Carnegie Mellon University
Computer Science Department

THESIS ORAL

JOSEPH TASSAROTTI

Verifying Concurrent Randomized Algorithms

Thursday, December 20, 2018 – 9:00 a.m. – GHC 8102

Concurrency and randomization are difficult to use correctly when programming. Because programs that use them no longer behave deterministically, programmers must take into account the set of all possible interactions and random choices that may occur. This dissertation describes a logic for reasoning about programs using both of these effects. The logic extends a recent concurrent separation logic with ideas from denotational semantics for probabilistic and non-deterministic choice, along with principles for probabilistic relational reasoning originally developed for sequential programs. The resulting logic is used to verify probabilistic behaviors of a randomized concurrent counter algorithm and a two-level concurrent skip list. The soundness of the logic, as well as the proofs of these examples, have been mechanized in Coq.

Thesis Committee:
Robert Harper, Chair
Jan Hoffmann
Jeremy Avigad
Derek Dreyer, MPI-SWS