Report - Faculty Exchange Program

Carla Ferreira

15th Feb — 31st May and 1st Jul — 31st Jul
2011

Introduction

My participation in this program had two goals: a research collaboration with Prof. Frank Pfenning on combining refinement types and information flow types; and attending the graduate course Programming Language Semantics with Prof. Stephen Brooks. During my stay, I decided to attend two other courses as it is explained later.

Education

During my stay at CMU I attend three courses at distinct educational levels: an introduction to programming languages, a graduate course on language semantics, and an advanced course on Separation Logic.

Principles of Imperative Computation

Undergraduate course that teaches imperative programming and methods for ensuring the correctness of programs. I teach a similar course at Universidade Nova de Lisboa (UNL), so it was interesting to compare the CMU course program and teaching approaches with those of our course at UNL. The CMU course puts a strong emphasis on the formal definition of invariants and pre and post-conditions for methods, and therefore on program correctness. This has been reflected in the course at UNL, as now the students learn and use pre-conditions in the introductory course to programming languages.

Programming Language Semantics

Graduate course that presents mathematical framework for analyzing, specifying and reasoning about programming languages and the behavior of programs. I have lectured twice a similar PhD course, although with a more restricted program. Attending this course at CMU was very enlightening as not only it provided a comprehensive presentation of approaches to program semantics, but also addressed several program paradigms.

Current Research on Separation Logic

Advanced graduate course with the objective of studying and discussing recent papers on separation logic and related topics. This course is not related to any of my teaching activities, but I took the opportunity of being at CMU to learn more about separation logic. In this course John Reynolds covers most relevant papers on the subject, from its foundations to current developments.

Research

Regarding research, I worked with Frank Pfenning's group. My work was developed in the context the CMU-Portugal INTERFACES project and it builds on previous research developed in that project, namely on λ_{DB} a typeful language for defining access control policies in data centric systems. It is well known that access control does not guarantee that classified information is not leaked. Therefore, the objective of my work at CMU was to extend the approach of λ_{DB} to ensure information flow security. This research was concerned with combining refinement types and information flow types, based on the introduction of dynamic state indexed security monad. The objective was to develop typeful programming language for statically verifying information flow security. The main novelty of this approach is that security levels are represented by logical conditions and depend on the actual value contained in the variable. Therefore, those security levels are dynamic as they may change as the state evolves. This research work is continuing within INTERFACES project.