

## Contents

<i>Preface</i>	<i>page ix</i>
<b>1 Introduction and Overview</b>	<b>1</b>
1.1 Obtaining Software Quality	2
1.2 What Is SPARK?	8
1.3 SPARK Tools	10
1.4 SPARK Example	12
Summary	16
Exercises	16
<b>2 The Basic SPARK Language</b>	<b>18</b>
2.1 Control Structures	21
2.2 Subprograms	27
2.3 Data Types	32
2.4 Subprograms, More Options	57
Summary	64
Exercises	65
<b>3 Programming in the Large</b>	<b>68</b>
3.1 Definition Packages	69
3.2 Utility Packages	71
3.3 Type Packages	73
3.4 Variable Packages	83
3.5 Child Packages	87
3.6 Elaboration	93
Summary	95
Exercises	96

<b>4</b>	<b>Dependency Contracts</b>	99
4.1	Data Dependency Contracts	100
4.2	Flow Dependency Contracts	104
4.3	Managing State	110
4.4	Default Initialization	124
4.5	Synthesis of Dependency Contracts	127
	Summary	130
	Exercises	132
<b>5</b>	<b>Mathematical Background</b>	135
5.1	Propositional Logic	135
5.2	Logical Equivalence	139
5.3	Arguments and Inference	141
5.4	Predicate Logic	144
	Summary	150
	Exercises	151
<b>6</b>	<b>Proof</b>	155
6.1	Runtime Errors	155
6.2	Contracts	162
6.3	Assert and Assume	189
6.4	Loop Invariants	201
6.5	Loop Variants	211
6.6	Discriminants	216
6.7	Generics	224
6.8	Suppression of Checks	235
	Summary	240
	Exercises	243
<b>7</b>	<b>Interfacing with SPARK</b>	247
7.1	SPARK and Ada	247
7.2	SPARK and C	261
7.3	External Subsystems	269
	Summary	282
	Exercises	283
<b>8</b>	<b>Software Engineering with SPARK</b>	286
8.1	Conversion of SPARK 2005	286
8.2	Legacy Ada Software	291
8.3	Creating New Software	296

Contents	<i>vii</i>
8.4 Proof and Testing	307
8.5 Case Study: Time Stamp Server	310
Summary	325
<b>9 Advanced Techniques</b>	326
9.1 Ghost Entities	326
9.2 Proof of Transitive Properties	330
9.3 Proof Debugging	336
9.4 SPARK Internals	347
<i>Notes</i>	355
<i>References</i>	359
<i>Index</i>	363