CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

Contents

I Mathematics 1

1 Mathematical Reasoning 3

1.1 Formal Reasoning 4
1.1.1 Sequent and Predicate 4
1.1.2 Rule of Inference 5
1.1.3 Proofs 6
1.1.4 Basic Rules 6
1.2 Propositional Calculus 9
1.2.1 The Notation of Elementary Assertions 9
1.2.2 Inference Rules for Propositional Calculus 11
1.2.3 Some Proofs 14
1.2.4 A Proof Procedure 22
1.2.5 Extending the Notation 26
1.2.6 Some Classical Results 27
1.3 Predicate Calculus 29
1.3.1 The Notation of Quantified Predicates and Substitutions 29
1.3.2 Universal Quantification 32
1.3.3 Non-freeness 32
1.3.4 Substitution 34
1.3.5 Inference Rules for Predicate Calculus 35
1.3.6 Some Proofs 36
1.3.7 Extending the Proof Procedure 38
1.3.8 Existential Quantification 39
1.3.9 Some Classical Results 41
1.4 Equality 42
1.5 Ordered Pairs 47
1.6 Exercises 51

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

2 Set Notation 55

2.1 Basic Set Constructs 56
2.1.1 Syntax 57
2.1.2 Axioms 60
2.1.3 Properties 62
2.2 Type-checking 64
2.3 Derived Constructs 72
2.3.1 Definitions 72
2.3.2 Examples 72
2.3.3 Type-checking 73
2.3.4 Properties 75
2.4 Binary Relations 77
2.4.1 Binary Relation Constructs: First Series 77
2.4.2 Binary Relation Constructs: Second Series 79
2.4.3 Examples of Binary Relation Constructs 82
2.4.4 Type-checking of Binary Relation Constructs 84
2.5 Functions 85
2.5.1 Function Constructs: First Series 86
2.5.2 Function Constructs: Second Series 89
2.5.3 Examples of Function Constructs 90
2.5.4 Properties of Function Evaluation 90
2.5.5 Type-checking of Function Constructs 93
2.6 Catalogue of Properties 94
2.6.1 Membership Laws 95
2.6.2 Monotonicity Laws 96
2.6.3 Inclusion Laws 97
2.6.4 Equality Laws 99
2.7 Example 115
2.8 Exercises 120

3 Mathematical Objects 123

3.1 Generalized Intersection and Union 123
3.2 Constructing Mathematical Objects 130
3.2.1 Informal Introduction 130
3.2.2 Fixpoints 131
3.2.3 Induction Principle 136
3.3 The Set of Finite Subsets of a Set 141
3.4 Finite and Infinite Sets 144
3.5 Natural Numbers 145
3.5.1 Definition 145
3.5.2 Peano's "Axioms" 148
3.5.3 Minimum 153
3.5.4 Strong Induction Principle 156
3.5.5 Maximum 158

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

3.5.6 Recursive Functions on Natural Numbers 158
3.5.7 Arithmetic 161
3.5.8 Iterate of a Relation 166
3.5.9 Cardinal of a Finite Set 167
3.5.10 Transitive Closures of a Relation 168
3.6 The Integers 170
3.7 Finite Sequences 174
3.7.1 Inductive Construction 174
3.7.2 Direct Construction 176
3.7.3 Operations on Sequences 177
3.7.4 Sorting and Related Topics 182
3.7.5 Lexicographical Order on Sequences of Integers 187
3.8 Finite Trees 188
3.8.1 Informal Introduction 188
3.8.2 Formal Construction 190
3.8.3 Induction 192
3.8.4 Recursion 194
3.8.5 Operations 197
3.8.6 Representing Trees 199
3.9 Labelled Trees 202
3.9.1 Direct Definition 203
3.9.2 Inductive Definition 203
3.9.3 Induction 205
3.9.4 Recursion 206
3.9.5 Operations Defined Recursively 206
3.9.6 Operations Defined Directly 208
3.10 Binary Trees 208
3.10.1 Direct Operations 209
3.10.2 Induction 209
3.10.3 Recursion 210
3.10.4 Operations Defined Recursively 210
3.11 Well-founded Relations 211
3.11.1 Definition 212
3.11.2 Proof by Induction on a Well-founded Set 213
3.11.3 Recursion on a Well-founded Set 214
3.11.4 Proving Well-foundedness 217
3.11.5 An Example of a Well-founded Relation 219
3.11.6 Other Examples of Non-classical Recursions 219
3.12 Exercises 221

II Abstract Machines 225

4 Introduction to Abstract Machines 227

4.1 Abstract Machines 228
4.2 The Statics: Specifying the State 229

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

4.3 The Dynamics: Specifying the Operations 230
4.4 Before-after Predicates as Specifications 231
4.5 Proof Obligation 232
4.6 Substitutions as Specifications 232
4.7 Pre-conditioned Substitution (Termination) 234
4.8 Parameterization and Initialization 236
4.9 Operations with Input Parameters 238
4.10 Operations with Output Parameters 240
4.11 Generous versus Defensive Style of Specification 241
4.12 Multiple Simple Substitution 243
4.13 Conditional Substitution 244
4.14 Bounded Choice Substitution 244
4.15 Guarded Substitution (Feasibility) 246
4.16 A Substitution with no Effect 247
4.17 Contextual Information: Sets and Constants 248
4.18 Unbounded Choice Substitution 252
4.19 Explicit Definitions 256
4.20 Assertions 260
4.21 Concrete Variables and Abstract Constants 261
4.22 Exercises 262

5 Formal Definition of Abstract Machines 265

5.1 Generalized Substitution 265
5.1.1 Syntax 265
5.1.2 Type-checking 270
5.1.3 Axioms 271
5.2 Abstract Machines 272
5.2.1 Syntax 272
5.2.2 Visibility Rules 274
5.2.3 Type-checking 275
5.2.4 On the Constants 278
5.2.5 Proof Obligations 278
5.2.6 About the Given Sets and the Pre-defined Constants 280

6 Theory of Abstract Machines 283

6.1 Normalized Form 283
6.2 Two Useful Properties 287
6.3 Termination, Feasibility and Before-after Predicate 288
6.3.1 Termination 289
6.3.2 Feasibility 290
6.3.3 Before-after Predicate 292
6.4 Set-Theoretic Models 295
6.4.1 First Model: a Set and a Relation 295
6.4.2 Second Model: Set Transformer 298
6.4.3 Set-theoretic Interpretations of the Constructs 301

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

6.5 Exercises 303

7 Constructing Large Abstract Machines 307

7.1 Multiple Generalized Substitution 307
7.1.1 Definition 308
7.1.2 Basic Properties 308
7.1.3 The Main Result 311
7.2 Incremental Specification 312
7.2.1 Informal Introduction 312
7.2.2 Operation Call 314
7.2.3 The INCLUDES Clause 316
7.2.4 Visibility Rules 318
7.2.5 Transitivity 319
7.2.6 Machine Renaming 320
7.2.7 The PROMOTES and the EXTENDS Clauses 320
7.2.8 Example 320
7.3 Incremental Specification and Sharing 322
7.3.1 Informal Introduction 322
7.3.2 The USES Clause 323
7.3.3 Visibility Rules 324
7.3.4 Transitivity 324
7.3.5 Machine Renaming 325
7.4 Formal Definition 325
7.4.1 Syntax 325
7.4.2 Type-checking 326
7.4.3 Proof Obligations for the INCLUDES Clause 331
7.4.4 Proof Obligations for the USES Clause 334
7.5 Exercises 336

8 Examples of Abstract Machines 337

8.1 An Invoice System 338
8.1.1 Informal Specification 338
8.1.2 The *Client* Machine 339
8.1.3 The *Product* Machine 341
8.1.4 The *Invoice* Machine 343
8.1.5 The *Invoice_System* Machine 348
8.2 A Telephone Exchange 349
8.2.1 Informal specification 349
8.2.2 The *Simple_Exchange* Machine 352
8.2.3 The *Exchange* Machine 355
8.3 A Lift Control System 358
8.3.1 Informal Specification 358
8.3.2 The *Lift* Machine 358
8.3.3 Liveness Proof 364
8.3.4 Expressing Liveness Proof Obligations 366

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

8.4 Exercises 369

III Programming 371

9 Sequencing and Loop 373

9.1 Sequencing 374
9.1.1 Syntax 374
9.1.2 Axiom 374
9.1.3 Basic Properties 374
9.2 Loop 377
9.2.1 Introduction 377
9.2.2 Definition 378
9.2.3 Interpretation of Loop Termination 382
9.2.4 Interpretation of the Before-after Relation of the Loop 385
9.2.5 Examples of Loop Termination 386
9.2.6 The Invariant Theorem 387
9.2.7 The Variant Theorem 388
9.2.8 Making the Variant and Invariant Theorem Practical 390
9.2.9 The Traditional Loop 392
9.3 Exercises 398

10 Programming Examples 403

10.0 Methodology 403
10.0.1 Re-use of Previous Algorithms 403
10.0.2 Loop Proof Rules 406
10.0.3 Sequencing Proof Rule 407
10.1 Unbounded Search 408
10.1.1 Introduction 408
10.1.2 Comparing two Sequences 411
10.1.3 Computing the Natural Number Inverse of a Function 416
10.1.4 Natural Number Division 420
10.1.5 The Special Case of Recursive Functions 422
10.1.6 Logarithm in a Given Base 424
10.1.7 Integer Square Root 425
10.2 Bounded Search 427
10.2.1 Introduction 427
10.2.2 Linear Search 430
10.2.3 Linear Search in an Array 431
10.2.4 Linear Search in a Matrix 433
10.2.5 Binary Search 435
10.2.6 Monotonic Functions Revisited 437
10.2.7 Binary Search in an Array 442
10.3 Natural Number 446
10.3.1 Basic Scheme 446
10.3.2 Natural Number Exponentiation 447

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

10.3.3 Extending the Basic Scheme 448
10.3.4 Summing a Sequence 450
10.3.5 Shifting a Sub-sequence 451
10.3.6 Insertion into a Sorted Array 453
10.4 Sequences 455
10.4.1 Introduction 455
10.4.2 Accumulating the Elements of a Sequence 458
10.4.3 Decoding the Based Representation of a Number 461
10.4.4 Transforming a Natural Number into its Based Representation 462
10.4.5 Fast Binary Operation Computations 465
10.4.6 Left and Right Recursion 469
10.4.7 Filters 473
10.5 Trees 482
10.5.1 The Notion of Formula 483
10.5.2 Transforming a Tree into a Formula 484
10.5.3 Transforming a Tree into a Polish String 487
10.5.4 Transforming a Formula into a Polish String 488
10.6 Exercises 496

IV Refinement 499

11 Refinement 501

11.1 Refinement of Generalized Substitutions 501
11.1.1 Informal Approach 501
11.1.2 Definition 503
11.1.3 Equality of Generalized Substitution 503
11.1.4 Monotonicity 504
11.1.5 Refining a Generalized Assignment 506
11.2 Refinement of Abstract Machines 507
11.2.1 Informal Approach 507
11.2.2 Formal Definition 511
11.2.3 Sufficient Conditions 512
11.2.4 Monotonicity 516
11.2.5 Example Revisited 522
11.2.6 The Final Touch 523
11.2.7 An Intuitive Explanation of the Refinement Condition 530
11.2.8 Application to the Little Example 532
11.3 Formal Definition 533
11.3.1 Syntax 533
11.3.2 Type-checking 534
11.3.3 Proof Obligations 537
11.4 Exercises 540

12 Constructing Large Software Systems 551

12.1 Implementing a Refinement 551

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

12.1.1 Introduction 551
12.1.2 The Practice of Importation 556
12.1.3 The IMPLEMENTATION Construct 559
12.1.4 The IMPORTS Clause 561
12.1.5 Visibility Rules 561
12.1.6 Machine Renaming 563
12.1.7 The VALUES Clause 563
12.1.8 Comparing the IMPORTS and the INCLUDES Clauses 565
12.1.9 The PROMOTES and EXTENDS Clauses 565
12.1.10 Concrete Constants and Concrete Variables Revisited 566
12.1.11 Allowed Constructs in an Implementation 566
12.2 Sharing 574
12.2.1 Introduction 574
12.2.2 The SEES Clause 579
12.2.3 Visibility Rules 579
12.2.4 Transitivity and Circularity 583
12.2.5 Machine Renaming 583
12.2.6 Comparing the USES and the SEES Clauses 583
12.3 Loops Revisited 584
12.4 Multiple Refinement and Implementation 584
12.5 Recursively Defined Operations 587
12.5.1 Introduction 588
12.5.2 Syntax 591
12.5.3 Proof Rule 591
12.6 Formal Definition 594
12.6.1 Syntax of an IMPLEMENTATION 594
12.6.2 Type-checking with an IMPORTS Clause 595
12.6.3 Type-checking with a SEES Clause 596
12.6.4 Proof Obligations of an IMPLEMENTATION 597
12.6.5 Proof Obligation for a SEES Clause 601

13 Examples of Refinements 603

13.1 A Library of Basic Machines 603
13.1.1 The *BASIC_CONSTANTS* Machine 604
13.1.2 The *BASIC_IO* Machine 604
13.1.3 The *BASIC_BOOL* Machine 605
13.1.4 The *BASIC_enum* Machine for Enumerated Sets 606
13.1.5 The *BASIC_FILE_VAR* Machine 607
13.2 Case Study: Data-base System 608
13.2.1 Machines for Files 611
13.2.2 Machines for Objects 623
13.2.3 A Data-base 630
13.2.4 Interfaces 637
13.3 A Library of Useful Abstract Machines 647
13.3.1 The *ARRAY_VAR* Machine 647

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

13.3.2 The *SEQUENCE_VAR* Machine 647
13.3.3 The *SET_VAR* Machine 647
13.3.4 The *ARRAY_COLLECTION* Machine 648
13.3.5 The *SEQUENCE_COLLECTION* Machine 648
13.3.6 The *SET_COLLECTION* Machine 650
13.3.7 The *TREE_VAR* Machine 650
13.4 Case Study: Boiler Control System 655
13.4.1 Introduction 655
13.4.2 Informal Specification 656
13.4.3 System Analysis 661
13.4.4 System Synthesis 673
13.4.5 Formal Specification and Design 676
13.4.6 Final Architecture 693
13.4.7 Modifying the Initial Specification 694
Appendix A **Summary of Notations** 701
A.1 Propositional Calculus 701
A.2 Predicate Calculus 702
A.3 Equality and Ordered Pairs 702
A.4 Basic and Derived Set Constructs 702
A.5 Binary Relations 703
A.6 Functions 705
A.7 Generalized Intersection and Union 706
A.8 Finiteness 706
A.9 Natural Numbers 707
A.10 Integers 709
A.11 Finite Sequences 711
A.12 Finite Trees 713
Appendix B **Syntax** 715
B.1 Predicate 715
B.2 Expression 716
B.3 Substitution 716
B.4 Machine 717
B.5 Refinement 719
B.6 Implementation 720
B.7 Statement 721
Appendix C **Definitions** 725
C.1 Logic Definitions 725
C.2 Basic Set-theoretic Definitions 726
C.3 Binary Relation Definitions 726
C.4 Function Definitions 728
C.5 Fixpoint Definitions 728
C.6 Finiteness Definitions 729
C.7 Natural Number Definitions 730
C.8 Integer Extensions 732
C.9 Finite Sequence Definitions 734

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521021758 - The B-Book: Assigning Programs to Meanings
J.-R. Abrial
Table of Contents
More information

C.10 Finite Tree Definitions 736
C.11 Well-founded Relation Definition 738
C.12 Generalized Substitution Definitions 738
C.13 Set-theoretic Models 741
C.14 Refinement Conditions 742
Appendix D **Visibility Rules** 743
D.1 Visibility of a Machine 743
D.2 Visibility of a Refinement 747
D.3 Visibility of an Implementation 750
Appendix E **Rules and Axioms** 753
E.1 Non-freeness Rules 753
E.2 Substitution Rules 754
E.3 Basic Inference Rules 756
E.4 Derived Inference Rules 758
E.5 Set Axioms 760
E.6 Generalized Substitution Axioms 761
E.7 Loop Proof Rules 761
E.8 Sequencing Proof Rule 762
Appendix F **Proof Obligations** 763
F.1 Machine Proof Obligations 763
F.2 INCLUDES Proof Obligations 765
F.3 USES Proof Obligations 767
F.4 Refinement Proof Obligations 769
F.5 Implementation Proof Obligations 771

Index 775

© Cambridge University Press www.cambridge.org