

Contents

1	Introduction	1
1.1	Formal Methods	1
1.2	The History of B	8
1.3	The Relationship of B to Other Formal Methods	11
1.4	Summary	13
2	The Foundations of B AMN	15
2.1	Mathematical Notation	15
2.2	Defining Operations	20
2.3	Abstract Machines	29
2.4	Machine Composition Mechanisms	41
2.5	Refinement	47
2.6	Implementation	54
2.7	Summary	73
2.8	Exercises 1	74
3	Analysis and Specification	77
3.1	Requirements Analysis	77
3.2	Specification Development	78
3.3	Animation	109
3.4	Proof of Internal Consistency Obligations	110
3.5	Ship Loading Case Study – Specification	112
3.6	Renaming	116
3.7	Aggregation	117
3.8	Summary	118
3.9	Exercises 2	119
4	Design and Implementation	124
4.1	The Layered Development Paradigm	125
4.2	Refinement Examples	129
4.3	Proofs of Refinement	144

4.4	Decomposing Implementations	147
4.5	Ship Loading Case Study – Implementation	149
4.6	Summary	155
4.7	Exercises 3	156
5	Case Studies	157
5.1	Personnel System Development	157
5.2	Mine Pump Control	172
5.3	Vending Machine	183
6	Conclusions	195
A	Exercise Solutions	203
A.1	Exercises 1	203
A.2	Exercises 2	206
A.3	Exercises 3	210
B	Properties of Weakest Preconditions	214
B.1	Termination and Feasibility	216
B.2	Set-theoretic Semantics	218
B.3	Refinement	219
B.4	Well-formedness Obligations	221
B.5	Normal Forms	222
B.6	Rules for $ $	223
B.7	Definition of $:=$	223
C	Proof Techniques	225