Lectures on Separation Logic

Peter O'Hearn
Queen Mary, University of London, United Kingdom

Separation logic is an extension of Hoare's logic for reasoning about programs that mutate data held in computer memory. Its assertion language extends classical logic with a separating conjunction operator $A * B$, which asserts that A and B hold for separate portions of memory.

In the first lecture I will first cover the basics of the logic [1, 2].

(i) The separating conjunction fits together with inductive definitions in a way that supports natural descriptions of mutable data structures.

(ii) Axiomatizations of pointer operations support *in-place reasoning*, where a portion of a formula is updated in place when passing from precondition to postcondition, mirroring the operational locality of heap update.

(iii) Frame axioms, which state what does not change, can be avoided when writing specifications.

These points together enable specifications and proofs for programs that alter data structures that are simpler than was possible previously.

After the basic part I will will give a lecture on semantic foundations. Using a model theoretic perspective [3-5], I will attempt to describe the extent to which separation logic's "benefits"do and do not depend on its language of assertions. The later lectures will move on to concurrency and to mechanized verification, in particular the use of the logic in proof via symbolic execution and static program analysis (e.g. [6-10]).

References

[1] P. W. O'Hearn, J. Reynolds, H. Yang. *Local Reasoning about Programs that alter Data Structures.* 15th CSL, pp.1-19, 2001.

[2] J. C. Reynolds. *Separation Logic: A Logic for Shared Mutable Data Structures.* 17th LICS, pp.55-74, 2002.

[3] P. W. O'Hearn, D. J. Pym. *The Logic of Bunched Implications.* Bulletin of Symbolic Logic, 5(2), pp.215-244, 1999.

[4] S. Isthiaq, P. W. O'Hearn. *BI as an Assertion Language for Mutable Data Structures.* 28th POPL, pp. 36-49, 2001.

[5] C. Calcagno, P. W. O'Hearn, H. Yang. *Local Action and Abstract Separation Logic.* LICS'07, pp. 366-378, 2007

[6] J. Berdine, C. Calcagno, P. W. O'Hearn. *Smallfoot: Automatic Modular Assertion Checking with Separation Logic.* 4th FMCO, pp. 115-137, 2006.

[7] D. Distefano, M. Parkinson. *jStar: Towards Practical Verification for Java.* OOPSLA, 2008.

[8] D. Distefano, P. W. O'Hearn, H. Yang. *A Local Shape Analysis based on Separation Logic* 12th TACAS, pp. 287-302, 2006.

[9] H. Yang, O. Lee, J. Berdine, C. Calcagno, B. Cook, D. Distefano, P. W. O'Hearn. *Scalable Shape Analysis for Systems Code.* 20th CAV, 2008.

[10] C. Calcagno, D. Distefano, P. W. O'Hearn, H. Yang. *Compositional Shape Analysis by Means of Bi-abduction.* 36th POPL, pp. 289-300, 2009.