Towards a verified and computable theory of compositional dynamic systems

Pieter Collins[1], Bas Laarakker[1], Sewon Park[2], Sacha Sindorf[1], and Holger Thies[2]

[1]Department of Advanced Computing Sciences,
Maastricht University, The Netherlands
[2]Kyoto University, Japan

August 8, 2023

A major challenge in computational systems theory is the rigorous verification of dynamic systems with respect to a specification of the behaviour. To achieve the utmost confidence that the toolchain used is correct, both the underlying theory and the implementation should be verified using a proof assistant such as Coq. Most relevant systems in applications are built up of smaller components, and practically efficient verification methods should use the compositional structure in the verification process.

An attempt to provide a framework for hybrid dynamic systems which is both compositional and computable (in the sense of type-two effectivity) is given in [BCGSVZ20]. Since this theory involves many subtle technical aspects, we would like verified proofs that the framework is correct. In this talk, we present progress towards such a verification.

We first present an overview of the systems-theoretic problems we aim to solve, and the core operations needed. We then describe the Incone library [STT21], and subsequent work on subsets of Euclidean space [KPT23], which formalise in Coq many of the operations of computable analysis which we need for the subsequent development. This includes continuous functions, open, closed, overt and compact sets, and also set-valued functions. We next give results on formalisations for two subclasses of hybrid systems, namely deterministic discrete-time systems [Sin23] and timed-event systems [Laa23]. Finally, we give some perspectives on synthesising these works into a coherent library [Col23] and extending to more complicated classes of systems.

Acknowledgements: Holger Thies is supported by JSPS KAKENHI Grant Numbers JP20K19744 and JP18H03203. Sewon Park is a JSPS International Research

Fellow supported by JSPS KAKENHI (Grant-in-Aid for JSPS Fellows) JP22F22071.
 This project has received funding from the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No 731143.

References

[BCGSVZ20] Davide Bresolin, Pieter Collins, Luca Geretti, Roberto Segala, Tiziano Villa, and Sanja Živanović Gonzalez. A computable and compositional semantics for hybrid automata. *Proceedings of the ACM International Conference on Hybrid Systems: Computation and Control*, April 2020.

[Col23] Pieter Collins. Verified rigorous numerics library, 2023. `https://github.com/ariadne-cps/verifiedcalculus`.

[KPT23] Michal Konečný, Sewon Park, and Holger Thies. Formalizing hyperspaces for extracting efficient exact real computation Proceedings of the 48th International Symposium on Mathematical Foundations of Computer Science, 2023.

[Laa23] Bastiaan Laarakker. A formalisation of timed behaviours in Coq. Bachelor Thesis, Maastricht University, 2023.

[Sin23] Sacha Sindorf. Proving correctness of compositional systems analysis using Coq. Master Thesis, Maastricht University, 2023.

[STT21] Florian Steinberg, Laurent Thery, and Holger Thies. Computable analysis and notions of continuity in Coq. *Logical Methods in Computer Science*, 17(2), May 2021.