Separation Logic
A Logic for Shared Data and Local Reasoning

John Reynolds
Carnegie Mellon University, Pittsburgh, USA

Separation logic, originally developed by OÕHearn and Reynolds [1], is an extension of Hoare logic originally intended for reasoning about programs that use shared mutable data structures. It was based on the concept of separating conjunction, which permits the concise expression of aliasing con- straints.

The logic also includes a "frame rule", which enables local reasoning that is the key to the scalability of proofs. Examples of nontrivial proofs include the Schorr-Waite marking algorithm [2] and the Cheney relocating garbage collector [3].

More recently, by generalizing the concept of storage access to owner- ship and permissions, the logic has been extended to encompass information hiding [4], shared-variable concurrency [5], and numerical permissions [6].

We will survey the current development of separation logic, including, as time permits, extensions to unrestricted address arithmetic, dynamically allocated arrays, recursive procedures, shared-variable concurrency, and read- only sharing. We will also discuss promising future directions.

References

1. J.C. Reynolds. *Separation logic: A Logic for Shared Mutable Data Structures.* In Proc 17th Annual IEEE Symposium on Logic in Computer Science; pp 55–74; IEEE Computer Society; 2002.

2. H. Yang. *An Example of Local Reasoning in BI Pointer Logic: The Schorr-Waite Graph Marking Algorithm.* Informal Proc of the Workshop on Semantics, Program Analysis and Computing Environments for Memory Management (SPACE 2001); F. Henglein, J. Hughes, H. Makholm, and H. Niss (eds); pp 41–68; IT University of Copenhagen; 2001.

3. L. Birkedal, N. Torp-Smith, and J.C. Reynolds. *Local Reasoning about a Copying Garbage Collector.* In Proc of the 31st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'04); pp 220–231; ACM Press; 2004. (*A revised version will appear in the ACM Transactions on Programming Languages and Systems.*)

4. P.W. O'Hearn, H. Yang, and J.C. Reynolds. *Separation and Information Hiding.* In Proc of the 31st ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'04); pp 268–280; ACM Press; 2004.

5. P.W. O'Hearn. *Resources, Concurrency and Local Reasoning.* In Proc of the 15th International Conference on "Concurrency Theory" (CONCUR'04); LNCS 3170, pp 49–67; Springer; 2004.

6. R. Bornat, C. Calcagno, P.W. O'Hearn, and M.Parkinson. *Permission Accounting in Separation Logic.* In Proc of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL'05); pp 259–270; ACM Press; 2005.