Charge! a framework for higher-order separation logic in Coq.

Lars Birkedal

Department of Computer Science
Aarhus University
Aarhus, Denmark

Higher-order separation logic (HOSL) is an extension of separation logic that allows for quantification over predicates in both the assertion logic (the logic of pre- and post-conditions) and the specification logic (the logic of Hoare triples). Higher-order separation logic has proved useful for modular reasoning about programs that use shared mutable data structures and data abstraction, via quantification over resource invariants, and for reasoning about various forms of higher-order programming (higher-order functions, code pointers, interfaces in object-oriented programming).

In this talk I will describe our work on Charge!, a separation-logic verification tool implemented in Coq, that aims to

1. prove full functional correctness of Java-like programs using higher-order separation logic,
2. produce machine-checkable correctness proofs,
3. work as close as possible to how informal separation logic proofs are carried out on pen and paper, and
4. automate tedious first-order reasoning where possible.

Joint work with Jesper Bengtson, Jonas B. Jensen, Hannes Mehnert, Peter Sestoft, and Filip Sieczkowski.