

# Separation Logic

Gregory M. Malecha

January 23, 2008

Based on recent research presented at POPL'08 [PB08, CDNQ08, BBC08] and Morrisett's work [MPBN07], I feel that a solid understanding of logic is required for developing more sophisticated systems. One common part of this logic is the topic of *separation logic*.

## 1 Goals

Separation logic is an extension to Hoare logic which helps to reason about data structures on the heap [Wik07]. The goal is to separate the heap into disjoint regions which can be reasoned about independently. Current uses of separation logic seem to focus on describing abstraction.

During the semester one of my presentations will be focused around material which is closely related to the field, namely Morrisett's work on Hoare Type Theory [MPBN07]. For my project, I propose a tutorial covering separation logic in particular with respect to its applications in system analysis.

## 2 Brief Overview & Applications

Separation logic accomplishes its goals through the introduction of several operators [Par] which I hope the learn more about through this work.

$$S, H \models E \mapsto E' \iff \text{dom}(H) = \{|E|_S\} \vee H(|E|_S) = |E'|_S$$

$$S, H \models P * Q \iff \exists H_1, H_2. (H_1 \perp H_2) \vee (H_1 \circ H_2 = H) \vee (S, H_1 \models P) \vee (S, H_2 \models Q)$$

$$S, H \models P * Q \iff \forall H'. (H \perp H') \vee (S, H' \models P) \Rightarrow S, H \circ H' \models Q$$

Where  $|E|_S$  denotes the evaluation of expression  $E$  in the stack  $S$  and  $H$  corresponds to the heap.

Two small example applications which I have found interesting are:

**Memory Management** Tracking memory allocation without the need to reason about the details of the memory allocation system.

**List/Tree Traversal** Freeing the contents of a linked list [Par] or binary tree and performing operations such as the reverse of a list.

## References

- [BBC08] James Brotherston, Richard Bornat, and Cristiano Calcagno. Cyclic proofs of program termination in separation logic. In *POPL*, 2008. Available from: [http://www.doc.ic.ac.uk/~jbrother/slides/oxford\\_06\\_07.pdf](http://www.doc.ic.ac.uk/~jbrother/slides/oxford_06_07.pdf).
- [CDNQ08] Wei-Ngan Chin, Cristina David, Huu Hai Nguyen, and Shengchao Qin. Enhancing modular oo verification with separation logic. In *POPL*, 2008. Available from: <https://www.dur.ac.uk/shengchao.qin/papers/popl08.pdf>.
- [MPBN07] Greg Morrisett, R. L. Peterson, L. Birkedal, and A. Nanevski. A realizability model for impredicative hoare type theory. In *POPL*, 2007. Available from: <http://www.itu.dk/people/rusmus/articles/HTTmodel.pdf>.
- [Par] Matthew Parkinson. Separation logic [online]. Available from: <http://www.cl.cam.ac.uk/~mjp41/IntroSep.pdf>.
- [PB08] Matthew J. Parkinson and Gavin M. Bierman. Separation logic, abstraction and inheritance. In *POPL*, 2008. Available from: <http://www.cl.cam.ac.uk/~mjp41/SeplogicInherit.pdf>.
- [Wik07] Wikipedia. Separation logic [online]. October 2007. Available from: [http://en.wikipedia.org/wiki/Separation\\_logic](http://en.wikipedia.org/wiki/Separation_logic).