Post-Doctoral Researcher Position – Research Program

Action Exploratoire (AEx) **IMPROOF** 2023

Porteur : Kaustuv Chaudhuri
Équipe-projet : PARTOUT
Centre : Saclay – Île-de-France

Background

Mainstream interactive theorem provers are designed with textual user interfaces that are nearly always mutually incompatible across systems. Even conceptually simple acts of formal reasoning such as composing lemmas or reasoning under quantifiers can be dramatically different from one system to the next. The IMPROOF project aims to find universal mechanisms for interactive proof development that are based on *direct manipulation* using rich user input devices such as mice, (multi-)touch screens, 3D graphical displays, virtual reality harnesses, etc. and to exploit the rich variety of interactive actions they enable to make interactive theorem proving easier for novices and powerful for experts.

Research Program

One of the main tasks of the IMPROOF project was enlarging the reach of direct manipulation to cover inductive and co-inductive reasoning, which forms the foundation of many modern theorem proving systems such as Coq, Isabelle/HOL, Lean, etc. Direct manipulation is itself based on *deep inference*, a style of proof representations where logical inferences are allowed to operate inside arbitrary formula contexts. Induction and co-induction remain largely unsolved in the deep inference framework.

The post-doctoral researcher will apply recent advances in the field of *cyclic proofs* for building human-comprehensible forms of (co-)inductive arguments. One immediate direction to explore is using *sized relations* as seen in the Abella theorem prover which uses syntactically guarded cycles to represent inductive arguments. The Actema implementation of direct manipulation can do some kinds of inductive reasoning on specific inductive types (such as natural numbers) by means of specific meanings given to user actions such as double-clicking. Another tantalizing possibility is to build inductive invariants in an incremental fashion by direct manipulation over *proof histories*.

Another important foundational direction is to consider the question of automatically deriving a direct manipulation interface from a *specification* of an object proof system. We already know that many proof systems can be specified as object theories in a *logical framework*, often using variants of *linear logic*. Direct manipulation is already known to work well on linear logic directly, so it would be interesting to test its compatibility with object logic specifications, and perhaps to design sufficient syntactic conditions that guarantee such a compatibility.

Finally, the researcher will also consider the issue of lemmas and proof libraries for specific theories. The direct manipulation prototypes that have so far been built have been tested only on simple examples without lemmas or theories. One possibility is to allow users to manipulate linkages between the current conjecture and (parts of) lemmas from existing libraries. Many proof systems already support a kind of search procedure that can query a library based on "formula patterns". With direct manipulation techniques, this automated search can be used as a filter: whenever the user indicates a subformula of the current conjecture as an endpoint of a link, the system can present the user with relevant lemmas that can immediately be used as the other endpoint of the link. For example, if the user indicates the a subterm $n + 0$ as the source of a link, the system will automatically present the lemma $\forall n,\ n + 0 = n$ as a potential link target on the side.

Candidate Profile

The candidate profile for this position is a recent PhD graduate who has worked on structural proof theory. The ideal candidate will have expertise with one or more deep inference formalisms, and will need to be broadly familiar with a variety of mathematical and computational logics. Familiarity with formal reasoning systems such as Coq, Lean, Isabelle/HOL, etc. is useful. Experience building prototype implementations of automated or interactive proof engines would also be highly relevant.

Duration

The duration of the position will be 12 months. (Extension beyond 12 months is possible with negotiation.)