

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
1.1	The Nature of Program Analysis . . . . .	1
1.2	Setting the Scene . . . . .	3
1.3	Data Flow Analysis . . . . .	5
1.3.1	The Equational Approach . . . . .	5
1.3.2	The Constraint Based Approach . . . . .	8
1.4	Constraint Based Analysis . . . . .	10
1.5	Abstract Interpretation . . . . .	13
1.6	Type and Effect Systems . . . . .	17
1.6.1	Annotated Type Systems . . . . .	18
1.6.2	Effect Systems . . . . .	22
1.7	Algorithms . . . . .	25
1.8	Transformations . . . . .	27
	Concluding Remarks . . . . .	29
	Mini Projects . . . . .	29
	Exercises . . . . .	31
<b>2</b>	<b>Data Flow Analysis</b>	<b>35</b>
2.1	Intraprocedural Analysis . . . . .	35
2.1.1	Available Expressions Analysis . . . . .	39
2.1.2	Reaching Definitions Analysis . . . . .	43
2.1.3	Very Busy Expressions Analysis . . . . .	46
2.1.4	Live Variables Analysis . . . . .	49
2.1.5	Derived Data Flow Information . . . . .	52

2.2	Theoretical Properties . . . . .	54
2.2.1	Structural Operational Semantics . . . . .	54
2.2.2	Correctness of Live Variables Analysis . . . . .	60
2.3	Monotone Frameworks . . . . .	65
2.3.1	Basic Definitions . . . . .	67
2.3.2	The Examples Revisited . . . . .	70
2.3.3	A Non-distributive Example . . . . .	72
2.4	Equation Solving . . . . .	74
2.4.1	The MFP Solution . . . . .	74
2.4.2	The MOP Solution . . . . .	78
2.5	Interprocedural Analysis . . . . .	82
2.5.1	Structural Operational Semantics . . . . .	85
2.5.2	Intraprocedural versus Interprocedural Analysis . . . . .	88
2.5.3	Making Context Explicit . . . . .	90
2.5.4	Call Strings as Context . . . . .	95
2.5.5	Assumption Sets as Context . . . . .	99
2.5.6	Flow-Sensitivity versus Flow-Insensitivity . . . . .	101
2.6	Shape Analysis . . . . .	104
2.6.1	Structural Operational Semantics . . . . .	105
2.6.2	Shape Graphs . . . . .	109
2.6.3	The Analysis . . . . .	115
	Concluding Remarks . . . . .	128
	Mini Projects . . . . .	132
	Exercises . . . . .	135
<b>3</b>	<b>Constraint Based Analysis</b> . . . . .	<b>141</b>
3.1	Abstract 0-CFA Analysis . . . . .	141
3.1.1	The Analysis . . . . .	143
3.1.2	Well-definedness of the Analysis . . . . .	150
3.2	Theoretical Properties . . . . .	153
3.2.1	Structural Operational Semantics . . . . .	153
3.2.2	Semantic Correctness . . . . .	158
3.2.3	Existence of Solutions . . . . .	162

---

3.2.4	Coinduction versus Induction . . . . .	165
3.3	Syntax Directed 0-CFA Analysis . . . . .	168
3.3.1	Syntax Directed Specification . . . . .	169
3.3.2	Preservation of Solutions . . . . .	171
3.4	Constraint Based 0-CFA Analysis . . . . .	173
3.4.1	Preservation of Solutions . . . . .	175
3.4.2	Solving the Constraints . . . . .	176
3.5	Adding Data Flow Analysis . . . . .	182
3.5.1	Abstract Values as Powersets . . . . .	182
3.5.2	Abstract Values as Complete Lattices . . . . .	185
3.6	Adding Context Information . . . . .	189
3.6.1	Uniform $k$ -CFA Analysis . . . . .	191
3.6.2	The Cartesian Product Algorithm . . . . .	196
	Concluding Remarks . . . . .	198
	Mini Projects . . . . .	202
	Exercises . . . . .	205
<b>4</b>	<b>Abstract Interpretation</b> . . . . .	<b>211</b>
4.1	A Mundane Approach to Correctness . . . . .	211
4.1.1	Correctness Relations . . . . .	214
4.1.2	Representation Functions . . . . .	216
4.1.3	A Modest Generalisation . . . . .	219
4.2	Approximation of Fixed Points . . . . .	221
4.2.1	Widening Operators . . . . .	224
4.2.2	Narrowing Operators . . . . .	230
4.3	Galois Connections . . . . .	233
4.3.1	Properties of Galois Connections . . . . .	239
4.3.2	Galois Insertions . . . . .	242
4.4	Systematic Design of Galois Connections . . . . .	246
4.4.1	Component-wise Combinations . . . . .	249
4.4.2	Other Combinations . . . . .	253
4.5	Induced Operations . . . . .	258
4.5.1	Inducing along the Abstraction Function . . . . .	258

4.5.2	Application to Data Flow Analysis . . . . .	262
4.5.3	Inducing along the Concretisation Function . . . . .	267
	Concluding Remarks . . . . .	270
	Mini Projects . . . . .	274
	Exercises . . . . .	276
<b>5</b>	<b>Type and Effect Systems</b>	<b>283</b>
5.1	Control Flow Analysis . . . . .	283
5.1.1	The Underlying Type System . . . . .	284
5.1.2	The Analysis . . . . .	287
5.2	Theoretical Properties . . . . .	291
5.2.1	Natural Semantics . . . . .	292
5.2.2	Semantic Correctness . . . . .	294
5.2.3	Existence of Solutions . . . . .	297
5.3	Inference Algorithms . . . . .	300
5.3.1	An Algorithm for the Underlying Type System . . . . .	300
5.3.2	An Algorithm for Control Flow Analysis . . . . .	306
5.3.3	Syntactic Soundness and Completeness . . . . .	312
5.3.4	Existence of Solutions . . . . .	317
5.4	Effects . . . . .	319
5.4.1	Side Effect Analysis . . . . .	319
5.4.2	Exception Analysis . . . . .	325
5.4.3	Region Inference . . . . .	330
5.5	Behaviours . . . . .	339
5.5.1	Communication Analysis . . . . .	339
	Concluding Remarks . . . . .	349
	Mini Projects . . . . .	353
	Exercises . . . . .	359
<b>6</b>	<b>Algorithms</b>	<b>365</b>
6.1	Worklist Algorithms . . . . .	365
6.1.1	The Structure of Worklist Algorithms . . . . .	368
6.1.2	Iterating in LIFO and FIFO . . . . .	372
6.2	Iterating in Reverse Postorder . . . . .	374

---

6.2.1	The Round Robin Algorithm . . . . .	378
6.3	Iterating Through Strong Components . . . . .	381
	Concluding Remarks . . . . .	384
	Mini Projects . . . . .	387
	Exercises . . . . .	389
<b>A</b>	<b>Partially Ordered Sets</b>	<b>393</b>
A.1	Basic Definitions . . . . .	393
A.2	Construction of Complete Lattices . . . . .	397
A.3	Chains . . . . .	398
A.4	Fixed Points . . . . .	402
	Concluding Remarks . . . . .	404
<b>B</b>	<b>Induction and Coinduction</b>	<b>405</b>
B.1	Proof by Induction . . . . .	405
B.2	Introducing Coinduction . . . . .	407
B.3	Proof by Coinduction . . . . .	411
	Concluding Remarks . . . . .	415
<b>C</b>	<b>Graphs and Regular Expressions</b>	<b>417</b>
C.1	Graphs and Forests . . . . .	417
C.2	Reverse Postorder . . . . .	421
C.3	Regular Expressions . . . . .	426
	Concluding Remarks . . . . .	427
	<b>Index of Notation</b>	<b>429</b>
	<b>Index</b>	<b>433</b>
	<b>Bibliography</b>	<b>439</b>



<http://www.springer.com/978-3-540-65410-0>

Principles of Program Analysis

Nielson, F.; Nielson, H.R.; Hankin, C.

1999, XXI, 452 p., Hardcover

ISBN: 978-3-540-65410-0