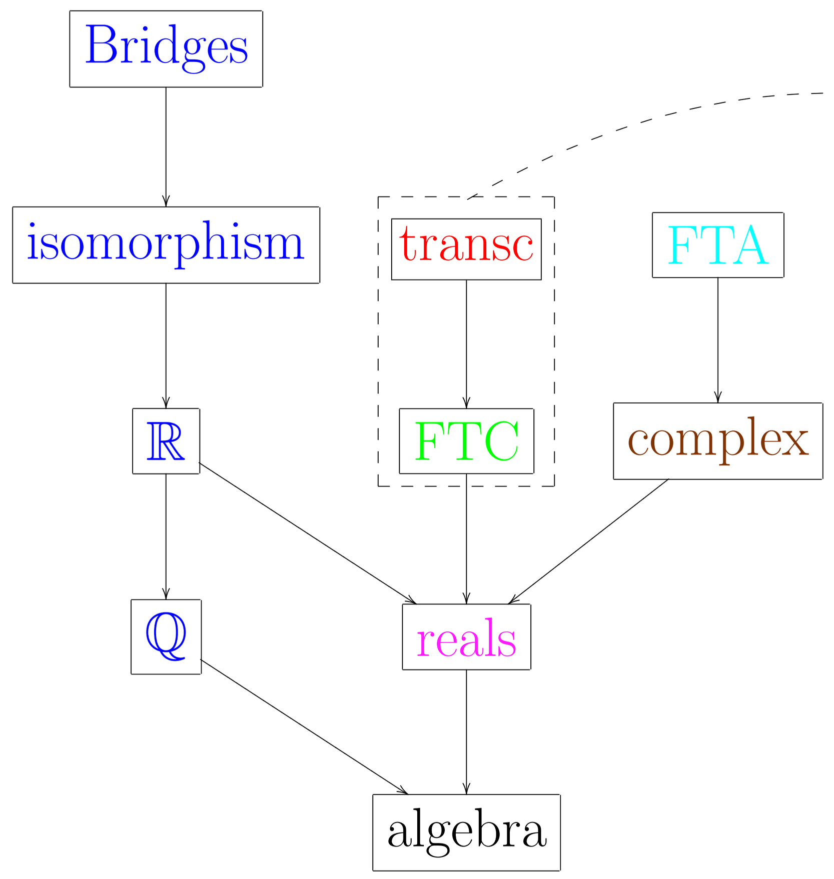
A Constructive Formalization of Real Analysis in `Coq`

Luís Cruz-Filipe (University of Nijmegen)

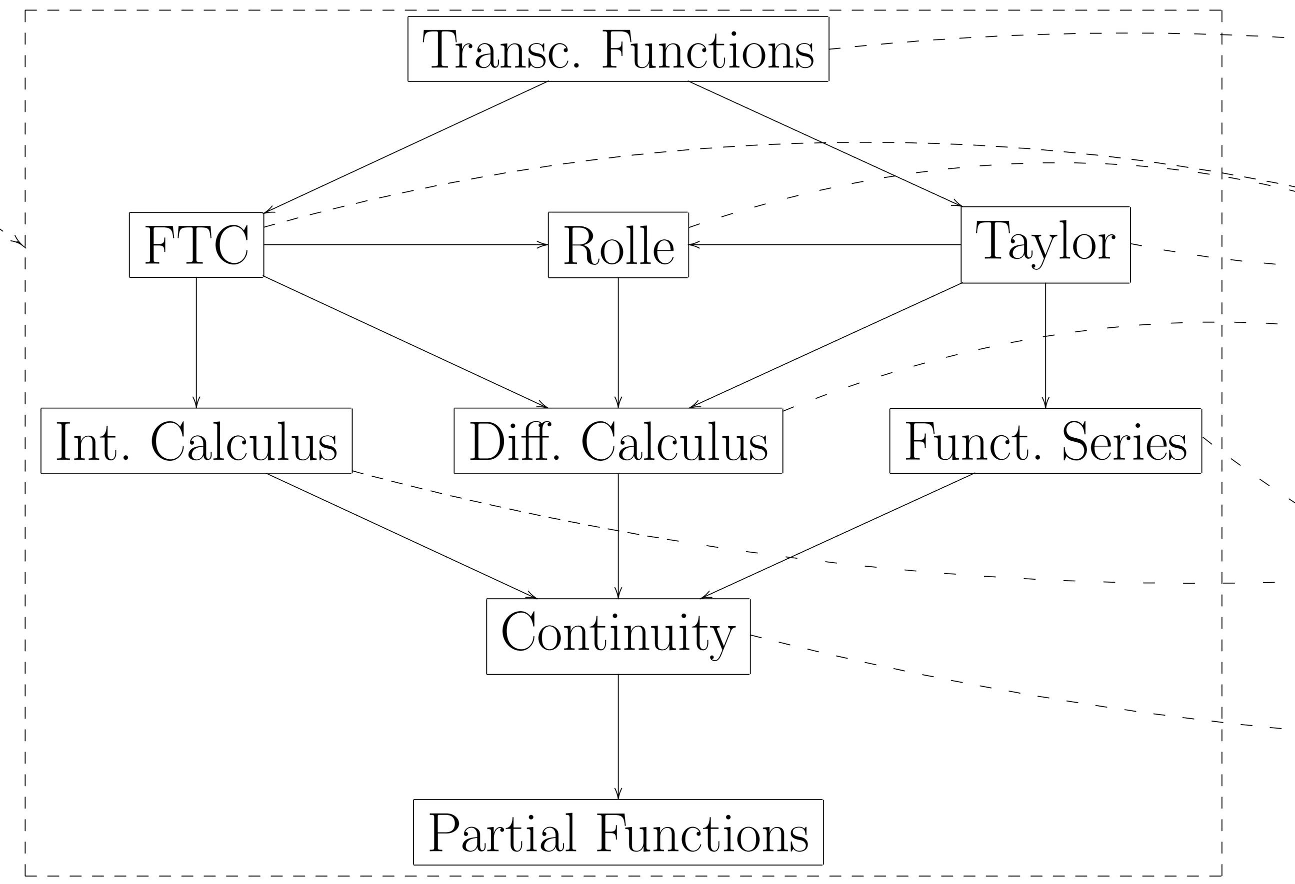
`lcf@cs.kun.nl`

The formalization contains:

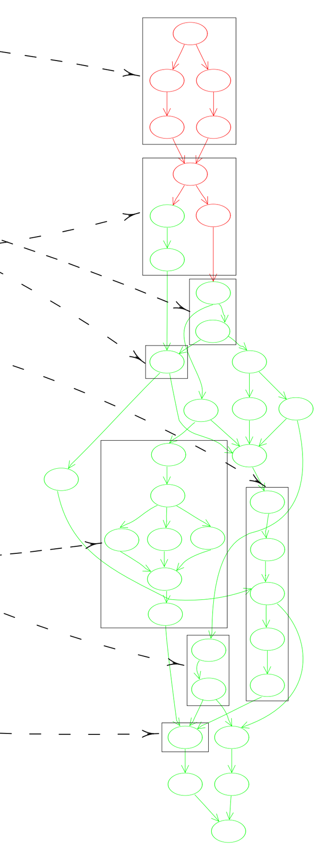
- definition of the necessary concepts;
- statement and proof of technical lemmas and useful theorems alike;
- development of automation strategies ("*tactics*") which can help to (partially) solve goals, i.e., build (parts of) proofs;
- documentation of all the work, both at the mathematical level (discussion of alternative definitions and statements and proofs of theorems) and at the technical level.



Contents of the main library and where the FTC fits in



The main topics in the formalization of the FTC and their inter-dependencies



Tree structure of the files in the formalization of the FTC

Partial Functions

We model a partial function $f : \mathbb{R} \not\to \mathbb{R}$ with domain characterized by a predicate P as a λ-term F of type $(\Pi x:\mathbb{R})(\Pi H_x : P(x))\mathbb{R}$; that is, as a binary function whose second argument is a proof term. They are required to meet the conditions

$$\forall_{x:\mathbb{R}}\forall_{H,H':P(x)}F(x,H) = F(x,H') \ ,$$

known as *proof irrelevance*, which allows us to write simply $F(x)$; and

$$\forall_{x,y:\mathbb{R}}(x = y) \Rightarrow (F(x) = F(y)) \ .$$

Using this definition and the library of real numbers developed at the University of Nijmegen, we formalized a constructive proof of the Fundamental Theorem of Calculus (FTC). Some of the main steps in the formalization are presented here.

The Fundamental Theorem of Calculus

If f is a continuous function with a primitive F, then integrals of f can be evaluated according to the rule

$$\int_a^b f(x)dx = F(b) - F(a) \ .$$

This equality is valid both classically and constructively.

Rolle's Theorem

Given $a, b \in \mathbb{R}$ such that $a \leq b$ and $f(a) = f(b)$, we can prove classically that

$$\exists_{x\in[a,b]}f'(x) = 0 \ ;$$

constructively, we can only prove the (weaker) condition

$$\forall_{\varepsilon>0}\exists_{x\in[a,b]}|f'(x)| \leq \varepsilon \ .$$

As a corollary, we get the result known as the *Mean Law*, which given a, b classically states that

$$\exists_{x\in[a,b]}\frac{f(b) - f(a)}{b - a} = f'(x) \ ;$$

constructively, it states that

$$\forall_{\varepsilon>0}\exists_{x\in[a,b]}|f(b) - f(a) - f'(x)(b - a)| \leq \varepsilon \ .$$

The Mean Law is an approximation theorem; in it, the value of x is unknown. Therefore, in practice both formulations will yield similar results.

Taylor's Theorem

If f is $n + 1$ times differentiable, then we can approximate f by a polynomial in terms of the derivatives of f; the estimate for the error is classically given by

$$\exists_{y\in I}f(x) - \sum_{i=0}^{n}\frac{f^{(i)}(x_0)}{i!}(x - x_0)^i = \frac{f^{(n+1)}(y)}{(n+1)!}(x - y)^{n+1} \ .$$

Constructively, we can only establish the weaker result

$$\forall_{\varepsilon>0}\exists_{y\in I}\left|f(x) - \sum_{i=0}^{n}\frac{f^{(i)}(x_0)}{i!}(x - x_0)^i - \frac{f^{(n+1)}(y)}{(n+1)!}(x - y)^{n+1}\right| \leq \varepsilon$$

This is also an approximation theorem. In practice, both formulations allow for the same results; also, both can be used to prove existence and uniqueness of solutions to some kinds of differential equations.