Coq with power series

Guillaume Allais

COQTAIL Junior Laboratory
ENS Lyon

July, 31st

Why? - COQTAIL

- We wanted to:
  - Tackle undergraduate programs
  - Prove nice results
  - Produce clean and reusable libraries
- We needed:
  - Good libraries
  - Good tactics

Why? - COQTAIL

- We wanted to:
  - Tackle undergraduate programs
  - Prove nice results
  - Produce clean and reusable libraries
- We needed:
  - Good libraries $\Rightarrow$ `Rsequence` (Pédrot)
  - Good tactics

Why? - Rpser

```
Definition cos_n (n:nat) : R :=
  (-1) ^ n / INR (fact (2 * n)).
```

Why? - Rpser

```
Definition cos_n (n:nat) : R :=
  (-1) ^ n / INR (fact (2 * n)).

Definition cos_in (x l:R) : Prop :=
  infinite_sum (fun i:nat => cos_n i * x ^ i) l.
```

Why? - Rpser

```
Definition cos_n (n:nat) : R :=
  (-1) ^ n / INR (fact (2 * n)).

Definition cos_in (x l:R) : Prop :=
  infinite_sum (fun i:nat => cos_n i * x ^ i) l.

Lemma exist_cos : forall x:R, { l:R | cos_in x l }.
```

Why? - `Rpser`

```
Definition cos_n (n:nat) : R :=
  (-1) ^ n / INR (fact (2 * n)).

Definition cos_in (x l:R) : Prop :=
  infinite_sum (fun i:nat => cos_n i * x ^ i) l.

Lemma exist_cos : forall x:R, { l:R | cos_in x l }.

Definition cos (x:R) : R := let (a,_) :=
  exist_cos (Rsqr x) in a.
```

Why? - Rpser

```
Definition cos_n (n:nat) : R :=
  (-1) ^ n / INR (fact (2 * n)).

Definition cos_in (x l:R) : Prop :=
  infinite_sum (fun i:nat => cos_n i * x ^ i) l.

Lemma exist_cos : forall x:R, { l:R | cos_in x l }.

Definition cos (x:R) : R := let (a,_) :=
  exist_cos (Rsqr x) in a.
```

But cos is much more than just a series!

Defining power series

- Convergence disk
  - Convergence radius
  - Criterion
- Sums
  - Abel's lemma
  - Compatibility with common operations
  - Formal derivatives

Convergence radius

- The usual definition

$$\rho\left(\sum_{n\in\mathbb{N}} a_n x^n\right) = \sup\left\{r \in \mathbb{R} \mid \text{the sequence } \left|a_n r^n\right| \text{ is bounded}\right\}$$

Convergence radius

- The usual definition

$$\rho\left(\sum_{n\in\mathbb{N}} a_n x^n\right) = \sup\left\{r \in \mathbb{R} \mid \text{the sequence } \left|a_n r^n\right| \text{ is bounded}\right\}$$

- But being a lub is not really informative!

Convergence radius

- The usual definition

$$\rho\left(\sum_{n\in\mathbb{N}} a_n x^n\right) = \textcolor{red}{\sup}\left\{r \in \mathbb{R} \mid \text{the sequence } \left|a_n r^n\right| \text{ is bounded}\right\}$$

- But being a lub is not really informative!
  - The convergence disk is convex

Convergence radius

- The usual definition

$$\rho\left(\sum_{n\in\mathbb{N}} a_n x^n\right) = \sup\left\{r \in \mathbb{R} \mid \text{the sequence } \left|a_n r^n\right| \text{ is bounded}\right\}$$

- But being a lub is not really informative!
  - The convergence disk is convex
    - But being bounded is not decidable

$$o_{i,j}(n) = \begin{cases} 0 & \text{if } \mathcal{T}_i(j) \text{ stops in less than } n \text{ steps} \\ n & \text{otherwise} \end{cases}$$

Convergence radius

- The usual definition

$$\rho\left(\sum_{n\in\mathbb{N}} a_n x^n\right) = \textcolor{red}{\sup}\left\{r \in \mathbb{R} \mid \text{the sequence } \left|a_n r^n\right| \text{ is bounded}\right\}$$

- But being a lub is not really informative!
  - The convergence disk is convex
    - But being bounded is not decidable
    - Hence not provable without EM

Our definition

- Being inside the convergence radius:

$$\texttt{Cv\_radius\_weak}\,(a_n, r) = |a_n r^n| \text{ is bounded}$$

Our definition

- Being inside the convergence radius:

$$\texttt{Cv\_radius\_weak}\,(a_n, r) = |a_n r^n| \text{ is bounded}$$

- Having a finite radius of convergence:

$$\texttt{finite\_cv\_radius}\,(a_n, r) =$$

$$\begin{array}{lllll} & \forall r', & 0 \leq r' < r & \Rightarrow \texttt{Cv\_radius\_weak}\,(a_n, r') \\ \wedge & \forall r', & r < r' & \Rightarrow \neg\,\texttt{Cv\_radius\_weak}\,(a_n, r') \end{array}$$

But... Do we have the right to do this?

- This definition is more informative:

$$\texttt{finite\_cv\_radius}\left(a_n, r\right) \Rightarrow r = \sup\left\{\ldots\right\}$$

But... Do we have the right to do this?

- This definition is more informative:

$$\texttt{finite\_cv\_radius}\,(a_n, r) \Rightarrow r = \sup\,\{\dots\}$$

- But given EM, it is equivalent:

$$EM \Rightarrow r = \sup\,\{\dots\} \Rightarrow \texttt{finite\_cv\_radius}\,(a_n, r)$$

But... Do we have the right to do this?

- This definition is more informative:

$$\texttt{finite\_cv\_radius}\,(a_n, r) \Rightarrow r = \sup\{\dots\}$$

- But given EM, it is equivalent:

$$EM \Rightarrow r = \sup\{\dots\} \Rightarrow \texttt{finite\_cv\_radius}\,(a_n, r)$$

  - Idea of the proof:

$$\forall r', 0 \le r' < r \Rightarrow \texttt{Cv\_radius\_weak}\,(a_n, r')$$

Convergence criterion

Alembert criteria

$$\lim_{n\to+\infty} \frac{a_{n+1}}{a_n} = \lambda \Rightarrow \rho(\sum_n a_n x^n) = \frac{1}{\lambda}$$

Another criteria

$$\sum_n a_n \lambda^n CV \wedge \sum_n a_n \lambda^n NCVN$$

$$\Rightarrow \rho(\sum_n a_n x^n) = |\lambda|$$

Sums

Abel's lemma

$$\forall r.\, |r| < \rho \left(\sum_n a_n x^n \right) \Rightarrow \exists l.\, \sum_{n=0}^{+\infty} a_n r^n = l$$

- Compatibility with common operations
  - Most of it is trivial thanks to `Rsequence`
  - The compatibility with `Rmult` comes from `Rseries`
- Formal derivatives
  - `An_deriv`$(a_n)(n) = (n+1)a_{n+1}$: the hard part
    - Convergence radius preservation
    - The formal derivative *is* the derivative
  - `An_nth_deriv`(a_n, k): by reccurence

Applications

- Usual functions defined in a couple of lines.
  - exp
  - cos, sin
- Properties for free
  - derivability
  - shape of the nth derivative

Build tactics on top of this

- What is annoying when proving lemmas?
  - Proving obvious equalities
  - Compatibility with common operations
  - Formal derivatives
- How to avoid proving everything by hand?
  - `ring`, `field`
  - `solve_diff_equa`

Why using reflection?

- Add more guarantees to your tactic
- Avoid the manipulation of huge terms
- Replace proofs by computations
- Easy to extend

Simple remarks

- Sums of power series are extentional:

$$a_n \equiv b_n \Rightarrow \sum_n a_n x^n \equiv \sum_n b_n x^n$$

- Sums of power series are compatible with addition:

$$\sum_n (a_n + b_n) x^n \equiv \sum_n a_n x^n + \sum_n b_n x^n$$

- We know the exact shape of the n$^t h$ derivative:

$$(\sum_n a_n x^n)^{(k)} \equiv \sum_n \texttt{An\_nth\_deriv}\, a_n x^n$$

`solve_diff_equa` - A very basic version

- Side equations: $E ::= y_i^{(k)} \mid E + E$

solve_diff_equa - A very basic version

- Side equations: $E ::= y_i^{(k)} \mid E + E$
- Equations: $E1 :=: E2$

`solve_diff_equa` - A very basic version

- Side equations: $E ::= y_i^{(k)} \mid E + E$
- Equations: $E1 :=: E2$
- Two semantics: talking about power series or sequences over $\mathbb{R}$

$[|\mathsf{E}_1 \mathbin{:=:} \mathsf{E}_2|]_{\mathbb{R}}\,\rho = ?$

- $\mathtt{interp}_{\mathbb{R}}$ is the trivial semantics à la Tarski that one could expect:

$$\mathtt{interp}_{\mathbb{R}}(y_i^{(k)}, \rho) = \left(\sum_n \rho(i)_n x^n\right)^{(k)}$$

$$\mathtt{interp}_{\mathbb{R}}(E_1 + E_2, \rho) = \mathtt{interp}_{\mathbb{R}}(E_1, \rho) + \mathtt{interp}_{\mathbb{R}}(E_2, \rho)$$

$[|\mathsf{E}_1 \mathrel{:=:} \mathsf{E}_2|]_{\mathbb{R}}\,\rho = ?$

- $\mathtt{interp}_{\mathbb{R}}$ is the trivial semantics à la Tarski that one could expect:

$$\mathtt{interp}_{\mathbb{R}}(y_i^{(k)}, \rho) = \left(\sum_n \rho(i)_n x^n\right)^{(k)}$$

$$\mathtt{interp}_{\mathbb{R}}(E_1 + E_2, \rho) = \mathtt{interp}_{\mathbb{R}}(E_1, \rho) + \mathtt{interp}_{\mathbb{R}}(E_2, \rho)$$

- It is used to define the semantics of equations:

$$[|\mathsf{E}_1 \mathrel{:=:} \mathsf{E}_2|]_{\mathbb{R}}\,\rho = (\mathtt{interp}_{\mathbb{R}}(E_1, \rho) \equiv \mathtt{interp}_{\mathbb{R}}(E_2, \rho))$$

$[|\mathsf{E}_1 \mathrel{:=:} \mathsf{E}_2|]_{\mathbb{N}}\, \rho = ?$

- $\mathtt{interp}_{\mathbb{N}}$ is a bit more subtle:

$$\mathtt{interp}_{\mathbb{N}}(y_i^{(k)}, \rho) = \mathtt{An\_nth\_deriv}\,(\rho(i), k)$$

$$\mathtt{interp}_{\mathbb{N}}(E_1 + E_2, \rho) = \mathtt{interp}_{\mathbb{N}}(E_1, \rho) + \mathtt{interp}_{\mathbb{N}}(E_2, \rho)$$

$[|\mathsf{E}_1 :=: \mathsf{E}_2|]_{\mathbb{N}}\,\rho = ?$

- $\mathtt{interp}_{\mathbb{N}}$ is a bit more subtle:

$$\mathtt{interp}_{\mathbb{N}}(y_i^{(k)}, \rho) = \mathtt{An\_nth\_deriv}\,(\rho(i), k)$$

$$\mathtt{interp}_{\mathbb{N}}(E_1 + E_2, \rho) = \mathtt{interp}_{\mathbb{N}}(E_1, \rho) + \mathtt{interp}_{\mathbb{N}}(E_2, \rho)$$

- It is used to define the semantics of equations:

$$[|\mathsf{E}_1 :=: \mathsf{E}_2|]_{\mathbb{N}}\,\rho = (\mathtt{interp}_{\mathbb{N}}(E_1, \rho) \equiv \mathtt{interp}_{\mathbb{N}}(E_2, \rho))$$

Main theorem

$$[|\mathsf{E}_1 :=: \mathsf{E}_2|]_{\mathbb{N}}\,\rho \Rightarrow [|\mathsf{E}_1 :=: \mathsf{E}_2|]_{\mathbb{R}}\,\rho$$

$\forall n.\, \exp^{(n+1)} = \exp^{(n)}$

$$\forall k \in \mathbb{N}, \frac{((n+1)+k)!}{k!} * \frac{1}{((n+1)+k)!} = \frac{(n+k)!}{k!} * \frac{1}{(n+k)!}$$

Thanks for your attention!

More information available online:

`http://coqtail.sf.net`