Classical Analysis with Coq

Reynald Affeldt[1], Cyril Cohen[2], Assia Mahboubi[2],
Damien Rouhling[2], and Pierre-Yves Strub[3]

[1] AIST, Japan
[2] Inria, France
[3] École polytechnique, France

1 Motivations and Related Work

In this talk we present an ongoing effort to develop a Coq formal library (hereafter, MathComp-Analysis[1]) about elementary real analysis, in a firmly classical setting. Almost all existing proof assistants on the market have been used to define real numbers, and to investigate the formalization of real, and sometimes also complex, analysis. A survey by Boldo et al. reviews the different approaches and the breadth of the existing developments [4]. In particular, the Coq standard library provides an axiomatization of real numbers [8], with a classical flavor and the Coquelicot external library is a conservative extension thereof [3]. By contrast, the C-CoRN [6] and MathClasses libraries adopt a constructive viewpoint [4, Sect. 3.2.3]. At the time of writing, these libraries however cover far less material that their analogues in the HOL ecosystem, including Harrison's HOL Light library and its translation to Isabelle/HOL.

MathComp-Analysis is yet another attempt at providing a library for classical analysis in Coq. The motivation is twofold. First, it relies on stronger classical axioms, so as to get closer to the logical formalism used in classical mathematics (Sect. 2). In particular, this impacts the formalization of compactness-related facts. Second, it is designed along the formalization methodology put into practice in the Mathematical Components libraries [7]. The latter libraries are essentially geared towards algebra and this work aims at providing an extension for topics in analysis. However, we incorporated a significant subset of the Coquelicot library. The main original contributions lie in the effort put in the infrastructure of MathComp-Analysis: automation, notations, etc. (Sect. 3). Though still in its infancy, our library already proved useful enough for a few applications (Sect. 4).

2 Axioms and Models

The formalization is carried in CIC augmented with three additional axioms, imported from the Coq standard library: the `propositional_extensionality` `functional_extensionality_dep` extensionality properties, and the `constructive_indefinite_description` choice principle. In particular, these axioms are used to derive the following properties:

```
propext: forall (P Q : Prop), (P <-> Q) -> (P = Q).
funext: forall {T U : Type} (f g : T -> U), (forall x, f x = g x) -> f = g

pselect: forall (P : Prop), {P} + {~P}.
gen_choiceMixin: forall {T : Type}, Choice.mixin_of T.
```

where `gen_choiceMixin` states that every type is equipped with an Hilbert ϵ operator. We provide an axiomatization of real numbers as an archimedean real closed field with a supremum, for which we show that the standard library axiomatization [8] is a model. We plan to ultimately provide an alternative model, obtained as a classical construction of the reals from the three aforementionned exentionality and choice axioms.

3 Classical Real Analysis

MathComp-Analysis provides a theory of sets, limits, continuity, compact sets, comparison of functions, differentials and derivatives. Most of the results about limits and continuity are ported from Coquelicot, through the adaptation of a significant part of its hierarchy to make it compatible with Mathematical Components (Fig. 1). We extended this hierarchy with structures that, combined with a new set of tactics, ease the handling of filters.

[1] https://github.com/math-comp/analysis

Our library contains in particular the proofs of various standard theorems: Zorn's Lemma, Tychonoff's Theorem, Heine-Borel's Theorem, the Intermediate Value Theorem, Rolle's Theorem and the Mean Value Theorem. Our proofs of Zorn's Lemma and Tychonoff's Theorem are inspired by D. Schepler's work [9, 10].

Infrastructure Formalizing analysis is a substantial endeavor and we are now in the process of sharpening adequate tools to facilitate the writing of scripts and their maintenance. For example, since Bachmann-Landau notations are pervasive, we chose to carefully craft an infrastructure for equational reasoning using little-o's and big-O's. It was in particular instrumental in producing a generic theory of differentiation.

Similarly, we provide an infrastructure to facilitate ε/δ-reasoning. Its main ingredients are a set of tactics, based on the idea of the `bigenough` tactic from the MATHEMATICAL COMPONENTS library, to delay the proof of witness properties in existential proofs and small scale automation to rule out proofs of positivity for ε's.

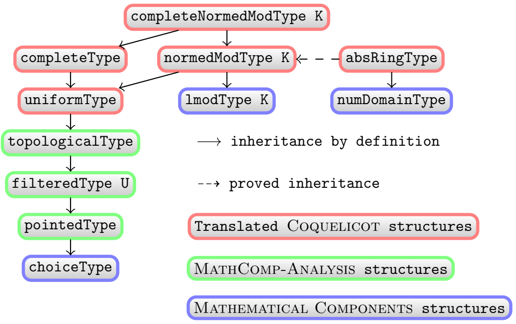

Figure 1: Augmented hierarchy

4 Applications and Perspectives

We briefly presented MATHCOMP-ANALYSIS, a COQ library about elementary real analysis. The library lies in a firmly classical setting and is integrated into the MATHEMATICAL COMPONENTS algebraic hierarchy.

This development has been used for the formalization [11] of the soundness of probabilistic relational logic. This logic is at the core of EasyCrypt[2] [2], a toolset for reasoning about probabilistic computations, and whose main application is the construction and verification of game-based cryptographic proofs. Notably, it required the development of a discrete probability distributions theory. We are also in the process of applying MATHCOMP-ANALYSIS to the formalization of motion and control theory in robotics, another topic that requires results on functional analysis [1, 5].

Our long term goal is to provide a comprehensive COQ library, that can serve the formal study of topics relying both on results in algebra and in analysis. Examples of such topics include: computer-algebra algorithms, cyber-physical systems, post-quantum cryptographic primitives, information theory, etc.

Acknowledgments. This work was supported in part by the project FastRelax ANR-14-CE25-0018-01 and JSPS KAKENHI Grant Number 15H02687.

References

[1] Reynald Affeldt and Cyril Cohen. Formal foundations of 3D geometry to model robot manipulators. In *6th ACM SIGPLAN Conference on Certified Programs and Proofs (CPP 2017)*, pages 30–42. https://github.com/affeldt-aist/coq-robot.

[2] Gilles Barthe, François Dupressoir, Benjamin Grégoire, César Kunz, Benedikt Schmidt, and Pierre-Yves Strub. Easycrypt: A tutorial. In *Foundations of Security Analysis and Design*, volume 8604 of *LNCS*, pages 146–166, 2013.

[3] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Coquelicot: A user-friendly library of real analysis for Coq. *Mathematics in Computer Science*, 9(1):41–62, 2015.

[4] Sylvie Boldo, Catherine Lelay, and Guillaume Melquiond. Formalization of real analysis: a survey of proof assistants and libraries. *Mathematical Structures in Computer Science*, 26(7):1196–1233, 2016.

[5] Cyril Cohen and Damien Rouhling. A formal proof in Coq of LaSalle's invariance principle. In *8th International Conference on Interactive Theorem Proving*, volume 10499 of *LNCS*, pages 148–163, 2017. https://github.com/drouhling/LaSalle/tree/mathcomp-analysis.

[6] Luís Cruz-Filipe, Herman Geuvers, and Freek Wiedijk. C-CoRN, the constructive Coq repository at Nijmegen. In *3rd International Conference on Mathematical Knowledge Management*, volume 3119 of *LNCS*, pages 88–103, 2004.

[7] Assia Mahboubi and Enrico Tassi. *Mathematical Components*. Available at: https://math-comp.github.io/mcb/, 2016. With contributions by Yves Bertot and Georges Gonthier.

[8] Micaela Mayero. *Formalisation et automatisation de preuves en analyses réelle et numérique*. PhD thesis, Université Paris VI, Dec. 2001.

[9] Daniel Schepler. Topology library. https://github.com/coq-contribs/topology.

[10] Daniel Schepler. Zorn's Lemma. https://github.com/coq-contribs/zorns-lemma.

[11] Pierre-Yves Strub. Probabilistic relational logic. https://github.com/strub/xhl.

[2] https://www.easycrypt.info/