S*pringer* **M***onographs* in **M***athematics*

For further volumes:
www.springer.com/series/3733

Pavel Pudlák

Logical Foundations of Mathematics and Computational Complexity

A Gentle Introduction

Springer

Pavel Pudlák
ASCR
Prague, Czech Republic

ISSN 1439-7382 Springer Monographs in Mathematics
ISBN 978-3-319-00118-0 ISBN 978-3-319-00119-7 (eBook)
DOI 10.1007/978-3-319-00119-7
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2013936799

Mathematics Subject Classification: 03D15, 03E30, 03E35, 03F03, 03F20, 03F30, 03F40, 68Q15

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Dedicated to my parents
Anna Pudláková and Ján Pudlák

Preface

As the title states, this book is about logic, foundations and complexity. My aim is to present these topics in a readable form, accessible to a wide spectrum of readers. The message that I want to convey is that complexity, either in the form of computational complexity or in the form of proof complexity, is as important for foundations as the more traditional concepts of computability and provability are. Rather than presenting my own philosophical doctrine in the foundations, my goal is to isolate the most important problems and invite the reader to think about them.

The foundations of mathematics has always attracted mathematicians and philosophers. There were periods of time when many mathematicians were involved in the discussion of foundations. The most important such period was at the beginning of the 20th century. At that time the set-theoretical foundations were laid down, but set theory itself ran into problems—paradoxes were found showing that the intuitive use of set theory sometimes leads to contradictions. This problem was solved by accepting a particular axiomatic system for set theory, and things settled down. Later the interest in the foundations was stirred by several events. In the 1930s, it was Gödel's Incompleteness Theorem that showed that Hilbert's program to prove the consistency of the foundations was not possible. The second major event was Cohen's proof of the independence of the Continuum Hypothesis in the 1960s. This was an open problem concerning a basic question about the cardinality of the real numbers, posed by Cantor already in the 1870s. Also in the late 1960s a new field emerged that seemed to be somehow connected with foundations. This was the computational complexity theory.

Achievements in foundations can be viewed as solutions of important problems, but in fact they present us with much deeper open problems. Do the axioms of set theory describe the real universe of sets? Can we trust the axiomatic system for set theory to be free of contradiction? When the consistency of a theory is only provable in a stronger theory, according to the Incompleteness Theorem, what are we going to do with the consistency problem? How are we going to decide the Continuum Hypothesis, when it is independent of the axioms of set theory? In computational complexity there are a number of open problems. They may just be very difficult solvable problems, but their nature, which is similar to logical problems, and their

resilience with which they resist any attempts to solve them, rather suggest that there are more fundamental reasons why they are still open.

These examples show that, in spite of all the progress that has been achieved, there are problems in the foundations that are still widely open. Many mathematicians and philosophers are aware of this fact and are thinking about the problems. But not only them; also physicists have realized that they must know something about the foundations of mathematics if they want to find the unified foundations of physics. One can observe a renewed interest in the foundations in the past decade notwithstanding the fact that there has been no breakthrough result obtained recently.

However, a mathematician with a deeper interest in this subject does not have much choice of suitable sources: on the one hand, there are many popular books that present the subject in a very superficial manner, and often incorrectly; on the other hand, there are monographs about various parts of logic, set theory and computational complexity theory that can only be read with considerable effort. Furthermore, these monographs always cover much more than is needed for understanding the basic questions about the foundations, and someone not acquainted with the field does not know what to read and what to skip.

This book is intended to fill this gap by presenting a survey of results related to the foundations of mathematics and complexity theory in a readable form and with a sufficient amount of detail. It focuses on explaining the essence of concepts and the ideas of proofs, rather than presenting precise formal statements and full proofs. Each section starts with concepts and results that can easily be explained, and gradually proceeds to more difficult ones. The idea is that the readers should not be lost before they get to the heart of the matter. But since mathematicians are always curious how the things are actually done, some formal definitions and sketches of proofs are provided in the notes to the sections.

The prospective readers of this book are mathematicians with an interest in the foundations, philosophers with a good background in mathematics and, perhaps, also philosophically minded physicists. Most of the book should be accessible to graduate students of mathematics. Logicians may find much of the material familiar, but they can profit from the chapters about computational and proof complexities, unless they also work in these fields.

I should also say what the reader should not expect from the book. Although the style of the presentation is often light (such as in the quotations from science fiction stories), the book is not popular science—its primary aim is not to entertain, but to educate the reader. So the readers will need to stop from time to time and ponder what they have read, or even to skip a part and return to it later. But the book is also not a typical dry monograph consisting of definitions, theorems and proofs. Concerning the history of mathematics, the facts that I occasionally mention are only meant to make the text more readable and are not intended to give a complete picture of the development of the field.

The book consists of seven chapters. The first two chapters are an introduction to the foundations of mathematics and mathematical logic. The material is explained

very informally and more detailed presentation is deferred to later chapters. For example, set theory is introduced by means of several informal principles that are presented more precisely as the axioms of Zermelo-Fraenkel Set Theory in Chap. 3. Similarly, the Incompleteness Theorem is only stated and the proof and the consequences are discussed in Chap. 4.

Chapter 3 is devoted to set theory, which is the most important part of the foundations of mathematics. The two main themes in this chapter are: (1) higher infinities as a source of powerful axioms, and (2) alternative axioms, such as the Axiom of Determinacy.

Proofs of impossibility, the topic of Chap. 4, are proofs that certain tasks are impossible, contrary to the original intuition. Nowadays we tend to equate impossibility with unprovability and non-computability, which is a rather narrow view. Therefore, it is worth recalling that the first important impossibility results were obtained in different contexts: geometry and algebra. The most important result presented in this chapter is the Incompleteness Theorem of Kurt Gödel. I believe that the essence of the proof of this theorem can be explained with very little formalism and this is what try to I do in this chapter. Due to the diversity of results and connections with concrete mathematics, this is probably the most interesting chapter.

Proofs of impossibility are, clearly, important in foundations. One field in which the most basic problems are about proving impossibility is computational complexity theory, the topic of Chap. 5. But there are more connections between computational complexity and the foundations. I think that one cannot study the foundations of mathematics without understanding computational complexity.

In fact, there is a field of research that studies connections between computational complexity and logic. It is called '*Proof Complexity*' and it is presented in Chap. 6. Although we do have indications that complexity should play a relevant role in the foundations, we do not have any results proving this connection. In the last section of this chapter I present some ideas of mine about the possible nature of these connections. I state several conjectures which, if true, would give an explicit link between these two areas.

Every book about the foundations of mathematics should mention the basic philosophical approaches to the foundations of mathematics. I also do it in Chap. 7, but as I am not a philosopher, the main part of the chapter rather concentrates on mathematical results and problems that are at the border of mathematics and philosophy. Since I feel that the field lacks innovative approaches, I present one at the end of the chapter. It is based on the idea that natural numbers that can be represented in the physical universe are different from those studied in mathematics.

I tried to be as neutral as possible, but one cannot avoid using a certain philosophical standpoint when explaining the foundations. At the beginning of the book I assume the point of view of a realist, because it is easier to explain logic to a beginner from this viewpoint. My actual philosophy is the one of a moderate formalist, which is certainly apparent from my comments throughout the book. The only special feature of my philosophy is the stress on the importance of the complexity issues.

Even a thick volume like this cannot cover everything that is relevant to the foundations of mathematics. The main omission that I am aware of concerns intuition-

istic type theories. These theories play a central role in the current research into the intuitionistic foundations of mathematics. The reasons for this omission is my lack of expertise in this field and the fact that the book is already fairly long as it is.

Prague, Czech Republic Pavel Pudlák
January 2013

Acknowledgements

I would like to thank all who helped me by reading parts of the manuscript, pointing out errors, suggesting improvements or answering questions related to the text: Paul Beame, Arnold Beckmann, Lev Beklemishev, Samuel Buss, Lorenzo Carlucci, Stephano Cavagnetto, Dmitri Gavinsky, Stefan Hetzl, Edward Hirsch, Radek Honzík, Pavel Hrubeš, Peter Koellner, Leszek Kolodziejczyk, Jan Krajíček, Sebastian Müller, Jan Nekovář, Adam Nohejl, Jeffrey Paris, Ján Pich, Michael Rathjen, Zenon Sadowski, Neil Thapen, Iddo Tzameret, Eva Vachková.

I am also grateful to the anonymous reviewers of the manuscript, whose critical remarks were very useful and helped me to correct several errors.

My thanks are further due to Julie Cismosky, Sean Miller and Neil Thapen for correcting the English, and to Petr Pudlák for helping me with computer related issues.

The photographs were kindly provided by: Fachbereich Mathematik, Universität Hamburg (Cantor, Dedekind); Kurt Gödel Society, Vienna (Gödel); Archives of the Mathematisches Forschungsinstitut Oberwolfach (D. Hilbert); King's College, Cambridge University (Turing); Princeton University Library (A. Church); Bertrand Russell Archives, McMaster University Library (Russell); Universitätsarchiv Zürich (Zermelo).

I appreciate the help of Lynn Brandon, Lauren Stoney and Catherine Waite from Springer-Verlag London during the preparation of the manuscript for publication.

Through all the work I was supported by the Institute of Mathematics of the Academy of Sciences of the Czech Republic and received additional support from several grants of the Grant Agency of the Academy of Sciences.

Last, but not least, I want to thank my wife Věra for her understanding and encouragement over the years of writing this book.

Contents

1 Mathematician's World 1
1.1 Mathematical Structures 2
1.2 Everything Is a Set 25
1.3 Antinomies of Set Theory 36
1.4 The Axiomatic Method 43
1.5 The Necessity of Using Abstract Concepts 54
Main Points of the Chapter 64

2 Language, Logic and Computations 65
2.1 The Language of Mathematics 66
2.2 Truth and Models 80
2.3 Proofs 92
2.4 Programs and Computations 123
2.5 The Lambda Calculus 146
Main Points of the Chapter 155

3 Set Theory 157
3.1 The Axioms of Set Theory 159
3.2 The Arithmetic of Infinity 176
3.3 What Is the Largest Number? 196
3.4 Controversial Axioms 215
3.5 Alternative Set-Theoretical Foundations 231
Main Points of the Chapter 253

4 Proofs of Impossibility 255
4.1 Impossibility Proofs in Geometry and Algebra 256
4.2 The Incompleteness Theorems 272
4.3 Algorithmically Unsolvable Problems 300
4.4 Concrete Independence 319
4.5 The Independent Sentences of Set Theory 340
Main Points of the Chapter 364

5 The Complexity of Computations 365
5.1 What Is Complexity? 366
5.2 Randomness, Interaction and Cryptography 410
5.3 Parallel Computations 437
5.4 Quantum Computations 448
5.5 Descriptional Complexity 479
Main Points of the Chapter 493

6 Proof Complexity 495
6.1 Proof Theory 496
6.2 Theories and Complexity Classes 523
6.3 Propositional Proofs 540
6.4 Feasible Incompleteness 562
Main Points of the Chapter 580

7 Consistency, Truth and Existence 583
7.1 Consistency and Existence 584
7.2 The Attributes of Reality 609
7.3 Finitism and Physical Reality 646
Main Points of the Chapter 664

Bibliographical Remarks 667

References 671

Name Index 683

Subject Index 687

Symbols and Abbreviations 695