

Invited Talk

Separation Logic and Concurrent Resource Management

Peter O'Hearn

Queen Mary, University of London
ohearn@dcs.qmul.ac.uk

Abstract

Concurrent separation logic provides a way of reasoning about the usage of resources in concurrent programs. Proofs in the logic track the transfer of ownership of portions of memory between concurrent processes, mirroring design principles for concurrent systems programs. This allows the safe treatment of "daring" concurrent programs, that access shared memory without explicit protection, outside of critical sections; canonical examples of such daring concurrency are resource managers of various kinds.

In this talk I will describe the underpinnings of the concurrent separation logic, and illustrate it with experimental tools -- SMALLFOOT and SPACE INVADER -- that are being developed to do automatic proofs with the logic.