Research Topic for the ParisTech/CSC PhD Program

Subfield: Computer Science and Mathematics

ParisTech School: MINES ParisTech

Title: Efficiency, Scalability and Interactivity for Rewriting at Higher-Order

Advisor(s): Frédéric Blanqui, Olivier Hermant, Emilio Gallego-Ariás
olivier.hermant@mines-paristech.fr, http://cri.ensmp.fr/people/hermant/
frederic.blanqui@inria.fr, http://rewriting.gforge.inria.fr/
emilio.gallego_arias@mines-paristech.fr

Short description of possible research topics for a PhD:

Computer-assisted proof verification has become a crucial tool to assist the development of safe software and protocols. We are developing Dedukti, a universal proof checker that allows to combine and verify proofs from various systems in a novel and convenient way. Dedukti is based on a logical framework extended with rewriting techniques, called deduction modulo theory. Our research thus range from extending the implementation of Dedukti to theoretical work on the formalism underneath, in consequence we propose research topics in this entire range, depending on the interests of the candidate.

On the implementation side, we propose to use the library Bindlib, developed in France, to get better rewriting performances, and to extend Dedukti towards rewriting modulo associativity-commutativity. We also plan to develop an interface for Dedukti by using SerAPI, developed at MINES ParisTech, and adopting an approach similar to jsCoq. One last step towards usability of Dedukti will be to implement proof tactics, so as to build interactive proofs.

We also propose topics, that make a bridge between theory and practice. As Dedukti is a logical framework, it is essential to ensure strong properties the system. This is why we would like to develop a termination checker to Dedukti, based on the Computability Path Ordering (CPO), developed at Inria. Another direction, that we are currently investigating is the development of refinement types, that is both a theoretical challenge and that would allow to develop interactive proofs in practice by "guessing" the proof-term, instead of asking the user for it. Lastly, we also are investigating new ways of computing, called normalization by evaluation, which is for the moment a theoretical work, but could at the same time lead to speedups in the implementation.

For more details, please refer to the webpages of the advisors, also do not hesitate to get in touch with them.

Required background of the student:

The main required background is a Master level in Computer Science or Mathematics.

An advanced course on the foundations of computer science/mathematics such as functional programming, logic, type theory, category theory would be a plus.

Representative publications of the group: (Related to the research topic)

Ronan Saillard, *Type Checking in the lambda-Pi Calculus modulo, Theory and Practice*, [http://www.cri.ensmp.fr/people/saillard/Files/thesis.pdf]

Gaëtan Gilbert, and Olivier Hermant, *Normalization by Completeness with Heyting Algebras*, In Logic for Programming, Aritificial Intelligence, and Reasoning, LPAR 2015. [http://www.cri.ensmp.fr/classement/doc/A-614.pdf]

Frédéric Blanqui, Jean-Pierre Jouannaud and A. Rubio, *The Computability Path Ordering*, in Logical Methods in Computer Science 11(4:3):1-45, 2015 [http://rewriting.gforge.inria.fr/lmcs15-pdf.html]

A. Asperti, W. Ricciotti, C. Sacerdoti Coen and E. Tassi, *A bi-directional refinement algorithm for the calculus of (co)inductive constructions*, in Logical Methods in Computer Science 8:1-49, 2012 [http://dx.doi.org/10.2168/LMCS-8(1:18)2012]

E. J. Gallego Arias, B. Pin, and P. Jouvelot, *jsCoq: towards hybrid theorem proving interfaces,* In Proceedings of the 12th Workshop on User Interfaces for Theorem Provers, Electronic Proceedings in Theoretical Computer Science, 2016. [http://feever.fr/Papers/jscoq.pdf]

A. Assaf, G. Burel, R. Cauderlier, D. Delahaye, G. Dowek, C. Dubois, F. Gilbert, P. Halmagrand, O. Hermant, and R. Saillard. *Expressing Theories in the lambda-Pi-Calculus Modulo Theory and in the Dedukti System,* 2016. Draft. [http://lsv.fr/~dowek/Publi/expressing.pdf]