


Review of Pablo Donato's doctoral dissertation *Deep Inference for Graphical Theorem Proving*

Nicolas Magaud (magaud@unistra.fr)
Professeur des Universités
Lab. ICube UMR 7357 CNRS Université de Strasbourg, France

Writing formal proofs in Interactive Theorem Provers (ITPs) such as Coq remains very technical and requires a high level of expertise. Indeed, the users have to master not only the scientific concepts (mathematics, computer science, physics, etc.) on which their proof relies, but also all the specific and sometimes intricate features of the logic implemented in their favorite ITP. Interfaces to develop proofs are usually rather basic and only provide minimal textual assistance for ITPs users.

Making proofs easier to achieve on a computer, especially through a comfortable and intuitive user interface, is useful both for beginners and for expert users. For beginners, it provides an enjoyable first experience and makes the proving process closer to pen-and-paper proofs. For expert users, it could significantly improve their productivity. Bringing (graphical) user interfaces for ITPs at the same level as in other fields of computer science is therefore unavoidable and is a key feature to speed up the adoption of proof assistants and make them a realistic alternative to pen-and-paper proofs in mathematics or computer science.

In his thesis, Pablo Donato deals with the issue of improving the way people interact with a proof assistant. He studies how to rely on a graphical interface rather than a textual one, introducing *graphical theorem proving*, especially through deep inference which allows to handle subformulas at an arbitrary depth in the goals.

The thesis is divided into 2 main parts: the first one deals with symbolic manipulations and explores the logical behavior of graphical actions whereas the second one deals with iconic manipulations and presents some original logical frameworks which aim at capturing the gestural approach to proof building from a proof theoretical perspective.

The first part of the thesis presents a prototype implementation (called Actema) of a graphical interface for theorem proving, which could replace the usual text-based approach used for about 30 years. For practical reasons and to be able to apply his ideas to several existing proof systems, Pablo focuses on first order logic. His work is inspired by the seminal work known as *proof by pointing* introduced by Bertot, Kahn and Théry and generalizes more recent work, namely *proof by linking*, initiated by Chaudhuri. Overall, Pablo names the approach that he follows *proof by action*. Indeed, he aims at replacing existing textual proof languages with gestural actions, which could be performed directly in a graphical user interface.

In Chap. 2, Pablo studies how both *click* and *drag-and-drop* (DnD) actions on some formulas of a sequent behave. It requires translating these actions into actual operations of the underlying logic, namely showing how to deal with logical connectives, universal and existential quantifications and equality. Pablo shows that deep inference allows to carry out more involved proof steps such as drag-and-drop actions through connectives, thus leading to elaborating more complex tactics in the background. In Chap. 3, the logical semantics of drag-and-drop actions are defined in the setting of deep inference proof theory. Following the subformula linking principles of Chaudhuri, he proposes to add a validity condition on linkages to avoid unproductive DnD actions. Under this condition, DnD actions are only permitted when the subformulas at stake are unifiable. In Chap. 4, Pablo shows, using three simple but carefully-chosen examples with an educational flavor, how actions can be used to carry out proofs. These three examples are representative of what can be achieved through the proof by action paradigm and deal with first-order logic, sets, relations and functions as well as Peano arithmetic. For each statement, the graphical proof by action comes together with an *equivalent* Coq proof script. It is worth noting that proof by action allows for both backward and forward reasoning, whereas common proof assistants usually strongly favor backward reasoning, making it hard to understand for beginners with little or no background in logic. In Chap. 5, Pablo advocates that an unusual feature in interactive theorem proving, namely multi-conclusion sequents, can be easily captured by the proof by action paradigm. He argues that direct manipulation through gestural actions makes it easy to deal with multiple conclusions, and introduces a new operator to model reasoning in classical logic that involves the interaction of several conclusions. Finally, in Chap. 6, Pablo explains how the proof-by-action principles can be implemented for first order logic as a web application (*Actema*). He also presents a prototype extension (*coq-actema*) to the Coq proof assistant, based on a plugin, which allows for direct manipulations of the proof state of Coq through gestural actions.

The second part of the thesis deals with iconic manipulations and explores new deep inference proof systems to give more structure to the notion of

goal. It consists in 4 chapters, one for each proposed system. These systems allow for both textual and graphical representations of the goals. The textual representation is well-suited for the backend of an ITP whereas the graphical representation, described in a so-callled *metaphorical notation* (bubbles or flowers) is well suited for direct manipulation and thus for the frontend of an ITP (its graphical user interface).

Chap. 7 and 8 introduce the Asymmetric and Symmetric Bubble Calculi, which are extensions of nested sequents and can be imagined as rewriting systems with a graphical interpretation. In Chap. 8, the concept (called the *metaphor* in the thesis) of bubbles and an associated calculus for intuitionistic logic (BJ) are introduced. They capture the separation and sharing of contexts between different subgoals. In Chap. 8, the calculus BJ is extended into a more general and symmetric calculus (B) for classical logic. A variant of this calculus, in which rules are all invertible (which is useful to ensure goals remain provable after each gestural action) is also proposed. In Chap. 9, existentials graphs, introduced by Pierce in the late nineteenth century/early twentieth century, are presented from an historical perspective and in a self-contained way, paving the way to Flower Calculus introduced in the next chapter. Existential graphs allow to achieve *full iconicity*, i.e. that every logical construction has an associated icon. Therefore, in this setting, connectives and qualifiers of symbolic formulas become useless.

The last chapter of this thesis (Chap. 10) introduces the principles of the Flower Calculus, a new proof system for intuitionistic predicate logic whose syntactic objects are called flowers. The Flower Calculus is the last of a sequence of calculi, inspired by Pierce's existentials graphs. Meta-theoretical properties of this new Calculus are investigated. Following the flowers metaphor, the system is splitted into a *natural* fragment (where every rule is analytic and invertible) and a *cultural* fragment (where every rule is non-invertible). Pablo shows the completeness of the natural fragment and uses this property to show that the cultural fragment is admissible. These meta-theoretical results are then put in practice to design the Flower Prover, a new Graphical User Interface which aims at unifying the notions of goal and theory. Goals are flowers, which are manipulated with the natural rules of the calculus whereas theories are the same flowers manipulated with the cultural rules. Finally, the author draws some perspectives, especially investigating how to ensure the proof seach procedure in this framework can be shown complete and terminating.

Overall this thesis presents not only some remarkable contributions to proof theory with a gestural-actions (i.e. graphical user interface) perspective but also some significant practical ones. Pablo proposes new original approaches to ease the interaction between humans and computers to carry out formal proofs. He also manages to describe them as formal calculi and to establish their expected meta-theoretical properties. In addition to the

theoretical contributions of this thesis, the author developed a large codebase and successfully implemented a realistic and usable graphical interface for ITPs (Actema) as well as a plugin to connect it to the Coq proof assistant (coq-actema). This is a very nice piece of software engineering, which combines advanced automated and/or interactive theorem proving technologies with web technologies.

In conclusion, I want to underline that the work achieved in this thesis is of paramount importance to make interactive theorem provers such as Coq easier and faster to adopt and use efficiently by newcomers, regardless of their initial level of expertise. Therefore I strongly support that the author of this very nice work be awarded *le grade de Docteur en informatique de l'Ecole Polytechnique*.

Strasbourg, April 24th 2024

Nicolas MAGAUD