Project Proposal **Renato Neves, José Proença**
Date: July 7, 2022

Verification of programs written in Lince

Motivation and Goals

Hybrid programs orchestrate classic computation with physical processes in order to reach prescribed goals. Examples of this are diverse and range from small medical devices, such as pacemakers and insulin pumps, to autonomous vehicles and district-wide electric/water grids. Their rapid development in the last decades lead to a flurry of research on suitable languages, semantics, and tools for their design and analysis [Pla10, Nev18, GNP20]; and even though great progress has been made on this area, several important challenges remain largely open. A prominent case concerns *the verification of hybrid programs* written in the tool Lince [GNP20]: the latter has simulation capabilities but cannot verify that a program will behave as expected under *all possible scenarios*.

The goal of this project is to extend the tool Lince with verification capabilities. Technically this will amount to implementing a *translator* from programs written in Lince to programs written in the tool KeYmaera [Pla10]. The latter also supports hybrid programs (albeit in a different form than those written in Lince) and is connected to a semi-automated theorem prover that has been used successfully to verify certain hybrid programs.

Research Plan

The first step of this project is to study the languages and corresponding semantics underlying the tools Lince and KeYmaera. The next step is to design a translation system from programs written in Lince to programs written in KeYmaera, and to prove that this translation agrees with the semantics. Subsequently the task is to implement this translation in a functional programming language such as Haskell. After that the goal is to benchmark the implemented translation against different scenarios, which among other things should include the complete verification of a simple autonomous driving system. The final step is to write a report detailing the theories and implementations developed throughout the project.

References

[GNP20] Sergey Goncharov, Renato Neves, and José Proença. Implementing hybrid semantics: From functional to imperative. In *International Colloquium on Theoretical Aspects of Computing*, pages 262–282. Springer, 2020.

[Nev18] Renato Neves. *Hybrid programs.* PhD thesis, Minho University, 2018.

[Pla10] André Platzer. *Logical Analysis of Hybrid Systems: Proving Theorems for Complex Dynamics.* Springer, Heidelberg, 2010.