Certified exact real computation on hyperspaces*

Michal Konečný[1], Sewon Park[2], and Holger Thies[2]

[1]Aston University, UK [2]Kyoto University, Japan

In recent ongoing work [KPT21, KPT22a, KPT22b] we develop a framework for verified exact real computation in a dependent type theory and build the Coq library CAERN based on the theory[1].

As before, we assume to work in a simple dependent type theory with basic types $\mathsf{0}, \mathsf{1}, \mathsf{2}, \mathsf{N}, \mathsf{Z}$ and universes Prop for classical proposition and Type as a universe of types. We assume classical axioms to hold in Prop and axiomatically define a type R of real numbers. The soundness of our axioms is justified by extending a realizability interpretation in the category of assemblies over Kleene's second algebra. We further extend Coq's program extraction to map R and basic operations on real numbers to the corresponding types and operations in the AERN Haskell framework for efficient exact real computation [Kon21].

Our previous work mostly deals with basic operations on real and complex numbers such as computation of square roots and other simple functions. In the present work we extend our framework to computation on higher-order objects such as spaces of functions and hyperspaces of real subsets. To this end, we need to have a continuity principle in our axiomatic system saying that every function in our type theory is continuous. Following the general approach of our project, we introduce the continuity principle in an abstract level without referring to specific constructions of continuous types:

$$\Pi(f : \mathsf{R} \to \mathsf{S}).\ \Pi(x : \mathsf{R}).\ (f\ x){\downarrow} \to \mathsf{M}\Sigma(n : \mathsf{N}).\ \Pi(y : \mathsf{N}).\ |x - y| < 2^{-n} \to (f\ y){\downarrow}$$

where S denotes Sierpinski space. That is, for any Sierpinski-valued mapping f from reals, when $f\ x$ is defined, there nondeterministically exists a natural number n such that f is defined also for any 2^{-n}-close real number y.

To express subsets classically we use the universe Prop and define

$$\mathsf{csubset}(X) :\equiv X \to \mathsf{Prop}\ .$$

and classical operations such as $\in, \cup, \cap$, etc. in the obvious way. Following e.g. [Pau16], we can further define spaces of open, closed, compact and overt subsets and prove some of their properties.

---

*Holger Thies is supported by JSPS KAKENHI Grant Number JP20K19744. Sewon Park is a JSPS International Research Fellow supported by JSPS KAKENHI (Grant-in-Aid for JSPS Fellows) 22F22071. This project has received funding from the EU's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 731143.

[1]Our Coq implementation and the extracted Haskell/AERN programs can be found at `https://github.com/holgerthies/coq-aern`

To extend the program extraction feature to subsets and function spaces, we also need to extend AERN by types for such spaces. We discuss how to implement these types in an efficient way and give some examples of extracted programs. We also discuss possible applications such as drawing of real subsets and reachability problems for simple dynamical systems.

References

[Kon21] Michal Konečný. aern2-real: A Haskell library for exact real number computation. `https://hackage.haskell.org/package/aern2-real`, 2021.

[KPT21] Michal Konečný, Sewon Park, and Holger Thies. Axiomatic reals and certified efficient exact real computation. In *International Workshop on Logic, Language, Information, and Computation*, pages 252–268. Springer, 2021.

[KPT22a] Michal Konečnỳ, Sewon Park, and Holger Thies. Certified computation of nondeterministic limits. In *NASA Formal Methods Symposium*, pages 771–789. Springer, 2022.

[KPT22b] Michal Konečnỳ, Sewon Park, and Holger Thies. Extracting efficient exact real number computation from proofs in constructive type theory. *arXiv preprint arXiv:2202.00891*, 2022.

[Pau16] Arno Pauly. On the topological aspects of the theory of represented spaces. *Comput.*, 5:159–180, 2016.