TYPE THEORY AND FORMAL PROOF

An Introduction

ROB NEDERPELT
Eindhoven University of Technology,
The Netherlands

HERMAN GEUVERS
Radboud University Nijmegen,
and
Eindhoven University of Technology,
The Netherlands

CAMBRIDGE
UNIVERSITY PRESS

Contents

	Foreword, by Henk Barendregt	*page* xiii
	Preface	xv
	Acknowledgements	xxvii
	Greek alphabet	xxviii
1	**Untyped lambda calculus**	1
	1.1 Input–output behaviour of functions	1
	1.2 The essence of functions	2
	1.3 Lambda-terms	4
	1.4 Free and bound variables	8
	1.5 Alpha conversion	9
	1.6 Substitution	11
	1.7 Lambda-terms modulo α-equivalence	14
	1.8 Beta reduction	16
	1.9 Normal forms and confluence	19
	1.10 Fixed Point Theorem	24
	1.11 Conclusions	26
	1.12 Further reading	27
	Exercises	29
2	**Simply typed lambda calculus**	33
	2.1 Adding types	33
	2.2 Simple types	34
	2.3 Church-typing and Curry-typing	36
	2.4 Derivation rules for Church's $\lambda\!\!\rightarrow$	39
	2.5 Different formats for a derivation in $\lambda\!\!\rightarrow$	44
	2.6 Kinds of problems to be solved in type theory	46
	2.7 Well-typedness in $\lambda\!\!\rightarrow$	47
	2.8 Type Checking in $\lambda\!\!\rightarrow$	50
	2.9 Term Finding in $\lambda\!\!\rightarrow$	51

2.10 General properties of $\lambda\!\!\rightarrow$ 53
2.11 Reduction and $\lambda\!\!\rightarrow$ 59
2.12 Consequences 63
2.13 Conclusions 64
2.14 Further reading 65
Exercises 66

3 Second order typed lambda calculus 69
3.1 Type-abstraction and type-application 69
3.2 Π-types 71
3.3 Second order abstraction and application rules 72
3.4 The system $\lambda 2$ 73
3.5 Example of a derivation in $\lambda 2$ 76
3.6 Properties of $\lambda 2$ 78
3.7 Conclusions 80
3.8 Further reading 80
Exercises 82

4 Types dependent on types 85
4.1 Type constructors 85
4.2 Sort-rule and var-rule in $\lambda\underline{\omega}$ 88
4.3 The weakening rule in $\lambda\underline{\omega}$ 90
4.4 The formation rule in $\lambda\underline{\omega}$ 93
4.5 Application and abstraction rules in $\lambda\underline{\omega}$ 94
4.6 Shortened derivations 95
4.7 The conversion rule 97
4.8 Properties of $\lambda\underline{\omega}$ 99
4.9 Conclusions 100
4.10 Further reading 100
Exercises 101

5 Types dependent on terms 103
5.1 The missing extension 103
5.2 Derivation rules of λP 105
5.3 An example derivation in λP 107
5.4 Minimal predicate logic in λP 109
5.5 Example of a logical derivation in λP 115
5.6 Conclusions 118
5.7 Further reading 119
Exercises 121

6 The Calculus of Constructions 123
6.1 The system λC 123
6.2 The λ-cube 125

6.3 Properties of λC 128
6.4 Conclusions 132
6.5 Further reading 133
Exercises 134

7 The encoding of logical notions in λC 137
7.1 Absurdity and negation in type theory 137
7.2 Conjunction and disjunction in type theory 139
7.3 An example of propositional logic in λC 144
7.4 Classical logic in λC 146
7.5 Predicate logic in λC 150
7.6 An example of predicate logic in λC 154
7.7 Conclusions 157
7.8 Further reading 159
Exercises 162

8 Definitions 165
8.1 The nature of definitions 165
8.2 Inductive and recursive definitions 167
8.3 The format of definitions 168
8.4 Instantiations of definitions 170
8.5 A formal format for definitions 172
8.6 Definitions depending on assumptions 174
8.7 Giving names to proofs 175
8.8 A general proof and a specialised version 178
8.9 Mathematical statements as formal definitions 180
8.10 Conclusions 182
8.11 Further reading 183
Exercises 185

9 Extension of λC with definitions 189
9.1 Extension of λC to the system λD_0 189
9.2 Judgements extended with definitions 190
9.3 The rule for adding a definition 192
9.4 The rule for instantiating a definition 193
9.5 Definition unfolding and δ-conversion 197
9.6 Examples of δ-conversion 200
9.7 The conversion rule extended with $\stackrel{\Delta}{\rightarrow}$ 202
9.8 The derivation rules for λD_0 203
9.9 A closer look at the derivation rules of λD_0 204
9.10 Conclusions 206
9.11 Further reading 207
Exercises 208

10 Rules and properties of λD 211
10.1 Descriptive versus primitive definitions 211
10.2 Axioms and axiomatic notions 212
10.3 Rules for primitive definitions 214
10.4 Properties of λD 215
10.5 Normalisation and confluence in λD 219
10.6 Conclusions 221
10.7 Further reading 221
Exercises 223

11 Flag-style natural deduction in λD 225
11.1 Formal derivations in λD 225
11.2 Comparing formal and flag-style λD 228
11.3 Conventions about flag-style proofs in λD 229
11.4 Introduction and elimination rules 232
11.5 Rules for constructive propositional logic 234
11.6 Examples of logical derivations in λD 237
11.7 Suppressing unaltered parameter lists 239
11.8 Rules for classical propositional logic 240
11.9 Alternative natural deduction rules for ∨ 243
11.10 Rules for constructive predicate logic 246
11.11 Rules for classical predicate logic 249
11.12 Conclusions 252
11.13 Further reading 253
Exercises 254

12 Mathematics in λD: a first attempt 257
12.1 An example to start with 257
12.2 Equality 259
12.3 The congruence property of equality 262
12.4 Orders 264
12.5 A proof about orders 266
12.6 Unique existence 268
12.7 The descriptor ι 271
12.8 Conclusions 274
12.9 Further reading 275
Exercises 276

13 Sets and subsets 279
13.1 Dealing with subsets in λD 279
13.2 Basic set-theoretic notions 282
13.3 Special subsets 287
13.4 Relations 288

13.5 Maps 291
13.6 Representation of mathematical notions 295
13.7 Conclusions 296
13.8 Further reading 297
Exercises 302

14 Numbers and arithmetic in λD 305
14.1 The Peano axioms for natural numbers 305
14.2 Introducing integers the axiomatic way 308
14.3 Basic properties of the 'new' ℕ 313
14.4 Integer addition 316
14.5 An example of a basic computation in λD 320
14.6 Arithmetical laws for addition 322
14.7 Closure under addition for natural and negative numbers 324
14.8 Integer subtraction 327
14.9 The opposite of an integer 330
14.10 Inequality relations on ℤ 332
14.11 Multiplication of integers 335
14.12 Divisibility 338
14.13 Irrelevance of proof 340
14.14 Conclusions 341
14.15 Further reading 343
Exercises 344

15 An elaborated example 349
15.1 Formalising a proof of Bézout's Lemma 349
15.2 Preparatory work 352
15.3 Part I of the proof of Bézout's Lemma 354
15.4 Part II of the proof 357
15.5 Part III of the proof 360
15.6 The holes in the proof of Bézout's Lemma 363
15.7 The Minimum Theorem for ℤ 364
15.8 The Division Theorem 369
15.9 Conclusions 371
15.10 Further reading 373
Exercises 376

16 Further perspectives 379
16.1 Useful applications of λD 379
16.2 Proof assistants based on type theory 380
16.3 Future of the field 384
16.4 Conclusions 386
16.5 Further reading 387

Appendix A **Logic in λD** 391
A.1 Constructive propositional logic 391
A.2 Classical propositional logic 393
A.3 Constructive predicate logic 395
A.4 Classical predicate logic 396

Appendix B **Arithmetical axioms, definitions and lemmas** 397

Appendix C **Two complete example proofs in λD** 403
C.1 Closure under addition in ℕ 403
C.2 The Minimum Theorem 405

Appendix D **Derivation rules for λD** 409

References 411
Index of names 419
Index of definitions 421
Index of symbols 423
Index of subjects 425