

# Contents

About this Book . . . . .	xiii
Acknowledgments . . . . .	xiv
<b>1 Introduction</b>	<b>1</b>
1.1 Who Am I? . . . . .	1
1.2 Who Are You? . . . . .	2
1.3 The Origin of the Science . . . . .	2
1.3.1 The Origin of the Theory . . . . .	2
1.3.2 The Origin of the Practice . . . . .	3
1.4 Correctness . . . . .	5
1.5 A Preview . . . . .	6
1.6 Why Math? . . . . .	9
<b>2 Ordinary Math</b>	<b>12</b>
2.1 Arithmetic as a Mathematical Theory . . . . .	13
2.2 The Mathematical Theory of Algebra . . . . .	14
2.3 Mathglish . . . . .	17
2.4 Boolean Arithmetic (Propositional Logic) . . . . .	18
2.5 ZF . . . . .	21
2.6 Meaningless Expressions . . . . .	23
2.7 Quantification and Bound Variables . . . . .	25
2.7.1 Quantification . . . . .	25
2.7.2 Bound Variables . . . . .	26
2.8 Defining Mappings and Functions . . . . .	28
2.8.1 Mappings . . . . .	28
2.8.2 Functions . . . . .	30
2.8.3 Sequences and Tuples . . . . .	31
2.9 Some Useful Notation . . . . .	32
2.9.1 IF/THEN/ELSE . . . . .	32
2.9.2 Conjunction and Disjunction Lists . . . . .	32

<b>3</b>	<b>Describing Abstract Programs with Math</b>	<b>34</b>
3.1	The Behavior of Physical Systems . . . . .	34
3.2	Behaviors of Digital Systems . . . . .	37
	Math I . . . . .	37
3.2.1	From Continuous to Discrete Time . . . . .	37
3.2.2	An Example: <i>Sqrs</i> . . . . .	40
3.2.3	A Finer-Grained Example: <i>FGSqrs</i> . . . . .	44
3.3	Nondeterminism . . . . .	46
	Math II . . . . .	46
3.3.1	Sources of Nondeterminism . . . . .	47
3.3.2	An Example: <i>Increment</i> . . . . .	48
3.4	Temporal Logic . . . . .	52
	Math III . . . . .	52
3.4.1	The Logic of Actions . . . . .	53
	3.4.1.1 Eliminating State Numbers . . . . .	53
	3.4.1.2 The Semantics of the Logic of Actions . . . . .	55
	3.4.1.3 The Prime Operator . . . . .	56
	3.4.1.4 Action Composition . . . . .	58
3.4.2	The Temporal Logic RTL <sub>A</sub> . . . . .	59
	3.4.2.1 Simple RTL <sub>A</sub> . . . . .	60
	3.4.2.2 The Complete RTL <sub>A</sub> . . . . .	62
	3.4.2.3 The $\square$ Operator . . . . .	63
	3.4.2.4 Eventually ( $\diamond$ ) . . . . .	64
	3.4.2.5 Eventually Always ( $\diamond\square$ ) . . . . .	66
	3.4.2.6 Infinitely Often ( $\square\diamond$ ) . . . . .	66
	3.4.2.7 The End of the Line . . . . .	67
	3.4.2.8 Leads To ( $\rightsquigarrow$ ) . . . . .	68
	3.4.2.9 Warning . . . . .	69
3.5	TLA . . . . .	70
	Math IV . . . . .	70
3.5.1	The Problem . . . . .	71
3.5.2	The Solution . . . . .	72
3.5.3	Stuttering Insensitivity . . . . .	74
3.5.4	The Definition of TLA . . . . .	76
<b>4</b>	<b>Safety, Liveness, and Fairness</b>	<b>79</b>
4.1	Safety and Liveness . . . . .	79
	Math V . . . . .	79
4.1.1	Definitions . . . . .	81
4.1.2	A Completeness Theorem . . . . .	82

<i>CONTENTS</i>		ix
4.1.3	The Operator $\mathcal{C}$ . . . . .	84
4.1.4	What Good is Liveness? . . . . .	85
4.2	Fairness . . . . .	86
4.2.1	Traditional Programs and Enabled . . . . .	86
4.2.2	Concurrent Programs . . . . .	87
4.2.2.1	Mutual Exclusion . . . . .	88
4.2.2.2	Machine Closure . . . . .	92
4.2.3	Weak Fairness . . . . .	93
4.2.4	Temporal Logic Reasoning . . . . .	96
4.2.5	Reasoning With Weak Fairness . . . . .	97
4.2.5.1	Liveness for Mutual Exclusion . . . . .	97
4.2.5.2	The One-Bit Algorithm . . . . .	98
4.2.5.3	Proving Liveness . . . . .	100
4.2.6	Strong Fairness . . . . .	104
4.2.6.1	Starvation Free Mutual Exclusion . . . . .	104
4.2.6.2	The Definition of Strong Fairness . . . . .	105
4.2.6.3	Using a Strongly Fair Semaphore . . . . .	106
4.2.7	Properties of WF and SF . . . . .	107
4.2.8	What is Fairness? . . . . .	109
<b>5</b>	<b>Interlude</b>	<b>111</b>
5.1	Possibility and Accuracy . . . . .	111
5.1.1	Possibility Conditions . . . . .	111
5.1.2	Expressing Possibility in TLA . . . . .	112
5.1.3	Checking Accuracy . . . . .	114
5.2	Real-Time Programs . . . . .	115
	Math VI . . . . .	116
5.2.1	Fischer's Algorithm . . . . .	117
5.2.2	Correctness of Fischer's Algorithm . . . . .	120
5.2.3	Fairness and Zeno Behaviors . . . . .	121
5.2.4	Discrete Time . . . . .	123
5.2.5	Hybrid Systems . . . . .	125
<b>6</b>	<b>Refinement</b>	<b>126</b>
6.1	A Sequential Algorithm . . . . .	128
	Math VII . . . . .	128
6.1.1	A One-Step Program . . . . .	129
6.1.2	Two Views of Refinement Mappings . . . . .	131
6.1.3	A Step and Data Refinement . . . . .	132
6.2	Invariance Under Refinement . . . . .	135

6.3	An Example: The Paxos Algorithm . . . . .	135
6.3.1	The Consensus Problem . . . . .	136
6.3.2	The Paxos Consensus Algorithm . . . . .	138
6.3.2.1	The Specification of Consensus . . . . .	139
6.3.2.2	The Voting Algorithm . . . . .	139
6.3.2.3	The Paxos Abstract Program . . . . .	142
6.3.3	Implementing Paxos . . . . .	144
6.4	Proving Refinement . . . . .	145
	Math VIII . . . . .	146
6.4.1	The Refinement Mapping . . . . .	148
6.4.2	Refinement of Safety . . . . .	149
6.4.3	Refinement of Fairness . . . . .	152
6.4.4	A Closer Look at $\mathbb{E}$ . . . . .	155
6.4.4.1	A Syntactic View . . . . .	155
6.4.4.2	Computing $\mathbb{E}$ . . . . .	156
6.4.4.3	The Trouble With $\mathbb{E}$ . . . . .	158
6.5	A Warning . . . . .	161
<b>7</b>	<b>Auxiliary Variables</b>	<b>163</b>
7.1	Variable Hiding . . . . .	163
	Math IX . . . . .	163
7.1.1	Introduction . . . . .	164
7.1.2	Reasoning About $\exists$ . . . . .	166
7.1.3	The Definition of $\exists$ . . . . .	167
7.2	History Variables . . . . .	169
7.2.1	How to Add a History Variable . . . . .	169
7.2.2	History Variables and Fairness . . . . .	173
7.2.3	A Completeness Result for History Variables . . . . .	174
7.3	Stuttering Variables . . . . .	175
	Math X . . . . .	175
7.3.1	The Example . . . . .	176
7.3.2	Adding Stuttering Steps After an Action . . . . .	178
7.3.3	Adding Stuttering Steps Before an Action . . . . .	182
7.3.4	Fairness and Stuttering Variables . . . . .	183
7.3.5	Infinite-Stuttering Variables . . . . .	186
7.4	Prophecy Variables . . . . .	187
	Math XI . . . . .	187
7.4.1	Simple Prophecy Variables . . . . .	188
7.4.2	Predicting the Impossible and Liveness . . . . .	192
7.4.3	General Prophecy Variables . . . . .	193

## CONTENTS

xi

7.4.3.1	A Sequence of Prophecies . . . . .	194
7.4.3.2	A Set of Prophecies . . . . .	197
7.4.3.3	Further Generalizations . . . . .	200
7.5	The Existence of Refinement Mappings . . . . .	202
7.6	The FIFO Queue . . . . .	203
7.6.1	<i>Fifo</i> – A Linearizable Specification . . . . .	203
7.6.2	<i>POFifo</i> – A More General Specification . . . . .	205
7.6.2.1	The Background . . . . .	205
7.6.2.2	Program <i>POFifo</i> . . . . .	207
7.6.3	Showing <i>IPOFifo</i> Implements <i>Fifo</i> . . . . .	211
7.6.3.1	The Prophecy Variable . . . . .	212
7.6.3.2	The History Variable $qBar$ . . . . .	213
7.6.3.3	Stuttering and the Refinement Mapping . . . . .	216
7.7	Prophecy Constants . . . . .	217
<b>8</b>	<b>Loose Ends</b> . . . . .	<b>220</b>
8.1	Reduction . . . . .	220
8.1.1	Introduction . . . . .	220
8.1.1.1	What Reduction Is . . . . .	220
8.1.1.2	The TLA Approach . . . . .	222
8.1.2	An Example . . . . .	224
8.1.2.1	The Reduced Behaviors . . . . .	224
8.1.2.2	The Program $S \otimes S^R$ . . . . .	226
8.1.2.3	The Invariant . . . . .	230
8.1.3	Reduction In General . . . . .	232
8.1.4	The Hypothesis $\Box \Diamond \neg \mathcal{L}$ . . . . .	236
8.1.5	Adding Liveness . . . . .	236
8.1.5.1	Fairness of Subactions of $E^R$ . . . . .	237
8.1.5.2	Fairness of Subactions of $M^R$ . . . . .	240
8.1.5.3	The Reduction Theorem with Fairness . . . . .	243
8.1.6	An Example: Making Critical Sections Atomic . . . . .	244
8.1.7	Another Example: Pipelining . . . . .	247
8.2	Decomposing and Composing Programs . . . . .	251
8.2.1	Decomposing Programs . . . . .	253
8.2.1.1	Writing a Program as a Conjunction . . . . .	253
8.2.1.2	Decomposing Proofs . . . . .	255
8.2.2	Composing Components . . . . .	261

<b>Appendix</b>	<b>266</b>
<b>A Miscellany</b>	<b>266</b>
A.1 Ordinary Math Summary . . . . .	266
A.1.1 Arithmetic . . . . .	266
A.1.2 Propositional Logic . . . . .	266
A.1.3 Predicate Logic . . . . .	267
A.1.4 Sets . . . . .	267
A.1.5 The CHOOSE Operator . . . . .	268
A.1.6 Functions . . . . .	269
A.1.7 Sequences . . . . .	269
A.1.8 Notation . . . . .	270
A.1.9 Recursive Definitions . . . . .	270
A.2 Structured Proofs . . . . .	271
A.3 Why Not All Mappings Are Sets . . . . .	274
A.4 How Not to Write $x'''$ . . . . .	275
A.5 Hoare Logic . . . . .	276
A.6 Another Way to Look at Safety and Liveness . . . . .	279
A.6.1 Metric Spaces . . . . .	279
A.6.2 The Metric Space of Behaviors . . . . .	282
<b>B Proofs</b>	<b>284</b>
B.1 Invariance Proof of <i>Increment</i> . . . . .	284
B.2 Proof of Theorem 4.3 . . . . .	287
B.3 Proof of Theorem 4.4 . . . . .	289
B.4 Proof of Theorem 4.5 . . . . .	290
B.5 Proof of Theorem 4.6 . . . . .	291
B.6 Proof of Theorem 4.7 . . . . .	291
B.7 Proof of Theorem 4.8 . . . . .	293
B.8 Proof Sketch of Theorem 4.9 . . . . .	295
B.9 Proof of Theorem 7.2 . . . . .	296
B.10 Proof Sketch of Theorem 7.3 . . . . .	298
B.11 Proof Sketch of Theorem 7.6 . . . . .	299
B.12 Proof of Theorem 8.2 . . . . .	302
B.13 Proof of Theorem 8.3 . . . . .	302
<b>Bibliography</b>	<b>304</b>
<b>Index</b>	<b>310</b>