PROGRAM LOGICS FOR CERTIFIED COMPILERS

ANDREW W. APPEL
Princeton University, Princeton, New Jersey

ROBERT DOCKINS
Portland State University, Portland, Oregon

AQUINAS HOBOR
National University of Singapore and Yale/NUS College, Singapore

LENNART BERINGER
Princeton University, Princeton, New Jersey

JOSIAH DODDS
Princeton University, Princeton, New Jersey

GORDON STEWART
Princeton University, Princeton, New Jersey

SANDRINE BLAZY
Université de Rennes 1

XAVIER LEROY
INRIA Paris-Rocquencourt
Contents

Road map ix
Acknowledgments x
1 Introduction 1

I  Generic separation logic 9
2 Hoare logic 10
3 Separation logic 16
4 Soundness of Hoare logic 25
5 Mechanized Semantic Library 33
6 Separation algebras 35
7 Operators on separation algebras 44
8 First-order separation logic 49
9 A little case study 55
10 Covariant recursive predicates 63
11 Share accounting 69

II Higher order separation logic 75
12 Separation logic as a logic 76
13 From separation algebras to separation logic 84
14 Simplification by rewriting 89
15 Introduction to step-indexing 94
16 Predicate implication and subtyping 99
17 General recursive predicates 104
18 Case study: Separation logic with first-class functions 111
Road map

Readers interested in the theory of separation logic (with some example applications) should read Chapters 1–21. Readers interested in the use of separation logic to verify C programs should read Chapters 1–6 and 8–30. Those interested in the theory of step-indexing and indirection theory should read Chapters 35–39. Those interested in building models of program logics proved sound for certified compilers should read Chapters 40–47, though it would be helpful to read Chapters 1–39 as a warm-up.