Formalizing Real Calculus in `Coq`

Luís Cruz-Filipe

University of Nijmegen, The Netherlands

Centro de Lógica e Computação, Portugal

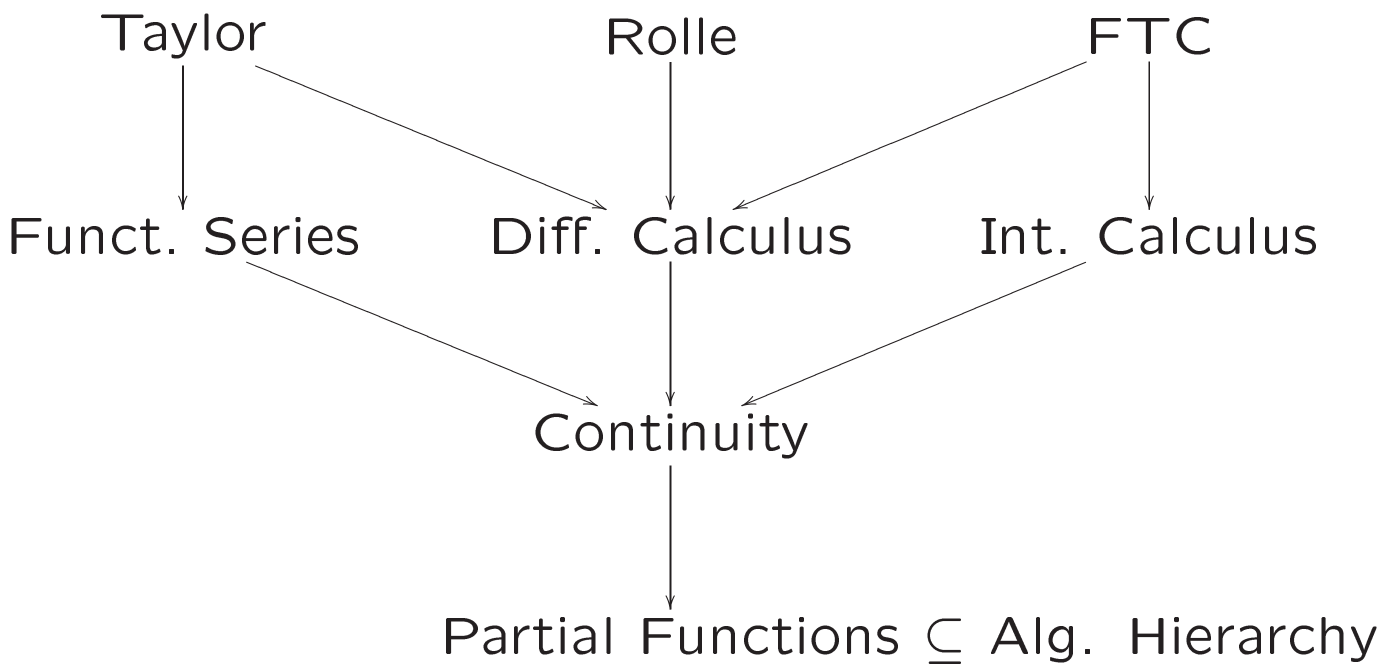
Overview

1. Introduction
2. Overview of the Formalization
3. Constructive Issues
4. Partial Functions
5. Example
6. Conclusions

The Algebraic Hierarchy in the FTA Project

	$\mathbb{C}$
$\vert\cdot\vert$, series	$\mathbb{R}$
$<, \leq$	OrdFields
$/$	Fields
$*, 1$	Rings
$-, \sum$	Groups
0	Monoids
$+$	SemiGroups
$\circ$	Setoids

The Library of Real Analysis



Some Statistics

Subject	# files	Script*(kb)	Compiled (kb)
Continuity	1	33,2	615
Diff. Calculus	6	102,2	2.910
Int. Calculus	8	222,8	12.398
Funct. Series	4	101,6	1.626
Rolle	1	19,5	1.998
Taylor	2	35,4	3.642
FTC	1	17,9	173
Other†	7	105,7	2.802
Total	30	638,3	25 Mb

*includes documentation

†includes tactics

Some Constructive Issues...

- Intuitionistic Logic (proofs are algorithms):
  - $\nvdash A \vee \neg A$;
  - $\nvdash \neg\neg A \rightarrow A$.
- No decidable equality:
  - Basic semi-decidable "apartness" $\#$;
  - $a = b$ iff $\neg(a\#b)$.
- Irrelevance of point-wise concepts;
- "Unfolding" of equivalent definitions.

Partial Functions

How to represent $f : \mathbb{R} \not\to \mathbb{R}$?

A partial function is a pair $F = \langle P, f \rangle$ where

- $P : \mathbb{R} \to \mathtt{P}rop$;
- $f : (\Pi x : \mathbb{R})(\Pi H : Px)\mathbb{R}$;

such that

$$\forall_{x,y:\mathbb{R}} \forall_{Hx:Px} \forall_{Hy:Py}\ f(x, Hx) \# f(y, Hy) \to x \# y$$

(strong extensionality)

Partial Functions (continued)

Consequences of this definition:

- $f(x, H) = f(x, H')$ for all $H, H' : Px$ (proof irrelevance);

- if $x = y$ then $f(x) = f(y)$.

Notation: in Coq, we denote $f(x, H)$ by the term `(F[@]x H)`, visually conveying the idea that the proof term plays no relevant role in the computation.

Example

Consider the following

Theorem: Let f be a function such that $f' = 0$ on a proper interval I. Then f is constant.

Proof: Let $x_0 \in I$; by the mean-value theorem, for any positive ε and every $x \in I$ there is a point y between x_0 and x such that

$$|f(x_0) - f(x) - f'(y)(x_0 - x)| \leq \varepsilon.$$

In other words, $|f(x_0) - f(x)|$ is smaller than any positive number, hence it must be zero.

Example (continued)

The Coq script for this proof reads as follows:

```
Lemma FConst_prop : (J:interval)(pJ:(proper J))
  (F':PartIR)(Derivative J pJ F' {-C-}Zero)->
    {c:IR & (Feq (iprop J) F' {-C-}c)}.
Intros.
Elim (nonvoid_point J (proper_nonvoid J pJ)); Intros x0 Hx0.
Exists (F'[@]x0 (Derivative_imp_inc ???? H x0 Hx0)).
FEQ.
Simpl; Simpl in Hx'.
Apply cg_inv_unique_2.
Apply abs_approach_zero; Intros.
Elim (Mean_Law J pJ F' {-C-}Zero H x0 x Hx0 H0 e H1).
Intros y Hy; Inversion_clear Hy.
Simpl in H3.
Apply leEq_wdl with
  (AbsIR ((F'[@]x Hx)[-](F'[@]x0 (Derivative_imp_inc ???? H ? Hx0)))
    [-]Zero[*](x[-]x0)).
Apply H3; Auto.
Apply abs_wdIR; Rational.
Qed.
```