The Fundamental Theorem of Calculus in Coq

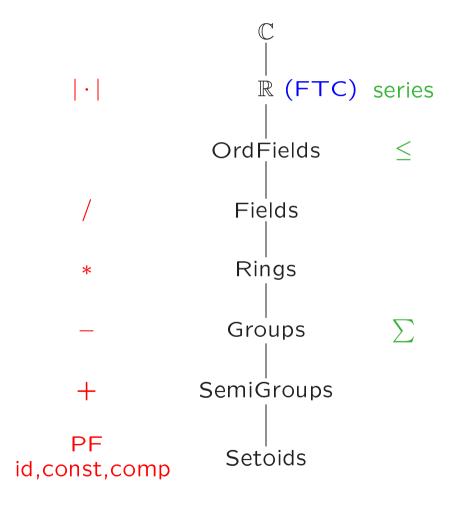
Luís Cruz-Filipe

University of Nijmegen, The Netherlands Centro de Lógica e Computação, Portugal

Overview

- 1. Introduction
- 2. Extending the FTA library
- 3. Partial functions
- 4. Consequences of constructivism
- 5. Domain-specific tactics
- 6. Conclusions

The Algebraic Hierarchy



Partial Functions

Let f be a partial function from A to B and x be an element of A.

In order to apply f to x we need to know that x is in the domain of f.

$$P(x) \stackrel{\mathsf{def}}{\Leftrightarrow} x \in \mathsf{dom}(f)$$

We can identify f with a total function from $\{x \in A : P(x)\}$ to B.

```
Record PartFunct : Type :=
  {pfpred : S->Set;
   pfprwd : (pred_well_def S predG);
   pfpfun : (Build_SubCSetoid S P)->S}
given
  f : PartFunct
  x : S
  H : (pfpred f x)
f(x) is represented by (pfpfun f (Build_subcsetoid_crr S P x H))
```

Advantages:

• Intuitive definition

• Strongly extensional, well defined

Shortcomings:

- Unnatural mixing up between setoid elements and proofs
- Expensive simplification procedure

```
Record PartFunct : Type :=
  {pfpred : S->Set;
   pfprwd : (pred_well_def S predG);
  pfpfun : (x:S)(predG x) -> S;
   pfstrx : (x,y:S)(Hx:(predG x))(Hy:(predG y))
             (((partG x Hx)[#](partG y Hy)) -> (x[#]y)).
given
  f : PartFunct
  x : S
  H : (pfpred f x)
f(x) is represented by (pfpfun f x H)
```

Advantages:

- More efficient
- Proofs are kept separate from setoid elements
- More suited to automation

Shortcomings:

• Duplicates the notion of setoid function

Constructive approach to analysis

- No pointwise concepts
- Some differences in statements of definitions/theorems
- Many differences in proofs

Derivative

Classically:

$$f'(x) = \lim_{y \to x} \frac{f(y) - f(x)}{y - x}$$

or, equivalently,

$$\forall_{\varepsilon>0}\exists_{\delta>0}\forall_y |x-y|<\delta \Rightarrow \left|\frac{f(y)-f(x)}{y-x}-f'(x)\right|<\varepsilon$$

Constructively:

$$\forall_{\varepsilon>0}\exists_{\delta>0}\forall_y |x-y| \leq \delta \Rightarrow |f(y)-f(x)-f'(x)(y-x)| \leq \varepsilon |y-x|$$

Rolle's Theorem:

Classically:

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

Constructively:

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

Taylor's Theorem

$$f(x) = \sum_{k=0}^{n} \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k + R(x)$$

Classically:

$$R(x) = \frac{f^{(n+1)}(c)}{(n+1)!} (x - x_0)^{n+1}$$

Constructively:

$$R(x) \approx \frac{f^{(n+1)}(c)}{n!} (x-c)^n (x-x_0)$$

Tactics

Typical goals:

- ullet $X\subseteq Y$, where typically Y is the domain of some function Auto with Hints
- f is continuous

 Auto with Hints
- f' = gAuto with Hints is not enough

$$f(x) = 3x + 4, \quad g(x) = 3$$

Reflection

• Inductive type symbPF

• Interpretation function $[\![\cdot]\!]$:symbPF \to $[\mathbb{R} \to \mathbb{R}]$

Symbolic derivation ':symbPF→symbPF

• Lemma: for all symbolic f, [f'] = [f]'

Tactic

Given f and g:

- Build s such that [s] = f Easy
- (Try to) prove that [s] = f Usually easy
- (Try to) prove that [s'] = g Not trivial!
- Apply the lemma