
Contents

Part I Isabelle

1	Introduction	3
2	Programming and Proving	5
2.1	Basics	5
2.2	Types <i>bool</i> , <i>nat</i> and <i>list</i>	7
2.3	Type and Function Definitions	15
2.4	Induction Heuristics	19
2.5	Simplification	21
3	Case Study: IMP Expressions	27
3.1	Arithmetic Expressions	27
3.2	Boolean Expressions	32
3.3	Stack Machine and Compilation	35
4	Logic and Proof Beyond Equality	37
4.1	Formulas	37
4.2	Sets	38
4.3	Proof Automation	39
4.4	Single Step Proofs	42
4.5	Inductive Definitions	45
5	Isar: A Language for Structured Proofs	53
5.1	Isar by Example	54
5.2	Proof Patterns	56
5.3	Streamlining Proofs	58
5.4	Case Analysis and Induction	61

Part II Semantics

6	Introduction	73
7	IMP: A Simple Imperative Language	75
7.1	IMP Commands	75
7.2	Big-Step Semantics	77
7.3	Small-Step Semantics	85
7.4	Summary and Further Reading	90
8	Compiler	95
8.1	Instructions and Stack Machine	95
8.2	Reasoning About Machine Executions	98
8.3	Compilation	99
8.4	Preservation of Semantics	102
8.5	Summary and Further Reading	112
9	Types	115
9.1	Typed IMP	117
9.2	Security Type Systems	128
9.3	Summary and Further Reading	140
10	Program Analysis	143
10.1	Definite Initialization Analysis	145
10.2	Constant Folding and Propagation	154
10.3	Live Variable Analysis	164
10.4	True Liveness	172
10.5	Summary and Further Reading	178
11	Denotational Semantics	179
11.1	A Relational Denotational Semantics	180
11.2	Summary and Further Reading	188
12	Hoare Logic	191
12.1	Proof via Operational Semantics	191
12.2	Hoare Logic for Partial Correctness	192
12.3	Soundness and Completeness	203
12.4	Verification Condition Generation	208
12.5	Hoare Logic for Total Correctness	212
12.6	Summary and Further Reading	215

13 Abstract Interpretation 219

 13.1 Informal Introduction 220

 13.2 Annotated Commands 224

 13.3 Collecting Semantics 225

 13.4 Abstract Values 236

 13.5 Generic Abstract Interpreter 241

 13.6 Executable Abstract States 253

 13.7 Analysis of Boolean Expressions 259

 13.8 Interval Analysis 264

 13.9 Widening and Narrowing 270

 13.10 Summary and Further Reading 279

A Auxiliary Definitions 281

B Symbols 283

C Theories 285

References 287

Index 293



<http://www.springer.com/978-3-319-10541-3>

Concrete Semantics

With Isabelle/HOL

Nipkow, T.; Klein, G.

2014, XIII, 298 p. 87 illus., 1 illus. in color., Hardcover

ISBN: 978-3-319-10541-3