Formalizing Coinduction via Closure Operators and Proof Cycles

Scientific Abstract

As software has become critical to societal infrastructure, mechanically certified software has grown increasingly important, feasible, and prevalent. A salient principle for reasoning about infinite data types, such as infinite streams or trees, which are omnipresent in modern computer science, is *the principle of coinduction*. Nonetheless, despite intensive progress in recent years, practical frameworks that support coinductive reasoning remain a significant challenge, especially in the context of machine-checked formalization. In particular, current approaches either do not account well for the intuitive use of coinduction, or do not offer a natural account for the combination of coinduction and its dual principle of induction.

The overall aim of the proposed study is to develop a natural, concise formal framework that integrates coinductive reasoning in a way that captures its intuitive use and clearly reveals the duality between induction and coinduction. Specifically, we will devise a framework that is both minimal and amenable for automation, on the one hand, but that captures coinductive reasoning in an intuitive manner, on the other hand — thus providing a robust formal framework for coinductive reasoning. We will accomplish this task by combining two powerful frameworks: semantically, we will follow the approach of transitive closure logic, a generic logic for expressing inductive structures; for deduction, we will adopt non–well-founded (cyclic) proof theory. **The combination of the extended semantical framework of transitive closure logic, which allows sharing the same signature for both inductive and coinductive data, with cyclic proof theory, which describes the intuitive dynamics of (co)inductive reasoning, will provide a unique basis for a formal framework in which inductive and coinductive reasoning are captured as we intuitively understand and use them.**

In preliminary work, we extended transitive closure logic with a 'co-closure' operator and provided a cyclic proof system for the extended logic. The proposed research will build on that work and address the following specific objectives: (1) we will characterize the expressivity of the extended logic, focusing on its ability to capture 'applicable' coinductive definitions and to support complex (co)inductive structures and techniques; (2) we will perfect the cyclic proof system for the extended logic, study its structural proof theory, and use it to compare explicit and implicit (co)induction; and (3) equipped with a robust proof theory, we will integrate the resulting proof system into a theorem prover and investigate the practicalities of the framework, focusing on automated proof search and verification.

The proposed research will push forward the state-of-the-art in the formal treatment of coinduction. Leveraging the combination of non–well-founded proof methods and the minimal, intuitive notion of transitive closures is expected to have major implications for the provision of proof support for automated coinductive reasoning and to facilitate significant advances in proof search and verification.