Visit of Philippa Gardner

Schedule for March 28th, 2017

14:00-16:30 Masterclass (room 26-00/101)

Short presentations by the PhD students. Each presentation (≈ 15 minutes) will be followed by an open discussion with Philippa Gardner (≈ 15 minutes).

14h00: Armaël Guéneau (Gallium team, Inria Paris)

Title: Formal proofs of asymptotic complexity of programs

Supervisors: Arthur Charguéraud, François Pottier

Abstract: I will present my progress on proving modular specifications about asymptotic complexity of higher-order imperative programs. Specifications are proved in a proof assistant, and expressed using higher-order separation logic. I will talk about formalising the $O()$ notation, in particular the multivariate case, and developing infrastructure for proving asymptotic costs.

14h30: Naomi Testard (Gallium team, Inria Paris)

Title: Towards proofs of programs with effect handlers, cooperative concurrency, and input/output

Supervisor: François Pottier

Abstract: In my PhD thesis, we're interested in specifying and verifying an OCaml library for cooperative concurrency. I'm implementing this library using a version of OCaml extended with algebraic effects, which lead us to determine reasoning rules in separation logic for this language. Finally, we think that cooperative concurrency is only useful in real-world programs when combined with input/output. Because of this, which means we are also interested in the specification of these features.

15h00: Lélio Brun (Parkas team, ENS – Inria Paris)

Title: Packing trees into C structs

Supervisor: Timothy Bourke, Marc Pouzet

Abstract: One way of compiling Lustre involves a translation pass from a simple imperative intermediary language to C. Thus it implies switching from a tree-shaped memory model to a memory model closer to the machine, with structs, addresses and offsets. In the context of a verified compiler, we have to find a way to relate the memory states between the source and target languages in order to prove the correctness of the compilation pass. We use separation logic to solve the issues that appears: aliasing, permissions, field overlapping.

15h30: Huisong Li (Antiques team, ENS – Inria Paris)

Title: Semantic-Directed Clumping of Disjunctive Abstract States

Supervisor: Xavier Rival

Abstract: To infer complex structural invariants, shape analyses rely on expressive families of logical properties. Many such analyses manipulate abstract memory states that consist of separating conjunctions of basic predicates describing atomic blocks or summaries. Moreover, they use finite disjunctions of abstract memory states in order to account for dissimilar shapes. Disjunctions should be kept small for scalability, though precision often requires keeping additional case splits. In this context, deciding when and how to merge case splits and to replace them with summaries is critical both for precision and efficiency. Existing techniques use sets of syntactic rules, which are tedious to design and prone to failure. In this work, we design a semantic criterion to clump abstract states based on their silhouette, which applies not only to the conservative union of disjuncts but also to the weakening of separating conjunctions of memory predicates into inductive summaries. Our approach allows us to define union and widening operators that aim at preserving the case splits that are required for the analysis to succeed. We implement this approach in the MemCAD analyzer and evaluate it on real-world C codes from existing libraries dealing with doubly-linked lists, red-black trees, AVL-trees and splay-trees.

16h00: Hugo Illous (Antiques team, CEA – ENS – Inria Paris)

Title: A relational shape abstract domain

Supervisor: Xavier Rival, Matthieu Lemerre

Abstract: We propose new logical connectives that extend separation logic to compute relations over input and output memory states of functions for programs manipulating shapes. These connectives can express that certain part of the memory was unchanged, freshly allocated, freed, or modified. We build an abstract domain over these connectives and design a static analysis that over approximates relations over memory states containing inductive structures.