Practical Theory of Programming

2010-1-11 edition

Eric C.R. Hehner

Department of Computer Science
University of Toronto
Toronto ON M5S 2E4
Canada

The first edition of this book was published by Springer-Verlag Publishers
New York
1993
ISBN 0-387-94106-1
QA76.6.H428

The current edition is available free at

www.cs.utoronto.ca/~hehner/aPToP

You may copy freely as long as you include all the information on this page.
# Contents

0 Preface 0
  0.0 Introduction 0
  0.1 Current Edition 1
  0.2 Quick Tour 1
  0.3 Acknowledgements 2

1 Basic Theories 3
  1.0 Boolean Theory 3
    1.0.0 Axioms and Proof Rules 5
    1.0.1 Expression and Proof Format 7
    1.0.2 Monotonicity and Antimonotonicity 9
    1.0.3 Context 10
    1.0.4 Formalization 12
  1.1 Number Theory 12
  1.2 Character Theory 13

2 Basic Data Structures 14
  2.0 Bunch Theory 14
  2.1 Set Theory (optional) 17
  2.2 String Theory 17
  2.3 List Theory 20
    2.3.0 Multidimensional Structures 22

3 Function Theory 23
  3.0 Functions 23
    3.0.0 Abbreviated Function Notations 25
    3.0.1 Scope and Substitution 25
  3.1 Quantifiers 26
  3.2 Function Fine Points (optional) 29
    3.2.0 Function Inclusion and Equality (optional) 30
    3.2.1 Higher-Order Functions (optional) 30
    3.2.2 Function Composition (optional) 31
  3.3 List as Function 32
  3.4 Limits and Reals (optional) 33

4 Program Theory 34
  4.0 Specifications 34
    4.0.0 Specification Notations 36
    4.0.1 Specification Laws 37
    4.0.2 Refinement 39
    4.0.3 Conditions (optional) 40
    4.0.4 Programs 41
  4.1 Program Development 43
    4.1.0 Refinement Laws 43
    4.1.1 List Summation 43
    4.1.2 Binary Exponentiation 45
4.2 Time
  4.2.0 Real Time
  4.2.1 Recursive Time
  4.2.2 Termination
  4.2.3 Soundness and Completeness (optional)
  4.2.4 Linear Search
  4.2.5 Binary Search
  4.2.6 Fast Exponentiation
  4.2.7 Fibonacci Numbers

4.3 Space
  4.3.0 Maximum Space
  4.3.1 Average Space

5 Programming Language
  5.0 Scope
    5.0.0 Variable Declaration
    5.0.1 Variable Suspension
  5.1 Data Structures
    5.1.0 Array
    5.1.1 Record
  5.2 Control Structures
    5.2.0 While Loop
    5.2.1 Loop with Exit
    5.2.2 Two-Dimensional Search
    5.2.3 For Loop
    5.2.4 Go To
  5.3 Time and Space Dependence
  5.4 Assertions (optional)
    5.4.0 Checking
    5.4.1 Backtracking
  5.5 Subprograms
    5.5.0 Result Expression
    5.5.1 Function
    5.5.2 Procedure
  5.6 Alias (optional)
  5.7 Probabilistic Programming (optional)
    5.7.0 Random Number Generators
    5.7.1 Information (optional)
  5.8 Functional Programming (optional)
    5.8.0 Function Refinement

6 Recursive Definition
  6.0 Recursive Data Definition
    6.0.0 Construction and Induction
    6.0.1 Least Fixed-Points
    6.0.2 Recursive Data Construction
  6.1 Recursive Program Definition
    6.1.0 Recursive Program Construction
    6.1.1 Loop Definition
7 Theory Design and Implementation 100
   7.0 Data Theories 100
      7.0.0 Data-Stack Theory 100
      7.0.1 Data-Stack Implementation 101
      7.0.2 Simple Data-Stack Theory 102
      7.0.3 Data-Queue Theory 103
      7.0.4 Data-Tree Theory 104
      7.0.5 Data-Tree Implementation 104
   7.1 Program Theories 106
      7.1.0 Program-Stack Theory 106
      7.1.1 Program-Stack Implementation 106
      7.1.2 Fancy Program-Stack Theory 107
      7.1.3 Weak Program-Stack Theory 107
      7.1.4 Program-Queue Theory 108
      7.1.5 Program-Tree Theory 108
   7.2 Data Transformation 109
      7.2.0 Security Switch 111
      7.2.1 Take a Number 112
      7.2.2 Parsing 113
      7.2.3 Limited Queue 115
      7.2.4 Soundness and Completeness (optional) 117

8 Concurrency 118
   8.0 Independent Composition 118
      8.0.0 Laws of Independent Composition 120
      8.0.1 List Concurrency 120
   8.1 Sequential to Parallel Transformation 121
      8.1.0 Buffer 122
      8.1.1 Insertion Sort 123
      8.1.2 Dining Philosophers 124

9 Interaction 126
   9.0 Interactive Variables 126
      9.0.0 Thermostat 128
      9.0.1 Space 129
   9.1 Communication 131
      9.1.0 Implementability 132
      9.1.1 Input and Output 133
      9.1.2 Communication Timing 134
      9.1.3 Recursive Communication (optional) 134
      9.1.4 Merge 135
      9.1.5 Monitor 136
      9.1.6 Reaction Controller 137
      9.1.7 Channel Declaration 138
      9.1.8 Deadlock 139
      9.1.9 Broadcast 140