

a  
**Practical  
Theory  
of  
Programming**

**2008-9-22 edition**

Eric C.R. Hehner



**a**  
**Practical**  
**Theory**  
**of**  
**Programming**

**2008-9-22 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](http://www.cs.utoronto.ca/~hehner/aPToP)**

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

# Contents

<b>0</b>	<b>Preface</b>	0
0.0	Introduction	0
0.1	Current Edition	1
0.2	Quick Tour	1
0.3	Acknowledgements	2
<b>1</b>	<b>Basic Theories</b>	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
<b>2</b>	<b>Basic Data Structures</b>	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
<b>3</b>	<b>Function Theory</b>	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
<b>4</b>	<b>Program Theory</b>	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	46
4.2.0	Real Time	46
4.2.1	Recursive Time	48
4.2.2	Termination	50
4.2.3	Soundness and Completeness (optional)	51
4.2.4	Linear Search	51
4.2.5	Binary Search	53
4.2.6	Fast Exponentiation	57
4.2.7	Fibonacci Numbers	59
4.3	Space	61
4.3.0	Maximum Space	63
4.3.1	Average Space	64
<b>5</b>	<b>Programming Language</b>	<b>66</b>
5.0	Scope	66
5.0.0	Variable Declaration	66
5.0.1	Variable Suspension	67
5.1	Data Structures	68
5.1.0	Array	68
5.1.1	Record	69
5.2	Control Structures	69
5.2.0	While Loop	69
5.2.1	Loop with Exit	71
5.2.2	Two-Dimensional Search	72
5.2.3	For Loop	74
5.2.4	Go To	76
5.3	Time and Space Dependence	76
5.4	Assertions (optional)	77
5.4.0	Checking	77
5.4.1	Backtracking	77
5.5	Subprograms	78
5.5.0	Result Expression	78
5.5.1	Function	79
5.5.2	Procedure	80
5.6	Alias (optional)	81
5.7	Probabilistic Programming (optional)	82
5.7.0	Random Number Generators	84
5.7.1	Information (optional)	87
5.8	Functional Programming (optional)	88
5.8.0	Function Refinement	89
<b>6</b>	<b>Recursive Definition</b>	<b>91</b>
6.0	Recursive Data Definition	91
6.0.0	Construction and Induction	91
6.0.1	Least Fixed-Points	94
6.0.2	Recursive Data Construction	95
6.1	Recursive Program Definition	97
6.1.0	Recursive Program Construction	98
6.1.1	Loop Definition	99

<b>7</b>	<b>Theory Design and Implementation</b>	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
<b>8</b>	<b>Concurrency</b>	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
<b>9</b>	<b>Interaction</b>	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

<b>10 Exercises</b>	147
10.0 Preface	147
10.1 Basic Theories	147
10.2 Basic Data Structures	154
10.3 Function Theory	156
10.4 Program Theory	161
10.5 Programming Language	177
10.6 Recursive Definition	181
10.7 Theory Design and Implementation	187
10.8 Concurrency	193
10.9 Interaction	195
<b>11 Reference</b>	201
11.0 Justifications	201
11.0.0 Notation	201
11.0.1 Basic Theories	201
11.0.2 Basic Data Structures	202
11.0.3 Function Theory	204
11.0.4 Program Theory	204
11.0.5 Programming Language	206
11.0.6 Recursive Definition	207
11.0.7 Theory Design and Implementation	207
11.0.8 Concurrency	208
11.0.9 Interaction	208
11.1 Sources	209
11.2 Bibliography	211
11.3 Index	215
11.4 Laws	223
11.4.0 Booleans	223
11.4.1 Generic	225
11.4.2 Numbers	225
11.4.3 Bunches	226
11.4.4 Sets	227
11.4.5 Strings	227
11.4.6 Lists	228
11.4.7 Functions	228
11.4.8 Quantifiers	229
11.4.9 Limits	231
11.4.10 Specifications and Programs	231
11.4.11 Substitution	232
11.4.12 Conditions	232
11.4.13 Refinement	232
11.5 Names	233
11.6 Symbols	234
11.7 Precedence	235
11.8 Distribution	235