Towards verified implementation of iterative and interactive real-RAM *

Sewon Park
Kyoto University, Japan

Holger Thies
Kyoto University, Japan

Recently, several studies have been focusing on verification methodologies for user programs of exact real computation frameworks under the assumption that the frameworks are sound; see [PBC+16, KPT21, KPT22] for some examples. In this work, we take this one step further and consider verifying if the frameworks themselves correctly realize basic exact computations with real numbers.

Amongst many different approaches in implementing exact real computation, we focus on iRRAM-like implementations. IRRAM, iterative and interactive real-RAM, is a C++ implementation simulating real number computations through indefinite reiterations of approximating computations [Mül00]. By abstracting away the reiterations, for the user variables seem to store exact real numbers supporting error-free computations. Furthermore, iRRAM provides user interactions, such as input and output of real numbers. As an inevitable side effect, dynamically allocated memory is extensively used in its implementation to force outputs shown to users at some iteration to be consistent in future reiterations regarding multi-valued choices; see *multi-value cache* in [Mül00].

As a first step, we formalize a simple imperative language over arbitrary discrete data. The language has heap memory support and can raise a *reiteration* exception. To make the language model iRRAM's implementation language well, we formalize its type-2 semantics: Infinite (converging) sequences of variable input stores are transformed to their limit by letting computations reiterate at a reiteration exception with the next input store. However, the heap is assumed to be carried on throughout reiterations allowing reiterations to communicate through heap memory. We recognize that this type-2 semantics is not compositional and propose solving this problem by using Hoare-style specification logic to achieve compositional reasoning about the non-compositional semantics.

References

[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.

*Sewon Park is a JSPS International Research Fellow supported by JSPS KAKENHI (Grant-in-Aid for JSPS Fellows) JP22F22071. Holger Thies is supported by JSPS KAKENHI Grant Numbers JP20K19744 and JP23H03346.

[KPT22] Michal Konečný, Sewon Park, and Holger Thies. Certified computation of nondeterministic limits. In Jyotirmoy V. Deshmukh, Klaus Havelund, and Ivan Perez, editors, *NASA Formal Methods*, pages 771–789, Cham, 2022. Springer International Publishing.

[Mül00] Norbert Th Müller. The iRRAM: Exact arithmetic in C++. In *International Workshop on Computability and Complexity in Analysis*, pages 222–252. Springer, 2000.

[PBC+16] Sewon Park, Franz Brauße, Pieter Collins, SunYoung Kim, Michal Konečnỳ, Gyesik Lee, Norbert Müller, Eike Neumann, Norbert Preining, and Martin Ziegler. Foundation of computer (algebra) ANALYSIS systems: Semantics, logic, programming, verification. *arXiv preprint arXiv:1608.05787*, 2016.