Coq with power series

Guillaume Allais
Junior Laboratory COQTAIL
Ens Lyon - France
guillaume.allais@ens-lyon.org

In the interactive theorem prover Coq[1], trigonometric functions are defined in the standard library. However they are not directly described as power series due to a lack of formalization of this concept. We present a strategy to describe the power series over $\mathbb{R}$ and then advocate for the broad use of abstract concepts in the standard library by showing the immediate benefits it brings.

Thanks to the power series framework we are able to redefine the usual functions (e.g. sin, cos, exp) in less than 80 lines, to get some of their properties for free (e.g. being in the C^∞ class) and to prove that they are solutions of particular differential equations just by studying sequences over $\mathbb{R}$.

Files: All the implementation mentioned in this paper are available for download via COQTAIL's svn repository[1].

1 Formalization

Power series are a rather intensional mathematical notion; therefore, its formalization in an interactive theorem prover is really close to textbooks' presentation. Except for one point: the definition of the convergence radius.

In an intuitionistic setting, our definition of the radius of convergence is much more informative than the standard one. This is however not harmful given that it has been proved classically equivalent to the standard one. This design choice allows us to get rid of the excluded-middle (henceforth EM) axiom in most proofs that traditionally use it. One could expect as a drawback that the lemmas with the existence of a radius of convergence as a conclusion not to be provable anymore. It is fortunately not the case[2].

1.1 The convergence radius

The convergence radius ρ of a power series whose coefficients are $(a_n)_{n\in\mathbb{N}}$ is usually defined as a lowest upper bound (in $\mathbb{R}\cup\{+\infty\}$):

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

As being bounded is not decidable, knowing that r is the convergence radius of $\sum_{n\in\mathbb{N}} a_n x^n$ is not sufficient to show without using EM that the sequence $(|a_n x^n|)_{n\in\mathbb{N}}$ is bounded for all x in $B_r(0)$. That is why we use a more verbose definition which describes exactly the same idea of being the lowest upper bound and is easier to use.

[1] see `http://sourceforge.net/projects/coqtail/develop` and in particular `src/Reals/Rpser.v`.

[2] At least for d'Alembert's ratio criterion which is one of the key lemmas that have this shape.

Submitted to:
THedu 2011

Definition 1 (Rpser_def) *We say that r is a weak convergence radius if it is a lower bound for the convergence radius (ie. r belongs to the disk of convergence).*

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

From this definition, we can obtain the definition of the finite convergence radius[3].

Definition 2 (Rpser_def) *The convergence radius is finite and equal to r if r is both bigger than all the weak convergence radiuses and smaller or equal to all the reals that are too big to be weak convergence radiuses.*

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

The classical equivalence between this definition and the usual one is proved through the two following lemmas. Unsurprisingly, the first implication does not need the excluded middle axiom: our definition is stronger in an EM-free setting than the usual one.

Lemma 1 (Rpser_base_facts) $\texttt{finite\_cv\_radius}(a_n, r) \Rightarrow r = \sup\{x | \texttt{Cv\_radius\_weak}(a_n, x)\}$

Lemma 2 (Rpser_base_facts) $EM \wedge r = \sup\{x | \texttt{Cv\_radius\_weak}(a_n, x)\} \Rightarrow \texttt{finite\_cv\_radius}(a_n, r)$

The first important tool that we can get is d'Alembert's ratio criterion. It can be used to prove that a particular power series has a given convergence radius; this result is for example used to prove that exp has an infinite convergence radius from which we can easily deduce that so do cos and sin.

Lemma 3 (Rpser_cv_facts) *D'Alembert's ratio criterion states that, given a sequence* $(a_n)_{n\in\mathbb{N}}$ *which ultimately contains only nonzero elements:*

$$\lim_{n\to+\infty} \left| \frac{a_{n+1}}{a_n} \right| = \lambda \neq 0 \Rightarrow \texttt{finite\_cv\_radius}(a_n, \frac{1}{\lambda})$$

1.2 Sum of a power series

When we know what is the power series' convergence radius, we can start summing it on the appropriate domain. Our cherished tool to define the sum of a power series is obviously Abel's lemma which states that given a convergence radius, we can sum the power series inside the corresponding ball.

Lemma 4 (Rpser_radius_facts)

$$\texttt{Cv\_radius\_weak}(a_n, r) \Rightarrow \forall x \in B_r(0), \exists l, \sum_{n=0}^{+\infty} a_n x^n = l$$

Definition 3 (Rpser_sums) *From this lemma we can construct the functions (namely* `weaksum_r`*,* `sum_r` *and* `sum`*) that given either* $\texttt{Cv\_radius\_weak}(a_n, r)$*,* $\texttt{finite\_cv\_radius}(a_n, r)$ *or* $\texttt{infinite\_cv\_radius}(a_n)$ *output the piecewise-defined function:*

$$x \mapsto \begin{cases} \sum_{n=0}^{+\infty} a_n x^n & \text{if } x \text{ is inside the convergence disk} \\ 0 & \text{otherwise} \end{cases}$$

[3]The extension to the infinite case is straightforward: the convergence radius is infinite if and only if all the reals are weak convergence radiuses.

1.3 Derivative of a power series

The formalization of the derivative of a power series is done in two steps. First of all, we define the formal derivative of a power series and prove that this definition makes sense (e.g. that the sum exists):

Definition 4 (Rpser_derivative) *The formal derivative of the power series defined by (a_n) is the one defined by:*

$$\texttt{An\_deriv}\,(a_n) = (n+1) * a_{n+1}$$

Lemma 5 (Rpser_radius_facts) *And its convergence radius is exactly the same as the one of the original series:*

$$\texttt{finite\_cv\_radius}\,(a_n, r) \Leftrightarrow \texttt{finite\_cv\_radius}\,(\texttt{An\_deriv}\,(a_n), r)$$

Now we know that the formal derivative is summable but we still have to somehow explicit the relation that exists between these two power series. This is maybe the most complex part of the library; it uses a theorem on sequences of functions (see infra) plus the fact that the sequence of the partial sums of a power series converges normally (thus uniformly) inside the disk of convergence.

Theorem 1 (RFsequence_facts) *On the ball $B_r(c)$ if $(f_n)_{n\in\mathbb{N}}$ is a sequence of derivable functions and if the following limits exist:*

$$f_n \xrightarrow{n\to+\infty} f \quad \textit{and} \quad f'_n \xrightarrow[CVU]{n\to+\infty} g$$

then f is derivable and its derivative is g.

As a consequence, we can conclude that the power series are derivable and that their derivative is precisely the sum of the formal derivative. As the derivative of a power series is another power series, it is trivial to show that the function defined as the sum belongs to the C^∞ class[4]. A simple induction can even give us the explicit description of the n^{th} derivative of a sum:

Definition 5 (Rpser_def) *The formal k^{th} derivative of the power series defined by (a_n) is the one defined by:*

$$\texttt{An\_nth\_deriv}\,(a_n, k) = \frac{(n+k)!}{n!} a_{n+k}$$

Lemma 6 (Rpser_derivative_facts) *Explicit description of the k^{th} derivative of the power series defined by $(a_n)_{n\in\mathbb{N}}$:*

$$\left(\sum_{n=0}^{+\infty} a_n x^n\right)^{(k)} = \sum_{n=0}^{+\infty} \texttt{An\_nth\_deriv}\,(a_n, k) x^n$$

2 Applications

2.1 Defining usual functions

Thanks to all the formalization work, we can now define all the usual functions in a few lines. We begin by defining the exponential using d'Alembert's ratio test to prove that its convergence radius is infinite (which is rather easy).

Then we can show easily that cosine and sine also have an infinite convergence radius by using one of the basic lemmas:

[4] See the C_n_* files for results on classes of functions.

Lemma 7 (Rpser_base_facts) `Cv_radius_weak` *is compatible with the pointwise order on the sequences over reals:*

$$(|b_n| \leq_{pointwise} |a_n|) \Rightarrow \forall r, \texttt{Cv\_radius\_weak}(a_n, r) \Rightarrow \texttt{Cv\_radius\_weak}(b_n, r)$$

We have been able to define exp, sin and cos in less than 80 lines of Coq source code. It has to be compared to the hundreds of lines and the ad-hoc arguments (e.g. convergence of alternating series) that Coq's standard library dedicates to the definition of these exact same functions.

Not only defining these functions is way easier, but we get for free their derivability (and even their being in the C^∞ class), the exact shape of their n^{th} derivative and therefore we can easily prove the relations that exist between them.

2.2 Finding solutions of linear differential equations

On top of the power series formalization, we constructed a small library that describes linear differential equations of arbitrary shape by reflection. It is based on two components:

- A datatype `side_equa` that is a descriptor of linear differential equations. A differential equation is a pair (E_1, E_2) of side equations (usually written $E_1 :=: E_2$).
- A (set of) semantics that given an inhabitant of this datatype and an environment, outputs a proposition.

Definition 6 (Dequa_def) *The grammar of the* `side_equa` *datatype is (where c is a real constant):*

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

Definition 7 (Dequa_def) *The semantics that translates differential equations into propositions on sequences over* $\mathbb{R}$ *is defined in two steps. First of all we define recursively the interpretation of the side of an equation:*

$$\begin{array}{lcl}
\texttt{interp_N} & : & \texttt{side_equa} \to \texttt{Rseq list} \to \texttt{Rseq} \\
\texttt{interp_N}(\quad c \quad, \rho) & = & \texttt{An_cst}(c) \\
\texttt{interp_N}(\quad y_i^{(k)} \quad, \rho) & = & \texttt{An_nth_deriv}(\rho(i), k) \\
\texttt{interp_N}(\quad -E \quad, \rho) & = & -\texttt{interp_N}(E, \rho) \\
\texttt{interp_N}(\quad E_1 + E_2 \quad, \rho) & = & \texttt{interp_N}(E_1, \rho) + \texttt{interp_N}(E_2, \rho)
\end{array}$$

and then we can construct the interpretation function:

$$[|E_1 :=: E_2|]_{\mathbb{N}} \rho = \forall n, \texttt{interp\_N}(E_1, \rho)(n) = \texttt{interp\_N}(E_2, \rho)(n)$$

We can define similarly the semantics $[|\_|]_{\mathbb{R}}$ that translates differential equations into propositions on power series. Having this generic representation of differential equations and this different semantics allows us to state general theorems about linear differential equations.

Lemma 8 (Dequa_facts) *Our main result states that given a context* ρ *of sequences of coefficients, we have (provided that the involved power series have an infinite radius of convergence):*

$$[|E_1 :=: E_2|]_{\mathbb{N}} \rho \Rightarrow [|E_1 :=: E_2|]_{\mathbb{R}} \rho$$

ie. we can prove that some functions (sums of power series) are solutions of a given differential equation by proving results on their coefficients.

By using this theorem, one can prove in less than 20 lines that the exponential is a solution of the equation $y^{(n+1)} = y^{(n)}$. Without much more work, one can also prove that cosine and sine are solutions of $y^{(2)} = -y$.

3 Extensions

3.1 Power series on other carriers

COQTAIL already has a basic library on the power series over the complex numbers[5] (definitions, differentiability, derivability). A future work could be to adapt the work done on the real numbers to the complex numbers. A better idea might be to formalize the power series on a more general structure (e.g. a ring equipped with a norm).

3.2 Improving the library on differential equations

Even if the work on the differential equations is already quite convenient, it is still rather limited: one can only derive variables and not composed expressions, there is currently no built-in minus function or multiplication by a constant and it is impossible to talk about the product of power series.

In the future, a description of the explicit shape of the product of two power series (the power series which is defined with the Cauchy product of the coefficients' sequences) could be a valuable addition.

References

[1] INRIA: *The Coq proof assistant*.

4 Acknowledgements

Thanks to all the COQTAIL project's members who helped proofreading the drafts. Special thanks to Sylvain Dailler and Marc Lasson for their useful comments and suggestions.

[5] See src/Complex/Cpser_*.v