

Contents

1	Program Graphs	1
1.1	Program Graphs	1
1.2	Semantics	3
1.3	The Structure of the Memory	7
1.4	Properties of Program Graphs	9
1.5	Bit-Level Semantics (Bonus Material)	11
2	Guarded Commands	15
2.1	Syntax	15
2.2	Program Graphs	17
2.3	Semantics	21
2.4	Alternative Approaches	24
2.5	More Control Structures (Bonus Material)	26
3	Program Verification	31
3.1	Predicates	31
3.2	Predicate Assignments	34
3.3	Partial Predicate Assignments	36
3.4	Guarded Commands with Predicates	40
3.5	Reverse Postorder (Bonus Material)	43

4	Program Analysis	47
4.1	Abstract Properties	47
4.2	Analysis Assignments	49
4.3	Analysis Functions	51
4.4	Analysis Specification	55
4.5	Computing Solutions (Bonus Material)	58
5	Language-Based Security	61
5.1	Information Flow	61
5.2	Reference-Monitor Semantics	63
5.3	Security Analysis	67
5.4	Multi-Level Security	70
5.5	Non-Interference (Bonus Material)	73
6	Model Checking	77
6.1	Transition Systems	77
6.2	Computation Tree Logic – CTL	80
6.3	Syntax and Semantics of CTL	82
6.4	From Program Graphs to Transition Systems	84
6.5	Towards an Algorithm (Bonus Material)	86
7	Procedures	91
7.1	Declarations	91
7.2	Blocks	93
7.3	Procedures with Dynamic Scope	98
7.4	Procedures with Static Scope	104
8	Concurrency	109
8.1	Shared Variables	109

8.2 Asynchronous Communication	112
8.3 Synchronous Communication	117
8.4 Broadcast and Gather (Bonus Material)	119
Epilogue	125
A The MicroC Language	129
B Programming Projects	133
C Realisation in F#	137
C.1 The Core Development	137
C.2 Program Verification	140
C.3 Program Analysis	142
C.4 Language-Based Security	145
D A Learning Environment	149
D.1 The Welcome Screen	150
D.2 Step-Wise Execution	151
D.3 Verification Conditions	152
D.4 Detection of Signs Analysis	153
D.5 Security Analysis	154
Symbols	155
Index	157