exists y \in \mathbb{Q}, x < y \wedge y \in L$.

$$\begin{aligned} [0; +\infty) &= \{\text{Dedekind cuts}\} \\ \mathbb{R} &= ([0; +\infty) \times [0; +\infty)) \,/ \approx \end{aligned}$$

A better definition of Dedekind cuts



Definition (Dedekind cut)

$L \subseteq \{r \in \mathbb{Q} \mid 0 \leq r\}$ where :

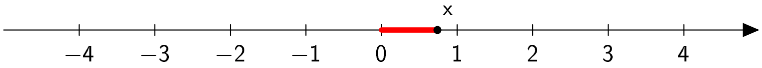
- $\exists M \in \mathbb{Q}, \forall x \in L, x \leq M,$
- $\forall x \in L, \forall y \in \mathbb{Q}, 0 \leq y < x \Rightarrow y \in L,$
- $\forall x \in L, \exists y \in \mathbb{Q}, x < y \wedge y \in L.$

$$
\begin{aligned}
[0; +\infty) &= \{\text{Dedekind cuts}\} \\
\mathbb{R} &= ([0; +\infty) \times [0; +\infty)) \,/ \approx
\end{aligned}
$$

$\oplus$ Easier to define

$\oplus$ Good definitions for operations

A better definition of Dedekind cuts



Definition (Dedekind cut)

$L \subseteq \{r \in \mathbb{Q} \mid 0 \leq r\}$ where :

- $\exists M \in \mathbb{Q}, \forall x \in L, x \leq M$,
- $\forall x \in L, \forall y \in \mathbb{Q}, 0 \leq y < x \Rightarrow y \in L$,
- $\forall x \in L, \exists y \in \mathbb{Q}, x < y \wedge y \in L$.

$$\begin{aligned} [0; +\infty) &= \{\text{Dedekind cuts}\} \\ \mathbb{R} &= ([0; +\infty) \times [0; +\infty)) \,/ \approx \end{aligned}$$

⊕ Easier to define

⊕ Good definitions for operations

? Quotients in Coq proof assistant

UniMath

A Coq library which aim to formalize a substantial body of mathematics using the univalent point of view.

UniMath website

UniMath

> A Coq library which aim to formalize a substantial body of mathematics using the univalent point of view.
>
> *UniMath website*

- Extension of the underlying theory of Coq
- Univalent point of view allow a few classical constructions in Coq which are previously impossible (or realy hard)

UniMath

A Coq library which aim to formalize a substantial body of mathematics using the univalent point of view.

UniMath website

- Extension of the underlying theory of Coq
- Univalent point of view allow a few classical constructions in Coq which are previously impossible (or realy hard)

For my work:

- New board
- Work with conceptors

Toward a new formalization of real numbers

$$\boxed{\begin{array}{c}\mathbb{R}^+ = [0; +\infty) \\ 0, 1, +, \times, \cdot^{-1}\end{array}}$$

$$\downarrow$$

$$\boxed{\begin{array}{c}\mathbb{R} = (\mathbb{R}^+ \times \mathbb{R}^+)/\approx \\ 0, 1, +, -, \times, \cdot^{-1}\end{array}}$$

To go further: real analysis