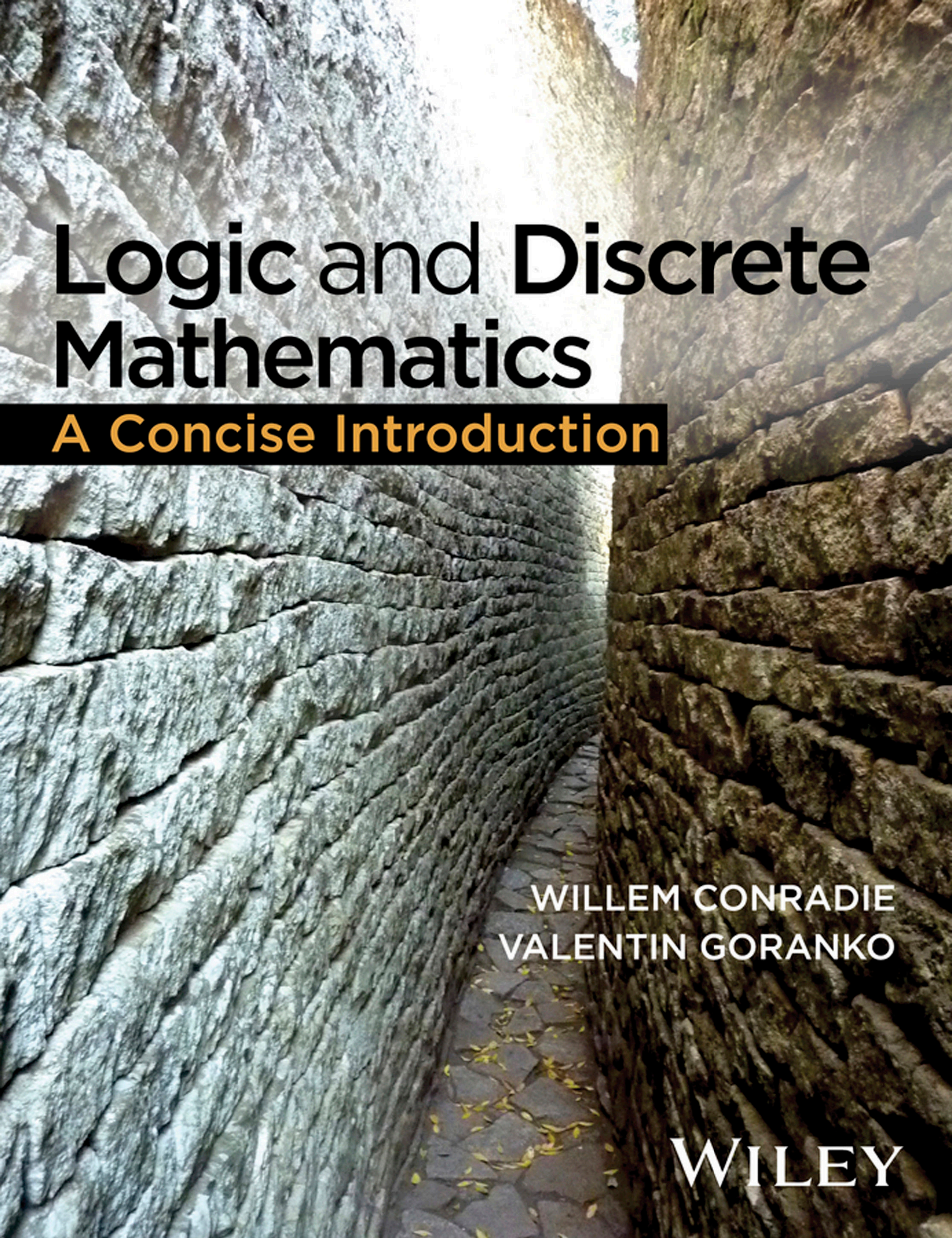

Logic and Discrete Mathematics

A Concise Introduction

WILLEM CONRADIE
VALENTIN GORANKO

WILEY

Logic and Discrete Mathematics

Logic and Discrete Mathematics

A Concise Introduction

Willem Conradie

*University of Johannesburg,
South Africa*

Valentin Goranko

Stockholm University, Sweden

WILEY

This edition first published 2015

Registered office
John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

For details of our global editorial offices, for customer services and for information about how to apply for permission to reuse the copyright material in this book please see our website at www.wiley.com.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

Limit of Liability/Disclaimer of Warranty: While the publisher and author have used their best efforts in preparing this book, they make no representations or warranties with respect to the accuracy or completeness of the contents of this book and specifically disclaim any implied warranties of merchantability or fitness for a particular purpose. It is sold on the understanding that the publisher is not engaged in rendering professional services and neither the publisher nor the author shall be liable for damages arising herefrom. If professional advice or other expert assistance is required, the services of a competent professional should be sought

Library of Congress Cataloging-in-Publication Data

Conradie, Willem, 1978- author.
Logic and discrete mathematics : a concise introduction / Willem Conradie, Valentin Goranko.
pages cm
Includes index.
ISBN 978-1-118-75127-5 (pbk.)
1. Logic, Symbolic and mathematical–Textbooks. 2. Computer science–Mathematics–Textbooks.
I. Goranko, Valentin, author. II. Title.
QA9.C7423 2015
511.3–dc23
2014035964

A catalogue record for this book is available from the British Library.

Front cover image: Narrow walkway inside the Great Enclosure at the Great Zimbabwe ruins. Reproduced by kind permission of Kenneth Meeks.

Set in 9/11pt, PalatinoLTStd by Laserwords Private Limited, Chennai, India

1 2015

Contents

List of Boxes xiii

Preface xvii

Acknowledgements xxi

About the Companion Website xxiii

1. Preliminaries 1

1.1 Sets 2

1.1.1 Exercises 7

1.2 Basics of logical connectives and expressions 9

1.2.1 Propositions, logical connectives, truth tables, tautologies 9

1.2.2 Individual variables and quantifiers 12

1.2.3 Exercises 15

1.3 Mathematical induction 17

1.3.1 Exercises 18

2. Sets, Relations, Orders 20

2.1 Set inclusions and equalities 21

2.1.1 Properties of the set theoretic operations 22

2.1.2 Exercises 26

2.2 Functions 28

2.2.1 Functions and their inverses 28

2.2.2 Composition of mappings 31

2.2.3 Exercises 33

2.3 Binary relations and operations on them 35

2.3.1 Binary relations 35

2.3.2 Matrix and graphical representations of relations on finite sets 38

2.3.3 Boolean operations on binary relations 39

2.3.4 Inverse and composition of relations 41

2.3.5 Exercises 42

2.4 Special binary relations 45

2.4.1 Properties of binary relations 45

2.4.2 Functions as relations 47

2.4.3 Reflexive, symmetric and transitive closures of a relation 47

2.4.4 Exercises 49

2.5 Equivalence relations and partitions 51

2.5.1 Equivalence relations 51

2.5.2 Quotient sets and partitions 53

2.5.3 The kernel equivalence of a mapping 56

2.5.4 Exercises 57

2.6 Ordered sets 59

2.6.1 Pre-orders and partial orders 59

2.6.2 Graphical representing posets: Hasse diagrams 61

2.6.3 Lower and upper bounds. Minimal and maximal elements 63

2.6.4 Well-ordered sets 65

2.6.5 Exercises 67

2.7 An introduction to cardinality 69

2.7.1 Equinumerosity and cardinality 69

2.7.2 Exercises 73

2.8 Isomorphisms of ordered sets. Ordinal numbers 75

2.8.1 Exercises 79

2.9 Application: relational databases 80

2.9.1 Exercises 86

3. Propositional Logic 89

3.1 Propositions, logical connectives, truth tables, tautologies 90

3.1.1 Propositions and propositional connectives. Truth tables 90

3.1.2 Some remarks on the meaning of the connectives 90

3.1.3 Propositional formulae 91

3.1.4 Construction and parsing tree of a propositional formula 92

3.1.5 Truth tables of propositional formulae 93
3.1.6 Tautologies 95
3.1.7 A better idea: search for a falsifying truth assignment 96
3.1.8 Exercises 97

3.2 Propositional logical consequence. Valid and invalid propositional inferences 101
3.2.1 Propositional logical consequence 101
3.2.2 Logically sound rules of propositional inference. Logically correct propositional arguments 104
3.2.3 Fallacies of the implication 106
3.2.4 Exercises 107

3.3 The concept and use of deductive systems 109

3.4 Semantic tableaux 113
3.4.1 Exercises 117

3.5 Logical equivalences. Negating propositional formulae 121
3.5.1 Logically equivalent propositional formulae 121
3.5.2 Some important equivalences 123
3.5.3 Exercises 124

3.6 Normal forms. Propositional resolution 126
3.6.1 Conjunctive and disjunctive normal forms of propositional formulae 126
3.6.2 Clausal form. Clausal resolution 129
3.6.3 Resolution-based derivations 130
3.6.4 Optimizing the method of resolution 131
3.6.5 Exercises 132

4. First-Order Logic 135

4.1 Basic concepts of first-order logic 136
4.1.1 First-order structures 136
4.1.2 First-order languages 138
4.1.3 Terms and formulae 139
4.1.4 The semantics of first-order logic: an informal outline 143
4.1.5 Translating first-order formulae to natural language 146
4.1.6 Exercises 147

4.2 The formal semantics of first–order logic 152
4.2.1 Interpretations 152
4.2.2 Variable assignment and term evaluation 153

4.2.3 Truth evaluation games 156
4.2.4 Exercises 159

4.3 The language of first-order logic: a deeper look 161
4.3.1 Translations from natural language into first-order languages 161
4.3.2 Restricted quantification 163
4.3.3 Free and bound variables. Scope of a quantifier 164
4.3.4 Renaming of a bound variable in a formula. Clean formulae 165
4.3.5 Substitution of a term for a variable in a formula. Capture of a variable 166
4.3.6 Exercises 167

4.4 Truth, logical validity, equivalence and consequence in first-order logic 171
4.4.1 More on truth of sentences in structures. Models and countermodels 171
4.4.2 Satisfiability and validity of first-order formulae 172
4.4.3 Logical equivalence in first-order logic 173
4.4.4 Some logical equivalences involving quantifiers 174
4.4.5 Negating first-order formulae 175
4.4.6 Logical consequence in first-order logic 176
4.4.7 Exercises 180

4.5 Semantic tableaux for first-order logic 185
4.5.1 Some derivations using first-order semantic tableau 186
4.5.2 Semantic tableaux for first-order logic with equality 189
4.5.3 Discussion on the quantifier rules and on termination of semantic tableaux 189
4.5.4 Exercises 191

4.6 Prenex and clausal normal forms 195
4.6.1 Prenex normal forms 195
4.6.2 Skolemization 197
4.6.3 Clausal forms 198
4.6.4 Exercises 199

4.7 Resolution in first-order logic 201
4.7.1 Propositional resolution rule in first-order logic 201
4.7.2 Substitutions of terms for variables revisited 201
4.7.3 Unification of terms 202
4.7.4 Resolution with unification in first-order logic 204
4.7.5 Examples of resolution-based derivations 205

4.7.6 Resolution for first-order logic with equality 207

4.7.7 Optimizations of the resolution method for first-order logic 207

4.7.8 Exercises 207

4.8 Applications of first-order logic to mathematical reasoning and proofs 211

4.8.1 Proof strategies: direct and indirect proofs 211

4.8.2 Tactics for logical reasoning 215

4.8.3 Exercises 216

5. Number Theory 219

5.1 The principle of mathematical induction revisited 220

5.1.1 Exercises 222

5.2 Divisibility 224

5.2.1 Basic properties of divisibility 224

5.2.2 Division with a remainder 224

5.2.3 Greatest common divisor 225

5.2.4 Exercises 227

5.3 Computing greatest common divisors. Least common multiples 230

5.3.1 Euclid's algorithm for computing greatest common divisors 230

5.3.2 Least common multiple 232

5.3.3 Exercises 233

5.4 Prime numbers. The fundamental theorem of arithmetic 236

5.4.1 Relatively prime numbers 236

5.4.2 Prime numbers 237

5.4.3 The fundamental theorem of arithmetic 238

5.4.4 On the distribution of prime numbers 239

5.4.5 Exercises 240

5.5 Congruence relations 243

5.5.1 Exercises 246

5.6 Equivalence classes and residue systems modulo *n* 248

5.6.1 Equivalence relations and partitions 248

5.6.2 Equivalence classes modulo n. Modular arithmetic 249

5.6.3 Residue systems 250

5.6.4 Multiplicative inverses in $\mathbb{Z}_n$ 251

5.6.5 Exercises 251

5.7 Linear Diophantine equations and linear congruences 253

5.7.1 Linear Diophantine equations 253

5.7.2 Linear congruences 254

5.7.3 Exercises 256

5.8 Chinese remainder theorem 257

5.8.1 Exercises 259

5.9 Euler's function. Theorems of Euler and Fermat 261

5.9.1 Theorems of Euler and Fermat 262

5.9.2 Exercises 264

5.10 Wilson's theorem. Order of an integer 266

5.10.1 Wilson's theorem 266

5.10.2 Order of an integer 266

5.10.3 Exercises 267

5.11 Application: public key cryptography 269

5.11.1 About cryptography 269

5.11.2 The idea of public key cryptography 269

5.11.3 The method RSA 270

5.11.4 Exercises 271

6. Combinatorics 274

6.1 Two basic counting principles 275

6.1.1 Exercises 281

6.2 Combinations. The binomial theorem 284

6.2.1 Counting sheep and combinations 284

6.2.2 Some important properties 286

6.2.3 Pascal's triangle 287

6.2.4 The binomial theorem 287

6.2.5 Exercises 289

6.3 The principle of inclusion-exclusion 293

6.3.1 Exercises 296

6.4 The Pigeonhole Principle 299
6.4.3 Exercises 302
6.5 Generalized permutations, distributions and the multinomial theorem 304
6.5.1 Arranging nondistinct objects 304
6.5.2 Distributions 306
6.5.3 The multinomial theorem 308
6.5.4 Summary 310
6.5.5 Exercises 311
6.6 Selections and arrangements with repetition; distributions of identical objects 312
6.6.1 Selections with repetition 312
6.6.2 Distributions of identical objects 314
6.6.3 Arrangements with repetition 315
6.6.4 Summary 316
6.6.5 Exercises 316
6.7 Recurrence relations and their solution 318
6.7.1 Recurrence relations. Fibonacci numbers 318
6.7.2 Catalan numbers 319
6.7.3 Solving homogeneous linear recurrence relations 322
6.7.4 Exercises 327
6.8 Generating functions 329
6.8.1 Introducing generating functions 329
6.8.2 Computing coefficients of generating functions 332
6.8.3 Exercises 335
6.9 Recurrence relations and generating functions 337
6.9.1 Exercises 341
6.10 Application: classical discrete probability 343
6.10.1 Common sense probability 343
6.10.2 Sample spaces 343
6.10.3 Discrete probability 345
6.10.4 Properties of probability measures 346
6.10.5 Conditional probability and independent events 348
6.10.6 Exercises 352

7. Graph Theory 356

7.1 Introduction to graphs and digraphs 357

7.1.1 Graphs 357

7.1.2 Digraphs 364

7.1.3 Exercises 367

7.2 Incidence and adjacency matrices 370

7.2.1 Exercises 374

7.3 Weighted graphs and path algorithms 377

7.3.1 Dijkstra's algorithm 378

7.3.2 The Floyd–Warshall algorithm 381

7.3.3 Exercises 383

7.4 Trees 385

7.4.1 Undirected trees 385

7.4.2 Computing spanning trees: Kruskal's algorithm 388

7.4.3 Rooted trees 390

7.4.4 Traversing rooted trees 392

7.4.5 Exercises 393

7.5 Eulerian graphs and Hamiltonian graphs 395

7.5.1 Eulerian graphs and digraphs 396

7.5.2 Hamiltonian graphs and digraphs 398

7.5.3 Exercises 400

7.6 Planar graphs 404

7.6.1 Exercises 408

7.7 Graph colourings 411

7.7.1 Colourings 411

7.7.2 The four- and five-colour theorems 413

7.7.3 Exercises 414

Index 419

List of Boxes

1. Preliminaries 1

Paradoxes 19

2. Sets, Relations, Orders 20

Russell’s paradox 27
Georg Cantor 35
The notation of set theory 45
Fuzzy sets 50
Zermelo–Fraenkel set theory 58
The axiom of choice 68
The continuum hypothesis 74
Hilbert’s Hotel 80
Charles Sanders Peirce 88

3. Propositional Logic 89

Aristotle 100
George Boole 109
David Hilbert 112
Early proof theory 120
Augustus De Morgan 126
The Boolean satisfiability problem and NP-completeness 133

4. First-Order Logic 135

Gottlob Frege 151
Giuseppe Peano 160
Bertrand Russell 170
Alfred Tarski 184
Kurt Gödel 194
Thoralf Skolem 200
Alonzo Church 210
Alan Turing 217

5. Number Theory 219

Carl Friedrich Gauss 223
Pythagoras of Samos 229
Euclid of Alexandria 235
Primality testing 242
Richard Dedekind 247
Babylonian mathematics 252
Diophantus of Alexandria 257
Ancient Chinese mathematics 260
Pierre de Fermat 265
Ancient and Medieval Indian and Arabic mathematics 268
History of codes and ciphers 272

6. Combinatorics 274

Stirling's approximation of n! 283
Pascal's triangle 292
Venn diagrams 298
Lejeune Dirichlet 304
Braille 312
Blaise Pascal 317
Fibonacci 328
Combinatorial games: Nim 336

Fibonacci numbers and the golden ratio 342

Pierre-Simon de Laplace 355

7. Graph Theory 356

Leonhard Euler 369

Ramsey theory 376

Edsger Dijkstra 385

Paul Erdõs 395

William Hamilton 403

Graph theory and Sudoku 410

The four-colour problem 417

Preface

Discrete Mathematics[1] refers to a range of mathematical disciplines that study discrete structures and phenomena, unlike other classical fields of mathematics, such as analysis, geometry and topology, which study continuous structures, processes and transformations. Intuitively put, discrete structures – such as the linear order of natural numbers or the set of cities and towns in a country together with the roads between them – consists of separable, discretely arranged objects, whereas continuous structures – such as the trajectory of a moving object, the real line, the Euclidian plane or a sphere – are densely filled, with no "gaps". The more important distinction, however, is between the types of problems studied and solved in discrete and continuous mathematics and also between the main ideas and techniques that underly and characterize these two branches of mathematics. Nevertheless, this distinction is often blurred and many ideas, methods and results from each of these branches have been fruitfully applied to the other.

The intuitive explanation above is not meant to define what should be classified as Discrete Mathematics, as every such definition would be incomplete or debatable. A more useful description would be to list what we consider to be the basic mathematical disciplines traditionally classified as Discrete Mathematics and included in most university courses on that subject: the Theory of Sets and Relations, Mathematical Logic, Number Theory, Graph Theory and Combinatorics. These are the topics covered in this book. Sometimes textbooks and courses on Discrete Mathematics also include Abstract Algebra, Classical Probability Theory, Automata Theory, etc. These topics are not included here, mainly for practical reasons.

Logic was born in the works of Aristotle as a philosophical study of reasoning some 25 centuries ago. Over the past 150 years it has gradually developed as a fundamental mathematical discipline, which nowadays has deep and mature mathematical content and also applications spreading far beyond foundational and methodological issues. While the field of Mathematical Logic is often regarded as included in the broad scope of Discrete Mathematics, in this book it is treated essentially on a par with it.

As mathematical fields of their own importance, both Logic and Discrete Mathematics are relatively young and very dynamically developing disciplines, especially since the mid 20th century, when the computer era began. Many of the most exciting current developments

[1] Not to be confused with discreetly done mathematics!

in Logic and Discrete Mathematics are motivated and inspired by applications in Computer Science, Artificial Intelligence and Bioinformatics. We have accordingly included some such selected applications in the book.

About the book

The work on this book started more than a decade ago as a loose collection of lecture notes that we wrote and used to teach courses on Logic and Discrete Mathematics, partly because we could not find available suitable textbooks that would meet our needs and requirements. Eventually we decided to write a book of our own, which would best reflect the content and features we consider most important:

1. Being logicians, we have provided a much more detailed and deeper treatment of Logic than is usual in textbooks on Discrete Mathematics. We believe that such a treatment is necessary for the proper understanding and use of Logic as a mathematical and general reasoning tool, and we consider it a distinguishing feature of the book.
2. We included only what we consider to be the core disciplines within the field of Discrete Mathematics (without claiming that ours is the only good choice) but have treated these disciplines in considerable depth for an undergraduate text. That enabled us to keep the book within reasonable size limits without compromising on the content and exposition of the topics included.
3. We have tried to keep the exposition clear and concise while still including the necessary technical detail and illustrating concepts and techniques with numerous examples.
4. We have included comprehensive sets of exercises, most of them provided with answers or solutions in an accompanying solutions manual.
5. We have also included "boxes" at the end of each section. Some contain mathematics titbits or applications of the content in the section. Others are short biographies of distinguished scientists who have made fundamental contributions to Discrete Mathematics. We hope the reader will find it inspiring to learn a little about their lives and their contributions to the fields covered in the book.

To the instructor

We have aimed this book to be suitable for a variety of courses for students in both Mathematics and Computer Science. Some parts of it are much more relevant to only one of these audiences and we have indicated them by introducing *Mathematics Track* and *Computer Science Track* markers in the text. We regard everything not explicitly on either of these tracks to be suitable for both groups.

In addition, the book can be used for designing courses on different undergraduate or lower graduate levels. Some material that could reasonably be omitted in courses at a lower undergraduate level is indicated with an *Advances Track* marker. These tracks are, of course, only suggestions, which should serve as our recommendations to the instructor.

The single stars shown in the exercises are deemed to be exercises that are more difficult, while the double stars are considered to be exercises that are challenging.

The whole book can be comfortably covered in two semester courses, or various selections can be made for a single semester course. Apart from assuming knowledge of the background material in the preliminary Chapter 1, the chapters are essentially independent and can be taught in any order. The only exception is Chapter 4 on first-order logic, which presupposes knowledge of the material on propositional logic covered in Chapter 3. Also, much of the content of Chapter 2 covers general mathematical background, useful for the rest of the book.

Acknowledgements

A number of people have contributed, one way or another, to our work on this book over the years. With the risk of inadvertently omitting some names, for which we apologize in advance, we would like to thank Gerhard Benadé, Thomas Bolander, Izak Broere, Ruaan Kellerman, Heidi Maartens, Chantel Marais and Claudette Robinson for helpful feedback, comments, technical or editorial corrections and some solutions to exercises. Besides them, thanks are due to many students at the University of Johannesburg, the University of the Witwatersrand and the Technical University of Denmark, who pointed out some errors in earlier versions of the manuscript. We thank Justin Southey for the use of the GraphScribe application authored by him, which greatly speeded up the drawing of some combinatorial graphs, and also for his suggestions on the applications of Graph Theory. Valentin is also grateful to Nina Ninova for her general support during the work on this book as well as help with collecting photos and references for many of the historical boxes. Willem would like to thank Dion Govender for his patience and support during the final months of intense work on the book. Last but not least, we wish to thank Richard Davies, Audrey Koh, Kathryn Sharples, Mark Styles and Jo Taylor from Wiley as well as Krupa Muthu from Laserwords for their kind support and technical advice during the work on this book.

About the Companion Website

This book is accompanied by a companion website:

www.wiley.com/go/conradie/logic

The website includes:

- Lecture Slides
- Quizzes

1

Preliminaries

1.1. Sets . . . 2
1.2. Basics of logical connectives and expressions . . . 9
1.3. Mathematical induction . . . 17

Here we briefly review some minimal background knowledge that we will assume in the rest of the book. Besides a small amount of that nebulous quality called "mathematical maturity", we only expect some basic concepts from set theory and mathematical indiction. The reader who is familiar with these concepts can safely skip on to the next chapter.

Some notation

We denote the set of natural numbers $\{0, 1, 2, \dots\}$ by $\mathbb{N}$. There is some inconsistency in the mathematical literature as to whether 0 belongs to the natural numbers or not: some authors choose to include it, other do not. For our purposes it is convenient to include 0 as a natural number. Other number sets which will be of importance to us include the sets of integers $\mathbb{Z}$, positive integers $\mathbb{Z}^+$, rational numbers $\mathbb{Q}$, positive rational numbers $\mathbb{Q}^+$, real numbers $\mathbb{R}$, and positive real numbers $\mathbb{R}^+$.

The product $1 \times 2 \times 3 \times \cdots \times n$ of the first n positive integers turns up in many mathematical situations. It is therefore convenient to have a more compact notation for it. We accordingly define $0! = 1$ and $n! = 1 \times 2 \times 3 \times \cdots \times n$, for $n \geq 1$. We read $n!$ as 'n factorial'. The definition of $0!$ as 1 is not supposed to carry any intuitive meaning: it is simply a useful convention.

Logic and Discrete Mathematics: A Concise Introduction, First Edition. Willem Conradie and Valentin Goranko.

Companion Website: www.wiley.com/go/conradie/logic

1.1. Sets

Sets and elements. By a **set** we intuitively mean a collection of objects of any nature (numbers, people, concepts, sets themselves, etc.) that is considered as a single entity. The objects in that collection are called **elements** of the set. If an object x is an element of a set A, we denote that fact by

$$x \in A;$$

otherwise we write

$$x \notin A.$$

We also say that *x is a member of the set A* or that *x belongs to A*. If a set has finitely many elements (here we rely on your intuition of what *finite* is), we can describe it precisely by listing all of them, for example:

$$A = \{3, 4, 5\}.$$

We often rely on our common intuition and use ellipses, as in

$$A = \{1, 2, \dots, n\}.$$

We sometimes go further and use the same for *infinite* sets; for example, the set of natural numbers can be specified as

$$\mathbb{N} = \{0, 1, 2, 3, \dots\}.$$

Further we will discuss a more universal method of describing sets.

Equality and containment of sets. Two sets are declared **equal** if and only if they have the same elements. In other words, the sets A and B are equal, denoted as usual by $A = B$, if every element of A is an element of B and every element of B is an element of A. For example, the sets $\{a, b, c\}$ and $\{b, c, a\}$ are equal, and so are the sets $\{1, 9, 9, 7\}$, $\{1, 9, 7\}$ and $\{7, 1, 9, 1, 7, 1\}$.

A set A is a **subset** of a set B, denoted $A \subseteq B$, if every element of A is an element of B. If $A \subseteq B$, we also say that A **is included in** B, or that B **contains** A. For example, $\{3, 5\} \subseteq \{5, 4, 3\}$. Note that every set is a subset of itself.

The following facts are very useful. They are direct consequences of the definitions of equality and containment of sets.

- Two sets A and B are equal if, and only if, $A \subseteq B$ and $B \subseteq A$.
- A set A is not a subset of a set B, denoted $A \nsubseteq B$, if, and only if, there is an element of A that is not an element of B.
- A set A is not equal to a set B if A is not a subset of B *or* if B is not a subset of A.

A set A is a **proper subset** of a set B, denoted $A \subset B$ or $A \subsetneq B$, if $A \subseteq B$ and $A \neq B$. In other words, A is a proper subset of B if A is a subset of B and B is *not* a subset of A, i.e. if at least one element of B is not in A. In particular, no set is a proper subset of itself. If A is not a proper subset of B, we denote that by $A \not\subset B$.

The empty set. Amongst all sets there is one that is particularly special. That is the **empty set**, i.e. the set that has no elements. By definition of equality of sets, there is only one empty set. One might think that the empty set is a useless abstraction. On the contrary, it is a very important set, and probably the most commonly used one in mathematics (like the number 0 is the most commonly used number). That is why it has a special notation: $\varnothing$.

Sets and properties. Set-builder notation. We cannot always list the elements of a set, even if it is finite, so we need a more universal method for specifying sets. The commonly used method is to *describe the property that determines membership of the set*, e.g.:

> "A is the set of all objects x such that $\ldots x \ldots$."

where "$\ldots x \ldots$" is a certain property (predicate) involving x. We use the following convenient notation, called the **set-builder notation** for the set described above:

$$A = \{x \mid \ldots x \ldots\}.$$

Here are some examples:

- $\{x \mid x \textit{ is a negative real number}\}$ defines the set of negative real numbers;
- $\{x \mid x \textit{ is a student in the MATH3029 class}\}$ defines the set of students in the MATH3029 class.
- $\{x \mid x \in \mathbb{Z} \textit{ and } 3 \geq x > -2\}$ defines the set $\{-1, 0, 1, 2, 3\}$.
- $\{x \mid x = \frac{m}{n}, \textit{ where } m \in \mathbb{Z} n \in \mathbb{Z} \textit{ and } n \neq 0\}$ defines the set of rational numbers.

Sometimes, we use the set-builder notation more liberally and, for instance, describe the set of rational numbers as $\left\{\frac{m}{n} \middle| m \text{ and } n \text{ are integers and } n \neq 0\right\}$ or the set of positive real numbers as $\{x \in \mathbb{R} \mid x > 0\}$.

Operations on sets. We describe below the basic operations on sets.

Intersection. The intersection of two sets A and B is the set

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}$$

consisting of all elements that are both in A and in B. If $A \cap B = \varnothing$, then A and B are called **disjoint**.

Union. The union of two sets A and B is the set

$$A \cup B = \{x \mid x \in A \text{ or } x \in B\}$$

consisting of all elements that are in at least one of A and B.

Difference. The difference of the sets A and B is the set

$$A - B = \{x \mid x \in A \text{ and } x \notin B\}$$

consisting of all elements that are in A but not in B. An alternative notation for $A - B$ is $A \backslash B$.

For example, if $A = \{1, 2, 3, 4\}$ and $B = \{3, 4, 5, 6, 7\}$ then $A \cap B = \{3, 4\}$, $A \cup B = \{1, 2, 3, 4, 5, 6, 7\}$, $A - B = \{1, 2\}$ and $B - A = \{5, 6, 7\}$.

Universal sets and complements of sets. Often, all sets that we consider are subsets of one set, called the **domain of discourse**. We also call that set the **universe** or the **universal set**. For example, in arithmetic, the universe is usually the set of natural numbers or the set of integers, while in algebra and calculus, the universe is the set of real numbers; talking about humans, the universe is the set of all humans, etc.

Definition 1.1.1 *Let a universal set* $\mathbf{U}$ *be fixed and* $A \subseteq \mathbf{U}$*. The* complement of A *(with respect to* $\mathbf{U}$*) is the set*

$$A' = \mathbf{U} - A.$$

The complement of a set A *is sometimes also denoted by* $\overline{A}$*.*

Thus, the complement of A consists of those objects from the universal set that do not belong to A. For example, if the universal set is $\mathbb{R}$, then the complement of the interval $(0, 2]$ is $(-\infty, 0] \cup (2, \infty)$; the complement of $\mathbb{Q}$ is the set of irrational numbers.

Powersets. The *power set of a set A* is the set of all subsets of A:

$$\mathscr{P}(A) = \{X \mid X \subseteq A\}.$$

Here are some examples:

- $\mathscr{P}(\emptyset) = \{\emptyset\}$;
- $\mathscr{P}(\{a\}) = \{\emptyset, \{a\}\}$, in particular, $\mathscr{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$;
- $\mathscr{P}(\{a, b\}) = \{\emptyset, \{a\}, \{b\}, \{a, b\}\}$;
- $\mathscr{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$.

Cartesian products of sets. In order to introduce the next operation we need the notion of **ordered pair**. Let a, b be any objects. Intuitively, the ordered pair of a and b, denoted (a, b) (do not confuse this with an open interval of real numbers!), is something like a set consisting of a as a *first element* (or first *component*) and b as a *second element* (or second *component*). Thus, if $a \neq b$, then the ordered pair (a, b) is *different* from the ordered pair (b, a) and each of these is different from the set $\{a, b\}$ because the elements of a set are not ordered. In particular, the ordered pair (a, a) is different from the set $\{a, a\} = \{a\}$. Here is a formal definition of an ordered pair as a set that satisfies the intuition:

Definition 1.1.2 *Given the objects a and b, the* **ordered pair** (a, b) *is the set* $\{\{a\}, \{a, b\}\}$*.*

Here is the fundamental property of ordered pairs:

Proposition 1.1.3 *The ordered pairs* (a_1, a_2) *and* (b_1, b_2) *are equal if and only if* $a_1 = b_1$ *and* $a_2 = b_2$*.*

Proof: Exercise.

Definition 1.1.4 *The* **Cartesian product** *of the sets A and B is the set*

$$A \times B = \{(a, b) \mid a \in A \text{ and } b \in B\},$$

consisting of all ordered pairs where the first component comes from A and the second component comes from B. In particular, we denote $A \times A$ *by* A^2 *and call it the* **Cartesian square** *of A.*

For example, if $A = \{a, b\}, B = \{1, 2, 3\}$, then

$$A \times B = \{(a, 1), (a, 2), (a, 3), (b, 1), (b, 2), (b, 3)\},$$

while

$$B \times A = \{(1, a), (1, b), (2, a), (2, b), (3, a), (3, b)\}.$$

Note that if A or B is empty, then $A \times B$ is empty too. Moreover, if A has n elements and B has m elements, then $A \times B$ has mn elements (why?). This is one of the reasons for the term "product".

The Cartesian coordinate system in the plane is a representation of the plane as the Cartesian[1] square $\mathbb{R}^2$ of the real line $\mathbb{R}$, where we associate a unique ordered pair of real numbers (its **coordinates**) with every point in the plane.

The notion of an ordered pair can be generalized to **ordered n-tuple**, for any $n \in \mathbb{N}^+$. An n-tuple is an object of the type $(a_1, a_2, \ldots, a_n)$ where the order of the components $a_1, a_2, \ldots, a_n$ matters. We will not give a formal set theoretic definition in the style of Definition 1.2.1, but leave this as an exercise (Exercise 11).

Accordingly, the Cartesian product can be extended to n sets:

$$A_1 \times A_2 \times \cdots \times A_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in A_1, a_2 \in A_2, \cdots, a_n \in A_n\}.$$

As before, we will use the notation A^n for $\underbrace{A \times A \times \cdots \times A}_{n \text{ times}}$.

Relations. Relations, also called **predicates**, are ubiquitous in mathematics. Relations between numbers like "being equal", "being less than" and "being divisible by" come to mind at once. As these examples indicate, many of the relations we commonly encounter are *binary*, i.e., relations relating *two* objects at a time. It will be convenient for us to identify a binary relation with the set of all ordered pairs of elements that stand in that relation. We thus have the following definition:

Definition 1.1.5 *A* **binary relation** *on a set A is any subset of* A^2.

For example the relation $<$ on the set $\mathbb{N}$ of natural numbers is a binary relation, which we identify with the set

$$\{(a, b) \mid a, b \in \mathbb{N} \text{ and } a \text{ is less than } b\}.$$

The relation of "being the mother of" is a binary relation on the set of humans, which we identify with the following set of ordered pairs:

$$\{(x, y) \mid x \text{ and } y \text{ are humans and } x \text{ is the mother of } y\}.$$

Definition 1.1.6 *An* **n-ary relation** *on a set A is any subset of* A^n.

[1] The term "Cartesian" comes from the name of the French mathematician René Descartes (1596–1650), who was the first to introduce coordinate systems and to apply algebraic methods in geometry.

More generally, relations may relate objects from different sets:

Definition 1.1.7 *An* **n-ary relation** between sets $A_1, A_2, \ldots, A_n$ *is any subset of* $A_1 \times A_2 \times \cdots \times A_n$.

If $n = 1$ we speak of a **unary relation**, when $n = 2$ of a **binary relation**, when $n = 3$ of a **ternary relation** and so on.

Unary relations correspond to sets. For instance, "being positive" is a unary relation on the set $\mathbb{R}$, which we identify with the set

$$\{a \mid a \in \mathbb{R} \text{ and } 0 < a\}.$$

Conversely, every set A defines the unary relation of "being a member of A".

The set

$$\{(f(x), a) \mid f(x) \text{ is a polynomial, } a \in \mathbb{R} \text{ and } f(a) = 0\}$$

is a binary relation between the set of all polynomials in x and the set $\mathbb{R}$ of real numbers, relating every polynomial to its real roots. The ordered pairs $(x^2 - 4, 2)$ and $(x^2 - 4, -2)$ are in this relation. There is no pair in this relation that has $x^2 + 2$ as first component. Why?

Examples of ternary relations are the relation "A is between B and C" relating triples of points in the plain or the relation "a is greater than $b + c$" between triples of real numbers.

Functions. Informally, a function from a set A to a set B, denoted by $f : A \to B$, can be though a rule that assigns to every element $a \in A$ a unique element $f(a) \in B$. A is called the **domain** of f while B is the **codomain**, or the **target set** of f.

Functions need not take only one argument. The function addition on $\mathbb{R}$, for example, takes two arguments. In general, a function can take any finite number of arguments, but it can always be regarded as a one-argument function if we consider the domain to be the Cartesian product of the domains of the different arguments. For instance, we can think of + as a one-argument function from $\mathbb{R} \times \mathbb{R}$ to $\mathbb{R}$. Here is the general definition.

Definition 1.1.8 *An* **n-ary function** *f from $A_1 \times A_2 \times \cdots \times A_n$ to B, denoted*

$$f : A_1 \times A_2 \times \cdots \times A_n \to B,$$

is any rule that to every ordered n-tuple $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$ assigns a unique value $f(a_1, a_2, \ldots, a_n) \in B$.

In particular, when $A_1 = A_2 = \cdots = A_n = A$ we call f an n-ary function on the set A, denoted

$$f : A^n \to A.$$

Functions are naturally associated with special relations, called their graphs. For instance, think of some familiar function $f : \mathbb{R} \to \mathbb{R}$, such as $f(x) = x^2$. The graph of this function, as drawn in the plane, consists of the sets of points (x, y) in the Cartesian plane such that $y = x^2$, i.e. the set $\{(x, x^2) \mid x \in \mathbb{R}\}$. This set completely determines the function. Here is the general definition.

Definition 1.1.9 *Given an n-ary function $f : A_1 \times \cdots \times A_n \to B$ the* **graph of f** *is the subset of $A_1 \times A_2 \times \cdots \times A_n \times B$, defined as follows:*

$$G_f = \{(a_1, a_2, \ldots, a_n, f(a_1, a_2, \ldots, a_n)) \mid (a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n\}$$

Sometimes it is technically convenient to identify functions with their graphs. Thus, an n-ary function f can be alternatively defined as a subset of $A_1 \times A_2 \times \cdots \times A_n \times B$, such that for all $(a_1, a_2, \ldots, a_n) \in A_1 \times A_2 \times \cdots \times A_n$, there is a unique $b \in B$ such that $(a_1, a_2, \ldots, a_n, b) \in f$. This last condition means that if $(a_1, a_2, \ldots, a_n, b) \in f$ and $(a_1, a_2, \ldots, a_n, b') \in f$ then $b = b'$. Thus an n-ary function can be regarded as a special type of $(n+1)$-ary relation. For instance, the multiplication of two integers can be regarded as the ternary relation:

$$\{(a, b, c) \mid a, b, c \in \mathbb{Z}, \text{and } a \times b = c\}.$$

We will generally use the standard definition of functions as rules but, whenever convenient, we may also adopt the handling functions in terms of their graphs.

1.1.1. *Exercises*

❶ List all elements of the following sets:

(a) $A = \{x \in \mathbb{R} \mid x^2 - 3x = 4\}$

(b) $B = \{y \in \mathbb{Z} \mid (y-1)(y+3)(2y+3)(y+5) = 0\}$

(c) $C = \{x \in \mathbb{Z} \mid -3 \leq x < 3\}$

(d) $D = \{x \in \mathbb{Z} \mid -3 \leq x < 3 \wedge x^2 - 3x = 4\}$

(e) $E = \{x \in \mathbb{Z} \mid -3 \leq x < 3 \wedge x^2 - 3x \neq 4\}$

(f) $F = \{x \in \mathbb{N} \mid x \text{ is an odd single-digit number}\}$

❷ Describe the following sets, using set-builder notation:

(a) $B = \{-\sqrt{3}, \sqrt{3}\}$

(b) $A = \{2, 4, 6, 8\}$

(c) $A = \{2, 4, 6, 8, 10, 12, \ldots\}$

(d) $A = \{\ldots, -7, -4, -1, 2, 5, 8, \ldots\}$

(e) $A = \{0, 1, 8, 27, 64, 125, \ldots\}$

(f) $A = \{-3, -2, -1, 1, 2, 3, 4, 5, 6\}$

(g) $A = \{\ldots, -6, -5, -4, -3, 5, 6, 7, 8, \ldots\}$

❸ Let $A = \{a, b, c\}$. Which of the following are true?

(a) $c \in A$

(b) $b \subset A$

(c) $b \subseteq A$

(d) $\{a\} \subset A$

(e) $\{a\} \subseteq A$

(f) $\{a\} \in A$

(g) $\{a, c\} \subset A$

(h) $\{a, c\} \subseteq A$

(i) $\{a, b, c\} \subset A$

(j) $\{a, b, c\} \subseteq A$

❹ Let $A = \{1, 2\}$, $B = \{1, \{2\}, A\}$. Which of the following are true?

(a) $1 \in A$

(b) $2 \in B$

(c) $\{2\} \subset B$

(d) $A \subset B$

(e) $2 \subset B$

(f) $\{2\} \subset B$

(g) $\{2\} \subset A$

(h) $\{A\} \subset A$

(i) $\{A\} \subseteq B$

(j) $A \in B$

(k) $\{A\} \in B$

(l) $\{\{2\}\} \subseteq B$

(m) $\{1, 2\} \in B$

(n) $\{\{1, 2\}\} \subseteq B$

❺ Let $\mathbf{U} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$ be the universal set, $A = \{1, 2, 4, 7\}$ and $B = \{0, 2, 5, 6, 7, 9\}$. Determine:

(a) $A \cap B$

(b) $A \cup B$

(c) $A - B$

(d) $B - A$

(e) $A - (A - B)$

(f) $B - (A - B)$

(g) B'

(h) $(A \cap B)'$

(i) $A \cap B'$

(j) $(A \cup B)'$

(k) $(A \cup B)' - (B - A)'$

❻ Let $A = \{0\}$, $B = \{0, A\}$ and $C = \{0, \{0\}, \{A\}\}$. Determine:

(a) $A \cap B$

(b) $A \cup B$

(c) $B - A$

(d) $A \cap (B \cup C)$

(e) $(B \cup C) - A$

(f) $(A \cap B) \cup (A \cap C)$

(g) $(C - B) - A$

(h) $A \cap (C - A)$

❼ If $A = \{1, 2, 3, 4\}$ and $B = \{0, 1\}$, list the elements of $A \times B$ and of $B \times A$.

❽ If $C = \{a, b\}$, $D = \{\alpha, \beta, \gamma, \delta, \theta\}$ and $E = \{a, c, d\}$, how many elements does each of the following sets have?

(a) $C \times D \times E$

(b) $C \times (D \cap E)$

(c) $D \times (C \cap E)$

(d) $D \cap (C \times E)$

(e) $(C \cup D) \times (C \times E)$

(f) $(C \times E) \cap (E \times C)$

❾ Which of the following relations are graphs of functions?

(a) $\{(a, b) \mid a, b \in \mathbb{R} \text{ and } b = a^2\}$

(b) $\{(a, b) \mid a, b \in \mathbb{R} \text{ and } a = b^2\}$

(c) $\{(a, b, c) \mid a, b, c \in \mathbb{Z}\text{and } c \text{ divides } a \times b \text{ without remainder}\}$

(d) $\{(x, y) \mid x \text{ and } y \text{ are humans and } y \text{ is a parent of } x\}$

(e) $\{(x, y) \mid x \text{ and } y \text{ are humans and } y \text{ is the mother of } x\}$

❿ Prove Proposition 1.2.1: two ordered pairs (a_1, a_2) and (b_1, b_2) (seen as special sets as in Definition 1.2.1) are equal if and only if $a_1 = b_1$ and $a_2 = b_2$.

⓫ Generalize Definition 1.2.1 to a formal set-theoretic definition of an ordered n-tuple.

1.2. Basics of logical connectives and expressions

Here we only provide a compendium of basic logical symbols and notation, commonly used in mathematics. We will not discuss here the underlying concepts of logical languages, semantics and deduction; these will be presented in a detailed and systematic way in the chapters on logic, Chapters 3 and 4.

1.2.1. Propositions, logical connectives, truth tables, tautologies

Propositions

The basic concept of propositional logic is the **proposition**. A proposition is a sentence that can be assigned a **truth value**: `true` or `false`.

Some simple examples are:

- The Sun is hot.
- The Earth is made of cheese.
- 2 plus 2 equals 22.
- The 999-th decimal digit of the number π is 9.

Here are some sentences that are not propositions (why?):

- Are you bored?
- Please, don't go away!
- She loves him.
- x is an integer.
- This sentence is false.

Propositional logical connectives

The propositions above are very simple. They have no logical structure, so we call them **primitive** propositions. From primitive propositions one can form **compound** ones by using **logical connectives**. The most commonly used connectives are:

- **not**, called **negation**, denoted by $\neg$;
- **and**, called **conjunction**, denoted by $\wedge$ (or sometimes, by &);
- **or**, called **disjunction**, denoted by $\vee$;
- **if** … **then** …, called **implication**, or **conditional**, denoted by $\to$;
- … **if and only if** … , called **biconditional**, denoted by $\leftrightarrow$.

Remark 1 *It is usually not grammatically correct to read compound propositions by simply inserting the names of the logical connectives in between the primitive components. A typical problem arises with the negation: one does not say "Not the earth is square". A uniform way to get round that difficulty and to negate a proposition P is to say "It is not the case that P".*

Thus, given the propositions

"Two plus two equals five" and "The Sun is hot"

we can form the propositions

- "It is **not** the case that two plus two equals five."
- "Two plus two equals five **and** the Sun is hot."
- "Two plus two equals five **or** the Sun is hot."
- "If two plus two equals five **then** the Sun is hot."
- "Two plus two equals five **if and only if** the Sun is hot."

Example 1.2.1

Here is a more involved example. Suppose Mary is a particular person, about whom it is known whether she is clever, lazy, and whether she likes logic. Then, we can consider the following sentences as propositions:

"Mary is clever", "Mary is lazy" and "Mary likes logic."

From these, we can compose a proposition (smoothed out a bit), such as

"Mary is not clever or if she likes logic then she is clever and not lazy."

Truth tables

How about the truth value of a compound proposition? It can be ***calculated*** from the truth values of the components (in much the same way as we can calculate the value of the algebraic expression $A \times (B - C) + B/A$ as soon as we know the values of A, B, C) by following the rules of "propositional arithmetic":

- The proposition $\neg A$ is true if and only if the proposition A is false.
- The proposition $A \wedge B$ is true if and only if both A and B are true.
- The proposition $A \vee B$ is true if and only if either of A or B (possibly both) is true.
- The proposition $A \rightarrow B$ is true if and only if A is false or B is true, i.e. if the truth of A implies the truth of B.
- The proposition $A \leftrightarrow B$ is true if and only if A and B have the same truth values.

We can systematize these rules in kinds of "multiplication tables". For that purpose, and to make it easier for symbolic (i.e. mathematical) manipulations, we introduce a special notation for the two truth values by denoting the value `true` by `T` and the value `false` by `F`. Another common notation, particularly used in computer science, is to denote `true` by **1** and `false` by **0**.