



SCHOOL OF COMPUTER SCIENCE

Faculty Candidate Talk

Giselle Reis

Who watches the watchmen? - Trusting theorem provers

As theorem provers become increasingly efficient, their code-bases become more complicated, using sophisticated algorithms and optimizations that are rarely considered on the theoretical counter-part. Theoreticians are used to working with non-deterministic and inefficient proof-systems, and a number of decisions must be made upon implementing them. Sometimes, for the sake of efficiency, one needs even to give up completeness. Coupled with this is the fact that different theorem provers implement different calculi and, thus, produce different proof objects that cannot be understood but by a dedicated parser/interpreter.

In such scenario, we ask ourselves how to trust theorem provers. It is an overwhelming task and so far people have concentrated in developing a syntax for proof objects of a certain kind (SAT, resolution, SMT), or building bridges between pairs of theorem provers by translating the output of one into another (checking HOL proofs in Coq), or using other theorem provers to check parts of a proof (DVDV checker for TPTP).

Recent projects propose a more general and fundamental approach: define a framework for specifying semantics of proof objects. In this talk, I will speak about one of these approaches and our experience with the implementation of a proof checker.



Giselle Reis is a computer scientist with a tendency to mathematics who ended up in logic. She has graduated from her master's degree in Brazil and got her PhD at Vienna University of Technology, Austria. She is currently a post-doc at Inria, near Paris, France. Dr. Reis' research is in the area of proof theory. She is interested mainly in the use of logic as a tool for building more trustworthy software.

Friday, April 1
2:00 p.m. GHC 4405

Host: Robert Simmons