Framing is important for specification and verification of object-oriented programs. This dissertation develops the local reasoning approach for framing in the presence of data structures with unrestricted sharing and subtyping. It can verify shared data structures specified in a concise way by unifying fine-grained region logic and separation logic. Then the fine-grained region logic is extended to reason about subtyping.

First, fine-grained region logic is adapted from region logic to express regions at the granularity of individual fields. Conditional region expressions are introduced; not only does this allow one to specify more precise frame conditions, it also has the ability to express footprints of separation logic assertions.

Second, fine-grained region logic is generalized to a new logic called unified fine-grained region logic by allowing the logic to restrict the heap in which a program runs. This feature allows one to express specifications in separation logic.

Third, both fine-grained region logic and separation logic can be encoded to unified fine-grained region logic. This result allows the proof system to reason about programs specified in both styles.

Finally, fine-grained region logic is extended to reason about a programming language that is similar to Java. To reason about inheritance locally, a frame condition for behavioral subtyping is defined and proved sound.

Major: Computer Science

Educational Career:
Bachelor's of Computer Science, BS, 2003, Beijing University of Technology
Master's of Software Engineering, MS, 2007, Beihang University

Committee in Charge:
Gary T. Leavens, Chair, Computer Science
Damian Dechev, University of Central Florida
Sumit Jha, University of Central Florida
Mason Cash, University of Central Florida
David Naumann, Stevens Institute of Technology

Approved for distribution by Gary T. Leavens, Committee Chair, on October 15, 2017.

The public is welcome to attend.