Proofs, Computability, Complexity, And the Lambda Calculus
An Introduction

Jean Gallier and Jocelyn Quaintance
Department of Computer and Information Science
University of Pennsylvania
Philadelphia, PA 19104, USA
e-mail: jean@cis.upenn.edu

© Jean Gallier
Please, do not reproduce without permission of the author

January 21, 2020
## Contents

1 Mathematical Reasoning And Basic Logic  
1.1 Introduction .............................................. 7  
1.2 Logical Connectives, Definitions .......................... 8  
1.3 Meaning of Implication and Proof Templates for Implication .... 12  
1.4 Proof Trees and Deduction Trees .......................... 16  
1.5 Proof Templates for ¬ .................................... 18  
1.6 Proof Templates for ∧, ∨, ≡ ............................... 22  
1.7 De Morgan Laws and Other Useful Rules of Logic ............... 30  
1.8 Formal Versus Informal Proofs; Some Examples ................ 31  
1.9 Truth Tables and Truth Value Semantics ..................... 35  
1.10 Proof Templates for the Quantifiers ....................... 38  
1.11 Sets and Set Operations ................................. 46  
1.12 Induction and Well–Ordering Principle .................... 51  
1.13 Summary ................................................. 53  
Problems .................................................. 55

Bibliography .................................................. 59

2 Mathematical Reasoning And Logic, A Deeper View  
2.1 Introduction .............................................. 61  
2.2 Inference Rules, Deductions, Proof Systems \( \mathcal{N}_m^= \) and \( \mathcal{N}_m^{=} \) .................... 62  
2.3 Proof Rules, Deduction and Proof Trees for Implication .......... 64  
2.4 Examples of Proof Trees .................................. 70  
2.5 A Gentzen-Style System for Natural Deduction ................. 76  
2.6 Adding ∧, ∨, ⊥; The Proof Systems \( \mathcal{N}_c^{=,\land,\lor,\bot} \) and \( \mathcal{N}_c^{=,\land,\lor,\bot} \) .................... 78  
2.7 Clearing Up Differences Among Rules Involving ⊥ ................ 88  
2.8 De Morgan Laws and Other Rules of Classical Logic ............... 91  
2.9 Formal Versus Informal Proofs .................................. 94  
2.10 Truth Value Semantics for Classical Logic ................... 95  
2.11 Kripke Models for Intuitionistic Logic ........................ 98  
2.12 Decision Procedures, Proof Normalization ..................... 101
## CONTENTS

2.13 The Simply-Typed λ-Calculus ................................................. 104
2.14 Completeness and Counter-Examples ..................................... 111
2.15 Adding Quantifiers; Proof Systems $\mathcal{N}_c^{\Rightarrow,\land,\lor,\exists,\bot}$, $\mathcal{N}_G^{\Rightarrow,\land,\lor,\exists,\bot}$ .................. 113
2.16 First-Order Theories .......................................................... 126
2.17 Basics Concepts of Set Theory .............................................. 132
2.18 Summary ........................................................................... 142
Problems .................................................................................. 146

Bibliography ............................................................................ 163

3 RAM Programs, Turing Machines ................................. 165
3.1 Partial Functions and RAM Programs .............................. 166
3.2 Definition of a Turing Machine ........................................... 171
3.3 Computations of Turing Machines ....................................... 173
3.4 RAM-computable functions are Turing-computable .............. 176
3.5 Turing-computable functions are RAM-computable ............. 177
3.6 Computably Enumerable and Computable Languages ............ 178
3.7 The Primitive Recursive Functions ....................................... 179
3.8 The Partial Computable Functions ........................................ 185

4 Universal RAM Programs and the Halting Problem .......... 191
4.1 Pairing Functions ................................................................. 191
4.2 Equivalence of Alphabets ...................................................... 194
4.3 Coding of RAM Programs ...................................................... 198
4.4 Kleene’s $T$-Predicate ........................................................... 207
4.5 A Simple Function Not Known to be Computable ................. 209
4.6 A Non-Computable Function; Busy Beavers ................. 211

5 Elementary Recursive Function Theory ...................... 215
5.1 Acceptable Indexings ............................................................. 215
5.2 Undecidable Problems .......................................................... 218
5.3 Listable (Recursively Enumerable) Sets ............................... 223
5.4 Reducibility and Complete Sets ........................................... 228
5.5 The Recursion Theorem ........................................................ 232
5.6 Extended Rice Theorem ......................................................... 236
5.7 Creative and Productive Sets ............................................... 239

6 The Lambda-Calculus ............................................................. 243
6.1 Syntax of the Lambda-Calculus ............................................ 245
6.2 $\beta$-Reduction and $\beta$-Conversion; the Church–Rosser Theorem 250
6.3 Some Useful Combinators ..................................................... 254
6.4 Representing the Natural Numbers ....................................... 256
6.5 Fixed-Point Combinators and Recursively Defined Functions 262
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>6.6</td>
<td>λ-Definability of the Computable Functions</td>
<td>264</td>
</tr>
<tr>
<td>6.7</td>
<td>Definability of Functions in Typed Lambda-Calculi</td>
<td>270</td>
</tr>
<tr>
<td>6.8</td>
<td>Head Normal-Forms and the Partial Computable Functions</td>
<td>277</td>
</tr>
<tr>
<td>7</td>
<td>Listable and Diophantine Sets; Hilbert’s Tenth</td>
<td>283</td>
</tr>
<tr>
<td>7.1</td>
<td>Diophantine Equations; Hilbert’s Tenth Problem</td>
<td>283</td>
</tr>
<tr>
<td>7.2</td>
<td>Diophantine Sets and Listable Sets</td>
<td>286</td>
</tr>
<tr>
<td>7.3</td>
<td>Some Applications of the DPRM Theorem</td>
<td>290</td>
</tr>
<tr>
<td>7.4</td>
<td>Gödel’s Incompleteness Theorem</td>
<td>293</td>
</tr>
<tr>
<td>8</td>
<td>The Post Correspondence Problem; Applications</td>
<td>299</td>
</tr>
<tr>
<td>8.1</td>
<td>The Post Correspondence Problem</td>
<td>299</td>
</tr>
<tr>
<td>8.2</td>
<td>Some Undecidability Results for CFG’s</td>
<td>300</td>
</tr>
<tr>
<td>8.3</td>
<td>More Undecidable Properties of Languages</td>
<td>303</td>
</tr>
<tr>
<td>9</td>
<td>Computational Complexity; $\mathcal{P}$ and $\mathcal{NP}$</td>
<td>305</td>
</tr>
<tr>
<td>9.1</td>
<td>The Class $\mathcal{P}$</td>
<td>305</td>
</tr>
<tr>
<td>9.2</td>
<td>Directed Graphs, Paths</td>
<td>307</td>
</tr>
<tr>
<td>9.3</td>
<td>Eulerian Cycles</td>
<td>308</td>
</tr>
<tr>
<td>9.4</td>
<td>Hamiltonian Cycles</td>
<td>309</td>
</tr>
<tr>
<td>9.5</td>
<td>Propositional Logic and Satisfiability</td>
<td>310</td>
</tr>
<tr>
<td>9.6</td>
<td>The Class $\mathcal{NP}$, $\mathcal{NP}$-Completeness</td>
<td>315</td>
</tr>
<tr>
<td>9.7</td>
<td>The Cook-Levin Theorem</td>
<td>319</td>
</tr>
<tr>
<td>10</td>
<td>Some $\mathcal{NP}$-Complete Problems</td>
<td>331</td>
</tr>
<tr>
<td>10.1</td>
<td>Statements of the Problems</td>
<td>331</td>
</tr>
<tr>
<td>10.2</td>
<td>Proofs of $\mathcal{NP}$-Completeness</td>
<td>342</td>
</tr>
<tr>
<td>10.3</td>
<td>Succinct Certificates, $\text{coNP}$, and $\mathcal{EXP}$</td>
<td>356</td>
</tr>
<tr>
<td>11</td>
<td>Primality Testing is in $\mathcal{NP}$</td>
<td>361</td>
</tr>
<tr>
<td>11.1</td>
<td>Prime Numbers and Composite Numbers</td>
<td>361</td>
</tr>
<tr>
<td>11.2</td>
<td>Methods for Primality Testing</td>
<td>362</td>
</tr>
<tr>
<td>11.3</td>
<td>Modular Arithmetic, the Groups $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^*$</td>
<td>365</td>
</tr>
<tr>
<td>11.4</td>
<td>The Lucas Theorem; Lucas Trees</td>
<td>373</td>
</tr>
<tr>
<td>11.5</td>
<td>Algorithms for Computing Powers Modulo $m$</td>
<td>378</td>
</tr>
<tr>
<td>11.6</td>
<td>PRIMES is in $\mathcal{NP}$</td>
<td>380</td>
</tr>
</tbody>
</table>

Bibliography 385
Symbol Index 387
Index 389
Chapter 1

Mathematical Reasoning And Basic Logic

1.1 Introduction

One of the main goals of this book is to show how to

construct and read mathematical proofs.

Why?

1. Computer scientists and engineers write programs and build systems.

2. It is very important to have rigorous methods to check that these programs and systems behave as expected (are correct, have no bugs).

3. It is also important to have methods to analyze the complexity of programs (time/space complexity).

More generally, it is crucial to have a firm grasp of the basic reasoning principles and rules of logic. This leads to the question:

What is a proof?

There is no short answer to this question. However, it seems fair to say that a proof is some kind of deduction (derivation) that proceeds from a set of hypotheses (premises, axioms) in order to derive a conclusion, using some proof templates (also called logical rules).

A first important observation is that there are different degrees of formality of proofs.

1. Proofs can be very informal, using a set of loosely defined logical rules, possibly omitting steps and premises.
2. Proofs can be completely formal, using a very clearly defined set of rules and premises. Such proofs are usually processed or produced by programs called proof checkers and theorem provers.

Thus, a human prover evolves in a spectrum of formality.

It should be said that it is practically impossible to write formal proofs. This is because it would be extremely tedious and time-consuming to write such proofs and these proofs would be huge and thus, very hard to read.

In principle, it is possible to write formalized proofs and sometimes it is desirable to do so if we want to have absolute confidence in a proof. For example, we would like to be sure that a flight-control system is not buggy so that a plane does not accidentally crash, that a program running a nuclear reactor will not malfunction, or that nuclear missiles will not be fired as a result of a buggy “alarm system.”

Thus, it is very important to develop tools to assist us in constructing formal proofs or checking that formal proofs are correct. Such systems do exist, for example Isabelle, COQ, TPS, NUPRL, PVS, Twelf. However, 99.99% of us will not have the time or energy to write formal proofs.

Even if we never write formal proofs, it is important to understand clearly what are the rules of reasoning (proof templates) that we use when we construct informal proofs.

The goal of this chapter is to explain what is a proof and how we construct proofs using various proof templates (also known as proof rules).

This chapter is an abbreviated and informal version of Chapter 2. It is meant for readers who have never been exposed to a presentation of the rules of mathematical reasoning (the rules for constructing mathematical proofs) and basic logic.

1.2 Logical Connectives, Definitions

In order to define the notion of proof rigorously, we would have to define a formal language in which to express statements very precisely and we would have to set up a proof system in terms of axioms and proof rules (also called inference rules). We do not go into this in this chapter as this would take too much time. Instead, we content ourselves with an intuitive idea of what a statement is and focus on stating as precisely as possible the rules of logic (proof templates) that are used in constructing proofs.

In mathematics and computer science, we prove statements. Statements may be atomic or compound, that is, built up from simpler statements using logical connectives, such as implication (if–then), conjunction (and), disjunction (or), negation (not), and (existential or universal) quantifiers.

As examples of atomic statements, we have:

1. “A student is eager to learn.”
2. “A student wants an A.”
3. “An odd integer is never 0.”

4. “The product of two odd integers is odd.”

Atomic statements may also contain “variables” (standing for arbitrary objects). For example

1. human(x): “x is a human.”
2. needs-to-drink(x): “x needs to drink.”

An example of a compound statement is

human(x) ⇒ needs-to-drink(x).

In the above statement, ⇒ is the symbol used for logical implication. If we want to assert that every human needs to drink, we can write

∀x(human(x) ⇒ needs-to-drink(x));

this is read: “For every x, if x is a human, then x needs to drink.”

If we want to assert that some human needs to drink we write

∃x(human(x) ⇒ needs-to-drink(x));

this is read: “There is some x such that, if x is a human, then x needs to drink.”

We often denote statements (also called propositions or (logical) formulae) using letters, such as A, B, P, Q, and so on, typically upper-case letters (but sometimes Greek letters, φ, ψ, etc.).

Compound statements are defined as follows: if P and Q are statements, then

1. the conjunction of P and Q is denoted P ∧ Q (pronounced, P and Q),
2. the disjunction of P and Q is denoted P ∨ Q (pronounced, P or Q),
3. the implication of P and Q is denoted by P ⇒ Q (pronounced, if P then Q, or P implies Q).

We also have the atomic statements ⊥ (falsity), think of it as the statement that is false no matter what; and the atomic statement ⊤ (truth), think of it as the statement that is always true.

The constant ⊥ is also called falsum or absurdum. It is a formalization of the notion of absurdity or inconsistency (a state in which contradictory facts hold).

Given any proposition P it is convenient to define

4. the negation ¬P of P (pronounced, not P) as P ⇒ ⊥. Thus, ¬P (sometimes denoted ¬ P) is just a shorthand for P ⇒ ⊥, and this is denoted by ¬P ≡ (P ⇒ ⊥).
The intuitive idea is that \( \neg P \equiv (P \Rightarrow \bot) \) is true if and only if \( P \) is false. Actually, because we don’t know what truth is, it is “safer” to say that \( \neg P \) is provable if and only if for every proof of \( P \) we can derive a contradiction (namely, \( \bot \) is provable). By provable, we mean that a proof can be constructed using some rules that will be described shortly (see Section 1.3).

Whenever necessary to avoid ambiguities, we add matching parentheses: \( (P \land Q), (P \lor Q), (P \Rightarrow Q) \). For example, \( P \lor Q \land R \) is ambiguous; it means either \( (P \lor (Q \land R)) \) or \( ((P \lor Q) \land R) \).

Another important logical operator is equivalence.

5. the equivalence of \( P \) and \( Q \) is denoted \( P \equiv Q \) (or \( P \iff Q \)); it is an abbreviation for \( (P \Rightarrow Q) \land (Q \Rightarrow P) \). We often say “\( P \) if and only if \( Q \)” or even “\( P \) iff \( Q \)” for \( P \equiv Q \).

As a consequence, to prove a logical equivalence \( P \equiv Q \), we have to prove both implications \( P \Rightarrow Q \) and \( Q \Rightarrow P \).

The meaning of the logical connectives \( (\land, \lor, \Rightarrow, \neg, \equiv) \) is intuitively clear. This is certainly the case for and \( (\land) \), since a conjunction \( P \land Q \) is true if and only if both \( P \) and \( Q \) are true (if we are not sure what “true” means, replace it by the word “provable”). However, for or \( (\lor) \), do we mean inclusive or or exclusive or? In the first case, \( P \lor Q \) is true if both \( P \) and \( Q \) are true, but in the second case, \( P \lor Q \) is false if both \( P \) and \( Q \) are true (again, in doubt change “true” to “provable”). We always mean inclusive or.

The situation is worse for implication \( (\Rightarrow) \). When do we consider that \( P \Rightarrow Q \) is true (provable)? The answer is that it depends on the rules! The “classical” answer is that \( P \Rightarrow Q \) is false (not provable) if and only if \( P \) is true and \( Q \) is false. For an alternative view (that of intuitionistic logic), see Chapter 2. In this chapter (and all others except Chapter 2), we adopt the classical view of logic. Since negation \( (\neg) \) is defined in terms of implication, in the classical view, \( \neg P \) is true if and only if \( P \) is false.

The purpose of the proof rules, or proof templates, is to spell out rules for constructing proofs which reflect, and in fact specify, the meaning of the logical connectives.

Before we present the proof templates it should be said that nothing of much interest can be proven in mathematics if we do not have at our disposal various objects such as numbers, functions, graphs, etc. This brings up the issue of where we begin, what may we assume. In set theory, everything, even the natural numbers, can be built up from the empty set! This is a remarkable construction but it takes a tremendous amount of work. For us, we assume that we know what the set

\[ \mathbb{N} = \{0, 1, 2, 3, \ldots\} \]

of natural numbers is, as well as the set

\[ \mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} \]

of integers (which allows negative natural numbers). We also assume that we know how to add, subtract and multiply (perhaps even divide) integers (as well as some of the basic properties of these operations), and we know what the ordering of the integers is.
1.2. LOGICAL CONNECTIVES, DEFINITIONS

The way to introduce new objects in mathematics is to make definitions. Basically, a definition characterizes an object by some property. Technically, we define a “gizmo” $x$ by introducing a so-called predicate (or property) $\text{gizmo}(x)$, which is an abbreviation for some possibly complicated logical proposition $P(x)$. The idea is that $x$ is a “gizmo” if and only if $\text{gizmo}(x)$ holds if and only if $P(x)$ holds. We may write

$$\text{gizmo}(x) \equiv P(x),$$

or

$$\text{gizmo}(x) \overset{\text{def}}{=} P(x).$$

Note that gizmo is just a name, but $P(x)$ is a (possibly complex) proposition.

It is also convenient to define properties (also called predicates) of one or more objects as abbreviations for possibly complicated logical propositions. In this case, a property $p(x_1, \ldots, x_n)$ of some objects $x_1, \ldots, x_n$ holds if and only if some logical proposition $P(x_1, \ldots, x_n)$ holds. We may write

$$p(x_1, \ldots, x_n) \equiv P(x_1, \ldots, x_n)$$

or

$$p(x_1, \ldots, x_n) \overset{\text{def}}{=} P(x_1, \ldots, x_n).$$

Here too, $p$ is just a name, but $P(x_1, \ldots, x_n)$ is a (possibly complex) proposition.

Let us give a few examples of definitions.

**Definition 1.1.** Given two integers $a, b \in \mathbb{Z}$, we say that $a$ is a multiple of $b$ if there is some $c \in \mathbb{Z}$ such that $a = bc$. In this case, we say that $a$ is divisible by $b$, that $b$ is a divisor of $a$ (or $b$ is a factor of $a$), and that $b$ divides $a$. We use the notation $b \mid a$.

In Definition 1.1, we define the predicate divisible($a, b$) in terms of the proposition $P(a, b)$ given by

$$\text{there is some } c \in \mathbb{N} \text{ such that } a = bc.$$  

For example, $15$ is divisible by $3$ since $15 = 3 \cdot 5$. On the other hand, $14$ is not divisible by $3$.

**Definition 1.2.** A integer $a \in \mathbb{Z}$ is even if it is of the form $a = 2b$ for some $b \in \mathbb{Z}$, odd if it is of the form $a = 2b + 1$ for some $b \in \mathbb{Z}$.

In Definition 1.2, the property even($a$) of $a$ being even is defined in terms of the predicate $P(a)$ given by

$$\text{there is some } b \in \mathbb{N} \text{ such that } a = 2b.$$  

The property odd($a$) is obtained by changing $a = 2b$ to $a = 2b + 1$ in $P(a)$. The integer $14$ is even, and the integer $15$ is odd. Beware that we can’t assert yet that if an integer is not even then it is odd. Although this is true, this needs to proven and requires induction, which we haven’t discussed yet.

Prime numbers play a fundamental role in mathematics. Let us review their definition.
Definition 1.3. A natural number \( p \in \mathbb{N} \) is prime if \( p \geq 2 \) and if the only divisors of \( p \) are 1 and \( p \).

In the above definition, the property \( \text{prime}(p) \) is defined by the predicate \( P(p) \) given by

\[
p \geq 2, \text{ and for all } q \in \mathbb{N}, \text{ if divisible}(p,q), \text{ then } q = 1 \text{ or } q = p.
\]

If we expand the definition of a prime number by replacing the predicate divisible by its defining formula we get a rather complicated formula. Definitions allow us to be more concise.

According to Definition 1.3, the number 1 is not prime even though it is only divisible by 1 and itself (again 1). The reason for not accepting 1 as a prime is not capricious. It has to do with the fact that if we allowed 1 to be a prime, then certain important theorems (such as the unique prime factorization theorem) would no longer hold.

Nonprime natural numbers (besides 1) have a special name too.

Definition 1.4. A natural number \( a \in \mathbb{N} \) is composite if \( a = bc \) for some natural numbers \( b, c \) with \( b, c \geq 2 \).

For example, 4, 15, 36 are composite. Note that 1 is neither prime nor a composite.
We are now ready to introduce the proof templates for implication.

1.3 Meaning of Implication and Proof Templates for Implication

First, it is important to say that there are two types of proofs:

1. Direct proofs.

2. Indirect proofs.

Indirect proofs use the proof–by–contradiction principle, which will be discussed soon.

Because propositions do not arise from the vacuum but instead are built up from a set of atomic propositions using logical connectives (here, \( \Rightarrow \)), we assume the existence of an “official set of atomic propositions,” or set of propositional symbols, \( \text{PS} = \{ P_1, P_2, P_3, \ldots \} \). So, for example, \( P_1 \Rightarrow P_2 \) and \( P_1 \Rightarrow (P_2 \Rightarrow P_1) \) are propositions. Typically, we use upper-case letters such as \( P, Q, R, S, A, B, C, \) and so on, to denote arbitrary propositions formed using atoms from \( \text{PS} \).

We begin by presenting proof templates to construct direct proofs of implications. An implication \( P \Rightarrow Q \) can be understood as an if–then statement; that is, if \( P \) is true then \( Q \) is also true. A better interpretation is that any proof of \( P \Rightarrow Q \) can be used to construct a proof of \( Q \) given any proof of \( P \). As a consequence of this interpretation, we show later that if \( \neg P \) is provable, then \( P \Rightarrow Q \) is also provable (instantly) whether or not \( Q \) is provable. In such
a situation, we often say that \( P \Rightarrow Q \) is *vacuously provable*. For example, \( (P \land \neg P) \Rightarrow Q \) is provable for any arbitrary \( Q \).

It might help to view the action of proving an implication \( P \Rightarrow Q \) as the construction of a program that converts a proof of \( P \) into a proof of \( Q \). Then, if we supply a proof of \( P \) as input to this program (the proof of \( P \Rightarrow Q \)), it will output a proof of \( Q \). So, if we don’t give the right kind of input to this program, for example, a “wrong proof” of \( P \), we should not expect the program to return a proof of \( Q \). However, this does not say that the program is incorrect; the program was designed to do the right thing only if it is given the right kind of input. From this functional point of view (also called constructive), we should not be shocked that the provability of an implication \( P \Rightarrow Q \) generally yields no information about the provability of \( Q \).

For a concrete example, say \( P \) stands for the statement, “Our candidate for president wins in Pennsylvania” and \( Q \) stands for “Our candidate is elected president.”

Then, \( P \Rightarrow Q \) asserts that if our candidate for president wins in Pennsylvania then our candidate is elected president.

If \( P \Rightarrow Q \) holds, then if indeed our candidate for president wins in Pennsylvania then for sure our candidate will win the presidential election. However, if our candidate does not win in Pennsylvania, we can’t predict what will happen. Our candidate may still win the presidential election but he may not.

If our candidate president does not win in Pennsylvania, then the statement \( P \Rightarrow Q \) should be regarded as holding, though perhaps uninteresting.

For one more example, let \( \text{odd}(n) \) assert that \( n \) is an odd natural number and let \( Q(n,a,b) \) assert that \( a^n + b^n \) is divisible by \( a + b \), where \( a, b \) are any given natural numbers. By divisible, we mean that we can find some natural number \( c \), so that

\[
a^n + b^n = (a + b)c.
\]

Then, we claim that the implication \( \text{odd}(n) \Rightarrow Q(n,a,b) \) is provable.

As usual, let us assume \( \text{odd}(n) \), so that \( n = 2k + 1 \), where \( k = 0, 1, 2, 3, \ldots \). But then, we can easily check that

\[
a^{2k+1} + b^{2k+1} = (a + b) \left( \sum_{i=0}^{2k} (-1)^i a^{2k-i} b^i \right),
\]

which shows that \( a^{2k+1} + b^{2k+1} \) is divisible by \( a + b \). Therefore, we proved the implication \( \text{odd}(n) \Rightarrow Q(n,a,b) \).

If \( n \) is not odd, then the implication \( \text{odd}(n) \Rightarrow Q(n,a,b) \) yields no information about the provability of the statement \( Q(n,a,b) \), and that is fine. Indeed, if \( n \) is even and \( n \geq 2 \), then in general, \( a^n + b^n \) is not divisible by \( a + b \), but this may happen for some special values of \( n, a, \) and \( b \), for example: \( n = 2, a = 2, b = 2 \).
During the process of constructing a proof, it may be necessary to introduce a list of hypotheses, also called premises (or assumptions), which grows and shrinks during the proof. When a proof is finished, it should have an empty list of premises.

The process of managing the list of premises during a proof is a bit technical. In Chapter 2 we study carefully two methods for managing the list of premises that may appear during a proof. In this chapter we are much more casual about it, which is the usual attitude when we write informal proofs. It suffices to be aware that at certain steps, some premises must be added, and at other special steps, premises must be discarded. We may view this as a process of making certain propositions active or inactive. To make matters clearer, we call the process of constructing a proof using a set of premises a deduction, and we reserve the word proof for a deduction whose set of premises is empty. Every deduction has a possibly empty list of premises, and a single conclusion. The list of premises is usually denoted by \( \Gamma \), and if the conclusion of the deduction is \( P \), we say that we have a deduction of \( P \) from the premises \( \Gamma \).

The first proof template allows us to make obvious deductions.

**Proof Template 1.1. (Trivial Deductions)**

If \( P_1, \ldots, P_i, \ldots, P_n \) is a list of propositions assumed as premises (where each \( P_i \) may occur more than once), then for each \( P_i \), we have a deduction with conclusion \( P_i \).

All other proof templates are of two kinds: introduction rules or elimination rules. The meaning of these words will be explained after stating the next two proof templates.

The second proof template allows the construction of a deduction whose conclusion is an implication \( P \Rightarrow Q \).

**Proof Template 1.2. (Implication–Intro)**

Given a list \( \Gamma \) of premises (possibly empty), to obtain a deduction with conclusion \( P \Rightarrow Q \), proceed as follows:

1. Add one or more occurrences of \( P \) as additional premises to the list \( \Gamma \).
2. Make a deduction of the conclusion \( Q \), from \( P \) and the premises in \( \Gamma \).
3. Delete \( P \) from the list of premises.

The third proof template allows the constructions of a deduction from two other deductions.

**Proof Template 1.3. (Implication–Elim, or Modus–Ponens)**

Given a deduction with conclusion \( P \Rightarrow Q \) from a list of premises \( \Gamma \) and a deduction with conclusion \( P \) from a list of premises \( \Delta \), we obtain a deduction with conclusion \( Q \). The list of premises of this new deduction is the list \( \Gamma, \Delta \).
The modus–ponens proof template formalizes the use of auxiliary lemmas, a mechanism that we use all the time in making mathematical proofs. Think of \( P \Rightarrow Q \) as a lemma that has already been established and belongs to some database of (useful) lemmas. This lemma says if I can prove \( P \) then I can prove \( Q \). Now, suppose that we manage to give a proof of \( P \). It follows from modus–ponens that \( Q \) is also provable.

Mathematicians are very fond of modus–ponens because it gives a potential method for proving important results. If \( Q \) is an important result and if we manage to build a large catalog of implications \( P \Rightarrow Q \), there may be some hope that, some day, \( P \) will be proven, in which case \( Q \) will also be proven. So, they build large catalogs of implications! This has been going on for the famous problem known as \( P \) versus \( NP \). So far, no proof of any premise of such an implication involving \( P \) versus \( NP \) has been found (and it may never be found).

Beware, when we deduce that an implication \( P \Rightarrow Q \) is provable, we do not prove that \( P \) and \( Q \) are provable; we only prove that if \( P \) is provable then \( Q \) is provable.

Example 1.1. Let us give a simple example of the use of Proof Template 1.2. Recall that a natural number \( n \) is odd iff it is of the form \( 2k + 1 \), where \( k \in \mathbb{N} \). Let us denote the fact that a number \( n \) is odd by \( \text{odd}(n) \). We would like to prove the implication\[ \text{odd}(n) \Rightarrow \text{odd}(n + 2). \]

Following Proof Template 1.2, we add \( \text{odd}(n) \) as a premise (which means that we take as proven the fact that \( n \) is odd) and we try to conclude that \( n + 2 \) must be odd. However, to say that \( n \) is odd is to say that \( n = 2k + 1 \) for some natural number \( k \). Now, \[ n + 2 = 2k + 1 + 2 = 2(k + 1) + 1, \] which means that \( n + 2 \) is odd. (Here, \( n = 2h + 1 \), with \( h = k + 1 \), and \( k + 1 \) is a natural number because \( k \) is.)
Thus, we proven that if we assume odd($n$), then we can conclude odd($n + 2$), and according to Proof Template 1.2, by step (3) we delete the premise odd($n$) and we obtain a proof of the proposition
\[ \text{odd}(n) \Rightarrow \text{odd}(n + 2). \]

It should be noted that the above proof of the proposition odd($n$) \( \Rightarrow \) odd($n + 2$) does not depend on any premises (other than the implicit fact that we are assuming $n$ is a natural number). In particular, this proof does not depend on the premise odd($n$), which was assumed (became “active”) during our subproof step. Thus, after having applied the Proof Template 1.2, we made sure that the premise odd($n$) is deactivated.

**Example 1.2.** For a second example, we wish to prove the proposition $P \Rightarrow P$.

According to Proof Template 1.2, we assume $P$. But then, by Proof Template 1.1, we obtain a deduction with premise $P$ and conclusion $P$; by executing step (3) of Proof Template 1.2, the premise $P$ is deleted, and we obtain a deduction of $P \Rightarrow P$ from the empty list of premises. Thank God, $P \Rightarrow P$ is provable!

Proofs described in words as above are usually better understood when represented as trees. We will reformulate our proof templates in tree form and explain very precisely how to build proofs as trees in Chapter 2. For now, we use tree representations of proofs in an informal way.

### 1.4 Proof Trees and Deduction Trees

A proof tree is drawn with its leaves at the top, corresponding to assumptions, and its root at the bottom, corresponding to the conclusion. In computer science, trees are usually drawn with their root at the top and their leaves at the bottom, but proof trees are drawn as the trees that we see in nature. Instead of linking nodes by edges, it is customary to use horizontal bars corresponding to the proof templates. One or more nodes appear as premises above a vertical bar, and the conclusion of the proof template appears immediately below the vertical bar.

According to the first step of proof of $P \Rightarrow P$ (presented in words) we move the premise $P$ to the list of premises, building a deduction of the conclusion $P$ from the premise $P$ corresponding to the following unfinished tree in which some leaf is labeled with the premise $P$ but with a missing subtree establishing $P$ as the conclusion:

\[
\begin{array}{c}
\text{Implication-Intro}\ x \\
\hline
P
\end{array}
\]

The premise $P$ is tagged with the label $x$ which corresponds to the proof rule which causes its deletion from the list of premises.

In order to obtain a proof we need to apply a proof template which allows use to deduce $P$ from $P$ and of course this is the Trivial Deduction proof template.
The finished proof is represented by the tree shown below. Observe that the premise $P$ is tagged with the symbol √, which means that it has been deleted from the list of premises. The tree representation of proofs also has the advantage that we can tag the premises in such a way that each tag indicates which rule causes the corresponding premise to be deleted. In the tree below, the premise $P$ is tagged with $x$, and it is deleted when the proof template indicated by $x$ is applied.

\[
\begin{array}{c}
\frac{P^x \checkmark}{P} \\
\text{Implication-Intro } x \\
\hline
\end{array}
\]

**Example 1.3.** For a third example, we prove the proposition $P \Rightarrow (Q \Rightarrow P)$.

According to Proof Template 1.2, we assume $P$ as a premise and we try to prove $Q \Rightarrow P$ assuming $P$. In order to prove $Q \Rightarrow P$, by Proof Template 1.2, we assume $Q$ as a new premise so the set of premises becomes \{P, Q\}, and then we try to prove $P$ from $P$ and $Q$.

At this stage we have the following unfinished tree with two leaves labeled $P$ and $Q$ but with a missing subtree establishing $P$ as the conclusion:

\[
\begin{array}{c}
P^x, Q^y \\
P \\
\hline
Q \Rightarrow P \\
\text{Implication-Intro } y \\
\hline
P \Rightarrow (Q \Rightarrow P) \\
\text{Implication-Intro } x \\
\end{array}
\]

We need to find a deduction of $P$ from the premises $P$ and $Q$. By Proof Template 1.1 (trivial deductions), we have a deduction with the list of premises \{P, Q\} and conclusion $P$. Then, executing step (3) of Proof Template 1.2 twice, we delete the premises $Q$, and then the premise $P$ (in this order), and we obtain a proof of $P \Rightarrow (Q \Rightarrow P)$. The above proof of $P \Rightarrow (Q \Rightarrow P)$ (presented in words) is represented by the following tree:

\[
\begin{array}{c}
P^{x\checkmark}, Q^{y\checkmark} \\
P \\
\hline
Q \Rightarrow P \\
\text{Implication-Intro } y \\
\hline
P \Rightarrow (Q \Rightarrow P) \\
\text{Implication-Intro } x \\
\end{array}
\]

Observe that both premises $P$ and $Q$ are tagged with the symbol √, which means that they have been deleted from the list of premises.

We tagged the premises in such a way that each tag indicates which rule causes the corresponding premise to be deleted. In the above tree, $Q$ is tagged with $y$, and it is deleted when the proof template indicated by $y$ is applied, and $P$ is tagged with $x$, and it is deleted when the proof template indicated by $x$ is applied. In a proof, all leaves must be tagged with the symbol √.
Example 1.4. Let us now give a proof of $P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)$.

Using Proof Template 1.2, we assume both $P$ and $P \Rightarrow Q$ and we try to prove $Q$. At this stage we have the following unfinished tree with two leaves labeled $P \Rightarrow Q$ and $P$ but with a missing subtree establishing $Q$ as the conclusion:

\[
\begin{array}{c}
(P \Rightarrow Q)^x \\
\downarrow \\
Q \\
\downarrow \\
(P \Rightarrow Q) \Rightarrow Q
\end{array}
\]

Implication-Intro $x$

\[
\begin{array}{c}
P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)
\end{array}
\]

Implication-Intro $y$

We can use Proof Template 1.3 to derive a deduction of $Q$ from $P \Rightarrow Q$ and $P$. Finally, we execute step (3) of Proof Template 1.2 to delete $P \Rightarrow Q$ and $P$ (in this order), and we obtain a proof of $P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)$. A tree representation of the above proof is shown below.

\[
\begin{array}{c}
(P \Rightarrow Q)^x \checkmark \\
\downarrow \\
\checkmark \\
\downarrow \\
Q \\
\downarrow \\
(P \Rightarrow Q) \Rightarrow Q
\end{array}
\]

Implication-Elim

\[
\begin{array}{c}
P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)
\end{array}
\]

Implication-Intro $x$

\[
\begin{array}{c}
(P \Rightarrow Q)^x \checkmark \\
\downarrow \\
\checkmark \\
\downarrow \\
Q \\
\downarrow \\
(P \Rightarrow Q) \Rightarrow Q
\end{array}
\]

Implication-Elim

\[
\begin{array}{c}
P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)
\end{array}
\]

Implication-Intro $y$

Remark: We have not yet examined how we can represent precisely arbitrary deductions. This can be done using certain types of trees where the nodes are tagged with lists of premises. Two methods for doing this are carefully defined in Chapter 2. It turns out that the same premise may be used in more than one location in the tree, but in our informal presentation, we ignore such fine details.

We now describe the proof templates dealing with the connectives $\neg, \land, \lor, \equiv$.

1.5 Proof Templates for $\neg$

Recall that $\neg P$ is an abbreviation for $P \Rightarrow \bot$. We begin with the proof templates for negation, for direct proofs.

Proof Template 1.4. (Negation–Intro)

Given a list $\Gamma$ of premises (possibly empty), to obtain a deduction with conclusion $\neg P$, proceed as follows:

1. Add one or more occurrences of $P$ as additional premises to the list $\Gamma$.

2. Derive a contradiction. More precisely, make a deduction of the conclusion $\bot$ from $P$ and the premises in $\Gamma$. 

3. Delete $P$ from the list of premises.

Proof Template 1.4 is a special case of Proof Template 1.2, since $\neg P$ is an abbreviation for $P \Rightarrow \bot$.

**Proof Template 1.5. (Negation–Elim)**

Given a deduction with conclusion $\neg P$ from a list of premises $\Gamma$ and a deduction with conclusion $P$ from a list of premises $\Delta$, we obtain a contradiction; that is, a deduction with conclusion $\bot$. The list of premises of this new deduction is $\Gamma, \Delta$.

Proof Template 1.5 is a special case of Proof Template 1.3, since $\neg P$ is an abbreviation for $P \Rightarrow \bot$.

**Proof Template 1.6. (Perp–Elim)**

Given a deduction with conclusion $\bot$ (a contradiction), for every proposition $Q$, we obtain a deduction with conclusion $Q$. The list of premises of this new deduction is the same as the original list of premises.

The last proof template for negation constructs an indirect proof; it is the proof–by–contradiction principle.

**Proof Template 1.7. (Proof–By–Contradiction Principle)**

Given a list $\Gamma$ of premises (possibly empty), to obtain a deduction with conclusion $P$, proceed as follows:

1. Add one of more occurrences of $\neg P$ as additional premises to the list $\Gamma$.

2. Derive a contradiction. More precisely, make a deduction of the conclusion $\bot$ from $\neg P$ and the premises in $\Gamma$.

3. Delete $\neg P$ from the list of premises.

Proof Template 1.7 (the proof–by–contradiction principle) also has the fancy name of *reductio ad absurdum rule*, for short *RAA*.

Proof Template 1.6 may seem silly and one might wonder why we stated it. It turns out that it is subsumed by Proof Template 1.7, but it is still useful to state it as a proof template.

**Example 1.5.** Let us prove that for every natural number $n$, if $n^2$ is odd, then $n$ itself must be odd.

We use the proof–by–contradiction principle (Proof Template 1.7), so we assume that $n$ is not odd, which means that $n$ is even. (Actually, in this step we are using a property of the natural numbers that is proven by induction but let’s not worry about that right now; a proof can be found in Section 1.12) But to say that $n$ is even means that $n = 2k$ for some $k$ and then $n^2 = 4k^2 = 2(2k^2)$, so $n^2$ is even, contradicting the assumption that $n^2$ is odd.

By the proof–by–contradiction principle (Proof Template 1.7), we conclude that $n$ must be odd.
Example 1.6. Let us prove that $\neg\neg P \Rightarrow P$.

It turns out that this requires using the proof–by–contradiction principle (Proof Template 1.7). First by Proof Template 1.2, assume $\neg\neg P$ as a premise. Then by the proof–by–contradiction principle (Proof template 1.7), in order to prove $P$, assume $\neg P$. By Proof Template 1.5, we obtain a contradiction ($\bot$). Thus, by step (3) of the proof–by–contradiction principle (Proof Template 1.7), we delete the premise $\neg P$ and we obtain a deduction of $P$ from $\neg\neg P$. Finally, by step (3) of Proof Template 1.2, we delete the premise $\neg\neg P$ and obtain a proof of $\neg\neg P \Rightarrow P$. This proof has the following tree representation.

$$
\begin{array}{c}
\neg\neg P^y \\
\bot \\
P \\
\hline
\neg P \\
\end{array}
\quad
\begin{array}{c}
\neg P^x \\
\bot \\
P \\
\hline
\neg\neg P \\
\end{array}
\quad
\begin{array}{c}
\text{Negation-Elim} \\
\text{RAA}_x \\
\text{Implication-Intro}_y \\
\end{array}
$$

Example 1.7. Now, we prove that $P \Rightarrow \neg\neg P$.

First by Proof Template 1.2, assume $P$ as a premise. In order to prove $\neg\neg P$ from $P$, by Proof Template 1.4, assume $\neg P$. We now have the two premises $\neg P$ and $P$, so by Proof Template 1.5, we obtain a contradiction ($\bot$). By step (3) of Proof Template 1.4, we delete the premise $\neg P$ and we obtain a deduction of $\neg\neg P$ from $P$. Finally, by step (3) of Proof Template 1.2, delete the premise $P$ to obtain a proof of $P \Rightarrow \neg\neg P$. This proof has the following tree representation.

$$
\begin{array}{c}
\neg P^y \\
\bot \\
\neg\neg P^x \\
\hline
P \\
\bot \\
\hline
\neg\neg P \\
\end{array}
\quad
\begin{array}{c}
\text{Negation-Elim} \\
\text{Negation-Intro}_x \\
\text{Implication-Intro}_y \\
\end{array}
$$

Observe that the previous two examples show that the equivalence $P \equiv \neg\neg P$ is provable. As a consequence of this equivalence, if we prove a negated proposition $\neg P$ using the proof–by–contradiction principle, we assume $\neg\neg P$ and we deduce a contradiction. But since $\neg\neg P$ and $P$ are equivalent (as far as provability), this amounts to deriving a contradiction from $P$, which is just the Proof Template 1.4.

In summary, to prove a negated proposition $\neg P$, always use Proof Template 1.4.

On the other hand, to prove a nonnegated proposition, it is generally not possible to tell if a direct proof exists or if the proof–by–contradiction principle is required. There are propositions for which it is required, for example $\neg\neg P \Rightarrow P$ and $(\neg(P \Rightarrow Q)) \Rightarrow P$.

Example 1.8. Let us now prove that $(\neg(P \Rightarrow Q)) \Rightarrow \neg Q$.

First by Proof Template 1.2, we add $\neg(P \Rightarrow Q)$ as a premise. Then, in order to prove $\neg Q$ from $\neg(P \Rightarrow Q)$, we use Proof Template 1.4 and we add $Q$ as a premise. Now, recall that we showed in Example 1.3 that $P \Rightarrow Q$ is provable assuming $Q$ (with $P$ and $Q$ switched).
Then since $\neg(P \Rightarrow Q)$ is a premise, by Proof Template 1.5, we obtain a deduction of $\bot$. We now execute step (3) of Proof Template 1.4, delete the premise $Q$ to obtain a deduction of $\neg Q$ from $\neg(P \Rightarrow Q)$, and we execute step (3) of Proof Template 1.2 to delete the premise $\neg(P \Rightarrow Q)$ and obtain a proof of $(\neg(P \Rightarrow Q)) \Rightarrow \neg Q$. The above proof corresponds to the following tree.

Here is an example using Proof Templates 1.6 (Perp–Elim) and 1.7 (RAA).

**Example 1.9.** Let us prove that $(\neg(P \Rightarrow Q)) \Rightarrow P$.

First we use Proof Template 1.2, and we assume $\neg(P \Rightarrow Q)$ as a premise. Next we use the proof–by–contradiction principle (Proof Template 1.7). So, in order to prove $P$, we assume $\neg P$ as another premise. The next step is to deduce $P \Rightarrow Q$. By Proof Template 1.2, we assume $P$ as an additional premise. By Proof Template 1.5, from $\neg P$ and $P$ we obtain a deduction of $\bot$, and then by Proof Template 1.6 a deduction of $Q$ from $\neg P$ and $P$. By Proof Template 1.2, executing step (3), we delete the premise $P$ and we obtain a deduction of $P \Rightarrow Q$. At this stage, we have the premises $\neg P$, $\neg(P \Rightarrow Q)$ and a deduction of $P \Rightarrow Q$, so by Proof Template 1.5, we obtain a deduction of $\bot$. This is a contradiction, so by step (3) of the proof–by–contradiction principle (Proof Template 1.7) we can delete the premise $\neg P$, and we have a deduction of $P$ from $\neg(P \Rightarrow Q)$. Finally, we execute step (3) of Proof Template 1.2 and delete the premise $\neg(P \Rightarrow Q)$, which yields the desired proof of $(\neg(P \Rightarrow Q)) \Rightarrow P$. The above proof has the following tree representation.
that the proof–by–contradiction principle must be used, and unfortunately there is no shorter proof.

Even though Proof Template 1.4 qualifies as a direct proof template, it proceeds by deriving a contradiction, so I suggest to call it the proof–by–contradiction for negated propositions principle.

**Remark:** The fact that the implication \( \neg \neg P \Rightarrow P \) is provable has the interesting consequence that if we take \( \neg \neg P \Rightarrow P \) as an axiom (which means that \( \neg \neg P \Rightarrow P \) is assumed to be provable without requiring any proof), then the proof–by–contradiction principle (Proof Template 1.7) becomes redundant. Indeed, Proof Template 1.7 is subsumed by Proof Template 1.4, because if we have a deduction of \( \bot \) from \( \neg P \), then by Proof Template 1.4 we delete the premise \( \neg P \) to obtain a deduction of \( \neg \neg P \). Since \( \neg \neg P \Rightarrow P \) is assumed to be provable, by Proof Template 1.3, we get a proof of \( P \). The tree shown below illustrates what is going on. In this tree, a proof of \( \bot \) from the premise \( \neg P \) is denoted by \( \mathcal{D} \).

\[
\begin{array}{c}
\neg \neg P \Rightarrow P \\
\neg P \\
\bot \\
\neg \neg P \Rightarrow P \\
\neg \neg P \\
P
\end{array}
\]

Negation-Intro \( x \)

Implication-Elim

Proof Templates 1.5 and 1.6 together imply that if a contradiction is obtained during a deduction because two inconsistent propositions \( P \) and \( \neg P \) are obtained, then all propositions are provable (anything goes). This explains why mathematicians are leary of inconsistencies.

### 1.6 Proof Templates for \( \land, \lor, \equiv \)

The proof templates for conjunction are the simplest.

**Proof Template 1.8. (And–Intro)**

*Given a deduction with conclusion \( P \) from a list of premises \( \Gamma \) and a deduction with conclusion \( Q \) from a list of premises \( \Delta \), we obtain a deduction with conclusion \( P \land Q \). The list of premises of this new deduction is \( \Gamma, \Delta \).*

**Proof Template 1.9. (And–Elim)**

*Given a deduction with conclusion \( P \land Q \), we obtain a deduction with conclusion \( P \), and a deduction with conclusion \( Q \). The list of premises of these new deductions is the same as the list of premises of the original deduction.*

Let us consider a few examples of proofs using the proof templates for conjunction as well as Proof Templates 1.4 and 1.7.
Example 1.10. Let us prove that for any natural number $n$, if $n$ is divisible by 2 and $n$ is divisible by 3, then $n$ is divisible by 6. This is expressed by the proposition

$$\left( (2 \mid n) \land (3 \mid n) \right) \Rightarrow (6 \mid n).$$

We start by using Proof Templates 1.2 and we add the premise $(2 \mid n) \land (3 \mid n)$. Using Proof Template 1.9 twice, we obtain deductions of $(2 \mid n)$ and $(3 \mid n)$ from $(2 \mid n) \land (3 \mid n)$. But $(2 \mid n)$ means that

$$n = 2a$$

for some $a \in \mathbb{N}$, and $3 \mid n$ means that

$$n = 3b$$

for some $b \in \mathbb{N}$. This implies that

$$n = 2a = 3b.$$ 

Because 2 and 3 are relatively prime (their only common divisor is 1), the number 2 must divide $b$ (and 3 must divide $a$) so $b = 2c$ for some $c \in \mathbb{N}$. Here we are using Euclid’s lemma. So, we have shown that

$$n = 3b = 3 \cdot 2c = 6c,$$

which says that $n$ is divisible by 6. We conclude with step (3) of Proof Template 1.2 by deleting the premise $(2 \mid n) \land (3 \mid n)$ and we obtain our proof.

Example 1.11. Let us prove that for any natural number $n$, if $n$ is divisible by 6, then $n$ is divisible by 2 and $n$ is divisible by 3. This is expressed by the proposition

$$(6 \mid n) \Rightarrow ((2 \mid n) \land (3 \mid n)).$$

We start by using Proof Template 1.2 and we add the premise $6 \mid n$. This means that

$$n = 6a = 2 \cdot 3a$$

for some $a \in \mathbb{N}$. This implies that $2 \mid n$ and $3 \mid n$, so we have a deduction of $2 \mid n$ from the premise $6 \mid n$ and a deduction of $3 \mid n$ from the premise $6 \mid n$. By Proof Template 1.8, we obtain a deduction of $(2 \mid n) \land (3 \mid n)$ from $6 \mid n$, and we apply step (3) of Proof Template 1.2 to delete the premise $6 \mid n$ and obtain our proof.

Example 1.12. Let us prove that a natural number $n$ cannot be even and odd simultaneously. This is expressed as the proposition

$$\neg((\text{odd}(n) \land \text{even}(n))).$$

We begin with Proof Template 1.4 and we assume $\text{odd}(n) \land \text{even}(n)$ as a premise. Using Proof Template 1.9 twice, we obtain deductions of $\text{odd}(n)$ and $\text{even}(n)$ from $\text{odd}(n) \land \text{even}(n)$. Now $\text{odd}(n)$ says that $n = 2a + 1$ for some $a \in \mathbb{N}$, and $\text{even}(n)$ says that $n = 2b$ for some $b \in \mathbb{N}$. But then,

$$n = 2a + 1 = 2b,$$
so we obtain $2(b - a) = 1$. Since $b - a$ is an integer, either $2(b - a) = 0$ (if $a = b$) or $|2(b - a)| \geq 2$, so we obtain a contradiction. Applying step (3) of Proof Template 1.4, we delete the premise odd($n$) $\land$ even($n$) and we have a proof of $\neg$(odd($n$) $\land$ even($n$)).

**Example 1.13.** Let us prove that $(\neg(P \Rightarrow Q)) \Rightarrow (P \land \neg Q)$.

We start by using Proof Templates 1.2 and we add $(\neg(P \Rightarrow Q))$ as a premise. Now, in Example 1.9 we showed that $(\neg(P \Rightarrow Q)) \Rightarrow P$ is provable, and this proof contains a deduction of $P$ from $(\neg(P \Rightarrow Q))$. Similarly, in Example 1.8 we showed that $(\neg(P \Rightarrow Q)) \Rightarrow \neg Q$ is provable, and this proof contains a deduction of $\neg Q$ from $(\neg(P \Rightarrow Q))$. By proof Template 1.8, we obtain a deduction of $P \land \neg Q$ from $(\neg(P \Rightarrow Q))$, and executing step (3) of Proof Templates 1.2, we obtain a proof of $(\neg(P \Rightarrow Q)) \Rightarrow (P \land \neg Q)$. The following tree represents the above proof. Observe that two copies of the premise $(\neg(P \Rightarrow Q))$ are needed.

![Tree representation of the proof](image)

Next, we present the proof templates for disjunction.

**Proof Template 1.10.** (Or–Intro)

Given a list $\Gamma$ of premises (possibly empty),

1. If we have a deduction with conclusion $P$, then we obtain a deduction with conclusion $P \lor Q$.

2. If we have a deduction with conclusion $Q$, then we obtain a deduction with conclusion $P \lor Q$.

In both cases, the new deduction has $\Gamma$ as premises.

**Proof Template 1.11.** (Or–Elim or Proof–By–Cases)

Given three lists of premises $\Gamma$, $\Delta$, $\Lambda$, to obtain a deduction of some proposition $R$ as conclusion, proceed as follows:

1. Construct a deduction of some disjunction $P \lor Q$ from the list of premises $\Gamma$.

2. Add one or more occurrences of $P$ as additional premises to the list $\Delta$ and find a deduction of $R$ from $P$ and $\Delta$. 


3. Add one or more occurrences of $Q$ as additional premises to the list $\Lambda$ and find a deduction of $R$ from $Q$ and $\Lambda$.

The list of premises after applying this rule is $\Gamma, \Delta, \Lambda$.

Note that in making the two deductions of $R$, the premise $P \lor Q$ is not assumed.

**Example 1.14.** Let us show that for any natural number $n$, if $4$ divides $n$ or $6$ divides $n$, then $2$ divides $n$. This can expressed as

$$((4 \mid n) \lor (6 \mid n)) \Rightarrow (2 \mid n).$$

First, by Proof Template 1.2, we assume $(4 \mid n) \lor (6 \mid n)$ as a premise. Next, we use Proof Template 1.11, the proof–by–cases principle. First, assume $(4 \mid n)$. This means that

$$n = 4a = 2 \cdot 2a$$

for some $a \in \mathbb{N}$. Therefore, we conclude that $2 \mid n$. Next, assume $(6 \mid n)$. This means that

$$n = 6b = 2 \cdot 3b$$

for some $b \in \mathbb{N}$. Again, we conclude that $2 \mid n$. Since $(4 \mid n) \lor (6 \mid n)$ is a premise, by Proof Template 1.11, we can obtain a deduction of $2 \mid n$ from $(4 \mid n) \lor (6 \mid n)$. Finally, by Proof Template 1.2, we delete the premise $(4 \mid n) \lor (6 \mid n)$ to obtain our proof.

Proof Template 1.10 (Or–Intro) may seem trivial, so let us show an example illustrating its use.

**Example 1.15.** Let us prove that $\neg(P \lor Q) \Rightarrow (\neg P \land \neg Q)$.

First by Proof Template 1.2, we assume $\neg(P \lor Q)$ (two copies). In order to derive $\neg P$, by Proof Template 1.4, we also assume $P$. Then by Proof Template 1.10 we deduce $P \lor Q$, and since we have the premise $\neg(P \lor Q)$, by Proof Template 1.5 we obtain a contradiction. By Proof Template 1.4, we can delete the premise $P$ and obtain a deduction of $\neg P$ from $\neg(P \lor Q)$.

In a similar way we can construct a deduction of $\neg Q$ from $\neg(P \lor Q)$. By Proof Template 1.8, we get a deduction of $\neg P \land \neg Q$ from $\neg(P \lor Q)$, and we finish by applying Proof Template 1.2. A tree representing the above proof is shown below.

```
\begin{align*}
\neg(P \lor Q) & \quad \quad \quad P^{\lor} \quad \text{Or-Intro} \quad \quad \quad Q^{\lor} \quad \text{Or-Intro} \\
\dfrac{\dfrac{P \lor Q}{\neg P \land \neg Q}}{\neg(P \lor Q) \Rightarrow (\neg P \land \neg Q)}
\end{align*}
```
The proposition \((\neg P \land \neg Q) \Rightarrow \neg (P \lor Q)\) is also provable using the proof–by–cases principle. Here is a proof tree; we leave it as an exercise to the reader to check that the proof templates have been applied correctly.

As a consequence the equivalence
\[
\neg (P \lor Q) \equiv (\neg P \land \neg Q)
\]
is provable. This is one of three identities known as de Morgan laws.

**Example 1.16.** Next let us prove that \(\neg(\neg P \lor \neg Q) \Rightarrow P\).

First by Proof Template 1.2, we assume \(\neg(\neg P \lor \neg Q)\) as a premise. In order to prove \(P\) from \(\neg(\neg P \lor \neg Q)\), we use the proof–by–contradiction principle (Proof Template 1.7). So, we add \(\neg P\) as a premise. Now, by Proof Template 1.10, we can deduce \(\neg P \lor \neg Q\) from \(\neg P\), and since \(\neg(\neg P \lor \neg Q)\) is a premise, by Proof Template 1.5, we obtain a contradiction. By the proof–by–contradiction principle (Proof Template 1.7), we delete the premise \(\neg P\) and we obtain a deduction of \(P\) from \(\neg(\neg P \lor \neg Q)\). We conclude by using Proof Template 1.2 to delete the premise \(\neg(\neg P \lor \neg Q)\) and to obtain our proof. A tree representing the above proof is shown below.

A similar proof shows that \(\neg(\neg P \lor \neg Q) \Rightarrow Q\) is provable. Putting together the proofs of \(P\) and \(Q\) from \(\neg(\neg P \lor \neg Q)\) using Proof Template 1.8, we obtain a proof of
\[
\neg(\neg P \lor \neg Q) \Rightarrow (P \land Q).
\]
A tree representing this proof is shown below.
Example 1.17. The proposition \(\neg(P \land Q) \Rightarrow (\neg P \lor \neg Q)\) is provable.

First by Proof Template 1.2, we assume \(\neg(P \land Q)\) as a premise. Next we use the proof–by–contradiction principle (Proof Template 1.7) to deduce \(\neg P \lor \neg Q\), so we also assume \(\neg(\neg P \lor \neg Q)\). Now, we just showed that \(P \land Q\) is provable from the premise \(\neg(\neg P \lor \neg Q)\).

Using the premise \(\neg(P \land Q)\), by Proof Principle 1.5, we derive a contradiction, and by the proof–by–contradiction principle, we delete the premise \(\neg(\neg P \lor \neg Q)\) to obtain a deduction of \(\neg P \lor \neg Q\) from \(\neg(P \land Q)\). We finish the proof by applying Proof Template 1.2. This proof is represented by the following tree.

\[
\begin{array}{c}
\neg(\neg P \lor \neg Q) \quad \neg P \lor \neg Q \\
\bot \quad \text{RAA}_x \\
P \land Q \\
\text{RAA}_y \\
\neg(\neg P \lor \neg Q) \Rightarrow (P \land Q)
\end{array}
\]

The next example is particularly interesting.

It can be shown that the proof–by–contradiction principle must be used.

Example 1.18. We prove the proposition

\[P \lor \neg P.\]

We use the proof–by–contradiction principle (Proof Template 1.7), so we assume \(\neg(P \lor \neg P)\) as a premise. The first tricky part of the proof is that we actually assume that we have two copies of the premise \(\neg(P \lor \neg P)\).

Next the second tricky part of the proof is that using one of the two copies of \(\neg(P \lor \neg P)\), we are going to deduce \(P \lor \neg P\). For this, we first derive \(\neg P\) using Proof Template 1.4, so we assume \(P\). By Proof Template 1.10, we deduce \(P \lor \neg P\), but we have the premise \(\neg(P \lor \neg P)\), so by Proof Template 1.5, we obtain a contradiction. Next, by Proof Template 1.4 we delete the premise \(P\), deduce \(\neg P\), and then by Proof Template 1.10 we deduce \(P \lor \neg P\).
Since we still have a second copy of the premise \( \neg(P \lor \neg P) \), by Proof Template 1.5, we get a contradiction! The only premise left is \( \neg(P \lor \neg P) \) (two copies of it), so by the proof–by–contradiction principle (Proof Template 1.7), we delete the premise \( \neg(P \lor \neg P) \) and we obtain the desired proof of \( P \lor \neg P \).

\[
\begin{align*}
\neg(P \lor \neg P)^\checkmark & \quad \frac{P \lor \neg P}{\bot} \text{ Negation-Elim} \\
& \quad \frac{\bot}{\neg P} \text{ Negation-Intro} \\
\neg(P \lor \neg P)^\checkmark & \quad \frac{P \lor \neg P}{\bot} \text{ Negation-Elim} \\
& \quad \frac{\bot}{P \lor \neg P} \text{ RAA}
\end{align*}
\]

If the above proof made you dizzy, this is normal. The sneaky part of this proof is that when we proceed by contradiction and assume \( \neg(P \lor \neg P) \), this proposition is an inconsistency, so it allows us to derive \( P \lor \neg P \), which then clashes with \( \neg(P \lor \neg P) \) to yield a contradiction. Observe that during the proof we actually showed that \( \neg\neg(P \lor \neg P) \) is provable. The proof–by–contradiction principle is needed to get rid of the double negation.

The fact is that even though the proposition \( P \lor \neg P \) seems obviously “true,” its truth is viewed as controversial by certain mathematicians and logicians. To some extent, this is why its proof has to be a bit tricky and has to involve the proof–by–contradiction principle. This matter is discussed quite extensively in Chapter 2. In this chapter, which is more informal, let us simply say that the proposition \( P \lor \neg P \) is known as the law of excluded middle. Indeed, intuitively, it says that for every proposition \( P \), either \( P \) is true or \( \neg P \) is true; there is no middle alternative.

It can be shown that if we take all formulae of the form \( P \lor \neg P \) as axioms, then the proof–by–contradiction principle is derivable from the other proof templates; see Section 2.7. Furthermore, the proposition \( \neg\neg P \Rightarrow P \) and \( P \lor \neg P \) are equivalent (that is, \( \neg\neg P \Rightarrow P \equiv (P \lor \neg P) \) is provable).

Typically, to prove a disjunction \( P \lor Q \), it is rare that we can use Proof Template 1.10 (Or–Intro), because this requires constructing of a proof of \( P \) or a proof of \( Q \) in the first place. But the fact that \( P \lor Q \) is provable does not imply in general that either a proof of \( P \) or a proof of \( Q \) can be produced, as the example of the proposition \( P \lor \neg P \) shows (other examples can be given). Thus, **usually to prove a disjunction we use the proof–by–contradiction principle.** Here is an example.

**Example 1.19.** Given some natural numbers \( p, q \), we wish to prove that if 2 divides \( pq \), then either 2 divides \( p \) or 2 divides \( q \). This can be expressed by

\[
(2 \mid pq) \Rightarrow ((2 \mid p) \lor (2 \mid q)).
\]

We use the proof–by–contradiction principle (Proof Template 1.7), so we assume \( \neg((2 \mid p) \lor (2 \mid q)) \) as a premise. This is a proposition of the form \( \neg(P \lor Q) \), and in Example 1.15
we showed that ¬((P ∨ Q) ⇒ (¬P ∧ ¬Q)) is provable. Thus, by Proof Template 1.3, we deduce that ¬((2 | p) ∧ ¬(2 | q)). By Proof Template 1.9, we deduce both ¬(2 | p) and ¬(2 | q). Using some basic arithmetic, this means that p = 2a + 1 and q = 2b + 1 for some a, b ∈ N. But then,

pq = 2(2ab + a + b) + 1.

and pq is not divisible by 2, a contradiction. By the proof–by-contradiction principle (Proof Template 1.7), we can delete the premise ¬((2 | p) ∨ (2 | q)) and obtain the desired proof.

Another proof template which is convenient to use in some cases is the proof–by–contrapositive principle.

**Proof Template 1.12. (Proof–By–Contrapositive)**

Given a list of premises Γ, to prove an implication P ⇒ Q, proceed as follows:

1. Add ¬Q to the list of premises Γ.
2. Construct a deduction of ¬P from the premises ¬Q and Γ.
3. Delete ¬Q from the list of premises.

It is not hard to see that the proof–by–contrapositive principle (Proof Template 1.12) can be derived from the proof–by–contradiction principle. We leave this as an exercise.

**Example 1.20.** We prove that for any two natural numbers m, n ∈ N, if m + n is even, then m and n have the same parity. This can be expressed as

\[
even(m + n) ⇒ ((\text{even}(m) ∧ \text{even}(n)) ∨ (\text{odd}(m) ∧ \text{odd}(n))).
\]

According to Proof Template 1.12 (proof–by–contrapositive principle), let us assume ¬((even(m) ∧ even(n)) ∨ (odd(m) ∧ odd(n))). Using the implication proven in Example 1.15 ((¬(P ∨ Q)) ⇒ ¬P ∧ ¬Q)) and Proof Template 1.3, we deduce that ¬(even(m) ∧ even(n)) and ¬(odd(m) ∧ odd(n)). Using the result of Example 1.17 and modus ponens (Proof Template 1.3), we deduce that ¬even(m) ∨ ¬even(n) and ¬odd(m) ∨ ¬odd(n). At this point, we can use the proof–by–cases principle (twice) to deduce that ¬even(m + n) holds. We leave some of the tedious details as an exercise. In particular, we use the fact proven in Chapter 2 that even(p) iff ¬odd(p) (see Section 2.16).

We treat logical equivalence as a derived connective: that is, we view P ≡ Q as an abbreviation for (P ⇒ Q) ∧ (Q ⇒ P). In view of the proof templates for ∧, we see that to prove a logical equivalence P ≡ Q, we just have to prove both implications P ⇒ Q and Q ⇒ P. For the sake of completeness, we state the following proof template.

**Proof Template 1.13. (Equivalence–Intro)**

Given a list of premises Γ, to obtain a deduction of an equivalence P ≡ Q, proceed as follows:
1. Construct a deduction of the implication $P \Rightarrow Q$ from the list of premises $\Gamma$.

2. Construct a deduction of the implication $Q \Rightarrow P$ from the list of premises $\Gamma$.

The proof templates described in this section and the previous one allow proving propositions which are known as the propositions of classical propositional logic. We also say that this set of proof templates is a natural deduction proof system for propositional logic; see Prawitz [6] and Gallier [3].

1.7 De Morgan Laws and Other Useful Rules of Logic

In Section 1.5, we proved certain implications that are special cases of the so-called de Morgan laws.

**Proposition 1.1.** The following equivalences (de Morgan laws) are provable:

$$
\neg \neg P \equiv P \\
\neg (P \land Q) \equiv \neg P \lor \neg Q \\
\neg (P \lor Q) \equiv \neg P \land \neg Q.
$$

The following equivalence expressing $\Rightarrow$ in terms of $\lor$ and $\neg$ is also provable:

$$
P \Rightarrow Q \equiv \neg P \lor Q.
$$

The following proposition (the law of the excluded middle) is provable:

$$
P \lor \neg P.
$$

The proofs that we have not shown are left as as exercises (sometimes tedious).

Proposition 1.1 shows a property that is very specific to classical logic, namely, that the logical connectives $\Rightarrow, \land, \lor, \neg$ are not independent. For example, we have $P \land Q \equiv \neg (\neg P \lor \neg Q)$, which shows that $\land$ can be expressed in terms of $\lor$ and $\neg$. Similarly, $P \Rightarrow Q \equiv \neg P \lor Q$ shows that $\Rightarrow$ can be expressed in terms of $\lor$ and $\neg$.

The next proposition collects a list of equivalences involving conjunction and disjunction that are used all the time. Constructing proofs using the proof templates is not hard but tedious.

**Proposition 1.2.** The following propositions are provable:

$$
P \lor P \equiv P \\
P \land P \equiv P \\
P \lor Q \equiv Q \lor P \\
P \land Q \equiv Q \land P.
$$
The last two assert the commutativity of $\lor$ and $\land$. We have distributivity of $\land$ over $\lor$ and of $\lor$ over $\land$:

\[
P \land (Q \lor R) \equiv (P \land Q) \lor (P \land R) \\
P \lor (Q \land R) \equiv (P \lor Q) \land (P \lor R).
\]

We have associativity of $\land$ and $\lor$:

\[
P \land (Q \land R) \equiv (P \land Q) \land R \\
P \lor (Q \lor R) \equiv (P \lor Q) \lor R.
\]

### 1.8 Formal Versus Informal Proofs; Some Examples

In this section we give some explicit examples of proofs illustrating the proof templates that we just discussed. But first it should be said that it is practically impossible to write formal proofs (i.e., proofs written using the proof templates of the system presented earlier) of “real” statements that are not “toy propositions.” This is because it would be extremely tedious and time-consuming to write such proofs and these proofs would be huge and thus very hard to read.

As we said before it is possible in principle to write formalized proofs, however, most of us will never do so. So what do we do?

Well, we construct “informal” proofs in which we still make use of the proof templates that we have presented but we take shortcuts and sometimes we even omit proof steps (some proof templates such as 1.9 (And–Elim) and 1.10 (Or–Intro)) and we use a natural language (here, presumably, English) rather than formal symbols (we say “and” for $\land$, “or” for $\lor$, etc.). As an example of a shortcut, when using the Proof Template 1.11 (Or–Elim), in most cases, the disjunction $P \lor Q$ has an “obvious proof” because $P$ and $Q$ “exhaust all the cases,” in the sense that $Q$ subsumes $\neg P$ (or $P$ subsumes $\neg Q$) and classically, $P \lor \neg P$ is an axiom. Also, we implicitly keep track of the open premises of a proof in our head rather than explicitly delete premises when required. This may be the biggest source of mistakes and we should make sure that when we have finished a proof, there are no “dangling premises,” that is, premises that were never used in constructing the proof. If we are “lucky,” some of these premises are in fact unnecessary and we should discard them. Otherwise, this indicates that there is something wrong with our proof and we should make sure that every premise is indeed used somewhere in the proof or else look for a counterexample.

We urge our readers to read Chapter 3 of Gowers [11] which contains very illuminating remarks about the notion of proof in mathematics.

The next question is then, “How does one write good informal proofs?”

It is very hard to answer such a question because the notion of a “good” proof is quite subjective and partly a social concept. Nevertheless, people have been writing informal proofs for centuries so there are at least many examples of what to do (and what not to do). As with everything else, practicing a sport, playing a music instrument, knowing “good”
wines, and so on, the more you practice, the better you become. Knowing the theory of swimming is fine but you have to get wet and do some actual swimming. Similarly, knowing the proof rules is important but you have to put them to use.

Write proofs as much as you can. Find good proof writers (like good swimmers, good tennis players, etc.), try to figure out why they write clear and easily readable proofs, and try to emulate what they do. Don’t follow bad examples (it will take you a little while to “smell” a bad proof style).

Another important point is that nonformalized proofs make heavy use of modus ponens. This is because, when we search for a proof, we rarely (if ever) go back to first principles. This would result in extremely long proofs that would be basically incomprehensible. Instead, we search in our “database” of facts for a proposition of the form $P \Rightarrow Q$ (an auxiliary lemma) that is already known to be proven, and if we are smart enough (lucky enough), we find that we can prove $P$ and thus we deduce $Q$, the proposition that we really want to prove. Generally, we have to go through several steps involving auxiliary lemmas. This is why it is important to build up a database of proven facts as large as possible about a mathematical field: numbers, trees, graphs, surfaces, and so on. This way we increase the chance that we will be able to prove some fact about some field of mathematics. practicing (constructing proofs).

And now we return to some explicit examples of informal proofs.

Recall that the set of integers is the set
\[ \mathbb{Z} = \{ \ldots, -2, -1, 0, 1, 2, \ldots \} \]
and that the set of natural numbers is the set
\[ \mathbb{N} = \{ 0, 1, 2, \ldots \}. \]
(Some authors exclude 0 from $\mathbb{N}$. We don’t like this discrimination against zero.) The following facts are essentially obvious from the definition of even and odd.

(a) The sum of even integers is even.

(b) The sum of an even integer and of an odd integer is odd.

(c) The sum of two odd integers is even.

(d) The product of odd integers is odd.

(e) The product of an even integer with any integer is even.

We will contruct deductions using sets of premises consisting of the above propositions. Now we prove the following fact using the proof–by–cases method.

**Proposition 1.3.** Let $a, b, c$ be odd integers. For any integers $p$ and $q$, if $p$ and $q$ are not both even, then
\[ ap^2 + bpq + cq^2 \]
is odd.
Proof. We consider the three cases:

1. $p$ and $q$ are odd. In this case as $a$, $b$, and $c$ are odd, by (d) all the products $ap^2$, $bpq$, and $cq^2$ are odd. By (c), $ap^2 + bpq$ is even and by (b), $ap^2 + bpq + cq^2$ is odd.

2. $p$ is even and $q$ is odd. In this case, by (e), both $ap^2$ and $bpq$ are even and by (d), $cq^2$ is odd. But then, by (a), $ap^2 + bpq$ is even and by (b), $ap^2 + bpq + cq^2$ is odd.

3. $p$ is odd and $q$ is even. This case is analogous to the previous case, except that $p$ and $q$ are interchanged. The reader should have no trouble filling in the details.

All three cases exhaust all possibilities for $p$ and $q$ not to be both even, thus the proof is complete by Proof Template 1.11 applied twice, because there are three cases instead of two.

The set of rational numbers $\mathbb{Q}$ consists of all fractions $p/q$, where $p, q \in \mathbb{Z}$, with $q \neq 0$. The set of real numbers is denoted by $\mathbb{R}$. A real number, $a \in \mathbb{R}$, is said to be irrational if it cannot be expressed as a number in $\mathbb{Q}$ (a fraction).

We now use Proposition 1.3 and the proof by contradiction method to prove the following.

**Proposition 1.4.** Let $a, b, c$ be odd integers. Then the equation

$$aX^2 + bX + c = 0$$

has no rational solution $X$. Equivalently, every zero of the above equation is irrational.

Proof. We proceed by contradiction (by this we mean that we use the proof–by–contradiction principle). So assume that there is a rational solution $X = p/q$. We may assume that $p$ and $q$ have no common divisor, which implies that $p$ and $q$ are not both even. As $q \neq 0$, if $aX^2 + bX + c = 0$, then by multiplying by $q^2$, we get

$$ap^2 + bpq + cq^2 = 0.$$ 

However, as $p$ and $q$ are not both even and $a, b, c$ are odd, we know from Proposition 1.3 that $ap^2 + bpq + cq^2$ is odd. This contradicts the fact that $p^2 + bpq + cq^2 = 0$ and thus finishes the proof.

As an example of the proof–by–contrapositive method, we prove that if an integer $n^2$ is even, then $n$ must be even.

Observe that if an integer is not even then it is odd (and vice versa). This fact may seem quite obvious but to prove it actually requires using induction (which we haven’t officially met yet). A rigorous proof is given in Section 1.12.

Now the contrapositive of our statement is: if $n$ is odd, then $n^2$ is odd. But, to say that $n$ is odd is to say that $n = 2k + 1$ and then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which shows that $n^2$ is odd.
As another illustration of the proof methods that we have just presented, let us prove that $\sqrt{2}$ is irrational, which means that $\sqrt{2}$ is not rational. The reader may also want to look at the proof given by Gowers in Chapter 3 of his book [11]. Obviously, our proof is similar but we emphasize step (2) a little more.

Because we are trying to prove that $\sqrt{2}$ is not rational, we use Proof Template 1.4. Thus let us assume that $\sqrt{2}$ is rational and derive a contradiction. Here are the steps of the proof.

1. If $\sqrt{2}$ is rational, then there exist some integers $p, q \in \mathbb{Z}$, with $q \neq 0$, so that $\sqrt{2} = p/q$.
2. Any fraction $p/q$ is equal to some fraction $r/s$, where $r$ and $s$ are not both even.
3. By (2), we may assume that
   \[ \sqrt{2} = \frac{p}{q}, \]
   where $p, q \in \mathbb{Z}$ are not both even and with $q \neq 0$.
4. By (3), because $q \neq 0$, by multiplying both sides by $q$, we get
   \[ q \sqrt{2} = p. \]
5. By (4), by squaring both sides, we get
   \[ 2q^2 = p^2. \]
6. Inasmuch as $p^2 = 2q^2$, the number $p^2$ must be even. By a fact previously established, $p$ itself is even; that is, $p = 2s$, for some $s \in \mathbb{Z}$.
7. By (6), if we substitute $2s$ for $p$ in the equation in (5) we get $2q^2 = 4s^2$. By dividing both sides by 2, we get
   \[ q^2 = 2s^2. \]
8. By (7), we see that $q^2$ is even, from which we deduce (as above) that $q$ itself is even.
9. Now, assuming that $\sqrt{2} = p/q$ where $p$ and $q$ are not both even (and $q \neq 0$), we concluded that both $p$ and $q$ are even (as shown in (6) and(8)), reaching a contradiction. Therefore, by negation introduction, we proved that $\sqrt{2}$ is not rational.

A closer examination of the steps of the above proof reveals that the only step that may require further justification is step (2): that any fraction $p/q$ is equal to some fraction $r/s$ where $r$ and $s$ are not both even.

This fact does require a proof and the proof uses the division algorithm, which itself requires induction. Besides this point, all the other steps only require simple arithmetic properties of the integers and are constructive.

**Remark:** Actually, every fraction $p/q$ is equal to some fraction $r/s$ where $r$ and $s$ have no common divisor except 1. This follows from the fact that every pair of integers has a greatest
common divisor (a gcd; s and r and s are obtained by dividing p and q by their gcd. Using this fact and Euclid’s lemma, we can obtain a shorter proof of the irrationality of \(\sqrt{2}\). First we may assume that p and q have no common divisor besides 1 (we say that p and q are relatively prime). From (5), we have

\[2q^2 = p^2,\]

so q divides \(p^2\). However, q and p are relatively prime and as q divides \(p^2 = p \times p\), by Euclid’s lemma, q divides p. But because 1 is the only common divisor of p and q, we must have q = 1. Now, we get \(p^2 = 2\), which is impossible inasmuch as 2 is not a perfect square.

The above argument can be easily adapted to prove that if the positive integer n is not a perfect square, then \(\sqrt{n}\) is not rational.

We conclude this section by showing that the proof–by–contradiction principle allows for proofs of propositions that may lack a constructive nature. In particular, it is possible to prove disjunctions \(P \lor Q\) which states some alternative that cannot be settled.

For example, consider the question: are there two irrational real numbers a and b such that \(a^b\) is rational? Here is a way to prove that this is indeed the case. Consider the number \(\sqrt{2}^{\sqrt{2}}\). If this number is rational, then \(a = \sqrt{2}\) and \(b = \sqrt{2}\) is an answer to our question (because we already know that \(\sqrt{2}\) is irrational). Now observe that

\[(\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} = \sqrt{2}^{\sqrt{2} \times \sqrt{2}} = \sqrt{2}^2 = 2\text{ is rational.}\]

Thus, if \(\sqrt{2}^{\sqrt{2}}\) is not rational, then \(a = \sqrt{2}^{\sqrt{2}}\) and \(b = \sqrt{2}\) is an answer to our question. Because \(P \lor \neg P\) is provable using the proof–by–contradiction principle (\(\sqrt{2}^{\sqrt{2}}\) is rational or it is not rational), we proved that

\[(\sqrt{2} \text{ is irrational and } \sqrt{2}^{\sqrt{2}} \text{ is rational}) \text{ or } (\sqrt{2}^{\sqrt{2}} \text{ and } \sqrt{2} \text{ are irrational and } (\sqrt{2}^{\sqrt{2}})^{\sqrt{2}} \text{ is rational}).\]

However, the above proof does not tell us whether \(\sqrt{2}^{\sqrt{2}}\) is rational!

We see one of the shortcomings of classical reasoning: certain statements (in particular, disjunctive or existential) are provable but their proof does not provide an explicit answer. For this reason, classical logic is considered to be nonconstructive.

Remark: Actually, it turns out that another irrational number \(b\) can be found so that \(\sqrt{2}^b\) is rational and the proof that \(b\) is not rational is fairly simple. It also turns out that the exact nature of \(\sqrt{2}^{\sqrt{2}}\) (rational or irrational) is known. The answers to these puzzles can be found in Section 1.10.

1.9 Truth Tables and Truth Value Semantics

So far we have deliberately focused on the construction of proofs using proof templates, we but have ignored the notion of truth. We can’t postpone any longer a discussion of the truth value semantics for classical propositional logic.
We all learned early on that the logical connectives ⇒, ∧, ∨, ¬ and ≡ can be interpreted as Boolean functions, that is, functions whose arguments and whose values range over the set of truth values,

\[ \text{BOOL} = \{ \text{true}, \text{false} \}. \]

These functions are given by the following truth tables.

<table>
<thead>
<tr>
<th>P</th>
<th>Q</th>
<th>P ⇒ Q</th>
<th>P ∧ Q</th>
<th>P ∨ Q</th>
<th>¬P</th>
<th>P ≡ Q</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>false</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

Note that the implication \( P \Rightarrow Q \) is false (has the value false) exactly when \( P = \text{true} \) and \( Q = \text{false} \).

Now any proposition \( P \) built up over the set of atomic propositions \( \mathbf{PS} \) (our propositional symbols) contains a finite set of propositional letters, say \( \{ P_1, \ldots, P_m \} \).

If we assign some truth value (from \( \text{BOOL} \)) to each symbol \( P_i \) then we can “compute” the truth value of \( P \) under this assignment by using recursively using the truth tables above. For example, the proposition \( P_1 \Rightarrow (P_1 \Rightarrow P_2) \), under the truth assignment \( v \) given by \( P_1 = \text{true}, P_2 = \text{false} \), evaluates to false. Indeed, the truth value, \( v(P_1 \Rightarrow (P_1 \Rightarrow P_2)) \), is computed recursively as

\[
v(P_1 \Rightarrow (P_1 \Rightarrow P_2)) = v(P_1) \Rightarrow v(P_1 \Rightarrow P_2).
\]

Now, \( v(P_1) = \text{true} \) and \( v(P_1 \Rightarrow P_2) \) is computed recursively as

\[
v(P_1 \Rightarrow P_2) = v(P_1) \Rightarrow v(P_2).
\]

Because \( v(P_1) = \text{true} \) and \( v(P_2) = \text{false} \), using our truth table, we get

\[
v(P_1 \Rightarrow P_2) = \text{true} \Rightarrow \text{false} = \text{false}.
\]

Plugging this into the right-hand side of \( v(P_1 \Rightarrow (P_1 \Rightarrow P_2)) \), we finally get

\[
v(P_1 \Rightarrow (P_1 \Rightarrow P_2)) = \text{true} \Rightarrow \text{false} = \text{false}.
\]

However, under the truth assignment \( v \) given by

\[ P_1 = \text{true}, P_2 = \text{true}, \]
we find that our proposition evaluates to true.

The values of a proposition can be determined by creating a truth table, in which a proposition is evaluated by computing recursively the truth values of its subexpressions. For example, the truth table corresponding to the proposition \( P_1 \Rightarrow (P_1 \Rightarrow P_2) \) is

<table>
<thead>
<tr>
<th>( P_1 )</th>
<th>( P_2 )</th>
<th>( P_1 \Rightarrow P_2 )</th>
<th>( P_1 \Rightarrow (P_1 \Rightarrow P_2) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

If we now consider the proposition \( P = (P_1 \Rightarrow (P_2 \Rightarrow P_1)) \), its truth table is

<table>
<thead>
<tr>
<th>( P_1 )</th>
<th>( P_2 )</th>
<th>( P_2 \Rightarrow P_1 )</th>
<th>( P_1 \Rightarrow (P_2 \Rightarrow P_1) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

which shows that \( P \) evaluates to true for all possible truth assignments.

The truth table of a proposition containing \( m \) variables has \( 2^m \) rows. When \( m \) is large, \( 2^m \) is very large, and computing the truth table of a proposition \( P \) may not be practically feasible. Even the problem of finding whether there is a truth assignment that makes \( P \) true is hard. This is actually a very famous problem in computer science.

A proposition \( P \) is said to be valid or a tautology if in the truth table for \( P \) all the entries in the column corresponding to \( P \) have the value true. This means that \( P \) evaluates to true for all \( 2^m \) truth assignments.

What’s the relationship between validity and provability? Remarkably, validity and provability are equivalent.

In order to prove the above claim, we need to do two things:

1. Prove that if a proposition \( P \) is provable using the proof templates that we described earlier, then it is valid. This is known as soundness or consistency (of the proof system).

2. Prove that if a proposition \( P \) is valid, then it has a proof using the proof templates. This is known as the completeness (of the proof system).

In general, it is relatively easy to prove (1) but proving (2) can be quite complicated. In this book we content ourselves with soundness.

**Proposition 1.5.** (Soundness of the proof templates) If a proposition \( P \) is provable using the proof templates described earlier, then it is valid (according to the truth value semantics).
**CHAPTER 1. MATHEMATICAL REASONING AND BASIC LOGIC**

**Sketch of Proof.** It is enough to prove that if there is a deduction of a proposition \( P \) from a set of premises \( \Gamma \), then for every truth assignment for which all the propositions in \( \Gamma \) evaluate to **true**, then \( P \) evaluates to **true**. However, this is clear for the axioms and every proof template preserves that property.

Now, if \( P \) is provable, a proof of \( P \) has an empty set of premises and so \( P \) evaluates to **true** for all truth assignments, which means that \( P \) is valid. \( \square \)

**Theorem 1.6. (Completeness)** If a proposition \( P \) is valid (according to the truth value semantics), then \( P \) is provable using the proof templates.

Proofs of completeness for classical logic can be found in van Dalen [24] or Gallier [4] (but for a different proof system).

Soundness (Proposition 1.5) has a very useful consequence: in order to prove that a proposition \( P \) is not provable, it is enough to find a truth assignment for which \( P \) evaluates to **false**. We say that such a truth assignment is a **counterexample** for \( P \) (or that \( P \) can be **falsified**).

For example, no propositional symbol \( P_i \) is provable because it is falsified by the truth assignment \( P_i = \text{false} \).

The soundness of our proof system also has the extremely important consequence that \( \perp \) **cannot be proven** in this system, which means that **contradictory statements** cannot be derived.

This is by no means obvious at first sight, but reassuring.

*Note that completeness amounts to the fact that every unprovable proposition has a counterexample.* Also, in order to show that a proposition is provable, it suffices to compute its truth table and check that the proposition is valid. This may still be a lot of work, but it is a more “mechanical” process than attempting to find a proof. For example, here is a truth table showing that \((P_1 \Rightarrow P_2) \equiv (\neg P_1 \lor P_2)\) is valid.

<table>
<thead>
<tr>
<th>(P_1)</th>
<th>(P_2)</th>
<th>(P_1 \Rightarrow P_2)</th>
<th>(\neg P_1 \lor P_2)</th>
<th>((P_1 \Rightarrow P_2) \equiv (\neg P_1 \lor P_2))</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

1.10 **Proof Templates for the Quantifiers**

As we mentioned in Section 1.1, atomic propositions may contain variables. The intention is that such variables correspond to arbitrary objects. An example is

\[ \text{human}(x) \Rightarrow \text{needs-to-drink}(x). \]

In mathematics, we usually prove universal statements, that is statements that hold for all possible “objects,” or existential statements, that is, statements asserting the existence of
some object satisfying a given property. As we saw earlier, we assert that every human needs
to drink by writing the proposition

$$\forall x (\text{human}(x) \Rightarrow \text{needs-to-drink}(x)).$$

The symbol $\forall$ is called a \textit{universal quantifier}. Observe that once the quantifier $\forall$ (pronounced
“for all” or “for every”) is applied to the variable $x$, the variable $x$ becomes a placeholder
and replacing $x$ by $y$ or any other variable does not change anything. We say that $x$ is a
\textit{bound variable} (sometimes a “dummy variable”).

If we want to assert that some human needs to drink we write

$$\exists x (\text{human}(x) \Rightarrow \text{needs-to-drink}(x));$$

The symbol $\exists$ is called an \textit{existential quantifier}. Again, once the quantifier $\exists$ (pronounced
“there exists”) is applied to the variable $x$, the variable $x$ becomes a placeholder. However,
the intended meaning of the second proposition is very different and weaker than the first.
It only asserts the existence of some object satisfying the statement

$$\text{human}(x) \Rightarrow \text{needs-to-drink}(x).$$

Statements may contain variables that are not bound by quantifiers. For example, in

$$\exists x \text{ parent}(x, y)$$

the variable $x$ is bound but the variable $y$ is not. Here, the intended meaning of parent($x, y$)
is that $x$ is a parent of $y$, and the intended meaning of $\exists x \text{ parent}(x, y)$ is that any given $y$
has some parent $x$. Variables that are not bound are called \textit{free}. The proposition

$$\forall y \exists x \text{ parent}(x, y),$$

which contains only bound variables is meant to assert that every $y$ has some parent $x$. Typically, in mathematics, we only prove statements without free variables. However, statements
with free variables may occur during intermediate stages of a proof.

Now, in addition to propositions of the form $P \land Q, P \lor Q, P \Rightarrow Q, \neg P, P \equiv Q$, we add
two new kinds of propositions (also called formulae):

1. \textit{Universal formulae}, which are formulae of the form $\forall x P$, where $P$ is any formula and $x$ is any variable.

2. \textit{Existential formulae}, which are formulae of the form $\exists x P$, where $P$ is any formula and $x$ is any variable.

The intuitive meaning of the statement $\forall x P$ is that $P$ holds for all possible objects $x$ and
the intuitive meaning of the statement $\exists x P$ is that $P$ holds for some object $x$. Thus we see
that it would be useful to use symbols to denote various objects. For example, if we want
to assert some facts about the “parent” predicate, we may want to introduce some constant symbols (for short, constants) such as “Jean,” “Mia,” and so on and write

\[ \text{parent}(\text{Jean}, \text{Mia}) \]

to assert that Jean is a parent of Mia. Often we also have to use function symbols (or operators, constructors), for instance, to write a statement about numbers: +, *, and so on. Using constant symbols, function symbols, and variables, we can form terms, such as

\[(x * x + 1) * (3 * y + 2)\].

In addition to function symbols, we also use predicate symbols, which are names for atomic properties. We have already seen several examples of predicate symbols: “odd,” “even,” “prime,” “human,” “parent.” So in general, when we try to prove properties of certain classes of objects (people, numbers, strings, graphs, and so on), we assume that we have a certain alphabet consisting of constant symbols, function symbols, and predicate symbols. Using these symbols and an infinite supply of variables we can form terms and predicate terms. We say that we have a (logical) language. Using this language, we can write compound statements. A detailed presentation of this approach is given in Chapter 2. Here we follow a more informal and more intuitive approach. We use the notion of term as a synonym for some specific object. Terms are often denoted by the Greek letter \( \tau \), sometimes subscripted. A variable qualifies as a term.

When working with propositions possibly containing quantifiers, it is customary to use the term formula instead of proposition. The term proposition is typically reserved to formulae without quantifiers.

Unlike the Proof Templates for \( \Rightarrow, \lor, \land \) and \( \bot \), which are rather straightforward, the Proof Templates for quantifiers are more subtle due to the presence of variables (occurring in terms and predicates) and the fact that it is sometimes necessary to make substitutions.

Given a formula \( P \) containing some free variable \( x \) and given a term \( \tau \), the result of replacing all occurrences of \( x \) by \( \tau \) in \( P \) is called a substitution and is denoted \( P[\tau/x] \) (and pronounced “the result of substituting \( \tau \) for \( x \) in \( P \)”). Substitutions can be defined rigorously by recursion. Let us simply give an example. Consider the predicate \( P(x) = \text{odd}(2x + 1) \). If we substitute the term \( \tau = (y + 1)^2 \) for \( x \) in \( P(x) \), we obtain

\[ P[\tau/x] = \text{odd}(2(y + 1)^2 + 1) \].

We have to be careful to forbid inferences that would yield “wrong” results and for this we have to be very precise about the way we use free variables. More specifically, we have to exercise care when we make substitutions of terms for variables in propositions. If \( P(t_1, t_2, \ldots, t_n) \) is a statement containing the free variables \( t_1, \ldots, t_n \) and if \( \tau_1, \ldots, \tau_n \) are terms, we can form the new statement

\[ P[\tau_1/t_1, \ldots, \tau_n/t_n] \].
obtained by substituting the term $\tau_i$ for all free occurrences of the variable $t_i$, for $i = 1, \ldots, n$. By the way, we denote terms by the Greek letter $\tau$ because we use the letter $t$ for a variable and using $t$ for both variables and terms would be confusing; sorry.

However, if $P(t_1, t_2, \ldots, t_n)$ contains quantifiers, some bad things can happen; namely, some of the variables occurring in some term $\tau_i$ may become quantified when $\tau_i$ is substituted for $t_i$. For example, consider

$$\forall x \exists y P(x, y, z)$$

which contains the free variable $z$ and substitute the term $x + y$ for $z$: we get

$$\forall x \exists y P(x, y, x + y).$$

We see that the variables $x$ and $y$ occurring in the term $x + y$ become bound variables after substitution. We say that there is a “capture” of variables.

This is not what we intended to happen. To fix this problem, we recall that bound variables are really place holders so they can be renamed without changing anything. Therefore, we can rename the bound variables $x$ and $y$ in $\forall x \exists y P(x, y, z)$ to $u$ and $v$, getting the statement $\forall u \exists v P(u, v, z)$ and now, the result of the substitution is

$$\forall u \exists v P(u, v, x + y),$$

where $x$ and $y$ are free. Again, all this needs to be explained very carefully but in this chapter we will content ourselves with an informal treatment.

We begin with the proof templates for the universal quantifier.

**Proof Template 1.14. (Forall–Intro)**

Let $\Gamma$ be a list of premises and let $y$ be a variable that does not occur free in any premise in $\Gamma$ or in $\forall x P$. If we have a deduction of the formula $P[y/x]$ from $\Gamma$, then we obtain a deduction of $\forall x P$ from $\Gamma$.

**Proof Template 1.15. (Forall–Elim)**

Let $\Gamma$ be a list of premises and let $\tau$ be a term representing some specific object. If we have a deduction of $\forall x P$ from $\Gamma$, then we obtain a deduction of $P[\tau/x]$ from $\Gamma$.

The Proof Template 1.14 may look a little strange but the idea behind it is actually very simple: Because $y$ is totally unconstrained, if $P[y/x]$ (the result of replacing all occurrences of $x$ by $y$ in $P$) is provable (from $\Gamma$), then intuitively $P[y/x]$ holds for any arbitrary object, and so, the statement $\forall x P$ should also be provable (from $\Gamma$).

Note that we can’t deduce $\forall x P$ from $P[y/x]$ because the deduction has the single premise $P[y/x]$ and $y$ occurs in $P[y/x]$ (unless $x$ does not occur in $P$).

The meaning of the Proof Template 1.15 is that if $\forall x P$ is provable (from $\Gamma$), then $P$ holds for all objects and so, in particular for the object denoted by the term $\tau$; that is, $P[\tau/x]$ should be provable (from $\Gamma$).

Here are the proof templates for the existential quantifier.
Proof Template 1.16. (Exist–Intro)

Let \( \Gamma \) be a list of premises and let \( \tau \) be a term representing some specific object. If we have a deduction of \( P[\tau/x] \) from \( \Gamma \), then we obtain a deduction of \( \exists x P(x) \) from \( \Gamma \).

Proof Template 1.17. (Exist–Elim)

Let \( \Gamma \) and \( \Delta \) be two lists of premises. Let \( C \) and \( \exists x P \) be formulae, and let \( y \) be a variable that does not occur free in any premise in \( \Gamma \), in \( \exists x P \), or in \( C \). To obtain a deduction of \( C \) from \( \Gamma, \Delta \), proceed as follows:

1. Make a deduction of \( \exists x P \) from \( \Gamma \).

2. Add one or more occurrences of \( P[y/x] \) as premises to \( \Delta \), and find a deduction of \( C \) from \( P[y/x] \) and \( \Delta \).

3. Delete the premise \( P[y/x] \).

If \( P[\tau/x] \) is provable (from \( \Gamma \)), this means that the object denoted by \( \tau \) satisfies \( P \), so \( \exists x P \) should be provable (this latter formula asserts the existence of some object satisfying \( P \), and \( \tau \) is such an object).

Proof Template 1.17 is reminiscent of the proof–by–cases principle (Proof template 1.11) and is a little more tricky. It goes as follows. Suppose that we proved \( \exists x P \) (from \( \Gamma \)). Moreover, suppose that for every possible case \( P[y/x] \) we were able to prove \( C \) (from \( \Delta \)). Then, as we have “exhausted” all possible cases and as we know from the provability of \( \exists x P \) that some case must hold, we can conclude that \( C \) is provable (from \( \Gamma, \Delta \)) without using \( P[y/x] \) as a premise.

Like the the proof–by–cases principle, Proof Template 1.17 is not very constructive. It allows making a conclusion \( (C) \) by considering alternatives without knowing which one actually occurs.

Constructing proofs using the proof templates for the quantifiers can be quite tricky due to the restrictions on variables. In practice, we always use “fresh” (brand new) variables to avoid problems. Also, when we use Proof Template 1.14, we begin by saying “let \( y \) be arbitrary,” then we prove \( P[y/x] \) (mentally substituting \( y \) for \( x \)), and we conclude with: “since \( y \) is arbitrary, this proves \( \forall x P \).” We proceed in a similar way when using Proof Template 1.17, but this time we say “let \( y \) be arbitrary” in step (2). When we use Proof Template 1.15, we usually say: “Since \( \forall x P \) holds, it holds for all \( x \), so in particular it holds for \( \tau \), and thus \( P[\tau/x] \) holds.” Similarly, when using Proof Template 1.16, we say “since \( P[\tau/x] \) holds for a specific object \( \tau \), we can deduce that \( \exists x P \) holds.”

Here is an example of a “wrong proof” in which the \( \forall \)-introduction rule is applied illegally, and thus, yields a statement that is actually false (not provable). In the incorrect “proof” below, \( P \) is an atomic predicate symbol taking two arguments (e.g., “parent”) and 0 is a constant denoting zero:
The problem is that the variable \( u \) occurs free in the premise \( P[u/t, 0] = P(u, 0) \) and therefore, the application of the \( \forall \)-introduction rule in the first step is illegal. However, note that this premise is discharged in the second step and so, the application of the \( \forall \)-introduction rule in the third step is legal. The (false) conclusion of this faulty proof is that \( P(0, 0) \Rightarrow \forall t P(t, 0) \) is provable. Indeed, there are plenty of properties such that the fact that the single instance \( P(0, 0) \) holds does not imply that \( P(t, 0) \) holds for all \( t \).

Let us now give two examples of a proof using the proof templates for \( \forall \) and \( \exists \).

**Example 1.21.** For any natural number \( n \), let \( \text{odd}(n) \) be the predicate that asserts that \( n \) is odd, namely

\[
\text{odd}(n) \equiv \exists m ((m \in \mathbb{N}) \land (n = 2m + 1)).
\]

First let us prove that

\[
\forall a ((a \in \mathbb{N}) \Rightarrow \text{odd}(2a + 1)).
\]

By Proof Template 1.14, let \( x \) be a fresh variable; we need to prove

\[
(x \in \mathbb{N}) \Rightarrow \text{odd}(2x + 1).
\]

By Proof Template 1.2, assume \( x \in \mathbb{N} \). If we consider the formula

\[
(m \in \mathbb{N}) \land (2x + 1 = 2m + 1),
\]

by substituting \( x \) for \( m \), we get

\[
(x \in \mathbb{N}) \land (2x + 1 = 2x + 1),
\]

which is provable since \( x \in \mathbb{N} \). By Proof Template 1.16, we obtain

\[
\exists m (m \in \mathbb{N}) \land (2x + 1 = 2m + 1);
\]

that is, \( \text{odd}(2x + 1) \) is provable. Using Proof Template 1.2, we delete the premise \( x \in \mathbb{N} \) and we have proven

\[
(x \in \mathbb{N}) \Rightarrow \text{odd}(2x + 1).
\]

This proof has no longer any premises, so we can safely conclude that

\[
\forall a ((a \in \mathbb{N}) \Rightarrow \text{odd}(2a + 1)).
\]
Next consider the term $\tau = 7$. By Proof Template 1.15, we obtain

$$(7 \in \mathbb{N}) \Rightarrow \text{odd}(15).$$

Since $7 \in \mathbb{N}$, by modus ponens we deduce that $15$ is odd.

Let us now consider the term $\tau = (b+1)^2$ with $b \in \mathbb{N}$. By Proof Template 1.15, we obtain

$$((b+1)^2 \in \mathbb{N}) \Rightarrow \text{odd}(2(b+1)^2 + 1)).$$

But $b \in \mathbb{N}$ implies that $(b+1)^2 \in \mathbb{N}$ so by modus ponens and Proof Template 1.2, we deduce that

$$(b \in \mathbb{N}) \Rightarrow \text{odd}(2(b+1)^2 + 1)).$$

**Example 1.22.** Let us prove the formula $\forall x(P \land Q) \Rightarrow \forall xP \land \forall xQ$.

First using Proof Template 1.2, we assume $\forall x(P \land Q)$ (two copies). The next step uses a trick. Since variables are terms, if $u$ is a fresh variable, then by Proof Template 1.15 we deduce $(P \land Q)[u/x]$. Now we use a property of substitutions which says that

$$(P \land Q)[u/x] = P[u/x] \land Q[u/x].$$

We can now use Proof Template 1.9 (twice) to deduce $P[u/x]$ and $Q[u/x]$. But, remember that the premise is $\forall x(P \land Q)$ (two copies), and since $u$ is a fresh variable, it does not occur in this premise, so we can safely apply Proof Template 1.14 and conclude $\forall xP$, and similarly $\forall xQ$. By Proof Template 1.8, we deduce $\forall xP \land \forall xQ$ from $\forall x(P \land Q)$. Finally, by Proof Template 1.2, we delete the premise $\forall x(P \land Q)$ and obtain our proof. The above proof has the following tree representation.

$$\begin{array}{c}
\forall x(P \land Q) \\
\hline
P[u/x] \land Q[u/x] \\
\hline
P[u/x] \\
\hline
\forall xP \\
\hline
\forall xQ \\
\hline
\forall xP \land \forall xQ \\
\hline
\forall x(P \land Q) \Rightarrow \forall xP \land \forall xQ
\end{array}$$

The reader should show that $\forall xP \land \forall xQ \Rightarrow \forall x(P \land Q)$ is also provable.

However, in general, one can’t just replace $\forall$ by $\exists$ (or $\land$ by $\lor$) and still obtain provable statements. For example, $\exists xP \land \exists xQ \Rightarrow \exists x(P \land Q)$ is not provable at all.

Here are some useful equivalences involving quantifiers. The first two are analogous to the de Morgan laws for $\land$ and $\lor$. 

$$\exists xP \land \forall xQ \Rightarrow \forall x(P \land Q)$$

$$\forall xP \lor \exists xQ \Rightarrow \exists x(P \lor Q)$$

The last two will be proved in the next chapter.
Proposition 1.7. The following formulae are provable:

\[ \neg \forall x P \equiv \exists x \neg P \]
\[ \neg \exists x P \equiv \forall x \neg P \]
\[ \forall x (P \land Q) \equiv \forall x P \land \forall x Q \]
\[ \exists x (P \lor Q) \equiv \exists x P \lor \exists x Q \]
\[ \exists x (P \land Q) \Rightarrow \exists x P \land \exists x Q \]
\[ \forall x P \lor \forall x Q \Rightarrow \forall x (P \lor Q). \]

The proof system that uses all the Proof Templates that we have defined proves formulae of classical first-order logic.

One should also be careful that the order the quantifiers is important. For example, a formula of the form

\[ \forall x \exists y P \]

is generally not equivalent to the formula

\[ \exists y \forall x P. \]

The second formula asserts the existence of some object \( y \) such that \( P \) holds for all \( x \). But in the first formula, for every \( x \), there is some \( y \) such that \( P \) holds, but each \( y \) depends on \( x \) and there may not be a single \( y \) that works for all \( x \).

Another amusing mistake involves negating a universal quantifier. The formula \( \forall x \neg P \) is not equivalent to \( \neg \forall x P \). Once traveling from Philadelphia to New York I heard a train conductor say: “all doors will not open.” Actually, he meant “not all doors will open,” which would give us a chance to get out!

Remark: We can illustrate, again, the fact that classical logic allows for nonconstructive proofs by re-examining the example at the end of Section 1.5. There we proved that if \( \sqrt{2}^{\sqrt{2}} \) is rational, then \( a = \sqrt{2} \) and \( b = \sqrt{2} \) are both irrational numbers such that \( a^b \) is rational and if \( \sqrt{2}^{\sqrt{2}} \) is irrational then \( a = \sqrt{2}^{\sqrt{2}} \) and \( b = \sqrt{2} \) are both irrational numbers such that \( a^b \) is rational. By Proof Template 1.16, we deduce that if \( \sqrt{2}^{\sqrt{2}} \) is rational, then there exist some irrational numbers \( a, b \) so that \( a^b \) is rational, and if \( \sqrt{2}^{\sqrt{2}} \) is irrational, then there exist some irrational numbers \( a, b \) so that \( a^b \) is rational. In classical logic, as \( P \lor \neg P \) is provable, by the proof–by–cases principle we just proved that there exist some irrational numbers \( a \) and \( b \) so that \( a^b \) is rational.

However, this argument does not give us explicitly numbers \( a \) and \( b \) with the required properties. It only tells us that such numbers must exist.

Now, it turns out that \( \sqrt{2}^{\sqrt{2}} \) is indeed irrational (this follows from the Gel’fond–Schneider theorem, a hard theorem in number theory). Furthermore, there are also simpler explicit solutions such as \( a = \sqrt{2} \) and \( b = \log_2 9 \), as the reader should check.
1.11 Sets and Set Operations

In this section we review the definition of a set and basic set operations. This section takes
the “naive” point of view that a set is an unordered collection of objects, without duplicates,
the collection being regarded as a single object.

Given a set $A$ we write that some object $a$ is an element of (belongs to) the set $A$ as

$$a \in A$$

and that $a$ is not an element of $A$ (does not belong to $A$) as

$$a \notin A.$$ 

The symbol $\in$ is the set membership symbol.

A set can either be defined explicitly by listing its elements within curly braces (the
symbols $\{ \text{ and } \}$) or as a collection of objects satisfying a certain property. For example, the
set $C$ consisting of the colors red, blue, green is given by

$$C = \{ \text{red, blue, green} \}. $$

Because the order of elements in a set is irrelevant, the set $C$ is also given by

$$C = \{ \text{green, red, blue} \}. $$

In fact, a moment of reflection reveals that there are six ways of writing the set $C$.

If we denote by $\mathbb{N}$ the set of natural numbers

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

then the set $E$ of even integers can be defined in terms of the property even of being even by

$$E = \{ n \in \mathbb{N} \mid \text{even}(n) \}.$$ 

More generally, given some property $P$ and some set $X$, we denote the set of all elements of
$X$ that satisfy the property $P$ by

$$\{ x \in X \mid P(x) \} \quad \text{or} \quad \{ x \mid x \in X \land P(x) \}. $$

When are two sets $A$ and $B$ equal? The answer is given by the first proof template of
set theory, called the Extensionality Axiom.

Proof Template 1.18. (Extensionality Axiom)

Two sets $A$ and $B$ are equal iff they have exactly the same elements; that is, every element
of $A$ is an element of $B$ and conversely. This can be written more formally as

$$\forall x(x \in A \Rightarrow x \in B) \land \forall x(x \in B \Rightarrow x \in A). $$
There is a special set having no elements at all, the *empty set*, denoted $\emptyset$. The empty set is characterized by the property

$$\forall x (x \notin \emptyset).$$

Next we define the notion of inclusion between sets

**Definition 1.5.** Given any two sets, $A$ and $B$, we say that $A$ is a *subset of $B$* (or that $A$ is *included in $B$*), denoted $A \subseteq B$, iff every element of $A$ is also an element of $B$, that is,

$$\forall x (x \in A \Rightarrow x \in B).$$

We say that $A$ is a *proper subset of $B$* iff $A \subseteq B$ and $A \neq B$. This implies that that there is some $b \in B$ with $b \notin A$. We usually write $A \subset B$.

For example, if $A = \{\text{green, blue}\}$ and $C = \{\text{green, red, blue}\}$, then

$$A \subseteq C.$$  

Note that the empty set is a subset of every set.

Observe the important fact that equality of two sets can be expressed by

$$A = B \iff A \subseteq B \text{ and } B \subseteq A.$$  

Proving that two sets are equal may be quite complicated if the definitions of these sets are complex, and the above method is the safe one.

If a set $A$ has a finite number of elements, then this number (a natural number) is called the *cardinality* of the set and is denoted by $|A|$ (sometimes by $\text{card}(A)$). Otherwise, the set is said to be *infinite*. The cardinality of the empty set is 0.

Sets can be combined in various ways, just as numbers can be added, multiplied, *etc.* However, operations on sets tend to mimic logical operations such as disjunction, conjunction, and negation, rather than the arithmetical operations on numbers. The most basic operations are union, intersection, and relative complement.

**Definition 1.6.** For any two sets $A$ and $B$, the *union of $A$ and $B$* is the set $A \cup B$ defined such that

$$x \in A \cup B \iff (x \in A) \lor (x \in B).$$

This reads, $x$ is a member of $A \cup B$ if either $x$ belongs to $A$ or $x$ belongs to $B$ (or both). We also write

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

The *intersection of $A$ and $B$* is the set $A \cap B$ defined such that

$$x \in A \cap B \iff (x \in A) \land (x \in B).$$

This reads, $x$ is a member of $A \cap B$ if $x$ belongs to $A$ and $x$ belongs to $B$. We also write

$$A \cap B = \{x \mid x \in A \text{ and } x \in B\}. $$
The relative complement (or set difference) of $A$ and $B$ is the set $A - B$ defined such that
\[ x \in A - B \text{ iff } (x \in A) \land \neg(x \in B). \]
This reads, $x$ is a member of $A - B$ if $x$ belongs to $A$ and $x$ does not belong to $B$. We also write
\[ A - B = \{ x \mid x \in A \text{ and } x \notin B \}. \]

For example, if $A = \{0, 2, 4, 6\}$ and $B = \{0, 1, 3, 5\}$, then
\[ A \cup B = \{0, 1, 2, 3, 4, 5, 6\} \]
\[ A \cap B = \{0\} \]
\[ A - B = \{2, 4, 6\}. \]

Two sets $A, B$ are said to be disjoint if $A \cap B = \emptyset$. It is easy to see that if $A$ and $B$ are two finite sets and if $A$ and $B$ are disjoint, then
\[ |A \cup B| = |A| + |B|. \]
In general, by writing
\[ A \cup B = (A \cap B) \cup (A - B) \cup (B - A), \]
if $A$ and $B$ are finite, it can be shown that
\[ |A \cup B| = |A| + |B| - |A \cap B|. \]

The situation in which we manipulate subsets of some fixed set $X$ often arises, and it is useful to introduce a special type of relative complement with respect to $X$. For any subset $A$ of $X$, the complement $\overline{A}$ of $A$ in $X$ is defined by
\[ \overline{A} = X - A, \]
which can also be expressed as
\[ \overline{A} = \{ x \in X \mid x \notin A \}. \]

Using the union operation, we can form bigger sets by taking unions with singletons. For example, we can form
\[ \{a, b, c\} = \{a, b\} \cup \{c\}. \]

**Remark:** We can systematically construct bigger and bigger sets by the following method: given any set $A$ let
\[ A^+ = A \cup \{A\}. \]
If we start from the empty set, we obtain the sets 

\[\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}, \{\emptyset, \{\emptyset\}, \{\emptyset\}\}\], etc.

These sets can be used to define the natural numbers and the + operation corresponds to the successor function on the natural numbers (i.e., \(n \mapsto n + 1\)).

The algebraic properties of union, intersection, and complementation are inherited from the properties of disjunction, conjunction, and negation. The following proposition lists some of the most important properties of union, intersection, and complementation. Some of these properties are versions of Proposition 1.2 for subsets.

**Proposition 1.8.** The following equations hold for all sets \(A, B, C\):

\[
A \cup \emptyset = A \\
A \cap \emptyset = \emptyset \\
A \cup A = A \\
A \cap A = A \\
A \cup B = B \cup A \\
A \cap B = B \cap A.
\]

The last two assert the commutativity of \(\cup\) and \(\cap\). We have distributivity of \(\cap\) over \(\cup\) and of \(\cup\) over \(\cap\):

\[
A \cap (B \cup C) = (A \cap B) \cup (A \cap C) \\
A \cup (B \cap C) = (A \cup B) \cap (A \cup C).
\]

We have associativity of \(\cap\) and \(\cup\):

\[
A \cap (B \cap C) = (A \cap B) \cap C \\
A \cup (B \cup C) = (A \cup B) \cup C.
\]

**Proof.** We use Proposition 1.2. Let us prove that \(A \cap (B \cup C) = (A \cap B) \cup (A \cap C)\), leaving the proof of the other equations as an exercise. We prove the two inclusions \(A \cap (B \cup C) \subseteq (A \cap B) \cup (A \cap C)\) and \((A \cap B) \cup (A \cap C) \subseteq A \cap (B \cup C)\).

Assume that \(x \in A \cap (B \cup C)\). This means that \(x \in A\) and \(x \in B \cup C\); that is,

\[(x \in A) \land ((x \in B) \lor (x \in C)).\]

Using the distributivity of \(\land\) over \(\lor\), we obtain

\[((x \in A) \land (x \in B)) \lor ((x \in A) \land (x \in C)).\]

But the above says that \(x \in (A \cap B) \cup (A \cap C)\), which proves our first inclusion.
Conversely assume that \( x \in (A \cap B) \cup (A \cap C) \). This means that \( x \in (A \cap B) \) or \( x \in (A \cap C) \); that is,
\[
((x \in A) \land (x \in B)) \lor ((x \in A) \land (x \in C)).
\]
Using the distributivity of \( \land \) over \( \lor \) (in the other direction), we obtain
\[
(x \in A) \land ((x \in B) \lor (x \in C)),
\]
which says that \( x \in A \cap (B \cup C) \), and proves our second inclusion.

Note that we could have avoided two arguments by proving that \( x \in A \cap (B \cup C) \) iff \((A \cap B) \cup (A \cap C)\) using the fact that the distributivity of \( \land \) over \( \lor \) is a logical equivalence. \( \square \)

We also have the following version of Proposition 1.1 for subsets.

**Proposition 1.9.** For every set \( X \) and any two subsets \( A, B \) of \( X \), the following identities hold:
\[
\overline{\overline{A}} = A \\
(A \cap B) = \overline{A} \cup B \\
(A \cup B) = \overline{A} \cap B.
\]

The last two are de Morgan laws.

Another operation is the power set formation. It is indeed a “powerful” operation, in the sense that it allows us to form very big sets.

**Definition 1.7.** Given any set \( A \), there is a set \( P(A) \) also denoted \( 2^A \) called the **power set** of \( A \) whose members are exactly the subsets of \( A \); that is,
\[
X \in P(A) \iff X \subseteq A.
\]

For example, if \( A = \{a, b, c\} \), then
\[
P(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\},
\]
a set containing eight elements. Note that the empty set and \( A \) itself are always members of \( P(A) \).

**Remark:** If \( A \) has \( n \) elements, it is not hard to show that \( P(A) \) has \( 2^n \) elements. For this reason, many people, including me, prefer the notation \( 2^A \) for the power set of \( A \).

It is possible to define the union of possibly infinitely many sets. Given any set \( X \) (think of \( X \) as a set of sets), there is a set \( \bigcup X \) defined so that
\[
x \in \bigcup X \iff \exists B (B \in X \land x \in B).
\]
This says that \( \bigcup X \) consists of all elements that belong to some member of \( X \).
If we take $X = \{A, B\}$, where $A$ and $B$ are two sets, we see that

$$\bigcup \{A, B\} = A \cup B.$$ 

Observe that

$$\bigcup \{A\} = A, \quad \bigcup \{A_1, \ldots, A_n\} = A_1 \cup \cdots \cup A_n.$$ 

and in particular, $\bigcup \emptyset = \emptyset$.

We can also define infinite intersections. For every nonempty set $X$ there is a set $\bigcap X$ defined by

$$x \in \bigcap X \iff \forall B \in X \Rightarrow x \in B.$$ 

Observe that

$$\bigcap \{A, B\} = A \cap B, \quad \bigcap \{A_1, \ldots, A_n\} = A_1 \cap \cdots \cap A_n.$$ 

However, $\bigcap \emptyset$ is undefined. Indeed, $\bigcap \emptyset$ would have to be the set of all sets, since the condition

$$\forall B (B \in \emptyset \Rightarrow x \in B)$$

holds trivially for all $B$ (as the empty set has no members). However there is no such set, because its existence would lead to a paradox! This point is discussed in Chapter 2. Let us simply say that dealing with big infinite sets is tricky.

Thorough and yet accessible presentations of set theory can be found in Halmos [5] and Enderton [1].

We close this chapter with a quick discussion of induction on the natural numbers.

## 1.12 Induction and The Well–Ordering Principle on the Natural Numbers

Recall that the set of natural numbers is the set $\mathbb{N}$ given by

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

In this chapter we do not attempt to define the natural numbers from other concepts, such as sets. We assume that they are “God given.” One of our main goals is to prove properties of the natural numbers. For this, certain subsets called inductive play a crucial role.

**Definition 1.8.** We say that a subset $S$ of $\mathbb{N}$ is *inductive* iff

1. $0 \in S$.
2. For every $n \in S$, we have $n + 1 \in S$. 
One of the most important proof principles for the natural numbers is the following:

**Proof Template 1.19. (Induction Principle for \( \mathbb{N} \))**

Every inductive subset \( S \) of \( \mathbb{N} \) is equal to \( \mathbb{N} \) itself; that is \( S = \mathbb{N} \).

Let us give one example illustrating Proof Template 1.19.

**Example 1.23.** We prove that for every real number \( a \neq 1 \) and every natural number \( n \), we have

\[
1 + a + \cdots + a^n = \frac{a^{n+1} - 1}{a - 1}.
\]

This can also be written as

\[
\sum_{i=1}^{n} a^i = \frac{a^{n+1} - 1}{a - 1}, \quad (\ast)
\]

with the convention that \( a^0 = 1 \), even if \( a = 0 \). Let \( S \) be the set of natural numbers \( n \) for which the identity \((\ast)\) holds, and let us prove that \( S \) is inductive.

First we need to prove that \( 0 \in S \). The lefthand side becomes \( a^0 = 1 \), and the righthand side is \((a - 1)/(a - 1)\), which is equal to 1 since we assume that \( a \neq 1 \). Therefore, \((\ast)\) holds for \( n = 0 \); that is, \( 0 \in S \).

Next assume that \( n \in S \) (this is called the *induction hypothesis*). We need to prove that \( n + 1 \in S \). Observe that

\[
\sum_{i=1}^{n+1} a^i = \sum_{i=1}^{n} a^i + a^{n+1}.
\]

Now since we assumed that \( n \in S \), we have

\[
\sum_{i=1}^{n} a^i = \frac{a^{n+1} - 1}{a - 1},
\]

and we deduce that

\[
\sum_{i=1}^{n+1} a^i = \sum_{i=1}^{n} a^i + a^{n+1} = \frac{a^{n+1} - 1}{a - 1} + a^{n+1} = \frac{a^{n+1} - 1}{a - 1} + a^{n+2} - a^{n+1} = \frac{a^{n+2} - 1}{a - 1}.
\]

This proves that \( n + 1 \in S \). Therefore, \( S \) is inductive, and so \( S = \mathbb{N} \).

Another important property of \( \mathbb{N} \) is the so-called *well–ordering principle*. This principle turns out to be equivalent to the induction principle for \( \mathbb{N} \). In this chapter we accept the well–ordering principle without proof.
Proof Template 1.20. (Well-Ordering Principle for \( \mathbb{N} \))

Every nonempty subset of \( \mathbb{N} \) has a smallest element.

Proof Template 1.20 can be used to prove properties of \( \mathbb{N} \) by contradiction. For example, consider the property that every natural number \( n \) is either even or odd.

For the sake of contradiction (here, we use the proof–by–contradiction principle), assume that our statement does not hold. If so, the subset \( S \) of natural numbers \( n \) for which \( n \) is neither even nor odd is nonempty. By the well–ordering principle, the set \( S \) has a smallest element, say \( m \).

If \( m = 0 \), then 0 would be neither even nor odd, a contradiction since 0 is even. Therefore, \( m > 0 \). But then, \( m - 1 \notin S \), since \( m \) is the smallest element of \( S \). This means that \( m - 1 \) is either even or odd. But if \( m - 1 \) is even, then \( m - 1 = 2k \) for some \( k \), so \( m = 2k + 1 \) is odd, and if \( m - 1 \) is odd, then \( m - 1 = 2k + 1 \) for some \( k \), so \( m = 2(k + 1) \) is even. We just proved that \( m \) is either even or odd, contradicting the fact that \( m \in S \). Therefore, \( S \) must be empty and we proved the desired result.

We conclude this section with one more example showing the usefulness of the well–ordering principle.

Example 1.24. Suppose we have a property \( P(n) \) of the natural numbers such that \( P(n) \) holds for at least some \( n \), and that for every \( n \) such that \( P(n) \) holds and \( n \geq 100 \), then there is some \( m < n \) such that \( P(m) \) holds. We claim that there is some \( m < 100 \) such that \( P(m) \) holds. Let \( S \) be the set of natural numbers \( n \) such that \( P(n) \) holds. By hypothesis, there is some some \( n \) such that \( P(n) \) holds, so \( S \) is nonempty. By the well–ordering principle, the set \( S \) has a smallest element, say \( m \). For the sake of contradiction, assume that \( m \geq 100 \). Then since \( P(m) \) holds and \( m \geq 100 \), by the hypothesis there is some \( m' < m \) such that \( P(m') \) holds, contradicting the fact that \( m \) is the smallest element of \( S \). Therefore, by the proof–by–contradiction principle, we conclude that \( m < 100 \), as claimed.

Beware that the well–ordering principle is false for \( \mathbb{Z} \), because \( \mathbb{Z} \) does not have a smallest element.

1.13 Summary

The main goal of this chapter is to describe how to construct proofs in terms of proof templates. A brief and informal introduction to sets and set operations is also provided.

- We describe the syntax of propositions.
- We define the proof templates for implication.
- We show that deductions proceed from assumptions (or premises) according to proof templates.
• We introduce falsity $\perp$ and negation $\neg P$ as an abbreviation for $P \Rightarrow \perp$. We describe the proof templates for conjunction, disjunction, and negation.

• We show that one of the rules for negation is the proof–by–contradiction rule (also known as RAA). It plays a special role, in the sense that it allows for the construction of indirect proofs.

• We present the proof–by–contrapositive rule.

• We present the de Morgan laws as well as some basic properties of $\lor$ and $\land$.

• We give some examples of proofs of “real” statements.

• We give an example of a nonconstructive proof of the statement: there are two irrational numbers, $a$ and $b$, so that $a^b$ is rational.

• We explain the truth-value semantics of propositional logic.

• We define the truth tables for the boolean functions associated with the logical connectives (and, or, not, implication, equivalence).

• We define the notion of validity and tautology.

• We discuss soundness (or consistency) and completeness.

• We state the soundness and completeness theorems for propositional classical logic.

• We explain how to use counterexamples to prove that certain propositions are not provable.

• We add first-order quantifiers (“for all” $\forall$ and “there exists” $\exists$) to the language of propositional logic and define first-order logic.

• We describe free and bound variables.

• We describe Proof Templates for the quantifiers.

• We prove some “de Morgan”-type rules for the quantified formulae.

• We introduce sets and explain when two sets are equal.

• We define the notion of subset.

• We define some basic operations on sets: the union $A \cup B$, intersection $A \cap B$, and relative complement $A - B$.

• We define the complement of a subset of a given set.
• We prove some basic properties of union, intersection and complementation, including the \textit{de Morgan laws}.

• We define the \textit{power set} of a set.

• We define \textit{inductive subsets} of \( \mathbb{N} \) and state the \textit{induction principle for} \( \mathbb{N} \).

• We state the \textit{well–ordering principle} for \( \mathbb{N} \).

\textbf{Problems}

\textbf{Problem 1.1.} Give a proof of the proposition \((P \Rightarrow Q) \Rightarrow ((P \Rightarrow (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R))\).

\textbf{Problem 1.2.} (a) Prove the “de Morgan” laws:

\[
\neg(P \land Q) \equiv \neg P \lor \neg Q \\
\neg(P \lor Q) \equiv \neg P \land \neg Q.
\]

(b) Prove the propositions \((P \land \neg Q) \Rightarrow \neg (P \Rightarrow Q)\) and \(\neg (P \Rightarrow Q) \Rightarrow (P \land \neg Q)\).

\textbf{Problem 1.3.} (a) Prove the equivalences

\[
P \lor P \equiv P \\
P \land P \equiv P \\
P \lor Q \equiv Q \lor P \\
P \land Q \equiv Q \land P.
\]

(b) Prove the equivalences

\[
P \land (P \lor Q) \equiv P \\
P \lor (P \land Q) \equiv P.
\]

\textbf{Problem 1.4.} Prove the propositions

\[
P \Rightarrow (Q \Rightarrow (P \land Q)) \\
(P \Rightarrow Q) \Rightarrow ((P \Rightarrow \neg Q) \Rightarrow \neg P) \\
(P \Rightarrow R) \Rightarrow ((Q \Rightarrow R) \Rightarrow ((P \lor Q) \Rightarrow R)).
\]

\textbf{Problem 1.5.} Prove the following equivalences:

\[
P \land (P \Rightarrow Q) \equiv P \land Q \\
Q \land (P \Rightarrow Q) \equiv Q \\
(P \Rightarrow (Q \land R)) \equiv ((P \Rightarrow Q) \land (P \Rightarrow R)).
\]
Problem 1.6. Prove the propositions
\[(P \Rightarrow Q) \Rightarrow \neg\neg(\neg P \vee Q)\]
\[\neg\neg(\neg\neg P \Rightarrow P).
\]

Problem 1.7. Prove the proposition \[\neg\neg(P \vee \neg P).
\]

Problem 1.8. Prove the propositions
\[(P \vee \neg P) \Rightarrow (\neg\neg P \Rightarrow P) \quad \text{and} \quad (\neg\neg P \Rightarrow P) \Rightarrow (P \vee \neg P).
\]

Problem 1.9. Prove the propositions
\[(P \Rightarrow Q) \Rightarrow \neg\neg(\neg P \vee Q) \quad \text{and} \quad (\neg P \Rightarrow Q) \Rightarrow \neg\neg(P \vee Q).
\]

Problem 1.10. (a) Prove the distributivity of \(\wedge\) over \(\vee\) and of \(\vee\) over \(\wedge\):
\[P \wedge (Q \vee R) \equiv (P \wedge Q) \vee (P \wedge R)\]
\[P \vee (Q \wedge R) \equiv (P \vee Q) \wedge (P \vee R).
\]

(b) Prove the associativity of \(\wedge\) and \(\vee\):
\[P \wedge (Q \wedge R) \equiv (P \wedge Q) \wedge R\]
\[P \vee (Q \vee R) \equiv (P \vee Q) \vee R.
\]

Problem 1.11. (a) Let \(X = \{X_i \mid 1 \leq i \leq n\}\) be a finite family of sets. Prove that if \(X_{i+1} \subseteq X_i\) for all \(i\), with \(1 \leq i \leq n - 1\), then
\[\bigcap X = X_n.
\]
Prove that if \(X_i \subseteq X_{i+1}\) for all \(i\), with \(1 \leq i \leq n - 1\), then
\[\bigcup X = X_n.
\]
(b) Recall that \(\mathbb{N}_+ = \mathbb{N} - \{0\} = \{1, 2, 3, \ldots, n, \ldots\}\). Give an example of an infinite family of sets, \(X = \{X_i \mid i \in \mathbb{N}_+\}\), such that
1. \(X_{i+1} \subseteq X_i\) for all \(i \geq 1\).
2. \(X_i\) is infinite for every \(i \geq 1\).
3. \(\bigcap X\) has a single element.

(c) Give an example of an infinite family of sets, \(X = \{X_i \mid i \in \mathbb{N}_+\}\), such that
1. \(X_{i+1} \subseteq X_i\) for all \(i \geq 1\).
2. \( X_i \) is infinite for every \( i \geq 1 \).

3. \( \bigcap X = \emptyset \).

**Problem 1.12.** An integer, \( n \in \mathbb{Z} \), is divisible by 3 iff \( n = 3k \), for some \( k \in \mathbb{Z} \). Thus (by the division theorem), an integer, \( n \in \mathbb{Z} \), is not divisible by 3 iff it is of the form \( n = 3k+1, 3k+2 \), for some \( k \in \mathbb{Z} \) (you don’t have to prove this).

Prove that for any integer, \( n \in \mathbb{Z} \), if \( n^2 \) is divisible by 3, then \( n \) is divisible by 3.

*Hint.* Prove the contrapositive. If \( n \) of the form \( n = 3k + 1, 3k + 2 \), then so is \( n^2 \) (for a different \( k \)).

**Problem 1.13.** Use Problem 1.12 to prove that \( \sqrt{3} \) is irrational, that is, \( \sqrt{3} \) can’t be written as \( \sqrt{3} = p/q \), with \( p, q \in \mathbb{Z} \) and \( q \neq 0 \).

**Problem 1.14.** Prove that \( b = \log_2 9 \) is irrational. Then, prove that \( a = \sqrt{2} \) and \( b = \log_2 9 \) are two irrational numbers such that \( a^b \) is rational.
Bibliography


Chapter 2

Mathematical Reasoning And Logic, A Deeper View

2.1 Introduction

This chapter is a more advanced and more formal version of Chapter 1. The reader should review Chapter 1 before reading this chapter which relies rather heavily on it.

As in Chapter 1, the goal of this chapter is to provide an answer to the question, “What is a proof?” We do so by formalizing the basic rules of reasoning that we use, most of the time subconsciously, in a certain kind of formalism known as a natural deduction system. We give a (very) quick introduction to mathematical logic, with a very deliberate proof-theoretic bent, that is, neglecting almost completely all semantic notions, except at a very intuitive level. We still feel that this approach is fruitful because the mechanical and rules-of-the-game flavor of proof systems is much more easily grasped than semantic concepts. In this approach, we follow Peter Andrews’ motto [1]:

“To truth through proof.”

We present various natural deduction systems due to Prawitz and Gentzen (in more modern notation), both in their intuitionistic and classical version. The adoption of natural deduction systems as proof systems makes it easy to question the validity of some of the inference rules, such as the principle of proof by contradiction. In brief, we try to explain to our readers the difference between constructive and classical (i.e., not necessarily constructive) proofs. In this respect, we plant the seed that there is a deep relationship between constructive proofs and the notion of computation (the “Curry–Howard isomorphism” or “formulae-as-types principle,” see Section 2.12 and Howard [14]).
In this section we review some basic proof principles and attempt to clarify, at least informally, what constitutes a mathematical proof.

In order to define the notion of proof rigorously, we would have to define a formal language in which to express statements very precisely and we would have to set up a proof system in terms of axioms and proof rules (also called inference rules). We do not go into this as this would take too much time. Instead, we content ourselves with an intuitive idea of what a statement is and focus on stating as precisely as possible the rules of logic that are used in constructing proofs. Readers who really want to see a thorough (and rigorous) introduction to logic are referred to Gallier [4], van Dalen [24], or Huth and Ryan [15], a nice text with a computer science flavor. A beautiful exposition of logic (from a proof-theoretic point of view) is also given in Troelstra and Schwichtenberg [23], but at a more advanced level. Frank Pfenning has also written an excellent and more extensive introduction to constructive logic. This is available on the web at


We also highly recommend the beautifully written little book by Timothy Gowers (Fields Medalist, 1998) [11] which, among other things, discusses the notion of proof in mathematics (as well as the necessity of formalizing proofs without going overboard).

In mathematics and computer science, we prove statements. Recall that statements may be atomic or compound, that is, built up from simpler statements using logical connectives, such as implication (if–then), conjunction (and), disjunction (or), negation (not), and (existential or universal) quantifiers.

As examples of atomic statements, we have:

1. “A student is eager to learn.”
2. “The product of two odd integers is odd.”

Atomic statements may also contain “variables” (standing for arbitrary objects). For example

1. human(x): “x is a human.”
2. needs-to-drink(x): “x needs to drink.”

An example of a compound statement is

human(x) ⇒ needs-to-drink(x).

In the above statement, ⇒ is the symbol used for logical implication. If we want to assert that every human needs to drink, we can write

∀x(human(x) ⇒ needs-to-drink(x));
this is read: “For every \( x \), if \( x \) is a human then \( x \) needs to drink.”

If we want to assert that some human needs to drink we write

\[
\exists x (\text{human}(x) \Rightarrow \text{needs-to-drink}(x));
\]

this is read: “There is some \( x \) such that, if \( x \) is a human then \( x \) needs to drink.”

We often denote statements (also called propositions or (logical) formulae) using letters, such as \( A, B, P, Q \), and so on, typically upper-case letters (but sometimes Greek letters, \( \varphi, \psi \), etc.).

Recall from Section 1.2 that Compound statements are defined as follows: If \( P \) and \( Q \) are statements, then

1. the conjunction of \( P \) and \( Q \) is denoted \( P \land Q \) (pronounced, \( P \) and \( Q \)),
2. the disjunction of \( P \) and \( Q \) is denoted \( P \lor Q \) (pronounced, \( P \) or \( Q \)),
3. the implication of \( P \) and \( Q \) is denoted by \( P \Rightarrow Q \) (pronounced, if \( P \) then \( Q \), or \( P \) implies \( Q \)).

Instead of using the symbol \( \Rightarrow \), some authors use the symbol \( \rightarrow \) and write an implication as \( P \rightarrow Q \). We do not like to use this notation because the symbol \( \rightarrow \) is already used in the notation for functions (\( f : A \rightarrow B \)). The symbol \( \supset \) is sometimes used instead of \( \Rightarrow \). We mostly use the symbol \( \Rightarrow \).

We also have the atomic statements \( \perp \) (falsity), think of it as the statement that is false no matter what; and the atomic statement \( \top \) (truth), think of it as the statement that is always true.

The constant \( \perp \) is also called falsum or absurdum. It is a formalization of the notion of absurdity inconsistency (a state in which contradictory facts hold).

Given any proposition \( P \) it is convenient to define

4. the negation \( \neg P \) of \( P \) (pronounced, not \( P \)) as \( P \Rightarrow \perp \). Thus, \( \neg P \) (sometimes denoted \( \sim P \)) is just a shorthand for \( P \Rightarrow \perp \). We write \( \neg P \equiv (P \Rightarrow \perp) \).

The intuitive idea is that \( \neg P \equiv (P \Rightarrow \perp) \) is true if and only if \( P \) is false. Actually, because we don’t know what truth is, it is “safer” (and more constructive) to say that \( \neg P \) is provable if and only if for every proof of \( P \) we can derive a contradiction (namely, \( \perp \) is provable). In particular, \( P \) should not be provable. For example, \( \neg(Q \land \neg Q) \) is provable (as we show later, because any proof of \( Q \land \neg Q \) yields a proof of \( \perp \)). However, the fact that a proposition \( P \) is not provable does not imply that \( \neg P \) is provable. There are plenty of propositions such that both \( P \) and \( \neg P \) are not provable, such as \( Q \Rightarrow R \), where \( Q \) and \( R \) are two unrelated propositions (with no common symbols).

Whenever necessary to avoid ambiguities, we add matching parentheses: \( (P \land Q) \), \( (P \lor Q) \), \( (P \Rightarrow Q) \). For example, \( P \lor Q \land R \) is ambiguous; it means either \( (P \lor (Q \land R)) \) or \( ((P \lor Q) \land R) \).

Another important logical operator is equivalence.

If \( P \) and \( Q \) are statements, then
5. The equivalence of $P$ and $Q$ is denoted $P \equiv Q$ (or $P \iff Q$); it is an abbreviation for $(P \Rightarrow Q) \land (Q \Rightarrow P)$. We often say "$P$ if and only if $Q$" or even "$P$ iff $Q$" for $P \equiv Q$.

To prove a logical equivalence $P \equiv Q$, we have to prove both implications $P \Rightarrow Q$ and $Q \Rightarrow P$.

As discussed in Sections 1.2 and 1.3, the meaning of the logical connectives ($\land$, $\lor$, $\Rightarrow$, $\neg$, $\equiv$) is intuitively clear. This is certainly the case for and ($\land$), since a conjunction $P \land Q$ is true if and only if both $P$ and $Q$ are true (if we are not sure what "true" means, replace it by the word "provable"). However, for or ($\lor$), do we mean inclusive or or exclusive or? In the first case, $P \lor Q$ is true if both $P$ and $Q$ are true, but in the second case, $P \lor Q$ is false if both $P$ and $Q$ are true (again, in doubt change "true" to "provable"). We always mean inclusive or. The situation is worse for implication ($\Rightarrow$). When do we consider that $P \Rightarrow Q$ is true (provable)? The answer is that it depends on the rules! The "classical" answer is that $P \Rightarrow Q$ is false (not provable) if and only if $P$ is true and $Q$ is false.

Of course, there are problems with the above paragraph. What does truth have to do with all this? What do we mean when we say, "$P$ is true"? What is the relationship between truth and provability?

These are actually deep (and tricky) questions whose answers are not so obvious. One of the major roles of logic is to clarify the notion of truth and its relationship to provability. We avoid these fundamental issues by dealing exclusively with the notion of proof. So, the big question is: what is a proof?

An alternative view (that of intuitionistic logic) of the meaning of implication is that any proof of $P \Rightarrow Q$ can be used to construct a proof of $Q$ given any proof of $P$. As a consequence of this interpretation, we show later that if $\neg P$ is provable, then $P \Rightarrow Q$ is also provable (instantly) whether or not $Q$ is provable. In such a situation, we often say that $P \Rightarrow Q$ is vacuously provable.

### 2.3 Proof Rules, Deduction and Proof Trees for Implication

During the process of constructing a proof, it may be necessary to introduce a list of hypotheses, also called premises (or assumptions), which grows and shrinks during the proof. When a proof is finished, it should have an empty list of premises. As we show shortly, this amounts to proving implications of the form

$$(P_1 \land P_2 \land \cdots \land P_n) \Rightarrow Q.$$  

However, there are certain advantages in defining the notion of proof (or deduction) of a proposition from a set of premises. Sets of premises are usually denoted using upper-case Greek letters such as $\Gamma$ or $\Delta$.

Roughly speaking, a deduction of a proposition $Q$ from a multiset of premises $\Gamma$ is a finite labeled tree whose root is labeled with $Q$ (the conclusion), whose leaves are labeled
2.3. PROOF RULES, DEDUCTION AND PROOF TREES FOR IMPLICATION

with premises from $\Gamma$ (possibly with multiple occurrences), and such that every interior node corresponds to a given set of proof rules (or inference rules). In Chapter 1, proof rules were called proof templates. Certain simple deduction trees are declared as obvious proofs, also called axioms. The process of managing the list of premises during a proof is a bit technical and can be achieved in various ways. We will present a method due to Prawitz and another method due to Gentzen.

There are many kinds of proof systems: Hilbert-style systems, natural-deduction systems, Gentzen sequents systems, and so on. We describe a so-called natural deduction system invented by G. Gentzen in the early 1930s (and thoroughly investigated by D. Prawitz in the mid 1960s).

The major advantage of this system is that it captures quite nicely the “natural” rules of reasoning that one uses when proving mathematical statements. This does not mean that it is easy to find proofs in such a system or that this system is indeed very intuitive. We begin with the inference rules for implication and first consider the following question.

How do we proceed to prove an implication, $A \Rightarrow B$? The proof rule corresponds to Proof Template 1.2 (Implication–Intro) and the reader may want to first review the examples discussed in Section 1.3. The rule, called $\Rightarrow$-intro, is: assume that $A$ has already been proven and then prove $B$, making as many uses of $A$ as needed.

An important point is that a proof should not depend on any “open” assumptions and to address this problem we introduce a mechanism of “discharging” or “closing” premises, as we discussed in Section 1.3.

What this means is that certain rules of our logic are required to discard (the usual terminology is “discharge”) certain occurrences of premises so that the resulting proof does not depend on these premises.

Technically, there are various ways of implementing the discharging mechanism but they all involve some form of tagging (with a “new” variable). For example, the rule formalizing the process that we have just described to prove an implication, $A \Rightarrow B$, known as $\Rightarrow$-introduction, uses a tagging mechanism described precisely in Definition 2.1.

Now, the rule that we have just described is not sufficient to prove certain propositions that should be considered provable under the “standard” intuitive meaning of implication. For example, after a moment of thought, I think most people would want the proposition
$P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)$ to be provable. If we follow the procedure that we have advocated, we assume both $P$ and $P \Rightarrow Q$ and we try to prove $Q$. For this, we need a new rule, namely:

If $P$ and $P \Rightarrow Q$ are both provable, then $Q$ is provable.

The above rule is known as the $\Rightarrow$-elimination rule (or modus ponens) and it is formalized in tree-form in Definition 2.1. It corresponds to Proof Template 1.3.

We now make the above rules precise and for this, we represent proofs and deductions as certain kinds of trees and view the logical rules (inference rules) as tree-building rules. In the definition below, the expression $\Gamma, P$ stands for the multiset obtained by adding one more occurrence of $P$ to $\Gamma$. So, $P$ may already belong to $\Gamma$. Similarly, if $\Gamma$ and $\Delta$ are two multisets of propositions, then $\Gamma, \Delta$ denotes the union of $\Gamma$ and $\Delta$ as a multiset, which means that if $P$ occurs $k_1$ times in $\Gamma$ and $P$ occurs $k_2$ times in $\Delta$, then $P$ occurs $k_1 + k_2$ times in $\Gamma, \Delta$ ($k_1, k_2 \in \mathbb{N}$).

A picture such as

```
   Δ
  /\D
 / \P
```

represents a deduction tree $D$ whose root is labeled with $P$ and whose leaves are labeled with propositions from the multiset $\Delta$ (a set possibly with multiple occurrences of its members). Some of the propositions in $\Delta$ may be tagged by variables. The list of untagged propositions in $\Delta$ is the list of premises of the deduction tree. We often use an abbreviated version of the above notation where we omit the deduction $D$, and simply write

```
   Δ
  /\P
```

For example, in the deduction tree below,

```
  P \Rightarrow (R \Rightarrow S)    P \Rightarrow Q    P
       \hline
           Q \Rightarrow R   \quad \hline
                  Q
       \hline
          R \Rightarrow S   \quad \hline
                  R
       \hline
          S
```

no leaf is tagged, so the premises form the multiset

$$\Delta = \{P \Rightarrow (R \Rightarrow S), P, Q \Rightarrow R, P \Rightarrow Q, P\},$$

with two occurrences of $P$, and the conclusion is $S$.

As we saw in our earlier example, certain inferences rules have the effect that some of the original premises may be discarded; the traditional jargon is that some premises may be discharged (or closed). This is the case for the inference rule whose conclusion is an implication. When one or several occurrences of some proposition $P$ are discharged by an inference rule, these occurrences (which label some leaves) are tagged with some new variable not already appearing in the deduction tree. If $x$ is a new tag, the tagged occurrences of $P$
are denoted $P^x$ and we indicate the fact that premises were discharged by that inference by writing $x$ immediately to the right of the inference bar. For example,

\[
\begin{array}{c}
\frac{P^x, Q}{Q} \\
\frac{}{P \Rightarrow Q}
\end{array}
\]

is a deduction tree in which the premise $P$ is discharged by the inference rule. This deduction tree only has $Q$ as a premise, inasmuch as $P$ is discharged.

What is the meaning of the horizontal bars? Actually, nothing really. Here, we are victims of an old habit in logic. Observe that there is always a single proposition immediately under a bar but there may be several propositions immediately above a bar. The intended meaning of the bar is that the proposition below it is obtained as the result of applying an inference rule to the propositions above it. For example, in

\[
\begin{array}{c}
\frac{Q \Rightarrow R}{Q} \\
\frac{}{R}
\end{array}
\]

the proposition $R$ is the result of applying the $\Rightarrow$-elimination rule (see Definition 2.1 below) to the two premises $Q \Rightarrow R$ and $Q$. Thus, the use of the bar is just a convention used by logicians going back at least to the 1900s. Removing the bar everywhere would not change anything in our trees, except perhaps reduce their readability. Most logic books draw proof trees using bars to indicate inferences, therefore we also use bars in depicting our proof trees.

Because propositions do not arise from the vacuum but instead are built up from a set of atomic propositions using logical connectives (here, $\Rightarrow$), we assume the existence of an “official set of atomic propositions,” or set of propositional symbols, $\text{PS} = \{P_1, P_2, P_3, \ldots\}$. So, for example, $P_1 \Rightarrow P_2$ and $P_1 \Rightarrow (P_2 \Rightarrow P_1)$ are propositions. Typically, we use upper-case letters such as $P, Q, R, S, A, B, C$, and so on, to denote arbitrary propositions formed using atoms from $\text{PS}$.

**Definition 2.1.** The axioms, inference rules, and deduction trees for *implicational logic* are defined as follows.

**Axioms.**

(i) Every one-node tree labeled with a single proposition $P$ is a deduction tree for $P$ with set of premises $\{P\}$.

(ii) The tree

\[
\begin{array}{c}
\frac{}{P}
\end{array}
\]

is a deduction tree for $P$ with multiset set of premises $\Gamma, P$.

The above is a concise way of denoting a two-node tree with its leaf labeled with the multiset consisting of $P$ and the propositions in $\Gamma$, each of these propositions (including $P$) having possibly multiple occurrences but at least one, and whose root is labeled with $P$. A more explicit form is
where \( k_1, \ldots, k_n \geq 1 \) and \( n \geq 1 \). This axiom says that we always have a deduction of \( P_i \) from any set of premises including \( P_i \). They correspond to the Proof Template 1.1 (Trivial Deduction).

The \( \Rightarrow \)-**introduction rule.**

If \( \mathcal{D} \) is a deduction tree for \( Q \) from the premises in \( \Gamma \) and one or more occurrences of the proposition \( P \), then

\[
\begin{array}{c}
\Gamma, P^x \\
\mathcal{D} \\
Q \\
\hline
P \Rightarrow Q
\end{array}
\]

is a deduction tree for \( P \Rightarrow Q \) from \( \Gamma \).

This proof rule is a formalization of Proof Template 1.2 (Implication–Intro). Note that this inference rule has the additional effect of discharging a nonempty set of occurrences of the premise \( P \) (which label leaves of the deduction \( \mathcal{D} \)). These occurrences are tagged with a new variable \( x \), and the tag \( x \) is also placed immediately to the right of the inference bar. This is a reminder that the deduction tree whose conclusion is \( P \Rightarrow Q \) no longer has the occurrences of \( P \) labeled with \( x \) as premises.

The \( \Rightarrow \)-**elimination rule.**

If \( \mathcal{D}_1 \) is a deduction tree for \( P \Rightarrow Q \) from the premises \( \Gamma \) and \( \mathcal{D}_2 \) is a deduction for \( P \) from the premises \( \Delta \), then

\[
\begin{array}{c}
\Gamma \\
\mathcal{D}_1 \\
\Delta \\
\mathcal{D}_2 \\
\hline
P \Rightarrow Q \\
P \\
\hline
Q
\end{array}
\]

is a deduction tree for \( Q \) from the premises in the multiset \( \Gamma, \Delta \). This rule is also known as *modus ponens*. This proof rule is a formalization of Proof Template 1.3 (Implication–Elim).

In the above axioms and rules, \( \Gamma \) or \( \Delta \) may be empty; \( P, Q \) denote arbitrary propositions built up from the atoms in \( \text{PS} \); and \( \mathcal{D}, \mathcal{D}_1, \) and \( \mathcal{D}_2 \) denote deductions, possibly a one-node tree.

A *deduction tree* is either a one-node tree labeled with a single proposition or a tree constructed using the above axioms and rules. A *proof tree* is a deduction tree such that *all its premises are discharged*. The above proof system is denoted \( N_m^\Rightarrow \) (here, the subscript \( m \) stands for *minimal*, referring to the fact that this a bare-bones logical system).

Observe that a proof tree has at least two nodes. A proof tree \( \Pi \) for a proposition \( P \) may be denoted
with an empty set of premises (we don’t display \( \emptyset \) on top of \( \Pi \)). We tend to denote deductions by the letter \( D \) and proof trees by the letter \( \Pi \), possibly subscripted.

We emphasize that the \( \Rightarrow \)-introduction rule says that in order to prove an implication \( P \Rightarrow Q \) from a set of premises \( \Gamma \), we assume that \( P \) has already been proven, add \( P \) to the premises in \( \Gamma \), and then prove \( Q \) from \( \Gamma \) and \( P \). Once this is done, the premise \( P \) is deleted.

This rule formalizes the kind of reasoning that we all perform whenever we prove an implication statement. In that sense, it is a natural and familiar rule, except that we perhaps never stopped to think about what we are really doing. However, the business about discharging the premise \( P \) when we are through with our argument is a bit puzzling. Most people probably never carry out this “discharge step” consciously, but such a process does take place implicitly.

Remarks:

1. Only the leaves of a deduction tree may be discharged. Interior nodes, including the root, are never discharged.

2. Once a set of leaves labeled with some premise \( P \) marked with the label \( x \) has been discharged, none of these leaves can be discharged again. So, each label (say \( x \)) can only be used once. This corresponds to the fact that some leaves of our deduction trees get “killed off” (discharged).

3. A proof is a deduction tree whose leaves are all discharged (\( \Gamma \) is empty). This corresponds to the philosophy that if a proposition has been proven, then the validity of the proof should not depend on any assumptions that are still active. We may think of a deduction tree as an unfinished proof tree.

4. When constructing a proof tree, we have to be careful not to include (accidentally) extra premises that end up not being discharged. If this happens, we probably made a mistake and the redundant premises should be deleted. On the other hand, if we have a proof tree, we can always add extra premises to the leaves and create a new proof tree from the previous one by discharging all the new premises.

5. Beware, when we deduce that an implication \( P \Rightarrow Q \) is provable, we do not prove that \( P \) and \( Q \) are provable; we only prove that if \( P \) is provable, then \( Q \) is provable.

The \( \Rightarrow \)-elimination rule formalizes the use of auxiliary lemmas, a mechanism that we use all the time in making mathematical proofs. Think of \( P \Rightarrow Q \) as a lemma that has already been established and belongs to some database of (useful) lemmas. This lemma says if I can prove \( P \) then I can prove \( Q \). Now, suppose that we manage to give a proof of \( P \). It follows from the \( \Rightarrow \)-elimination rule that \( Q \) is also provable.
Observe that in an introduction rule, the conclusion contains the logical connective associated with the rule, in this case, $\Rightarrow$; this justifies the terminology “introduction”. On the other hand, in an elimination rule, the logical connective associated with the rule is gone (although it may still appear in $Q$). The other inference rules for $\land$, $\lor$, and the like, follow this pattern of introduction and elimination.

### 2.4 Examples of Proof Trees

(a) Here is a proof tree for $P \Rightarrow P$:

$$
\begin{array}{c}
P^x \\
\hline
P \\
\hline
P \Rightarrow P
\end{array}
$$

So, $P \Rightarrow P$ is provable; this is the least we should expect from our proof system! Note that

$$
\begin{array}{c}
P^x \\
\hline
P \Rightarrow P
\end{array}
$$

is also a valid proof tree for $P \Rightarrow P$, because the one-node tree labeled with $P$ is a deduction tree.

(b) Here is a proof tree for $(P \Rightarrow Q) \Rightarrow ((Q \Rightarrow R) \Rightarrow (P \Rightarrow R))$:

$$
\begin{array}{c}
(P \Rightarrow Q)^x \\
\hline
P \Rightarrow P \\
\hline
(Q \Rightarrow R)^y \\
\hline
R \\
\hline
P \Rightarrow R \\
\hline
(Q \Rightarrow R) \Rightarrow (P \Rightarrow R)
\end{array}
$$

In order to better appreciate the difference between a deduction tree and a proof tree, consider the following two examples.

1. The tree below is a deduction tree because two of its leaves are labeled with the premises $P \Rightarrow Q$ and $Q \Rightarrow R$, that have not been discharged yet. So this tree represents a deduction of $P \Rightarrow R$ from the set of premises $\Gamma = \{P \Rightarrow Q, Q \Rightarrow R\}$ but it is not a proof tree because $\Gamma \neq \emptyset$. However, observe that the original premise $P$, labeled $x$, has been discharged.

$$
\begin{array}{c}
Q \Rightarrow R \\
\hline
P \Rightarrow Q \\
\hline
R \\
\hline
P \Rightarrow R
\end{array}
$$
2. The next tree was obtained from the previous one by applying the $\Rightarrow$-introduction rule which triggered the discharge of the premise $Q \Rightarrow R$ labeled $y$, which is no longer active. However, the premise $P \Rightarrow Q$ is still active (has not been discharged yet), so the tree below is a deduction tree of $(Q \Rightarrow R) \Rightarrow (P \Rightarrow R)$ from the set of premises $\Gamma = \{P \Rightarrow Q\}$. It is not yet a proof tree inasmuch as $\Gamma \neq \emptyset$.

\[
\begin{array}{c}
(Q \Rightarrow R)^y \\
\phantom{(Q \Rightarrow R)^y} \frac{P \Rightarrow Q}{\phantom{\vdots}} \\
\phantom{(Q \Rightarrow R)^y} \frac{P^x}{Q} \\
\hline
\phantom{(Q \Rightarrow R)^y} \frac{R}{P \Rightarrow R} \\
\hline
\phantom{(Q \Rightarrow R)^y} (Q \Rightarrow R) \Rightarrow (P \Rightarrow R)
\end{array}
\]

Finally, one more application of the $\Rightarrow$-introduction rule discharged the premise $P \Rightarrow Q$, at last, yielding the proof tree in (b).

(c) This example illustrates the fact that different proof trees may arise from the same set of premises $\{P, Q\}$. For example, here are proof trees for $Q \Rightarrow (P \Rightarrow P)$ and $P \Rightarrow (Q \Rightarrow P)$:

\[
\begin{array}{c}
P^x, Q^y \\
\phantom{P^x, Q^y} \frac{P}{\phantom{\vdots}} \\
\phantom{P^x, Q^y} \frac{P \Rightarrow P}{\phantom{\vdots}} \\
\hline
\phantom{P^x, Q^y} \frac{Q \Rightarrow (P \Rightarrow P)}{\phantom{\vdots}}
\end{array}
\]

and

\[
\begin{array}{c}
P^x, Q^y \\
\phantom{P^x, Q^y} \frac{P}{\phantom{\vdots}} \\
\phantom{P^x, Q^y} \frac{Q \Rightarrow P}{\phantom{\vdots}} \\
\hline
\phantom{P^x, Q^y} \frac{P \Rightarrow (Q \Rightarrow P)}{\phantom{\vdots}}
\end{array}
\]

Similarly, there are six proof trees with a conclusion of the form

\[A \Rightarrow (B \Rightarrow (C \Rightarrow P))\]

begining with the deduction

\[
\begin{array}{c}
P^x, Q^y, R^z \\
\phantom{P^x, Q^y, R^z} \frac{P}{\phantom{\vdots}}
\end{array}
\]

where $A, B, C$ correspond to the six permutations of the premises $P, Q, R$.

Note that we would not have been able to construct the above proofs if Axiom (ii),

\[
\frac{\Gamma, P}{P}
\]
were not available. We need a mechanism to “stuff” more premises into the leaves of our deduction trees in order to be able to discharge them later on. We may also view Axiom (ii) as a weakening rule whose purpose is to weaken a set of assumptions. Even though we are assuming all of the proposition in Γ and P, we only use the assumption P. The necessity of allowing multisets of premises is illustrated by the following proof of the proposition P \Rightarrow (P \Rightarrow (Q \Rightarrow (P \Rightarrow P))):

\[
\frac{P^u, P^v, P^y, Q^w, Q^x}{P} \quad \frac{P \Rightarrow P}{P} \quad \frac{Q \Rightarrow (P \Rightarrow P)}{Q \Rightarrow (Q \Rightarrow (P \Rightarrow P))} \quad \frac{P \Rightarrow (Q \Rightarrow (Q \Rightarrow (P \Rightarrow P)))}{P \Rightarrow (P \Rightarrow (Q \Rightarrow (Q \Rightarrow (P \Rightarrow P))))}
\]

(d) In the next example which shows a proof of

\[(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)),\]

the two occurrences of A labeled x are discharged simultaneously:

\[
\frac{(A \Rightarrow (B \Rightarrow C))^z}{B \Rightarrow C} \quad \frac{A^x}{B} \quad \frac{(A \Rightarrow B)^y}{A \Rightarrow C} \quad \frac{A^z}{(A \Rightarrow B) \Rightarrow (A \Rightarrow C)}
\]

(e) In contrast to Example (d), in the proof tree below with conclusion

\[A \Rightarrow \left( (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C)) \right),\]

the two occurrences of A are discharged separately. To this effect, they are labeled differently.
2.4. EXAMPLES OF PROOF TREES

\[
\begin{array}{c}
(A \Rightarrow (B \Rightarrow C)) \\
B \Rightarrow C
\end{array} \quad \begin{array}{c}
A^x \\
C
\end{array} \quad \begin{array}{c}
(A \Rightarrow B)^y \\
B
\end{array} \quad \begin{array}{c}
A^t
\end{array}
\]

How do we find these proof trees? Well, we could try to enumerate all possible proof trees systematically and see if a proof of the desired conclusion turns up. Obviously, this is a very inefficient procedure and moreover, how do we know that all possible proof trees will be generated and how do we know that such a method will terminate after a finite number of steps (what if the proposition proposed as a conclusion of a proof is not provable)?

Finding an algorithm to decide whether a proposition is provable is a very difficult problem and for sets of propositions with enough “expressive power” (such as propositions involving first-order quantifiers), it can be shown that there is no procedure that will give an answer in all cases and terminate in a finite number of steps for all possible input propositions. We come back to this point in Section 2.12. However, for the system \( \mathcal{N}_m \Rightarrow \), such a procedure exists but it is not easy to prove that it terminates in all cases and in fact, it can take a very long time.

What we did, and we strongly advise our readers to try it when they attempt to construct proof trees, is to construct the proof tree from the bottom up, starting from the proposition labeling the root, rather than top-down, that is, starting from the leaves. During this process, whenever we are trying to prove a proposition \( P \Rightarrow Q \), we use the \( \Rightarrow \)-introduction rule backward, that is, we add \( P \) to the set of active premises and we try to prove \( Q \) from this new set of premises. At some point, we get stuck with an atomic proposition, say \( R \). Call the resulting deduction \( \mathcal{D}_{bu} \); note that \( R \) is the only active (undischarged) premise of \( \mathcal{D}_{bu} \) and the node labeled \( R \) immediately below it plays a special role; we call it the special node of \( \mathcal{D}_{bu} \).

Here is an illustration of this method for Example (d). At the end of the bottom-up process, we get the deduction tree \( \mathcal{D}_{bu} \):

\[
\begin{array}{c}
(A \Rightarrow (B \Rightarrow C)) \\
C
\end{array} \quad \begin{array}{c}
(A \Rightarrow B)^y \\
A^x \\
C
\end{array} \quad \begin{array}{c}
A^t
\end{array}
\]
In the above deduction tree the proposition $R = C$ is the only active (undischarged) premise. To turn the above deduction tree into a proof tree we need to construct a deduction of $C$ from the premises other than $C$. This is a more creative step which can be quite difficult. The trick is now to switch strategies and start building a proof tree top-down, starting from the leaves, using the $\Rightarrow$-elimination rule. If everything works out well, we get a deduction with root $R$, say $D_{td}$, and then we glue this deduction $D_{td}$ to the deduction $D_{bu}$ in such a way that the root of $D_{td}$ is identified with the special node of $D_{bu}$ labeled $R$.

We also have to make sure that all the discharged premises are linked to the correct instance of the $\Rightarrow$-introduction rule that caused them to be discharged. One of the difficulties is that during the bottom-up process, we don’t know how many copies of a premise need to be discharged in a single step. We only find out how many copies of a premise need to be discharged during the top-down process.

Going back to our example, at the end of the top-down process, we get the deduction tree $D_{td}$:

$$\frac{A \Rightarrow (B \Rightarrow C) \quad A \Rightarrow B \quad A}{B \Rightarrow C \quad A \quad B \quad C}$$

Finally, after gluing $D_{td}$ on top of $D_{bu}$ (which has the correct number of premises to be discharged), we get our proof tree:

$$\frac{(A \Rightarrow (B \Rightarrow C))z \quad A^x \quad (A \Rightarrow B)^y \quad A^x}{B \Rightarrow C \quad A \Rightarrow C \quad B \quad C \quad A \Rightarrow C}$$

$$(A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))$$

(f) The following example shows that proofs may be redundant. The proposition $P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)$ has the following proof.

$$\frac{(P \Rightarrow Q)^x \quad P^y}{Q \quad (P \Rightarrow Q) \Rightarrow Q \quad P \Rightarrow ((P \Rightarrow Q) \Rightarrow Q)}$$

Now, say $P$ is the proposition $R \Rightarrow R$, which has the proof

$$\frac{Rz}{R \Rightarrow R}$$
Using \( \Rightarrow \)-elimination, we obtain a proof of \((R \Rightarrow R) \Rightarrow Q\) from the proof of \((R \Rightarrow R) \Rightarrow ((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q\) and the proof of \(R \Rightarrow R\) shown above:

\[
\frac{(R \Rightarrow R) \Rightarrow Q^x \quad (R \Rightarrow R)^y}{Q} \quad \frac{Q}{((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q} \quad \frac{R^z}{R} \quad \frac{R}{R} \quad \frac{((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q}{(R \Rightarrow R) \Rightarrow ((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q}
\]

Note that the above proof is redundant. The deduction tree shown in blue has the proposition \((R \Rightarrow R) \Rightarrow Q\) as conclusion but the proposition \(R \Rightarrow R\) is introduced in the step labeled \(y\) and immediately eliminated in the next step. A more direct proof can be obtained as follows. Undo the last \(\Rightarrow\)-introduction (involving the proposition \(R \Rightarrow R\) and the tag \(y\)) in the proof of \((R \Rightarrow R) \Rightarrow ((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q\) obtaining the deduction tree shown in blue above

\[
\frac{(R \Rightarrow R) \Rightarrow Q^x \quad R \Rightarrow R}{Q} \quad \frac{Q}{((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q}
\]

and then glue the proof of \(R \Rightarrow R\) on top of the leaf \(R \Rightarrow R\), obtaining the desired proof of \((R \Rightarrow R) \Rightarrow Q\) \Rightarrow Q:\n
\[
\frac{R^z}{R} \quad \frac{R \Rightarrow R}{Q} \quad \frac{(R \Rightarrow R) \Rightarrow Q^x}{x} \quad \frac{(R \Rightarrow R) \Rightarrow Q}{x}
\]

In general, one has to exercise care with the label variables. It may be necessary to rename some of these variables to avoid clashes. What we have above is an example of proof substitution also called proof normalization. We come back to this topic in Section 2.12.

While it is necessary to allow multisets of premises as shown in Example (c), our definition allows undesirable proof trees such as

\[
\frac{P^x, P^x, Q^y, Q^y}{P} \quad \frac{P}{P \Rightarrow P} \quad \frac{Q \Rightarrow (P \Rightarrow P)}{y}
\]

in which the two occurrences of \(P\) labeled \(x\) are discharged at the same time and the two
occurrences of $Q$ labeled $y$ are discharged at the same time. Obviously, the above proof tree is equivalent to the proof tree

$$\frac{P^x, Q^y}{P} \quad \frac{P}{Q \Rightarrow (P \Rightarrow P)}$$

We leave it as an exercise to show that we can restrict ourselves to deduction trees and proof trees in which the labels of propositions appearing as premises of Rule Axioms (ii) are all distinct.

## 2.5 A Gentzen-Style System for Natural Deduction

The process of discharging premises when constructing a deduction is admittedly a bit confusing. Part of the problem is that a deduction tree really represents the last of a sequence of stages (corresponding to the application of inference rules) during which the current set of “active” premises, that is, those premises that have not yet been discharged (closed, cancelled) evolves (in fact, shrinks). Some mechanism is needed to keep track of which premises are no longer active and this is what this business of labeling premises with variables achieves. Historically, this is the first mechanism that was invented. However, Gentzen (in the 1930s) came up with an alternative solution that is mathematically easier to handle. Moreover, it turns out that this notation is also better suited to computer implementations, if one wishes to implement an automated theorem prover.

The point is to keep a record of all undischarged assumptions at every stage of the deduction. Thus, a deduction is now a tree whose nodes are labeled with pairs of the form $\langle \Gamma, P \rangle$, where $P$ is a proposition, and $\Gamma$ is a record of all undischarged assumptions at the stage of the deduction associated with this node.

Instead of using the notation $\langle \Gamma, P \rangle$, which is a bit cumbersome, Gentzen used expressions of the form $\Gamma \rightarrow P$, called sequents

It should be noted that the symbol $\rightarrow$ is used as a separator between the left-hand side $\Gamma$, called the antecedent, and the right-hand side $P$, called the conclusion (or succedent) and any other symbol could be used. Of course $\rightarrow$ is reminiscent of implication but we should not identify $\rightarrow$ and $\Rightarrow$. Still, it turns out that a sequent $\Gamma \rightarrow P$ is provable if and only if $(P_1 \land \cdots \land P_m) \Rightarrow P$ is provable, where $\Gamma = (P_1, \ldots, P_m)$.

During the construction of a deduction tree, it is necessary to discharge packets of assumptions consisting of one or more occurrences of the same proposition. To this effect, it is convenient to tag packets of assumptions with labels, in order to discharge the propositions in these packets in a single step. We use variables for the labels, and a packet labeled with $x$ consisting of occurrences of the proposition $P$ is written as $x: P$. 
Definition 2.2. A sequent is an expression $\Gamma \rightarrow P$, where $\Gamma$ is any finite set of the form $\{x_1: P_1, \ldots, x_m: P_m\}$ called a context, where the $x_i$ are pairwise distinct (but the $P_i$ need not be distinct). Given $\Gamma = \{x_1: P_1, \ldots, x_m: P_m\}$, the notation $\Gamma, x: P$ is only well defined when $x \neq x_i$ for all $i$, $1 \leq i \leq m$, in which case it denotes the set $\{x_1: P_1, \ldots, x_m: P_m, x: P\}$. Given two contexts $\Gamma$ and $\Delta$, the context $\Gamma \cup \Delta$ is the union of the sets of pairs $(x_i: P_i)$ in $\Gamma$ and the set of pairs $(y_k: Q_j)$ in $\Delta$, provided that if $x: P \in \Gamma$ and $x: Q \in \Delta$ for the same variable $x$, then $P = Q$. In this case we say that $\Gamma$ and $\Delta$ are consistent. So if $x: P$ occurs both in $\Gamma$ and $\Delta$, then $x: P$ also occurs in $\Gamma \cup \Delta$ (once).

One can think of a context $\Gamma = \{x_1: P_1, \ldots, x_m: P_m\}$ as a set of type declarations for the variables $x_1, \ldots, x_m$ ($x_i$ has type $P_i$). It should be noted that in the Prawitz-style formalism for proof trees, premises are treated as multisets, but in the Genten-style formalism, premises are sets of tagged pairs.

Using sequents, the axioms and rules of Definition 2.3 are now expressed as follows.

Definition 2.3. The axioms and inference rules of the system $\mathcal{NG}^\Rightarrow_m$ (implicational logic, Gentzen-sequent style (the $\mathcal{G}$ in $\mathcal{NG}$ stands for Gentzen)) are listed below:

\[
\Gamma, x: P \Rightarrow P \quad \text{(Axioms)}
\]

\[
\frac{\Gamma, x: P \Rightarrow Q}{\Gamma \Rightarrow P \Rightarrow Q} \quad (\Rightarrow\text{-intro})
\]

\[
\frac{\Gamma \Rightarrow P \Rightarrow Q \quad \Delta \Rightarrow P}{\Gamma \cup \Delta \Rightarrow Q} \quad (\Rightarrow\text{-elim})
\]

In an application of the rule $(\Rightarrow\text{-intro})$, observe that in the lower sequent, the proposition $P$ (labeled $x$) is deleted from the list of premises occurring on the left-hand side of the arrow in the upper sequent. We say that the proposition $P$ that appears as a hypothesis of the deduction is discharged (or closed). In the rule $(\Rightarrow\text{-elim})$, it is assumed that $\Gamma$ and $\Delta$ are consistent contexts. A deduction tree is either a one-node tree labeled with an axiom or a tree constructed using the above inference rules. A proof tree is a deduction tree whose conclusion is a sequent with an empty set of premises (a sequent of the form $\rightarrow P$).

It is important to note that the ability to label packets consisting of occurrences of the same proposition with different labels is essential in order to be able to have control over which groups of packets of assumptions are discharged simultaneously. Equivalently, we could avoid tagging packets of assumptions with variables if we assume that in a sequent $\Gamma \rightarrow C$, the expression $\Gamma$ is a multiset of propositions.

Let us display the proof tree for the second proof tree in Example (c) in our new Gentzen-sequent system. The original proof tree is

\[
\frac{P^x, Q^y}{P^x \Rightarrow Q^y}{\text{P}} \quad \frac{P}{Q \Rightarrow P^y} \quad y \quad \frac{Q \Rightarrow P^x \Rightarrow (Q \Rightarrow P)}{P \Rightarrow (Q \Rightarrow P)} \quad x
\]
and the corresponding proof tree in our new system is

\[
x: P, y: Q \Rightarrow P \\
x: P \Rightarrow Q \Rightarrow P \\
\Rightarrow P \Rightarrow (Q \Rightarrow P)
\]

Below we show a proof of the first proposition of Example (d) given above in our new system.

\[
z: A \Rightarrow (B \Rightarrow C) \Rightarrow A \Rightarrow (B \Rightarrow C) \\
x: A \Rightarrow A \\
y: A \Rightarrow B \Rightarrow A \Rightarrow B \\
x: A \Rightarrow A
\]

\[
z: A \Rightarrow (B \Rightarrow C), x: A \Rightarrow B \Rightarrow C \\
y: A \Rightarrow B, x: A \Rightarrow B \\
z: A \Rightarrow (B \Rightarrow C), y: A \Rightarrow B \Rightarrow A \Rightarrow C \\
z: A \Rightarrow (B \Rightarrow C) \Rightarrow (A \Rightarrow B) \Rightarrow (A \Rightarrow C)
\]

\[
\Rightarrow (A \Rightarrow (B \Rightarrow C)) \Rightarrow ((A \Rightarrow B) \Rightarrow (A \Rightarrow C))
\]

It is not hard to design an algorithm that converts a deduction tree (or a proof tree) in the system \(N_m\Rightarrow\) into a deduction tree (or a proof tree) in the system \(NG_m\Rightarrow\), and vice-versa. In both cases the underlying tree is exactly the same and there is a bijection between the sets of undischarged premises in both representations.

After experimenting with the construction of proofs, one gets the feeling that every proof can be simplified to a “unique minimal” proof, if we define “minimal” in a suitable sense, namely, that a minimal proof never contains an elimination rule immediately following an introduction rule (for more on this, see Section 2.12). Then it turns out that to define the notion of uniqueness of proofs, the second version is preferable. However, it is important to realize that in general, a proposition may possess distinct minimal proofs.

In principle, it does not matter which of the two systems \(N_m\Rightarrow\) or \(NG_m\Rightarrow\) we use to construct deductions; it is basically a matter of taste. The Prawitz-style system \(N_m\Rightarrow\) produces proofs that are closer to the informal proofs that humans construct. One the other hand, the Gentzen-style system \(NG_m\Rightarrow\) is better suited for implementing theorem provers. My experience is that I make fewer mistakes with the Gentzen-sequent style system \(NG_m\Rightarrow\).

We now describe the inference rules dealing with the connectives \(\land\), \(\lor\) and \(\bot\).

### 2.6 Adding \(\land\), \(\lor\), \(\bot\); The Proof Systems \(N_c\Rightarrow,\land,\lor,\bot\) and \(NG_c\Rightarrow,\land,\lor,\bot\)

In this section we describe the proof rules for all the connectives of propositional logic both in Prawitz-style and in Gentzen-style. As we said earlier, the rules of the Prawitz-style system are closer to the rules that human use informally, and the rules of the Gentzen-style system are more convenient for computer implementations of theorem provers.
2.6. ADDING $\land$, $\lor$, $\bot$; THE PROOF SYSTEMS $\mathcal{N}^{\Rightarrow, \land, \lor, \bot}_C$ AND $\mathcal{N}^{\Rightarrow, \land, \lor, \bot}_G$

The rules involving $\bot$ are not as intuitively justified as the other rules. In fact, in the early 1900s, some mathematicians especially L. Brouwer (1881–1966), questioned the validity of the proof-by-contradiction rule, among other principles. This led to the idea that it may be useful to consider proof systems of different strength. The weakest (and considered the safest) system is called minimal logic. This system rules out the $\bot$-elimination rule (the ability to deduce any proposition once a contradiction has been established) and the proof-by-contradiction rule. Intuitionistic logic rules out the proof-by-contradiction rule, and classical logic allows all the rules. Most people use classical logic, but intuitionistic logic is an interesting alternative because it is more constructive. We will elaborate on this point later. Minimal logic is just too weak.

Recall that $\neg P$ is an abbreviation for $P \Rightarrow \bot$.

**Definition 2.4.** The axioms, inference rules, and deduction trees for (propositional) classical logic are defined as follows. In the axioms and rules below, $\Gamma$, $\Delta$, or $\Lambda$ may be empty; $P, Q, R$ denote arbitrary propositions built up from the atoms in $\text{PS}$; $D, D_1, D_2$ denote deductions, possibly a one-node tree; and all the premises labeled $x$ or $y$ are discharged.

**Axioms:**

(i) Every one-node tree labeled with a single proposition $P$ is a deduction tree for $P$ with set of premises $\{P\}$.

(ii) The tree

$$
\begin{array}{c}
\Gamma, P \\
\hline
P
\end{array}
$$

is a deduction tree for $P$ with multiset of premises $\Gamma, P$.

The $\Rightarrow$-introduction rule:

If $D$ is a deduction of $Q$ from the premises in $\Gamma$ and one or more occurrences of the proposition $P$, then

$$
\begin{array}{c}
\Gamma, P^x \\
D \\
\hline
Q
\end{array}
$$

$$
\begin{array}{c}
\Gamma \\
\hline
P \Rightarrow Q
\end{array}
$$

is a deduction tree for $P \Rightarrow Q$ from $\Gamma$. Note that this inference rule has the additional effect of discharging a nonempty set of occurrences of the premise $P$ (which label leaves of the deduction $D$). These occurrences are tagged with a new variable $x$, and the tag $x$ is also placed immediately to the right of the inference bar. This proof rule corresponds to Proof Template 1.2 (Implication–Intro).

The $\Rightarrow$-elimination rule (or modus ponens):

If $D_1$ is a deduction tree for $P \Rightarrow Q$ from the premises $\Gamma$, and $D_2$ is a deduction for $P$ from the premises $\Delta$, then
is a deduction tree for $Q$ from the premises in the multiset $\Gamma, \Delta$. This proof rule corresponds to Proof Template 1.3 (Implication–Elim).

The $\wedge$-introduction rule:
If $\mathcal{D}_1$ is a deduction tree for $P$ from the premises $\Gamma$, and $\mathcal{D}_2$ is a deduction for $Q$ from the premises $\Delta$, then

\[
\begin{array}{c}
\Gamma & \Delta \\
\mathcal{D}_1 & \mathcal{D}_2 \\
\hline
P & Q \\
\hline
P \wedge Q
\end{array}
\]

is a deduction tree for $P \wedge Q$ from the premises in the multiset $\Gamma, \Delta$. This proof rule corresponds to Proof Template 1.8 (And–Intro).

The $\wedge$-elimination rule:
If $\mathcal{D}$ is a deduction tree for $P \wedge Q$ from the premises $\Gamma$, then

\[
\begin{array}{c}
\Gamma & \Gamma \\
\mathcal{D} & \mathcal{D} \\
\hline
P \wedge Q & P \wedge Q \\
\hline
P & Q
\end{array}
\]

are deduction trees for $P$ and $Q$ from the premises $\Gamma$. This proof rule corresponds to Proof Template 1.9 (And–elim).

The $\lor$-introduction rule:
If $\mathcal{D}$ is a deduction tree for $P$ or for $Q$ from the premises $\Gamma$, then

\[
\begin{array}{c}
\Gamma & \Gamma \\
\mathcal{D} & \mathcal{D} \\
\hline
P \lor Q & P \lor Q \\
\hline
P & Q
\end{array}
\]

are deduction trees for $P \lor Q$ from the premises in $\Gamma$. This proof rule corresponds to Proof Template 1.10 (Or–Intro).

The $\lor$-elimination rule:
If $\mathcal{D}_1$ is a deduction tree for $P \lor Q$ from the premises $\Gamma$, $\mathcal{D}_2$ is a deduction for $R$ from the premises in the multiset $\Delta$ and one or more occurrences of $P$, and $\mathcal{D}_3$ is a deduction for $R$ from the premises in the multiset $\Lambda$ and one or more occurrences of $Q$, then

\[
\begin{array}{c}
\Gamma & \Delta \\
\mathcal{D}_1 & \mathcal{D}_2 \\
\hline
P \lor Q & P \lor Q \\
\hline
R
\end{array}
\]
2.6. ADDING $\land$, $\lor$, $\bot$; THE PROOF SYSTEMS $\mathcal{N}^\land,\lor,\bot_C$ AND $\mathcal{N}^\land,\lor,\bot_G$

\[
\begin{array}{ccc}
\Gamma & \Delta, P^x & \Lambda, Q^y \\
\mathcal{D}_1 & \mathcal{D}_2 & \mathcal{D}_3 \\
P \lor Q & R & R \\
\hline \\
R & x, y
\end{array}
\]

is a deduction tree for $R$ from the premises in the multiset $\Gamma, \Delta, \Lambda$. A nonempty set of premises $P$ in $\mathcal{D}_2$ labeled $x$ and a nonempty set of premises $Q$ in $\mathcal{D}_3$ labeled $y$ are discharged. This proof rule corresponds to Proof Template 1.11 (Or–Elim).

The $\bot$-elimination rule:

If $\mathcal{D}$ is a deduction tree for $\bot$ from the premises $\Gamma$, then

\[
\begin{array}{c}
\Gamma \\
\mathcal{D} \\
\bot \\
\hline \\
P \\
x
\end{array}
\]

is a deduction tree for $P$ from the premises $\Gamma$, for any proposition $P$. This proof rule corresponds to Proof Template 1.6 (Perp–Elim).

The proof–by–contradiction rule (also known as reductio ad absurdum rule, for short RAA):

If $\mathcal{D}$ is a deduction tree for $\bot$ from the premises in the multiset $\Gamma$ and one or more occurrences of $\neg P$, then

\[
\begin{array}{c}
\Gamma, \neg P^x \\
\mathcal{D} \\
\bot \\
\hline \\
\neg P \\
x
\end{array}
\]

is a deduction tree for $P$ from the premises $\Gamma$. A nonempty set of premises $\neg P$ labeled $x$ are discharged. This proof rule corresponds to Proof Template 1.7 (Proof–By–Contradiction Principle).

Because $\neg P$ is an abbreviation for $P \Rightarrow \bot$, the $\neg$-introduction rule is a special case of the $\Rightarrow$-introduction rule (with $Q = \bot$). However, it is worth stating it explicitly.

The $\neg$-introduction rule:

If $\mathcal{D}$ is a deduction tree for $\bot$ from the premises in the multiset $\Gamma$ and one or more occurrences of $P$, then

\[
\begin{array}{c}
\Gamma, P^x \\
\mathcal{D} \\
\bot \\
\hline \\
\neg P \\
x
\end{array}
\]

is a deduction tree for $\neg P$ from the premises $\Gamma$. A nonempty set of premises $P$ labeled $x$ are discharged. This proof rule corresponds to Proof Template 1.4 (Negation–Intro).
The above rule can be viewed as a proof–by–contradiction principle applied to negated propositions.

Similarly, the \( \neg \)-elimination rule is a special case of \( \Rightarrow \)-elimination applied to
\( \neg P (= P \Rightarrow \bot) \) and \( P \).

The \( \neg \)-elimination rule:
If \( D_1 \) is a deduction tree for \( \neg P \) from the premises \( \Gamma \), and \( D_2 \) is a deduction for \( P \) from the premises \( \Delta \), then

\[
\begin{array}{c}
\Gamma \\
D_1 \\
\neg P \\
\Delta \\
D_2 \\
P \\
\bot
\end{array}
\]

is a deduction tree for \( \bot \) from the premises in the multiset \( \Gamma, \Delta \). This proof rule corresponds to Proof Template 1.5 (Negation–Elim).

A deduction tree is either a one-node tree labeled with a single proposition or a tree constructed using the above axioms and inference rules. A proof tree is a deduction tree such that all its premises are discharged. The above proof system is denoted \( \mathcal{N}'_{\Rightarrow, \land, \lor, \bot} \) (here, the subscript \( c \) stands for classical).

The system obtained by removing the proof–by–contradiction (RAA) rule is called (propositional) intuitionistic logic and is denoted \( \mathcal{N}'_{\Rightarrow, \land, \lor, \bot} \). The system obtained by deleting both the \( \bot \)-elimination rule and the proof–by–contradiction rule is called (propositional) minimal logic and is denoted \( \mathcal{N}'_{\Rightarrow, \land, \lor, \bot} \).

The version of \( \mathcal{N}'_{\Rightarrow, \land, \lor, \bot} \) in terms of Gentzen sequents is the following.

**Definition 2.5.** The axioms and inference rules of the system \( \mathcal{N}'_{\Rightarrow, \land, \lor, \bot} \) (of propositional classical logic, Gentzen-sequent style) are listed below.

\[
\begin{align*}
\Gamma, x: & P \rightarrow P \quad \text{(Axioms)} \\
\Gamma, x: & P \rightarrow Q \quad \Rightarrow\text{-intro} \\
\Gamma \rightarrow P & \Rightarrow Q \quad \Rightarrow\text{-elim} \\
\Delta \rightarrow P & \land Q \quad \Rightarrow\text{-elim} \\
\Gamma \cup \Delta & \rightarrow P \quad \land\text{-intro} \\
\Gamma \rightarrow P & \land Q \quad \land\text{-elim} \\
\Gamma & \rightarrow P \quad \lor\text{-intro} \\
\Gamma & \rightarrow P \quad \lor\text{-intro}
\end{align*}
\]
A deduction tree is either a one-node tree labeled with an axiom or a tree constructed using the above inference rules. A proof tree is a deduction tree whose conclusion is a sequent with an empty set of premises (a sequent of the form \( \emptyset \to P \)).

The rule \((\bot\text{-elim})\) is trivial (does nothing) when \( P = \bot \), therefore from now on we assume that \( P \neq \bot \). Propositional minimal logic, denoted \( \mathcal{NG}_m^{\Rightarrow, \land, \lor, \bot} \), is obtained by dropping the \((\bot\text{-elim})\) and \((\text{by-contra})\) rules. Propositional intuitionistic logic, denoted \( \mathcal{NG}_i^{\Rightarrow, \land, \lor, \bot} \), is obtained by dropping the \((\text{by-contra})\) rule.

When we say that a proposition \( P \) is provable from \( \Gamma \), we mean that we can construct a proof tree whose conclusion is \( P \) and whose set of premises is \( \Gamma \), in one of the systems \( \mathcal{N}_c^{\Rightarrow, \land, \lor, \bot} \) or \( \mathcal{NG}_c^{\Rightarrow, \land, \lor, \bot} \). Therefore, when we use the word “provable” unqualified, we mean provable in classical logic. If \( P \) is provable from \( \Gamma \) in one of the intuitionistic systems \( \mathcal{N}_i^{\Rightarrow, \land, \lor, \bot} \) or \( \mathcal{NG}_i^{\Rightarrow, \land, \lor, \bot} \), then we say intuitionistically provable (and similarly, if \( P \) is provable from \( \Gamma \) in one of the systems \( \mathcal{N}_m^{\Rightarrow, \land, \lor, \bot} \) or \( \mathcal{NG}_m^{\Rightarrow, \land, \lor, \bot} \), then we say provable in minimal logic). When \( P \) is provable from \( \Gamma \), most people write \( \Gamma \vdash P \), or \( \vdash \Gamma \to P \), sometimes with the name of the corresponding proof system tagged as a subscript on the sign \( \vdash \) if necessary to avoid ambiguities. When \( \Gamma \) is empty, we just say \( P \) is provable (provable in intuitionistic logic, and so on) and write \( \vdash P \).

We treat logical equivalence as a derived connective: that is, we view \( P \equiv Q \) as an abbreviation for \((P \Rightarrow Q) \land (Q \Rightarrow P)\). In view of the inference rules for \( \land \), we see that to prove a logical equivalence \( P \equiv Q \), we just have to prove both implications \( P \Rightarrow Q \) and \( Q \Rightarrow P \).

Since the only difference between the proof systems \( \mathcal{N}_m^{\Rightarrow, \land, \lor, \bot} \) and \( \mathcal{NG}_m^{\Rightarrow, \land, \lor, \bot} \) is the way in which they perform the bookkeeping of premises, it is intuitively clear that they are equivalent. However, they produce different kinds of proof so to be rigorous we must check that the proof systems \( \mathcal{N}_m^{\Rightarrow, \land, \lor, \bot} \) and \( \mathcal{NG}_m^{\Rightarrow, \land, \lor, \bot} \) (as well as the systems \( \mathcal{N}_c^{\Rightarrow, \land, \lor, \bot} \) and \( \mathcal{NG}_c^{\Rightarrow, \land, \lor, \bot} \)) are equivalent. This is not hard to show but is a bit tedious; see Problem 2.14.

In view of the \( \neg\text{-elimination} \) rule, we may be tempted to interpret the provability of a negation \( \neg P \) as “\( P \) is not provable.” Indeed, if \( \neg P \) and \( P \) were both provable, then \( \bot \) would
be provable. So, $P$ should not be provable if $\neg P$ is. However, if $P$ is not provable, then $\neg P$ is not provable in general. There are plenty of propositions such that neither $P$ nor $\neg P$ is provable (for instance, $P$, with $P$ an atomic proposition). Thus, the fact that $P$ is not provable is not equivalent to the provability of $\neg P$ and we should not interpret $\neg P$ as “$P$ is not provable.”

Let us now make some (much-needed) comments about the above inference rules. There is no need to repeat our comments regarding the $\Rightarrow$-rules. The $\lor$-introduction rule says that if $P$ (or $Q$) has been proved from $\Gamma$, then $P \lor Q$ is also provable from $\Gamma$. Again, this makes sense intuitively as $P \lor Q$ is “weaker” than $P$ and $Q$.

The $\lor$-elimination rule formalizes the proof–by–cases method. It is a more subtle rule. The idea is that if we know that in the case where $P$ is already assumed to be provable and similarly in the case where $Q$ is already assumed to be provable that we can prove $R$ (also using premises in $\Gamma$), then if $P \lor Q$ is also provable from $\Gamma$, as we have “covered both cases,” it should be possible to prove $R$ from $\Gamma$ only (i.e., the premises $P$ and $Q$ are discarded). For example, if remain1$(n)$ is the proposition that asserts $n$ is a natural number of the form $4k + 1$ and remain3$(n)$ is the proposition that asserts $n$ is a natural number of the form $4k + 3$ (for some natural number $k$), then we can prove the implication

$$(\text{remain1}(n) \lor \text{remain3}(n)) \Rightarrow \text{odd}(n),$$

where $\text{odd}(n)$ asserts that $n$ is odd, namely, that $n$ is of the form $2h + 1$ for some $h$.

To prove the above implication we first assume the premise, remain1$(n) \lor \text{remain3}(n)$. Next we assume each of the alternatives in this proposition. When we assume remain1$(n)$, we have $n = 4k + 1 = 2(2k) + 1$ for some $k$, so $n$ is odd. When we assume remain3$(n)$, we have $n = 4k + 3 = 2(2k + 1) + 1$, so again, $n$ is odd. By $\lor$-elimination, we conclude that $\text{odd}(n)$ follows from the premise remain1$(n) \lor \text{remain3}(n)$, and by $\Rightarrow$-introduction, we obtain a proof of our implication.

The $\bot$-elimination rule formalizes the principle that once a false statement has been established, then anything should be provable.

The $\neg$-introduction rule is a proof–by–contradiction principle applied to negated propositions. In order to prove $\neg P$, we assume $P$ and we derive a contradiction ($\bot$). It is a more restrictive principle than the classical proof–by–contradiction rule (RAA). Indeed, if the proposition $P$ to be proven is not a negation ($P$ is not of the form $\neg Q$), then the $\neg$-introduction rule cannot be applied. On the other hand, the classical proof-by-contradiction rule can be applied but we have to assume $\neg P$ as a premise. For further comments on the difference between the $\neg$-introduction rule and the classical proof–by–contradiction rule, see Section 2.7.

The proof–by–contradiction rule formalizes the method of proof by contradiction. That is, in order to prove that $P$ can be deduced from some premises $\Gamma$, one may assume the negation $\neg P$ of $P$ (intuitively, assume that $P$ is false) and then derive a contradiction from $\Gamma$ and $\neg P$ (i.e., derive falsity). Then $P$ actually follows from $\Gamma$ without using $\neg P$ as a premise, that is, $\neg P$ is discharged. For example, let us prove by contradiction that if $n^2$ is odd, then $n$ itself must be odd, where $n$ is a natural number.
According to the proof–by–contradiction rule, let us assume that \( n \) is not odd, which means that \( n \) is even. (Actually, in this step we are using a property of the natural numbers that is proven by induction but let’s not worry about that right now. A proof is given in Section 2.16.) But to say that \( n \) is even means that \( n = 2k \) for some \( k \) and then \( n^2 = 4k^2 = 2(2k^2) \), so \( n^2 \) is even, contradicting the assumption that \( n^2 \) is odd. By the proof–by–contradiction rule, we conclude that \( n \) must be odd.

**Remark:** If the proposition to be proven, \( P \), is of the form \( \neg Q \), then if we use the proof-by-contradiction rule, we have to assume the premise \( \neg
eg Q \) and then derive a contradiction. Because we are using classical logic, we often make implicit use of the fact that \( \neg
eg Q \) is equivalent to \( Q \) (see Proposition 2.2) and instead of assuming \( \neg
eg Q \) as a premise, we assume \( Q \) as a premise. But then, observe that we are really using \( \neg \)-introduction.

In summary, when trying to prove a proposition \( P \) by contradiction, proceed as follows.

1. If \( P \) is a negated formula (\( P \) is of the form \( \neg Q \)), then use the \( \neg \)-introduction rule; that is, assume \( Q \) as a premise and derive a contradiction.

2. If \( P \) is not a negated formula, then use the the proof-by-contradiction rule; that is, assume \( \neg P \) as a premise and derive a contradiction.

Most people, I believe, will be comfortable with the rules of minimal logic and will agree that they constitute a “reasonable” formalization of the rules of reasoning involving \( \Rightarrow \), \( \wedge \), and \( \vee \). Indeed, these rules seem to express the intuitive meaning of the connectives \( \Rightarrow \), \( \wedge \), and \( \vee \). However, some may question the two rules \( \bot \)-elimination and proof-by-contradiction. Indeed, their meaning is not as clear and, certainly, the proof-by-contradiction rule introduces a form of indirect reasoning that is somewhat worrisome.

The problem has to do with the meaning of disjunction and negation and more generally, with the notion of constructivity in mathematics. In fact, in the early 1900s, some mathematicians, especially L. Brouwer (1881–1966), questioned the validity of the proof-by-contradiction rule, among other principles.

Two specific cases illustrate the problem, namely, the propositions

\[ P \lor \neg P \quad \text{and} \quad \neg
eg P \Rightarrow P. \]
As we show shortly, the above propositions are both provable in classical logic; see Proposition 2.1 and Proposition 2.2.

Now Brouwer and some mathematicians belonging to his school of thought (the so-called “intuitionists” or “constructivists”) advocate that in order to prove a disjunction $P \vee Q$ (from some premises $\Gamma$) one has to either exhibit a proof of $P$ or a proof or $Q$ (from $\Gamma$). However, it can be shown that this fails for $P \vee \neg P$. The fact that $P \vee \neg P$ is provable (in classical logic) does not imply (in general) that either $P$ is provable or that $\neg P$ is provable. That $P \vee \neg P$ is provable is sometimes called the principle (or law) of the excluded middle. In intuitionistic logic, $P \vee \neg P$ is not provable (in general). Of course, if one gives up the proof-by-contradiction rule, then fewer propositions become provable. On the other hand, one may claim that the propositions that remain provable have more constructive proofs and thus feel on safer grounds.

A similar controversy arises with the proposition $\neg \neg P \Rightarrow P$ (double-negation rule). If we give up the proof-by-contradiction rule, then this formula is no longer provable (i.e., $\neg \neg P$ is no longer equivalent to $P$). Perhaps this relates to the fact that if one says “I don’t have no money,” then this does not mean that this person has money. (Similarly with “I can’t get no satisfaction.”) However, note that one can still prove $P \Rightarrow \neg \neg P$ in minimal logic (try doing it). Even stranger, $\neg \neg \neg P \Rightarrow \neg P$ is provable in intuitionistic (and minimal) logic, so $\neg \neg \neg P$ and $\neg P$ are equivalent intuitionistically.

**Remark:** Suppose we have a deduction

$$
\Gamma, \neg P \\
\mathcal{D} \\
\bot
$$

as in the proof-by-contradiction rule. Then by $\neg$-introduction, we get a deduction of $\neg \neg P$ from $\Gamma$:

$$
\Gamma, \neg P^x \\
\mathcal{D} \\
\bot \\
\neg \neg P \quad x
$$

So, if we knew that $\neg \neg P$ was equivalent to $P$ (actually, if we knew that $\neg \neg P \Rightarrow P$ is provable), then the proof-by-contradiction rule would be justified as a valid rule (it follows from modus ponens). We can view the proof-by-contradiction rule as a sort of act of faith that consists in saying that if we can derive an inconsistency (i.e., chaos) by assuming the falsity of a statement $P$, then $P$ has to hold in the first place. It not so clear that such an act of faith is justified and the intuitionists refuse to take it.

Constructivity in mathematics is a fascinating subject but it is a topic that is really outside the scope in this book. What we hope is that our brief and very incomplete discussion of constructivity issues made the reader aware that the rules of logic are not cast in stone and that, in particular, there isn’t only one logic.
2.6. ADDING $\land$, $\lor$, $\bot$; THE PROOF SYSTEMS $\mathcal{N}_C^{\land, \lor, \bot}$ AND $\mathcal{N}_G^{\land, \lor, \bot}$

We feel safe in saying that most mathematicians work with classical logic and only a few of them have reservations about using the proof-by-contradiction rule. Nevertheless, intuitionistic logic has its advantages, especially when it comes to proving the correctness of programs (a branch of computer science). We come back to this point several times in this book.

In the rest of this section we make further useful remarks about (classical) logic and give some explicit examples of proofs illustrating the inference rules of classical logic. We begin by proving that $P \lor \neg P$ is provable in classical logic.

**Proposition 2.1.** The proposition $P \lor \neg P$ is provable in classical logic.

**Proof.** We prove that $P \lor (P \Rightarrow \bot)$ is provable by using the proof-by-contradiction rule as shown below:

\[
\frac{\left((P \lor (P \Rightarrow \bot)) \Rightarrow \bot\right)^y}{P \lor (P \Rightarrow \bot)} \quad \lor\text{-intro}
\]

\[
\frac{\bot}{P \Rightarrow \bot} \quad x \quad \land\text{-intro}
\]

\[
\frac{P \lor (P \Rightarrow \bot) \quad \lor\text{-intro}}{\bot} \quad y \quad \text{(by-contra)}
\]

Next, we consider the equivalence of $P$ and $\neg\neg P$.

**Proposition 2.2.** The proposition $P \Rightarrow \neg\neg P$ is provable in minimal logic. The proposition $\neg\neg P \Rightarrow P$ is provable in classical logic. Therefore, in classical logic, $P$ is equivalent to $\neg\neg P$.

**Proof.** We leave that $P \Rightarrow \neg\neg P$ is provable in minimal logic as an exercise. Below is a proof of $\neg\neg P \Rightarrow P$ using the proof-by-contradiction rule:

\[
\frac{\left((P \Rightarrow \bot) \Rightarrow \bot\right)^y}{P \Rightarrow \bot} \quad (\Rightarrow\text{-intro})
\]

\[
\frac{\bot}{P} \quad (\land\text{-intro)}
\]

\[
\frac{\left((P \Rightarrow \bot) \Rightarrow \bot\right)}{P \lor (P \Rightarrow \bot)} \quad \lor\text{-intro}
\]

\[
\frac{\bot}{P \lor (P \Rightarrow \bot)} \quad y \quad \text{(by-contra)}
\]

The next proposition shows why $\bot$ can be viewed as the “ultimate” contradiction.

**Proposition 2.3.** In intuitionistic logic, the propositions $\bot$ and $P \land \neg P$ are equivalent for all $P$. Thus, $\bot$ and $P \land \neg P$ are also equivalent in classical propositional logic.
Proof. We need to show that both $\bot \Rightarrow (P \land \neg P)$ and $(P \land \neg P) \Rightarrow \bot$ are provable in intuitionistic logic. The provability of $\bot \Rightarrow (P \land \neg P)$ is an immediate consequence of $\bot$-elimination, with $\Gamma = \emptyset$. For $(P \land \neg P) \Rightarrow \bot$, we have the following proof.

$$
\begin{array}{c}
(P \land \neg P) \\Gamma
\end{array}
\begin{array}{c}
\neg P \\
\bot
\end{array}
\begin{array}{c}
P \\
(P \land \neg P) \Rightarrow \bot
\end{array}
$$

So, in intuitionistic logic (and also in classical logic), $\bot$ is equivalent to $P \land \neg P$ for all $P$. This means that $\bot$ is the “ultimate” contradiction; it corresponds to total inconsistency. By the way, we could have had the bad luck that the system $N_{c,\Rightarrow,\land,\lor,\bot}$ (or $N_{l,\Rightarrow,\land,\lor,\bot}$ or even $N_{m,\Rightarrow,\land,\lor,\bot}$) is inconsistent, that is, that $\bot$ is provable. Fortunately, this is not the case, although this is hard to prove. (It is also the case that $P \lor \neg P$ and $\neg \neg P \Rightarrow P$ are not provable in intuitionistic logic, but this too is hard to prove.)

2.7 Clearing Up Differences Among $\neg$-Introduction, $\bot$-Elimination, and RAA

The differences between the rules, $\neg$-introduction, $\bot$-elimination, and the proof-by-contradiction rule (RAA) are often unclear to the uninitiated reader and this tends to cause confusion. In this section we try to clear up some common misconceptions about these rules.

Confusion 1. Why is RAA not a special case of $\neg$-introduction?

$$(\Gamma, P^x) \quad (\Gamma, \neg P^x)$$

$$(\neg \text{-intro}) \quad (\bot) \quad (P \lor \neg P) \Rightarrow (\neg \text{-intro})$$

The only apparent difference between $\neg$-introduction (on the left) and RAA (on the right) is that in RAA, the premise $P$ is negated but the conclusion is not, whereas in $\neg$-introduction the premise $P$ is not negated but the conclusion is.

The important difference is that the conclusion of RAA is not negated. If we had applied $\neg$-introduction instead of RAA on the right, we would have obtained

$$
\begin{array}{c}
\Gamma, \neg P^x \\
\bot
\end{array}
\begin{array}{c}
\neg \neg P
\end{array}
$$

$$(\neg \text{-intro})$$
where the conclusion would have been \( \neg \neg P \) as opposed to \( P \). However, as we already said earlier, \( \neg \neg P \Rightarrow P \) is not provable intuitionistically. Consequently, RAA is not a special case of \( \neg \)-introduction. On the other hand, one may view \( \neg \)-introduction as a “constructive” version of RAA applying to negated propositions (propositions of the form \( \neg P \)).

**Confusion 2.** Is there any difference between \( \bot \)-elimination and RAA?

\[
\begin{array}{c}
\Gamma \\
\mathcal{D} \\
\bot \quad (\bot\text{-elim}) \\
P
\end{array}
\quad
\begin{array}{c}
\Gamma, \neg P \\
\mathcal{D} \\
\bot \quad \text{(RAA)} \\
P
\end{array}
\]

The difference is that \( \bot \)-elimination does not discharge any of its premises. In fact, RAA is a stronger rule that implies \( \bot \)-elimination as we now demonstrate.

**RAA implies \( \bot \)-Elimination**

Suppose we have a deduction

\[
\begin{array}{c}
\Gamma \\
\mathcal{D} \\
\bot
\end{array}
\]

Then, for any proposition \( P \), we can add the premise \( \neg P \) to every leaf of the above deduction tree and we get the deduction tree

\[
\begin{array}{c}
\Gamma, \neg P \\
\mathcal{D}' \\
\bot
\end{array}
\]

We can now apply RAA to get the following deduction tree of \( P \) from \( \Gamma \) (because \( \neg P \) is discharged), and this is just the result of \( \bot \)-elimination:

\[
\begin{array}{c}
\Gamma, \neg P \\
\mathcal{D}' \\
\bot \\
P \quad \text{x (RAA)}
\end{array}
\]

The above considerations also show that RAA is obtained from \( \neg \)-introduction by adding the new rule of \( \neg \neg \)-elimination (also called double-negation elimination):

\[
\begin{array}{c}
\Gamma \\
\mathcal{D} \\
\neg \neg P \quad (\neg \neg\text{-elimination}) \\
P
\end{array}
\]

Some authors prefer adding the \( \neg \neg \)-elimination rule to intuitionistic logic instead of RAA in order to obtain classical logic. As we just demonstrated, the two additions are equivalent: by adding either RAA or \( \neg \neg \)-elimination to intuitionistic logic, we get classical logic.
There is another way to obtain RAA from the rules of intuitionistic logic, this time, using the propositions of the form \( P \lor \neg P \). We saw in Proposition 2.1 that all formulae of the form \( P \lor \neg P \) are provable in classical logic (using RAA).

**Confusion 3.** Are propositions of the form \( P \lor \neg P \) provable in intuitionistic logic?

The answer is no, which may be disturbing to some readers. In fact, it is quite difficult to prove that propositions of the form \( P \lor \neg P \) are not provable in intuitionistic logic. One method consists in using the fact that intuitionistic proofs can be normalized (see Section 2.12 for more on normalization of proofs). Another method uses Kripke models (see Section 2.11 and van Dalen [24]).

Part of the difficulty in understanding at some intuitive level why propositions of the form \( P \lor \neg P \) are not provable in intuitionistic logic is that the notion of truth based on the truth values true and false is deeply rooted in all of us. In this frame of mind, it seems ridiculous to question the provability of \( P \lor \neg P \), because its truth value is true whether \( P \) is assigned the value true or false. Classical two-valued truth value semantics is too crude for intuitionistic logic.

Another difficulty is that it is tempting to equate the notion of truth and the notion of provability. Unfortunately, because classical truth values semantics is too crude for intuitionistic logic, there are propositions that are universally true (i.e., they evaluate to true for all possible truth assignments of the atomic letters in them) and yet they are not provable intuitionistically. The propositions \( P \lor \neg P \) and \( \neg \neg P \Rightarrow P \) are such examples.

One of the major motivations for advocating intuitionistic logic is that it yields proofs that are more constructive than classical proofs. For example, in classical logic, when we prove a disjunction \( P \lor Q \), we generally can’t conclude that either \( P \) or \( Q \) is provable, as exemplified by \( P \lor \neg P \). A more interesting example involving a nonconstructive proof of a disjunction is given in Section 2.8. But in intuitionistic logic, from a proof of \( P \lor Q \), it is possible to extract either a proof of \( P \) or a proof of \( Q \) (and similarly for existential statements; see Section 2.15). This property is not easy to prove. It is a consequence of the normal form for intuitionistic proofs (see Section 2.12).

In brief, besides being a fun intellectual game, intuitionistic logic is only an interesting alternative to classical logic if we care about the constructive nature of our proofs. But then we are forced to abandon the classical two-valued truth values semantics and adopt other semantics such as Kripke semantics. If we do not care about the constructive nature of our proofs and if we want to stick to two-valued truth values semantics, then we should stick to classical logic. Most people do that, so don’t feel bad if you are not comfortable with intuitionistic logic.

One way to gauge how intuitionistic logic differs from classical logic is to ask what kind of propositions need to be added to intuitionistic logic in order to get classical logic. It turns out that if all the propositions of the form \( P \lor \neg P \) are considered to be axioms, then RAA follows from some of the rules of intuitionistic logic.

**RAA Holds in Intuitionistic Logic + All Axioms** \( P \lor \neg P \).

The proof involves a subtle use of the \( \bot \)-elimination and \( \lor \)-elimination rules which may be a bit puzzling. Assume, as we do when we use the proof-by-contradiction rule (RAA) that
we have a deduction

\[ \Gamma, \neg P \]

\[ \mathcal{D} \]

\[ \bot \]

Here is the deduction tree demonstrating that RAA is a derived rule:

\[
\begin{array}{c}
\Gamma, \neg P^y \\
\mathcal{D} \\
\bot \\
P^{x} \\
P \\
P_{x,y} \quad (\bot\text{-elim}) \\
P \\
P_{x,y} \quad (\lor\text{-elim})
\end{array}
\]

At first glance, the rightmost subtree

\[
\Gamma, \neg P^y \\
\mathcal{D} \\
\bot \\
P \\
(P^{x} \\
P \\
P_{x,y} \quad (\bot\text{-elim})
\]

appears to use RAA and our argument looks circular. But this is not so because the premise \( \neg P \) labeled \( y \) is \textit{not} discharged in the step that yields \( P \) as conclusion; the step that yields \( P \) is a \( \bot \)-elimination step. The premise \( \neg P \) labeled \( y \) is actually discharged by the \( \lor \)-elimination rule (and so is the premise \( P \) labeled \( x \)). So our argument establishing RAA is not circular after all.

In conclusion, intuitionistic logic is obtained from classical logic by \textit{taking away the proof-by-contradiction rule (RAA)}. In this more restrictive proof system, we obtain more constructive proofs. In that sense, the situation is better than in classical logic. The major drawback is that we can’t think in terms of classical truth values semantics anymore.

Conversely, classical logic is obtained from intuitionistic logic in at least three ways:

1. Add the proof-by-contradiction rule (RAA).
2. Add the \( \neg \neg \)-elimination rule.
3. Add all propositions of the form \( P \lor \neg P \) as axioms.

### 2.8 De Morgan Laws and Other Rules of Classical Logic

In Section 1.7 we discussed the de Morgan laws. Now that we also know about intuitionistic logic we revisit these laws.
Proposition 2.4. The following equivalences (de Morgan laws) are provable in classical logic.

\[ \neg(P \land Q) \equiv \neg P \lor \neg Q \]
\[ \neg(P \lor Q) \equiv \neg P \land \neg Q. \]

In fact, \( \neg(P \lor Q) \equiv \neg P \land \neg Q \) and \( \neg(P \land \neg Q) \Rightarrow \neg(P \land Q) \) are provable in intuitionistic logic. The proposition \( (P \land \neg Q) \Rightarrow (P \Rightarrow Q) \) is provable in intuitionistic logic and \( \neg(P \Rightarrow Q) \Rightarrow (P \land \neg Q) \) is provable in classical logic. Therefore, \( \neg(P \Rightarrow Q) \) and \( P \land \neg Q \) are equivalent in classical logic. Furthermore, \( P \Rightarrow Q \) and \( \neg P \lor Q \) are equivalent in classical logic and \( \neg(P \lor Q) \Rightarrow (P \Rightarrow Q) \) is provable in intuitionistic logic.

Proof. We only prove the very last part of Proposition 2.4 leaving the other parts as a series of exercises. Here is an intuitionistic proof of \( (\neg P \lor Q) \Rightarrow (P \Rightarrow Q) \):

```
(\neg P \lor Q)^w
  \hline
  P \Rightarrow Q
  Q \Downarrow x
  P \Rightarrow Q
  \hline
  (\neg P \lor Q) \Rightarrow (P \Rightarrow Q)
```

Here is a classical proof of \( (P \Rightarrow Q) \Rightarrow (\neg P \lor Q) \):

```
(P \Rightarrow Q)^z
  \hline
  \neg P \lor Q
  Q \Downarrow x
  \ hline
  \neg(P \lor Q)^y
  \hline
  Q \Downarrow y
  \hline
  \neg P \lor Q \Rightarrow (P \Rightarrow Q)
```

The other proofs are left as exercises. \[ \square \]

Propositions 2.2 and 2.4 show a property that is very specific to classical logic, namely, that the logical connectives \( \Rightarrow, \land, \lor, \neg \) are not independent. For example, we have \( P \land Q \equiv \neg(\neg P \lor \neg Q) \), which shows that \( \land \) can be expressed in terms of \( \lor \) and \( \neg \). In intuitionistic logic, \( \land \) and \( \lor \) cannot be expressed in terms of each other via negation.
2.8. DE MORGAN LAWS AND OTHER RULES OF CLASSICAL LOGIC

The fact that the logical connectives $\Rightarrow, \land, \lor, \neg$ are not independent in classical logic suggests the following question. Are there propositions, written in terms of $\Rightarrow$ only, that are provable classically but not provable intuitionistically?

The answer is yes. For instance, the proposition $((P \Rightarrow Q) \Rightarrow P) \Rightarrow P$ (known as Peirce’s law) is provable classically (do it) but it can be shown that it is not provable intuitionistically.

In addition to the proof-by-cases method and the proof-by-contradiction method, we also have the proof-by-contrapositive method valid in classical logic:

**Proof-by-contrapositive rule:**

$$
\begin{array}{c}
\Gamma, \neg Q^x \\
\vdash \\
D \\
\neg P \\
\hline
P \Rightarrow Q \\
x
\end{array}
$$

This rule says that in order to prove an implication $P \Rightarrow Q$ (from $\Gamma$), one may assume $\neg Q$ as proven, and then deduce that $\neg P$ is provable from $\Gamma$ and $\neg Q$. This inference rule is valid in classical logic because we can construct the following deduction.

$$
\begin{array}{c}
\Gamma, \neg Q^x \\
\vdash \\
D \\
\neg P \\
\hline
P \Rightarrow Q \\
x \text{ (by-contra)}
\end{array}
$$

As as example of the proof-by-contrapositive method, we prove that if an integer $n^2$ is even, then $n$ must be even.

Observe that if an integer is not even, then it is odd (and vice versa). This fact may seem quite obvious but to prove it actually requires using induction (which we haven’t officially met yet). A rigorous proof is given in Section 2.16.

Now the contrapositive of our statement is: if $n$ is odd, then $n^2$ is odd. But to say that $n$ is odd is to say that $n = 2k + 1$ and then, $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$, which shows that $n^2$ is odd.

As it is, because the above proof uses the proof-by-contrapositive method, it is not constructive. Thus, the question arises, is there a constructive proof of the above fact?

Indeed there is a constructive proof if we observe that every integer $n$ is either even or odd but not both. Now, one might object that we just relied on the law of the excluded middle but there is a way to circumvent this problem by using induction; see Section 2.16 for a rigorous proof.

Now, because an integer is odd iff it is not even, we may proceed to prove that if $n^2$ is even, then $n$ is not odd, by using our constructive version of the proof-by-contradiction principle, namely, $\neg$-introduction.
Therefore, assume that \( n^2 \) is even and that \( n \) is odd. Then \( n = 2k + 1 \), which implies that \( n^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1 \), an odd number, contradicting the fact that \( n^2 \) is assumed to be even.

The next proposition collects a list of equivalences involving conjunction and disjunction that are used all the time. Proofs of these propositions are left as exercises (see the problems).

**Proposition 2.5.** All the propositions below are provable intuitionistically:

\[
\begin{align*}
P \lor P & \equiv P \\
P \land P & \equiv P \\
P \lor Q & \equiv Q \lor P \\
P \land Q & \equiv Q \land P.
\end{align*}
\]

The last two assert the commutativity of \( \lor \) and \( \land \). We have distributivity of \( \land \) over \( \lor \) and of \( \lor \) over \( \land \):

\[
\begin{align*}
P \land (Q \lor R) & \equiv (P \land Q) \lor (P \land R) \\
P \lor (Q \land R) & \equiv (P \lor Q) \land (P \lor R).
\end{align*}
\]

We have associativity of \( \land \) and \( \lor \):

\[
\begin{align*}
P \land (Q \land R) & \equiv (P \land Q) \land R \\
P \lor (Q \lor R) & \equiv (P \lor Q) \lor R.
\end{align*}
\]

## 2.9 Formal Versus Informal Proofs

As we said before, it is practically impossible to write formal proofs (i.e., proofs written as proof trees using the rules of one of the systems presented earlier) of “real” statements that are not “toy propositions.” This is because it would be extremely tedious and time-consuming to write such proofs and these proofs would be huge and thus very hard to read.

What we do instead is to construct “informal” proofs in which we still make use of the logical rules that we have presented but we take shortcuts and sometimes we even omit proof steps (some elimination rules, such as \( \land \)-elimination and some introduction rules, such as \( \lor \)-introduction) and we use a natural language (here, presumably, English) rather than formal symbols (we say “and” for \( \land \), “or” for \( \lor \), etc.). We refer the reader to Section 1.8 for a discussion of these issues. We also urge our readers to read Chapter 3 of Gowers [11] which contains very illuminating remarks about the notion of proof in mathematics.

Here is a concrete example illustrating the usefulness of auxiliary lemmas in constructing informal proofs.

Say we wish to prove the implication

\[
\neg (P \land Q) \Rightarrow ((\neg P \land \neg Q) \lor (\neg P \land Q) \lor (P \land \neg Q)).
\]

\[(*)\]
It can be shown that the above proposition is not provable intuitionistically, so we have to use the proof-by-contradiction method in our proof. One quickly realizes that any proof ends up re-proving basic properties of $\land$ and $\lor$, such as associativity, commutativity, distributivity, and so on, some of the de Morgan laws, and that the complete proof is very large. However, if we allow ourselves to use the de Morgan laws as well as various basic properties of $\land$ and $\lor$, such as distributivity,

$$(A \land B) \lor C \equiv (A \land C) \lor (B \land C),$$

commutativity of $\land$ and $\lor$ $(A \land B \equiv B \land A, A \lor B \equiv B \lor A)$, associativity of $\land$ and $\lor$ $(A \land (B \land C) \equiv (A \land B) \land C, A \lor (B \lor C) \equiv (A \lor B) \lor C)$, and the idempotence of $\land$ and $\lor$ $(A \land A \equiv A, A \lor A \equiv A)$, then we get

$$\neg P \land \neg Q \lor (\neg P \land Q) \lor (P \land \neg Q) \equiv \neg P \land (\neg P \lor Q) \lor (P \land \neg Q)$$

$$\equiv \neg P \land \neg Q \lor (\neg P \land Q) \lor (P \land \neg Q)$$

$$\equiv \neg P \lor (\neg P \land Q) \lor (P \land \neg Q)$$

$$\equiv \neg P \lor (\neg P \land Q) \lor (P \land \neg Q)$$

where we make implicit uses of commutativity and associativity, and the fact that $R \land (P \lor \neg P) \equiv R$, and by de Morgan,

$$\neg (P \land Q) \equiv \neg P \lor \neg Q,$$

using auxiliary lemmas, we end up proving (*) without too much pain.

## 2.10 Truth Value Semantics for Classical Logic

### Soundness and Completeness

In Section 1.9 we introduced the truth value semantics for classical propositional logic. The logical connectives $\Rightarrow$, $\land$, $\lor$, $\neg$ and $\equiv$ can be interpreted as Boolean functions, that is, functions whose arguments and whose values range over the set of truth values,

$$BOOL = \{true, false\}.$$ 

These functions are given by the following truth tables.

<table>
<thead>
<tr>
<th>$P$</th>
<th>$Q$</th>
<th>$P \Rightarrow Q$</th>
<th>$P \land Q$</th>
<th>$P \lor Q$</th>
<th>$\neg P$</th>
<th>$P \equiv Q$</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>true</td>
<td>false</td>
<td>false</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>true</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>
Now, any proposition $P$ built up over the set of atomic propositions $PS$ (our propositional symbols) contains a finite set of propositional letters, say

$$\{P_1, \ldots, P_m\}.$$  

If we assign some truth value (from $BOOL$) to each symbol $P_i$ then we can “compute” the truth value of $P$ under this assignment by using recursively using the truth tables above.

For example, the proposition $P_1 \Rightarrow (P_1 \Rightarrow P_2)$, under the truth assignment $v$ given by $P_1 = \text{true}$, $P_2 = \text{false}$, evaluates to $\text{false}$; see Section 1.9.

The values of a proposition can be determined by creating a truth table, in which a proposition is evaluated by computing recursively the truth values of its subexpressions. See Section 1.9.

The truth table of a proposition containing $m$ variables has $2^m$ rows. When $m$ is large, $2^m$ is very large, and computing the truth table of a proposition $P$ may not be practically feasible. Even the problem of finding whether there is a truth assignment that makes $P$ true is hard.

**Definition 2.6.** We say that a proposition $P$ is *satisfiable* iff it evaluates to $\text{true}$ for some truth assignment (taking values in $BOOL$) of the propositional symbols occurring in $P$ and otherwise we say that it is *unsatisfiable*. A proposition $P$ is *valid* (or a *tautology*) iff it evaluates to $\text{true}$ for all truth assignments of the propositional symbols occurring in $P$.

Observe that a proposition $P$ is valid if in the truth table for $P$ all the entries in the column corresponding to $P$ have the value $\text{true}$. The proposition $P$ is satisfiable if some entry in the column corresponding to $P$ has the value $\text{true}$.

The problem of deciding whether a proposition is satisfiable is called the *satisfiability problem* and is sometimes denoted by SAT. The problem of deciding whether a proposition is valid is called the *validity problem*.

For example, the proposition

$$P = (P_1 \lor \neg P_2 \lor \neg P_3) \land (\neg P_1 \lor \neg P_3) \land (P_1 \lor P_2 \lor P_4) \land (\neg P_3 \lor P_4) \land (\neg P_1 \lor P_4)$$

is satisfiable because it evaluates to $\text{true}$ under the truth assignment $P_1 = \text{true}$, $P_2 = \text{false}$, $P_3 = \text{false}$, and $P_4 = \text{true}$. On the other hand, the proposition

$$Q = (P_1 \lor P_2 \lor P_3) \land (\neg P_1 \lor P_2) \land (\neg P_2 \lor P_3) \land (P_1 \lor \neg P_3) \land (\neg P_1 \lor \neg P_2 \lor \neg P_3)$$

is unsatisfiable as one can verify by trying all eight truth assignments for $P_1, P_2, P_3$. The reader should also verify that the proposition

$$R = (\neg P_1 \land \neg P_2 \land \neg P_3) \lor (P_1 \land \neg P_2) \lor (P_2 \land \neg P_3) \lor (\neg P_1 \land P_3) \lor (P_1 \land P_2 \land P_3)$$
is valid (observe that the proposition $R$ is the negation of the proposition $Q$).

The satisfiability problem is a famous problem in computer science because of its complexity. Try it: solving it is not as easy as you think. The difficulty is that if a proposition $P$ contains $n$ distinct propositional letters, then there are $2^n$ possible truth assignments and checking all of them is practically impossible when $n$ is large.

In fact, the satisfiability problem turns out to be an $NP$-complete problem, a very important concept that you will learn about in a course on the theory of computation and complexity. Very good expositions of this kind of material are found in Hopcroft, Motwani, and Ullman [13] and Lewis and Papadimitriou [17]. The validity problem is also important and it is related to SAT. Indeed, it is easy to see that a proposition $P$ is valid iff $\neg P$ is unsatisfiable.

What's the relationship between validity and provability in the system $\mathcal{N}_c \Rightarrow, \land, \lor, \bot$?

Remarkably, in classical logic, validity and provability are equivalent.

In order to prove the above claim, we need to do two things:

1. Prove that if a proposition $P$ is provable in the system $\mathcal{N}_c \Rightarrow, \land, \lor, \bot$ (or the system $\mathcal{NG}_c \Rightarrow, \land, \lor, \bot$), then it is valid. This is known as soundness or consistency (of the proof system).

2. Prove that if a proposition $P$ is valid, then it has a proof in the system $\mathcal{N}_c \Rightarrow, \land, \lor, \bot$ (or $\mathcal{NG}_c \Rightarrow, \land, \lor, \bot$). This is known as the completeness (of the proof system).

In general, it is relatively easy to prove (1) but proving (2) can be quite complicated. In fact, some proof systems are not complete with respect to certain semantics. For instance, the proof system for intuitionistic logic $\mathcal{N}_i \Rightarrow, \land, \lor, \bot$ (or $\mathcal{NG}_i \Rightarrow, \land, \lor, \bot$) is not complete with respect to truth value semantics. As an example, ((($P \Rightarrow Q$) $\Rightarrow P$) $\Rightarrow P$) (known as Peirce’s law), is valid but it can be shown that it cannot be proven in intuitionistic logic.

In this book we content ourselves with soundness.

**Proposition 2.6.** (Soundness of $\mathcal{N}_c \Rightarrow, \land, \lor, \bot$ and $\mathcal{NG}_c \Rightarrow, \land, \lor, \bot$) If a proposition $P$ is provable in the system $\mathcal{N}_c \Rightarrow, \land, \lor, \bot$ (or $\mathcal{NG}_c \Rightarrow, \land, \lor, \bot$), then it is valid (according to the truth value semantics).

**Sketch of Proof.** It is enough to prove that if there is a deduction of a proposition $P$ from a set of premises $\Gamma$ then for every truth assignment for which all the propositions in $\Gamma$ evaluate to true, then $P$ evaluates to true. However, this is clear for the axioms and every inference rule preserves that property.

Now if $P$ is provable, a proof of $P$ has an empty set of premises and so $P$ evaluates to true for all truth assignments, which means that $P$ is valid. \qed

**Theorem 2.7.** (Completeness of $\mathcal{N}_c \Rightarrow, \land, \lor, \bot$ and $\mathcal{NG}_c \Rightarrow, \land, \lor, \bot$) If a proposition $P$ is valid (according to the truth value semantics), then $P$ is provable in the system $\mathcal{N}_c \Rightarrow, \land, \lor, \bot$ (or $\mathcal{NG}_c \Rightarrow, \land, \lor, \bot$).
Proofs of completeness for classical logic can be found in van Dalen [24] or Gallier [4] (but for a different proof system).

Soundness (Proposition 2.6) has a very useful consequence: in order to prove that a proposition \( P \) is not provable, it is enough to find a truth assignment for which \( P \) evaluates to false. We say that such a truth assignment is a counterexample for \( P \) (or that \( P \) can be falsified). For example, no propositional symbol \( P_i \) is provable because it is falsified by the truth assignment \( P_i = \text{false} \).

The soundness of the proof system \( \mathcal{N}_{\Rightarrow, \land, \lor, \bot} \) also has the extremely important consequence that \( \bot \) cannot be proven in this system, which means that contradictory statements cannot be derived.

This is by no means obvious at first sight, but reassuring. It is also possible to prove that the proof system \( \mathcal{N}_{\Rightarrow, \land, \lor, \bot} \) is consistent (i.e., \( \bot \) cannot be proven) by purely proof-theoretic means involving proof normalization (See Section 2.12), but this requires a lot more work.

Note that completeness amounts to the fact that every unprovable formula has a counterexample. Also, in order to show that a proposition is classically provable, it suffices to compute its truth table and check that the proposition is valid. This may still be a lot of work, but it is a more “mechanical” process than attempting to find a proof.

For example, here is a truth table showing that \( (P_1 \Rightarrow P_2) \equiv (\neg P_1 \lor P_2) \) is valid.

<table>
<thead>
<tr>
<th>( P_1 )</th>
<th>( P_2 )</th>
<th>( P_1 \Rightarrow P_2 )</th>
<th>( \neg P_1 \lor P_2 )</th>
<th>( (P_1 \Rightarrow P_2) \equiv (\neg P_1 \lor P_2) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>true</td>
<td>false</td>
<td>false</td>
<td>false</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
<tr>
<td>false</td>
<td>false</td>
<td>true</td>
<td>true</td>
<td>true</td>
</tr>
</tbody>
</table>

Remark: Truth value semantics is not the right kind of semantics for intuitionistic logic; it is too coarse. A more subtle kind of semantics is required. Among the various semantics for intuitionistic logic, one of the most natural is the notion of the Kripke model. Then again, soundness and completeness hold for intuitionistic proof systems (see Section 2.11 and van Dalen [24]).

2.11 Kripke Models for Intuitionistic Logic
Soundness and Completeness

In this section, we briefly describe the semantics of intuitionistic propositional logic in terms of Kripke models.

This section has been included to quench the thirst of those readers who can’t wait to see what kind of decent semantics can be given for intuitionistic propositional logic and it can be safely omitted.

In classical truth value semantics based on \( \text{BOOL} = \{\text{true}, \text{false}\} \), we might say that truth is absolute. The idea of Kripke semantics is that there is a set of worlds (or states)
$W$ together with a partial ordering $\leq$ on $W$, and that truth depends on in which world we are. Furthermore, as we “go up” from a world $u$ to a world $v$ with $u \leq v$, truth “can only increase,” that is, whatever is true in world $u$ remains true in world $v$. Also, the truth of some propositions, such as $P \Rightarrow Q$ or $\neg P$, depends on “future worlds.” With this type of semantics, which is no longer absolute, we can capture exactly the essence of intuitionistic logic. We now make these ideas precise.

![Image](270x526 to 342x616)

Figure 2.3: Saul Kripke, 1940–

**Definition 2.7.** A *Kripke model* for intuitionistic propositional logic is a pair $K = (W, \varphi)$ where $W$ is a partially ordered (nonempty) set called a set of worlds and $\varphi$ is a function $\varphi: W \rightarrow \text{BOOL}^{PS}$ such that for every $u \in W$, the function $\varphi(u): PS \rightarrow \text{BOOL}$ is an assignment of truth values to the propositional symbols in $PS$ satisfying the following property. For all $u, v \in W$, for all $P_i \in PS$,

$$
\text{if } u \leq v \text{ and } \varphi(u)(P_i) = \text{true}, \text{ then } \varphi(v)(P_i) = \text{true}.
$$

As we said in our informal comments, truth can’t decrease when we move from a world $u$ to a world $v$ with $u \leq v$ but truth can increase; it is possible that $\varphi(u)(P_i) = \text{false}$ and yet, $\varphi(v)(P_i) = \text{true}$.

If $W = \{0, 1\}$ ordered so that $0 \leq 1$ and if $\varphi$ is given by

$$
\varphi(0)(P_i) = \text{false} \\
\varphi(1)(P_i) = \text{true},
$$

then $K_{\text{bad}} = (W, \varphi)$ is a Kripke structure.

We use Kripke models to define the semantics of propositions as follows.

**Definition 2.8.** Given a Kripke model $K = (W, \varphi)$, for every $u \in W$ and for every proposition $P$ we say that $P$ is satisfied by $K$ at $u$ and we write $\varphi(u)(P) = \text{true}$ iff

(a) If $P = P_i \in PS$, then $\varphi(u)(P_i) = \text{true}$.

(b) If $P = Q \land R$, then $\varphi(u)(Q) = \text{true}$ and $\varphi(u)(R) = \text{true}$.

(c) If $P = Q \lor R$, then $\varphi(u)(Q) = \text{true}$ or $\varphi(u)(R) = \text{true}$.
(d) If $P = Q \Rightarrow R$, then for all $v$ such that $u \leq v$, if $\varphi(v)(Q) = \textbf{true}$, then $\varphi(v)(R) = \textbf{true}$.

(e) If $P = \neg Q$, then for all $v$ such that $u \leq v$, $\varphi(v)(Q) = \textbf{false}$,

(f) $\varphi(u)(\bot) = \textbf{false}$; that is, $\bot$ is not satisfied by $\mathcal{K}$ at $u$ (for any $\mathcal{K}$ and any $u$).

We say that $P$ is valid in $\mathcal{K}$ (or that $\mathcal{K}$ is a model of $P$) iff $P$ is satisfied by $\mathcal{K} = (W, \varphi)$ at $u$ for all $u \in W$ and we say that $P$ is intuitionistically valid iff $P$ is valid in every Kripke model $\mathcal{K}$.

When $P$ is satisfied by $\mathcal{K}$ at $u$ we also say that $P$ is true at $u$ in $\mathcal{K}$. Note that the truth at $u \in W$ of a proposition of the form $Q \Rightarrow R$ or $\neg Q$ depends on the truth of $Q$ and $R$ at all “future worlds,” $v \in W$, with $u \leq v$. Observe that classical truth value semantics corresponds to the special case where $W$ consists of a single element (a single world).

Given the Kripke structure $\mathcal{K}_{bad}$ defined earlier, the reader should check that the proposition $P = (P_i \lor \neg P_i)$ has the value false at 0 because $\varphi(0)(P_i) = \textbf{false}$, but $\varphi(1)(P_i) = \textbf{true}$, so clause (e) fails for $\neg P_i$ at $u = 0$. Therefore, $P = (P_i \lor \neg P_i)$ is not valid in $\mathcal{K}_{bad}$ and thus, it is not intuitionistically valid. We escaped the classical truth value semantics by using a universe with two worlds. The reader should also check that

$$\varphi(u)(\neg \neg P) = \textbf{true} \text{ iff } \text{ for all } v \text{ such that } u \leq v$$
$$\text{there is some } w \text{ with } v \leq w \text{ so that } \varphi(w)(P) = \textbf{true}.\$$

This shows that in Kripke semantics, $\neg \neg P$ is weaker than $P$, in the sense that $\varphi(u)(\neg \neg P) = \textbf{true}$ does not necessarily imply that $\varphi(u)(P) = \textbf{true}$. The reader should also check that the proposition $\neg P_i \Rightarrow P_i$ is not valid in the Kripke structure $\mathcal{K}_{bad}$.

As we said in the previous section, Kripke semantics is a perfect fit to intuitionistic provability in the sense that soundness and completeness hold.

**Proposition 2.8. (Soundness of $\mathcal{N}^{\Rightarrow, \land, \lor, \bot}_{i}$ and $\mathcal{N}G^{\Rightarrow, \land, \lor, \bot}_{i}$)** If a proposition $P$ is provable in the system $\mathcal{N}^{\Rightarrow, \land, \lor, \bot}_{i}$ (or $\mathcal{N}G^{\Rightarrow, \land, \lor, \bot}_{i}$), then it is valid in every Kripke model, that is, it is intuitionistically valid.

Proposition 2.8 is not hard to prove. We consider any deduction of a proposition $P$ from a set of premises $\Gamma$ and we prove that for every Kripke model $\mathcal{K} = (W, \varphi)$, for every $u \in W$, if every premise in $\Gamma$ is satisfied by $\mathcal{K}$ at $u$, then $P$ is also satisfied by $\mathcal{K}$ at $u$. This is obvious for the axioms and it is easy to see that the inference rules preserve this property.

Completeness also holds, but it is harder to prove (see van Dalen [24]).

**Theorem 2.9. (Completeness of $\mathcal{N}^{\Rightarrow, \land, \lor, \bot}_{i}$ and $\mathcal{N}G^{\Rightarrow, \land, \lor, \bot}_{i}$)** If a proposition $P$ is intuitionistically valid, then $P$ is provable in the system $\mathcal{N}^{\Rightarrow, \land, \lor, \bot}_{i}$ (or $\mathcal{N}G^{\Rightarrow, \land, \lor, \bot}_{i}$).

Another proof of completeness for a different proof system for propositional intuitionistic logic (a Gentzen-sequent calculus equivalent to $\mathcal{N}G^{\Rightarrow, \land, \lor, \bot}_{i}$) is given in Takeuti [22]. We find this proof more instructive than van Dalen’s proof. This proof also shows that if a
If proposition $P$ is not intuitionistically provable, then there is a Kripke model $K$ where $W$ is a finite tree in which $P$ is not valid. Such a Kripke model is called a counterexample for $P$.

Several times in this chapter, we have claimed that certain formulae are not provable in some logical system. What kind of reasoning do we use to validate such claims? In the next section, we briefly address this question as well as related ones.

### 2.12 Decision Procedures, Proof Normalization

In the previous sections we saw how the rules of mathematical reasoning can be formalized in various natural deduction systems and we defined a precise notion of proof. We observed that finding a proof for a given proposition was not a simple matter, nor was it to ascertain that a proposition is unprovable. Thus, it is natural to ask the following question.

**The Decision Problem**: Is there a general procedure that takes any arbitrary proposition $P$ as input, always terminates in a finite number of steps, and tells us whether $P$ is provable?

Clearly, it would be very nice if such a procedure existed, especially if it also produced a proof of $P$ when $P$ is provable.

Unfortunately, for rich enough languages, such as first-order logic (discussed in Section 2.15) it is impossible to find such a procedure. This deep result known as the undecidability of the decision problem or Church’s theorem was proven by A. Church in 1936 (actually, Church proved the undecidability of the validity problem but, by Gödel’s completeness theorem, validity and provability are equivalent).

Proving Church’s theorem is hard and a lot of work. One needs to develop a good deal of what is called the theory of computation. This involves defining models of computation such as Turing machines and proving other deep results such as the undecidability of the halting problem and the undecidability of the Post correspondence problem, among other things; see Hopcroft, Motwani, and Ullman [13] and Lewis and Papadimitriou [17].

So our hopes to find a “universal theorem prover” are crushed. However, if we restrict ourselves to propositional logic, classical or intuitionistic, it turns out that procedures solving the decision problem do exist and they even produce a proof of the input proposition when that proposition is provable.
Unfortunately, proving that such procedures exist, and are correct in the propositional case is rather difficult, especially for intuitionistic logic. The difficulties have a lot to do with our choice of a natural deduction system. Indeed, even for the system $\mathcal{N}_{\Rightarrow m}$ (or $\mathcal{NG}_{\Rightarrow m}$), provable propositions may have infinitely many proofs. This makes the search process impossible; when do we know how to stop, especially if a proposition is not provable. The problem is that proofs may contain redundancies (Gentzen said “detours”). A typical example of redundancy is when an elimination immediately follows an introduction, as in the following example:

\[
\begin{align*}
    y: ((R \Rightarrow R) \Rightarrow Q) & \rightarrow ((R \Rightarrow R) \Rightarrow Q) & x: (R \Rightarrow R) & \rightarrow (R \Rightarrow R) \\
    x: (R \Rightarrow R), y: ((R \Rightarrow R) \Rightarrow Q) & \rightarrow Q \\
    & \rightarrow (R \Rightarrow R) \Rightarrow ((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q \\
    & \rightarrow (R \Rightarrow R) \Rightarrow Q \\
    \quad \quad \quad z: R \rightarrow R & \rightarrow R \Rightarrow R
\end{align*}
\]

The blue deduction already has $((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q$ as conclusion but it is not a proof because the assumption $x: (R \Rightarrow R)$ is present. However we have a proof of $R \Rightarrow R$, namely

\[
\begin{align*}
    z: R \rightarrow R & \rightarrow R \Rightarrow R
\end{align*}
\]

We can obtain a proof of $((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q$ from the blue deduction tree by replacing the leaf labeled $x: (R \Rightarrow R) \rightarrow (R \Rightarrow R)$ by the proof tree for $R \Rightarrow R$, obtaining

\[
\begin{align*}
    y: ((R \Rightarrow R) \Rightarrow Q) & \rightarrow ((R \Rightarrow R) \Rightarrow Q) \\
    x: (R \Rightarrow R), y: ((R \Rightarrow R) \Rightarrow Q) & \rightarrow Q \\
    & \rightarrow (R \Rightarrow R) \Rightarrow ((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q \\
    & \rightarrow (R \Rightarrow R) \Rightarrow Q \\
    \quad \quad \quad z: R \rightarrow R & \rightarrow R \Rightarrow R
\end{align*}
\]

The above is not quite a proof tree, but it becomes one if we delete the premise $x: (R \Rightarrow R)$ which is now redundant:

\[
\begin{align*}
    y: ((R \Rightarrow R) \Rightarrow Q) & \rightarrow ((R \Rightarrow R) \Rightarrow Q) \\
    \quad \quad \quad z: R \rightarrow R & \rightarrow R \Rightarrow R
\end{align*}
\]

\[
\begin{align*}
    y: ((R \Rightarrow R) \Rightarrow Q) & \rightarrow Q \\
    & \rightarrow ((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q
\end{align*}
\]

The procedure that we just described for eliminating a redundancy can be generalized. Consider the deduction tree below in which $D_1$ denotes a deduction with conclusion $\Gamma, x: A \rightarrow B$ and $D_2$ denotes a deduction with conclusion $\Delta \rightarrow A$. 
It should be possible to construct a deduction for $\Gamma \rightarrow B$ from the two deductions $D_1$ and $D_2$ without using at all the hypothesis $x : A$. This is indeed the case. If we look closely at the deduction $D_1$, from the shape of the inference rules, assumptions are never created, and the leaves must be labeled with expressions of the form either

1. $\Gamma, \Lambda, x : A \rightarrow A$, or
2. $\Gamma, \Lambda, x : A, y : C \rightarrow C$ if $\Gamma = \Gamma', y : C$ and $y \neq x$, or
3. $\Gamma, \Lambda, x : A, y : C \rightarrow C$ if $y : C \notin \Gamma$ and $y \neq x$.

We can form a new deduction for $\Gamma \rightarrow B$ as follows. In $D_1$, wherever a leaf of the form $\Gamma, \Lambda, x : A \rightarrow A$ occurs, replace it by the deduction obtained from $D_2$ by adding $\Lambda$ to the premise of each sequent in $D_2$.

In our previous example, we have $A = (R \rightarrow R)$, $B = ((R \rightarrow R) \rightarrow Q)$, $Q$, $C = (R \rightarrow R) \rightarrow Q$, $\Gamma = \Delta = \Lambda = \emptyset$.

Actually, one should be careful to first make a fresh copy of $D_2$ by renaming all the variables so that clashes with variables in $D_1$ are avoided. Finally, delete the assumption $x : A$ from the premise of every sequent in the resulting proof. The resulting deduction is obtained by a kind of substitution and may be denoted as $D_1[D_2/x]$, with some minor abuse of notation. Note that the assumptions $x : A$ occurring in the leaves of type (2) or (3) were never used anyway. The step that consists in transforming the above redundant proof figure into the deduction $D_1[D_2/x]$ is called a reduction step or normalization step.

The idea of proof normalization goes back to Gentzen ([8], 1935). Gentzen noted that (formal) proofs can contain redundancies, or “detours,” and that most complications in the analysis of proofs are due to these redundancies. Thus, Gentzen had the idea that the analysis of proofs would be simplified if it were possible to show that every proof can be converted to an equivalent irredundant proof, a proof in normal form. Gentzen proved a technical result to that effect, the “cut-elimination theorem,” for a sequent-calculus formulation of first-order logic [8]. Cut-free proofs are direct, in the sense that they never use auxiliary lemmas via the cut rule.

Remark: It is important to note that Gentzen’s result gives a particular algorithm to produce a proof in normal form. Thus we know that every proof can be reduced to some normal form using a specific strategy, but there may be more than one normal form, and certain normalization strategies may not terminate.

About 30 years later, Prawitz ([18], 1965) reconsidered the issue of proof normalization, but in the framework of natural deduction rather than the framework of sequent calculi.\(^1\)

\(^1\)This is somewhat ironical, inasmuch as Gentzen began his investigations using a natural deduction system, but decided to switch to sequent calculi (known as Gentzen systems) for technical reasons.
Prawitz explained very clearly what redundancies are in systems of natural deduction, and he proved that every proof can be reduced to a normal form. Furthermore, this normal form is unique. A few years later, Prawitz ([19], 1971) showed that in fact, every reduction sequence terminates, a property also called strong normalization.

A remarkable connection between proof normalization and the notion of computation must also be mentioned. Curry (1958) made the remarkably insightful observation that certain typed combinators can be viewed as representations of proofs (in a Hilbert system) of certain propositions. (See in Curry and Feys [2] (1958), Chapter 9E, pages 312–315.)

Building up on this observation, Howard ([14], 1969) described a general correspondence among propositions and types, proofs in natural deduction and certain typed $\lambda$-terms, and proof normalization and $\beta$-reduction (The simply typed $\lambda$-calculus was invented by Church, 1940). This correspondence, usually referred to as the Curry–Howard isomorphism or formulae-as-types principle, is fundamental and very fruitful.

Let us elaborate on this correspondence.

## 2.13 The Simply-Typed $\lambda$-Calculus

First we need to define the simply-typed $\lambda$-calculus and the first step is to define simple types. We assume that we have a countable set $\{T_0, T_1, \ldots, T_n, \ldots\}$ of base types (or atomic types). For example, the base types may include types such as Nat for the natural numbers, Bool for the booleans, String for strings, Tree for trees, etc. In the Curry–Howard isomorphism, the base types correspond to the propositional symbols $\{P_0, P_1, \ldots, P_n, \ldots\}$.

**Definition 2.9.** The simple types $\sigma$ are defined inductively as follows:

1. If $T_i$ is a base type, then $T_i$ is a simple type.
2. If $\sigma$ and $\tau$ are simple types, then $(\sigma \to \tau)$ is a simple type.

Thus $(T_1 \to T_1), (T_1 \to (T_2 \to T_1)), ((T_1 \to T_2) \to T_1)$, are simple types.

The standard abbreviation for $(\sigma_1 \to (\sigma_2 \to (\cdots \to \sigma_n)))$ is $\sigma_1 \to \sigma_2 \to \cdots \to \sigma_n$.

There is obviously a bijection between propositions and simple types. Every propositional symbol $P_i$ can be viewed as a base type, and the proposition $(P \Rightarrow Q)$ corresponds to the
simple type \((P \rightarrow Q)\). The only difference is that the custom is to use \(\Rightarrow\) to denote logical implication and \(\rightarrow\) for simple types. The reason is that intuitively a simple type \((\sigma \rightarrow \tau)\) corresponds to a set of functions from a domain of type \(\sigma\) to a range of type \(\tau\).

The next crucial step is to define simply-typed \(\lambda\)-terms. This is done in two stages. First we define raw simply-typed \(\lambda\)-terms. They have a simple inductive definition but they do not necessarily type-check so we define some type-checking rules that turn out to be the Gentzen-style deduction proof rules annotated with simply-typed \(\lambda\)-terms. These simply-typed \(\lambda\)-terms are representations of natural deductions.

We have a countable set of variables \(\{x_0, x_1, \ldots, x_n, \ldots\}\) that correspond to the atomic raw \(\lambda\)-terms. These are also the variables that are used for tagging assumptions when constructing deductions.

**Definition 2.10.** The raw simply-typed \(\lambda\)-terms (for short raw terms or \(\lambda\)-terms) \(M\) are defined inductively as follows:

1. If \(x_i\) is a variable, then \(x_i\) is a raw term.
2. If \(M\) and \(N\) are raw terms, then \((MN)\) is a raw term called an application.
3. If \(M\) is a raw term, \(\sigma\) is a simple type, and \(x\) is a variable, then the expression \(\lambda x: \sigma. M\) is a raw term called a \(\lambda\)-abstraction.

Matching parentheses may be dropped or added for convenience. In a raw \(\lambda\)-term \(M\), a variable \(x\) appearing in an expression \(\lambda x: \sigma\) is said to be bound in \(M\). The other variables in \(M\) (if any) are said to be free in \(M\). A \(\lambda\)-term \(M\) is closed if it has no free variables.

For example, in the term \(\lambda x: \sigma. (yx)\), the variable \(x\) is bound and the variable \(y\) is free. This term is not closed. The term \(\lambda y: \sigma \rightarrow \sigma. (\lambda x: \sigma. (yx))\) is closed.

The intuition is that a term of the form \(\lambda x: \sigma. M\) represents a function. How such a function operates will be defined in terms of \(\beta\)-reduction.

**Definition 2.11.** The depth \(d(M)\) of a raw \(\lambda\)-term \(M\) is defined inductively as follows.

1. If \(M\) is a variable \(x\), then \(d(x) = 0\).
2. If \(M\) is an application \((M_1M_2)\), then \(d(M) = \max\{d(M_1), d(M_2)\} + 1\).
3. If \(M\) is a \(\lambda\)-abstraction \((\lambda x: \sigma. M_1)\), then \(d(M) = d(M_1) + 1\).

It is pretty clear that raw \(\lambda\)-terms have representations as (ordered) labeled trees.

**Definition 2.12.** Given a raw \(\lambda\)-term \(M\), the tree \(\text{tree}(M)\) representing \(M\) is defined inductively as follows:

1. If \(M\) is a variable \(x\), then \(\text{tree}(M)\) is the one-node tree labeled \(x\).
2. If \(M\) is an application \((M_1M_2)\), then \(\text{tree}(M)\) is the tree with a binary root node labeled \(\_\), and with a left subtree \(\text{tree}(M_1)\) and a right subtree \(\text{tree}(M_2)\).
3. If $M$ is a $\lambda$-abstraction $\lambda x: \sigma. M_1$, then $\text{tree}(M)$ is the tree with a unary root node labeled $\lambda x: \sigma$, and with one subtree $\text{tree}(M_1)$.

Definition 2.12 is illustrated in Figure 2.6.

![Figure 2.6: The tree $\text{tree}(M)$ associated with a raw $\lambda$-term $M$.](image)

Obviously, the depth $d(M)$ of raw $\lambda$-term is the depth of its tree representation $\text{tree}(M)$.

Definition 2.12 could be used to deal with bound variables. For every leaf labeled with a bound variable $x$, we draw a backpointer to an ancestor of $x$ determined as follows. Given a leaf labeled with a bound variable $x$, climb up to the closest ancestor labeled $\lambda x: \sigma$, and draw a backpointer to this node. Then all bound variables can be erased. See Figure 2.7 for an example.

Definition 2.10 allows the construction of undesirable terms such as $(xx)$ or $(\lambda x: \sigma. (xx))(\lambda x: \sigma. (xx))$ because no type-checking is done. Part of the problem is that the variables occurring in a raw term have not been assigned types. This can be done using a context (or type assignment), which is a set of pairs $\Gamma = \{x_1: \sigma_1, \ldots, x_n: \sigma_n\}$ where the $\sigma_i$ are simple types. Once a type assignment has been provided, the type-checking rules are basically the proof rules of natural deduction in Gentzen-style. The fact that a raw term $M$ has type $\sigma$ given a type assignment $\Gamma$ that assigns types to all the free variables in $M$ is written as

$$\Gamma \triangleright M : \sigma.$$

Such an expression is called a judgement. The symbol $\triangleright$ is used instead of the symbol $\rightarrow$ because $\rightarrow$ occurs in simple types. Here are the typing-checking rules.

**Definition 2.13.** The type-checking rules of the simply-typed $\lambda$-calculus $\lambda^\rightarrow$ are listed below:

$$\Gamma, x : \sigma \triangleright x : \sigma$$
2.13. THE SIMPLY-TYPED \( \lambda \)-CALCULUS

\[ \frac{\Gamma, x: \sigma \vdash M: \tau}{\Gamma \vdash (\lambda x: \sigma. M): \sigma \rightarrow \tau} \]  
\text{(abstraction)}

\[ \frac{\Gamma \vdash M: \sigma \rightarrow \tau \quad \Delta \vdash N: \tau}{\Gamma \cup \Delta \vdash (MN): \tau} \]  
\text{(application)}

We write \( \vdash \Gamma \vdash M: \sigma \) to express that the judgement \( \Gamma \vdash M: \sigma \) is provable. Given a raw simply-typed \( \lambda \)-term \( M \), if there is a type-assigment \( \Gamma \) and a simple type \( \sigma \) such that the judgement \( \Gamma \vdash M: \sigma \) is provable, we say that \( M \) type-checks with type \( \sigma \).

It can be shown by induction on the depth of raw terms that for a fixed type-assigment \( \Gamma \), if a raw simply-typed \( \lambda \)-term \( M \) type-checks with some simple type \( \sigma \), then \( \sigma \) is unique.

The correspondence between proofs in natural deduction and simply-typed \( \lambda \)-terms (the Curry/Howard isomorphism) is now clear: the blue term is a representation of the deduction of the sequents \( \Gamma, x: \sigma \rightarrow \sigma \), \( \Gamma \rightarrow \sigma \Rightarrow \tau \), and \( \Gamma \cup \Delta \rightarrow \tau \), with the types \( \sigma, \sigma \Rightarrow \tau \) and \( \tau \) viewed as propositions. Note that proofs correspond to closed \( \lambda \)-terms.

For example, we have the type-checking proof

\[ \frac{y: ((R \Rightarrow R) \Rightarrow Q) \triangleright y: ((R \Rightarrow R) \Rightarrow Q) \quad z: R \triangleright z: R}{\triangleright \lambda y: ((R \Rightarrow R) \Rightarrow Q). y(\lambda z: R. z): Q} \]

which shows that the simply-typed \( \lambda \)-term

\[ M = \lambda y: ((R \Rightarrow R) \Rightarrow Q). y(\lambda z: R. z) \]

represents the proof.
The proposition \(((R \Rightarrow R) \Rightarrow Q) \Rightarrow Q\) being proven is the type of the \(\lambda\)-term \(M\). The tree representing the \(\lambda\)-term \(M = \lambda y: ((R \Rightarrow R) \Rightarrow Q). y(\lambda z: R. z)\) is shown in Figure 2.8.

Figure 2.8: The tree representation of the \(\lambda\)-term \(M\).

Furthermore, and this is the deepest aspect of the Curry/Howard isomorphism, proof normalization corresponds to \(\beta\)-reduction in the simply-typed \(\lambda\)-calculus.

The notion of \(\beta\)-reduction is defined in terms of substitutions. A substitution \(\varphi\) is a finite set of pairs \(\varphi = \{(x_1, N_1), \ldots, (x_n, N_n)\}\), where the \(x_i\) are distinct variables and the \(N_i\) are raw \(\lambda\)-terms. We write

\[\varphi = [N_1/x_1, \ldots, N_n/x_n]\]

The second notation indicates more clearly that each term \(N_i\) is substituted for the variable \(x_i\) and it seems to have been almost universally adopted.

Given a substitution \(\varphi = [x_1 := N_1, \ldots, x_n := N_n]\), for any variable \(x_i\), we denote by \(\varphi_{-x_i}\) the new substitution where the pair \((x_i, N_i)\) is replaced by the pair \((x_i, x_i)\) (that is, the new substitution leaves \(x_i\) unchanged).

Given any raw \(\lambda\)-term \(M\) and any substitution \(\varphi = [x_1 := N_1, \ldots, x_n := N_n]\), we define the raw \(\lambda\)-term \(M[\varphi]\), the result of applying the substitution \(\varphi\) to \(M\), as follows:

1. If \(M = y\), with \(y \neq x_i\) for \(i = 1, \ldots, n\), then \(M[\varphi] = y = M\).
2. If \(M = x_i\) for some \(i \in \{1, \ldots, n\}\), then \(M[\varphi] = N_i\).
2.13. THE SIMPLY-TYPED $\lambda$-CALCULUS

(3) If $M = (PQ)$, then $M[\varphi] = (P[\varphi]Q[\varphi])$.

(4) If $M = \lambda x: \sigma. N$ and $x \neq x_i$ for $i = 1, \ldots, n$, then $M[\varphi] = \lambda x: \sigma. N[\varphi]$,

(5) If $M = \lambda x: \sigma. N$ and $x = x_i$ for some $i \in \{1, \ldots, n\}$, then $M[\varphi] = \lambda x: \sigma. N[\varphi]_{-x_i}$.

There is a problem with the present definition of a substitution in Cases (4) and (5), which is that the result of substituting a term $N_i$ containing the variable $x$ free causes this variable to become bound after the substitution. We say that $x$ is captured. To remedy this problem, Church defined $\alpha$-conversion.

The idea of $\alpha$-conversion is that in a raw term $M$ any subterm of the form $\lambda x: \sigma. P$ can be replaced by the subterm $\lambda z: \sigma. P[x:=z]$ where $z$ is a new variable not occurring at all (free or bound) in $M$ to obtain a new term $M'$. We write $M \equiv_\alpha M'$ and we view $M$ and $M'$ as equivalent.

For example, $\lambda x: \sigma. yx \equiv_\alpha \lambda z: \sigma. yz$ and $\lambda y: \sigma \rightarrow \sigma. (\lambda x: \sigma. yx) \equiv_\alpha \lambda w: \sigma \rightarrow \sigma. (\lambda z: \sigma. wz)$.

The variables $x$ and $y$ are just place-holders.

Then given a raw $\lambda$-term $M$ and a substitution $\varphi = [x_1 := N_1, \ldots, x_n := N_n]$, before applying $\varphi$ to $M$ we first apply some $\alpha$-conversion to rename all bound variables in $M$ obtaining $M' \equiv_\alpha M$ so that they do not occur in any of the $N_i$, and then safely apply the substitution $\varphi$ to $M'$ without any capture of variables. We say that the term $M'$ is safe for the substitution $\varphi$. The details are a bit tedious and we omit them. We refer the interested reader to Gallier [5] for a comprehensive discussion.

The following result shows that substitutions behave well with respect to type-checking.

Proposition 2.10. For any raw $\lambda$-term $M$ and any substitution $\varphi = [x_1 := N_1, \ldots, x_n := N_n]$, whose domain contains the set of free variables of $M$, if the judgement $\Gamma \vdash M: \tau$ is provable for some context $\Gamma$ and some simple type $\tau$, and if there is some context $\Delta$ such that for every free variable $x_j$ in $M$ the judgement $\Delta \vdash N_j: \Gamma(x) \vdash \tau$ is provable, then there some $M' \equiv_\alpha M$ such that the judgment $\Delta \vdash M'[\varphi]: \tau$ is provable.

Finally we define $\beta$-reduction and $\beta$-conversion as follows.

Definition 2.14. The relation $\rightarrow_\beta$, called immediate $\beta$-reduction, is the smallest relation satisfying the following properties for all raw $\lambda$-terms $M, N, P, Q$:

$$(\lambda x: \sigma. M)N \rightarrow_\beta M[x:=N]$$

provided that $M$ is safe for $[x := N]$;

$$M \rightarrow_\beta N \quad \frac{M \rightarrow_\beta N}{MQ \rightarrow_\beta NQ} \quad \frac{M \rightarrow_\beta N}{PM \rightarrow_\beta PN} \quad \text{for all } P, Q \quad \text{(congruence)}$$
\[
\frac{M \to^\beta N}{\lambda x: \sigma. M \to^\beta \lambda x: \sigma. N}
\] for all \(\sigma\) \hfill (\xi)

The transitive closure of \(\to^\beta\) is denoted by \(\to^+\), the reflexive and transitive closure of \(\to^\beta\) is denoted by \(\to^*\), and we define \(\beta\)-conversion, denoted by \(\leftrightarrow^*\), as the smallest equivalence relation \(\leftrightarrow^* = (\to^\beta \cup \to^{-1})^*\) containing \(\to^\beta\).

For example, we have

\[
(\lambda u: \sigma. (vu))(\lambda x: \sigma \to \sigma.(xy))(\lambda z: \sigma. z) \to^\beta
\]

\[
(\lambda u: \sigma. (vu))(\lambda x: \sigma \to \sigma.(xy))[x := (\lambda z: \sigma. z)] = (\lambda u: \sigma. (vu))(\lambda z: \sigma. z)y
\]

\[
\to^\beta (\lambda u: \sigma. (vu))z[z := y] = (\lambda u: \sigma. (vu))y \to^\beta (vu)[u := y] = vy.
\]

The following result shows that \(\beta\)-reduction (and \(\beta\)-conversion) behave well with respect to type-checking.

**Proposition 2.11.** For any two raw \(\lambda\)-terms \(M\) and \(N\), if there is a proof of the judgement \(\Gamma \vdash M: \sigma\) for some context \(\Gamma\) and some simple type \(\sigma\), and if \(M \to^+\beta N\) (or \(M \leftrightarrow^*\beta N\)), then the judgement \(\Gamma \vdash N: \sigma\) is provable. Thus \(\beta\)-reduction and \(\beta\)-conversion preserve type-checking.

We say that a \(\lambda\)-term \(M\) is \(\beta\)-irreducible or a \(\beta\)-normal form if there is no term \(N\) such that \(M \to^\beta N\).

The fundamental result about the simply-typed \(\lambda\)-calculus is this.

**Theorem 2.12.** For every raw \(\lambda\)-term \(M\), if \(M\) type-checks, which means that there a provable judgement \(\Gamma \vdash M: \sigma\) for some context \(\Gamma\) and some simple type \(\sigma\), then the following results hold:

1. If \(M \to^*\beta M_1\) and \(M \to^*\beta M_2\), then there is some \(M_3\) such that \(M_1 \to^*\beta M_3\) and \(M_2 \to^*\beta M_3\). We say that \(\to^*\beta\) is confluent.

2. Every reduction sequence \(M \to^+\beta N\) is finite. We that that the simply-typed \(\lambda\)-calculus is strongly normalizing (for short, \(\text{SN}\)).

As a consequence of (1) and (2), there is a unique \(\beta\)-irreducible term \(N\) (called a \(\beta\)-normal form) such that \(M \to^*\beta N\).

A proof of Theorem 2.12 can be found in Gallier [7]. See also Gallier [5] which contains a thorough discussion of the techniques involved in proving these results.

In Theorem 2.12, the fact that the term \(M\) type-checks is crucial. Indeed the term

\[
(\lambda x. (xx))(\lambda x. (xx)),
\]

which does not type-check (we omitted the type tags \(\sigma\) of the variable \(x\) since they do not play any role), gives rise to an infinite \(\beta\)-reduction sequence!
In summary, the correspondence between proofs in intuitionistic logic and typed \( \lambda \)-terms on one hand and between proof normalization and \( \beta \)-reduction, can be used to translate results about typed \( \lambda \)-terms into results about proofs in intuitionistic logic. These results can be generalized to typed \( \lambda \)-calculi with product types and union types; see Gallier [7].

Using some suitable intuitionistic sequent calculi and Gentzen’s cut elimination theorem or some suitable typed \( \lambda \)-calculi and (strong) normalization results about them, it is possible to prove that there is a decision procedure for propositional intuitionistic logic. However, it can also be shown that the time-complexity of any such procedure is very high. As a matter of fact, it was shown by Statman (1979) that deciding whether a proposition is intuitionistically provable is P-space complete [20]. Here, we are alluding to complexity theory, another active area of computer science, Hopcroft, Motwani, and Ullman [13] and Lewis and Papadimitriou [17].

Readers who wish to learn more about these topics can read my two survey papers Gallier [7] (On the Correspondence Between Proofs and \( \lambda \)-Terms) and Gallier [6] (A Tutorial on Proof Systems and Typed \( \lambda \)-Calculi), both available on the website http://www.cis.upenn.edu/~jean/gbooks/logic.html and the excellent introduction to proof theory by Troelstra and Schwichtenberg [23].

Anybody who really wants to understand logic should of course take a look at Kleene [16] (the famous “I.M.”), but this is not recommended to beginners.

### 2.14 Completeness and Counter-Examples

Let us return to the question of deciding whether a proposition is not provable. To simplify the discussion, let us restrict our attention to propositional classical logic. So far, we have presented a very proof-theoretic view of logic, that is, a view based on the notion of provability as opposed to a more semantic view of based on the notions of truth and models. A possible excuse for our bias is that, as Peter Andrews (from CMU) puts it, “truth is elusive.” Therefore, it is simpler to understand what truth is in terms of the more “mechanical” notion of provability. (Peter Andrews even gave the subtitle

*To Truth Through Proof*

To his logic book Andrews [1],.)
However, mathematicians are not mechanical theorem provers (even if they prove lots of stuff). Indeed, mathematicians almost always think of the objects they deal with (functions, curves, surfaces, groups, rings, etc.) as rather concrete objects (even if they may not seem concrete to the uninitiated) and not as abstract entities solely characterized by arcane axioms.

It is indeed natural and fruitful to try to interpret formal statements semantically. For propositional classical logic, this can be done quite easily if we interpret atomic propositional letters using the truth values true and false, as explained in Section 2.10. Then, the crucial point that every provable proposition (say in $\mathcal{NG}_{c,\Rightarrow,\lor,\land,\bot}$) has the value true no matter how we assign truth values to the letters in our proposition. In this case, we say that $P$ is valid.

The fact that provability implies validity is called soundness or consistency of the proof system. The soundness of the proof system $\mathcal{NG}_{c,\Rightarrow,\lor,\land,\bot}$ is easy to prove, as sketched in Section 2.10.

We now have a method to show that a proposition $P$ is not provable: find some truth assignment that makes $P$ false. Such an assignment falsifying $P$ is called a counterexample. If $P$ has a counterexample, then it can’t be provable because if it were, then by soundness it would be true for all possible truth assignments.

But now, another question comes up. If a proposition is not provable, can we always find a counterexample for it? Equivalently, is every valid proposition provable? If every valid proposition is provable, we say that our proof system is complete (this is the completeness of our system).

The system $\mathcal{NG}_{c,\Rightarrow,\lor,\land,\bot}$ is indeed complete. In fact, all the classical systems that we have discussed are sound and complete. Completeness is usually a lot harder to prove than soundness. For first-order classical logic, this is known as Gödel's completeness theorem (1929). Again, we refer our readers to Gallier [4], van Dalen [24], or Huth and Ryan [15] for a thorough discussion of these matters. In the first-order case, one has to define first-order structures (or first-order models).

What about intuitionistic logic?

Well, one has to come up with a richer notion of semantics because it is no longer true that if a proposition is valid (in the sense of our two-valued semantics using true, false), then it is provable. Several semantics have been given for intuitionistic logic. In our opinion, the most natural is the notion of the Kripke model, presented in Section 2.11. Then, again, soundness and completeness hold for intuitionistic proof systems, even in the first-order case.
In summary, semantic models can be used to provide counterexamples of unprovable propositions. This is a quick method to establish that a proposition is not provable.

We close this section by repeating something we said earlier: there isn’t just one logic but instead, many logics. In addition to classical and intuitionistic logic (propositional and first-order), there are: modal logics, higher-order logics, and linear logic, a logic due to Jean-Yves Girard, attempting to unify classical and intuitionistic logic (among other goals).

An excellent introduction to these logics can be found in Troelstra and Schwichtenberg [23]. We warn our readers that most presentations of linear logic are (very) difficult to follow. This is definitely true of Girard’s seminal paper [10]. A more approachable version can be found in Girard, Lafont, and Taylor [9], but most readers will still wonder what hit them when they attempt to read it.

In computer science, there is also dynamic logic, used to prove properties of programs and temporal logic and its variants (originally invented by A. Pnueli), to prove properties of real-time systems. So logic is alive and well.

We now add quantifiers to our language and give the corresponding inference rules.

### 2.15 Adding Quantifiers; Proof Systems $\mathcal{N}_c \Rightarrow \land, \lor, \forall, \exists, \bot$ and $\mathcal{NG}_c \Rightarrow \land, \lor, \forall, \exists, \bot$

As we mentioned in Section 2.1, atomic propositions may contain variables. The intention is that such variables correspond to arbitrary objects. An example is

$$\text{human}(x) \Rightarrow \text{needs-to-drink}(x).$$

Now in mathematics, we usually prove universal statements, that is statements that hold for all possible “objects,” or existential statements, that is, statements asserting the existence of some object satisfying a given property. As we saw earlier, we assert that every human needs to drink by writing the proposition

$$\forall x (\text{human}(x) \Rightarrow \text{needs-to-drink}(x)).$$
Observe that once the quantifier $\forall$ (pronounced “for all” or “for every”) is applied to the variable $x$, the variable $x$ becomes a placeholder and replacing $x$ by $y$ or any other variable does not change anything. What matters is the locations to which the outer $x$ points in the inner proposition. We say that $x$ is a bound variable (sometimes a “dummy variable”).

If we want to assert that some human needs to drink we write

$$\exists x \text{human}(x) \Rightarrow \text{needs-to-drink}(x);$$

Again, once the quantifier $\exists$ (pronounced “there exists”) is applied to the variable $x$, the variable $x$ becomes a placeholder. However, the intended meaning of the second proposition is very different and weaker than the first. It only asserts the existence of some object satisfying the statement

$$\text{human}(x) \Rightarrow \text{needs-to-drink}(x).$$

Statements may contain variables that are not bound by quantifiers. For example, in

$$\exists x \text{parent}(x, y)$$

the variable $x$ is bound but the variable $y$ is not. Here the intended meaning of $\text{parent}(x, y)$ is that $x$ is a parent of $y$, and the intended meaning of $\exists x \text{parent}(x, y)$ is that any given $y$ has some parent $x$. Variables that are not bound are called free. The proposition

$$\forall y \exists x \text{parent}(x, y),$$

which contains only bound variables is meant to assert that every $y$ has some parent $x$. Typically, in mathematics, we only prove statements without free variables. However, statements with free variables may occur during intermediate stages of a proof.

The intuitive meaning of the statement $\forall x P$ is that $P$ holds for all possible objects $x$, and the intuitive meaning of the statement $\exists x P$ is that $P$ holds for some object $x$. Thus, we see that it would be useful to use symbols to denote various objects. For example, if we want to assert some facts about the “parent” predicate, we may want to introduce some constant symbols (for short, constants) such as “Jean,” “Mia,” and so on and write

$$\text{parent}(\text{Jean, Mia})$$

to assert that Jean is a parent of Mia. Often, we also have to use function symbols (or operators, constructors), for instance, to write a statement about numbers: $+, \times$, and so on. Using constant symbols, function symbols, and variables, we can form terms, such as

$$(x \times x + 1) \times (3 \times y + 2).$$

In addition to function symbols, we also use predicate symbols, which are names for atomic properties. We have already seen several examples of predicate symbols: “human,” “parent.” So, in general, when we try to prove properties of certain classes of objects (people, numbers, strings, graphs, and so on), we assume that we have a certain alphabet consisting of constant
symbols, function symbols, and predicate symbols. Using these symbols and an infinite supply of variables (assumed distinct from the variables we use to label premises) we can form terms and predicate terms. We say that we have a (logical) language. Using this language, we can write compound statements.

Let us be a little more precise. In a first-order language $L$ in addition to the logical connectives $\Rightarrow, \land, \lor, \neg, \perp, \forall,$ and $\exists,$ we have a set $L$ of nonlogical symbols consisting of

(i) A set $CS$ of constant symbols, $c_1, c_2, \ldots$.

(ii) A set $FS$ of function symbols, $f_1, f_2, \ldots$. Each function symbol $f$ has a rank $n_f \geq 1,$ which is the number of arguments of $f$.

(iii) A set $PS$ of predicate symbols, $P_1, P_2, \ldots$. Each predicate symbol $P$ has a rank $n_P \geq 0,$ which is the number of arguments of $P$. Predicate symbols of rank 0 are propositional symbols as in earlier sections.

(iv) The equality predicate $=$ is added to our language when we want to deal with equations.

(v) First-order variables $t_1, t_2, \ldots$ used to form quantified formulae.

The difference between function symbols and predicate symbols is that function symbols are interpreted as functions defined on a structure (e.g., addition, $+$, on $\mathbb{N}$), whereas predicate symbols are interpreted as properties of objects, that is, they take the value true or false.

An example is the language of Peano arithmetic, $L = \{0, S, +, *, =\}$, where 0 is a constant symbol, $S$ is a function symbol with one argument, and $+,*$ are function symbols with two arguments. Here, the intended structure is $\mathbb{N}$, 0 is of course zero, $S$ is interpreted as the function $S(n) = n + 1,$ the symbol $+$ is addition, $*$ is multiplication, and $=$ is equality.

Using a first-order language $L,$ we can form terms, predicate terms, and formulae. The terms over $L$ are the following expressions.

(i) Every variable $t$ is a term.

(ii) Every constant symbol $c \in CS,$ is a term.

(iii) If $f \in FS$ is a function symbol taking $n$ arguments and $\tau_1, \ldots, \tau_n$ are terms already constructed, then $f(\tau_1, \ldots, \tau_n)$ is a term.

The predicate terms over $L$ are the following expressions.

(i) If $P \in PS$ is a predicate symbol taking $n$ arguments and $\tau_1, \ldots, \tau_n$ are terms already constructed, then $P(\tau_1, \ldots, \tau_n)$ is a predicate term. When $n = 0,$ the predicate symbol $P$ is a predicate term called a propositional symbol.

(ii) When we allow the equality predicate, for any two terms $\tau_1$ and $\tau_2,$ the expression $\tau_1 = \tau_2$ is a predicate term. It is usually called an equation.
The \textit{(first-order)} formulae over $L$ are the following expressions.

(i) Every predicate term $P(\tau_1, \ldots, \tau_n)$ is an atomic formula. This includes all propositional letters. We also view $\bot$ (and sometimes $\top$) as an atomic formula.

(ii) When we allow the equality predicate, every equation $\tau_1 = \tau_2$ is an atomic formula.

(iii) If $P$ and $Q$ are formulae already constructed, then $P \Rightarrow Q$, $P \land Q$, $P \lor Q$, $\neg P$ are compound formulae. We treat $P \equiv Q$ as an abbreviation for $(P \Rightarrow Q) \land (Q \Rightarrow P)$, as before.

(iv) If $P$ is a formula already constructed and $t$ is any variable, then $\forall t P$ and $\exists t P$ are quantified compound formulae.

All this can be made very precise but this is quite tedious. Our primary goal is to explain the basic rules of logic and not to teach a full-fledged logic course. We hope that our intuitive explanations will suffice, and we now come to the heart of the matter, the inference rules for the quantifiers. Once again, for a complete treatment, readers are referred to Gallier \cite{4}, van Dalen \cite{24}, or Huth and Ryan \cite{15}.

Unlike the rules for $\Rightarrow, \lor, \land$ and $\bot$, which are rather straightforward, the rules for quantifiers are more subtle due to the presence of variables (occurring in terms and predicates). We have to be careful to forbid inferences that would yield “wrong” results and for this we have to be very precise about the way we use free variables. More specifically, we have to exercise care when we make substitutions of terms for variables in propositions. For example, say we have the predicate “odd,” intended to express that a number is odd. Now we can substitute the term $(2y+1)^2$ for $x$ in $\text{odd}(x)$ and obtain

$$\text{odd}((2y+1)^2).$$

More generally, if $P(t_1, t_2, \ldots, t_n)$ is a statement containing the free variables $t_1, \ldots, t_n$ and if $\tau_1, \ldots, \tau_n$ are terms, we can form the new statement

$$P[\tau_1/t_1, \ldots, \tau_n/t_n]$$

obtained by substituting the term $\tau_i$ for all free occurrences of the variable $t_i$, for $i = 1, \ldots, n$. By the way, we denote terms by the Greek letter $\tau$ because we use the letter $t$ for a variable and using $t$ for both variables and terms would be confusing.

However, if $P(t_1, t_2, \ldots, t_n)$ contains quantifiers, some bad things can happen; namely, some of the variables occurring in some term $\tau_i$ may become quantified when $\tau_i$ is substituted for $t_i$. For example, consider

$$\forall x \exists y P(x, y, z)$$

which contains the free variable $z$ and substitute the term $x + y$ for $z$: we get

$$\forall x \exists y P(x, y, x + y).$$
We see that the variables \( x \) and \( y \) occurring in the term \( x + y \) become bound variables after substitution. We say that there is a “capture of variables.”

This is not what we intended to happen. To fix this problem, we recall that bound variables are really placeholders, so they can be renamed without changing anything. Therefore, we can rename the bound variables \( x \) and \( y \) in \( \forall x \exists y P(x, y, z) \) to \( u \) and \( v \), getting the statement \( \forall u \exists v P(u, v, z) \) and now, the result of the substitution is

\[
\forall u \exists v P(u, v, x + y).
\]

Again, all this needs to be explained very carefully but this can be done.

Finally, here are the inference rules for the quantifiers, first stated in a natural deduction style and then in sequent style. It is assumed that we use two disjoint sets of variables for labeling premises \( (x, y, \ldots) \) and free variables \( (t, u, v, \ldots) \). As we show, the \( \forall \)-introduction rule and the \( \exists \)-elimination rule involve a crucial restriction on the occurrences of certain variables. Remember, variables are terms.

**Definition 2.15.** The inference rules for the quantifiers are

- **\( \forall \)-introduction:**
  If \( D \) is a deduction tree for \( P[u/t] \) from the premises \( \Gamma \), then

\[
\begin{array}{c}
\Gamma \\
D \\
P[u/t] \\
\end{array}
\over\forall t P
\]

is a deduction tree for \( \forall t P \) from the premises \( \Gamma \). Here, \( u \) must be a variable that does not occur free in any of the propositions in \( \Gamma \) or in \( \forall t P \). The notation \( P[u/t] \) stands for the result of substituting \( u \) for all free occurrences of \( t \) in \( P \).

Recall that \( \Gamma \) denotes the multiset of premises of the deduction tree \( D \), so if \( D \) only has one node, then \( \Gamma = \{ P[u/t] \} \) and \( t \) should not occur in \( P \).

- **\( \forall \)-elimination:**
  If \( D \) is a deduction tree for \( \forall t P \) from the premises \( \Gamma \), then

\[
\begin{array}{c}
\Gamma \\
D \\
\forall t P \\
P[\tau/t] \\
\end{array}
\overP[\tau/t]
\]

is a deduction tree for \( P[\tau/t] \) from the premises \( \Gamma \). Here \( \tau \) is an arbitrary term and it is assumed that bound variables in \( P \) have been renamed so that none of the variables in \( \tau \) are captured after substitution.

- **\( \exists \)-introduction:**
  If \( D \) is a deduction tree for \( P[\tau/t] \) from the premises \( \Gamma \), then
Γ
D

\[ P[τ/t] \]

\[ ∃tP \]

is a deduction tree for ∃tP from the premises Γ. As in ∀-elimination, τ is an arbitrary term and the same proviso on bound variables in P applies (no capture of variables when τ is substituted).

**∃-elimination:**

If D₁ is a deduction tree for ∃tP from the premises Γ, and if D₂ is a deduction tree for C from the premises in the multiset Δ and one or more occurrences of P[τ/t], then

Γ
D₁

\[ Δ, P[u/t] \]

Δ


\[ P[u/t] \]

D₂

∃tP

C

x

is a deduction tree of C from the set of premises in the multiset Γ, Δ. Here, u must be a variable that *does not occur free in any of the propositions in Δ, ∃tP, or C*, and all premises P[τ/t] labeled x are discharged.

In the ∀-introduction and the ∃-elimination rules, the variable u is called the *eigenvariable* of the inference.

In the above rules, Γ or Δ may be empty; P, C denote arbitrary propositions constructed from a first-order language L; D, D₁, D₂ are deductions, possibly a one-node tree; and t is *any* variable.

The system of *first-order classical logic* \( N_c^\Rightarrow,∨,∧,⊥,∀,∃ \) is obtained by adding the above rules to the system of propositional classical logic \( N_c^\Rightarrow,∨,∧,⊥ \). The system of *first-order intuitionistic logic* \( N_i^\Rightarrow,∨,∧,⊥,∀,∃ \) is obtained by adding the above rules to the system of propositional intuitionistic logic \( N_i^\Rightarrow,∨,∧,⊥ \). Deduction trees and proof trees are defined as in the propositional case except that the quantifier rules are also allowed.

Using sequents, the quantifier rules in first-order logic are expressed as follows:

**Definition 2.16.** The inference rules for the quantifiers in Gentzen-sequent style are

\[
\frac{Γ \rightarrow P[τ/t]}{Γ \rightarrow ∀tP} \quad (∀\text{-intro}) \quad \frac{Γ \rightarrow ∀tP}{Γ \rightarrow P[τ/t]} \quad (∀\text{-elim})
\]

where in (∀-intro), u does not occur free in Γ or ∀tP;

\[
\frac{Γ \rightarrow P[τ/t]}{Γ \rightarrow ∃tP} \quad (∃\text{-intro}) \quad \frac{Γ \rightarrow ∃tP \quad z: P[u/t], Δ \rightarrow C}{Γ \cup Δ \rightarrow C} \quad (∃\text{-elim}),
\]

where in (∃-elim), u does not occur free in Γ, ∃tP, or C. Again, t is *any* variable.
The variable $u$ is called the *eigenvariable* of the inference. The systems $\mathcal{N}_c^{\Rightarrow, \wedge, \vee, \exists, \bot}$ and $\mathcal{N}_i^{\Rightarrow, \wedge, \vee, \exists, \bot}$ are defined from the systems $\mathcal{N}_c^{\Rightarrow, \wedge, \bot}$ and $\mathcal{N}_i^{\Rightarrow, \wedge, \bot}$, respectively, by adding the above rules. As usual, a *deduction tree* is either a one-node tree or a tree constructed using the above rules and a *proof tree* is a deduction tree whose conclusion is a sequent with an empty set of premises (a sequent of the form $\emptyset \rightarrow \text{conclusion}$).

When we say that a proposition $P$ is provable from $\Gamma$ we mean that we can construct a proof tree whose conclusion is $P$ and whose set of premises is $\Gamma$ in one of the systems $\mathcal{N}_c^{\Rightarrow, \wedge, \vee, \exists, \bot}$ or $\mathcal{N}_i^{\Rightarrow, \wedge, \vee, \exists, \bot}$. Therefore, as in propositional logic, when we use the word “provable” unqualified, we mean provable in classical logic. Otherwise, we say *intuitionistically provable*.

It is not hard to show that the proof systems $\mathcal{N}_c^{\Rightarrow, \wedge, \vee, \exists, \bot}$ and $\mathcal{N}_i^{\Rightarrow, \wedge, \vee, \exists, \bot}$ are equivalent (and similarly for $\mathcal{N}_i^{\Rightarrow, \wedge, \vee, \exists, \bot}$ and $\mathcal{N}_c^{\Rightarrow, \wedge, \vee, \exists, \bot}$). We leave the details as Problem 2.16.

A first look at the above rules shows that universal formulae $\forall t P$ behave somewhat like infinite conjunctions and that existential formulae $\exists t P$ behave somewhat like infinite disjunctions.

The $\forall$-introduction rule looks a little strange but the idea behind it is actually very simple: because $u$ is totally unconstrained, if $P[u/t]$ is provable (from $\Gamma$), then intuitively $P[u/t]$ holds of any arbitrary object, and so, the statement $\forall t P$ should also be provable (from $\Gamma$). Note that the tree

$$
\begin{array}{c}
P[u/t] \\
\forall t P
\end{array}
$$

is generally not a deduction, because the deduction tree above $\forall t P$ is a one-node tree consisting of the single premise $P[u/t]$, and $u$ occurs in $P[u/t]$ unless $t$ does not occur in $P$.

The meaning of the $\forall$-elimination rule is that if $\forall t P$ is provable (from $\Gamma$), then $P$ holds for all objects and so, in particular for the object denoted by the term $\tau$; that is, $P[\tau/t]$ should be provable (from $\Gamma$).

The $\exists$-introduction rule is dual to the $\forall$-elimination rule. If $P[\tau/t]$ is provable (from $\Gamma$), this means that the object denoted by $\tau$ satisfies $P$, so $\exists t P$ should be provable (this latter formula asserts the existence of some object satisfying $P$, and $\tau$ is such an object).

The $\exists$-elimination rule is reminiscent of the $\forall$-elimination rule and is a little more tricky. It goes as follows. Suppose that we proved $\exists t P$ (from $\Gamma$). Moreover, suppose that for every possible case $P[u/t]$ we were able to prove $C$ (from $\Gamma$). Then as we have “exhausted” all possible cases and as we know from the provability of $\exists t P$ that some case must hold, we can conclude that $C$ is provable (from $\Gamma$) without using $P[u/t]$ as a premise.

Like the $\forall$-elimination rule, the $\exists$-elimination rule is not very constructive. It allows making a conclusion ($C$) by considering alternatives *without knowing which one actually occurs*.

**Remark:** Analogously to disjunction, in (first-order) intuitionistic logic, if an existential statement $\exists t P$ is provable, then from any proof of $\exists t P$, some term $\tau$ can be extracted so that $P[\tau/t]$ is provable. Such a term $\tau$ is called a *witness*.

The witness property is not easy
to prove. It follows from the fact that intuitionistic proofs have a normal form (see Section 2.12). However, no such property holds in classical logic.

We can illustrate, again, the fact that classical logic allows for nonconstructive proofs by re-examining the example at the end of Section 2.6. There we proved that if $\sqrt{2}$ is rational, then $a = \sqrt{2}$ and $b = \sqrt{2}$ are both irrational numbers such that $a^b$ is rational, and if $\sqrt{2}$ is irrational, then $a = \sqrt{2}$ and $b = \sqrt{2}$ are both irrational numbers such that $a^b$ is rational. By $\exists$-introduction, we deduce that if $\sqrt{2}$ is rational, then there exist some irrational numbers $a, b$ so that $a^b$ is rational, and if $\sqrt{2}$ is irrational, then there exist some irrational numbers $a, b$ so that $a^b$ is rational. In classical logic, as $P \lor \lnot P$ is provable, by $\lor$-elimination, we just proved that there exist some irrational numbers $a, b$ so that $a^b$ is rational. However, this argument does not give us explicitly numbers $a, b$ with the required properties. It only tells us that such numbers must exist. Now it turns out that $\sqrt{2}$ is indeed irrational (this follows from the Gel’fond–Schneider theorem, a hard theorem in number theory). Furthermore, there are also simpler explicit solutions such as $a = \sqrt{2}$ and $b = \log_2 9$, as the reader should check.

Here is an example of a proof in the system $\mathcal{N}_c^{\Rightarrow, \mathcal{V}, \land, \lor, \forall, \exists}$ (actually, in $\mathcal{N}_i^{\Rightarrow, \mathcal{V}, \land, \lor, \forall, \exists}$) of the formula $\forall t (P \land Q) \Rightarrow \forall t P \land \forall t Q$.

\[
\begin{array}{c}
\frac{\forall t (P \land Q)[x]}{P[u/t] \land Q[u/t]} \\
\frac{P[u/t]}{\forall t P} \\
\frac{\forall t P}{\forall t (P \land Q) \Rightarrow \forall t P} \\
\frac{Q[u/t]}{\forall t Q} \\
\frac{\forall t P \land \forall t Q}{\forall t (P \land Q) \Rightarrow \forall t P \land \forall t Q} \\
\end{array}
\]

In the above proof, $u$ is a new variable, that is, a variable that does not occur free in $P$ or $Q$. We also have used some basic properties of substitutions such as

\[
\begin{align*}
(P \land Q)[\tau/t] &= P[\tau/t] \land Q[\tau/t] \\
(P \lor Q)[\tau/t] &= P[\tau/t] \lor Q[\tau/t] \\
(P \Rightarrow Q)[\tau/t] &= P[\tau/t] \Rightarrow Q[\tau/t] \\
(\neg P)[\tau/t] &= \neg P[\tau/t] \\
(\forall s P)[\tau/t] &= \forall s P[\tau/t] \\
(\exists s P)[\tau/t] &= \exists s P[\tau/t],
\end{align*}
\]

for any term $\tau$ such that no variable in $\tau$ is captured during the substitution (in particular, in the last two cases, the variable $s$ does not occur in $\tau$).

The reader should show that $\forall t P \land \forall t Q \Rightarrow \forall t (P \land Q)$ is also provable in the system
2.15. ADDING QUANTIFIERS; PROOF SYSTEMS $\mathcal{N}_C^{\Rightarrow, \land, \lor, \forall, \exists, \bot}$, $\mathcal{N}_G^{\Rightarrow, \land, \lor, \forall, \exists, \bot}$

However, in general, one can’t just replace $\forall$ by $\exists$ (or $\land$ by $\lor$) and still obtain provable statements. For example, $\exists t P \land \exists t Q \Rightarrow \exists t (P \land Q)$ is not provable at all.

Here is an example in which the $\forall$-introduction rule is applied illegally, and thus, yields a statement that is actually false (not provable). In the incorrect “proof” below, $P$ is an atomic predicate symbol taking two arguments (e.g., “parent”) and 0 is a constant denoting zero:

$\begin{align*}
P(u, 0) & \quad \text{illegal step!} \\
\forall t P(t, 0) & \quad \text{Implication-Intro } x \\
P(u, 0) \Rightarrow \forall t P(t, 0) & \quad \text{Forall-Intro} \\
\forall s (P(s, 0) \Rightarrow \forall t P(t, 0)) & \quad \text{Forall-Elim} \\
P(0, 0) \Rightarrow \forall t P(t, 0) & 
\end{align*}$

The problem is that the variable $u$ occurs free in the premise $P[u/t, 0] = P(u, 0)$ and therefore, the application of the $\forall$-introduction rule in the first step is illegal. However, note that this premise is discharged in the second step and so, the application of the $\forall$-introduction rule in the third step is legal. The (false) conclusion of this faulty proof is that $P(0, 0) \Rightarrow \forall t P(t, 0)$ is provable. Indeed, there are plenty of properties such that the fact that the single instance $P(0, 0)$ holds does not imply that $P(t, 0)$ holds for all $t$.

**Remark:** The above example shows why it is desirable to have premises that are universally quantified. A premise of the form $\forall t P$ can be instantiated to $P[u/t]$, using $\forall$-elimination, where $u$ is a brand new variable. Later on, it may be possible to use $\forall$-introduction without running into trouble with free occurrences of $u$ in the premises. But we still have to be very careful when we use $\forall$-introduction or $\exists$-elimination.

Here are some useful equivalences involving quantifiers. The first two are analogous to the de Morgan laws for $\land$ and $\lor$.

**Proposition 2.13.** The following equivalences are provable in classical first-order logic.

$\begin{align*}
\neg \forall t P & \equiv \exists t \neg P \\
\neg \exists t P & \equiv \forall t \neg P \\
\forall t (P \land Q) & \equiv \forall t P \land \forall t Q \\
\exists t (P \lor Q) & \equiv \exists t P \lor \exists t Q.
\end{align*}$

In fact, the last three and $\exists t \neg P \Rightarrow \neg \forall t P$ are provable intuitionistically. Moreover, the formulae

$\exists t (P \land Q) \Rightarrow \exists t P \land \exists t Q$ and $\forall t P \lor \forall t Q \Rightarrow \forall t (P \lor Q)$

are provable in intuitionistic first-order logic (and thus, also in classical first-order logic).

**Proof.** Left as an exercise to the reader. $\square$
Before concluding this section, let us give a few more examples of proofs using the rules for the quantifiers. First let us prove that
\[ \forall t P \equiv \forall u P[u/t], \]
where \( u \) is any variable not free in \( \forall t P \) and such that \( u \) is not captured during the substitution. This rule allows us to rename bound variables (under very mild conditions). We have the proofs

\[ \frac{(\forall t P)^{\alpha}}{P[u/t]} \]
\[ \frac{\forall u P[u/t]}{\forall t P \Rightarrow \forall u P[u/t]} \]

and

\[ \frac{(\forall u P[u/t])^{\alpha}}{P[u/t]} \]
\[ \frac{\forall t P}{\forall u P[u/t] \Rightarrow \forall t P} \]

Here is now a proof (intuitionistic) of
\[ \exists t (P \Rightarrow Q) \Rightarrow (\forall t P \Rightarrow Q), \]
where \( t \) does not occur (free or bound) in \( Q \).

\[ \frac{(\exists t (P \Rightarrow Q))^z}{P[u/t]} \]
\[ \frac{(\forall t P)^{y}}{Q} \]
\[ \frac{(P[u/t] \Rightarrow Q)^x}{Q} \]
\[ \frac{Q}{\forall t P \Rightarrow Q} \]
\[ \frac{\exists t (P \Rightarrow Q) \Rightarrow (\forall t P \Rightarrow Q)}{x (\exists\text{-elim})} \]

In the above proof, \( u \) is a new variable that does not occur in \( Q, \forall t P, \) or \( \exists t (P \Rightarrow Q) \). Because \( t \) does not occur in \( Q \), we have
\[ (P \Rightarrow Q)[u/t] = P[u/t] \Rightarrow Q. \]

The converse requires (RAA) and is a bit more complicated. Here is a classical proof:
Next, we give intuitionistic proofs of

\((\exists tP \land Q) \Rightarrow \exists t(P \land Q)\)

and

\(\exists t(P \land Q) \Rightarrow (\exists tP \land Q),\)

where \(t\) does not occur (free or bound) in \(Q\).

Here is an intuitionistic proof of the first implication:

\[
\frac{(\exists tP \land Q)^x}{P[u/t]^y} \quad \frac{(\exists tP \land Q)^x}{\exists tP} \quad \frac{P[u/t] \land Q}{\exists t(P \land Q)} \quad \frac{\exists t(P \land Q)}{(\exists tP \land Q) \Rightarrow \exists t(P \land Q)}
\]

In the above proof, \(u\) is a new variable that does not occur in \(\exists tP\) or \(Q\). Because \(t\) does not occur in \(Q\), we have

\( (P \land Q)[u/t] = P[u/t] \land Q.\)

Here is an intuitionistic proof of the converse:
Finally, we give a proof (intuitionistic) of  

\[(\forall t P \lor Q) \Rightarrow \forall t (P \lor Q),\]

where \(t\) does not occur (free or bound) in \(Q\).

In the above proof, \(u\) is a new variable that does not occur in \(\forall t P\) or \(Q\). Because \(t\) does not occur in \(Q\), we have  

\[(P \lor Q)[u/t] = P[u/t] \lor Q.\]

The converse requires (RAA).

The useful above equivalences (and more) are summarized in the following propositions.

**Proposition 2.14.** (1) The following equivalences are provable in classical first-order logic, provided that \(t\) does not occur (free or bound) in \(Q\).

\[
\begin{align*}
\forall t P \land Q &\equiv \forall t (P \land Q) \\
\exists t P \lor Q &\equiv \exists t (P \lor Q) \\
\exists t P \land Q &\equiv \exists t (P \land Q) \\
\forall t P \lor Q &\equiv \forall t (P \lor Q).
\end{align*}
\]

Furthermore, the first three are provable intuitionistically and so is \((\forall t P \lor Q) \Rightarrow \forall t (P \lor Q)\).

(2) The following equivalences are provable in classical logic, provided that \(t\) does not occur (free or bound) in \(P\).

\[
\begin{align*}
\forall t (P \Rightarrow Q) &\equiv (P \Rightarrow \forall t Q) \\
\exists t (P \Rightarrow Q) &\equiv (P \Rightarrow \exists t Q).
\end{align*}
\]
2.15. ADDING QUANTIFIERS; PROOF SYSTEMS $\mathcal{N}_C^{\Rightarrow,\land,\lor,\neg,\exists,\forall}$, $\mathcal{NG}_C^{\Rightarrow,\land,\lor,\neg,\exists,\forall}$  

Furthermore, the first one is provable intuitionistically and so is $\exists t (P \Rightarrow Q) \Rightarrow (P \Rightarrow \exists t Q)$.

(3) The following equivalences are provable in classical logic, provided that $t$ does not occur (free or bound) in $Q$.

$$\forall t (P \Rightarrow Q) \equiv (\exists t P \Rightarrow Q)$$

$$\exists t (P \Rightarrow Q) \equiv (\forall t P \Rightarrow Q).$$

Furthermore, the first one is provable intuitionistically and so is $\exists t (P \Rightarrow Q) \Rightarrow (\forall t P \Rightarrow Q)$.

Proofs that have not been supplied are left as exercises.

Obviously, every first-order formula that is provable intuitionistically is also provable classically and we know that there are formulae that are provable classically but not provable intuitionistically. Therefore, it appears that classical logic is more general than intuitionistic logic. However, this not not quite so because there is a way of translating classical logic into intuitionistic logic. To be more precise, every classical formula $A$ can be translated into a formula $A^*$ where $A^*$ is classically equivalent to $A$ and $A$ is provable classically iff $A^*$ is provable intuitionistically. Various translations are known, all based on a “trick” involving double-negation (This is because $\neg\neg\neg A$ and $\neg A$ are intuitionistically equivalent).

Translations were given by Kolmogorov (1925), Gödel (1933), and Gentzen (1933).

For example, Gödel used the following translation.

$$A^* = \neg \neg A,$$  

$$\neg A^* = \neg \neg A,$$  

$$(A \land B)^* = (A^* \land B^*),$$  

$$(A \Rightarrow B)^* = (A^* \Rightarrow \neg B^*),$$  

$$(A \lor B)^* = (A^* \lor \neg B^*),$$  

$$\forall x A^* = \forall x A^*,$$  

$$\exists x A^* = \exists x \neg A^*.$$  

Actually, if we restrict our attention to propositions (i.e., formulae without quantifiers), a theorem of V. Glivenko (1929) states that if a proposition $A$ is provable classically, then $\neg \neg A$ is provable intuitionistically. In view of these results, the proponents of intuitionistic
logic claim that classical logic is really a special case of intuitionistic logic. However, the
above translations have some undesirable properties, as noticed by Girard. For more details
on all this, see Gallier [6].

2.16 First-Order Theories

The way we presented deduction trees and proof trees may have given our readers the
impression that the set of premises Γ was just an auxiliary notion. Indeed, in all of our
examples, Γ ends up being empty. However, nonempty Γs are crucially needed if we want to
develop theories about various kinds of structures and objects, such as the natural numbers,
groups, rings, fields, trees, graphs, sets, and the like. Indeed, we need to make definitions
about the objects we want to study and we need to state some axioms asserting the main
properties of these objects. We do this by putting these definitions and axioms in Γ. Actually,
we have to allow Γ to be infinite but we still require that our deduction trees be finite; they
can only use finitely many of the formulae in Γ. We are then interested in all formulæ P
such that ∆ → P is provable, where ∆ is any finite subset of Γ; the set of all such Ps is
called a theory (or first-order theory). Of course we have the usual problem of consistency:
if we are not careful, our theory may be inconsistent, that is, it may consist of all formulæ.

Let us give two examples of theories.

Our first example is the theory of equality. Indeed, our readers may have noticed that
we have avoided dealing with the equality relation. In practice, we can’t do that.

Given a language L with a given supply of constant, function, and predicate symbols,
the theory of equality consists of the following formulæ taken as axioms.

∀x(x = x)
∀x₁⋯∀xₙ∀y₁⋯∀yₙ[(x₁ = y₁ ∧ ⋮ ∧ xₙ = yₙ) ⇒ f(x₁, ⋮, xₙ) = f(y₁, ⋮, yₙ)]
∀x₁⋯∀xₙ∀y₁⋯∀yₙ[(x₁ = y₁ ∧ ⋮ ∧ xₙ = yₙ) ∧ P(x₁, ⋮, xₙ) ⇒ P(y₁, ⋮, yₙ)],

for all function symbols (of n arguments) and all predicate symbols (of n arguments), in-
cluding the equality predicate, =, itself.

It is not immediately clear from the above axioms that = is symmetric and transitive
but this can be shown easily.

Our second example is the first-order theory of the natural numbers known as Peano
arithmetic (for short, PA).

In this case the language L consists of the nonlogical symbols \{0,S,+,*,=\}. Here,
we have the constant 0 (zero), the unary function symbol S (for successor function; the
intended meaning is S(n) = n + 1) and the binary function symbols + (for addition) and
* (for multiplication). In addition to the axioms for the theory of equality we have the
following axioms:

\[
\begin{align*}
\forall x & \neg(S(x) = 0) \\
\forall x \forall y (S(x) = S(y) \Rightarrow x = y) \\
\forall x (x + 0 = x) \\
\forall x \forall y (x + S(y) = S(x + y)) \\
\forall x (x \times 0 = 0) \\
\forall x \forall y (x \times S(y) = x \times y + x) \\
[A(0) \land \forall x (A(x) \Rightarrow A(S(x)))] \Rightarrow \forall n A(n),
\end{align*}
\]

where \( A \) is any first-order formula with one free variable.

This last axiom is the induction axiom. Observe how + and \( \times \) are defined recursively in terms of 0 and \( S \) and that there are infinitely many induction axioms (countably many).

Many properties that hold for the natural numbers (i.e., are true when the symbols 0, S, +, \( \times \) have their usual interpretation and all variables range over the natural numbers) can be proven in this theory (Peano arithmetic), but not all. This is another very famous result of Gödel known as Gödel’s incompleteness theorem (1931). However, the topic of incompleteness is definitely outside the scope in this book, so we do not say any more about it.

However, we feel that it should be instructive for the reader to see how simple properties of the natural numbers can be derived (in principle) in Peano arithmetic.
First it is convenient to introduce abbreviations for the terms of the form \( S^n(0) \), which represent the natural numbers. Thus, we add a countable supply of constants, 0, 1, 2, 3, ..., to denote the natural numbers and add the axioms

\[
n = S^n(0),
\]

for all natural numbers \( n \). We also write \( n + 1 \) for \( S(n) \).

Let us illustrate the use of the quantifier rules involving terms (\( \forall \)-elimination and \( \exists \)-introduction) by proving some simple properties of the natural numbers, namely, being even or odd. We also prove a property of the natural number that we used before (in the proof that \( \sqrt{2} \) is irrational), namely, that every natural number is either even or odd. For this, we add the predicate symbols, “even” and “odd”, to our language, and assume the following axioms defining these predicates:

\[
\begin{align*}
\forall n (\text{even}(n) & \equiv \exists k (n = 2 \cdot k)) \\
\forall n (\text{odd}(n) & \equiv \exists k (n = 2 \cdot k + 1)).
\end{align*}
\]

Consider the term, \( 2 \cdot (m + 1) \cdot (m + 2) + 1 \), where \( m \) is any given natural number. We need a few preliminary results.

**Proposition 2.15.** The statement \( \text{odd}(2 \cdot (m + 1) \cdot (m + 2) + 1) \) is provable in Peano arithmetic.

As an auxiliary lemma, we first prove

**Proposition 2.16.** The formula

\[
\forall x \text{ odd}(2 \cdot x + 1)
\]

is provable in Peano arithmetic.

**Proof.** Let \( p \) be a variable not occurring in any of the axioms of Peano arithmetic (the variable \( p \) stands for an arbitrary natural number). From the axiom,

\[
\forall n (\text{odd}(n) \equiv \exists k (n = 2 \cdot k + 1)),
\]

by \( \forall \)-elimination where the term \( 2 \cdot p + 1 \) is substituted for the variable \( n \) we get

\[
\text{odd}(2 \cdot p + 1) \equiv \exists k (2 \cdot p + 1 = 2 \cdot k + 1).
\]

Now we can think of the provable equation \( 2 \cdot p + 1 = 2 \cdot k + 1 \) as

\[
(2 \cdot p + 1 = 2 \cdot k + 1)[p/k],
\]

so by \( \exists \)-introduction, we can conclude that

\[
\exists k (2 \cdot p + 1 = 2 \cdot k + 1),
\]
which, by (⋆), implies that
\[ \text{odd}(2 \cdot p + 1). \]

But now, because \( p \) is a variable not occurring free in the axioms of Peano arithmetic, by \( \forall \)-introduction, we conclude that
\[ \forall x \text{ odd}(2 \cdot x + 1), \]
as claimed.

Proof of Proposition 2.15. If we use \( \forall \)-elimination in the above formula where we substitute the term, \( \tau = (m + 1) \cdot (m + 2) \), for \( x \), we get
\[ \text{odd}(2 \cdot (m + 1) \cdot (m + 2) + 1), \]
as claimed.

Now we wish to prove

**Proposition 2.17.** The formula
\[ \forall n (\text{even}(n) \lor \text{odd}(n)) \]
is provable in Peano arithmetic.

Proof. We use the induction principle of Peano arithmetic with
\[ A(n) = \text{even}(n) \lor \text{odd}(n). \]

For the base case, \( n = 0 \), because \( 0 = 2 \cdot 0 \) (which can be proven from the Peano axioms), we see that \( \text{even}(0) \) holds and so \( \text{even}(0) \lor \text{odd}(0) \) is proven.

For \( n = 1 \), because \( 1 = 2 \cdot 0 + 1 \) (which can be proven from the Peano axioms), we see that \( \text{odd}(1) \) holds and so \( \text{even}(1) \lor \text{odd}(1) \) is proven.

For the induction step, we may assume that \( A(n) \) has been proven and we need to prove that \( A(n + 1) \) holds.

So, assume that \( \text{even}(n) \lor \text{odd}(n) \) holds. We do a proof by cases.

(a) If \( \text{even}(n) \) holds, by definition this means that \( n = 2k \) for some \( k \) and then, \( n + 1 = 2k + 1 \), which again, by definition means that \( \text{odd}(n + 1) \) holds and thus, \( \text{even}(n + 1) \lor \text{odd}(n + 1) \) holds.

(b) If \( \text{odd}(n) \) holds, by definition this means that \( n = 2k + 1 \) for some \( k \) and then, \( n + 1 = 2k + 2 = 2(k + 1) \), which again, by definition means that \( \text{even}(n + 1) \) holds and thus, \( \text{even}(n + 1) \lor \text{odd}(n + 1) \) holds.

By \( \lor \)-elimination, we conclude that \( \text{even}(n + 1) \lor \text{odd}(n + 1) \) holds, establishing the induction step.

Therefore, using induction, we have proven that
\[ \forall n (\text{even}(n) \lor \text{odd}(n)), \]
as claimed.
Actually, we can show that even\((n)\) and odd\((n)\) are mutually exclusive as we now prove.

**Proposition 2.18.** The formula

\[
\forall n \neg (\text{even}(n) \land \text{odd}(n))
\]

is provable in Peano arithmetic.

**Proof.** We prove this by induction. For \(n = 0\), the statement odd\((0)\) means that \(0 = 2k + 1 = S(2k)\), for some \(k\). However, the first axiom of Peano arithmetic states that \(S(x) \neq 0\) for all \(x\), so we get a contradiction.

For the induction step, assume that \(\neg (\text{even}(n) \land \text{odd}(n))\) holds. We need to prove that \(\neg (\text{even}(n + 1) \land \text{odd}(n + 1))\) holds, and we can do this by using our constructive proof-by-contradiction rule. So, assume that \(\text{even}(n + 1) \land \text{odd}(n + 1)\) holds. At this stage, we realize that if we could prove that

\[
\forall n (\text{even}(n + 1) \Rightarrow \text{odd}(n))
\]

and

\[
\forall n (\text{odd}(n + 1) \Rightarrow \text{even}(n))
\]

then \(\text{even}(n + 1) \land \text{odd}(n + 1)\) would imply \(\text{even}(n) \land \text{odd}(n)\), contradicting the assumption \(\neg (\text{even}(n) \land \text{odd}(n))\). Therefore, the proof is complete if we can prove \((\ast)\) and \((\ast\ast)\).

Let’s consider the implication \((\ast)\) leaving the proof of \((\ast\ast)\) as an exercise.

Assume that \(\text{even}(n + 1)\) holds. Then \(n + 1 = 2k\), for some natural number \(k\). We can’t have \(k = 0\) because otherwise we would have \(n + 1 = 0\), contradicting one of the Peano axioms. But then \(k\) is of the form \(k = h + 1\) for some natural number \(h\), so

\[
n + 1 = 2k = 2(h + 1) = 2h + 2 = (2h + 1) + 1.
\]

By the second Peano axiom, we must have

\[
n = 2h + 1,
\]

which proves that \(n\) is odd, as desired.

In that last proof, we made implicit use of the fact that every natural number \(n\) different from zero is of the form \(n = m + 1\), for some natural number \(m\) which is formalized as

\[
\forall n ((n \neq 0) \Rightarrow \exists m (n = m + 1)).
\]

This is easily proven by induction.

Having done all this work, we have finally proven \((\ast)\) and after proving \((\ast\ast)\), we will have proven that

\[
\forall n \neg (\text{even}(n) \land \text{odd}(n)),
\]

as claimed. \(\Box\)
It is also easy to prove that

\[ \forall n (\text{even}(n) \lor \text{odd}(n)) \]

and

\[ \forall n \neg (\text{even}(n) \land \text{odd}(n)) \]

together imply that

\[ \forall n (\text{even}(n) \equiv \neg \text{odd}(n)) \quad \text{and} \quad \forall n (\text{odd}(n) \equiv \neg \text{even}(n)) \]

are provable, facts that we used several times in Section 2.9. This is because, if

\[ \forall x (P \lor Q) \quad \text{and} \quad \forall x \neg (P \land Q) \]

can be deduced intuitionistically from a set of premises, \( \Gamma \), then

\[ \forall x (P \equiv \neg Q) \quad \text{and} \quad \forall x (Q \equiv \neg P) \]

can also be deduced intuitionistically from \( \Gamma \). In this case it also follows that \( \forall x (\neg \neg P \equiv P) \) and \( \forall x (\neg \neg Q \equiv Q) \) can be deduced intuitionistically from \( \Gamma \).

**Remark:** Even though we proved that every nonzero natural number \( n \) is of the form \( n = m + 1 \), for some natural number \( m \), the expression \( n - 1 \) does not make sense because the predecessor function \( n \mapsto n - 1 \) has not been defined yet in our logical system. We need to define a function symbol “pred” satisfying the axioms:

\[
\begin{align*}
\text{pred}(0) &= 0 \\
\forall n (\text{pred}(n + 1) &= n).
\end{align*}
\]

For simplicity of notation, we write \( n - 1 \) instead of \( \text{pred}(n) \). Then we can prove that if \( k \neq 0 \), then \( 2k - 1 = 2(k - 1) + 1 \) (which really should be written as \( \text{pred}(2k) = 2\text{pred}(k) + 1 \)). This can indeed be done by induction; we leave the details as an exercise. We can also define substraction, \( - \), as a function satisfying the axioms

\[
\begin{align*}
\forall n (n - 0 &= n) \\
\forall n \forall m (n - (m + 1) &= \text{pred}(n - m)).
\end{align*}
\]

It is then possible to prove the usual properties of substraction (by induction).

These examples of proofs in the theory of Peano arithmetic illustrate the fact that constructing proofs in an axiomatized theory is a very laborious and tedious process. Many small technical lemmas need to be established from the axioms, which renders these proofs very lengthy and often unintuitive. It is therefore important to build up a database of useful basic facts if we wish to prove, with a certain amount of comfort, properties of objects whose properties are defined by an axiomatic theory (such as the natural numbers). However, when
in doubt, we can always go back to the formal theory and try to prove rigorously the facts that we are not sure about, even though this is usually a tedious and painful process. Human provers navigate in a “spectrum of formality,” most of the time constructing informal proofs containing quite a few (harmless) shortcuts, sometimes making extra efforts to construct more formalized and rigorous arguments if the need arises.

Now what if the theory of Peano arithmetic were inconsistent! How do know that Peano arithmetic does not imply any contradiction? This is an important and hard question that motivated a lot of the work of Gentzen. An easy answer is that the standard model $\mathbb{N}$ of the natural numbers under addition and multiplication validates all the axioms of Peano arithmetic. Therefore, if both $P$ and $\neg P$ could be proven from the Peano axioms, then both $P$ and $\neg P$ would be true in $\mathbb{N}$, which is absurd. To make all this rigorous, we need to define the notion of truth in a structure, a notion explained in every logic book. It should be noted that the constructivists will object to the above method for showing the consistency of Peano arithmetic, because it assumes that the infinite set $\mathbb{N}$ exists as a completed entity. Until further notice, we have faith in the consistency of Peano arithmetic (so far, no inconsistency has been found).

Another very interesting theory is set theory. There are a number of axiomatizations of set theory and we discuss one of them (ZF) very briefly in Section 2.17.

2.17 Basics Concepts of Set Theory

Having learned some fundamental notions of logic, it is now a good place before proceeding to more interesting things, such as functions and relations, to go through a very quick review of some basic concepts of set theory. This section takes the very “naive” point of view that a set is an unordered collection of objects, without duplicates, the collection being regarded as a single object. Having first-order logic at our disposal, we could formalize set theory very rigorously in terms of axioms. This was done by Zermelo first (1908) and in a more satisfactory form by Zermelo and Fraenkel in 1921, in a theory known as the “Zermelo–Fraenkel” (ZF) axioms. Another axiomatization was given by John von Neumann in 1925 and later improved by Bernays in 1937. A modification of Bernay’s axioms was used by Kurt Gödel in 1940. This approach is now known as “von Neumann–Bernays” (VNB) or “Gödel–Bernays” (GB) set theory. There are many books that give an axiomatic presentation of set theory. Among them, we recommend Enderton [3], which we find remarkably clear and elegant, Suppes [21] (a little more advanced), and Halmos [12], a classic (at a more elementary level).

However, it must be said that set theory was first created by Georg Cantor (1845–1918) between 1871 and 1879. However, Cantor’s work was not unanimously well received by all mathematicians.

Cantor regarded infinite objects as objects to be treated in much the same way as finite sets, a point of view that was shocking to a number of very prominent mathematicians who bitterly attacked him (among them, the powerful Kronecker). Also, it turns out that some paradoxes in set theory popped up in the early 1900s, in particular, Russell’s paradox.
2.17. BASICS CONCEPTS OF SET THEORY

Figure 2.15: Ernst F. Zermelo, 1871–1953 (left), Adolf A. Fraenkel, 1891–1965 (middle left), John von Neumann, 1903–1957 (middle right) and Paul I. Bernays, 1888–1977 (right)

Figure 2.16: Georg F. L. P. Cantor, 1845–1918

Russell’s paradox (found by Russell in 1902) has to do with the “set of all sets that are not members of themselves,” which we denote by

\[ R = \{ x \mid x \notin x \}. \]

(In general, the notation \( \{ x \mid P \} \) stand for the set of all objects satisfying the property \( P \).)

Now, classically, either \( R \in R \) or \( R \notin R \). However, if \( R \in R \), then the definition of \( R \) says that \( R \notin R \); if \( R \notin R \), then again, the definition of \( R \) says that \( R \in R \). So, we have a contradiction and the existence of such a set is a paradox. The problem is that we are allowing a property (here, \( P(x) = x \notin x \)), which is “too wild” and circular in nature. As we show, the way out, as found by Zermelo, is to place a restriction on the

Figure 2.17: Bertrand A. W. Russell, 1872–1970
property $P$ and to also make sure that $P$ picks out elements from some already given set (see the subset axioms below).

The apparition of these paradoxes prompted mathematicians, with Hilbert among its leaders, to put set theory on firmer ground. This was achieved by Zermelo, Fraenkel, von Neumann, Bernays, and Gödel, to name only the major players.

In what follows, we are assuming that we are working in classical logic. The language $L$ of set theory consists of the symbols $\{\emptyset, \in, =\}$, where $\emptyset$ is a constant symbol (corresponding to the empty set) and $\in$ is binary predicate symbol (denoting set membership). Instead of writing $\in (a, A)$, we write $a \in A$ ($a$ belongs to the set $A$). Instead of $\neg (a \in A)$, we write $a \notin A$.

We introduce various operations on sets using definitions involving the logical connectives $\land$, $\lor$, $\neg$, $\forall$, and $\exists$.

In order to ensure the existence of some of these sets requires some of the axioms of set theory, but we are rather casual about that.

When are two sets $A$ and $B$ equal? This corresponds to the first axiom of set theory, called the

**Extensionality Axiom**
Two sets $A$ and $B$ are equal iff they have exactly the same elements; that is,

$$\forall x (x \in A \Rightarrow x \in B) \land \forall x (x \in B \Rightarrow x \in A).$$

The above says: every element of $A$ is an element of $B$ and conversely.

There is a special set having no elements at all, the *empty set*, denoted $\emptyset$. This is the following.

**Empty Set Axiom** There is a set having no members. This set is denoted $\emptyset$ and it is characterized by the property

$$\forall x (x \notin \emptyset).$$

**Remark:** Beginners often wonder whether there is more than one empty set. For example, is the empty set of professors distinct from the empty set of potatoes?

The answer is, by the extensionality axiom, there is only one empty set.

Given any two objects $a$ and $b$, we can form the set $\{a, b\}$ containing exactly these two objects. Amazingly enough, this must also be an axiom:

**Pairing Axiom**
Given any two objects $a$ and $b$ (think sets), there is a set $\{a, b\}$ having as members just $a$ and $b$.

Observe that if $a$ and $b$ are identical, then we have the set $\{a, a\}$, which is denoted by $\{a\}$ and is called a *singleton set* (this set has $a$ as its only element).

To form bigger sets, we use the union operation. This too requires an axiom.

**Union Axiom (Version 1)**
For any two sets $A$ and $B$, there is a set $A \cup B$ called the union of $A$ and $B$ defined by

$$x \in A \cup B \text{ iff } (x \in A) \lor (x \in B).$$

This reads, $x$ is a member of $A \cup B$ if either $x$ belongs to $A$ or $x$ belongs to $B$ (or both). We also write

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

Using the union operation, we can form bigger sets by taking unions with singletons. For example, we can form

$$\{a, b, c\} = \{a, b\} \cup \{c\}.$$

**Remark:** We can systematically construct bigger and bigger sets by the following method:

Given any set $A$ let

$$A^+ = A \cup \{A\}.$$  

If we start from the empty set, we obtain sets that can be used to define the natural numbers and the $+$ operation corresponds to the successor function on the natural numbers (i.e., $n \mapsto n + 1$).

Another operation is the power set formation. It is indeed a “powerful” operation, in the sense that it allows us to form very big sets. For this, it is helpful to define the notion of inclusion between sets. Given any two sets, $A$ and $B$, we say that $A$ is a subset of $B$ (or that $A$ is included in $B$), denoted $A \subseteq B$, iff every element of $A$ is also an element of $B$, that is,

$$\forall x (x \in A \Rightarrow x \in B).$$

We say that $A$ is a proper subset of $B$ iff $A \subseteq B$ and $A \neq B$. This implies that that there is some $b \in B$ with $b \notin A$. We usually write $A \subset B$.

Observe that the equality of two sets can be expressed by

$$A = B \text{ iff } A \subseteq B \text{ and } B \subseteq A.$$  

**Power Set Axiom**

Given any set $A$, there is a set $\mathcal{P}(A)$ (also denoted $2^A$) called the power set of $A$ whose members are exactly the subsets of $A$; that is,

$$X \in \mathcal{P}(A) \text{ iff } X \subseteq A.$$  

For example, if $A = \{a, b, c\}$, then

$$\mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\},$$

a set containing eight elements. Note that the empty set and $A$ itself are always members of $\mathcal{P}(A)$.  

Remark: If $A$ has $n$ elements, it is not hard to show that $\mathcal{P}(A)$ has $2^n$ elements. For this reason, many people, including me, prefer the notation $2^A$ for the power set of $A$.

At this stage, we define intersection and complementation. For this, given any set $A$ and given a property $P$ (specified by a first-order formula) we need to be able to define the subset of $A$ consisting of those elements satisfying $P$. This subset is denoted by

$$\{x \in A \mid P\}.$$ 

Unfortunately, there are problems with this construction. If the formula $P$ is somehow a circular definition and refers to the subset that we are trying to define, then some paradoxes may arise.

The way out is to place a restriction on the formula used to define our subsets, and this leads to the subset axioms, first formulated by Zermelo. These axioms are also called comprehension axioms or axioms of separation.

Subset Axioms

For every first-order formula $P$ we have the axiom:

$$\forall A \exists X \forall x (x \in X \iff (x \in A) \land P),$$

where $P$ does not contain $X$ as a free variable. (However, $P$ may contain $x$ free.)

The subset axioms says that for every set $A$ there is a set $X$ consisting exactly of those elements of $A$ so that $P$ holds. For short, we usually write

$$X = \{x \in A \mid P\}.$$ 

As an example, consider the formula

$$P(B, x) = x \in B.$$ 

Then, the subset axiom says

$$\forall A \exists X \forall x (x \in A \land x \in B),$$

which means that $X$ is the set of elements that belong both to $A$ and $B$. This is called the intersection of $A$ and $B$, denoted by $A \cap B$. Note that

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

We can also define the relative complement of $B$ in $A$, denoted $A - B$, given by the formula $P(B, x) = x \notin B$, so that

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

In particular, if $A$ is any given set and $B$ is any subset of $A$, the set $A - B$ is also denoted $\overline{B}$ and is called the complement of $B$.

The algebraic properties of union, intersection, and complementation are inherited from the properties of disjunction, conjunction, and negation. The following proposition lists some of the most important properties of union, intersection, and complementation.
Proposition 2.19. The following equations hold for all sets $A, B, C$:

\[
\begin{align*}
A \cup \emptyset &= A \\
A \cap \emptyset &= \emptyset \\
A \cup A &= A \\
A \cap A &= A \\
A \cup B &= B \cup A \\
A \cap B &= B \cap A.
\end{align*}
\]

The last two assert the commutativity of $\cup$ and $\cap$. We have distributivity of $\cap$ over $\cup$ and of $\cup$ over $\cap$:

\[
\begin{align*}
A \cap (B \cup C) &= (A \cap B) \cup (A \cap C) \\
A \cup (B \cap C) &= (A \cup B) \cap (A \cup C).
\end{align*}
\]

We have associativity of $\cap$ and $\cup$:

\[
\begin{align*}
A \cap (B \cap C) &= (A \cap B) \cap C \\
A \cup (B \cup C) &= (A \cup B) \cup C.
\end{align*}
\]

Proof. Use Proposition 2.5. \qed

Because $\land$, $\lor$, and $\neg$ satisfy the de Morgan laws (remember, we are dealing with classical logic), for any set $X$, the operations of union, intersection, and complementation on subsets of $X$ satisfy the de Morgan laws.

Proposition 2.20. For every set $X$ and any two subsets $A, B$ of $X$, the following identities (de Morgan laws) hold:

\[
\begin{align*}
\overline{A} &= A \\
\overline{(A \cap B)} &= \overline{A} \cup \overline{B} \\
\overline{(A \cup B)} &= \overline{A} \cap \overline{B}.
\end{align*}
\]

So far, the union axiom only applies to two sets but later on we need to form infinite unions. Thus, it is necessary to generalize our union axiom as follows.

Union Axiom (Final Version)

Given any set $X$ (think of $X$ as a set of sets), there is a set $\cup X$ defined so that

\[
x \in \bigcup X \quad \text{iff} \quad \exists B (B \in X \land x \in B).
\]

This says that $\bigcup X$ consists of all elements that belong to some member of $X$. 


If we take \( X = \{A, B\} \), where \( A \) and \( B \) are two sets, we see that
\[
\bigcup \{A, B\} = A \cup B,
\]
and so, our final version of the union axiom subsumes our previous union axiom which we now discard in favor of the more general version.

Observe that
\[
\bigcup \{A\} = A, \quad \bigcup \{A_1, \ldots, A_n\} = A_1 \cup \cdots \cup A_n.
\]
and in particular, \( \bigcup \emptyset = \emptyset \).

Using the subset axioms, we can also define infinite intersections. For every nonempty set \( X \) there is a set \( \bigcap X \) defined by
\[
x \in \bigcap X \iff \forall B (B \in X \Rightarrow x \in B).
\]

The existence of \( \bigcap X \) is justified as follows: Because \( X \) is nonempty, it contains some set, \( A \); let
\[
P(X, x) = \forall B (B \in X \Rightarrow x \in B).
\]
Then, the subset axioms asserts the existence of a set \( Y \) so that for every \( x \),
\[
x \in Y \iff x \in A \quad \text{and} \quad P(X, x)
\]
which is equivalent to
\[
x \in Y \iff P(X, x).
\]
Therefore, the set \( Y \) is our desired set, \( \bigcap X \).

Observe that
\[
\bigcap \{A, B\} = A \cap B, \quad \bigcap \{A_1, \ldots, A_n\} = A_1 \cap \cdots \cap A_n.
\]
Note that \( \bigcap \emptyset \) is not defined. Intuitively, it would have to be the set of all sets, but such a set does not exist, as we now show. This is basically a version of Russell’s paradox.

**Theorem 2.21.** (Russell) There is no set of all sets, that is, there is no set to which every other set belongs.

**Proof.** Let \( A \) be any set. We construct a set \( B \) that does not belong to \( A \). If the set of all sets existed, then we could produce a set that does not belong to it, a contradiction. Let
\[
B = \{a \in A \mid a \notin a\}.
\]
We claim that \( B \notin A \). We proceed by contradiction, so assume \( B \in A \). However, by the definition of \( B \), we have
\[
B \in B \iff B \in A \quad \text{and} \quad B \notin B.
\]
Because $B \in A$, the above is equivalent to

$$B \in B \iff B \notin B,$$

which is a contradiction. Therefore, $B \notin A$ and we deduce that there is no set of all sets. \qed

Remarks:

(1) We should justify why the equivalence $B \in B$ iff $B \notin B$ is a contradiction. What we mean by “a contradiction” is that if the above equivalence holds, then we can derive $\bot$ (falsity) and thus, all propositions become provable. This is because we can show that for any proposition $P$ if $P \equiv \neg P$ is provable, then every proposition is provable. We leave the proof of this fact as an easy exercise for the reader. By the way, this holds classically as well as intuitionistically.

(2) We said that in the subset axioms, the variable $X$ is not allowed to occur free in $P$. A slight modification of Russell’s paradox shows that allowing $X$ to be free in $P$ leads to paradoxical sets. For example, pick $A$ to be any nonempty set and set $P(X, x) = x \notin X$. Then, look at the (alleged) set

$$X = \{x \in A \mid x \notin X\}.$$

As an exercise, the reader should show that $X$ is empty iff $X$ is nonempty,

This is as far as we can go with the elementary notions of set theory that we have introduced so far. In order to proceed further, we need to define relations and functions, which is the object of the next chapter.

The reader may also wonder why we have not yet discussed infinite sets. This is because we don’t know how to show that they exist. Again, perhaps surprisingly, this takes another axiom, the *axiom of infinity*. We also have to define when a set is infinite. However, we do not go into this right now. Instead, we accept that the set of natural numbers $\mathbb{N}$ exists and is infinite. Once we have the notion of a function, we will be able to show that other sets are infinite by comparing their “size” with that of $\mathbb{N}$ (This is the purpose of *cardinal numbers*, but this would lead us too far afield).

Remark: In an axiomatic presentation of set theory, the natural numbers can be defined from the empty set using the operation $A \mapsto A^+ = A \cup \{A\}$ introduced just after the union axiom. The idea due to von Neumann is that the natural numbers, 0, 1, 2, 3, \ldots, can be
viewed as concise notations for the following sets.

\[
\begin{align*}
0 &= \emptyset \\
1 &= 0^+ = \{\emptyset\} = \{0\} \\
2 &= 1^+ = \{\emptyset, \{\emptyset\}\} = \{0, 1\} \\
3 &= 2^+ = \{\emptyset, \emptyset, \emptyset, \emptyset\} = \{0, 1, 2\} \\
& \vdots \\
n + 1 &= n^+ = \{0, 1, 2, \ldots, n\} \\
& \vdots
\end{align*}
\]

However, the above subsumes induction. Thus, we have to proceed in a different way to avoid circularities.

**Definition 2.17.** We say that a set \(X\) is **inductive** iff

1. \(\emptyset \in X\).
2. For every \(A \in X\), we have \(A^+ \in X\).

**Axiom of Infinity**

There is some inductive set.

Having done this, we make the following.

**Definition 2.18.** A **natural number** is a set that belongs to every inductive set.

Using the subset axioms, we can show that there is a set whose members are exactly the natural numbers. The argument is very similar to the one used to prove that arbitrary intersections exist. By the axiom of infinity, there is some inductive set, say \(A\). Now consider the property \(P(x)\) which asserts that \(x\) belongs to every inductive set. By the subset axioms applied to \(P\), there is a set, \(\mathbb{N}\), such that

\[
x \in \mathbb{N} \iff x \in A \text{ and } P(x)
\]
and because $A$ is inductive and $P$ says that $x$ belongs to every inductive set, the above is equivalent to
\[ x \in \mathbb{N} \quad \text{iff} \quad P(x); \]
that is, $x \in \mathbb{N}$ iff $x$ belongs to every inductive set. Therefore, the set of all natural numbers $\mathbb{N}$ does exist. The set $\mathbb{N}$ is also denoted $\omega$. We can now easily show the following.

**Theorem 2.22.** The set $\mathbb{N}$ is inductive and it is a subset of every inductive set.

**Proof.** Recall that $\emptyset$ belongs to every inductive set; so, $\emptyset$ is a natural number (0). As $\mathbb{N}$ is the set of natural numbers, $\emptyset (= 0)$ belongs to $\mathbb{N}$. Secondly, if $n \in \mathbb{N}$, this means that $n$ belongs to every inductive set ($n$ is a natural number), which implies that $n^+ = n + 1$ belongs to every inductive set, which means that $n + 1$ is a natural number, that is, $n + 1 \in \mathbb{N}$. Because $\mathbb{N}$ is the set of natural numbers and because every natural number belongs to every inductive set, we conclude that $\mathbb{N}$ is a subset of every inductive set. \qed

It would be tempting to view $\mathbb{N}$ as the intersection of the family of inductive sets, but unfortunately this family is not a set; it is too “big” to be a set.

As a consequence of the above fact, we obtain the following.

**Induction Principle for $\mathbb{N}$:** Any inductive subset of $\mathbb{N}$ is equal to $\mathbb{N}$ itself.

Now, in our setting, $0 = \emptyset$ and $n^+ = n + 1$, so the above principle can be restated as follows.

**Induction Principle for $\mathbb{N}$ (Version 2):** For any subset, $S \subseteq \mathbb{N}$, if $0 \in S$ and $n + 1 \in S$ whenever $n \in S$, then $S = \mathbb{N}$.

We show how to rephrase this induction principle a little more conveniently in terms of the notion of function in the next chapter.

**Remarks:**

1. We still don’t know what an infinite set is or, for that matter, that $\mathbb{N}$ is infinite.

2. Zermelo–Fraenkel set theory (+ Choice) has three more axioms that we did not discuss: The axioms of choice, the replacement axioms and the regularity axiom. For our purposes, only the axiom of choice is needed. Let us just say that the replacement axioms are needed to deal with ordinals and cardinals and that the regularity axiom is needed to show that every set is grounded. For more about these axioms, see Enderton [3], Chapter 7. The regularity axiom also implies that no set can be a member of itself, an eventuality that is not ruled out by our current set of axioms.

As we said at the beginning of this section, set theory can be axiomatized in first-order logic. To illustrate the generality and expressiveness of first-order logic, we conclude this section by stating the axioms of Zermelo–Fraenkel set theory (for short, $ZF$) as first-order formulae. The language of Zermelo–Fraenkel set theory consists of the constant $\emptyset$ (for the empty set), the equality symbol, and of the binary predicate symbol $\in$ for set membership.
It is convenient to abbreviate $\neg(x = y)$ as $x \neq y$ and $\neg(x \in y)$ as $x \notin y$. The axioms are the equality axioms plus the following seven axioms.

$$\forall A \forall B(\forall x (x \in A \equiv x \in B) \Rightarrow A = B)$$
$$\forall x (x \notin \emptyset)$$
$$\forall a \forall b \exists Z \forall x (x \in Z \equiv (x = a \lor x = b))$$
$$\forall X \exists Y \forall x (x \in Y \equiv \exists B (B \in X \land x \in B))$$
$$\forall A \exists Y \forall X (X \in Y \equiv \forall z (z \in X \Rightarrow z \in A))$$
$$\forall A \exists X \forall x (x \in X \equiv (x \in A) \land P)$$
$$\exists X (\emptyset \in X \land \forall y (y \in X \Rightarrow y \cup \{y\} \in X)),$$

where $P$ is any first-order formula that does not contain $X$ free.

- Axiom (1) is the extensionality axiom.
- Axiom (2) is the empty set axiom.
- Axiom (3) asserts the existence of a set $Y$ whose only members are $a$ and $b$. By extensionality, this set is unique and it is denoted $\{a, b\}$. We also denote $\{a, a\}$ by $\{a\}$.
- Axiom (4) asserts the existence of set $Y$ which is the union of all the sets that belong to $X$. By extensionality, this set is unique and it is denoted $\bigcup X$. When $X = \{A, B\}$, we write $\bigcup \{A, B\} = A \cup B$.
- Axiom (5) asserts the existence of set $Y$ which is the set of all subsets of $A$ (the power set of $A$). By extensionality, this set is unique and it is denoted $\mathcal{P}(A)$ or $2^A$.
- Axioms (6) are the subset axioms (or axioms of separation).
- Axiom (7) is the infinity axiom, stated using the abbreviations introduced above.

For a comprehensive treatment of axiomatic theory (including the missing three axioms), see Enderton [3] and Suppes [21].

### 2.18 Summary

The main goal of this chapter is to describe precisely the logical rules used in mathematical reasoning and the notion of a mathematical proof. A brief introduction to set theory is also provided. We decided to describe the rules of reasoning in a formalism known as a natural deduction system because the logical rules of such a system mimic rather closely the informal rules that (nearly) everybody uses when constructing a proof in everyday life. Another advantage of natural deduction systems is that it is very easy to present various versions of the rules involving negation and thus, to explain why the “proof-by-contradiction”
proof rule or the “law of the excluded middle” allow for the derivation of “nonconstructive” proofs. This is a subtle point often not even touched in traditional presentations of logic. However, inasmuch as most of our readers write computer programs and expect that their programs will not just promise to give an answer but will actually produce results, we feel that they will grasp rather easily the difference between constructive and nonconstructive proofs, and appreciate the latter, even if they are harder to find.

- We describe the syntax of propositional logic.
- The proof rules for implication are defined in a natural deduction system (Prawitz-style).
- Deductions proceed from assumptions (or premises) using inference rules.
- The process of discharging (or closing) a premise is explained. A proof is a deduction in which all the premises have been discharged.
- We explain how we can search for a proof using a combined bottom-up and top-down process.
- We propose another mechanism for describing the process of discharging a premise and this leads to a formulation of the rules in terms of sequents and to a Gentzen system.
- We introduce falsity ⊥ and negation ¬P as an abbreviation for P ⇒ ⊥. We describe the inference rules for conjunction, disjunction, and negation, in both Prawitz style and Gentzen-sequent style natural deduction systems.
- One of the rules for negation is the proof-by-contradiction rule (also known as RAA).
- We define intuitionistic and classical logic.
- We introduce the notion of a constructive (or intuitionistic) proof and discuss the two nonconstructive culprits: P ∨ ¬P (the law of the excluded middle) and ¬¬P ⇒ P (double-negation rule).
- We show that P ∨ ¬P and ¬¬P ⇒ P are provable in classical logic.
- We clear up some potential confusion involving the various versions of the rules regarding negation.
  1. RAA is not a special case of ¬-introduction.
  2. RAA is not equivalent to ⊥-elimination; in fact, it implies it.
  3. Not all propositions of the form P ∨ ¬P are provable in intuitionistic logic. However, RAA holds in intuitionistic logic plus all propositions of the form P ∨ ¬P.
  4. We define double-negation elimination.
• We present the de Morgan laws and prove their validity in classical logic.
• We present the proof-by-contrapositive rule and show that it is valid in classical logic.
• We give some examples of proofs of “real” statements.
• We give an example of a nonconstructive proof of the statement: there are two irrational numbers, \(a\) and \(b\), so that \(a^b\) is rational.
• We explain the truth-value semantics of propositional logic.
• We define the truth tables for the propositional connectives.
• We define the notions of satisfiability, unsatisfiability, validity, and tautology.
• We define the satisfiability problem and the validity problem (for classical propositional logic).
• We mention the NP-completeness of satisfiability.
• We discuss soundness (or consistency) and completeness.
• We state the soundness and completeness theorems for propositional classical logic formulated in natural deduction.
• We explain how to use counterexamples to prove that certain propositions are not provable.
• We give a brief introduction to Kripke semantics for propositional intuitionistic logic.
• We define Kripke models (based on a set of worlds).
• We define validity in a Kripke model.
• We state the the soundness and completeness theorems for propositional intuitionistic logic formulated in natural deduction.
• We add first-order quantifiers (“for all” \(\forall\) and “there exists” \(\exists\)) to the language of propositional logic and define first-order logic.
• We describe free and bound variables.
• We give inference rules for the quantifiers in Prawitz-style and Gentzen sequent-style natural deduction systems.
• We explain the eigenvariable restriction in the \(\forall\)-introduction and \(\exists\)-elimination rules.
- We prove some “de Morgan”-type rules for the quantified formulae valid in classical logic.
- We discuss the nonconstructiveness of proofs of certain existential statements.
- We explain briefly how classical logic can be translated into intuitionistic logic (the Gödel translation).
- We define first-order theories and give the example of Peano arithmetic.
- We revisit the decision problem and mention the undecidability of the decision problem for first-order logic (Church’s theorem).
- We discuss the notion of detours in proofs and the notion of proof normalization.
- We mention strong normalization.
- We mention the correspondence between propositions and types and proofs and typed λ-terms (the Curry–Howard isomorphism).
- We mention Gödel’s completeness theorem for first-order logic.
- Again, we mention the use of counterexamples.
- We mention Gödel’s incompleteness theorem.
- We present informally the axioms of Zermelo–Fraenkel set theory (ZF).
- We present Russell’s paradox, a warning against “self-referential” definitions of sets.
- We define the empty set (0), the set \{a, b\}, whose elements are a and b, the union \( A \cup B \), of two sets A and B, and the power set \( 2^A \), of A.
- We state carefully Zermelo’s subset axioms for defining the subset \( \{ x \in A \mid P \} \) of elements of a given set A satisfying a property P.
- Then, we define the intersection \( A \cap B \), and the relative complement \( A - B \), of two sets A and B.
- We also define the union \( \bigcup A \) and the intersection \( \bigcap A \), of a set of sets A.
- We show that one should avoid sets that are “too big;” in particular, we prove that there is no set of all sets.
- We define the natural numbers “a la Von Neumann.”
- We define inductive sets and state the axiom of infinity.
• We show that the natural numbers form an inductive set \( \mathbb{N} \), and thus, obtain an *induction principle for \( \mathbb{N} \).*

• We summarize the axioms of Zermelo–Fraenkel set theory in first-order logic.

**Problems**

**Problem 2.1.** (a) Give a proof of the proposition \( P \Rightarrow (Q \Rightarrow P) \) in the system \( \mathcal{N}_m^\Rightarrow \).

(b) Prove that if there are deduction trees of \( P \Rightarrow Q \) and \( Q \Rightarrow R \) from the set of premises \( \Gamma \) in the system \( \mathcal{N}_m^\Rightarrow \), then there is a deduction tree for \( P \Rightarrow R \) from \( \Gamma \) in \( \mathcal{N}_m^\Rightarrow \).

**Problem 2.2.** Give a proof of the proposition \( (P \Rightarrow Q) \Rightarrow ((P \Rightarrow (Q \Rightarrow R)) \Rightarrow (P \Rightarrow R)) \) in the system \( \mathcal{N}_m^\Rightarrow \).

**Problem 2.3.** (a) Prove the “de Morgan” laws in classical logic:

\[
\neg(P \land Q) \equiv \neg P \lor \neg Q \\
\neg(P \lor Q) \equiv \neg P \land \neg Q.
\]

(b) Prove that \( \neg(P \lor Q) \equiv \neg P \land \neg Q \) is also provable in intuitionistic logic.

(c) Prove that the proposition \( (P \land \neg Q) \Rightarrow \neg(P \Rightarrow Q) \) is provable in intuitionistic logic and \( (P \Rightarrow Q) \Rightarrow (P \land \neg Q) \) is provable in classical logic.

**Problem 2.4.** (a) Show that \( P \Rightarrow \neg \neg P \) is provable in intuitionistic logic.

(b) Show that \( \neg \neg \neg P \) and \( \neg P \) are equivalent in intuitionistic logic.

**Problem 2.5.** Recall that an integer is *even* if it is divisible by 2, that is, if it can be written as \( 2k \), where \( k \in \mathbb{Z} \). An integer is *odd* if it is not divisible by 2, that is, if it can be written as \( 2k + 1 \), where \( k \in \mathbb{Z} \). Prove the following facts.

(a) The sum of even integers is even.

(b) The sum of an even integer and of an odd integer is odd.

(c) The sum of two odd integers is even.

(d) The product of odd integers is odd.

(e) The product of an even integer with any integer is even.

**Problem 2.6.** (a) Show that if we assume that all propositions of the form

\[
P \Rightarrow (Q \Rightarrow R)
\]

are axioms (where \( P, Q, R \) are arbitrary propositions), then *every proposition* is provable.

(b) Show that if \( P \) is provable (intuitionistically or classically), then \( Q \Rightarrow P \) is also provable for *every* proposition \( Q \).
Problem 2.7. (a) Give intuitionistic proofs for the equivalences
\[
P \lor P \equiv P \\
P \land P \equiv P \\
P \lor Q \equiv Q \lor P \\
P \land Q \equiv Q \land P.
\]
(b) Give intuitionistic proofs for the equivalences
\[
P \land (P \lor Q) \equiv P \\
P \lor (P \land Q) \equiv P.
\]

Problem 2.8. Give intuitionistic proofs for the propositions
\[
P \Rightarrow (Q \Rightarrow (P \land Q)) \\
(P \Rightarrow Q) \Rightarrow ((P \Rightarrow \neg Q) \Rightarrow \neg P) \\
(P \Rightarrow R) \Rightarrow ((Q \Rightarrow R) \Rightarrow ((P \lor Q) \Rightarrow R)).
\]

Problem 2.9. Prove that the following equivalences are provable intuitionistically:
\[
P \land (P \Rightarrow Q) \equiv P \land Q \\
Q \land (P \Rightarrow Q) \equiv Q \\
(P \Rightarrow (Q \land R)) \equiv ((P \Rightarrow Q) \land (P \Rightarrow R)).
\]

Problem 2.10. Give intuitionistic proofs for
\[
(P \Rightarrow Q) \Rightarrow \neg \neg (\neg P \lor Q) \\
\neg \neg (\neg \neg P \Rightarrow P).
\]

Problem 2.11. Give an intuitionistic proof for \(\neg \neg (P \lor \neg P)\).

Problem 2.12. Give intuitionistic proofs for the propositions
\[
(P \lor \neg P) \Rightarrow (\neg \neg P \Rightarrow P) \text{ and } (\neg \neg P \Rightarrow P) \Rightarrow (P \lor \neg P).
\]

*Hint.* For the second implication, you may want to use Problem 2.11.

Problem 2.13. Give intuitionistic proofs for the propositions
\[
(P \Rightarrow Q) \Rightarrow \neg \neg (\neg P \lor Q) \text{ and } (\neg P \Rightarrow Q) \Rightarrow \neg \neg (P \lor Q).
\]

Problem 2.14. (1) Design an algorithm for converting a deduction of a proposition \(P\) in the system \(N_i^{=,\land,\lor,\bot}\) into a deduction in the system \(NG_i^{=,\land,\lor,\bot}\).

(2) Design an algorithm for converting a deduction of a proposition \(P\) in the system \(N_e^{=,\land,\lor,\bot}\) into a deduction in the system \(NG_e^{=,\land,\lor,\bot}\).
(3) Design an algorithm for converting a deduction of a proposition $P$ in the system $\mathcal{G}_i^{\Rightarrow,\land,\lor,\bot}$ into a deduction in the system $\mathcal{N}_i^{\Rightarrow,\land,\lor,\bot}$.

(4) Design an algorithm for converting a deduction of a proposition $P$ in the system $\mathcal{G}_c^{\Rightarrow,\land,\lor,\bot}$ into a deduction in the system $\mathcal{N}_c^{\Rightarrow,\land,\lor,\bot}$.

**Hint.** Use induction on deduction trees.

Problem 2.15. Prove that the following version of the $\lor$-elimination rule formulated in Gentzen-sequent style is a consequence of the rules of intuitionistic logic:

$$\Gamma, x: P \rightarrow R \quad \Gamma, y: Q \rightarrow R \quad \frac{\Gamma, z: P \lor Q \rightarrow R}{\Gamma \rightarrow R}$$

Conversely, if we assume that the above rule holds, then prove that the $\lor$-elimination rule

$$\Gamma \rightarrow P \lor Q \quad \Gamma, x: P \rightarrow R \quad \Gamma, y: Q \rightarrow R \quad \frac{\Gamma \rightarrow R}{\(\lor\text{-elim}\)}$$

follows from the rules of intuitionistic logic (of course, excluding the $\lor$-elimination rule).

Problem 2.16. (1) Give algorithms for converting a deduction in $\mathcal{N}_c^{\Rightarrow,\land,\lor,\bot,\forall,\exists}$ to a deduction in $\mathcal{N}_i^{\Rightarrow,\land,\lor,\bot,\forall,\exists}$ and vice-versa.

(2) Give algorithms for converting a deduction in $\mathcal{N}_i^{\Rightarrow,\land,\lor,\bot,\forall,\exists}$ to a deduction in $\mathcal{G}_c^{\Rightarrow,\land,\lor,\bot,\forall,\exists}$ and vice-versa.

Problem 2.17. (a) Give intuitionistic proofs for the distributivity of $\land$ over $\lor$ and of $\lor$ over $\land$:

$$P \land (Q \lor R) \equiv (P \land Q) \lor (P \land R)$$

$$P \lor (Q \land R) \equiv (P \lor Q) \land (P \lor R).$$

(b) Give intuitionistic proofs for the associativity of $\land$ and $\lor$:

$$P \land (Q \land R) \equiv (P \land Q) \land R$$

$$P \lor (Q \lor R) \equiv (P \lor Q) \lor R.$$

Problem 2.18. Recall that in Problem 2.1 we proved that if $P \Rightarrow Q$ and $Q \Rightarrow R$ are provable, then $P \Rightarrow R$ is provable. Deduce from this fact that if $P \equiv Q$ and $Q \equiv R$ hold, then $P \equiv R$ holds (intuitionistically or classically).

Prove that if $P \equiv Q$ holds then $Q \equiv P$ holds (intuitionistically or classically). Finally, check that $P \equiv P$ holds (intuitionistically or classically).

Problem 2.19. Prove (intuitionistically or classically) that if $P_1 \Rightarrow Q_1$ and $P_2 \Rightarrow Q_2$ then

1. $(P_1 \land P_2) \Rightarrow (Q_1 \land Q_2)$
2. $(P_1 \lor P_2) \Rightarrow (Q_1 \lor Q_2)$. 


(b) Prove (intuitionistically or classically) that if \( Q_1 \Rightarrow P_1 \) and \( P_2 \Rightarrow Q_2 \) then

1. \( (P_1 \Rightarrow P_2) \Rightarrow (Q_1 \Rightarrow Q_2) \)
2. \( \neg P_1 \Rightarrow \neg Q_1 \).

(c) Prove (intuitionistically or classically) that if \( Q \Rightarrow P \), then

1. \( \forall tP \Rightarrow \forall tQ \)
2. \( \exists tP \Rightarrow \exists tQ \).

(d) Prove (intuitionistically or classically) that if \( P_1 \equiv Q_1 \) and \( P_2 \equiv Q_2 \) then

1. \( (P_1 \land P_2) \equiv (Q_1 \land Q_2) \)
2. \( (P_1 \lor P_2) \equiv (Q_1 \lor Q_2) \)
3. \( (P_1 \Rightarrow P_2) \equiv (Q_1 \Rightarrow Q_2) \)
4. \( \neg P_1 \equiv \neg Q_1 \)
5. \( \forall tP_1 \equiv \forall tQ_1 \)
6. \( \exists tP_1 \equiv \exists tQ_1 \).

**Problem 2.20.** Show that the following are provable in classical first-order logic:

\[
\neg \forall tP \equiv \exists t\neg P \\
\neg \exists tP \equiv \forall t\neg P \\
\forall t(P \land Q) \equiv \forall tP \land \forall tQ \\
\exists t(P \lor Q) \equiv \exists tP \lor \exists tQ.
\]

Moreover, show that the propositions \( \exists t(P \land Q) \Rightarrow \exists tP \land \exists tQ \) and \( \forall tP \lor \forall tQ \Rightarrow \forall t(P \lor Q) \) are provable in intuitionistic first-order logic (and thus, also in classical first-order logic).

(c) Prove intuitionistically that

\[ \exists x \forall y P \Rightarrow \forall y \exists x P. \]

Give an informal argument to the effect that the converse, \( \forall y \exists x P \Rightarrow \exists x \forall y P \), is not provable, even classically.

**Problem 2.21.** (a) Assume that \( Q \) is a formula that does not contain the variable \( t \) (free or bound). Give a classical proof of

\[ \forall t(P \lor Q) \Rightarrow (\forall tP \lor Q). \]
(b) If $P$ is a proposition, write $P(x)$ for $P[x/t]$ and $P(y)$ for $P[y/t]$, where $x$ and $y$ are distinct variables that do not occur in the original proposition $P$. Give an intuitionistic proof for

$$\neg \forall x \exists y (\neg P(x) \land P(y)).$$

(c) Give a classical proof for

$$\exists x \forall y (P(x) \lor \neg P(y)).$$

*Hint.* Negate the above, then use some identities we’ve shown (such as de Morgan) and reduce the problem to part (b).

**Problem 2.22.** (a) Let $X = \{X_i \mid 1 \leq i \leq n\}$ be a finite family of sets. Prove that if $X_{i+1} \subseteq X_i$ for all $i$, with $1 \leq i \leq n - 1$, then

$$\bigcap X = X_n.$$

Prove that if $X_i \subseteq X_{i+1}$ for all $i$, with $1 \leq i \leq n - 1$, then

$$\bigcup X = X_n.$$

(b) Recall that $\mathbb{N}_+ = \mathbb{N} - \{0\} = \{1, 2, 3, \ldots, n, \ldots\}$. Give an example of an infinite family of sets, $X = \{X_i \mid i \in \mathbb{N}_+\}$, such that

1. $X_{i+1} \subseteq X_i$ for all $i \geq 1$.
2. $X_i$ is infinite for every $i \geq 1$.
3. $\bigcap X$ has a single element.

(c) Give an example of an infinite family of sets, $X = \{X_i \mid i \in \mathbb{N}_+\}$, such that

1. $X_{i+1} \subseteq X_i$ for all $i \geq 1$.
2. $X_i$ is infinite for every $i \geq 1$.
3. $\bigcap X = \emptyset$.

**Problem 2.23.** Prove that the following propositions are provable intuitionistically:

$$(P \Rightarrow \neg P) \equiv \neg P, \quad (\neg P \Rightarrow P) \equiv \neg \neg P.$$ 

Use these to conclude that if the equivalence $P \equiv \neg P$ is provable intuitionistically, then every proposition is provable (intuitionistically).
Problem 2.24. (1) Prove that if we assume that all propositions of the form,

\[(P \Rightarrow Q) \Rightarrow P,\]

are axioms (Peirce’s law), then \(\neg\neg P \Rightarrow P\) becomes provable in intuitionistic logic. Thus, another way to get classical logic from intuitionistic logic is to add Peirce’s law to intuitionistic logic.

Hint. Pick \(Q\) in a suitable way and use Problem 2.23.

(2) Prove \(((P \Rightarrow Q) \Rightarrow P) \Rightarrow P\) in classical logic.

Hint. Use the de Morgan laws.

Problem 2.25. Let \(A\) be any nonempty set. Prove that the definition

\[X = \{ a \in A \mid a \notin X \}\]

yields a “set,” \(X\), such that \(X\) is empty iff \(X\) is nonempty and therefore does not define a set, after all.

Problem 2.26. Prove the following fact: if

\[\Gamma \quad \Gamma, R \quad \text{and} \quad \text{\(D_1\)} \quad \text{\(D_2\)} \quad \text{\(P \lor Q\)} \quad \text{\(Q\)}\]

are deduction trees provable intuitionistically, then there is a deduction tree

\[\Gamma, P \Rightarrow R \quad \text{\(D\)} \quad \text{\(Q\)}\]

for \(Q\) from the premises in \(\Gamma \cup \{P \Rightarrow S\}\).

Problem 2.27. Recall that the constant \(\top\) stands for true. So, we add to our proof systems (intuitionistic and classical) all axioms of the form

\[\underbrace{P_1, \ldots, P_1, \ldots}_{k_1}, \ldots, \underbrace{P_i, \ldots, P_i, \ldots}_{k_i}, \ldots, \underbrace{P_n, \ldots, P_n}_{k_n}\]

\[\top\]

where \(k_i \geq 1\) and \(n \geq 0\); note that \(n = 0\) is allowed, which amounts to the one-node tree, \(\top\).

(a) Prove that the following equivalences hold intuitionistically.

\[P \lor \top \equiv \top\]
\[P \land \top \equiv P.\]
Prove that if \( P \) is intuitionistically (or classically) provable, then \( P \equiv \top \) is also provable intuitionistically (or classically). In particular, in classical logic, \( P \lor \neg P \equiv \top \). Also prove that

\[
P \lor \bot \equiv P \\
P \land \bot \equiv \bot
\]

hold intuitionistically.

(b) In the rest of this problem, we are dealing only with classical logic. The connective exclusive or, denoted \( \oplus \), is defined by

\[
P \oplus Q \equiv (P \land \neg Q) \lor (\neg P \land Q).
\]

In solving the following questions, you will find that constructing proofs using the rules of classical logic is very tedious because these proofs are very long. Instead, use some identities from previous problems.

Prove the equivalence

\[
\neg P \equiv P \oplus \top.
\]

(c) Prove that

\[
P \oplus P \equiv \bot \\
P \oplus Q \equiv Q \oplus P \\
(P \oplus Q) \oplus R \equiv P \oplus (Q \oplus R).
\]

(d) Prove the equivalence

\[
P \lor Q \equiv (P \land Q) \oplus (P \oplus Q).
\]

**Problem 2.28.** Give a classical proof of

\[
\neg(P \Rightarrow \neg Q) \Rightarrow (P \land Q).
\]

**Problem 2.29.** (a) Prove that the rule

\[
\begin{array}{c}
\Gamma \\
\mathcal{D}_1 \\

\end{array}
\begin{array}{c}
\Delta \\
\mathcal{D}_2 \\

\end{array}
\begin{array}{c}
P \Rightarrow Q \\
\neg Q
\end{array}
\begin{array}{c}
\neg P
\end{array}
\]

can be derived from the other rules of intuitionistic logic.

(b) Give an intuitionistic proof of \( \neg P \) from \( \Gamma = \{\neg(\neg P \lor Q), P \Rightarrow Q\} \) or equivalently, an intuitionistic proof of

\[
\left(\neg(\neg P \lor Q) \land (P \Rightarrow Q)\right) \Rightarrow \neg P.
\]
Problem 2.30. (a) Give intuitionistic proofs for the equivalences
\[ \exists x \exists y P \equiv \exists y \exists x P \quad \text{and} \quad \forall x \forall y P \equiv \forall y \forall x P. \]

(b) Give intuitionistic proofs for
\[ (\forall t P \land Q) \Rightarrow \forall t (P \land Q) \quad \text{and} \quad \forall t (P \land Q) \Rightarrow (\forall t P \land Q), \]
where \( t \) does not occur (free or bound) in \( Q \).

(c) Give intuitionistic proofs for
\[ (\exists t P \lor Q) \Rightarrow \exists t (P \lor Q) \quad \text{and} \quad \exists t (P \lor Q) \Rightarrow (\exists t P \lor Q), \]
where \( t \) does not occur (free or bound) in \( Q \).

Problem 2.31. An integer, \( n \in \mathbb{Z} \), is divisible by 3 iff \( n = 3k \), for some \( k \in \mathbb{Z} \). Thus (by the division theorem), an integer, \( n \in \mathbb{Z} \), is not divisible by 3 iff it is of the form \( n = 3k+1, 3k+2 \), for some \( k \in \mathbb{Z} \) (you don’t have to prove this).

Prove that for any integer, \( n \in \mathbb{Z} \), if \( n^2 \) is divisible by 3, then \( n \) is divisible by 3.

Hint. Prove the contrapositive. If \( n \) of the form \( n = 3k+1, 3k+2 \), then so is \( n^2 \) (for a different \( k \)).

Problem 2.32. Use Problem 2.31 to prove that \( \sqrt{3} \) is irrational, that is, \( \sqrt{3} \) can’t be written as \( \sqrt{3} = p/q \), with \( p, q \in \mathbb{Z} \) and \( q \neq 0 \).

Problem 2.33. Give an intuitionistic proof of the proposition
\[ ((P \Rightarrow R) \land (Q \Rightarrow R)) \equiv ((P \lor Q) \Rightarrow R). \]

Problem 2.34. Give an intuitionistic proof of the proposition
\[ ((P \land Q) \Rightarrow R) \equiv (P \Rightarrow (Q \Rightarrow R)). \]

Problem 2.35. (a) Give an intuitionistic proof of the proposition
\[ (P \land Q) \Rightarrow (P \lor Q). \]

(b) Prove that the proposition \( (P \lor Q) \Rightarrow (P \land Q) \) is not valid, where \( P, Q \), are propositional symbols.

(c) Prove that the proposition \( (P \lor Q) \Rightarrow (P \land Q) \) is not provable in general and that if we assume that all propositions of the form \( (P \lor Q) \Rightarrow (P \land Q) \) are axioms, then every proposition becomes provable intuitionistically.

Problem 2.36. Give the details of the proof of Proposition 2.6; namely, if a proposition \( P \) is provable in the system \( N'_{c,\Rightarrow,\land,\lor,\perp} \) (or \( NG'_{c,\Rightarrow,\land,\lor,\perp} \)), then it is valid (according to the truth value semantics).
Problem 2.37. Give the details of the proof of Theorem 2.8; namely, if a proposition $P$ is provable in the system $\mathcal{N}^e,\land,\lor,\bot$ (or $\mathcal{NG}^e,\land,\lor,\bot$), then it is valid in every Kripke model; that is, it is intuitionistically valid.

Problem 2.38. Prove that $b = \log_2 9$ is irrational. Then, prove that $a = \sqrt{2}$ and $b = \log_2 9$ are two irrational numbers such that $a^b$ is rational.

Problem 2.39. (1) Prove that if $\forall x (P \land Q)$ can be deduced intuitionistically from a set of premises $\Gamma$, then $\forall x (P \Rightarrow \neg Q)$ and $\forall x (Q \Rightarrow \neg P)$ can also be deduced intuitionistically from $\Gamma$.

(2) Prove that if $\forall x (P \lor Q)$ can be deduced intuitionistically from a set of premises $\Gamma$, then $\forall x (\neg P \Rightarrow Q)$ and $\forall x (\neg Q \Rightarrow P)$ can also be deduced intuitionistically from $\Gamma$.

Conclude that if
\[
\forall x (P \lor Q) \quad \text{and} \quad \forall x (P \land Q)
\]
can be deduced intuitionistically from a set of premises $\Gamma$, then
\[
\forall x (P \equiv \neg Q) \quad \text{and} \quad \forall x (Q \equiv \neg P)
\]
can also be deduced intuitionistically from $\Gamma$.

(3) Prove that if $\forall x (P \Rightarrow Q)$ can be deduced intuitionistically from a set of premises $\Gamma$, then $\forall x (\neg Q \Rightarrow \neg P)$ can also be deduced intuitionistically from $\Gamma$. Use this to prove that if
\[
\forall x (P \equiv \neg Q) \quad \text{and} \quad \forall x (Q \equiv \neg P)
\]
can be deduced intuitionistically from a set of premises $\Gamma$, then $\forall x (\neg \neg P \equiv P)$ and $\forall x (\neg \neg Q \equiv Q)$ can be deduced intuitionistically from $\Gamma$.

Problem 2.40. Prove that the formula,
\[
\forall x \text{ even}(2 \ast x),
\]
is provable in Peano arithmetic. Prove that
\[
\text{even}(2 \ast (n + 1) \ast (n + 3)),
\]
is provable in Peano arithmetic for any natural number $n$.

Problem 2.41. A first-order formula $A$ is said to be in prenex-form if either

(1) $A$ is a quantifier-free formula.

(2) $A = \forall t B$ or $A = \exists t B$, where $B$ is in prenex-form.

In other words, a formula is in prenex form iff it is of the form
\[
Q_1 t_1 Q_2 t_2 \cdots Q_m t_m P,
\]
where $P$ is quantifier-free and where $Q_1 Q_2 \cdots Q_m$ is a string of quantifiers, $Q_i \in \{\forall, \exists\}$.

Prove that every first-order formula $A$ is classically equivalent to a formula $B$ in prenex form.
Problem 2.42. Even though natural deduction proof systems for classical propositional logic are complete (with respect to the truth value semantics), they are not adequate for designing algorithms searching for proofs (because of the amount of nondeterminism involved).

Gentzen designed a different kind of proof system using sequents (later refined by Kleene, Smullyan, and others) that is far better suited for the design of automated theorem provers. Using such a proof system (a sequent calculus), it is relatively easy to design a procedure that terminates for all input propositions $P$ and either certifies that $P$ is (classically) valid or else returns some (or all) falsifying truth assignment(s) for $P$. In fact, if $P$ is valid, the tree returned by the algorithm can be viewed as a proof of $P$ in this proof system.

For this miniproject, we describe a Gentzen sequent-calculus $G'$ for propositional logic that lends itself well to the implementation of algorithms searching for proofs or falsifying truth assignments of propositions.

Such algorithms build trees whose nodes are labeled with pairs of sets called sequents. A sequent is a pair of sets of propositions denoted by $P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n$, with $m, n \geq 0$. Symbolically, a sequent is usually denoted $\Gamma \rightarrow \Delta$, where $\Gamma$ and $\Delta$ are two finite sets of propositions (not necessarily disjoint).

For example, $\rightarrow P \Rightarrow (Q \Rightarrow P)$, $P \lor Q \rightarrow$, $P, Q \rightarrow P \land Q$ are sequents. The sequent $\rightarrow$, where both $\Gamma = \Delta = \emptyset$ corresponds to falsity.

The choice of the symbol $\rightarrow$ to separate the two sets of propositions $\Gamma$ and $\Delta$ is commonly used and was introduced by Gentzen but there is nothing special about it. If you don’t like it, you may replace it by any symbol of your choice as long as that symbol does not clash with the logical connectives ($\Rightarrow, \land, \lor, \neg$). For example, you could denote a sequent $P_1, \ldots, P_m; Q_1, \ldots, Q_n$, using the semicolon as a separator.

Given a truth assignment $v$ to the propositional letters in the propositions $P_i$ and $Q_j$, we say that $v$ satisfies the sequent, $P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n$, iff

$$v(P_1 \land \cdots \land P_m) \Rightarrow (Q_1 \lor \cdots \lor Q_n) = \text{true},$$

or equivalently, $v$ falsifies the sequent, $P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n$, iff

$$v(P_1 \land \cdots \land P_m \land \neg Q_1 \land \cdots \land \neg Q_n) = \text{true},$$

iff

$$v(P_i) = \text{true}, \ 1 \leq i \leq m \ \text{and} \ v(Q_j) = \text{false}, \ 1 \leq j \leq n.$$ 

A sequent is valid iff it is satisfied by all truth assignments iff it cannot be falsified.

Note that a sequent $P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n$ can be falsified iff some truth assignment satisfies all of $P_1, \ldots, P_m$ and falsifies all of $Q_1, \ldots, Q_n$. In particular, if $\{P_1, \ldots, P_m\}$ and
{Q_1, \ldots, Q_n} have some common proposition (they have a nonempty intersection), then the sequent, P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n, is valid. On the other hand if all the P_i's and Q_j's are propositional letters and \{P_1, \ldots, P_m\} and \{Q_1, \ldots, Q_n\} are disjoint (they have no symbol in common), then the sequent, P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n, is falsified by the truth assignment v where v(P_i) = true, for i = 1, \ldots m and v(Q_j) = false, for j = 1, \ldots, n.

The main idea behind the design of the proof system G' is to systematically try to falsify a sequent. If such an attempt fails, the sequent is valid and a proof tree is found. Otherwise, all falsifying truth assignments are returned. In some sense

\textit{failure to falsify is success (in finding a proof).}

The rules of G' are designed so that the conclusion of a rule is falsified by a truth assignment v iff its single premise of one of its two premises is falsified by v. Thus, these rules can be viewed as \textit{two-way} rules that can either be read bottom-up or top-down.

Here are the axioms and the rules of the \textit{sequent calculus} G':

\textbf{Axioms:} \Gamma, P \rightarrow P, \Delta

\textbf{Inference rules:}

\[
\begin{align*}
\Gamma, P, Q, \Delta & \rightarrow \Lambda \quad \wedge: \text{left} & \Gamma \rightarrow \Delta, P, \Lambda \quad \Gamma \rightarrow \Delta, Q, \Lambda \quad \wedge: \text{right} \\
\Gamma, P, \Delta & \rightarrow \Lambda \quad \Gamma, Q, \Delta & \rightarrow \Lambda \quad \vee: \text{left} & \Gamma \rightarrow \Delta, P, Q, \Lambda \quad \vee: \text{right} \\
\Gamma, Q, \Delta & \rightarrow \Lambda \quad \Gamma & \rightarrow \Delta, Q, \Delta & \rightarrow \Lambda \quad \Rightarrow: \text{left} & P, \Gamma \rightarrow Q, \Delta, \Lambda \quad \Gamma \rightarrow \Delta, P \Rightarrow Q, \Lambda \quad \Rightarrow: \text{right} \\
\Gamma, \Delta & \rightarrow \Lambda \quad P, \Gamma & \rightarrow \Delta, \Lambda \quad \neg: \text{left} & P, \Gamma \rightarrow \Delta, \Lambda \quad \Gamma \rightarrow \Delta, \neg P, \Lambda \quad \neg: \text{right}
\end{align*}
\]

where \( \Gamma, \Delta, \Lambda \) are any finite sets of propositions, possibly the empty set.

A \textit{deduction tree} is either a one-node tree labeled with a sequent or a tree constructed according to the rules of system G'. A \textit{proof tree} (or \textit{proof}) is a deduction tree whose leaves are \textit{all} axioms. A proof tree for a proposition \( P \) is a proof tree for the sequent \( \rightarrow P \) (with an empty left-hand side).

For example,

\[ P, Q \rightarrow P \]

is a proof tree.

Here is a proof tree for \( (P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P) \):
The following is a deduction tree but not a proof tree,

\[
\frac{P, \neg Q \rightarrow P}{\neg Q \rightarrow \neg P, P} \quad \frac{Q \rightarrow Q, \neg P}{\neg Q, Q \rightarrow \neg P} \quad \frac{(P \Rightarrow Q) \rightarrow (\neg Q \Rightarrow \neg P)}{\rightarrow (P \Rightarrow Q) \Rightarrow (\neg Q \Rightarrow \neg P)}
\]

because its rightmost leaf, \( R, Q, P \rightarrow \), is falsified by the truth assignment \( v(P) = v(Q) = v(R) = \text{true} \), which also falsifies \( (P \Rightarrow Q) \Rightarrow (R \Rightarrow \neg P) \).

Let us call a sequent \( P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n \) finished if either it is an axiom \( P_i = Q_j \) for some \( i \) and some \( j \) or all the propositions \( P_i \) and \( Q_j \) are atomic and \( \{P_1, \ldots, P_m\} \cap \{Q_1, \ldots, Q_n\} = \emptyset \). We also say that a deduction tree is finished if all its leaves are finished sequents.

The beauty of the system \( G' \) is that for every sequent, \( P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n \), the process of building a deduction tree from this sequent always terminates with a tree where all leaves are finished independently of the order in which the rules are applied. Therefore, we can apply any strategy we want when we build a deduction tree and we are sure that we will get a deduction tree with all its leaves finished. If all the leaves are axioms, then we have a proof tree and the sequent is valid, or else all the leaves that are not axioms yield a falsifying assignment, and all falsifying assignments for the root sequent are found this way.

If we only want to know whether a proposition (or a sequent) is valid, we can stop as soon as we find a finished sequent that is not an axiom because in this case, the input sequent is falsifiable.

(1) Prove that for every sequent \( P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n \) any sequence of applications of the rules of \( G' \) terminates with a deduction tree whose leaves are all finished sequents (a finished deduction tree).

**Hint.** Define the number of connectives \( c(P) \) in a proposition \( P \) as follows.

1. If \( P \) is a propositional symbol, then
   \[ c(P) = 0. \]

2. If \( P = \neg Q \), then
   \[ c(\neg Q) = c(Q) + 1. \]
(3) If \( P = Q \ast R \), where \( \ast \in \{ \Rightarrow, \lor, \land \} \), then
\[
c(Q \ast R) = c(Q) + c(R) + 1.
\]

Given a sequent,
\[
\Gamma \rightarrow \Delta = P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n,
\]
define the number of connectives, \( c(\Gamma \rightarrow \Delta) \), in \( \Gamma \rightarrow \Delta \) by
\[
c(\Gamma \rightarrow \Delta) = c(P_1) + \cdots + c(P_m) + c(Q_1) + \cdots + c(Q_n).
\]

Prove that the application of every rule decreases the number of connectives in the premise(s) of the rule.

(2) Prove that for every sequent \( P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n \) for every finished deduction tree \( T \) constructed from \( P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n \) using the rules of \( G' \), every truth assignment \( v \) satisfies \( P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n \) iff \( v \) satisfies every leaf of \( T \). Equivalently, a truth assignment \( v \) falsifies \( P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n \) iff \( v \) falsifies some leaf of \( T \).

Deduce from the above that a sequent is valid iff all leaves of every finished deduction tree \( T \) are axioms. Furthermore, if a sequent is not valid, then for every finished deduction tree \( T \), for that sequent, every falsifying assignment for that sequent is a falsifying assignment of some leaf of the tree, \( T \).

(3) Programming Project:
Design an algorithm taking any sequent as input and constructing a finished deduction tree. If the deduction tree is a proof tree, output this proof tree in some fashion (such a tree can be quite big so you may have to find ways of “flattening” these trees). If the sequent is falsifiable, stop when the algorithm encounters the first leaf that is not an axiom and output the corresponding falsifying truth assignment.

I suggest using a depth-first expansion strategy for constructing a deduction tree. What this means is that when building a deduction tree, the algorithm will proceed recursively as follows. Given a nonfinished sequent
\[
A_1, \ldots, A_p \rightarrow B_1, \ldots, B_q,
\]
if \( A_i \) is the leftmost nonatomic proposition if such proposition occurs on the left or if \( B_j \) is the leftmost nonatomic proposition if all the \( A_i \)s are atomic, then

(1) The sequent is of the form
\[
\Gamma, A_i, \Delta \rightarrow \Lambda,
\]
with \( A_i \) the leftmost nonatomic proposition. Then either

(a) \( A_i = C_i \land D_i \) or \( A_i = \neg C_i \), in which case either we recursively construct a (finished) deduction tree
\[
\mathcal{D}_1
\]
\[
\Gamma, C_i, D_i, \Delta \rightarrow \Lambda
\]
to get the deduction tree

\[
\begin{array}{l}
D_1 \\
\Gamma, C_i, D_i, \Delta \rightarrow \Lambda \\
\end{array}
\]

\[
\begin{array}{l}
\Gamma, C_i \land D_i, \Delta \rightarrow \Lambda \\
\end{array}
\]
or we recursively construct a (finished) deduction tree

\[
\begin{array}{l}
D_1 \\
\Gamma, \Delta \rightarrow C_i, \Lambda \\
\end{array}
\]
to get the deduction tree

\[
\begin{array}{l}
D_1 \\
\Gamma, \Delta \rightarrow C_i, \Lambda \\
\end{array}
\]

or

\[
\begin{array}{l}
\Gamma, \neg C_i, \Delta \rightarrow \Lambda \\
\end{array}
\]

or

(b) \( A_i = C_i \lor D_i \) or \( A_i = C_i \Rightarrow D_i \), in which case either we recursively construct two (finished) deduction trees

\[
\begin{array}{ll}
D_1 & D_2 \\
\Gamma, C_i, \Delta \rightarrow \Lambda & \Gamma, D_i, \Delta \rightarrow \Lambda \\
\end{array}
\]
to get the deduction tree

\[
\begin{array}{ll}
D_1 & D_2 \\
\Gamma, C_i, \Delta \rightarrow \Lambda & \Gamma, D_i, \Delta \rightarrow \Lambda \\
\end{array}
\]

\[
\Gamma, C_i \lor D_i, \Delta \rightarrow \Lambda 
\]
or we recursively construct two (finished) deduction trees

\[
\begin{array}{ll}
D_1 & D_2 \\
\Gamma, \Delta \rightarrow C_i, \Lambda & \Gamma, D_i, \Gamma, \Delta \rightarrow \Lambda \\
\end{array}
\]
to get the deduction tree

\[
\begin{array}{ll}
D_1 & D_2 \\
\Gamma, \Delta \rightarrow C_i, \Lambda & \Gamma, D_i, \Gamma, \Delta \rightarrow \Lambda \\
\end{array}
\]

\[
\Gamma, C_i \Rightarrow D_i, \Delta \rightarrow \Lambda 
\]

(2) The nonfinished sequent is of the form

\[
\Gamma \rightarrow \Delta, B_j, \Lambda, 
\]

with \( B_j \) the leftmost nonatomic proposition. Then either
(a) $B_j = C_j \lor D_j$ or $B_j = C_j \Rightarrow D_j$, or $B_j = \neg C_j$, in which case either we recursively construct a (finished) deduction tree

$$D_1$$

$$\Gamma \rightarrow \Delta, C_j, D_j, \Lambda$$

to get the deduction tree

$$D_1$$

$$\Gamma \rightarrow \Delta, C_j, D_j, \Lambda$$

$$\Gamma \rightarrow \Delta, C_j \lor D_j, \Lambda$$

or we recursively construct a (finished) deduction tree

$$D_1$$

$$C_j, \Gamma \rightarrow D_j, \Delta, \Lambda$$

to get the deduction tree

$$D_1$$

$$C_j, \Gamma \rightarrow D_j, \Delta, \Lambda$$

$$\Gamma \rightarrow \Delta, C_j \Rightarrow D_j, \Lambda$$

or we recursively construct a (finished) deduction tree

$$D_1$$

$$C_j, \Gamma \rightarrow \Delta, \Lambda$$

to get the deduction tree

$$D_1$$

$$C_j, \Gamma \rightarrow \Delta, \Lambda$$

$$\Gamma \rightarrow \Delta, \neg C_j, \Lambda$$

or

(b) $B_j = C_j \land D_j$, in which case we recursively construct two (finished) deduction trees

$$D_1$$

$$\Gamma \rightarrow \Delta, C_j, \Lambda$$

and

$$D_2$$

$$\Gamma \rightarrow \Delta, D_j, \Lambda$$

to get the deduction tree

$$D_1$$

$$\Gamma \rightarrow \Delta, C_j, \Lambda$$

$$\Gamma \rightarrow \Delta, D_j, \Lambda$$

$$\Gamma \rightarrow \Delta, C_j \land D_j, \Lambda$$

If you prefer, you can apply a breadth-first expansion strategy for constructing a deduction tree.
Problem 2.43. Let $A$ and be $B$ be any two sets of sets.

1. Prove that
   \[
   \left( \bigcup A \right) \cup \left( \bigcup B \right) = \bigcup (A \cup B).
   \]

2. Assume that $A$ and $B$ are nonempty. Prove that
   \[
   \left( \bigcap A \right) \cap \left( \bigcap B \right) = \bigcap (A \cup B).
   \]

3. Assume that $A$ and $B$ are nonempty. Prove that
   \[
   \bigcup (A \cap B) \subseteq \left( \bigcup A \right) \cap \left( \bigcup B \right)
   \]
   and give a counterexample of the inclusion
   \[
   \left( \bigcup A \right) \cap \left( \bigcup B \right) \subseteq \bigcup (A \cap B).
   \]

*Hint.* Reduce the above questions to the provability of certain formulae that you have already proved in a previous assignment (you need not re-prove these formulae).

Problem 2.44. A set $A$ is said to be *transitive* iff for all $a \in A$ and all $x \in a$, then $x \in A$, or equivalently, for all $a \in A$,
   \[
a \in A \Rightarrow a \subseteq A.
   \]

1. Check that a set $A$ is transitive iff
   \[
   \bigcup A \subseteq A
   \]
   iff
   \[
   A \subseteq 2^A.
   \]
   (2) Recall the definition of the von Neumann successor of a set $A$ given by
   \[
   A^+ = A \cup \{A\}.
   \]
   Prove that if $A$ is a transitive set, then
   \[
   \bigcup (A^+) = A.
   \]

3. Recall the von Neumann definition of the natural numbers. Check that for every natural number $m$
   \[
m \in m^+ \text{ and } m \subseteq m^+.
   \]
   Prove that every natural number is a transitive set.
   *Hint.* Use induction.

4. Prove that for any two von Neumann natural numbers $m$ and $n$, if $m^+ = n^+$, then $m = n$.

5. Prove that the set, $N$, of natural numbers is a transitive set.
   *Hint.* Use induction.
Bibliography


Chapter 3

RAM Programs, Turing Machines, and the Partial Computable Functions

See the scanned version of this chapter found in the web page for CIS511:

3.1 Partial Functions and RAM Programs

We define an abstract machine model for computing functions
\[ f : \Sigma^* \times \cdots \times \Sigma^* \to \Sigma^*, \]
where \( \Sigma = \{a_1, \ldots, a_k\} \) is some input alphabet.

Numerical functions \( f : \mathbb{N}^n \to \mathbb{N} \) can be viewed as functions defined over the one-letter alphabet \( \{a_1\} \), using the bijection \( m \mapsto a_1^m \).

Let us recall the definition of a partial function.

**Definition 3.1.** A binary relation \( R \subseteq A \times B \) between two sets \( A \) and \( B \) is **functional** iff, for all \( x \in A \) and \( y, z \in B \),
\[ (x, y) \in R \text{ and } (x, z) \in R \text{ implies that } y = z. \]

A **partial function** is a triple \( f = \langle A, G, B \rangle \), where \( A \) and \( B \) are arbitrary sets (possibly empty) and \( G \) is a functional relation (possibly empty) between \( A \) and \( B \), called the **graph** of \( f \).

Hence, a partial function is a functional relation such that every argument has at most one image under \( f \).

The graph of a function \( f \) is denoted as \( \text{graph}(f) \). When no confusion can arise, a function \( f \) and its graph are usually identified.

A partial function \( f = \langle A, G, B \rangle \) is often denoted as \( f : A \to B \).

The **domain** \( \text{dom}(f) \) of a partial function \( f = \langle A, G, B \rangle \) is the set
\[ \text{dom}(f) = \{ x \in A \mid \exists y \in B, (x, y) \in G \}. \]

For every element \( x \in \text{dom}(f) \), the unique element \( y \in B \) such that \( (x, y) \in \text{graph}(f) \) is denoted as \( f(x) \). We say that \( f(x) \) **converges**, also denoted as \( f(x) \downarrow \).

If \( x \in A \) and \( x \notin \text{dom}(f) \), we say that \( f(x) \) **diverges**, also denoted as \( f(x) \uparrow \).

Intuitively, if a function is partial, it does not return any output for any input not in its domain. This corresponds to an infinite computation.

A partial function \( f : A \to B \) is a **total function** iff \( \text{dom}(f) = A \). It is customary to call a total function simply a function.

We now define a model of computation know as the **RAM programs**, or **Post machines**.

RAM programs are written in a sort of assembly language involving simple instructions manipulating strings stored into registers.
3.1. PARTIAL FUNCTIONS AND RAM PROGRAMS

Every RAM program uses a fixed and finite number of registers denoted as $R_1, \ldots, R_p$, with no limitation on the size of strings held in the registers.

RAM programs can be defined either in flowchart form or in linear form. Since the linear form is more convenient for coding purposes, we present RAM programs in linear form.

A RAM program $P$ (in linear form) consists of a finite sequence of instructions using a finite number of registers $R_1, \ldots, R_p$.

Instructions may optionally be labeled with line numbers denoted as $N_1, \ldots, N_q$.

It is neither mandatory to label all instructions, nor to use distinct line numbers!

Thus, the same line number can be used in more than one line. As we will see later on, this makes it easier to concatenate two different programs without performing a renumbering of line numbers.

Every instruction has four fields, not necessarily all used. The main field is the op-code. Here is an example of a RAM program to concatenate two strings $x_1$ and $x_2$.

```
R3 ← R1
R4 ← R2
N0 R4 jmp_a N1b
R4 jmp_b N2b
    jmp N3b
N1 add_a R3
tail R4
    jmp N0a
N2 add_b R3
tail R4
    jmp N0a
N3 R1 ← R3
    continue
```

**Definition 3.2.** RAM programs are constructed from seven types of instructions shown below:

1. $N \text{ add}_j \ Y$
2. $N \text{ tail} \ Y$
3. $N \text{ clr} \ Y$
4. $N \ Y \ ← X$
5. $N \text{ jmp} \ N1a$
6. $N \text{ jmp}_j \ N1b$
7. $N \text{ continue}$
1. An instruction of type $(1_j)$ concatenates the letter $a_j$ to the right of the string held by register $Y$ ($1 \leq j \leq k$). The effect is the assignment

$$Y := Ya_j.$$ 

2. An instruction of type (2) deletes the leftmost letter of the string held by the register $Y$. This corresponds to the function $\text{tail}$, defined such that

$$\text{tail}(\epsilon) = \epsilon,$$
$$\text{tail}(a_ju) = u.$$ 

The effect is the assignment

$$Y := \text{tail}(Y).$$ 

3. An instruction of type (3) clears register $Y$, i.e., sets its value to the empty string $\epsilon$. The effect is the assignment

$$Y := \epsilon.$$

4. An instruction of type (4) assigns the value of register $X$ to register $Y$. The effect is the assignment

$$Y := X.$$ 

5. An instruction of type (5a) or (5b) is an unconditional jump.

The effect of (5a) is to jump to the closest line number $N1$ occurring above the instruction being executed, and the effect of (5b) is to jump to the closest line number $N1$ occurring below the instruction being executed.

6. An instruction of type $(6 Ja)$ or $(6 Jb)$ is a conditional jump. Let $\text{head}$ be the function defined as follows:

$$\text{head}(\epsilon) = \epsilon,$$
$$\text{head}(a_ju) = a_j.$$ 

The effect of $(6 Ja)$ is to jump to the closest line number $N1$ occurring above the instruction being executed iff $\text{head}(Y) = a_j$, else to execute the next instruction (the one immediately following the instruction being executed).
The effect of \((6, b)\) is to jump to the closest line number \(N_1\) occurring below the instruction being executed iff \(head(Y) = a_j\), else to execute the next instruction.

When computing over \(\mathbb{N}\), instructions of type \((6, b)\) jump to the closest \(N_1\) above or below iff \(Y\) is nonnull.

7. An instruction of type \((7)\) is a no-op, i.e., the registers are unaffected. If there is a next instruction, then it is executed, else, the program stops.

Obviously, a program is syntactically correct only if certain conditions hold.

**Definition 3.3.** A *RAM program* \(P\) is a finite sequence of instructions as in Definition 3.2, and satisfying the following conditions:

1. For every jump instruction (conditional or not), the line number to be jumped to must exist in \(P\).

2. The last instruction of a RAM program is a *continue*.

The reason for allowing multiple occurrences of line numbers is to make it easier to concatenate programs without having to perform a renaming of line numbers.

The technical choice of jumping to the closest address \(N_1\) above or below comes from the fact that it is easy to search up or down using primitive recursion, as we will see later on.

For the purpose of computing a function \(f: \Sigma^* \times \cdots \times \Sigma^* \to \Sigma^*\) using a RAM program \(P\), we assume that \(P\) has at least \(n\) registers called *input registers*, and that these registers \(R_1, \ldots, R_n\) are initialized with the input values of the function \(f\).

We also assume that the output is returned in register \(R_1\).

The following RAM program concatenates two strings \(x_1\) and \(x_2\) held in registers \(R_1\) and \(R_2\).

\[
\begin{align*}
R3 & \leftarrow R1 \\
R4 & \leftarrow R2 \\
N0 & \text{jmp}_a \quad N1b \\
N1 & \text{add}_a \quad R3 \\
N2 & \text{add}_b \quad R3 \\
N3 & R1 \leftarrow R3 \\
\end{align*}
\]
Since $\Sigma = \{a, b\}$, for more clarity, we wrote $\text{jmp}_a$ instead of $\text{jmp}_1$, $\text{jmp}_b$ instead of $\text{jmp}_2$, $\text{add}_a$ instead of $\text{add}_1$, and $\text{add}_b$ instead of $\text{add}_2$.

**Definition 3.4.** A RAM program $P$ computes the partial function $\varphi : (\Sigma^*)^n \to \Sigma^*$ if the following conditions hold: For every input $(x_1, \ldots, x_n) \in (\Sigma^*)^n$, having initialized the input registers $R_1, \ldots, R_n$ with $x_1, \ldots, x_n$, the program eventually halts iff $\varphi(x_1, \ldots, x_n)$ converges, and if and when $P$ halts, the value of $R_1$ is equal to $\varphi(x_1, \ldots, x_n)$. A partial function $\varphi$ is RAM-computable if it is computed by some RAM program.

For example, the following program computes the *erase function* $E$ defined such that

$$E(u) = \epsilon$$

for all $u \in \Sigma^*$:

```
clr  R1
continue
```

The following program computes the *$j$th successor function* $S_j$ defined such that

$$S_j(u) = ua_j$$

for all $u \in \Sigma^*$:

```
add_j  R1
continue
```

The following program (with $n$ input variables) computes the *projection function* $P^n_i$ defined such that

$$P^n_i(u_1, \ldots, u_n) = u_i,$$

where $n \geq 1$, and $1 \leq i \leq n$:

```
R1 ← Ri
continue
```

Note that $P^1_1$ is the identity function.

Having a programming language, we would like to know how powerful it is, that is, we would like to know what kind of functions are RAM-computable.

At first glance, RAM programs don’t do much, but this is not so. Indeed, we will see shortly that the class of RAM-computable functions is quite extensive.
One way of getting new programs from previous ones is via composition. Another one is by primitive recursion.

We will investigate these constructions after introducing another model of computation, Turing machines.

Remarkably, the classes of (partial) functions computed by RAM programs and by Turing machines are identical.

This is the class of partial computable functions, also called partial recursive functions, a term which is now considered old-fashioned.

This class can be given several other definitions. We will present the definition of the so-called μ-recursive functions (due to Kleene).

The following proposition will be needed to simplify the encoding of RAM programs as numbers.

**Proposition 3.1.** Every RAM program can be converted to an equivalent program only using the following type of instructions:

- (1) \( N \ add_j \ Y \)
- (2) \( N \ tail \ Y \)
- (6a) \( N Y \ jmp_j \ N1a \)
- (6b) \( N Y \ jmp_j \ N1b \)
- (7) \( N \ continue \)

The proof is fairly simple. For example, instructions of the form \( Ri \leftarrow Rj \)

can be eliminated by transferring the contents of \( Rj \) into an auxiliary register \( Rk \), and then by transferring the contents of \( Rk \) into \( Ri \) and \( Rj \).

### 3.2 Definition of a Turing Machine

We define a Turing machine model for computing functions

\[
    f: \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_n \rightarrow \Sigma^*,
\]

where \( \Sigma = \{a_1, \ldots, a_N\} \) is some input alphabet. We only consider deterministic Turing machines.

A Turing machine also uses a tape alphabet \( \Gamma \) such that \( \Sigma \subseteq \Gamma \). The tape alphabet contains some special symbol \( B \notin \Sigma \), the blank.
In this model, a Turing machine uses a single tape. This tape can be viewed as a string over $\Gamma$. The tape is both an input tape and a storage mechanism.

Symbols on the tape can be overwritten, and the tape can grow either on the left or on the right. There is a read/write head pointing to some symbol on the tape.

**Definition 3.5.** A (deterministic) *Turing machine* (or *TM*) $M$ is a sextuple $M = (K, \Sigma, \Gamma, \{L, R\}, \delta, q_0)$, where

- $K$ is a finite set of *states*;
- $\Sigma$ is a finite *input alphabet*;
- $\Gamma$ is a finite *tape alphabet*, s.t. $\Sigma \subseteq \Gamma$, $K \cap \Gamma = \emptyset$, and with blank $B \notin \Sigma$;
- $q_0 \in K$ is the *start state* (or *initial state*);
- $\delta$ is the *transition function*, a (finite) set of quintuples

$$\delta \subseteq K \times \Gamma \times \Gamma \times \{L, R\} \times K,$$

such that for all $(p, a) \in K \times \Gamma$, there is at most one triple $(b, m, q) \in \Gamma \times \{L, R\} \times K$ such that $(p, a, b, m, q) \in \delta$.

A quintuple $(p, a, b, m, q) \in \delta$ is called an *instruction*. It is also denoted as

$$p, a \rightarrow b, m, q.$$

The effect of an instruction is to switch from state $p$ to state $q$, overwrite the symbol currently scanned $a$ with $b$, and move the read/write head either left or right, according to $m$.

Here is an example of a Turing machine.

$K = \{q_0, q_1, q_2, q_3\}$;

$\Sigma = \{a, b\}$;

$\Gamma = \{a, b, B\}$;

The instructions in $\delta$ are:
3.3. COMPUTATIONS OF TURING MACHINES

To explain how a Turing machine works, we describe its action on Instantaneous descriptions. We take advantage of the fact that $K \cap \Gamma = \emptyset$ to define instantaneous descriptions.

Definition 3.6. Given a Turing machine

$$M = (K, \Sigma, \Gamma, \{L, R\}, \delta, q_0),$$

an instantaneous description (for short an ID) is a (nonempty) string in $\Gamma^* K \Gamma^+$, that is, a string of the form

$$u p a v,$$

where $u, v \in \Gamma^*$, $p \in K$, and $a \in \Gamma$.

The intuition is that an ID $u p a v$ describes a snapshot of a TM in the current state $p$, whose tape contains the string $u a v$, and with the read/write head pointing to the symbol $a$.

Thus, in $u p a v$, the state $p$ is just to the left of the symbol presently scanned by the read/write head.

We explain how a TM works by showing how it acts on ID’s.

Definition 3.7. Given a Turing machine

$$M = (K, \Sigma, \Gamma, \{L, R\}, \delta, q_0),$$

the yield relation (or compute relation) $\vdash$ is a binary relation defined on the set of ID’s as follows. For any two ID’s $ID_1$ and $ID_2$, we have $ID_1 \vdash ID_2$ iff either

1. $(p, a, b, R, q) \in \delta$, and either

$$q_0, B \to B, R, q_3,$$
$$q_0, a \to b, R, q_1,$$
$$q_0, b \to a, R, q_1,$$
$$q_1, a \to b, R, q_1,$$
$$q_1, b \to a, R, q_1,$$
$$q_1, B \to B, L, q_2,$$
$$q_2, a \to a, L, q_2,$$
$$q_2, b \to b, L, q_2,$$
$$q_2, B \to B, R, q_3.$$. 

$$q_0, B \to B, R, q_3,$$
$$q_0, a \to b, R, q_1,$$
$$q_0, b \to a, R, q_1,$$
$$q_1, a \to b, R, q_1,$$
$$q_1, b \to a, R, q_1,$$
$$q_1, B \to B, L, q_2,$$
$$q_2, a \to a, L, q_2,$$
$$q_2, b \to b, L, q_2,$$
$$q_2, B \to B, R, q_3.$$
(a) $ID_1 = upacv, \ c \in \Gamma, \ and \ ID_2 = ubqcv, \ or$
(b) $ID_1 = upa \ and \ ID_2 = ubqB$,

or

(2) $(p, a, b, L, q) \in \delta, \ and \ either$
(a) $ID_1 = ucpav, \ c \in \Gamma, \ and \ ID_2 = uqcbv, \ or$
(b) $ID_1 = pav \ and \ ID_2 = qBbv$.

Note how the tape is extended by one blank after the rightmost symbol in case (1)(b),
and by one blank before the leftmost symbol in case (2)(b).

As usual, we let $\vdash^+$ denote the transitive closure of $\vdash$, and we let $\vdash^*$ denote
the reflexive and transitive closure of $\vdash$.

We can now explain how a Turing machine computes a partial function

$$f: \Sigma^* \times \cdots \times \Sigma^* \to \Sigma^*.$$ 

Since we allow functions taking $n \geq 1$ input strings, we assume that $\Gamma$ contains the
special delimiter $\$, not in $\Sigma$, used to separate the various input strings.

It is convenient to assume that a Turing machine “cleans up” its tape when it halts,
before returning its output. For this, we will define proper ID’s.

**Definition 3.8.** Given a Turing machine

$$M = (K, \Sigma, \Gamma, \{L, R\}, \delta, q_0),$$

where $\Gamma$ contains some delimiter $\$, not in $\Sigma$ in addition to the blank $B$, a **starting ID** is of
the form

$$q_0w_1, w_2, \ldots, w_n$$

where $w_1, \ldots, w_n \in \Sigma^*$ and $n \geq 2$, or $q_0w$ with $w \in \Sigma^+$, or $q_0B$.

A **blocking (or halting) ID** is an ID $upav$ such that there are no instructions $(p, a, b, m, q) \in \delta$
for any $(b, m, q) \in \Gamma \times \{L, R\} \times K$.

A **proper ID** is a halting ID of the form

$$B^kpwB^l,$$

where $w \in \Sigma^*$, and $k, l \geq 0$ (with $l \geq 1$ when $w = \epsilon$).

Computation sequences are defined as follows.
Definition 3.9. Given a Turing machine
\[ M = (K, \Sigma, \Gamma, \{L, R\}, \delta, q_0), \]
a computation sequence (or computation) is a finite or infinite sequence of ID’s
\[ ID_0, ID_1, \ldots, ID_i, ID_{i+1}, \ldots, \]
such that \( ID_i \vdash ID_{i+1} \) for all \( i \geq 0 \).

A computation sequence halts iff it is a finite sequence of ID’s, so that
\[ ID_0 \vdash^* ID_n, \]
and \( ID_n \) is a halting ID.

A computation sequence diverges if it is an infinite sequence of ID’s.

We now explain how a Turing machine computes a partial function.

Definition 3.10. A Turing machine
\[ M = (K, \Sigma, \Gamma, \{L, R\}, \delta, q_0) \]
computes the partial function
\[ f: \Sigma^* \times \cdots \times \Sigma^* \rightarrow \Sigma^* \]
iff the following conditions hold:

(1) For every \( w_1, \ldots, w_n \in \Sigma^* \), given the starting ID
\[ ID_0 = q_0w_1, w_2, \ldots, w_n \]
or \( q_0w \) with \( w \in \Sigma^+ \), or \( q_0B \), the computation sequence of \( M \) from \( ID_0 \) halts in a proper ID
iff \( f(w_1, \ldots, w_n) \) is defined.

(2) If \( f(w_1, \ldots, w_n) \) is defined, then \( M \) halts in a proper ID of the form
\[ ID_n = B^k pf(w_1, \ldots, w_n) B^h, \]
which means that it computes the right value.

A function \( f \) (over \( \Sigma^* \)) is Turing computable iff it is computed by some Turing machine \( M \).
Note that by (1), the TM $M$ may halt in an improper ID, in which case $f(w_1, \ldots, w_n)$ must be undefined. This corresponds to the fact that we only accept to retrieve the output of a computation if the TM has cleaned up its tape, i.e., produced a proper ID. In particular, intermediate calculations have to be erased before halting.

**Example.**

$K = \{q_0, q_1, q_2, q_3\}$;

$\Sigma = \{a, b\}$;

$\Gamma = \{a, b, B\}$;

The instructions in $\delta$ are:

\[
\begin{align*}
q_0, B & \rightarrow B, R, q_3, \\
nq_0, a & \rightarrow b, R, q_1, \\
nq_0, b & \rightarrow a, R, q_1, \\
nq_1, a & \rightarrow b, R, q_1, \\
nq_1, b & \rightarrow a, R, q_1, \\
nq_1, B & \rightarrow B, L, q_2, \\
nq_2, a & \rightarrow a, L, q_2, \\
nq_2, b & \rightarrow b, L, q_2, \\
nq_2, B & \rightarrow B, R, q_3.
\end{align*}
\]

The reader can easily verify that this machine exchanges the $a$’s and $b$’s in a string. For example, on input $w = aaababb$, the output is $bbbabaa$.

### 3.4 RAM-computable functions are Turing-computable

Turing machines can simulate RAM programs, and as a result, we have the following Theorem.

**Theorem 3.2.** Every RAM-computable function is Turing-computable. Furthermore, given a RAM program $P$, we can effectively construct a Turing machine $M$ computing the same function.

The idea of the proof is to represent the contents of the registers $R1, \ldots, Rp$ on the Turing machine tape by the string

$$#r1#r2# \cdots #rp#,$$
Where \( \# \) is a special marker and \( r_i \) represents the string held by \( R_i \), we also use Proposition 3.1 to reduce the number of instructions to be dealt with.

The Turing machine \( M \) is built of blocks, each block simulating the effect of some instruction of the program \( P \). The details are a bit tedious, and can be found in the notes or in Machtey and Young.

### 3.5 Turing-computable functions are RAM-computable

RAM programs can also simulate Turing machines.

**Theorem 3.3.** Every Turing-computable function is RAM-computable. Furthermore, given a Turing machine \( M \), one can effectively construct a RAM program \( P \) computing the same function.

The idea of the proof is to design a RAM program containing an encoding of the current ID of the Turing machine \( M \) in register \( R_1 \), and to use other registers \( R_2, R_3 \) to simulate the effect of executing an instruction of \( M \) by updating the ID of \( M \) in \( R_1 \).

The details are tedious and can be found in the notes.

Another proof can be obtained by proving that the class of Turing computable functions coincides with the class of *partial computable functions* (formerly called *partial recursive functions*).

Indeed, it turns out that both RAM programs and Turing machines compute precisely the class of partial recursive functions. For this, we need to define the *primitive recursive functions*.

Informally, a primitive recursive function is a total recursive function that can be computed using only *for* loops, that is, loops in which the number of iterations is fixed (unlike a *while* loop).

A formal definition of the primitive functions is given in Section 3.7.

**Definition 3.11.** Let \( \Sigma = \{a_1, \ldots, a_N\} \). The class of *partial computable functions* also called *partial recursive functions* is the class of partial functions (over \( \Sigma^* \)) that can be computed by RAM programs (or equivalently by Turing machines).

The class of *computable functions* also called *recursive functions* is the subset of the class of partial computable functions consisting of functions defined for every input (i.e., total functions).

We can also deal with languages.
3.6 Computably Enumerable Languages and Computable Languages

We define the computably enumerable languages, also called listable languages, and the computable languages.

The old-fashion terminology for computably enumerable languages is recursively enumerable languages, and for computable languages is recursive languages.

We assume that the TM’s under consideration have a tape alphabet containing the special symbols 0 and 1.

**Definition 3.12.** Let $\Sigma = \{a_1, \ldots, a_N\}$. A language $L \subseteq \Sigma^*$ is (Turing) computably enumerable (for short, a c.e. set), or (Turing) listable (or recursively enumerable (for short, a r.e. set)) iff there is some TM $M$ such that for every $w \in L$, $M$ halts in a proper ID with the output 1, and for every $w \notin L$, either $M$ halts in a proper ID with the output 0, or it runs forever.

A language $L \subseteq \Sigma^*$ is (Turing) computable (or recursive) iff there is some TM $M$ such that for every $w \in L$, $M$ halts in a proper ID with the output 1, and for every $w \notin L$, $M$ halts in a proper ID with the output 0.

Thus, given a computably enumerable language $L$, for some $w \notin L$, it is possible that a TM accepting $L$ runs forever on input $w$. On the other hand, for a computable (recursive) language $L$, a TM accepting $L$ always halts in a proper ID.

When dealing with languages, it is often useful to consider nondeterministic Turing machines. Such machines are defined just like deterministic Turing machines, except that their transition function $\delta$ is just a (finite) set of quintuples

$$\delta \subseteq K \times \Gamma \times \Gamma \times \{L, R\} \times K,$$

with no particular extra condition.

It can be shown that every nondeterministic Turing machine can be simulated by a deterministic Turing machine, and thus, nondeterministic Turing machines also accept the class of c.e. sets.

It can be shown that a computably enumerable language is the range of some computable (recursive) function. It can also be shown that a language $L$ is computable (recursive) iff both $L$ and its complement are computably enumerable. There are computably enumerable languages that are not computable (recursive).

Turing machines were invented by Turing around 1935. The primitive recursive functions were known to Hilbert circa 1890. Gödel formalized their definition in 1929. The partial recursive functions were defined by Kleene around 1934.
Church also introduced the $\lambda$-calculus as a model of computation around 1934. Other models: Post systems, Markov systems. The equivalence of the various models of computation was shown around 1935/36. RAM programs were only defined around 1963 (they are a slight generalization of Post system).

A further study of the partial recursive functions requires the notions of pairing functions and of universal functions (or universal Turing machines).

### 3.7 The Primitive Recursive Functions

The class of primitive recursive functions is defined in terms of base functions and closure operations.

**Definition 3.13.** Let $\Sigma = \{a_1, \ldots, a_N\}$. The *base functions* over $\Sigma$ are the following functions:

1. The *erase function* $E$, defined such that $E(w) = \epsilon$, for all $w \in \Sigma^*$;
2. For every $j$, $1 \leq j \leq N$, the *$j$-successor function* $S_j$, defined such that $S_j(w) = wa_j$, for all $w \in \Sigma^*$;
3. The *projection functions* $P^n_i$, defined such that
   
   $$P^n_i(w_1, \ldots, w_n) = w_i,$$
   
   for every $n \geq 1$, every $i$, $1 \leq i \leq n$, and for all $w_1, \ldots, w_n \in \Sigma^*$.

Note that $P^1_1$ is the identity function on $\Sigma^*$. Projection functions can be used to permute the arguments of another function.

A crucial closure operation is (extended) composition.

**Definition 3.14.** Let $\Sigma = \{a_1, \ldots, a_N\}$. For any function

$$g: \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{m} \to \Sigma^*,$$

and any $m$ functions

$$h_i: \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{n} \to \Sigma^*,$$

the *composition of $g$ and the $h_i$* is the function

$$f: \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{n} \to \Sigma^*,$$

denoted as $g \circ (h_1, \ldots, h_m)$, such that

$$f(w_1, \ldots, w_n) = g(h_1(w_1, \ldots, w_n), \ldots, h_m(w_1, \ldots, w_n)),$$

for all $w_1, \ldots, w_n \in \Sigma^*$. 
As an example, \( f = g \circ (P_2^2, P_1^2) \) is such that
\[
f(w_1, w_2) = g(P_2^2(w_1, w_2), P_1^2(w_1, w_2)) = g(w_2, w_1).
\]

Another crucial closure operation is **primitive recursion**.

**Definition 3.15.** Let \( \Sigma = \{a_1, \ldots, a_N\} \). For any function
\[
g: \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_m \rightarrow \Sigma^*,
\]
where \( m \geq 2 \), and any \( N \) functions
\[
h_i: \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{m+1} \rightarrow \Sigma^*,
\]
the function
\[
f: \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_m \rightarrow \Sigma^*,
\]
is defined by **primitive recursion from \( g \) and \( h_1, \ldots, h_N \)**, if
\[
\begin{align*}
f(\epsilon, w_2, \ldots, w_m) &= g(w_2, \ldots, w_m), \\
f(ua_1, w_2, \ldots, w_m) &= h_1(u, f(u, w_2, \ldots, w_m), w_2, \ldots, w_m), \\
& \quad \cdots \\
f(ua_N, w_2, \ldots, w_m) &= h_N(u, f(u, w_2, \ldots, w_m), w_2, \ldots, w_m),
\end{align*}
\]
for all \( u, w_2, \ldots, w_m \in \Sigma^* \).

When \( m = 1 \), for some fixed \( w \in \Sigma^* \), we have
\[
\begin{align*}
f(\epsilon) &= w, \\
f(ua_1) &= h_1(u, f(u)), \\
& \quad \cdots \\
f(ua_N) &= h_N(u, f(u)),
\end{align*}
\]
for all \( u \in \Sigma^* \).

For numerical functions (i.e., when \( \Sigma = \{a_1\} \)), the scheme of primitive recursion is simpler:
\[
\begin{align*}
f(0, x_2, \ldots, x_m) &= g(x_2, \ldots, x_m), \\
f(x + 1, x_2, \ldots, x_m) &= h_1(x, f(x, x_2, \ldots, x_m), x_2, \ldots, x_m),
\end{align*}
\]
for all $x, x_2, \ldots, x_m \in \mathbb{N}$.

The successor function $S$ is the function

$$S(x) = x + 1.$$  

Addition, multiplication, exponentiation, and super-exponentiation, can be defined by primitive recursion as follows (being a bit loose, we should use some projections ...):

$$
\begin{align*}
add(0, n) &= P^1_1(n) = n, \\
add(m + 1, n) &= S \circ P^3_2(m, add(m, n), n) \\
&= S(add(m, n)) \\
mult(0, n) &= E(n) = 0, \\
mult(m + 1, n) &= add \circ (P^3_2, P^3_3)(m, mult(m, n), n) \\
&= add(mult(m, n), n), \\
rexp(0, n) &= S \circ E(n) = 1, \\
rexp(m + 1, n) &= mult(rexp(m, n), n), \\
exp(m, n) &= rexp \circ (P^2_2, P^2_1)(m, n), \\
supexp(0, n) &= 1, \\
supexp(m + 1, n) &= exp(n, supexp(m, n)).
\end{align*}
$$

We usually write $m + n$ for $add(m, n)$, $m \cdot n$ or even $mn$ for $mult(m, n)$, and $m^n$ for $exp(m, n)$.

There is a minus operation on $\mathbb{N}$ named $\text{monus}$. This operation denoted by $\cdot -$ is defined by

$$m \cdot - n = \begin{cases} 
    m - n & \text{if } m \geq n \\
    0 & \text{if } m < n.
\end{cases}$$

To show that it is primitive recursive, we define the function $\text{pred}$. Let $\text{pred}$ be the primitive recursive function given by

$$
\begin{align*}
\text{pred}(0) &= 0 \\
\text{pred}(m + 1) &= P^2_1(m, \text{pred}(m)) = m.
\end{align*}
$$

Then $\text{monus}$ is defined by

$$
\begin{align*}
\text{monus}(m, 0) &= m \\
\text{monus}(m, n + 1) &= \text{pred}(\text{monus}(m, n)),
\end{align*}
$$

except that the above is not a legal primitive recursion. It is left as an exercise to give a proper primitive recursive definition of $\text{monus}$.
As an example over \( \{a, b\}^* \), the following function
\( g: \Sigma^* \times \Sigma^* \to \Sigma^* \), is defined by primitive recursion:

\[
\begin{align*}
g(\epsilon, v) &= P_1^1(v), \\
g(ua_i, v) &= S_i \circ P_2^2(u, g(u, v), v),
\end{align*}
\]

where \( 1 \leq i \leq N \). It is easily verified that \( g(u, v) = vu \). Then,

\[
f = g \circ (P_2^2, P_1^2)
\]

computes the concatenation function, i.e. \( f(u, v) = uv \).

The following functions are also primitive recursive:

\[
sg(n) = \begin{cases} 
1 & \text{if } n > 0 \\
0 & \text{if } n = 0
\end{cases}
\]

\[
\overline{sg}(n) = \begin{cases} 
0 & \text{if } n > 0 \\
1 & \text{if } n = 0
\end{cases}
\]

as well as

\[
abs(m, n) = |m - m| = m - n + n - m,
\]

and

\[
eq(m, n) = \begin{cases} 
1 & \text{if } m = n \\
0 & \text{if } m \neq n
\end{cases}
\]

Indeed

\[
sg(0) = 0
\]

\[
sg(n + 1) = S \circ E \circ P_1^2(n, sg(n)),
\]

\[
\overline{sg}(n) = S(E(n)) \cdot sg(n) = 1 \cdot sg(n),
\]

and

\[
eq(m, n) = sg(|m - n|).
\]

Finally, the function

\[
\text{cond}(m, n, p, q) = \begin{cases} 
p & \text{if } m = n \\
q & \text{if } m \neq n
\end{cases}
\]

is primitive recursive since

\[
\text{cond}(m, n, p, q) = eq(m, n) \ast p + \overline{sg}(eq(m, n)) \ast q.
\]
3.7. THE PRIMITIVE RECURSIVE FUNCTIONS

We can also design more general version of \( \text{cond} \). For example, define \( \text{compare} \leq \) as

\[
\text{compare}_\leq(m, n) = \begin{cases} 
1 & \text{if } m \leq n \\
0 & \text{if } m > n,
\end{cases}
\]

which is given by

\[
\text{compare}_\leq(m, n) = 1 - sg(m - n).
\]

Then we can define

\[
\text{cond}_\leq(m, n, p, q) = \begin{cases} 
p & \text{if } m \leq n \\
q & \text{if } m > n,
\end{cases}
\]

with

\[
\text{cond}_\leq(m, n, n, p) = \text{compare}_\leq(m, n) \ast p + s\overline{g}(\text{compare}_\leq(m, n)) \ast q.
\]

The above allows to define functions by cases.

**Definition 3.16.** Let \( \Sigma = \{a_1, \ldots, a_N\} \). The class of **primitive recursive functions** is the smallest class of functions (over \( \Sigma^* \)) which contains the base functions and is closed under composition and primitive recursion.

We leave as an exercise to show that every primitive recursive function is a total function. The class of primitive recursive functions may not seem very big, but it contains all the total functions that we would ever want to compute.

Although it is rather tedious to prove, the following theorem can be shown.

**Theorem 3.4.** For an alphabet \( \Sigma = \{a_1, \ldots, a_N\} \), every primitive recursive function is Turing computable.

The best way to prove the above theorem is to use the computation model of RAM programs. Indeed, it was shown in Theorem 3.2 that every RAM program can be converted to a Turing machine.

It is also rather easy to show that the primitive recursive functions are RAM-computable.

In order to define new functions it is also useful to use predicates.

**Definition 3.17.** An \( n \)-ary predicate \( P \) (over \( \Sigma^* \)) is any subset of \((\Sigma^*)^n\). We write that a tuple \((x_1, \ldots, x_n)\) satisfies \( P \) as \((x_1, \ldots, x_n) \in P\) or as \( P(x_1, \ldots, x_n) \). The **characteristic function** of a predicate \( P \) is the function \( C_P : (\Sigma^*)^n \rightarrow \{a_1\}^* \) defined by

\[
C_P(x_1, \ldots, x_n) = \begin{cases} 
a_1 & \text{iff } P(x_1, \ldots, x_n) \\
\epsilon & \text{iff not } P(x_1, \ldots, x_n).
\end{cases}
\]

A predicate \( P \) is **primitive recursive** iff its characteristic function \( C_P \) is primitive recursive.
We leave to the reader the obvious adaptation of the notion of primitive recursive predicate to functions defined over \( \mathbb{N} \). In this case, 0 plays the role of \( \epsilon \) and 1 plays the role of \( a_1 \).

It is easily shown that if \( P \) and \( Q \) are primitive recursive predicates (over \(( \Sigma^* )^n\)), then \( P \lor Q \), \( P \land Q \) and \( \neg P \) are also primitive recursive.

As an exercise, the reader may want to prove that the predicate (defined over \( \mathbb{N} \)):
\[
\text{prime}(n) \text{ iff } n \text{ is a prime number},
\]
is a primitive recursive predicate.

For any fixed \( k \geq 1 \), the function:
\[
\text{ord}(k, n) = \text{exponent of the } k\text{th prime in the prime factorization of } n,
\]
is a primitive recursive function.

We can also define functions by cases.

**Proposition 3.5.** If \( P_1, \ldots, P_n \) are pairwise disjoint primitive recursive predicates (which means that \( P_i \cap P_j = \emptyset \) for all \( i \neq j \)) and \( f_1, \ldots, f_{n+1} \) are primitive recursive functions, the function \( g \) defined below is also primitive recursive:
\[
g(\bar{x}) = \begin{cases} 
  f_1(\bar{x}) & \text{iff } P_1(\bar{x}) \\
  \vdots \\
  f_n(\bar{x}) & \text{iff } P_n(\bar{x}) \\
  f_{n+1}(\bar{x}) & \text{otherwise}.
\end{cases}
\]
(\text{writing } \bar{x} \text{ for } (x_1, \ldots, x_n).)

It is also useful to have bounded quantification and bounded minimization.

**Definition 3.18.** If \( P \) is an \((n+1)\)-ary predicate, then the **bounded existential predicate** \( \exists y/x P(y, z) \) holds iff some prefix \( y \) of \( x \) makes \( P(y, z) \) true.

The **bounded universal predicate** \( \forall y/x P(y, z) \) holds iff every prefix \( y \) of \( x \) makes \( P(y, z) \) true.

**Proposition 3.6.** If \( P \) is an \((n+1)\)-ary primitive recursive predicate, then \( \exists y/x P(y, z) \) and \( \forall y/x P(y, z) \) are also primitive recursive predicates.

As an application, we can show that the equality predicate, \( u = v \)?, is primitive recursive.

**Definition 3.19.** If \( P \) is an \((n+1)\)-ary predicate, then the **bounded minimization of } \), \( P \), \( \text{min } y/x P(y, z) \), is the function defined such that \( \text{min } y/x P(y, z) \) is the shortest prefix of \( x \) such that \( P(y, z) \) if such a \( y \) exists, \( xa_1 \) otherwise.

The **bounded maximization of } \), \( P \), \( \text{max } y/x P(y, z) \), is the function defined such that \( \text{max } y/x P(y, z) \) is the longest prefix of \( x \) such that \( P(y, z) \) if such a \( y \) exists, \( xa_1 \) otherwise.
Proposition 3.7. If \( P \) is an \((n + 1)\)-ary primitive recursive predicate, then \( \min y/x P(y, z) \) and \( \max y/x P(y, z) \) are primitive recursive functions.

So far, the primitive recursive functions do not yield all the Turing-computable functions. In order to get a larger class of functions, we need the closure operation known as minimization.

3.8 The Partial Computable Functions

Minimization can be viewed as an abstract version of a while loop.

Let \( \Sigma = \{a_1, \ldots, a_N\} \). For any function

\[
g : \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{m+1} \rightarrow \Sigma^*,
\]

where \( m \geq 0 \), for every \( j, 1 \leq j \leq N \), the function

\[
f : \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{m} \rightarrow \Sigma^*
\]

looks for the shortest string \( u \) over \( a_j^* \) (for a given \( j \)) such that

\[
g(u, w_1, \ldots, w_m) = \epsilon : u := \epsilon;
\]

\[\text{while } g(u, w_1, \ldots, w_m) \neq \epsilon \text{ do} \]

\[u := ua_j;\]

\[\text{endwhile}\]

\[\text{let } f(w_1, \ldots, w_m) = u\]

The operation of minimization (sometimes called minimalization) is defined as follows.

Definition 3.20. Let \( \Sigma = \{a_1, \ldots, a_N\} \). For any function

\[
g : \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{m+1} \rightarrow \Sigma^*,
\]

where \( m \geq 0 \), for every \( j, 1 \leq j \leq N \), the function

\[
f : \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{m} \rightarrow \Sigma^*,
\]

is defined by \emph{minimization over} \( \{a_j\}^* \) \emph{from} \( g \), if the following conditions hold for all \( w_1, \ldots, w_m \in \Sigma^* \):
(1) \( f(w_1, \ldots, w_m) \) is defined iff there is some \( n \geq 0 \) such that \( g(a_j^p, w_1, \ldots, w_m) \) is defined for all \( p, 0 \leq p \leq n \), and \( g(a_j^n, w_1, \ldots, w_m) = \epsilon \).

(2) When \( f(w_1, \ldots, w_m) \) is defined,
\[
f(w_1, \ldots, w_m) = a_j^n,
\]
where \( n \) is such that
\[
g(a_j^n, w_1, \ldots, w_m) = \epsilon
\]
and
\[
g(a_j^p, w_1, \ldots, w_m) \neq \epsilon
\]
for every \( p, 0 \leq p \leq n - 1 \).

We also write
\[
f(w_1, \ldots, w_m) = \min_j \{ u : g(u, w_1, \ldots, w_m) = \epsilon \}.
\]

Note: When \( f(w_1, \ldots, w_m) \) is defined,
\[
f(w_1, \ldots, w_m) = a_j^n,
\]
where \( n \) is the smallest integer such that condition (1) holds. It is very important to require that all the values \( g(a_j^p, w_1, \ldots, w_m) \) be defined for all \( p, 0 \leq p \leq n \), when defining \( f(w_1, \ldots, w_m) \). Failure to do so allows non-computable functions.

Remark: Kleene used the \( \mu \)-notation:
\[
f(w_1, \ldots, w_m) = \mu_j \{ u : g(u, w_1, \ldots, w_m) = \epsilon \},
\]
actually, its numerical form:
\[
f(x_1, \ldots, x_m) = \mu x \{ g(x, x_1, \ldots, x_m) = 0 \}.
\]

The class of partial computable functions is defined as follows.

**Definition 3.21.** Let \( \Sigma = \{ a_1, \ldots, a_N \} \). The class of partial computable functions also called partial recursive functions is the smallest class of partial functions (over \( \Sigma^* \)) which contains the base functions and is closed under composition, primitive recursion, and minimization.

The class of computable functions also called recursive functions is the subset of the class of partial computable functions consisting of functions defined for every input (i.e., total functions).

One of the major results of computability theory is the following theorem.
Theorem 3.8. For an alphabet $\Sigma = \{a_1, \ldots, a_N\}$, every partial computable function (partial recursive function) is Turing-computable. Conversely, every Turing-computable function is a partial computable function (partial recursive function). Similarly, the class of computable functions (recursive functions) is equal to the class of Turing-computable functions that halt in a proper ID for every input.

To prove that every partial computable function is indeed Turing-computable, since by Theorem 3.2, every RAM program can be converted to a Turing machine, the simplest thing to do is to show that every partial computable function is RAM-computable.

For the converse, one can show that given a Turing machine, there is a primitive recursive function describing how to go from one ID to the next. Then, minimization is used to guess whether a computation halts. The proof shows that every partial computable function needs minimization at most once. The characterization of the computable functions in terms of TM’s follows easily.

There are computable functions (recursive functions) that are not primitive recursive. Such an example is given by Ackermann’s function.

**Ackermann’s function.**

This is a function $A: \mathbb{N} \times \mathbb{N} \rightarrow \mathbb{N}$ which is defined by the following recursive clauses:

\[
A(0, y) = y + 1, \\
A(x + 1, 0) = A(x, 1), \\
A(x + 1, y + 1) = A(x, A(x + 1, y)).
\]

It turns out that $A$ is a computable function which is not primitive recursive. It can be shown that:

\[
A(0, x) = x + 1, \\
A(1, x) = x + 2, \\
A(2, x) = 2x + 3, \\
A(3, x) = 2^{x+3} - 3,
\]

and

\[
A(4, x) = 2^{2^{2^{16}} - 3},
\]

with $A(4, 0) = 16 - 3 = 13$.

For example

\[
A(4, 1) = 2^{16} - 3, \quad A(4, 2) = 2^{2^{16}} - 3.
\]
Actually, it is not so obvious that $A$ is a total function. This can be shown by induction, using the lexicographic ordering $\preceq$ on $\mathbb{N} \times \mathbb{N}$, which is defined as follows:

$$(m, n) \preceq (m', n') \text{ iff either}$$

$$(m = m' \text{ and } n = n'), \text{ or}$$

$$m < m', \text{ or}$$

$$m = m' \text{ and } n < n'.$$

We write $(m, n) \prec (m', n')$ when $(m, n) \preceq (m', n')$ and $(m, n) \neq (m', n').$

We prove that $A(m, n)$ is defined for all $(m, n) \in \mathbb{N} \times \mathbb{N}$ by complete induction over the lexicographic ordering on $\mathbb{N} \times \mathbb{N}$.

In the base case, $(m, n) = (0, 0)$, and since $A(0, n) = n + 1$, we have $A(0, 0) = 1$, and $A(0, 0)$ is defined.

For $(m, n) \neq (0, 0)$, the induction hypothesis is that $A(m', n')$ is defined for all $(m', n') \prec (m, n)$. We need to conclude that $A(m, n)$ is defined.

If $m = 0$, since $A(0, n) = n + 1$, $A(0, n)$ is defined.

If $m \neq 0$ and $n = 0$, since

$$(m - 1, 1) \prec (m, 0),$$

by the induction hypothesis, $A(m - 1, 1)$ is defined, but $A(m, 0) = A(m - 1, 1)$, and thus $A(m, 0)$ is defined.

If $m \neq 0$ and $n \neq 0$, since

$$(m, n - 1) \prec (m, n),$$

by the induction hypothesis, $A(m, n - 1)$ is defined. Since

$$(m - 1, A(m, n - 1)) \prec (m, n),$$

by the induction hypothesis, $A(m - 1, A(m, n - 1))$ is defined. But $A(m, n) = A(m - 1, A(m, n - 1))$, and thus $A(m, n)$ is defined.

Thus, $A(m, n)$ is defined for all $(m, n) \in \mathbb{N} \times \mathbb{N}$. It is possible to show that $A$ is a recursive function, although the quickest way to prove it requires some fancy machinery (the recursion theorem).

Proving that $A$ is not primitive recursive is harder.

The following proposition shows that restricting ourselves to total functions is too limiting.

Let $\mathcal{F}$ be any set of total functions that contains the base functions and is closed under composition and primitive recursion (and thus, $\mathcal{F}$ contains all the primitive recursive functions).
Definition 3.22. We say that a function \( f : \Sigma^* \times \Sigma^* \to \Sigma^* \) is \textit{universal} for the one-argument functions in \( \mathcal{F} \) iff for every function \( g : \Sigma^* \to \Sigma^* \) in \( \mathcal{F} \), there is some \( n \in \mathbb{N} \) such that
\[
f(a^n_1, u) = g(u)
\]
for all \( u \in \Sigma^* \).

Proposition 3.9. For any countable set \( \mathcal{F} \) of total functions containing the base functions and closed under composition and primitive recursion, if \( f \) is a universal function for the functions \( g : \Sigma^* \to \Sigma^* \) in \( \mathcal{F} \), then \( f \notin \mathcal{F} \).

Proof. Assume that the universal function \( f \) is in \( \mathcal{F} \). Let \( g \) be the function such that
\[
g(u) = f(a^{\mid u\mid}_1, u)a_1
\]
for all \( u \in \Sigma^* \). We claim that \( g \in \mathcal{F} \). It it enough to prove that the function \( h \) such that
\[
h(u) = a^{\mid u\mid}_1
\]
is primitive recursive, which is easily shown.

Then, because \( f \) is universal, there is some \( m \) such that
\[
g(u) = f(a^m_1, u)
\]
for all \( u \in \Sigma^* \). Letting \( u = a^m_1 \), we get
\[
g(a^m_1) = f(a^m_1, a^m_1) = f(a^m_1, a^m_1)a_1,
\]
a contradiction. \( \square \)

Thus, either a universal function for \( \mathcal{F} \) is partial, or it is not in \( \mathcal{F} \).
Chapter 4

Universal RAM Programs and Undecidability of the Halting Problem

4.1 Pairing Functions

Pairing functions are used to encode pairs of integers into single integers, or more generally, finite sequences of integers into single integers. We begin by exhibiting a bijective pairing function $J : \mathbb{N}^2 \rightarrow \mathbb{N}$. The function $J$ has the graph partially showed below:

\[
\begin{array}{cccccccccccc}
& & & & & & & & 0 & 1 & 2 & 3 & 4 \\
& & & & & & & 0 & 2 & 5 & 9 & 14 \\
& & & & & & 1 & 1 & 4 & 8 & 13 \\
& & & & 2 & 3 & 7 & 12 \\
& & 3 & 6 & 11 \\
& 4 & 10 \\
\end{array}
\]

The function $J$ corresponds to a certain way of enumerating pairs of integers $(x, y)$. Note that the value of $x + y$ is constant along each descending diagonal, and consequently, we have

\[
J(x, y) = 1 + 2 + \cdots + (x + y) + x,
\]

\[
= ((x + y)(x + y + 1) + 2x)/2,
\]

\[
= ((x + y)^2 + 3x + y)/2,
\]

that is,

\[
J(x, y) = ((x + y)^2 + 3x + y)/2.
\]
For example, \( J(0, 3) = 6 \), \( J(1, 2) = 7 \), \( J(2, 2) = 12 \), \( J(3, 1) = 13 \), \( J(4, 0) = 14 \).

Let \( K : \mathbb{N} \to \mathbb{N} \) and \( L : \mathbb{N} \to \mathbb{N} \) be the projection functions onto the axes, that is, the unique functions such that

\[
K(J(a, b)) = a \quad \text{and} \quad L(J(a, b)) = b,
\]

for all \( a, b \in \mathbb{N} \). For example, \( K(11) = 1 \), and \( L(11) = 3 \); \( K(12) = 2 \), and \( L(12) = 2 \); \( K(13) = 3 \) and \( L(13) = 1 \).

The functions \( J, K, L \) are called Cantor’s pairing functions. They were used by Cantor to prove that the set \( \mathbb{Q} \) of rational numbers is countable.

Clearly, \( J \) is primitive recursive, since it is given by a polynomial. It is not hard to prove that \( J \) is injective and surjective, and that it is strictly monotonic in each argument, which means that for all \( x, x', y, y' \in \mathbb{N} \), if \( x < x' \) then \( J(x, y) < J(x', y) \), and if \( y < y' \) then \( J(x, y) < J(x, y') \).

The projection functions can be computed explicitly, although this is a bit tricky. We only need to observe that by monotonicity of \( J \),

\[
x \leq J(x, y) \quad \text{and} \quad y \leq J(x, y),
\]

and thus,

\[
K(z) = \min(x \leq z)(\exists y \leq z)[J(x, y) = z],
\]

and

\[
L(z) = \min(y \leq z)(\exists x \leq z)[J(x, y) = z].
\]

Therefore, \( K \) and \( L \) are primitive recursive. It can be verified that \( J(K(z), L(z)) = z \), for all \( z \in \mathbb{N} \).

More explicit formulae can be given for \( K \) and \( L \). If we define

\[
Q_1(z) = \lfloor \sqrt{8z + 1} \rfloor + 1/2 - 1,
\]

\[
Q_2(z) = 2z - (Q_1(z))^2,
\]

then it can be shown that

\[
K(z) = \frac{1}{2}(Q_2(z) - Q_1(z))
\]

\[
L(z) = Q_1(z) - \frac{1}{2}(Q_2(z) - Q_1(z)).
\]

In the above formula, the function \( m \mapsto \lfloor \sqrt{m} \rfloor \) yields the largest integer \( s \) such that \( s^2 \leq m \). It can be computed by a RAM program.

The pairing function \( J(x, y) \) is also denoted as \( \langle x, y \rangle \), and \( K \) and \( L \) are also denoted as \( \Pi_1 \) and \( \Pi_2 \).
By induction, we can define bijections between \( \mathbb{N}^n \) and \( \mathbb{N} \) for all \( n \geq 1 \). We let \( \langle z \rangle_1 = z \),

\[
\langle x_1, x_2 \rangle_2 = \langle x_1, x_2 \rangle,
\]

and

\[
\langle x_1, \ldots, x_n, x_{n+1} \rangle_{n+1} = \langle x_1, \ldots, x_{n-1}, \langle x_n, x_{n+1} \rangle \rangle_n.
\]

For example.

\[
\langle x_1, x_2, x_3 \rangle_3 = \langle x_1, \langle x_2, x_3 \rangle \rangle_2 = \langle x_1, x_2, x_3 \rangle
\]

\[
\langle x_1, x_2, x_3, x_4 \rangle_4 = \langle x_1, x_2, \langle x_3, x_4 \rangle \rangle_3 = \langle x_1, x_2, x_3, x_4 \rangle
\]

\[
\langle x_1, x_2, x_3, x_4, x_5 \rangle_5 = \langle x_1, x_2, x_3, \langle x_4, x_5 \rangle \rangle_4 = \langle x_1, x_2, x_3, x_4, x_5 \rangle
\]

It can be shown by induction on \( n \) that

\[
\langle x_1, \ldots, x_n, x_{n+1} \rangle_{n+1} = \langle x_1, \langle x_2, \ldots, x_{n+1} \rangle \rangle_n.
\]

The function \( \langle -, \ldots, - \rangle_n : \mathbb{N}^n \to \mathbb{N} \) is called an extended pairing function.

Observe that if \( z = \langle x_1, \ldots, x_n \rangle_n \), then \( x_1 = \Pi_1(z) \), \( x_2 = \Pi_1(\Pi_2(z)) \), \( x_3 = \Pi_1(\Pi_2(\Pi_2(z))) \), \( x_4 = \Pi_1(\Pi_2(\Pi_2(\Pi_2(z)))) \), \( x_5 = \Pi_2(\Pi_2(\Pi_2(\Pi_2(z)))) \).

We can also define a uniform projection function \( \Pi \) with the following property: if \( z = \langle x_1, \ldots, x_n \rangle \), with \( n \geq 2 \), then

\[
\Pi(i, n, z) = x_i
\]

for all \( i \), where \( 1 \leq i \leq n \). The idea is to view \( z \) as a \( n \)-tuple, and \( \Pi(i, n, z) \) as the \( i \)-th component of that \( n \)-tuple. The function \( \Pi \) is defined by cases as follows:

\[
\Pi(i, 0, z) = 0, \quad \text{for all } i \geq 0,
\]

\[
\Pi(i, 1, z) = z, \quad \text{for all } i \geq 0,
\]

\[
\Pi(i, 2, z) = \Pi_1(z), \quad \text{if } 0 \leq i \leq 1,
\]

\[
\Pi(i, 2, z) = \Pi_2(z), \quad \text{for all } i \geq 2,
\]

and for all \( n \geq 2 \),

\[
\Pi(i, n+1, z) = \begin{cases} 
\Pi(i, n, z) & \text{if } 0 \leq i < n, \\
\Pi_1(\Pi(n, n, z)) & \text{if } i = n, \\
\Pi_2(\Pi(n, n, z)) & \text{if } i > n.
\end{cases}
\]

By a previous exercise, this is a legitimate primitive recursive definition.

Some basic properties of \( \Pi \) are given as exercises. In particular, the following properties are easily shown:
(a) \( \langle 0, \ldots, 0 \rangle_n = 0, \langle x, 0 \rangle = \langle x, 0, \ldots, 0 \rangle_n \);

(b) \( \Pi(0, n, z) = \Pi(1, n, z) \) and \( \Pi(i, n, z) = \Pi(n, n, z) \), for all \( i \geq n \) and all \( n, z \in \mathbb{N} \);

(c) \( \langle \Pi(1, n, z), \ldots, \Pi(n, n, z) \rangle_n = z \), for all \( n \geq 1 \) and all \( z \in \mathbb{N} \);

(d) \( \Pi(i, n, z) \leq z \), for all \( i, n, z \in \mathbb{N} \);

(e) There is a primitive recursive function Large, such that,

\[ \Pi(i, n + 1, \text{Large}(n + 1, z)) = z, \]

for \( i, n, z \in \mathbb{N} \).

As a first application, we observe that we need only consider partial computable functions (partial recursive functions)\(^1\) of a single argument. Indeed, let \( \varphi : \mathbb{N}^n \to \mathbb{N} \) be a partial computable function of \( n \geq 2 \) arguments. Let

\[ \overline{\varphi}(z) = \varphi(\Pi(1, n, z), \ldots, \Pi(n, n, z)), \]

for all \( z \in \mathbb{N} \). Then, \( \overline{\varphi} \) is a partial computable function of a single argument, and \( \varphi \) can be recovered from \( \overline{\varphi} \), since

\[ \varphi(x_1, \ldots, x_n) = \overline{\varphi}(\langle x_1, \ldots, x_n \rangle). \]

Thus, using \( \langle -, - \rangle \) and \( \Pi \) as coding and decoding functions, we can restrict our attention to functions of a single argument.

Next, we show that there exist coding and decoding functions between \( \Sigma^* \) and \( \{a_1\}^* \), and that partial computable functions over \( \Sigma^* \) can be recoded as partial computable functions over \( \{a_1\}^* \). Since \( \{a_1\}^* \) is isomorphic to \( \mathbb{N} \), this shows that we can restrict out attention to functions defined over \( \mathbb{N} \).

### 4.2 Equivalence of Alphabets

Given an alphabet \( \Sigma = \{a_1, \ldots, a_k\} \), strings over \( \Sigma \) can be ordered by viewing strings as numbers in a number system where the digits are \( a_1, \ldots, a_k \). In this number system, which is almost the number system with base \( k \), the string \( a_i \) corresponds to zero, and \( a_k \) to \( k - 1 \). Hence, we have a kind of shifted number system in base \( k \). For example, if \( \Sigma = \{a, b, c\} \), a listing of \( \Sigma^* \) in the ordering corresponding to the number system begins with

\[ a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, aaa, aab, aac, aba, abb, abc, \ldots. \]

Clearly, there is an ordering function from \( \Sigma^* \) to \( \mathbb{N} \) which is a bijection. Indeed, if \( u = a_{i_1} \cdots a_{i_n} \), this function \( f : \Sigma^* \to \mathbb{N} \) is given by

\[ f(u) = i_1 k^{n-1} + i_2 k^{n-2} + \cdots + i_{n-1} k + i_n. \]

\(^1\)The term *partial recursive* is now considered old-fashioned. Many researchers have switched to the term *partial computable*.
4.2. EQUIVALENCE OF ALPHABETS

Since we also want a decoding function, we define the coding function \( C_k : \Sigma^* \rightarrow \Sigma^* \) as follows:

\[ C_k(\epsilon) = \epsilon, \quad \text{and if } u = a_{i_1} \cdots a_{i_n}, \text{ then } \]
\[ C_k(u) = a_{i_1}^{i_1 k^{i_1 k - 1 + i_2 k^{i_2 k - 2} + \cdots + i_{n-1} k^{i_{n-1} k - 1} + i_n}. \]

The function \( C_k \) is primitive recursive, because

\[ C_k(\epsilon) = \epsilon, \]
\[ C_k(x a_i) = C_k(x)^{i} a_i. \]

The inverse of \( C_k \) is a function \( D_k : \{a_1\}^* \rightarrow \Sigma^* \). However, primitive recursive functions are total, and we need to extend \( D_k \) to \( \Sigma^* \). This is easily done by letting

\[ D_k(x) = D_k(a_1^{\left| x \right|}) \]

for all \( x \in \Sigma^* \). It remains to define \( D_k \) by primitive recursion over \( \Sigma^* = \{a_1, \ldots, a_k\}^* \). For this, we introduce three auxiliary functions \( p, q, r \), defined as follows. Let

\[ p(\epsilon) = \epsilon, \]
\[ p(x a_i) = x a_i, \quad \text{if } i \neq k, \]
\[ p(x a_k) = p(x). \]

Note that \( p(x) \) is the result of deleting consecutive \( a_k \)'s in the tail of \( x \). Let

\[ q(\epsilon) = \epsilon, \]
\[ q(x a_i) = q(x) a_1. \]

Note that \( q(x) = a_1^{\left| x \right|} \). Finally, let

\[ r(\epsilon) = a_1, \]
\[ r(x a_i) = x a_{i+1}, \quad \text{if } i \neq k, \]
\[ r(x a_k) = x a_k. \]

The function \( r \) is almost the successor function for the ordering. Then the trick is that \( D_k(x a_i) \) is the successor of \( D_k(x) \) in the ordering so usually \( D_k(x a_i) = r(D_k(x)) \), except if

\[ D_k(x) = y a_j a_k^n \]

with \( j \neq k \), since the successor of \( y a_j a_k^n \) is \( y a_{j+1} a_k^n \). Thus, we have

\[ D_k(\epsilon) = \epsilon, \]
\[ D_k(x a_i) = r(p(D_k(x)))q(D_k(x) - p(D_k(x))), \quad a_i \in \Sigma. \]
Then, both $C_k$ and $D_k$ are primitive recursive, and $D_k \circ C_k = \text{id}$. Here

$$u - v = \begin{cases} 
\epsilon & \text{if } |u| \leq |v| \\
w & \text{if } u = xw \text{ and } |x| = |v|.
\end{cases}$$

In other words, $u - v$ is $u$ with its first $|v|$ letters deleted. We can show that this function can be defined by primitive recursion by first defining $\text{rdiff}(u, v)$ as $v$ with its first $|u|$ letters deleted, and then

$$u - v = \text{rdiff}(v, u).$$

To define $\text{rdiff}$, we use $\text{tail}$ given by

$$\text{tail}(\epsilon) = \epsilon,$$

$$\text{tail}(a_iu) = u, \quad a_i \in \Sigma, \ u \in \Sigma^*.$$

To show that $\text{tail}$ is primitive recursive, we can show that

$$\text{tail}(u) = \text{rev}(\text{dell}(\text{rev}(u))),$$

where $\text{rev}(u) = u^R$ (the reverse function) and $\text{dell}$ is given by

$$\text{dell}(\epsilon) = \epsilon,$$

$$\text{dell}(ua_i) = u, \quad a_i \in \Sigma.$$

Then

$$\text{rdiff}(\epsilon, v) = v,$$

$$\text{rdiff}(ua_i, v) = \text{rdiff}(u, \text{tail}(v)), \quad a_i \in \Sigma.$$

We leave as an exercise to put all these definitions into the proper format of primitive recursion using projections.

Let $\varphi: \Sigma^* \to \Sigma^*$ be a partial function over $\Sigma^*$, and let

$$\varphi^+(x_1, \ldots, x_n) = C_k(\varphi(D_k(x_1), \ldots, D_k(x_n))).$$

The function $\varphi^+$ is defined over $\{a_1\}^*$. Also, for any partial function $\psi$ over $\{a_1\}^*$, let

$$\psi^*(x_1, \ldots, x_n) = D_k(\psi(C_k(x_1), \ldots, C_k(x_n))).$$

We claim that if $\psi$ is a partial computable function over $\{a_1\}^*$, then $\psi^*$ is partial computable over $\Sigma^*$, and that if $\varphi$ is a partial computable function over $\Sigma^*$, then $\varphi^+$ is partial computable over $\{a_1\}^*$.

First, $\psi$ can be extended to $\Sigma^*$ by letting

$$\psi(x) = \psi(a_1^{|x|})$$
for all $x \in \Sigma^*$, and so, if $\psi$ is partial computable, then so is $\psi^z$ by composition. This seems equally obvious for $\varphi$ and $\varphi^+$, but there is a difficulty. The problem is that $\varphi^+$ is defined as a composition of functions over $\Sigma^*$. We have to show how $\varphi^+$ can be defined directly over $\{a_1\}^*$ without using any additional alphabet symbols. This is done in Machtey and Young [18], see Section 2.2, Lemma 2.2.3.

Pairing functions can also be used to prove that certain functions are primitive recursive, even though their definition is not a legal primitive recursive definition. For example, consider the Fibonacci function defined as follows:

$$
\begin{align*}
  f(0) &= 1, \\
  f(1) &= 1, \\
  f(n+2) &= f(n+1) + f(n),
\end{align*}
$$

for all $n \in \mathbb{N}$. This is not a legal primitive recursive definition, since $f(n+2)$ depends both on $f(n+1)$ and $f(n)$. In a primitive recursive definition, $g(y+1, x)$ is only allowed to depend upon $g(y, x)$.

**Definition 4.1.** Given any function $f : \mathbb{N}^n \to \mathbb{N}$, the function $\overline{f} : \mathbb{N}^{n+1} \to \mathbb{N}$ defined such that

$$
\overline{f}(y, x) = \langle f(0, x), \ldots, f(y, x) \rangle_{y+1}
$$

is called the *course-of-value function* for $f$.

The following lemma holds.

**Proposition 4.1.** Given any function $f : \mathbb{N}^n \to \mathbb{N}$, if $f$ is primitive recursive, then so is $\overline{f}$.

**Proof.** First, it is necessary to define a function $\text{con}$ such that if $x = \langle x_1, \ldots, x_m \rangle$ and $y = \langle y_1, \ldots, y_n \rangle$, where $m, n \geq 1$, then

$$
\text{con}(m, x, y) = \langle x_1, \ldots, x_m, y_1, \ldots, y_n \rangle.
$$

This fact is left as an exercise. Now, if $f$ is primitive recursive, let

$$
\begin{align*}
  \overline{f}(0, x) &= f(0, x), \\
  \overline{f}(y+1, x) &= \text{con}(y+1, \overline{f}(y, x), f(y+1, x)),
\end{align*}
$$

showing that $\overline{f}$ is primitive recursive. Conversely, if $\overline{f}$ is primitive recursive, then

$$
  f(y, x) = \Pi(y+1, y+1, \overline{f}(y, x)),
$$

and so, $f$ is primitive recursive. \(\square\)

**Remark:** Why is it that

$$
\overline{f}(y+1, x) = \langle \overline{f}(y, x), f(y+1, x) \rangle
$$

does not work?

We define *course-of-value recursion* as follows.
Definition 4.2. Given any two functions \( g : \mathbb{N}^n \rightarrow \mathbb{N} \) and \( h : \mathbb{N}^{n+2} \rightarrow \mathbb{N} \), the function \( f : \mathbb{N}^{n+1} \rightarrow \mathbb{N} \) is defined by course-of-value recursion from \( g \) and \( h \) if

\[
\begin{align*}
    f(0, \bar{x}) &= g(\bar{x}), \\
    f(y + 1, \bar{x}) &= h(y, f(y, \bar{x}), \bar{x}).
\end{align*}
\]

The following lemma holds.

Proposition 4.2. If \( f : \mathbb{N}^{n+1} \rightarrow \mathbb{N} \) is defined by course-of-value recursion from \( g \) and \( h \) and \( g, h \) are primitive recursive, then \( f \) is primitive recursive.

Proof. We prove that \( \overline{f} \) is primitive recursive. Then, by Proposition 4.1, \( f \) is also primitive recursive. To prove that \( \overline{f} \) is primitive recursive, observe that

\[
\begin{align*}
    \overline{f}(0, \bar{x}) &= g(\bar{x}), \\
    \overline{f}(y + 1, \bar{x}) &= \text{con}(y + 1, \overline{f}(y, \bar{x}), h(y, \overline{f}(y, \bar{x}), \bar{x})).
\end{align*}
\]

When we use Proposition 4.2 to prove that a function is primitive recursive, we rarely bother to construct a formal course-of-value recursion. Instead, we simply indicate how the value of \( f(y + 1, \bar{x}) \) can be obtained in a primitive recursive manner from \( f(0, \bar{x}) \) through \( f(y, \bar{x}) \). Thus, an informal use of Proposition 4.2 shows that the Fibonacci function is primitive recursive. A rigorous proof of this fact is left as an exercise.

4.3 Coding of RAM Programs

In this Section, we present a specific encoding of RAM programs which allows us to treat programs as integers. Encoding programs as integers also allows us to have programs that take other programs as input, and we obtain a universal program. Universal programs have the property that given two inputs, the first one being the code of a program and the second one an input data, the universal program simulates the actions of the encoded program on the input data. A coding scheme is also called an indexing or a Gödel numbering, in honor to Gödel, who invented this technique.

From results of the previous Chapter, without loss of generality, we can restrict our attention to RAM programs computing partial functions of one argument over \( \mathbb{N} \). Furthermore, we only need the following kinds of instructions, each instruction being coded as shown below. Since we are considering functions over the natural numbers, which corresponds to a one-letter alphabet, there is only one kind of instruction of the form \texttt{add} and \texttt{jmp} (and \texttt{add} increments by 1 the contents of the specified register \( R_j \)).
4.3. CODING OF RAM PROGRAMS

Recall that a conditional jump causes a jump to the closest address $Nk$ above or below iff $Rj$ is nonzero, and if $Rj$ is null, the next instruction is executed. We assume that all lines in a RAM program are numbered. This is always feasible, by labeling unnamed instructions with a new and unused line number.

The code of an instruction $I$ is denoted as $\#I$. To simplify the notation, we introduce the following decoding primitive recursive functions $\text{Typ}$, $\text{Nam}$, $\text{Reg}$, and $\text{Jmp}$, defined as follows:

$$\text{Typ}(x) = \Pi(1, 4, x),$$
$$\text{Nam}(x) = \Pi(2, 4, x),$$
$$\text{Reg}(x) = \Pi(3, 4, x),$$
$$\text{Jmp}(x) = \Pi(4, 4, x).$$

The functions yield the type, line number, register name, and line number jumped to, if any, for an instruction coded by $x$. Note that we have no need to interpret the values of these functions if $x$ does not code an instruction.

We can define the primitive recursive predicate $\text{INST}$, such that $\text{INST}(x)$ holds iff $x$ codes an instruction. First, we need the connective $\supset$ (implies), defined such that

$$P \supset Q \iff \neg P \lor Q.$$  

Then, $\text{INST}(x)$ holds iff:

$$[1 \leq \text{Typ}(x) \leq 5] \land [1 \leq \text{Reg}(x)] \land$$
$$[\text{Typ}(x) \leq 3 \supset \text{Jmp}(x) = 0] \land$$
$$[\text{Typ}(x) = 3 \supset \text{Reg}(x) = 1].$$

Programs are coded as follows. If $P$ is a RAM program composed of the $n$ instructions $I_1, \ldots, I_n$, the code of $P$, denoted as $\#P$, is

$$\#P = \langle n, \#I_1, \ldots, \#I_n \rangle.$$  

Recall from a previous exercise that

$$\langle n, \#I_1, \ldots, \#I_n \rangle = \langle n, \langle \#I_1, \ldots, \#I_n \rangle \rangle.$$
Also recall that
\[ \langle x, y \rangle = \left( (x + y)^2 + 3x + y \right) / 2. \]
Consider the following program \( P_{\text{add2}} \) computing the function \( \text{add2} : \mathbb{N} \rightarrow \mathbb{N} \) given by
\[ \text{add2}(n) = n + 2. \]

\[
\begin{align*}
I_1: & \quad 1 \quad \text{add} \quad R1 \\
I_2: & \quad 2 \quad \text{add} \quad R1 \\
I_3: & \quad 3 \quad \text{continue}
\end{align*}
\]
We have
\[
\begin{align*}
\#I_1 &= \langle 1, 1, 1, 0 \rangle_4 = \langle 1, \langle 1, 0 \rangle \rangle = 37 \\
\#I_2 &= \langle 1, 2, 1, 0 \rangle_4 = \langle 1, \langle 2, 0 \rangle \rangle = 92 \\
\#I_3 &= \langle 3, 3, 1, 0 \rangle_4 = \langle 3, \langle 3, 0 \rangle \rangle = 234
\end{align*}
\]
and
\[
\begin{align*}
\#P_{\text{add2}} &= \langle 3, \#I_1, \#I_2, \#I_3 \rangle_4 = \langle 3, \langle 37, 92, 234 \rangle \rangle \\
&= 1\,018\,748\,519\,973\,070\,618.
\end{align*}
\]
The codes get big fast!

We define the primitive recursive functions \( L_n, \ P_g, \) and \( \text{Line}, \) such that:
\[
\begin{align*}
L_n(x) &= \Pi(1, 2, x), \\
P_g(x) &= \Pi(2, 2, x), \\
\text{Line}(i, x) &= \Pi(i, L_n(x), P_g(x)).
\end{align*}
\]
The function \( L_n \) yields the length of the program (the number of instructions), \( P_g \) yields the sequence of instructions in the program (really, a code for the sequence), and \( \text{Line}(i, x) \) yields the code of the \( i \)th instruction in the program. Again, if \( x \) does not code a program, there is no need to interpret these functions. However, note that by a previous exercise, it happens that
\[
\begin{align*}
\text{Line}(0, x) &= \text{Line}(1, x), \quad \text{and} \\
\text{Line}(L_n(x), x) &= \text{Line}(i, x), \quad \text{for all } i \geq x.
\end{align*}
\]
The primitive recursive predicate \( \text{PROG} \) is defined such that \( \text{PROG}(x) \) holds iff \( x \) codes a program. Thus, \( \text{PROG}(x) \) holds if each line codes an instruction, each jump has an
instruction to jump to, and the last instruction is a continue. Thus, PROG(x) holds iff

\[ \forall i \leq \text{Ln}(x)[i \geq 1 \supset \right. \]
\[ \text{INST(Line}(i, x)) \land \text{Typ(Line(Ln(x), x))} = 3 \]
\[ \land [\text{Typ(Line}(i, x)) = 4 \supset \right. \]
\[ \exists j \leq i - 1[j \geq 1 \land \text{Nam(Line}(j, x)) = \text{Jmp(Line}(i, x)))] \land \]
\[ [\text{Typ(Line}(i, x)) = 5 \supset \right. \]
\[ \exists j \leq \text{Ln}(x)[j > i \land \text{Nam(Line}(j, x)) = \text{Jmp(Line}(i, x))]]] \]

Note that we have used the fact proved as an exercise that if \( f \) is a primitive recursive function and \( P \) is a primitive recursive predicate, then \( \exists x \leq f(y)P(x) \) is primitive recursive.

We are now ready to prove a fundamental result in the theory of algorithms. This result points out some of the limitations of the notion of algorithm.

**Theorem 4.3. (Undecidability of the halting problem)** There is no RAM program Decider which halts for all inputs and has the following property when started with input \( x \) in register \( R_1 \) and with input \( i \) in register \( R_2 \) (the other registers being set to zero):

1. **Decider** halts with output 1 iff \( i \) codes a program that eventually halts when started on input \( x \) (all other registers set to zero).

2. **Decider** halts with output 0 in \( R_1 \) iff \( i \) codes a program that runs forever when started on input \( x \) in \( R_1 \) (all other registers set to zero).

3. If \( i \) does not code a program, then **Decider** halts with output 2 in \( R_1 \).

**Proof.** Assume that **Decider** is such a RAM program, and let \( Q \) be the following program with a single input:

\[
\text{Program } Q \text{ (code } q) \left\{ \begin{array}{c}
R_2 \leftarrow R_1 \\
P \\
N_1 \text{ continue} \\
R_1 \text{ jmp } N_1a \\
R_1 \text{ continue} \\
\end{array} \right.
\]

Let \( i \) be the code of some program \( P \). The key point is that the termination behavior of \( Q \) on input \( i \) is exactly the opposite of the termination behavior of **Decider** on input \( i \) and code \( i \).

1. If **Decider** says that program \( P \) coded by \( i \) halts on input \( i \), then \( R_1 \) just after the continue in line \( N_1 \) contains 1, and \( Q \) loops forever.

2. If **Decider** says that program \( P \) coded by \( i \) loops forever on input \( i \), then \( R_1 \) just after continue in line \( N_1 \) contains 0, and \( Q \) halts.
The program $Q$ can be translated into a program using only instructions of type 1, 2, 3, 4, 5, described previously, and let $q$ be the code of the program $Q$.

Let us see what happens if we run the program $Q$ on input $q$ in $R1$ (all other registers set to zero).

Just after execution of the assignment $R2 \leftarrow R1$, the program $\text{Decider}$ is started with $q$ in both $R1$ and $R2$. Since $\text{Decider}$ is supposed to halt for all inputs, it eventually halts with output 0 or 1 in $R1$. If $\text{Decider}$ halts with output 1 in $R1$, then $Q$ goes into an infinite loop, while if $\text{Decider}$ halts with output 0 in $R1$, then $Q$ halts. But then, because of the definition of $\text{Decider}$, we see that $\text{Decider}$ says that $Q$ halts when started on input $q$ iff $Q$ loops forever on input $q$, and that $Q$ loops forever on input $q$ iff $Q$ halts on input $q$, a contradiction. Therefore, $\text{Decider}$ cannot exist. 

If we identify the notion of algorithm with that of a RAM program which halts for all inputs, the above theorem says that there is no algorithm for deciding whether a RAM program eventually halts for a given input. We say that the halting problem for RAM programs is undecidable (or unsolvable).

The above theorem also implies that the halting problem for Turing machines is undecidable. Indeed, if we had an algorithm for solving the halting problem for Turing machines, we could solve the halting problem for RAM programs as follows: first, apply the algorithm for translating a RAM program into an equivalent Turing machine, and then apply the algorithm solving the halting problem for Turing machines. The argument is typical in computability theory and is called a “reducibility argument.”

Our next goal is to define a primitive recursive function that describes the computation of RAM programs. Assume that we have a RAM program $P$ using $n$ registers $R1, \ldots, Rn$, whose contents are denoted as $r_1, \ldots, r_n$. We can code $r_1, \ldots, r_n$ into a single integer $\langle r_1, \ldots, r_n \rangle$. Conversely, every integer $x$ can be viewed as coding the contents of $R1, \ldots, Rn$, by taking the sequence $\Pi(1, n, x), \ldots, \Pi(n, n, x)$.

Actually, it is not necessary to know $n$, the number of registers, if we make the following observation:

$$\text{Reg} (\text{Line}(i, x)) \leq \text{Line}(i, x) \leq \text{Pg}(x)$$

for all $i, x \in \mathbb{N}$. Then, if $x$ codes a program, then $R1, \ldots, Rx$ certainly include all the registers in the program. Also note that from a previous exercise,

$$\langle r_1, \ldots, r_n, 0, \ldots, 0 \rangle = \langle r_1, \ldots, r_n, 0 \rangle.$$

We now define the primitive recursive functions Nextline, Nextcont, and Comp, describing the computation of RAM programs.

**Definition 4.3.** Let $x$ code a program and let $i$ be such that $1 \leq i \leq \text{Ln}(x)$. The following functions are defined:
(1) Nextline($i, x, y$) is the number of the next instruction to be executed after executing the $i$th instruction in the program coded by $x$, where the contents of the registers is coded by $y$.

(2) Nextcont($i, x, y$) is the code of the contents of the registers after executing the $i$th instruction in the program coded by $x$, where the contents of the registers is coded by $y$.

(3) $\text{Comp}(x, y, m) = \langle i, z \rangle$, where $i$ and $z$ are defined such that after running the program coded by $x$ for $m$ steps, where the initial contents of the program registers are coded by $y$, the next instruction to be executed is the $i$th one, and $z$ is the code of the current contents of the registers.

**Proposition 4.4.** The functions Nextline, Nextcont, and Comp, are primitive recursive.

**Proof.** (1) Nextline($i, x, y$) = $i + 1$, unless the $i$th instruction is a jump and the contents of the register being tested is nonzero:

$$\text{Nextline}(i, x, y) = \begin{cases} 
\max j \leq \text{Ln}(x)[j < i \land \text{Nam(Line}(j, x)) = \text{Jmp(Line}(i, x))] \\
\text{if Typ(Line}(i, x)) = 4 \land \Pi(\text{Reg(Line}(i, x)), x, y) \neq 0 \\
\min j \leq \text{Ln}(x)[j > i \land \text{Nam(Line}(j, x)) = \text{Jmp(Line}(i, x))] \\
\text{if Typ(Line}(i, x)) = 5 \land \Pi(\text{Reg(Line}(i, x)), x, y) \neq 0 \\
i + 1 \text{ otherwise.}
\end{cases}$$

Note that according to this definition, if the $i$th line is the final continue, then Nextline signals that the program has halted by yielding

$$\text{Nextline}(i, x, y) > \text{Ln}(x).$$

(2) We need two auxiliary functions Add and Sub defined as follows.

Add($j, x, y$) is the number coding the contents of the registers used by the program coded by $x$ after register $Rj$ coded by $\Pi(j, x, y)$ has been increased by 1, and

Sub($j, x, y$) codes the contents of the registers after register $Rj$ has been decremented by 1 ($y$ codes the previous contents of the registers). It is easy to see that

$$\text{Sub}(j, x, y) = \min z \leq y[\Pi(j, x, z) = \Pi(j, x, y) - 1 \land \forall k \leq x[0 < k \neq j \supset \Pi(k, x, z) = \Pi(k, x, y)].$$

The definition of Add is slightly more tricky. We leave as an exercise to the reader to prove that:

$$\text{Add}(j, x, y) = \min z \leq \text{Large}(x, y + 1) [\Pi(j, x, z) = \Pi(j, x, y) + 1 \land \forall k \leq x[0 < k \neq j \supset \Pi(k, x, z) = \Pi(k, x, y)].$$
where the function $\text{Large}$ is the function defined in an earlier exercise. Then

$$\text{Nextcont}(i, x, y) =$$

$$\begin{align*}
\text{Add}(\text{Reg}(\text{Line}(i, x), x, y) & \quad \text{if } \text{Typ}(\text{Line}(i, x)) = 1 \\
\text{Sub}(\text{Reg}(\text{Line}(i, x), x, y) & \quad \text{if } \text{Typ}(\text{Line}(i, x)) = 2 \\
y & \quad \text{if } \text{Typ}(\text{Line}(i, x)) \geq 3.
\end{align*}$$

(3) Recall that $\Pi_1(z) = \Pi(1, 2, z)$ and $\Pi_2(z) = \Pi(2, 2, z)$. The function $\text{Comp}$ is defined by primitive recursion as follows:

$$\begin{align*}
\text{Comp}(x, y, 0) &= \langle 1, y \rangle \\
\text{Comp}(x, y, m + 1) &= \langle \text{Nextline}(\Pi_1(\text{Comp}(x, y, m)), x, \Pi_2(\text{Comp}(x, y, m))), \\
& \quad \text{Nextcont}(\Pi_1(\text{Comp}(x, y, m)), x, \Pi_2(\text{Comp}(x, y, m)))) \rangle.
\end{align*}$$

Recall that $\Pi_1(\text{Comp}(x, y, m))$ is the number of the next instruction to be executed and that $\Pi_2(\text{Comp}(x, y, m))$ codes the current contents of the registers.

We can now reprove that every RAM computable function is partial computable. Indeed, assume that $x$ codes a program $P$.

We define the partial function $\text{End}$ so that for all $x, y$, where $x$ codes a program and $y$ codes the contents of its registers, $\text{End}(x, y)$ is the number of steps for which the computation runs before halting, if it halts. If the program does not halt, then $\text{End}(x, y)$ is undefined. Since

$$\text{End}(x, y) = \min m [\Pi_1(\text{Comp}(x, y, m)) = \text{Ln}(x)],$$

if $y$ is the value of the register $R_1$ before the program $P$ coded by $x$ is started, recall that the contents of the registers is coded by $\langle y, 0 \rangle$. Noticing that 0 and 1 do not code programs, we note that if $x$ codes a program, then $x \geq 2$, and $\Pi_1(z) = \Pi(1, x, z)$ is the contents of $R_1$ as coded by $z$.

Since $\text{Comp}(x, y, m) = \langle i, z \rangle$, we have

$$\Pi_1(\text{Comp}(x, y, m)) = i,$$

where $i$ is the number (index) of the instruction reached after running the program $P$ coded by $x$ with initial values of the registers coded by $y$ for $m$ steps. Thus, $P$ halts if $i$ is the last instruction in $P$, namely $\text{Ln}(x)$, iff

$$\Pi_1(\text{Comp}(x, y, m)) = \text{Ln}(x).$$

End is a partial computable function; it can be computed by a RAM program involving only one while loop searching for the number of steps $m$. However, in general, End is not a total function.
If $\varphi$ is the partial computable function computed by the program $P$ coded by $x$, then we have

$$\varphi(y) = \Pi_1(\Pi_2(\text{Comp}(x, \langle y, 0 \rangle, \text{End}(x, \langle y, 0 \rangle))).$$

This is because if $m = \text{End}(x, \langle y, 0 \rangle)$ is the number of steps after which the program $P$ coded by $x$ halts on input $y$, then

$$\text{Comp}(x, \langle y, 0 \rangle, m) = \langle \text{Ln}(x), z \rangle,$$

where $z$ is the code of the register contents when the program stops. Consequently

$$z = \Pi_2(\text{Comp}(x, \langle y, 0 \rangle, m))$$

and

$$z = \Pi_2(\text{Comp}(x, \langle y, 0 \rangle, \text{End}(x, \langle y, 0 \rangle))).$$

The value of the register $R1$ is $\Pi_1(z)$, that is

$$\varphi(y) = \Pi_1(\Pi_2(\text{Comp}(x, \langle y, 0 \rangle, \text{End}(x, \langle y, 0 \rangle))).$$

Observe that $\varphi$ is written in the form $\varphi = g \circ \min f$, for some primitive recursive functions $f$ and $g$.

We can also exhibit a partial computable function which enumerates all the unary partial computable functions. It is a universal function.

Abusing the notation slightly, we will write $\varphi(x, y)$ for $\varphi(\langle x, y \rangle)$, viewing $\varphi$ as a function of two arguments (however, $\varphi$ is really a function of a single argument). We define the function $\varphi_{\text{univ}}$ as follows:

$$\varphi_{\text{univ}}(x, y) = \begin{cases} 
\Pi_1(\Pi_2(\text{Comp}(x, \langle y, 0 \rangle, \text{End}(x, \langle y, 0 \rangle)))) & \text{if PROG}(x), \\
\text{undefined} & \text{otherwise}.
\end{cases}$$

The function $\varphi_{\text{univ}}$ is a partial computable function with the following property: for every $x$ coding a RAM program $P$, for every input $y$,

$$\varphi_{\text{univ}}(x, y) = \varphi_x(y),$$

the value of the partial computable function $\varphi_x$ computed by the RAM program $P$ coded by $x$. If $x$ does not code a program, then $\varphi_{\text{univ}}(x, y)$ is undefined for all $y$.

By Proposition 3.9, the partial function $\varphi_{\text{univ}}$ is not computable (recursive).\footnote{The term \textit{recursive function} is now considered old-fashion. Many researchers have switched to the term \textit{computable function}.} Indeed, being an enumerating function for the partial computable functions, it is an enumerating function for the total computable functions, and thus, it cannot be computable. Being a partial function saves us from a contradiction.

The existence of the function $\varphi_{\text{univ}}$ leads us to the notion of an indexing of the RAM programs.
We can define a listing of the RAM programs as follows. If \( x \) codes a program (that is, if \( \text{PROG}(x) \) holds) and \( P \) is the program that \( x \) codes, we call this program \( P \) the \( x \)th RAM program and denote it as \( P_x \). If \( x \) does not code a program, we let \( P_x \) be the program that diverges for every input:

\[
\begin{align*}
N1 & \quad \text{add} \quad R1 \\
N1 & \quad R1 \quad \text{jmp} \quad N1a \\
N1 & \quad \text{continue}
\end{align*}
\]

Therefore, in all cases, \( P_x \) stands for the \( x \)th RAM program. Thus, we have a listing of RAM programs, \( P_0, P_1, P_2, P_3, \ldots \), such that every RAM program (of the restricted type considered here) appears in the list exactly once, except for the “infinite loop” program. For example, the program \( \text{Padd2} \) (adding 2 to an integer) appears as

\[ P_{1018748519973070618}. \]

In particular, note that \( \varphi_{\text{univ}} \) being a partial computable function, it is computed by some RAM program \( \text{UNIV} \) that has a code \( \text{univ} \) and is the program \( P_{\text{univ}} \) in the list.

Having an indexing of the RAM programs, we also have an indexing of the partial computable functions.

**Definition 4.4.** For every integer \( x \geq 0 \), we let \( P_x \) be the RAM program coded by \( x \) as defined earlier, and \( \varphi_x \) be the partial computable function computed by \( P_x \).

For example, the function \( \text{add2} \) (adding 2 to an integer) appears as

\[ \varphi_{1018748519973070618}. \]

**Remark:** Kleene used the notation \( \{x\} \) for the partial computable function coded by \( x \). Due to the potential confusion with singleton sets, we follow Rogers, and use the notation \( \varphi_x \).

It is important to observe that different programs \( P_x \) and \( P_y \) may compute the same function, that is, while \( P_x \neq P_y \) for all \( x \neq y \), it is possible that \( \varphi_x = \varphi_y \). In fact, it is undecidable whether \( \varphi_x = \varphi_y \).

The existence of the universal function \( \varphi_{\text{univ}} \) is sufficiently important to be recorded in the following proposition.

**Proposition 4.5.** For the indexing of RAM programs defined earlier, there is a universal partial computable function \( \varphi_{\text{univ}} \) such that, for all \( x, y \in \mathbb{N} \), if \( \varphi_x \) is the partial computable function computed by \( P_x \), then

\[ \varphi_x(y) = \varphi_{\text{univ}}((x, y)). \]
The program UNIV computing $\varphi_{\text{univ}}$ can be viewed as an *interpreter* for RAM programs. By giving the universal program UNIV the “program” $x$ and the “data” $y$, we get the result of executing program $P_x$ on input $y$. We can view the RAM model as a *stored program computer*.

By Theorem 4.3 and Proposition 4.5, the halting problem for the single program UNIV is undecidable. Otherwise, the halting problem for RAM programs would be decidable, a contradiction. It should be noted that the program UNIV can actually be written (with a certain amount of pain).

The object of the next Section is to show the existence of Kleene’s $T$-predicate. This will yield another important normal form. In addition, the $T$-predicate is a basic tool in recursion theory.

### 4.4 Kleene’s $T$-Predicate

In Section 4.3, we have encoded programs. The idea of this Section is to also encode *computations* of RAM programs. Assume that $x$ codes a program, that $y$ is some input (not a code), and that $z$ codes a computation of $P_x$ on input $y$. The predicate $T(x, y, z)$ is defined as follows:

$T(x, y, z)$ holds iff $x$ codes a RAM program, $y$ is an input, and $z$ codes a halting computation of $P_x$ on input $y$.

We will show that $T$ is primitive recursive. First, we need to encode computations. We say that $z$ codes a computation of length $n \geq 1$ if

$$z = \langle n + 2, \langle 1, y_0 \rangle, \langle i_1, y_1 \rangle, \ldots, \langle i_n, y_n \rangle \rangle,$$

where each $i_j$ is the physical location of the next instruction to be executed and each $y_j$ codes the contents of the registers just before execution of the instruction at the location $i_j$. Also, $y_0$ codes the initial contents of the registers, that is, $y_0 = \langle y, 0 \rangle$, for some input $y$. We let $\text{Ln}(z) = \Pi_1(z)$. Note that $i_j$ denotes the physical location of the next instruction to be executed in the sequence of instructions constituting the program coded by $x$, and not the line number (label) of this instruction. Thus, the first instruction to be executed is in location 1, $1 \leq i_j \leq \text{Ln}(x)$, and $i_{n-1} = \text{Ln}(x)$. Since the last instruction which is executed is the last physical instruction in the program, namely, a *continue*, there is no next instruction to be executed after that, and $i_n$ is irrelevant. Writing the definition of $T$ is a little simpler if we let $i_n = \text{Ln}(x) + 1$. 
**Definition 4.5.** The $T$-predicate is the primitive recursive predicate defined as follows:

$T(x, y, z) \iff \text{PROG}(x)$ and $(\text{Ln}(z) \geq 3)$ and
\[
\forall j \leq \text{Ln}(z) - 3 [0 \leq j \supset 
\text{Nextline}(\Pi_1(\Pi(j + 2, \text{Ln}(z), z)) = \Pi_1(\Pi(j + 3, \text{Ln}(z), z)) 
\text{and} 
\text{Nextcont}(\Pi_1(\Pi(j + 2, \text{Ln}(z), z)), x, \Pi_2(\Pi(j + 2, \text{Ln}(z), z))) = \Pi_2(\Pi(j + 3, \text{Ln}(z), z)) 
\text{and} 
\Pi_1(\Pi(\text{Ln}(z) - 1, \text{Ln}(z), z)) = \text{Ln}(x) 
\text{and} 
\Pi_1(\Pi(2, \text{Ln}(z), z)) = 1 
\text{and} 
y = \Pi_1(\Pi_2(\Pi(2, \text{Ln}(z), z))) \text{ and } \Pi_2(\Pi_2(\Pi(2, \text{Ln}(z), z))) = 0]
\]

The reader can verify that $T(x, y, z)$ holds iff $x$ codes a RAM program, $y$ is an input, and $z$ codes a halting computation of $P_x$ on input $y$. In order to extract the output of $P_x$ from $z$, we define the primitive recursive function $\text{Res}$ as follows:

$$\text{Res}(z) = \Pi_1(\Pi_2(\Pi(\text{Ln}(z), \text{Ln}(z), z))).$$

The explanation for this formula is that $\text{Res}(z)$ are the contents of register $R1$ when $P_x$ halts, that is, $\Pi_1(y_{\text{Ln}(z)})$. Using the $T$-predicate, we get the so-called Kleene normal form.

**Theorem 4.6.** (Kleene Normal Form) Using the indexing of the partial computable functions defined earlier, we have

$$\varphi_x(y) = \text{Res}[\min z(T(x, y, z))],$$

where $T(x, y, z)$ and $\text{Res}$ are primitive recursive.

Note that the universal function $\varphi_{\text{univ}}$ can be defined as

$$\varphi_{\text{univ}}(x, y) = \text{Res}[\min z(T(x, y, z))].$$

There is another important property of the partial computable functions, namely, that composition is effective. We need two auxiliary primitive recursive functions. The function $\text{Conprogs}$ creates the code of the program obtained by concatenating the programs $P_x$ and $P_y$, and for $i \geq 2$, $\text{Cumclr}(i)$ is the code of the program which clears registers $R2, \ldots, Ri$. To get $\text{Cumclr}$, we can use the function $\text{clr}(i)$ such that $\text{clr}(i)$ is the code of the program

\[
\begin{align*}
N1 & \quad \text{tail} & Ri \\
N1 & \quad Ri & \quad \text{jmp} & \quad N1a \\
N & \quad \text{continue}
\end{align*}
\]

We leave it as an exercise to prove that $\text{clr}$, $\text{Conprogs}$, and $\text{Cumclr}$, are primitive recursive.

**Theorem 4.7.** There is a primitive recursive function $c$ such that

$$\varphi_{c(x,y)} = \varphi_x \circ \varphi_y.$$
4.5. A SIMPLE FUNCTION NOT KNOWN TO BE COMPUTABLE

Proof. If both $x$ and $y$ code programs, then $\varphi_x \circ \varphi_y$ can be computed as follows: Run $P_y$, clear all registers but $R1$, then run $P_x$. Otherwise, let loop be the index of the infinite loop program:

$$c(x, y) = \begin{cases} 
\text{Conprogs}(y, \text{Conprogs}((\text{Cumclr}(y), x)) & \text{if PROG}(x) \text{ and PROG}(y) \\
\text{loop} & \text{otherwise}.
\end{cases}$$

\[\square\]

4.5 A Simple Function Not Known to be Computable

The “3n + 1 problem” proposed by Collatz around 1937 is the following:

Given any positive integer $n \geq 1$, construct the sequence $c_i(n)$ as follows starting with $i = 1$:

\[
c_1(n) = n \\
c_{i+1}(n) = \begin{cases} 
c_i(n)/2 & \text{if } c_i(n) \text{ is even} \\
3c_i(n) + 1 & \text{if } c_i(n) \text{ is odd}
\end{cases}
\]

Observe that for $n = 1$, we get the infinite periodic sequence

$$1 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1 \Rightarrow \cdots,$$

so we may assume that we stop the first time that the sequence $c_i(n)$ reaches the value 1 (if it actually does). Such an index $i$ is called the stopping time of the sequence. And this is the problem:

Conjecture (Collatz):

For any starting integer value $n \geq 1$, the sequence $(c_i(n))$ always reaches 1.

Starting with $n = 3$, we get the sequence

$$3 \Rightarrow 10 \Rightarrow 5 \Rightarrow 16 \Rightarrow 8 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1.$$

Starting with $n = 5$, we get the sequence

$$5 \Rightarrow 16 \Rightarrow 8 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1.$$

Starting with $n = 6$, we get the sequence

$$6 \Rightarrow 3 \Rightarrow 10 \Rightarrow 5 \Rightarrow 16 \Rightarrow 8 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1.$$

Starting with $n = 7$, we get the sequence

$$7 \Rightarrow 22 \Rightarrow 11 \Rightarrow 34 \Rightarrow 17 \Rightarrow 52 \Rightarrow 26 \Rightarrow 13 \Rightarrow 40 \Rightarrow 20 \Rightarrow 10 \Rightarrow 25 \Rightarrow 16 \Rightarrow 8 \Rightarrow 4 \Rightarrow 2 \Rightarrow 1.$$
One might be surprised to find that for $n = 27$, it takes 111 steps to reach 1, and for $n = 97$, it takes 118 steps. I computed the stopping times for $n$ up to $10^7$ and found that the largest stopping time, 686 (685 steps) is obtained for $n = 8400511$. The terms of this sequence reach values over $1.5 \times 10^{11}$. The graph of the sequence $c(8400511)$ is shown in Figure 4.1.

![Graph of the sequence for n = 8400511.](image)

Figure 4.1: Graph of the sequence for $n = 8400511$.

We can define the partial computable function $C$ (with positive integer inputs) defined by

$$C(n) = \text{the smallest } i \text{ such that } c_i(n) = 1 \text{ if it exists.}$$

Then the Collatz conjecture is equivalent to asserting that the function $C$ is (total) computable. The graph of the function $C$ for $1 \leq n \leq 10^7$ is shown in Figure 4.2.

So far, the conjecture remains open. It has been checked by computer for all integers less than or equal to $87 \times 2^{60}$. 
4.6 A Non-Computable Function; Busy Beavers

Total functions that are not computable must grow very fast and thus are very complicated. Yet, in 1962, Radó published a paper in which he defined two functions $\Sigma$ and $S$ (involving computations of Turing machines) that are total and not computable.

Consider Turing machines with a tape alphabet $\Gamma = \{1, B\}$ with two symbols ($B$ being the blank). We also assume that these Turing machines have a special final state $q_F$, which is a blocking state (there are no transitions from $q_F$). We do not count this state when counting the number of states of such Turing machines. The game is to run such Turing machines with a fixed number of states $n$ starting on a blank tape, with the goal of producing the maximum number of (not necessarily consecutive) ones (1).

**Definition 4.6.** The function $\Sigma$ (defined on the positive natural numbers) is defined as the maximum number $\Sigma(n)$ of (not necessarily consecutive) 1’s written on the tape after a Turing machine with $n \geq 1$ states started on the blank tape halts. The function $S$ is defined as the maximum number $S(n)$ of moves that can be made by a Turing machine of the above
type with \( n \) states before it halts, started on the blank tape.

A Turing machine with \( n \) states that writes the maximum number \( \Sigma(n) \) of 1’s when started on the blank tape is called a \textit{busy beaver}.

Busy beavers are hard to find, even for small \( n \). First, it can be shown that the number of distinct Turing machines of the above kind with \( n \) states is \((4(n+1))^{2^n}\). Second, since it is undecidable whether a Turing machine halts on a given input, it is hard to tell which machines loop or halt after a very long time.

Here is a summary of what is known for \( 1 \leq n \leq 6 \). Observe that the exact value of \( \Sigma(5), \Sigma(6), S(5) \) and \( S(6) \) is unknown.

<table>
<thead>
<tr>
<th>( n )</th>
<th>( \Sigma(n) )</th>
<th>( S(n) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>4</td>
<td>6</td>
</tr>
<tr>
<td>3</td>
<td>6</td>
<td>21</td>
</tr>
<tr>
<td>4</td>
<td>13</td>
<td>107</td>
</tr>
<tr>
<td>5</td>
<td>( \geq 4098 )</td>
<td>( \geq 47,176,870 )</td>
</tr>
<tr>
<td>6</td>
<td>( \geq 95,524,079 )</td>
<td>( \geq 8,690,333,381,690,951 )</td>
</tr>
<tr>
<td>6</td>
<td>( \geq 3.515 \times 10^{18267} )</td>
<td>( \geq 7.412 \times 10^{36534} )</td>
</tr>
</tbody>
</table>

The first entry in the table for \( n = 6 \) corresponds to a machine due to Heiner Marxen (1999). This record was surpassed by Pavel Kropitz in 2010, which corresponds to the second entry for \( n = 6 \). The machines achieving the record in 2017 for \( n = 4, 5, 6 \) are shown below, where the blank is denoted \( \Delta \) instead of \( B \), and where the special halting states is denoted \( H \):

4-state busy beaver:

\[
\begin{array}{c|c|c|c|c}
\Delta & (1, R, B) & (1, L, A) & (1, R, H) & (1, R, D) \\
1 & (1, L, B) & (\Delta, L, C) & (1, L, D) & (\Delta, R, A) \\
\end{array}
\]

The above machine output 13 ones in 107 steps. In fact, the output is

\[\Delta \Delta 1 \Delta 1 1 1 1 1 1 1 1 \Delta \Delta.\]

5-state best contender:

\[
\begin{array}{c|c|c|c|c}
\Delta & (1, R, B) & (1, R, C) & (1, R, D) & (1, L, A) \\
1 & (1, L, C) & (1, R, B) & (\Delta, L, E) & (1, L, D) \\
\end{array}
\]

The above machine output 4098 ones in 47,176,870 steps.
6-state contender (Heiner Marxen):

<table>
<thead>
<tr>
<th>Action</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\Delta)</td>
<td>((1, R, B))</td>
<td>((1, L, C))</td>
<td>((\Delta, R, F))</td>
<td>((1, R, A))</td>
<td>((1, L, H))</td>
<td>((\Delta, L, A))</td>
</tr>
<tr>
<td>1</td>
<td>((1, R, A))</td>
<td>((1, L, B))</td>
<td>((1, L, D))</td>
<td>((\Delta, L, E))</td>
<td>((1, L, F))</td>
<td>((\Delta, L, C))</td>
</tr>
</tbody>
</table>

The above machine outputs 96,524,079 ones in 8,690,333,381,690,951 steps.

6-state best contender (Pavel Kropitz):

<table>
<thead>
<tr>
<th>Action</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>(\Delta)</td>
<td>((1, R, B))</td>
<td>((1, R, C))</td>
<td>((1, L, D))</td>
<td>((1, R, E))</td>
<td>((1, L, A))</td>
<td>((1, L, H))</td>
</tr>
<tr>
<td>1</td>
<td>((1, L, E))</td>
<td>((1, R, F))</td>
<td>((\Delta, R, B))</td>
<td>((\Delta, L, C))</td>
<td>((\Delta, R, D))</td>
<td>((1, R, C))</td>
</tr>
</tbody>
</table>

The above machine output at least \(3.515 \times 10^{18267}\) ones!

The reason why it is so hard to compute \(\Sigma\) and \(S\) is that they are not computable!

**Theorem 4.8.** The functions \(\Sigma\) and \(S\) are total functions that are not computable (not recursive).

**Proof sketch.** The proof consists in showing that \(\Sigma\) (and similarly for \(S\)) eventually outgrows any computable function. More specifically, we claim that for every computable function \(f\), there is some positive integer \(k_f\) such that

\[
\Sigma(n + k_f) \geq f(n) \quad \text{for all } n \geq 0.
\]

We simply have to pick \(k_f\) to be the number of states of a Turing machine \(M_f\) computing \(f\). Then, we can create a Turing machine \(M_{n,f}\) that works as follows. Using \(n\) of its states, it writes \(n\) ones on the tape, and then it simulates \(M_f\) with input \(1^n\). Since the output of \(M_{n,f}\) started on the blank tape consists of \(f(n)\) ones, and since \(\Sigma(n + k_f)\) is the maximum number of ones that a Turing machine with \(n + k_f\) states will output when it stops, we must have

\[
\Sigma(n + k_f) \geq f(n) \quad \text{for all } n \geq 0.
\]

Next observe that \(\Sigma(n) < \Sigma(n + 1)\), because we can create a Turing machine with \(n + 1\) states which simulates a busy beaver machine with \(n\) states, and then writes an extra 1 when the busy beaver stops, by making a transition to the \((n + 1)\)th state. It follows immediately that if \(m < n\) then \(\Sigma(m) < \Sigma(n)\). If \(\Sigma\) was computable, then so would be the function \(g\) given by \(g(n) = \Sigma(2n)\). By the above, we would have

\[
\Sigma(n + k_f) \geq g(n) = \Sigma(2n) \quad \text{for all } n \geq 0,
\]

and for \(n > k_g\), since \(2n > n + k_k\), we would have \(\Sigma(n + n_g) < \Sigma(2n)\), contradicting the fact that \(\Sigma(n + n_g) \geq \Sigma(2n)\).

Since by definition \(S(n)\) is the maximum number of moves that can be made by a Turing machine of the above type with \(n\) states before it halts, \(S(n) \geq \Sigma(n)\). Then the same reasoning as above shows that \(S\) is not a computable function.

The zoo of computable and non-computable functions is illustrated in Figure 4.3.
CHAPTER 4. UNIVERSAL RAM PROGRAMS AND THE HALTING PROBLEM

Figure 4.3: Computability Classification of Functions.
Chapter 5

Elementary Recursive Function Theory

5.1 Acceptable Indexings

In Chapter 4, we have exhibited a specific indexing of the partial computable functions by encoding the RAM programs. Using this indexing, we showed the existence of a universal function $\varphi_{\text{univ}}$ and of a computable function $c$, with the property that for all $x, y \in \mathbb{N}$,

$$\varphi_c(x, y) = \varphi_x \circ \varphi_y.$$  

It is natural to wonder whether the same results hold if a different coding scheme is used or if a different model of computation is used, for example, Turing machines. In other words, we would like to know if our results depend on a specific coding scheme or not.

Our previous results showing the characterization of the partial computable functions being independent of the specific model used, suggests that it might be possible to pinpoint certain properties of coding schemes which would allow an axiomatic development of recursive function theory. What we are aiming at is to find some simple properties of “nice” coding schemes that allow one to proceed without using explicit coding schemes, as long as the above properties hold.

Remarkably, such properties exist. Furthermore, any two coding schemes having these properties are equivalent in a strong sense (effectively equivalent), and so, one can pick any such coding scheme without any risk of losing anything else because the wrong coding scheme was chosen. Such coding schemes, also called indexings, or Gödel numberings, or even programming systems, are called acceptable indexings.

**Definition 5.1.** An *indexing* of the partial computable functions is an infinite sequence $\varphi_0, \varphi_1, \ldots$, of partial computable functions that includes all the partial computable functions of one argument (there might be repetitions, this is why we are not using the term enumeration). An indexing is *universal* if it contains the partial computable function $\varphi_{\text{univ}}$.
such that
\[ \varphi_{\text{univ}}(i, x) = \varphi_i(x) \]
for all \( i, x \in \mathbb{N} \). An indexing is \textit{acceptable} if it is universal and if there is a total computable function \( c \) for composition, such that
\[ \varphi_{c(i, j)} = \varphi_i \circ \varphi_j \]
for all \( i, j \in \mathbb{N} \).

From Chapter 4, we know that the specific indexing of the partial computable functions given for RAM programs is acceptable. Another characterization of acceptable indexings left as an exercise is the following: an indexing \( \psi_0, \psi_1, \psi_2, \ldots \) of the partial computable functions is acceptable iff there exists a total computable function \( f \) translating the RAM indexing of Section 4.3 into the indexing \( \psi_0, \psi_1, \psi_2, \ldots \), that is,
\[ \varphi_i = \psi_{f(i)} \]
for all \( i \in \mathbb{N} \).

A very useful property of acceptable indexings is the so-called “s-m-n Theorem”. Using the slightly loose notation \( \varphi(x_1, \ldots, x_n) \) for \( \varphi(\langle x_1, \ldots, x_n \rangle) \), the s-m-n theorem says the following. Given a function \( \varphi \) considered as having \( m + n \) arguments, if we fix the values of the first \( m \) arguments and we let the other \( n \) arguments vary, we obtain a function \( \psi \) of \( n \) arguments. Then, the index of \( \psi \) depends in a computable fashion upon the index of \( \varphi \) and the first \( m \) arguments \( x_1, \ldots, x_m \). We can “pull” the first \( m \) arguments of \( \varphi \) into the index of \( \psi \).

\textbf{Theorem 5.1. (The “s-m-n Theorem”)} For any acceptable indexing \( \varphi_0, \varphi_1, \ldots \), there is a total computable function \( s \), such that, for all \( i, m, n \geq 1 \), for all \( x_1, \ldots, x_m \) and all \( y_1, \ldots, y_n \), we have
\[ \varphi_{s(i, m, x_1, \ldots, x_m)}(y_1, \ldots, y_n) = \varphi_i(x_1, \ldots, x_m, y_1, \ldots, y_n). \]

\textit{Proof.} First, note that the above identity is really
\[ \varphi_{s(i, m, \langle x_1, \ldots, x_m \rangle)}(\langle y_1, \ldots, y_n \rangle) = \varphi_i(\langle x_1, \ldots, x_m, y_1, \ldots, y_n \rangle). \]
Recall that there is a primitive recursive function \( \text{Con} \) such that
\[ \text{Con}(m, \langle x_1, \ldots, x_m \rangle, \langle y_1, \ldots, y_n \rangle) = \langle x_1, \ldots, x_m, y_1, \ldots, y_n \rangle \]
for all \( x_1, \ldots, x_m, y_1, \ldots, y_n \in \mathbb{N} \). Hence, a computable function \( s \) such that
\[ \varphi_{s(i, m, x)}(y) = \varphi_i(\text{Con}(m, x, y)) \]
will do. We define some auxiliary primitive recursive functions as follows:
\[ P(y) = \langle 0, y \rangle \quad \text{and} \quad Q(\langle x, y \rangle) = \langle x + 1, y \rangle. \]
Since we have an indexing of the partial computable functions, there are indices $p$ and $q$ such that $P = \varphi_p$ and $Q = \varphi_q$. Let $R$ be defined such that
\[
R(0) = p,
R(x + 1) = c(q, R(x)),
\]
where $c$ is the computable function for composition given by the indexing. We leave as an exercise to prove that
\[
\varphi_{R(x)}(y) = \langle x, y \rangle
\]
for all $x, y \in \mathbb{N}$. Also, recall that $\langle x, y, z \rangle = \langle x, \langle y, z \rangle \rangle$, by definition of pairing. Then, we have
\[
\varphi_{R(x)} \circ \varphi_{R(y)}(z) = \varphi_{R(x)}(\langle y, z \rangle) = \langle x, y, z \rangle.
\]
Finally, let $k$ be an index for the function Con, that is, let
\[
\varphi_k(\langle m, x, y \rangle) = \text{Con}(m, x, y).
\]
Define $s$ by
\[
s(i, m, x) = c(i, c(k, c(R(m), R(x)))).
\]
Then, we have
\[
\varphi_{s(i, m, x)}(y) = \varphi_i \circ \varphi_k \circ \varphi_{R(m)} \circ \varphi_{R(x)}(y) = \varphi_i(\text{Con}(m, x, y)),
\]
as desired. Notice that if the composition function $c$ is primitive recursive, then $s$ is also primitive recursive. In particular, for the specific indexing of the RAM programs given in Section 4.3, the function $s$ is primitive recursive.

As a first application of the s-m-n Theorem, we show that any two acceptable indexings are effectively inter-translatable.

**Theorem 5.2.** Let $\varphi_0, \varphi_1, \ldots,$ be a universal indexing, and let $\psi_0, \psi_1, \ldots,$ be any indexing with a total computable s-1-1 function, that is, a function $s$ such that
\[
\psi_{s(i, m, x)}(y) = \psi_i(x, y)
\]
for all $i, x, y \in \mathbb{N}$. Then, there is a total computable function $t$ such that $\varphi_i = \psi_{t(i)}$.

**Proof.** Let $\varphi_{\text{univ}}$ be a universal partial computable function for the indexing $\varphi_0, \varphi_1, \ldots$. Since $\psi_0, \psi_1, \ldots,$ is also an indexing, $\varphi_{\text{univ}}$ occurs somewhere in the second list, and thus, there is some $k$ such that $\varphi_{\text{univ}} = \psi_k$. Then, we have
\[
\psi_{s(k, 1, i)}(x) = \psi_k(i, x) = \varphi_{\text{univ}}(i, x) = \varphi_i(x),
\]
for all $i, x \in \mathbb{N}$. Therefore, we can take the function $t$ to be the function defined such that
\[
t(i) = s(k, 1, i)
\]
for all $i \in \mathbb{N}$. \qed
Using Theorem 5.2, if we have two acceptable indexings \( \varphi_0, \varphi_1, \ldots \), and \( \psi_0, \psi_1, \ldots \), there exist total computable functions \( t \) and \( u \) such that
\[
\varphi_i = \psi_{t(i)} \quad \text{and} \quad \psi_i = \varphi_{u(i)}
\]
for all \( i \in \mathbb{N} \). Also note that if the composition function \( c \) is primitive recursive, then any \( s\text{-m\text{-}n} \) function is primitive recursive, and the translation functions are primitive recursive. Actually, a stronger result can be shown. It can be shown that for any two acceptable indexings, there exist total computable\footnote{We will see later that any total computable \( s\text{-m\text{-}n} \) function is primitive recursive.} injective and surjective translation functions. In other words, any two acceptable indexings are recursively isomorphic (Roger’s isomorphism theorem). Next, we turn to algorithmically unsolvable, or \textit{undecidable}, problems.

### 5.2 Undecidable Problems

We saw in Section 4.3 that the halting problem for RAM programs is undecidable. In this section, we take a slightly more general approach to study the undecidability of problems, and give some tools for resolving decidability questions.

First, we prove again the undecidability of the halting problem, but this time, for \textit{any} indexing of the partial computable functions.

**Theorem 5.3. (Halting Problem, Abstract Version)** Let \( \psi_0, \psi_1, \ldots \), be any indexing of the partial computable functions. Then, the function \( f \) defined such that
\[
f(x, y) = \begin{cases} 
1 & \text{if } \psi_x(y) \text{ is defined}, \\
0 & \text{if } \psi_x(y) \text{ is undefined},
\end{cases}
\]
is not computable.

**Proof.** Assume that \( f \) is computable, and let \( g \) be the function defined such that
\[
g(x) = f(x, x)
\]
for all \( x \in \mathbb{N} \). Then \( g \) is also computable. Let \( \theta \) be the function defined such that
\[
\theta(x) = \begin{cases} 
0 & \text{if } g(x) = 0, \\
\text{undefined} & \text{if } g(x) = 1.
\end{cases}
\]
We claim that \( \theta \) is not even partial computable. Observe that \( \theta \) is such that
\[
\theta(x) = \begin{cases} 
0 & \text{if } \psi_x(x) \text{ is undefined}, \\
\text{undefined} & \text{if } \psi_x(x) \text{ is defined}.
\end{cases}
\]
If \( \theta \) was partial computable, it would occur in the list as some \( \psi_i \), and we would have
\[
\theta(i) = \psi_i(i) = 0 \quad \text{iff} \quad \psi_i(i) \text{ is undefined},
\]
a contradiction. Therefore, \( f \) and \( g \) can’t be computable. \( \square \)
Observe that the proof of Theorem 5.3 does not use the fact that the indexing is universal or acceptable, and thus, the theorem holds for any indexing of the partial computable functions. The function \( g \) defined in the proof of Theorem 5.3 is the characteristic function of a set denoted as \( K \), where

\[
K = \{ x \mid \psi_x(x) \text{ is defined} \}.
\]

Given any set, \( X \), for any subset, \( A \subseteq X \), of \( X \), recall that the characteristic function, \( C_A \) (or \( \chi_A \)), of \( A \) is the function, \( C_A : X \to \{0, 1\} \), defined so that, for all \( x \in X \),

\[
C_A(x) = \begin{cases} 1 & \text{if } x \in A \\ 0 & \text{if } x \notin A. \end{cases}
\]

The set \( K \) is an example of a set which is not computable (or not recursive). Since this fact is quite important, we give the following definition:

**Definition 5.2.** A subset, \( A \), of \( \Sigma^* \) (or a subset, \( A \), of \( \mathbb{N} \)) is **computable**, or **recursive**,\(^1\) or **decidable** iff its characteristic function, \( C_A \), is a total computable function.

Using Definition 5.2, Theorem 5.3 can be restated as follows.

**Proposition 5.4.** For any indexing \( \varphi_0, \varphi_1, \ldots \) of the partial computable functions (over \( \Sigma^* \) or \( \mathbb{N} \)), the set \( K = \{ x \mid \varphi_x(x) \text{ is defined} \} \) is not computable (not recursive).

Computable (recursive) sets allow us to define the concept of a decidable (or undecidable) problem. The idea is to generalize the situation described in Section 4.3 and Section 4.4, where a set of objects, the RAM programs, is encoded into a set of natural numbers, using a coding scheme.

**Definition 5.3.** Let \( C \) be a countable set of objects, and let \( P \) be a property of objects in \( C \). We view \( P \) as the set

\[
\{ a \in C \mid P(a) \}.
\]

A **coding-scheme** is an injective function \( \# : C \to \mathbb{N} \) that assigns a unique code to each object in \( C \). The property \( P \) is **decidable (relative to \( \# \))** iff the set \( \{ \#(a) \mid a \in C \text{ and } P(a) \} \) is computable (recursive). The property \( P \) is **undecidable (relative to \( \# \))** iff the set \( \{ \#(a) \mid a \in C \text{ and } P(a) \} \) is not computable (not recursive).

Observe that the decidability of a property \( P \) of objects in \( C \) depends upon the coding scheme \( \# \). Thus, if we are cheating in using a non-effective coding scheme, we may declare that a property is decidable even though it is not decidable in some reasonable coding scheme. Consequently, we require a coding scheme \( \# \) to be **effective** in the following sense. Given any

---

\(^1\)Since 1996, the term *recursive* has been considered old-fashioned by many researchers, and the term *computable* has been used instead.
object \( a \in C \), we can effectively (i.e., algorithmically) determine its code \( \#(a) \). Conversely, given any integer \( n \in \mathbb{N} \), we should be able to tell effectively if \( n \) is the code of some object in \( C \), and if so, to find this object. In practice, it is always possible to describe the objects in \( C \) as strings over some (possibly complex) alphabet \( \Sigma \) (sets of trees, graphs, etc). In such cases, the coding schemes are computable functions from \( \Sigma^* \) to \( \mathbb{N} = \{a_1\}^* \).

For example, let \( C = \mathbb{N} \times \mathbb{N} \), where the property \( P \) is the equality of the partial functions \( \varphi_x \) and \( \varphi_y \). We can use the pairing function \( \langle -, - \rangle \) as a coding function, and the problem is formally encoded as the computability (recursiveness) of the set

\[
\{ \langle x, y \rangle \mid x, y \in \mathbb{N}, \varphi_x = \varphi_y \}.
\]

In most cases, we don’t even bother to describe the coding scheme explicitly, knowing that such a description is routine, although perhaps tedious.

We now show that most properties about programs (except the trivial ones) are undecidable. First, we show that it is undecidable whether a RAM program halts for every input. In other words, it is undecidable whether a procedure is an algorithm. We actually prove a more general fact.

**Proposition 5.5.** For any acceptable indexing \( \varphi_0, \varphi_1, \ldots \) of the partial computable functions, the set

\[
\text{TOTAL} = \{ x \mid \varphi_x \text{ is a total function} \}
\]

is not computable (not recursive).

**Proof.** The proof uses a technique known as reducibility. We try to reduce a set \( A \) known to be noncomputable (nonrecursive) to TOTAL via a computable function \( f : A \to \text{TOTAL} \), so that

\[
x \in A \iff f(x) \in \text{TOTAL}.
\]

If TOTAL were computable (recursive), its characteristic function \( g \) would be computable, and thus, the function \( g \circ f \) would be computable, a contradiction, since \( A \) is assumed to be noncomputable (nonrecursive). In the present case, we pick \( A = K \). To find the computable function \( f : K \to \text{TOTAL} \), we use the s-m-n Theorem. Let \( \vartheta \) be the function defined below: for all \( x, y \in \mathbb{N} \),

\[
\vartheta(x, y) = \begin{cases} 
\varphi_x(x) & \text{if } x \in K, \\
\text{undefined} & \text{if } x \not\in K.
\end{cases}
\]

Note that \( \vartheta \) does not depend on \( y \). The function \( \vartheta \) is partial computable. Indeed, we have

\[
\vartheta(x, y) = \varphi_x(x) = \varphi_{\text{univ}}(x, x).
\]

Thus, \( \vartheta \) has some index \( j \), so that \( \vartheta = \varphi_j \), and by the s-m-n Theorem, we have

\[
\varphi_{s(j, 1, x)}(y) = \varphi_j(x, y) = \vartheta(x, y).
\]
5.2. UNDECIDABLE PROBLEMS

Let \( f \) be the computable function defined such that

\[
f(x) = s(j, 1, x)
\]

for all \( x \in \mathbb{N} \). Then, we have

\[
\varphi_{f(x)}(y) = \begin{cases} 
\varphi_x(y) & \text{if } x \in K, \\
\text{undefined} & \text{if } x \notin K
\end{cases}
\]

for all \( y \in \mathbb{N} \). Thus, observe that \( \varphi_{f(x)} \) is a total function iff \( x \in K \), that is,

\[
x \in K \iff f(x) \in \text{TOTAL},
\]

where \( f \) is computable. As we explained earlier, this shows that \( \text{TOTAL} \) is not computable (not recursive).

The above argument can be generalized to yield a result known as Rice’s Theorem. Let \( \varphi_0, \varphi_1, \ldots \) be any indexing of the partial computable functions, and let \( C \) be any set of partial computable functions. We define the set \( P_C \) as

\[
P_C = \{ x \in \mathbb{N} | \varphi_x \in C \}.
\]

We can view \( C \) as a property of some of the partial computable functions. For example

\[
C = \{ \text{all total computable functions} \}.
\]

We say that \( C \) is nontrivial if \( C \) is neither empty nor the set of all partial computable functions. Equivalently \( C \) is nontrivial iff \( P_C \neq \emptyset \) and \( P_C \neq \mathbb{N} \). We may think of \( P_C \) as the set of programs computing the functions in \( C \).

**Theorem 5.6. (Rice’s Theorem)** For any acceptable indexing \( \varphi_0, \varphi_1, \ldots \) of the partial computable functions, for any set \( C \) of partial computable functions, the set

\[
P_C = \{ x \in \mathbb{N} | \varphi_x \in C \}
\]

is not computable (not recursive) unless \( C \) is trivial.

**Proof.** Assume that \( C \) is nontrivial. A set is computable (recursive) iff its complement is computable (recursive) (the proof is trivial). Hence, we may assume that the totally undefined function is not in \( C \), and since \( C \neq \emptyset \), let \( \psi \) be some other function in \( C \). We produce a computable function \( f \) such that

\[
\varphi_{f(x)}(y) = \begin{cases} 
\psi(y) & \text{if } x \in K, \\
\text{undefined} & \text{if } x \notin K
\end{cases}
\]

for all \( y \in \mathbb{N} \). We get \( f \) by using the s-m-n Theorem. Let \( \psi = \varphi_i \), and define \( \theta \) as follows:

\[
\theta(x, y) = \varphi_{\text{univ}}(i, y) + (\varphi_{\text{univ}}(x, x) - \varphi_{\text{univ}}(x, x)),
\]
where \(-\) is the primitive recursive function for truncated subtraction (monus). Clearly, \(\theta\) is partial computable, and let \(\theta = \varphi_j\). By the s-m-n Theorem, we have
\[
\varphi_{s(j,1,x)}(y) = \varphi_j(x, y) = \theta(x, y)
\]
for all \(x, y \in \mathbb{N}\). Letting \(f\) be the computable function such that
\[
f(x) = s(j, 1, x),
\]
by definition of \(\theta\), we get
\[
\varphi_{f(x)}(y) = \theta(x, y) = \begin{cases} 
\psi(y) & \text{if } x \in K, \\
\text{undefined} & \text{if } x \notin K.
\end{cases}
\]
Thus, \(f\) is the desired reduction function. Now, we have
\[
x \in K \iff f(x) \in P_C,
\]
and thus, the characteristic function \(C_K\) of \(K\) is equal to \(C_P \circ f\), where \(C_P\) is the characteristic function of \(P_C\). Therefore, \(P_C\) is not computable (not recursive), since otherwise, \(K\) would be computable, a contradiction.

Rice’s Theorem shows that all nontrivial properties of the input/output behavior of programs are undecidable!

The scenario to apply Rice’s Theorem to a class \(C\) of partial functions is to show that some partial computable function belongs to \(C\) (\(C\) is not empty), and that some partial computable function does not belong to \(C\) (\(C\) is not all the partial computable functions). This demonstrates that \(C\) is nontrivial.

In particular, the following properties are undecidable.

**Proposition 5.7.** The following properties of partial computable functions are undecidable.

(a) A partial computable function is a constant function.
(b) Given any integer \(y \in \mathbb{N}\), is \(y\) in the range of some partial computable function.
(c) Two partial computable functions \(\varphi_x\) and \(\varphi_y\) are identical. More precisely, the set \(\{\langle x, y \rangle \mid \varphi_x = \varphi_y\}\) is not computable.
(d) A partial computable function \(\varphi_x\) is equal to a given partial computable function \(\varphi_a\).
(e) A partial computable function yields output \(z\) on input \(y\), for any given \(y, z \in \mathbb{N}\).
(f) A partial computable function diverges for some input.
(g) A partial computable function diverges for all input.
5.3. LISTABLE (RECURSIVELY ENUMERABLE) SETS

The above proposition is left as an easy exercise. For example, in (a), we need to exhibit a constant (partial) computable function, such as \( \text{zero}(n) = 0 \), and a nonconstant (partial) computable function, such as the identity function (or \( \text{succ}(n) = n + 1 \)).

A property may be undecidable although it is partially decidable. By partially decidable, we mean that there exists a computable function \( g \) that enumerates the set \( P_C = \{ x \mid \varphi_x \in C \} \). This means that there is a computable function \( g \) whose range is \( P_C \). We say that \( P_C \) is listable, or computably enumerable, or recursively enumerable. Indeed, \( g \) provides a recursive enumeration of \( P_C \), with possible repetitions. Listable sets are the object of the next Section.

5.3 Listable (Recursively Enumerable) Sets

Consider the set

\[
A = \{ x \in \mathbb{N} \mid \varphi_x(a) \text{ is defined} \},
\]

where \( a \in \mathbb{N} \) is any fixed natural number. By Rice’s Theorem, \( A \) is not computable (not recursive); check this. We claim that \( A \) is the range of a computable function \( g \). For this, we use the \( T \)-predicate. We produce a function which is actually primitive recursive. First, note that \( A \) is nonempty (why?), and let \( x_0 \) be any index in \( A \). We define \( g \) by primitive recursion as follows:

\[
g(0) = x_0,
\]

\[
g(x + 1) = \begin{cases} 
\Pi_1(x) & \text{if } T(\Pi_1(x), a, \Pi_2(x)), \\
x_0 & \text{otherwise}.
\end{cases}
\]

Since this type of argument is new, it is helpful to explain informally what \( g \) does. For every input \( x \), the function \( g \) tries finitely many steps of a computation on input \( a \) of some partial computable function. The computation is given by \( \Pi_2(x) \), and the partial function is given by \( \Pi_1(x) \). Since \( \Pi_1 \) and \( \Pi_2 \) are projection functions, when \( x \) ranges over \( \mathbb{N} \), both \( \Pi_1(x) \) and \( \Pi_2(x) \) also range over \( \mathbb{N} \).

Such a process is called a dovetailing computation. Therefore all computations on input \( a \) for all partial computable functions will be tried, and the indices of the partial computable functions converging on input \( a \) will be selected. This type of argument will be used over and over again.

**Definition 5.4.** A subset \( X \) of \( \mathbb{N} \) is listable, or computably enumerable, or recursively enumerable\(^2\) iff either \( X = \emptyset \), or \( X \) is the range of some total computable function (total recursive function). Similarly, a subset \( X \) of \( \Sigma^* \) is listable or computably enumerable, or recursively enumerable iff either \( X = \emptyset \), or \( X \) is the range of some total computable function (total recursive function).

---

\(^2\)Since 1996, the term recursively enumerable has been considered old-fashioned by many researchers, and the terms listable and computably enumerable have been used instead.
We will often abbreviate computably enumerable as *c.e.*, (and recursively enumerable as *r.e.*). A computably enumerable set is sometimes called a *partially decidable* or *semidecidable* set.

**Remark:** It should be noted that the definition of a *listable set* (*r.e.* set or *c.e.* set) given in Definition 5.4 is different from an earlier definition given in terms of acceptance by a Turing machine and it is by no means obvious that these two definitions are equivalent. This equivalence will be proved in Proposition 5.9 ((1) $\iff$ (4)).

The following proposition relates computable sets and listable sets (recursive sets and recursively enumerable sets).

**Proposition 5.8.** A set $A$ is computable (recursive) iff both $A$ and its complement $\overline{A}$ are listable (recursively enumerable).

**Proof.** Assume that $A$ is computable. Then, it is trivial that its complement is also computable. Hence, we only have to show that a computable set is listable. The empty set is listable by definition. Otherwise, let $y \in A$ be any element. Then, the function $f$ defined such that

$$f(x) = \begin{cases} x & \text{iff } C_A(x) = 1, \\ y & \text{iff } C_A(x) = 0, \end{cases}$$

for all $x \in \mathbb{N}$ is computable and has range $A$.

Conversely, assume that both $A$ and $\overline{A}$ are computably enumerable. If either $A$ or $\overline{A}$ is empty, then $A$ is computable. Otherwise, let $A = f(\mathbb{N})$ and $\overline{A} = g(\mathbb{N})$, for some computable functions $f$ and $g$. We define the function $C_A$ as follows:

$$C_A(x) = \begin{cases} 1 & \text{if } f(\min_y [f(y) = x \lor g(y) = x]) = x, \\ 0 & \text{otherwise}. \end{cases}$$

The function $C_A$ lists $A$ and $\overline{A}$ in parallel, waiting to see whether $x$ turns up in $A$ or in $\overline{A}$. Note that $x$ must eventually turn up either in $A$ or in $\overline{A}$, so that $C_A$ is a total computable function.

Our next goal is to show that the listable (recursively enumerable) sets can be given several equivalent definitions.

**Proposition 5.9.** For any subset $A$ of $\mathbb{N}$, the following properties are equivalent:

1. $A$ is empty or $A$ is the range of a primitive recursive function (Rosser, 1936).
2. $A$ is listable (recursively enumerable).
3. $A$ is the range of a partial computable function.
4. $A$ is the domain of a partial computable function.
5.3. LISTABLE (RECURSIVELY ENUMERABLE) SETS

Proof. The implication (1) $\Rightarrow$ (2) is trivial, since $A$ is r.e. iff either it is empty or it is the range of a (total) computable function.

To prove the implication (2) $\Rightarrow$ (3), it suffices to observe that the empty set is the range of the totally undefined function (computed by an infinite loop program), and that a computable function is a partial computable function.

The implication (3) $\Rightarrow$ (4) is shown as follows. Assume that $A$ is the range of $\varphi_i$. Define the function $f$ such that

$$f(x) = \min y [T(i, \Pi_1(y), \Pi_2(y)) \land \text{Res}(\Pi_2(y)) = x]$$

for all $x \in \mathbb{N}$. Clearly, $f$ is partial computable and has domain $A$.

The implication (4) $\Rightarrow$ (1) is shown as follows. The only nontrivial case is when $A$ is nonempty. Assume that $A$ is the domain of $\varphi_i$. Since $A \neq \emptyset$, there is some $a \in \mathbb{N}$ such that $a \in A$, so the quantity

$$\min y [T(i, \Pi_1(y), \Pi_2(y))]$$

is defined and we can pick $a$ to be

$$a = \Pi_1(\min y [T(i, \Pi_1(y), \Pi_2(y))]).$$

We define the primitive recursive function $f$ as follows:

$$f(0) = a,$$

$$f(x + 1) = \begin{cases} 
\Pi_1(x) & \text{if } T(i, \Pi_1(x), \Pi_2(x)), \\
 a & \text{if } \neg T(i, \Pi_1(x), \Pi_2(x)).
\end{cases}$$

Clearly, $A$ is the range of $f$ and $f$ is primitive recursive.

More intuitive proofs of the implications (3) $\Rightarrow$ (4) and (4) $\Rightarrow$ (1) can be given. Assume that $A \neq \emptyset$ and that $A = \text{range}(g)$, where $g$ is a partial computable function. Assume that $g$ is computed by a RAM program $P$. To compute $f(x)$, we start computing the sequence $g(0), g(1), \ldots$ looking for $x$. If $x$ turns up as say $g(n)$, then we output $n$. Otherwise the computation diverges. Hence, the domain of $f$ is the range of $g$.

Assume now that $A$ is the domain of some partial computable function $g$, and that $g$ is computed by some Turing machine $M$. Since the case where $A = \emptyset$ is trivial, we may assume that $A \neq \emptyset$, and let $n_0 \in A$ be some chosen element in $A$. We construct another Turing machine performing the following steps: On input $n$,

(0) Do one step of the computation of $g(0)$

\ldots
(n) Do $n+1$ steps of the computation of $g(0)$
Do $n$ steps of the computation of $g(1)$

\ldots

Do 2 steps of the computation of $g(n-1)$
Do 1 step of the computation of $g(n)$

During this process, whenever the computation of $g(m)$ halts for some $m \leq n$, we output $m$. Otherwise, we output $n_0$.

In this fashion, we will enumerate the domain of $g$, and since we have constructed a Turing machine that halts for every input, we have a total computable function.

The following proposition can easily be shown using the proof technique of Proposition 5.9.

**Proposition 5.10.** (1) There is a computable function $h$ such that

\[
\text{range}(\varphi_x) = \text{dom}(\varphi_{h(x)})
\]

for all $x \in \mathbb{N}$.

(2) There is a computable function $k$ such that

\[
\text{dom}(\varphi_x) = \text{range}(\varphi_{k(x)})
\]

and $\varphi_{k(x)}$ is total computable, for all $x \in \mathbb{N}$ such that $\text{dom}(\varphi_x) \neq \emptyset$.

The proof of Proposition 5.10 is left as an exercise. Using Proposition 5.9, we can prove that $K$ is a listable set. Indeed, we have $K = \text{dom}(f)$, where

\[
f(x) = \varphi_{\text{univ}}(x, x)
\]

for all $x \in \mathbb{N}$. The set

\[
K_0 = \{ \langle x, y \rangle \mid \varphi_x(y) \text{ converges} \}
\]

is also a listable set, since $K_0 = \text{dom}(g)$, where

\[
g(z) = \varphi_{\text{univ}}(\Pi_1(z), \Pi_2(z)),
\]

which is partial computable. It worth recording these facts in the following lemma.

**Proposition 5.11.** The sets $K$ and $K_0$ are listable sets that are not computable (r.e. sets that are not recursive).

We can now prove that there are sets that are not c.e. (r.e.).
Proposition 5.12. For any indexing of the partial computable functions, the complement $\overline{K}$ of the set

$$K = \{ x \in \mathbb{N} \mid \varphi_x(x) \text{ converges} \}$$

is not listable (not recursively enumerable).

Proof. If $\overline{K}$ was listable, since $K$ is also listable, by Proposition 5.8, the set $K$ would be computable, a contradiction. \qed

The sets $\overline{K}$ and $\overline{K}_0$ are examples of sets that are not c.e. (r.e.). This shows that the c.e. sets (r.e. sets) are not closed under complementation. However, we leave it as an exercise to prove that the c.e. sets (r.e. sets) are closed under union and intersection.

We will prove later on that TOTAL is not c.e. (r.e.). This is rather unpleasant. Indeed, this means that there is no way of effectively listing all algorithms (all total computable functions). Hence, in a certain sense, the concept of partial computable function (procedure) is more natural than the concept of a (total) computable function (algorithm).

The next two propositions give other characterizations of the c.e. sets (r.e. sets) and of the computable sets (recursive sets). The proofs are left as an exercise.

Proposition 5.13. (1) A set $A$ is c.e. (r.e.) iff either it is finite or it is the range of an injective computable function.

(2) A set $A$ is c.e. (r.e.) if either it is empty or it is the range of a monotonic partial computable function.

(3) A set $A$ is c.e. (r.e.) iff there is a Turing machine $M$ such that, for all $x \in \mathbb{N}$, $M$ halts on $x$ iff $x \in A$.

Proposition 5.14. A set $A$ is computable (recursive) iff either it is finite or it is the range of a strictly increasing computable function.

Another important result relating the concept of partial computable function and that of a c.e. set (r.e. set) is given below.

Theorem 5.15. For every unary partial function $f$, the following properties are equivalent:

(1) $f$ is partial computable.

(2) The set

$$\{ \langle x, f(x) \rangle \mid x \in \text{dom}(f) \}$$

is c.e. (r.e.).

Proof. Let $g(x) = \langle x, f(x) \rangle$. Clearly, $g$ is partial computable, and

$$\text{range}(g) = \{ \langle x, f(x) \rangle \mid x \in \text{dom}(f) \}.$$
Conversely, assume that
\[
\text{range}(g) = \{ \langle x, f(x) \rangle \mid x \in \text{dom}(f) \}
\]
for some computable function \( g \). Then, we have
\[
f(x) = \Pi_2(g(\min y[\Pi_1(g(y)) = x]))
\]
for all \( x \in \mathbb{N} \), so that \( f \) is partial computable.

Using our indexing of the partial computable functions and Proposition 5.9, we obtain an indexing of the c.e. sets. (r.e. sets).

**Definition 5.5.** For any acceptable indexing \( \varphi_0, \varphi_1, \ldots \) of the partial computable functions, we define the enumeration \( W_0, W_1, \ldots \) of the c.e. sets (r.e. sets) by setting
\[
W_x = \text{dom}(\varphi_x).
\]

We now describe a technique for showing that certain sets are c.e. (r.e.) but not computable (not recursive), or complements of c.e. sets (r.e. sets) that are not computable (not recursive), or not c.e. (not r.e.), or neither c.e. (r.e.) nor the complement of a c.e. set (r.e. set). This technique is known as *reducibility*.

### 5.4 Reducibility and Complete Sets

We already used the notion of reducibility in the proof of Proposition 5.5 to show that \( \text{TOTAL} \) is not computable (not recursive).

**Definition 5.6.** Let \( A \) and \( B \) be subsets of \( \mathbb{N} \) (or \( \Sigma^* \)). We say that the set \( A \) is many-one reducible to the set \( B \) if there is a total computable function (or total recursive function) \( f : \mathbb{N} \to \mathbb{N} \) (or \( f : \Sigma^* \to \Sigma^* \)) such that
\[
x \in A \text{ iff } f(x) \in B \text{ for all } x \in \mathbb{N}.
\]
We write \( A \leq B \), and for short, we say that \( A \) is *reducible* to \( B \). Sometimes, the notation \( A \leq_m B \) is used to stress that this is a many-to-one reduction (that is, \( f \) is not necessarily injective).

Intuitively, deciding membership in \( B \) is as hard as deciding membership in \( A \). This is because any method for deciding membership in \( B \) can be converted to a method for deciding membership in \( A \) by first applying \( f \) to the number (or string) to be tested.

The following simple proposition is left as an exercise to the reader.
5.4. REDUCIBILITY AND COMPLETE SETS

Proposition 5.16. Let $A, B, C$ be subsets of $\mathbb{N}$ (or $\Sigma^*\Gamma^*$). The following properties hold:

(1) If $A \leq B$ and $B \leq C$, then $A \leq C$.

(2) If $A \leq B$ then $\overline{A} \leq \overline{B}$.

(3) If $A \leq B$ and $B$ is c.e., then $A$ is c.e.

(4) If $A \leq B$ and $A$ is not c.e., then $B$ is not c.e.

(5) If $A \leq B$ and $B$ is computable, then $A$ is computable.

(6) If $A \leq B$ and $A$ is not computable, then $B$ is not computable.

Another important concept is the concept of a complete set.

Definition 5.7. A c.e. set (r.e. set) $A$ is complete w.r.t. many-one reducibility iff every c.e. set (r.e. set) $B$ is reducible to $A$, i.e., $B \leq A$.

For simplicity, we will often say complete for complete w.r.t. many-one reducibility. Intuitively, a complete c.e. set (r.e. set) is a “hardest” c.e. set (r.e. set) as far as membership is concerned.

Theorem 5.17. The following properties hold:

(1) If $A$ is complete, $B$ is c.e (r.e.), and $A \leq B$, then $B$ is complete.

(2) $K_0$ is complete.

(3) $K_0$ is reducible to $K$. Consequently, $K$ is also complete.

Proof. (1) This is left as a simple exercise.

(2) Let $W_x$ be any c.e. set. Then

$$y \in W_x \iff \langle x, y \rangle \in K_0,$$

and the reduction function is the computable function $f$ such that

$$f(y) = \langle x, y \rangle$$

for all $y \in \mathbb{N}$.

(3) We use the s-m-n Theorem. First, we leave it as an exercise to prove that there is a computable function $f$ such that

$$\varphi_f(x)(y) = \begin{cases} 1 & \text{if } \varphi_{\Pi_1(x)}(\Pi_2(x)) \text{ converges,} \\ \text{undefined} & \text{otherwise,} \end{cases}$$

for all $x, y \in \mathbb{N}$. Then, for every $z \in \mathbb{N}$,

$$z \in K_0 \iff \varphi_{\Pi_1(z)}(\Pi_2(z)) \text{ converges},$$
iff \( \varphi_{f(z)}(y) = 1 \) for all \( y \in \mathbb{N} \). However,

\[
\varphi_{f(z)}(y) = 1 \quad \text{iff} \quad \varphi_{f(z)}(f(z)) = 1,
\]

since \( \varphi_{f(z)} \) is a constant function. This means that

\[ z \in K_0 \quad \text{iff} \quad f(z) \in K, \]

and \( f \) is the desired function.

As a corollary of Theorem 5.17, the set \( K \) is also complete.

**Definition 5.8.** Two sets \( A \) and \( B \) have the same *degree of unsolvability* or are *equivalent* iff \( A \leq B \) and \( B \leq A \).

Since \( K \) and \( K_0 \) are both complete, they have the same degree of unsolvability. We will now investigate the reducibility and equivalence of various sets. Recall that

\[
\text{TOTAL} = \{ x \in \mathbb{N} \mid \varphi_x \text{ is total} \}.
\]

We define \( \text{EMPTY} \) and \( \text{FINITE} \), as follows:

\[
\text{EMPTY} = \{ x \in \mathbb{N} \mid \varphi_x \text{ is undefined for all input} \},
\]

\[
\text{FINITE} = \{ x \in \mathbb{N} \mid \varphi_x \text{ is defined only for finitely many input} \}.
\]

Obviously, \( \text{EMPTY} \subset \text{FINITE} \), and since

\[ \text{FINITE} = \{ x \in \mathbb{N} \mid \varphi_x \text{ has a finite domain} \}, \]

we have

\[ \text{FINITE} = \{ x \in \mathbb{N} \mid \varphi_x \text{ has an infinite domain} \}, \]

and thus, \( \text{TOTAL} \subset \text{FINITE} \).

**Proposition 5.18.** We have \( K_0 \leq \text{EMPTY} \).

The proof of Proposition 5.18 follows from the proof of Theorem 5.17. We also have the following proposition.

**Proposition 5.19.** The following properties hold:

1. \( \text{EMPTY} \) is not c.e. (not r.e.).
2. \( \overline{\text{EMPTY}} \) is c.e. (r.e.).
3. \( \overline{K} \) and \( \text{EMPTY} \) are equivalent.
4. \( \text{EMPTY} \) is complete.
Proof. We prove (1) and (3), leaving (2) and (4) as an exercise (Actually, (2) and (4) follow easily from (3)). First, we show that $\mathcal{K} \leq \text{EMPTY}$. By the s-m-n Theorem, there exists a computable function $f$ such that

$$\varphi_{f(x)}(y) = \begin{cases} \varphi_x(x) & \text{if } \varphi_x(x) \text{ converges,} \\ \text{undefined} & \text{if } \varphi_x(x) \text{ diverges,} \end{cases}$$

for all $x, y \in \mathbb{N}$. Note that for all $x \in \mathbb{N}$,

$$x \in \mathcal{K} \iff f(x) \in \text{EMPTY},$$

and thus, $\mathcal{K} \leq \text{EMPTY}$. Since $\mathcal{K}$ is not c.e., EMPTY is not c.e.

By the s-m-n Theorem, there is a computable function $g$ such that

$$\varphi_{g(x)}(y) = \min z[T(x, \Pi_1(z), \Pi_2(z))],$$

for all $x, y \in \mathbb{N}$. Note that

$$x \in \text{EMPTY} \iff g(x) \in \mathcal{K}$$

for all $x \in \mathbb{N}$. Therefore, EMPTY $\leq \mathcal{K}$, and since we just showed that $\mathcal{K} \leq \text{EMPTY}$, the sets $\mathcal{K}$ and EMPTY are equivalent. \hfill \Box

**Proposition 5.20.** The following properties hold:

1. **TOTAL** and **TOTAL** are not c.e. (not r.e.).
2. **FINITE** and **FINITE** are not c.e (not r.e.).

Proof. Checking the proof of Theorem 5.17, we note that $K_0 \leq \text{TOTAL}$ and $K_0 \leq \text{FINITE}$. Hence, we get $\overline{K_0} \leq \text{TOTAL}$ and $\overline{K_0} \leq \text{FINITE}$, and neither **TOTAL** nor **FINITE** is c.e. If TOTAL was c.e., then there would be a computable function $f$ such that TOTAL $= \text{range}(f)$. Define $g$ as follows:

$$g(x) = \varphi_{f(x)}(x) + 1 = \varphi_{\text{univ}}(f(x), x) + 1$$

for all $x \in \mathbb{N}$. Since $f$ is total and $\varphi_{f(x)}$ is total for all $x \in \mathbb{N}$, the function $g$ is total computable. Let $e$ be an index such that

$$g = \varphi_{f(e)}.$$

Since $g$ is total, $g(e)$ is defined. Then, we have

$$g(e) = \varphi_{f(e)}(e) + 1 = g(e) + 1,$$

a contradiction. Hence, TOTAL is not c.e. Finally, we show that **TOTAL** $\leq \text{FINITE}$. This also shows that **FINITE** is not c.e. By the s-m-n Theorem, there is a computable function $f$ such that

$$\varphi_{f(x)}(y) = \begin{cases} 1 & \text{if } \forall z \leq y(\varphi_x(z) \downarrow) \\ \text{undefined} & \text{otherwise,} \end{cases}$$
for all \( x, y \in \mathbb{N} \). It is easily seen that
\[
x \in \text{TOTAL} \iff f(x) \in \text{FINITE}
\]
for all \( x \in \mathbb{N} \). \( \square \)

From Proposition 5.20, we have \( \text{TOTAL} \leq \text{FINITE} \). It turns out that \( \text{FINITE} \leq \text{TOTAL} \), and \( \text{TOTAL} \) and \( \text{FINITE} \) are equivalent.

**Proposition 5.21.** The sets \( \text{TOTAL} \) and \( \text{FINITE} \) are equivalent.

**Proof.** We show that \( \text{FINITE} \leq \text{TOTAL} \). By the s-m-n Theorem, there is a computable function \( f \) such that
\[
\varphi_{f(x)}(y) = \begin{cases} 1 & \text{if } \exists z \geq y (\varphi_x(z) \downarrow), \\ \text{undefined} & \text{if } \forall z \geq y (\varphi_x(z) \uparrow), \end{cases}
\]
for all \( x, y \in \mathbb{N} \). It is easily seen that
\[
x \in \text{FINITE} \iff f(x) \in \text{TOTAL}
\]
for all \( x \in \mathbb{N} \). \( \square \)

We now turn to the recursion theorem.

### 5.5 The Recursion Theorem

The recursion theorem, due to Kleene, is a fundamental result in recursion theory. Let \( f \) be a total computable function. Then, it turns out that there is some \( n \) such that
\[
\varphi_n = \varphi_{f(n)}.
\]

**Theorem 5.22.** (Recursion Theorem, Version 1) Let \( \varphi_0, \varphi_1, \ldots \) be any acceptable indexing of the partial computable functions. For every total computable function \( f \), there is some \( n \) such that
\[
\varphi_n = \varphi_{f(n)}.
\]

**Proof.** Consider the function \( \theta \) defined such that
\[
\theta(x, y) = \varphi_{\text{univ}}(\varphi_{\text{univ}}(x, x), y)
\]
for all \( x, y \in \mathbb{N} \). The function \( \theta \) is partial computable, and there is some index \( j \) such that \( \varphi_j = \theta \). By the s-m-n Theorem, there is a computable function \( g \) such that
\[
\varphi_{g(x)}(y) = \theta(x, y).
\]
Consider the function $f \circ g$. Since it is computable, there is some index $m$ such that $\varphi_m = f \circ g$. Let
\[ n = g(m). \]
Since $\varphi_m$ is total, $\varphi_m(m)$ is defined, and we have
\[
\begin{align*}
\varphi_n(y) &= \varphi_{g(m)}(y) = \theta(m, y) = \varphi_{\text{univ}}(\varphi_{\text{univ}}(m, m), y) = \varphi_{\varphi_{\text{univ}}(m, m)}(y) \\
&= \varphi_{\varphi_m}(m)(y) = \varphi_{f \circ g}(m)(y) = \varphi_{f(g(m))}(y) = \varphi_f(n)(y),
\end{align*}
\]
for all $y \in \mathbb{N}$. Therefore, $\varphi_n = \varphi_{f(n)}$, as desired. \qed

The recursion Theorem can be strengthened as follows.

**Theorem 5.23. (Recursion Theorem, Version 2)** Let $\varphi_0, \varphi_1, \ldots$ be any acceptable indexing of the partial computable functions. There is a total computable function $h$ such that for all $x \in \mathbb{N}$, if $\varphi_x$ is total, then
\[
\varphi_{\varphi_x(h(x))} = \varphi_h(x).
\]

**Proof.** The computable function $g$ obtained in the proof of Theorem 5.22 satisfies the condition
\[
\varphi_g(x) = \varphi_{\varphi_x}(x),
\]
and it has some index $i$ such that $\varphi_i = g$. Recall that $c$ is a computable composition function such that
\[
\varphi_c(x, y) = \varphi_x \circ \varphi_y.
\]
It is easily verified that the function $h$ defined such that
\[
h(x) = g(c(x, i))
\]
for all $x \in \mathbb{N}$ does the job. \qed

A third version of the recursion Theorem is given below.

**Theorem 5.24. (Recursion Theorem, Version 3)** For all $n \geq 1$, there is a total computable function $h$ of $n+1$ arguments, such that for all $x \in \mathbb{N}$, if $\varphi_x$ is a total computable function of $n+1$ arguments, then
\[
\varphi_{\varphi_x(h(x, x_1, \ldots, x_n), x_1, \ldots, x_n)} = \varphi_{h(x, x_1, \ldots, x_n)},
\]
for all $x_1, \ldots, x_n \in \mathbb{N}$.

**Proof.** Let $\theta$ be the function defined such that
\[
\theta(x, x_1, \ldots, x_n, y) = \varphi_{\varphi_x(x, x_1, \ldots, x_n)}(y) = \varphi_{\text{univ}}(\varphi_{\text{univ}}(x, x_1, \ldots, x_n), y)
\]
for all \(x, x_1, \ldots, x_n, y \in \mathbb{N}\). By the s-m-n Theorem, there is a computable function \(g\) such that
\[
\varphi_{g(x, x_1, \ldots, x_n)} = \varphi_{\varphi_x(x, x_1, \ldots, x_n)}.
\]
It is easily shown that there is a computable function \(c\) such that
\[
\varphi_{c(x, j)}(x, x_1, \ldots, x_n) = \varphi_{\varphi_i(\varphi_j(x, x_1, \ldots, x_n), x_1, \ldots, x_n)}
\]
for any two partial computable functions \(\varphi_i\) and \(\varphi_j\) (viewed as functions of \(n + 1\) arguments) and all \(x, x_1, \ldots, x_n \in \mathbb{N}\). Let \(\varphi_i = g\), and define \(h\) such that
\[
h(x, x_1, \ldots, x_n) = g(c(x, i), x_1, \ldots, x_n),
\]
for all \(x, x_1, \ldots, x_n \in \mathbb{N}\). We have
\[
\varphi_h(x, x_1, \ldots, x_n) = \varphi_{g(c(x, i), x_1, \ldots, x_n)} = \varphi_{\varphi_{c(x, i)}(c(x, i), x_1, \ldots, x_n)},
\]
and
\[
\varphi_{\varphi_{c(x, i)}(c(x, i), x_1, \ldots, x_n)} = \varphi_{\varphi_{x}(c(x, i), x_1, \ldots, x_n), x_1, \ldots, x_n)};
\]
\[= \varphi_{\varphi_{x}(g(c(x, i), x_1, \ldots, x_n), x_1, \ldots, x_n)},
\]
\[= \varphi_{\varphi_{x}(h(x, x_1, \ldots, x_n), x_1, \ldots, x_n)}.\]

As a first application of the recursion theorem, we can show that there is an index \(n\) such that \(\varphi_n\) is the constant function with output \(n\). Loosely speaking, \(\varphi_n\) prints its own name. Let \(f\) be the computable function such that
\[
f(x, y) = x
\]
for all \(x, y \in \mathbb{N}\). By the s-m-n Theorem, there is a computable function \(g\) such that
\[
\varphi_{g(x)}(y) = f(x, y) = x
\]
for all \(x, y \in \mathbb{N}\). By the recursion Theorem 5.22, there is some \(n\) such that
\[
\varphi_{g(n)} = \varphi_n,
\]
the constant function with value \(n\).

As a second application, we get a very short proof of Rice’s Theorem. Let \(C\) be such that \(P_C \neq \emptyset\) and \(P_C \neq \mathbb{N}\), and let \(j \in P_C\) and \(k \in \mathbb{N} - P_C\). Define the function \(f\) as follows:
\[
f(x) = \begin{cases} j & \text{if } x \notin P_C, \\ k & \text{if } x \in P_C. \end{cases}
\]
If $P_C$ is computable, then $f$ is computable. By the recursion Theorem 5.22, there is some $n$ such that

$$\varphi_{f(n)} = \varphi_n.$$ 

But then, we have

$$n \in P_C \iff f(n) \notin P_C$$

by definition of $f$, and thus,

$$\varphi_{f(n)} \neq \varphi_n,$$

a contradiction. Hence, $P_C$ is not computable.

As a third application, we prove the following proposition.

**Proposition 5.25.** Let $C$ be a set of partial computable functions and let

$$A = \{x \in \mathbb{N} \mid \varphi_x \in C\}.$$ 

The set $A$ is not reducible to its complement $\overline{A}$.

**Proof.** Assume that $A \leq \overline{A}$. Then, there is a computable function $f$ such that

$$x \in A \iff f(x) \in \overline{A}$$

for all $x \in \mathbb{N}$. By the recursion Theorem, there is some $n$ such that

$$\varphi_{f(n)} = \varphi_n.$$ 

But then,

$$\varphi_n \in C \iff n \in A \iff f(n) \in \overline{A} \iff \varphi_{f(n)} \in \overline{C},$$

contradicting the fact that

$$\varphi_{f(n)} = \varphi_n.$$ 

The recursion Theorem can also be used to show that functions defined by recursive definitions other than primitive recursion are partial computable. This is the case for the function known as *Ackermann’s function*, defined recursively as follows:

$$f(0, y) = y + 1,$$

$$f(x + 1, 0) = f(x, 1),$$

$$f(x + 1, y + 1) = f(x, f(x + 1, y)).$$

It can be shown that this function is not primitive recursive. Intuitively, it outgrows all primitive recursive functions. However, $f$ is computable, but this is not so obvious. We can
use the recursion Theorem to prove that $f$ is computable. Consider the following definition by cases:

\[
\begin{align*}
g(n, 0, y) &= y + 1, \\
g(n, x + 1, 0) &= \varphi_{\text{univ}}(n, x, 1), \\
g(n, x + 1, y + 1) &= \varphi_{\text{univ}}(n, x, \varphi_{\text{univ}}(n, x + 1, y)).
\end{align*}
\]

Clearly, $g$ is partial computable. By the s-m-n Theorem, there is a computable function $h$ such that

\[
\varphi_{h(n)}(x, y) = g(n, x, y).
\]

By the recursion Theorem, there is an $m$ such that

\[
\varphi_{h(m)} = \varphi_m.
\]

Therefore, the partial computable function $\varphi_m(x, y)$ satisfies the definition of Ackermann’s function. We showed in a previous Section that $\varphi_m(x, y)$ is a total function, and thus, Ackermann’s function is a total computable function.

Hence, the recursion Theorem justifies the use of certain recursive definitions. However, note that there are some recursive definitions that are only satisfied by the completely undefined function.

In the next Section, we prove the extended Rice Theorem.

### 5.6 Extended Rice Theorem

The extended Rice Theorem characterizes the sets of partial computable functions $C$ such that $P_C$ is c.e. (r.e.). First, we need to discuss a way of indexing the partial computable functions that have a finite domain. Using the uniform projection function $\Pi$, we define the primitive recursive function $F$ such that

\[
F(x, y) = \Pi(y + 1, \Pi_1(x) + 1, \Pi_2(x)).
\]

We also define the sequence of partial functions $P_0, P_1, \ldots$ as follows:

\[
P_x(y) = \begin{cases} 
F(x, y) - 1 & \text{if } 0 < F(x, y) \text{ and } y < \Pi_1(x) + 1, \\
\text{undefined} & \text{otherwise}.
\end{cases}
\]

**Proposition 5.26.** Every $P_x$ is a partial computable function with finite domain, and every partial computable function with finite domain is equal to some $P_x$.

The proof is left as an exercise. The easy part of the extended Rice Theorem is the following lemma. Recall that given any two partial functions $f: A \to B$ and $g: A \to B$, we say that $g$ extends $f$ iff $f \subseteq g$, which means that $g(x)$ is defined whenever $f(x)$ is defined, and if so, $g(x) = f(x)$. 
Proposition 5.27. Let $C$ be a set of partial computable functions. If there is a c.e. set (r.e. set) $A$ such that, $\varphi_x \in C$ iff there is some $y \in A$ such that $\varphi_x$ extends $P_y$, then $P_C = \{x \mid \varphi_x \in C\}$ is c.e. (r.e.).

Proof. Proposition 5.27 can be restated as

$$P_C = \{x \mid \exists y \in A, P_y \subseteq \varphi_x\}$$

is c.e. If $A$ is empty, so is $P_C$, and $P_C$ is c.e. Otherwise, let $f$ be a computable function such that $A = \text{range}(f)$.

Let $\psi$ be the following partial computable function:

$$\psi(z) = \begin{cases} 
\Pi_1(z) & \text{if } P_{f(P_2(z))} \subseteq \varphi_{\Pi_2(z)}, \\
\text{undefined} & \text{otherwise}.
\end{cases}$$

It is clear that $P_C = \text{range}(\psi)$.

To see that $\psi$ is partial computable, write $\psi(z)$ as follows:

$$\psi(z) = \begin{cases} 
\Pi_1(z) & \text{if } \forall w \leq \Pi_1(f(P_2(z)))[F(f(P_2(z)), w) > 0 \\
\sup_{\varphi_{\Pi_2(z)}}(w) = F(f(P_2(z)), w) - 1], \\
\text{undefined} & \text{otherwise}.
\end{cases}$$

To establish the converse of Proposition 5.27, we need two propositions.

Proposition 5.28. If $P_C$ is c.e. (r.e.) and $\varphi \in C$, then there is some $P_y \subseteq \varphi$ such that $P_y \in C$.

Proof. Assume that $P_C$ is c.e. and that $\varphi \in C$. By an s-m-n construction, there is a computable function $g$ such that

$$\varphi_{g(x)}(y) = \begin{cases} 
\varphi(y) & \text{if } \forall z \leq y[\neg T(x, x, z)], \\
\text{undefined} & \text{if } \exists z \leq y[T(x, x, z)],
\end{cases}$$

for all $x, y \in \mathbb{N}$. Observe that if $x \in K$, then $\varphi_{g(x)}$ is a finite subfunction of $\varphi$, and if $x \in \overline{K}$, then $\varphi_{g(x)} = \varphi$. Assume that no finite subfunction of $\varphi$ is in $C$. Then,

$$x \in \overline{K} \text{ iff } g(x) \in P_C$$

for all $x \in \mathbb{N}$, that is, $\overline{K} \leq P_C$. Since $P_C$ is c.e., $\overline{K}$ would also be c.e., a contradiction.

As a corollary of Proposition 5.28, we note that TOTAL is not c.e.
**Proposition 5.29.** If $P_C$ is c.e. (r.e.), $\varphi \in C$, and $\varphi \subseteq \psi$, where $\psi$ is a partial computable function, then $\psi \in C$.

**Proof.** Assume that $P_C$ is c.e. We claim that there is a computable function $h$ such that

$$\varphi_{h(x)}(y) = \begin{cases} 
\psi(y) & \text{if } x \in K, \\
\varphi(y) & \text{if } x \in \overline{K}, 
\end{cases}$$

for all $x, y \in \mathbb{N}$. Assume that $\psi \notin C$. Then

$$x \in \overline{K} \iff h(x) \in P_C$$

for all $x \in \mathbb{N}$, that is, $\overline{K} \leq P_C$, a contradiction, since $P_C$ is c.e. Therefore, $\psi \in C$. To find the function $h$ we proceed as follows: Let $\varphi = \varphi_j$ and define $\Theta$ such that

$$\Theta(x, y, z) = \begin{cases} 
\varphi(y) & \text{if } T(j, y, z) \land \neg T(x, y, w), \text{ for } 0 \leq w < z \\
\psi(y) & \text{if } T(x, x, z) \land \neg T(j, y, w), \text{ for } 0 \leq w < z \\
\text{undefined} & \text{otherwise}.
\end{cases}$$

Observe that if $x = y = j$, then $\Theta(j, j, z)$ is multiply defined, but since $\psi$ extends $\varphi$, we get the same value $\psi(y) = \varphi(y)$, so $\Theta$ is a well defined partial function. Clearly, for all $(m, n) \in \mathbb{N}^2$, there is at most one $z \in \mathbb{N}$ so that $\Theta(x, y, z)$ is defined, so the function $\sigma$ defined by

$$\sigma(x, y) = \begin{cases} 
z & \text{if } (x, y, z) \in \text{dom}(\Theta) \\
\text{undefined} & \text{otherwise}
\end{cases}$$

is a partial computable function. Finally, let

$$\theta(x, y) = \Theta(x, y, \sigma(x, y)),$$

a partial computable function. It is easy to check that

$$\theta(x, y) = \begin{cases} 
\psi(y) & \text{if } x \in K, \\
\varphi(y) & \text{if } x \in \overline{K},
\end{cases}$$

for all $x, y \in \mathbb{N}$. By the s-m-n Theorem, there is a computable function $h$ such that

$$\varphi_{h(x)}(y) = \theta(x, y)$$

for all $x, y \in \mathbb{N}$. 

Observe that Proposition 5.29 yields a new proof that $\overline{\text{TOTAL}}$ is not c.e. (not r.e.). Finally, we can prove the extended Rice Theorem.

**Theorem 5.30.** (Extended Rice Theorem) The set $P_C$ is c.e. (r.e.) iff there is a c.e. set (r.e. set) $A$ such that

$$\varphi_x \in C \iff \exists y \in A (P_y \subseteq \varphi_x).$$
5.7. CREATIVE AND PRODUCTIVE SETS

Proof. Let $P_C = \text{dom}(\varphi_i)$. Using the s-m-n Theorem, there is a computable function $k$ such that

$$\varphi_{k(y)} = P_y$$

for all $y \in \mathbb{N}$. Define the c.e. set $A$ such that

$$A = \text{dom}(\varphi_i \circ k).$$

Then,

$$y \in A \iff \varphi_i(k(y)) \downarrow \iff P_y \in C.$$ 

Next, using Proposition 5.28 and Proposition 5.29, it is easy to see that

$$\varphi_x \in C \iff \exists y \in A (P_y \subseteq \varphi_x).$$

Indeed, if $\varphi_x \in C$, by Proposition 5.28, there is a finite subfunction $P_y \subseteq \varphi_x$ such that $P_y \in C$, but

$$P_y \in C \iff y \in A,$$

as desired. On the other hand, if

$$P_y \subseteq \varphi_x$$

for some $y \in A$, then

$$P_y \in C,$$

and by Proposition 5.29, since $\varphi_x$ extends $P_y$, we get

$$\varphi_x \in C.$$

$\square$

5.7 Creative and Productive Sets

In this section, we discuss some special sets that have important applications in logic: creative and productive sets. The concepts to be described are illustrated by the following situation. Assume that

$$W_x \subseteq K$$

for some $x \in \mathbb{N}$. We claim that

$$x \in \overline{K} - W_x.$$ 

Indeed, if $x \in W_x$, then $\varphi_x(x)$ is defined, and by definition of $K$, we get $x \notin \overline{K}$, a contradiction. Therefore, $\varphi_x(x)$ must be undefined, that is,

$$x \in \overline{K} - W_x.$$ 

The above situation can be generalized as follows.
CHAPTER 5. ELEMENTARY RECURSIVE FUNCTION THEORY

Definition 5.9. A set $A$ is **productive** iff there is a total computable function $f$ such that

$$
\text{if } W_x \subseteq A \text{ then } f(x) \in A - W_x
$$

for all $x \in \mathbb{N}$. The function $f$ is called the **productive function of** $A$. A set $A$ is **creative** if it is c.e (r.e.) and if its complement $\overline{A}$ is productive.

As we just showed, $K$ is creative and $\overline{K}$ is productive. The following facts are immediate consequences of the definition.

1. A productive set is not c.e. (r.e.).
2. A creative set is not computable (not recursive).

Creative and productive sets arise in logic. The set of theorems of a logical theory is often creative. For example, the set of theorems in Peano’s arithmetic is creative. This yields incompleteness results.

**Proposition 5.31.** If a set $A$ is productive, then it has an infinite c.e. (r.e.) subset.

**Proof.** We first give an informal proof. Let $f$ be the computable productive function of $A$. We define a computable function $g$ as follows: Let $x_0$ be an index for the empty set, and let

$$
g(0) = f(x_0).
$$

Assuming that

$$
\{g(0), g(1), \ldots, g(y)\}
$$

is known, let $x_{y+1}$ be an index for this finite set, and let

$$
g(y + 1) = f(x_{y+1}).
$$

Since $W_{x_{y+1}} \subseteq A$, we have $f(x_{y+1}) \in A$.

For the formal proof, we use the following facts whose proof is left as an exercise:

1. There is a computable function $u$ such that

$$
W_{u(x, y)} = W_x \cup W_y.
$$

2. There is a computable function $t$ such that

$$
W_{t(x)} = \{x\}.
$$

Letting $x_0$ be an index for the empty set, we define the function $h$ as follows:

$$
h(0) = x_0,
$$

$$
h(y + 1) = u(t(f(y)), h(y)).
$$

We define $g$ such that

$$
g = f \circ h.
$$

It is easily seen that $g$ does the job. \qed
Another important property of productive sets is the following.

**Proposition 5.32.** If a set $A$ is productive, then $\overline{K} \leq A$.

**Proof.** Let $f$ be a productive function for $A$. Using the s-m-n Theorem, we can find a computable function $h$ such that

$$W_{h(y,x)} = \begin{cases} \{f(y)\} & \text{if } x \in K, \\ \emptyset & \text{if } x \in \overline{K}. \end{cases}$$

The above can be restated as follows:

$$\varphi_{h(y,x)}(z) = \begin{cases} 1 & \text{if } x \in K \text{ and } z = f(y), \\ \text{undefined} & \text{if } x \in \overline{K}, \end{cases}$$

for all $x, y, z \in \mathbb{N}$. By the third version of the recursion Theorem (Theorem 5.24), there is a computable function $g$ such that

$$W_g(x) = W_{h(g(x),x)}$$

for all $x \in \mathbb{N}$. Let

$$k = f \circ g.$$ 

We claim that

$$x \in \overline{K} \iff k(x) \in A$$

for all $x \in \mathbb{N}$. The verification of this fact is left as an exercise. Thus, $\overline{K} \leq A$. $\square$

Using Proposition 5.32, the following results can be shown.

**Proposition 5.33.** The following facts hold.

1. If $A$ is productive and $A \leq B$, then $B$ is productive.
2. $A$ is creative iff $A$ is equivalent to $K$.
3. $A$ is creative iff $A$ is complete,
Chapter 6

The Lambda-Calculus

The original motivation of Alonzo Church for inventing the \( \lambda \)-calculus was to provide a type-free foundation for mathematics (alternate to set theory) based on higher-order logic and the notion of function in the early 1930’s (1932, 1933). This attempt to provide such a foundation for mathematics failed due to a form of Russell’s paradox. Church was clever enough to turn the technical reason for this failure, the existence of fixed-point combinators, into a success, namely to view the \( \lambda \)-calculus as a formalism for defining the notion of computability (1932, 1933, 1935). The \( \lambda \)-calculus is indeed one of the first computation models, slightly preceding the Turing machine.

Kleene proved in 1936 that all the computable functions (recursive functions) in the sense of Herbrand and Gödel are definable in the \( \lambda \)-calculus, showing that the \( \lambda \)-calculus has universal computing power. In 1937, Turing proved that Turing machines compute the same class of computable functions. (This paper is very hard to read, in part because the definition of a Turing machine is not included in this paper). In short, the \( \lambda \)-calculus and Turing machines have the same computing power. Here we have to be careful. To be precise we should have said that all the total computable functions (total recursive functions) are definable in the \( \lambda \)-calculus. In fact, it is also true that all the partial computable functions (partial recursive functions) are definable in the \( \lambda \)-calculus but this requires more care.

Since the \( \lambda \)-calculus does not have any notion of tape, register, or any other means of storing data, it quite amazing that the \( \lambda \)-calculus has so much computing power.

The \( \lambda \)-calculus is based on three concepts:

1. Application.
2. Abstraction (also called \( \lambda \)-abstraction).
3. \( \beta \)-reduction (and \( \beta \)-conversion).

If \( f \) is a function, say the exponential function \( f : \mathbb{N} \to \mathbb{N} \) given by \( f(n) = 2^n \), and if \( n \) a natural number, then the result of applying \( f \) to a natural number, say 5, is written as

\[ (f5) \]
and is called an application. Here we can agree that \( f \) and 5 do not have the same type, in the sense that \( f \) is a function and 5 is a number, so applications such as \((ff)\) or \((55)\) do not make sense, but the \(\lambda\)-calculus is type-free so expressions such as \((ff)\) as allowed. This may seem silly, and even possibly undesirable, but allowing self application turns out to a major reason for the computing power of the \(\lambda\)-calculus.

Given an expression \(M\) containing a variable \(x\), say
\[
M(x) = x^2 + x + 1,
\]
as \(x\) ranges over \(\mathbb{N}\), we obtain the function represented in standard mathematical notation by \(x \mapsto x^2 + x + 1\). If we supply the input value 5 for \(x\), then the value of the function is \(5^2 + 5 + 1 = 31\). Church introduced the notation
\[
\lambda x. (x^2 + x + 1)
\]
for this function. Here, we have an abstraction, in the sense that the static expression \(M(x)\) for \(x\) fixed becomes an “abstract” function denoted \(\lambda x. M\).

It would be pointless to only have the two concepts of application and abstraction. The glue between these two notions is a form of evaluation called \(\beta\)-reduction. Given a \(\lambda\)-abstraction \(\lambda x. M\) and some other term \(N\) (thought of as an argument), we have the “evaluation” rule, we say \(\beta\)-reduction,
\[
(\lambda x. M) N \xrightarrow{+} \beta M[x := N],
\]
where \(M[x := N]\) denotes the result of substituting \(N\) for all occurrences of \(x\) in \(M\). For example, if \(M = \lambda x. (x^2 + x + 1)\) and \(N = 2y + 1\), we have
\[
(\lambda x. (x^2 + x + 1))(2y + 1) \xrightarrow{+} \beta (2y + 1)^2 + 2y + 1 + 1.
\]

Observe that \(\beta\)-reduction is a purely formal operation (plugging \(N\) wherever \(x\) occurs in \(M\)), and that the expression \((2y+1)^2 + 2y + 1 + 1\) is not instantly simplified to \(4y^2 + 6y + 3\). In the \(\lambda\)-calculus, the natural numbers as well as the arithmetic operations \(+\) and \(\times\) need to be represented as \(\lambda\)-terms in such a way that they “evaluate” correctly using only \(\beta\)-conversion. In this sense, the \(\lambda\)-calculus is an incredibly low-level programming language. Nevertheless, the \(\lambda\)-calculus is the core of various functional programming languages such as OCaml, ML, Miranda and Haskell, among others.

We now proceed with precise definitions and results. But first we ask the reader not to think of functions as the functions we encounter in analysis or algebra. Instead think of functions as rules for computing (by moving and plugging arguments around), a more combinatory (which does not mean combinatorial) viewpoint.

This chapter relies heavily on the masterly expositions by Barendregt \[3, 4\]. We also found inspiration from very informative online material by Henk Barendregt, Peter Selinger, and J.R.B. Cockett, whom we thank. Hindley and Seldin \[16\] is also an excellent source (and not as advanced as Barendregt \[3\]).

\[1\]Apparently, Church was fond of Greek letters.
6.1 Syntax of the Lambda-Calculus

We begin by defining the lambda-calculus, also called untyped lambda-calculus or pure lambda-calculus, to emphasize that the terms of this calculus are not typed. This formal system consists of

1. A set of terms, called \( \lambda \)-terms.

2. A notion of reduction, called \( \beta \)-reduction, which allows a term \( M \) to be transformed into another term \( N \) in a way that mimics a kind of evaluation.

First we define (pure) \( \lambda \)-terms. We have a countable set of variables \( \{ x_0, x_1, \ldots, x_n \ldots \} \) that correspond to the atomic \( \lambda \)-terms.

**Definition 6.1.** The \( \lambda \)-terms \( M \) are defined inductively as follows:

1. If \( x_i \) is a variable, then \( x_i \) is a \( \lambda \)-term.

2. If \( M \) and \( N \) are \( \lambda \)-terms, then \( (MN) \) is a \( \lambda \)-term called an application.

3. If \( M \) is a \( \lambda \)-term, and \( x \) is a variable, then the expression \( (\lambda x. M) \) is a \( \lambda \)-term called a \( \lambda \)-abstraction.

Note that the only difference between the \( \lambda \)-terms of Definition 6.1 and the raw simply-typed \( \lambda \)-terms of Definition 2.13 is that in Clause (3), in a \( \lambda \)-abstraction term \( (\lambda x. M) \), the variable \( x \) occurs without any type information, whereas in a simply-typed \( \lambda \)-abstraction term \( (\lambda x: \sigma. M) \), the variable \( x \) is assigned the type \( \sigma \). At this stage this is only a cosmetic difference because raw \( \lambda \)-terms are not yet assigned types. But there are type-checking rules for assigning types to raw simply-typed \( \lambda \)-terms that restrict application, so the set of simply-typed \( \lambda \)-terms that type-check is much more restricted than the set of (untyped) \( \lambda \)-terms. In particular, no simply-typed \( \lambda \)-term that type-checks can be a self-application \( (MM) \). The fact that self-application is allowed in the untyped \( \lambda \)-calculus is what gives it its computational power (through fixed-point combinators, see Section 6.5).

**Definition 6.2.** The depth \( d(M) \) of a \( \lambda \)-term \( M \) is defined inductively as follows.

1. If \( M \) is a variable \( x \), then \( d(x) = 0 \).

2. If \( M \) is an application \( (M_1M_2) \), then \( d(M) = \max\{d(M_1), d(M_2)\} + 1 \).

3. If \( M \) is a \( \lambda \)-abstraction \( (\lambda x. M_1) \), then \( d(M) = d(M_1) + 1 \).

It is pretty clear that \( \lambda \)-terms have representations as (ordered) labeled trees.

**Definition 6.3.** Given a \( \lambda \)-term \( M \), the tree \( \text{tree}(M) \) representing \( M \) is defined inductively as follows:

1. If \( M \) is a variable \( x \), then \( \text{tree}(M) \) is the one-node tree labeled \( x \).
2. If $M$ is an application $(M_1 M_2)$, then $\text{tree}(M)$ is the tree with a binary root node labeled $\cdot$, and with a left subtree $\text{tree}(M_1)$ and a right subtree $\text{tree}(M_2)$.

3. If $M$ is a $\lambda$-abstraction $\lambda x. M_1$, then $\text{tree}(M)$ is the tree with a unary root node labeled $\lambda x$, and with one subtree $\text{tree}(M_1)$.

Definition 6.3 is illustrated in Figure 6.1.

![Figure 6.1: The tree $\text{tree}(M)$ associated with a pure $\lambda$-term $M$.](image)

Obviously, the depth $d(M)$ of $\lambda$-term is the depth of its tree representation $\text{tree}(M)$. Unfortunately $\lambda$-terms contain a profusion of parentheses so some conventions are commonly used:

1. A term of the form
   
   $$(\cdots ((FM_1) M_2) \cdots) M_n)$$

   is abbreviated (association to the left) as

   $$FM_1 \cdots M_n.$$  

2. A term of the form
   
   $$\lambda x_1. (\lambda x_2. (\cdots (\lambda x_n. M) \cdots))$$

   is abbreviated (association to the right) as

   $$\lambda x_1 \cdots x_n. M.$$
Matching parentheses may be dropped or added for convenience. Here are some examples of λ-terms (and their abbreviation):

\[
\begin{align*}
& y \\
& (yx) \\
& \lambda x. (yx) \\
& ((\lambda x. (yx))z) \\
& (((\lambda x. (\lambda y. (yx)))z)w)
\end{align*}
\]

\[
\begin{align*}
& y \\
& yx \\
& \lambda x. yx \\
& (\lambda x. yx)z \\
& (\lambda xy. yx)zw.
\end{align*}
\]

Note that \( \lambda x. yx \) is an abbreviation for \((\lambda x. (yx))\), not \((\lambda x. y)x\).

The variables occurring in a λ-term are free of bound.

**Definition 6.4.** For any λ-term \( M \), the set \( FV(M) \) of free variables of \( M \) and the set \( BV(M) \) of bound variables in \( M \) are defined inductively as follows:

1. If \( M = x \) (a variable), then
   \[ FV(x) = \{ x \}, \quad BV(x) = \emptyset. \]

2. If \( M = (M_1M_2) \), then
   \[ FV(M) = FV(M_1) \cup FV(M_2), \quad BV(M) = BV(M_1) \cup BV(M_2). \]

3. If \( M = (\lambda x. M_1) \), then
   \[ FV(M) = FV(M_1) - \{ x \}, \quad BV(M) = BV(M_1) \cup \{ x \}. \]

If \( x \in FV(M_1) \), we say that the occurrences of the variable \( x \) occur in the scope of \( \lambda \).

A λ-term \( M \) is closed or a combinator if \( FV(M) = \emptyset \), that is, if it has no free variables.

For example

\[ FV((\lambda x. yx)z) = \{ y, z \}, \quad BV((\lambda x. yx)z) = \{ x \}, \]

and

\[ FV((\lambda xy. yx)zw) = \{ z \}, \quad BV((\lambda xy. yx)zw) = \{ x, y \}. \]

Before proceeding with the notion of substitution we must address an issue with bound variables. The point is that bound variables are really place-holders so they can be renamed freely without changing the reduction behavior of the term as long as they do not clash with free variables. For example, the terms \( \lambda x. (x(\lambda y. yx)) \) and \( \lambda x. (x(\lambda z. xzx)) \) should be considered as equivalent. Similarly, the terms \( \lambda x. (x(\lambda y. yx)) \) and \( \lambda w. (w(\lambda z. wzw)) \) should be considered as equivalent.
One way to deal with this issue is to use the tree representation of $\lambda$-terms given in Definition 6.3. For every leaf labeled with a bound variable $x$, we draw a backpointer to an ancestor of $x$ determined as follows. Given a leaf labeled with a bound variable $x$, climb up to the closest ancestor labeled $\lambda x$, and draw a backpointer to this node. Then all bound variables can be erased. An example is shown in Figure 6.2 for the term $M = \lambda x. x(\lambda y. (x(yx)))$.

A clever implementation of the idea of backpointers is the formalism of de Bruijn indices; see Pierce [20] (Chapter 6) or Barendregt [3] (Appendix C).

Church introduced the notion of $\alpha$-conversion to deal with this issue. First we need to define substitutions.

A substitution $\varphi$ is a finite set of pairs $\varphi = \{(x_1, N_1), \ldots, (x_n, N_n)\}$, where the $x_i$ are distinct variables and the $N_i$ are $\lambda$-terms. We write

$$\varphi = [N_1/x_1, \ldots, N_n/x_n] \quad \text{or} \quad \varphi = [x_1 := N_1, \ldots, x_n := N_n].$$

The second notation indicates more clearly that each term $N_i$ is substituted for the variable $x_i$, and it seems to have been almost universally adopted.

Given a substitution $\varphi = [x_1 := N_1, \ldots, x_n := N_n]$, for any variable $x_i$, we denote by $\varphi_{-x_i}$ the new substitution where the pair $(x_i, N_i)$ is replaced by the pair $(x_i, x_i)$ (that is, the new substitution leaves $x_i$ unchanged).

**Definition 6.5.** Given any $\lambda$-term $M$ and any substitution $\varphi = [x_1 := N_1, \ldots, x_n := N_n]$, we define the $\lambda$-term $M[\varphi]$, the result of applying the substitution $\varphi$ to $M$, as follows:
6.1. SYNTAX OF THE LAMBDA-CALCULUS

(1) If \( M = y \), with \( y \neq x_i \) for \( i = 1, \ldots, n \), then \( M[\varphi] = y = M \).

(2) If \( M = x_i \) for some \( i \in \{1, \ldots, n\} \), then \( M[\varphi] = N_i \).

(3) If \( M = (PQ) \), then \( M[\varphi] = (P[\varphi]Q[\varphi]) \).

(4) If \( M = \lambda x. N \) and \( x \neq x_i \) for \( i = 1, \ldots, n \), then \( M[\varphi] = \lambda x. N[\varphi] \).

(5) If \( M = \lambda x. N \) and \( x = x_i \) for some \( i \in \{1, \ldots, n\} \), then
\[
M[\varphi] = \lambda x. N[\varphi]_{-x_i}.
\]

The term \( M \) is safe for the substitution \( \varphi = [x_1 := N_1, \ldots, x_n := N_n] \) if \( BV(M) \cap (FV(N_1) \cup \cdots \cup FV(N_n)) = \emptyset \), that is, if the free variables in the substitution do not become bound.

Note that Clause (5) ensures that a substitution only substitutes the terms \( N_i \) for the variables \( x_i \) free in \( M \). Thus if \( M \) is a closed term, then for every substitution \( \varphi \), we have \( M[\varphi] = M \).

There is a problem with the present definition of a substitution in Cases (4) and (5), which is that the result of substituting a term \( N_i \) containing the variable \( x \) free causes this variable to become bound after the substitution. We say that \( x \) is captured. We should only apply a substitution \( \varphi \) to a term \( M \) if \( M \) is safe for \( \varphi \). To remedy this problem, Church defined \( \alpha \)-conversion.

**Definition 6.6.** The binary relation \( \longrightarrow_\alpha \) on \( \lambda \)-terms called immediate \( \alpha \)-conversion\(^2\) is the smallest relation satisfying the following properties: for all \( \lambda \)-terms \( M, N, P, Q \):

\[
\lambda x. M \longrightarrow_\alpha \lambda y. M[x := y], \quad \text{for all } y \notin FV(M) \cup BV(M)
\]

if \( M \longrightarrow_\alpha N \) then \( MQ \longrightarrow_\alpha NQ \) and \( PM \longrightarrow_\alpha PN \)

if \( M \longrightarrow_\alpha N \) then \( \lambda x. M \longrightarrow_\alpha \lambda x. N \).

The least equivalence relation \( \equiv_\alpha = (\longrightarrow_\alpha \cup \longrightarrow_\alpha^{-1})^* \) containing \( \longrightarrow_\alpha \) (the reflexive and transitive closure of \( \longrightarrow_\alpha \cup \longrightarrow_\alpha^{-1} \)) is called \( \alpha \)-conversion. Here \( \longrightarrow_\alpha^{-1} \) denotes the converse of the relation \( \longrightarrow_\alpha \), that is, \( M \longrightarrow_\alpha^{-1} N \) iff \( N \longrightarrow_\alpha M \).

For example,

\[
\lambda f. x. f(f(x)) = \lambda f. \lambda x. f(f(x)) \longrightarrow_\alpha \lambda f. \lambda y. f(f(y)) \longrightarrow_\alpha \lambda g. \lambda y. g(g(y)) = \lambda g. \lambda y. g(g(y)).
\]

Now given a \( \lambda \)-term \( M \) and a substitution \( \varphi = [x_1 := N_1, \ldots, x_n := N_n] \), before applying \( \varphi \) to \( M \) we first perform some \( \alpha \)-conversion to obtain a term \( M' \equiv_\alpha M \) whose set of bound variables \( BV(M') \) is disjoint from \( FV(N_1) \cup \cdots \cup FV(N_n) \) so that \( M' \) is safe for \( \varphi \), and the result of the substitution is \( M'[\varphi] \). For example,

\[
(\lambda x y z. (x y) z) (y z) \equiv_\alpha (\lambda x u v. (x u) v) (y z) \longrightarrow_\beta (\lambda u v. (x u) v)[x := y z] = \lambda u v. ((y z) u) v.
\]

\(^2\)We told you that Church was fond of Greek letters.
From now on, we consider two $\lambda$-terms $M$ and $M'$ such that $M \equiv_\alpha M'$ as identical (to be rigorous, we deal with equivalence classes of terms with respect to $\alpha$-conversion). Even the experts are lax about $\alpha$-conversion so we happily go along with them. The convention is that bound variables are always renamed to avoid clashes (with free or bound variables).

Note that the representation of $\lambda$-terms as trees with back-pointers also ensures that substitutions are safe. However, this requires some extra effort. No matter what, it takes some effort to deal properly with bound variables.

6.2 $\beta$-Reduction and $\beta$-Conversion; the Church–Rosser Theorem

The computational engine of the $\lambda$-calculus is $\beta$-reduction.

**Definition 6.7.** The relation $\rightarrow$, called immediate $\beta$-reduction, is the smallest relation satisfying the following properties for all $\lambda$-terms $M, N, P, Q$:

\[(\lambda x. M) N \rightarrow M[x := N], \text{ where } M \text{ is safe for } [x := N]\]

if $M \rightarrow N$ then $M \rightarrow N \rightarrow N$ and $PM \rightarrow PN$

if $M \rightarrow N$ then $\lambda x. M \rightarrow \lambda x. N$.

The transitive closure of $\rightarrow$ is denoted by $\rightarrow_\beta$, the reflexive and transitive closure of $\rightarrow_\beta$ is denoted by $\rightarrow_\beta^*$, and we define $\beta$-conversion, denoted by $\leftarrow_\beta$, as the smallest equivalence relation $\leftarrow_\beta = (\rightarrow_\beta \cup \rightarrow_\beta^{-1})^*$ containing $\rightarrow_\beta$. A subterm of the form $(\lambda x. M) N$ occurring in another term is called a $\beta$-redex. A $\lambda$-term $M$ is a $\beta$-normal form if there is no $\lambda$-term $N$ such that $M \rightarrow_\beta N$, equivalently if $M$ contains no $\beta$-redex.

For example,

\[(\lambda xy. x) uv = ((\lambda x. (\lambda y. x) u) v \rightarrow (\lambda y. x)[x := u]) v = (\lambda y. u) v \rightarrow u[y := v] = u\]

and

\[(\lambda xy. y) uv = ((\lambda x. (\lambda y. y) u) v \rightarrow (\lambda y. y)[x := u]) v = (\lambda y. y) v \rightarrow y[y := v] = v.\]

This shows that $\lambda xy. x$ behaves like the projection onto the first argument and $\lambda xy. y$ behaves like the projection onto the second. More interestingly, if we let $\omega = \lambda x. (xx)$, then

\[\Omega = \omega \omega = (\lambda x. (xx)) (\lambda x. (xx)) \rightarrow (xx)[x := \lambda x. (xx)] = \omega \omega = \Omega.\]

The above example shows that $\beta$-reduction sequences may be infinite. This is a curse and a miracle of the $\lambda$-calculus!
There are even \( \beta \)-reductions where the evolving term grows in size:

\[
(\lambda x. xxx)(\lambda x. xxx) \xrightarrow{+} \beta (\lambda x. xxx)(\lambda x. xxx)(\lambda x. xxx) \xrightarrow{+} \beta (\lambda x. xxx)(\lambda x. xxx)(\lambda x. xxx)(\lambda x. xxx) \xrightarrow{+} \beta \ldots
\]

In general, a \( \lambda \)-term contains many different \( \beta \)-redex. One then might wonder if there is any sort of relationship between any two terms \( M_1 \) and \( M_2 \) arising through two \( \beta \)-reduction sequences \( M \xrightarrow{\ast} \beta M_1 \) and \( M \xrightarrow{\ast} \beta M_2 \) starting with the same term \( M \). The answer is given by the following famous theorem.

**Theorem 6.1. (Church–Rosser Theorem)** The following two properties hold:

1. The \( \lambda \)-calculus is **confluent**: for any three \( \lambda \)-terms \( M, M_1, M_2 \), if \( M \xrightarrow{\ast} \beta M_1 \) and \( M \xrightarrow{\ast} \beta M_2 \), then there is some \( \lambda \)-term \( M_3 \) such that \( M_1 \xrightarrow{\ast} \beta M_3 \) and \( M_2 \xrightarrow{\ast} \beta M_3 \). See Figure 6.3.

\[\text{Given}\]
\[ M \xrightarrow{\ast} M_1 \quad \text{and} \quad M \xrightarrow{\ast} M_2 \]
\[ \Downarrow \]
\[ M \xrightarrow{\ast} M_3 \]

**Figure 6.3: The confluence property**

2. The \( \lambda \)-calculus has the **Church–Rosser property**: for any two \( \lambda \)-terms \( M_1, M_2 \), if \( M_1 \xrightarrow{\ast} \beta M_2 \), then there is some \( \lambda \)-term \( M_3 \) such that \( M_1 \xrightarrow{\ast} \beta M_3 \) and \( M_2 \xrightarrow{\ast} \beta M_3 \). See Figure 6.4.

Furthermore (1) and (2) are equivalent, and if a \( \lambda \)-term \( M \) \( \beta \)-reduces to a \( \beta \)-normal form \( N \), then \( N \) is unique (up to \( \alpha \)-conversion).

**Proof.** I am not aware of any easy proof of Part (1) or Part (2) of Theorem 6.1, but the equivalence of (1) and (2) is easily shown by induction.
Assume that (2) holds. Since $\beta \rightarrow$ is contained in $\leftrightarrow$, if $M \beta \rightarrow M_1$ and $M \beta \rightarrow M_2$, then $M \leftrightarrow \beta M_2$, and since (2) holds, there is some $\lambda$-term $M_3$ such that $M_1 \beta \rightarrow M_3$ and $M_2 \beta \rightarrow M_3$, which is (1).

To prove that (1) implies (2) we need the following observation.

Since $\leftrightarrow \beta = (\rightarrow \beta \cup \leftarrow \beta^{-1})^*$, we see immediately that $M_1 \leftrightarrow \beta M_2$ iff either

(a) $M_1 = M_2$, or

(b) there is some $M_3$ such that $M_1 \rightarrow \beta M_3$ and $M_3 \leftrightarrow \beta M_2$, or

(c) there is some $M_3$ such that $M_3 \rightarrow \beta M_1$ and $M_3 \leftrightarrow \beta M_2$.

Assume (1). We proceed by induction on the number of steps in $M_1 \leftrightarrow \beta M_2$. If $M_1 \leftrightarrow \beta M_2$, as discussed before, there are three cases.

Case a. Base case, $M_1 = M_2$. Then (2) holds with $M_3 = M_1 = M_2$.

Case b. There is some $M_3$ such that $M_1 \rightarrow \beta M_3$ and $M_3 \leftrightarrow \beta M_2$. Since $M_3 \leftrightarrow \beta M_2$ contains one less step than $M_1 \leftrightarrow \beta M_2$, by the induction hypothesis there is some $M_4$ such that $M_3 \beta \rightarrow M_4$ and $M_2 \beta \rightarrow M_4$, and then $M_1 \rightarrow \beta M_3 \beta \rightarrow \beta M_4$ and $M_2 \beta \rightarrow \beta M_4$, proving (2). See Figure 6.5.

Case c. There is some $M_3$ such that $M_3 \rightarrow \beta M_1$ and $M_3 \leftrightarrow \beta M_2$. Since $M_3 \leftrightarrow \beta M_2$ contains one less step than $M_1 \leftrightarrow \beta M_2$, by the induction hypothesis there is some $M_4$ such that $M_3 \beta \rightarrow M_4$ and $M_2 \beta \rightarrow M_4$. Now $M_3 \rightarrow \beta M_1$ and $M_3 \beta \rightarrow M_4$, so by (1) there is some $M_5$ such that $M_1 \beta \rightarrow M_5$ and $M_4 \beta \rightarrow M_5$. Putting derivations together we get $M_1 \beta \rightarrow M_5$ and $M_2 \beta \rightarrow M_4 \beta \rightarrow \beta M_5$, which proves (2). See Figure 6.6.
6.2. β-REDUCTION AND β-CONVERSION; THE CHURCH–ROSSER THEOREM 253

Suppose \( M \rightarrow^\beta N_1 \) and \( M \rightarrow^\beta N_2 \) where \( N_1 \) and \( N_2 \) are both \( \beta \)-normal forms. Then by confluence there is some \( N \) such that \( N_1 \rightarrow^\beta N \) and \( N_2 \rightarrow^\beta N \). Since \( N_1 \) and \( N_2 \) are both \( \beta \)-normal forms, we must have \( N_1 = N = N_2 \) (up to \( \alpha \)-conversion).

Barendregt gives an elegant proof of the confluence property in [3] (Chapter 11).

Another immediate corollary of the Church–Rosser theorem is that if \( M \leftrightarrow^\beta N \) and if \( N \) is a \( \beta \)-normal form, then in fact \( M \rightarrow^\beta N \). We leave this fact as an exercise.

This fact will be useful in showing that the recursive functions are computable in the \( \lambda \)-calculus.
6.3 Some Useful Combinators

In this section we provide some evidence for the expressive power of the \( \lambda \)-calculus.

First we make a remark about the representation of functions of several variables in the \( \lambda \)-calculus. The \( \lambda \)-calculus makes the implicit assumption that a function has a single argument. This is the idea behind application: given a term \( M \) viewed as a function and an argument \( N \), the term \( (MN) \) represents the result of applying \( M \) to the argument \( N \), except that the actual evaluation is suspended. Evaluation is performed by \( \beta \)-conversion. To deal with functions of several arguments we use a method known as Currying (after Haskell Curry). In this method, a function of \( n \) arguments is viewed as a function of one argument taking a function of \( n-1 \) arguments as argument. Consider the case of two arguments, the general case being similar. Consider a function \( f : \mathbb{N} \times \mathbb{N} \to \mathbb{N} \). For any fixed \( x \), we define the function \( F_x : \mathbb{N} \to \mathbb{N} \) given by

\[
F_x(y) = f(x, y) \quad y \in \mathbb{N}.
\]

Using the \( \lambda \)-notation we can write

\[
F_x = \lambda y. f(x, y),
\]

and then the function \( x \mapsto F_x \), which is a function from \( \mathbb{N} \) to the set of functions \([\mathbb{N} \to \mathbb{N}]\) (also denoted \( \mathbb{N}^\mathbb{N} \)), is denoted by the \( \lambda \)-term

\[
F = \lambda x. F_x = \lambda x. (\lambda y. f(x, y)).
\]

And indeed,

\[
(FM)N \xrightarrow{+\beta} F_M N \xrightarrow{+\beta} f(M, N).
\]

Remark: Currying is a way to realizing the isomorphism between the sets of functions \([\mathbb{N} \times \mathbb{N} \to \mathbb{N}]\) and \([\mathbb{N} \to ([\mathbb{N} \to \mathbb{N}])]\) (or in the standard set-theoretic notation, between \( \mathbb{N}^{\mathbb{N} \times \mathbb{N}} \) and \( (\mathbb{N}^\mathbb{N})^\mathbb{N} \)). Does this remind you of the identity

\[
(m^n)^p = m^{n*p}?
\]

It should.

The function space \([\mathbb{N} \to \mathbb{N}]\) is called an exponential. There is a very abstract way to view all this which is to say that we have an instance of a Cartesian closed category (CCC).

**Proposition 6.2.** If \( I, K, K_* \), and \( S \) are the combinators defined by

\[
I = \lambda x. x
\]

\[
K = \lambda xy. x
\]

\[
K_* = \lambda xy. y
\]

\[
S = \lambda xyz. (xz)(yz),
\]

then

\[
I, K, K_* \text{ are dual to } S.
\]
then for all \( \lambda \)-terms \( M, N, P \), we have

\[
\begin{align*}
IM & \xrightarrow{\beta} M \\
KMN & \xrightarrow{\beta} MN \\
K_MN & \xrightarrow{\beta} M \\
SMNP & \xrightarrow{\beta} (MP)(NP) \\
KI & \xrightarrow{\beta} K \\
SKK & \xrightarrow{\beta} I.
\end{align*}
\]

The proof is left as an easy exercise. For example,

\[
SMNP = (\lambda xyz. (xz)(yz))MNP \xrightarrow{\beta} ((\lambda yz. (xz)(yz))[x := M])(NP) = (\lambda yz. (Mz)(yz))NP
\]

\[
\xrightarrow{\beta} ((\lambda z. (Mz)(yz))[y := N])P = (\lambda z. (Mz)(Nz))P
\]

\[
\xrightarrow{\beta} ((Mz)(Nz))[z := P] = (MP)(NP).
\]

The need for a conditional construct if \texttt{then} else such that if \texttt{T} then \( P \) else \( Q \) yields \( P \) and if \texttt{F} then \( P \) else \( Q \) yields \( Q \) is indispensable to write nontrivial programs. There is a trick to encode the boolean values \texttt{T} and \texttt{F} in the \( \lambda \)-calculus to mimick the above behavior of if \texttt{B} then \( P \) else \( Q \), provided that \( B \) is a truth value. Since everything in the \( \lambda \)-calculus is a function, the booleans values \( \texttt{T} \) and \( \texttt{F} \) are encoded as \( \lambda \)-terms. At first, this seems quite odd, but what counts is the behavior of if \texttt{B} then \( P \) else \( Q \), and it works!

The truth values \( \texttt{T}, \texttt{F} \) and the conditional construct if \texttt{B} then \( P \) else \( Q \) can be encoded in the \( \lambda \)-calculus as follows.

**Proposition 6.3.** Consider the combinators given by \( \texttt{T} = K, \texttt{F} = K_*, \) and

\[
\text{if then else} = \lambda bxy. bxy.
\]

Then for all \( \lambda \)-terms we have

\[
\begin{align*}
\text{if T then P else Q} & \xrightarrow{\beta} P \\
\text{if F then P else Q} & \xrightarrow{\beta} Q.
\end{align*}
\]

The proof is left as an easy exercise. For example,

\[
\begin{align*}
\text{if T then P else Q} &= (\text{if then else})TPQ \\
&= (\lambda bxy. bxy)TPQ \\
&\xrightarrow{\beta} ((\lambda xy. bxy)[b := \texttt{T}])PQ = (\lambda xy. Txy)PQ \\
&\xrightarrow{\beta} ((\lambda y. Txy)[x := P])Q = (\lambda y. TPy)Q \\
&\xrightarrow{\beta} (TPy)[y := Q] = TPQ \\
&= KPQ \xrightarrow{\beta} P,
\end{align*}
\]
by Proposition 6.2.

The boolean operations \( \land, \lor, \neg \) can be defined in terms of if \( \text{then} \) \( \text{else} \). For example,

\[
\text{And } b_1 b_2 = \text{if } b_1 \text{ then } (\text{if } b_2 \text{ then } \text{T} \text{ else } \text{F} ) \text{ else } \text{F}.
\]

Remark: If \( B \) is a term different from \( \text{T} \) or \( \text{F} \), then if \( B \) \( \text{then} \) \( P \) \( \text{else} \) \( Q \) may not reduce at all, or reduce to something different from \( P \) or \( Q \). The problem is that the conditional statement that we designed only works properly if the input \( B \) is of the correct type, namely a boolean. If we give garbage as input, then we can’t expect a correct result. The \( \lambda \)-calculus being type-free, it is unable to check for the validity of the input. In this sense this is a defect, but it also accounts for its power.

The ability to construct ordered pairs is also crucial.

**Proposition 6.4.** For any two \( \lambda \)-terms \( M \) and \( N \) consider the combinator \( \langle M, N \rangle \) and the combinator \( \pi_1 \) and \( \pi_2 \) given by

\[
\langle M, N \rangle = \lambda z. zMN = \lambda z. \text{if } z \text{ then } M \text{ else } N
\]

\[
\pi_1 = \lambda z. zK \\
\pi_2 = \lambda z. zK_\ast.
\]

Then

\[
\pi_1(M, N) \xrightarrow{+}_{\beta} M \\
\pi_2(M, N) \xrightarrow{+}_{\beta} N \\
\langle M, N \rangle \text{T} \xrightarrow{+}_{\beta} M \\
\langle M, N \rangle \text{F} \xrightarrow{+}_{\beta} N.
\]

The proof is left as an easy exercise. For example,

\[
\pi_1(M, N) = (\lambda z. zK)(\lambda z. zMN) \\
\xrightarrow{\beta} (zK)[z := \lambda z. zMN] = (\lambda z. zMN)K \\
\xrightarrow{\beta} (zMN)[z := K] = KMN \xrightarrow{+}_{\beta} M,
\]

by Proposition 6.2.

In the next section we show how to encode the natural numbers in the \( \lambda \)-calculus and how to compute various arithmetical functions.

### 6.4 Representing the Natural Numbers

Historically the natural numbers were first represented in the \( \lambda \)-calculus by Church in the 1930’s. Later in 1976 Barendregt came up with another representation which is more convenient to show that the recursive functions are \( \lambda \)-definable. We start with Church’s representation.
First, given any two λ-terms \( F \) and \( M \), for any natural number \( n \in \mathbb{N} \), we define \( F^n(M) \) inductively as follows:

\[
F^0(M) = M \\
F^{n+1}(M) = F(F^n(M)).
\]

**Definition 6.8.** (Church Numerals) The *Church numerals* \( c_0, c_1, c_2, \ldots \) are defined by

\[
c_n = \lambda fx. f^n(x).
\]

So \( c_0 = \lambda fx. x = K \), \( c_1 = \lambda fx. fx \), \( c_2 = \lambda fx. f(fx) \), etc. The Church numerals are \( \beta \)-normal forms.

Observe that

\[
c_n F z = (\lambda fx. f^n(x)) F z \xrightarrow{\beta} F^n(z). \tag{†}
\]

This shows that \( c_n \) *iterates* \( n \) times the function represented by the term \( F \) on initial input \( z \). This is the trick behind the definition of the Church numerals. This suggests the following definition.

**Definition 6.9.** The *iteration combinator* \( \text{Iter} \) is given by

\[
\text{Iter} = \lambda nfx. nf x.
\]

Observe that

\[
\text{Iter} c_n F X \xrightarrow{\beta} F^n(X),
\]

that is, the result of iterating \( F \) for \( n \) steps starting with the initial term \( X \).

Let us show how some basic functions on the natural numbers can be defined. We begin with the constant function \( Z \) given by \( Z(n) = 0 \) for all \( n \in \mathbb{N} \). We claim that \( Z_c = \lambda x. c_0 \) works. Indeed, we have

\[
Z_c c_n = (\lambda x. c_0) c_n \xrightarrow{\beta} c_0[x := c_n] = c_0
\]

since \( c_0 \) is a closed term.

The successor function \( \text{Succ} \) is given by

\[
\text{Succ}(n) = n + 1.
\]

We claim that

\[
\text{Succ}_c = \lambda nx. f(nfx)
\]

computes \( \text{Succ} \). Indeed we have

\[
\begin{align*}
\text{Succ}_c c_n & = (\lambda nx. f(nfx)) c_n \\
& \xrightarrow{\beta} (\lambda nx. f(nfx))[n := c_n] = \lambda fx. f(c_n f x) \\
& \xrightarrow{\beta} \lambda fx. f(f^n(x)) \\
& = \lambda fx. f^{n+1}(x) = c_{n+1}.
\end{align*}
\]
The function IsZero which tests whether a natural number is equal to 0 is defined by the combinator

\[ \text{IsZero}_c = \lambda x. (x \mathcal{K} \mathcal{F}) \mathcal{T}. \]

The proof that it works is left as an exercise.

Addition and multiplication are a little more tricky to define.

**Proposition 6.5. (J.B. Rosser)** Define Add and Mult as the combinators given by

\[
\begin{align*}
\text{Add} &= \lambda m n f x. m f (n f x) \\
\text{Mult} &= \lambda x y z. x (y z).
\end{align*}
\]

We have

\[
\begin{align*}
\text{Add}_c m c_n & \rightarrow^\beta c_{m+n} \\
\text{Mult}_c m c_n & \rightarrow^\beta c_{m \ast n}
\end{align*}
\]

for all \( m, n \in \mathbb{N} \).

**Proof.** We have

\[
\begin{align*}
\text{Add}_c m c_n &= (\lambda m n f x. m f (n f x)) c_m c_n \\
& \rightarrow^\beta (\lambda f x. c_m f (c_n f x)) \\
& \rightarrow^\beta \lambda f x. f^m (f^n (x)) \\
& = \lambda f x. f^{m+n} (x) = c_{m+n}.
\end{align*}
\]

For multiplication we need to prove by induction on \( m \) that

\[
(c_n x)^m (y) \rightarrow^{*} \beta x^{m \ast n} (y). \tag{*}
\]

If \( m = 0 \) then both sides are equal to \( y \).

For the induction step we have

\[
\begin{align*}
(c_n x)^{m+1} (y) &= c_n x ((c_n x)^m (y)) \\
& \rightarrow^{*} \beta c_n x (x^{m \ast n} (y)) \\
& \rightarrow^{*} \beta x^n (x^{m \ast n} (y)) \\
& = x^{n+m \ast n} (y) = x^{(m+1) \ast n} (y).
\end{align*}
\]

We now have

\[
\begin{align*}
\text{Mult}_c m c_n &= (\lambda x y z. x (y z)) c_m c_n \\
& \rightarrow^\beta \lambda z. (c_m (c_n z)) \\
& = \lambda z. ((\lambda f y. f^m (y)) (c_n z)) \\
& \rightarrow^\beta \lambda z y. (c_n z)^m (y),
\end{align*}
\]
and since we proved in (*) that
\[(c_n z)^m(y) \leftrightarrow^\beta z^{m\cdot n}(y),\]
we get
\[
\text{Mult } c_m c_n \rightarrow^\beta \lambda z y. (c_n z)^m(y) \rightarrow^\beta \lambda z y. z^{m\cdot n}(y) = c_m^n,
\]
which completes the proof.

As an exercise the reader should prove that addition and multiplication can also be defined in terms of \text{Iter} (see Definition 6.9) by
\[
\begin{align*}
\text{Add} & = \lambda m n. \text{Iter } m \text{ Succ}_c n \\
\text{Mult} & = \lambda m n. \text{ Iter } m (\text{ Add } n) c_0.
\end{align*}
\]
The above expressions are close matches to the primitive recursive definitions of addition and multiplication. To check that they work, prove that
\[
\begin{align*}
\text{Add } c_m c_n & \rightarrow^\beta (\text{Succ}_c)^m(c_n) \rightarrow^\beta c_{m+n} \\
\text{Mult } c_m c_n & \rightarrow^\beta (\text{Add } n)^m(c_0) \rightarrow^\beta c_{m^n}.
\end{align*}
\]
A version of the exponential function can also be defined. A function that plays an important technical role is the predecessor function \text{Pred} defined such that
\[
\begin{align*}
\text{Pred}(0) & = 0 \\
\text{Pred}(n + 1) & = n.
\end{align*}
\]
It turns out that it is quite tricky to define this function in terms of the Church numerals. Church and his students struggled for a while until Kleene found a solution in his famous 1936 paper. The story goes that Kleene found his solution when he was sitting in the dentist’s chair! The trick is to make use of pairs. Kleene’s solution is
\[
\text{Pred}_K = \lambda n. \pi_2(\text{Iter } n \lambda z. \langle \text{Succ}_c(\pi_1 z), \pi_1 z \rangle \langle c_0, c_0 \rangle).
\]
The reason this works is that we can prove that
\[
(\lambda z. \langle \text{Succ}_c(\pi_1 z), \pi_1 z \rangle)^0 \langle c_0, c_0 \rangle \rightarrow^\beta \langle c_0, c_0 \rangle,
\]
and by induction that
\[
(\lambda z. \langle \text{Succ}_c(\pi_1 z), \pi_1 z \rangle)^n \langle c_0, c_0 \rangle \rightarrow^\beta \langle c_n, c_n \rangle.
\]
For the base case \(n = 0\) we get
\[
(\lambda z. \langle \text{Succ}_c(\pi_1 z), \pi_1 z \rangle) \langle c_0, c_0 \rangle \rightarrow^\beta \langle c_1, c_0 \rangle.
\]
For the induction step we have
\[(\lambda z. (\textbf{Succ}_c(\pi_1 z), \pi_1 z))^{n+2} (c_0, c_0) =
(\lambda z. (\textbf{Succ}_c(\pi_1 z), \pi_1 z))((\lambda z. (\textbf{Succ}_c(\pi_1 z), \pi_1 z))^{n+1} (c_0, c_0))
\]
\[\xrightarrow{+\beta} (\lambda z. (\textbf{Succ}_c(\pi_1 z), \pi_1 z))(c_{n+1}, c_n) \xrightarrow{+\beta} (c_{n+2}, c_{n+1}) .\]

Here is another tricky solution due to J. Velmans (according to H. Barendregt):
\[
\textbf{Pred}_c = \lambda xyz.x(\lambda pq.q(py))(\textbf{K}_z)\textbf{I}.
\]
We leave it to the reader to verify that it works.

The ability to construct pairs together with the \textbf{Iter} combinator allows the definition of a large class of functions, because \textbf{Iter} is “type-free” in its second and third arguments so it really allows higher-order primitive recursion.

For example, the factorial function defined such that
\[0! = 1\]
\[(n + 1)! = (n + 1)n!\]
can be defined. First we define \(h\) by
\[h = \lambda xn. \text{Mult} \textbf{Succ}_c n x\]
and then
\[
\textbf{fact} = \lambda n. \pi_1 (\textbf{Iter} n \lambda z. (h(\pi_1 z) (\pi_2 z), \textbf{Succ}_c(\pi_2 z)) (c_1, c_0)).
\]
The above term works because
\[\text{\textbf{Succ}_c(\pi_2 z)}\] is a function, and
\[
(\lambda z. (h(\pi_1 z) (\pi_2 z), \textbf{Succ}_c(\pi_2 z)))^0 (c_1, c_0) \xrightarrow{+\beta} (c_1, c_0) = (c_0!, c_0),
\]
and
\[
(\lambda z. (h(\pi_1 z) (\pi_2 z), \textbf{Succ}_c(\pi_2 z)))^{n+1} (c_1, c_0) \xrightarrow{+\beta} (c_{(n+1)!}, c_{n+1}) = (c_{(n+1)!}, c_{n+1}).
\]
We leave the details as an exercise.

Barendregt came up with another way of representing the natural numbers that makes things easier.

\textbf{Definition 6.10.} (Barendregt Numerals) The Barendregt numerals \(b_n\) are defined as follows:
\[
b_0 = I = \lambda x. x
\]
\[
b_{n+1} = \langle F, b_n \rangle.
\]
The Barendregt numerals are \(\beta\)-normal forms. Barendregt uses the notation \(\mathfrak{n} n \mathfrak{m}\) instead of \(b_n\) but this notation is also used for the Church numerals by other authors so we prefer using \(b_n\) (which is consistent with the use of \(c_n\) for the Church numerals). The Barendregt numerals are tuples, which makes operating on them simpler than the Church numerals which encode \(n\) as the composition \(f^n\).
Proposition 6.6. The functions \textbf{Succ}, \textbf{Pred} and \textbf{IsZero} are defined in terms of the Barendregt numerals by the combinators

\begin{align*}
\text{Succ}_b &= \lambda x. \langle F, x \rangle \\
\text{Pred}_b &= \lambda x. \langle x F \rangle \\
\text{IsZero}_b &= \lambda x. \langle x T \rangle ,
\end{align*}

and we have

\begin{align*}
\text{Succ}_b b_n &\rightarrow^\beta b_{n+1} \\
\text{Pred}_b b_0 &\rightarrow^\beta b_0 \\
\text{Pred}_b b_{n+1} &\rightarrow^\beta b_n \\
\text{IsZero}_b b_0 &\rightarrow^\beta T \\
\text{IsZero}_b b_{n+1} &\rightarrow^\beta F.
\end{align*}

The proof is left as an exercise.

Since there is an obvious bijection between the Church combinators and the Barendregt combinators there should be combinators effecting the translations. Indeed we have the following result.

Proposition 6.7. The combinator \textbf{T} given by

\[ T = \lambda x. \langle x \text{Succ}_b \rangle b_0 \]

has the property that

\[ T c_n \rightarrow^\beta b_n \quad \text{for all } n \in \mathbb{N}. \]

Proof. We proceed by induction on \( n \). For the base case

\[ T c_0 = (\lambda x. \langle x \text{Succ}_b \rangle b_0)c_0 \]

\[ \rightarrow^\beta c_0(\text{Succ}_b)b_0 \]

\[ \rightarrow^\beta b_0. \]

For the induction step,

\[ T c_n = (\lambda x. \langle x \text{Succ}_b \rangle b_0)c_n \]

\[ \rightarrow^\beta (c_n \text{Succ}_b)b_0 \]

\[ \rightarrow^\beta \text{Succ}_b^n(b_0). \]

Thus we need to prove that

\[ \text{Succ}_b^n(b_0) \rightarrow^\beta b_n. \quad (\ast) \]
For the base case $n = 0$, the left-hand side reduces to $b_0$. For the induction step, we have
\[
\text{Succ}_b^{n+1}(b_0) = \text{Succ}_b(\text{Succ}_b^n(b_0))
\]
\[
= \xrightarrow{\beta} \text{Succ}_b(b_n) \quad \text{by induction}
\]
\[
= \xrightarrow{\beta} b_{n+1},
\]
which concludes the proof. \qed

There is also a combinator defining the inverse map but it is defined recursively and we don’t know how to express recursive definitions in the $\lambda$-calculus. This is achieved by using fixed-point combinators.

### 6.5 Fixed-Point Combinators and Recursively Defined Functions

Fixed-point combinators are the key to the definability of recursive functions in the $\lambda$-calculus. We begin with the $Y$-combinator due to Curry.

**Proposition 6.8.** (Curry $Y$-combinator) If we define the combinator $Y$ as
\[
Y = \lambda f. (\lambda x. f(xx))(\lambda x. f(xx)),
\]
then for any $\lambda$-term $F$ we have
\[
F(YF) \xleftarrow{\beta} YF.
\]

**Proof.** Write $W = \lambda x. F(xx)$. We have
\[
F(YF) = F((\lambda f. (\lambda x. f(xx))(\lambda x. f(xx)))F) \xrightarrow{\beta} F((\lambda x. F(xx))(\lambda x. F(xx))) = F(WW),
\]
and
\[
YF = (\lambda f. (\lambda x. f(xx))(\lambda x. f(xx)))F \xrightarrow{\beta} (\lambda x. F(xx))(\lambda x. F(xx)) = (\lambda x. F(xx))W \xrightarrow{\beta} F(WW).
\]
Therefore $F(YF) \xleftarrow{\beta} YF$, as claimed. \qed

Observe that neither $F(YF) \xrightarrow{\beta} YF$ nor $YF \xrightarrow{\beta} F(YF)$. This is a slight disadvantage of the Curry $Y$-combinator. Turing came up with another fixed-point combinator that does not have this problem.
Proposition 6.9. (Turing $\Theta$-combinator) If we define the combinator $\Theta$ as

$$\Theta = (\lambda xy. y(xxy))(\lambda xy. y(xxy)),$$

then for any $\lambda$-term $F$ we have

$$\Theta F \xrightarrow{\beta} F(\Theta F).$$

Proof. If we write $A = (\lambda xy. y(xxy))$, then $\Theta = AA$. We have

$$\Theta F = (AA)F = ((\lambda xy. y(xxy))A)F \xrightarrow{\beta} (\lambda y. y(AAy))F \xrightarrow{\beta} F(AAF) = F(\Theta F),$$

as claimed. $\square$

Now we show how to use the fixed-point combinators to represent recursively-defined functions in the $\lambda$-calculus. For example, there is a combinator $G$ such that

$$GX \xrightarrow{\beta} X(XG) \text{ for all } X.$$

Informally the idea is to consider the “functional” $F = \lambda gx. x(xg)$, and to find a fixed-point of this functional. Pick

$$G = \Theta \lambda gx. x(xg) = \Theta F.$$

Since by Proposition 6.9 we have $G = \Theta F \xrightarrow{\beta} F(\Theta F) = FG$, and we also have

$$FG = (\lambda gx. x(xg))G \xrightarrow{\beta} \lambda x. x(xG),$$

so $G \xrightarrow{\beta} \lambda x. x(xG)$, which implies

$$GX \xrightarrow{\beta} (\lambda x. x(xG))X \xrightarrow{\beta} X(XG).$$

In general, if we want to define a function $G$ recursively such that

$$GX \xrightarrow{\beta} M(X, G)$$

where $M(X, G)$ is $\lambda$-term containing recursive occurrences of $G$, we let $F = \lambda gx. M(x, g)$ and

$$G = \Theta F.$$

Then we have

$$G \xrightarrow{\beta} FG = (\lambda gx. M(x, g))G \xrightarrow{\beta} \lambda x. M(x, g)[g := G] = \lambda x. M(x, G),$$

so

$$GX \xrightarrow{\beta} (\lambda x. M(x, G))X \xrightarrow{\beta} M(x, G)[x := X] = M(X, G),$$
as desired.

As another example, here is how the factorial function can be defined (using the Church numerals). Let

$$ F = \lambda g . n \text{ if } \text{IsZero}_c \ n \ \text{then } c_1 \ \text{else } \text{Mult}_c \ n \ g(\text{Pred}_c \ n). $$

Then the term $G = \Theta F$ defines factorial function. The verification of the above fact is left as an exercise.

As usual with recursive definitions there is no guarantee that the function that we obtain terminates for all input. For example, if we consider

$$ F = \lambda g . n \text{ if } \text{IsZero}_c \ n \ \text{then } c_1 \ \text{else } \text{Mult}_c \ n \ g(\text{Succ}_c \ n) $$

then for $n \geq 1$ the reduction behavior is

$$ Gc_n \xrightarrow{\beta} \text{Mult}_c \ n \ Gc_{n+1}, $$

which does not terminate.

We leave it as an exercise to show that the inverse of the function $T$ mapping the Church numerals to the Barendregt numerals is given by the combinator

$$ T^{-1} = \Theta(\lambda f . x \text{ if } \text{IsZero}_b \ x \ \text{then } c_0 \ \text{else } \text{Succ}_c(f(\text{Pred}_b \ x))). $$

It is remarkable that the $\lambda$-calculus allows the implementation of arbitrary recursion without a stack, just using $\lambda$-terms are the data-structure and $\beta$-reduction. This does not mean that this evaluation mechanism is efficient but this is another story (as well as evaluation strategies, which have to do with parameter-passing strategies, call-by-name, call-by-value).

Now we have all the ingredients to show that all the (total) computable functions are definable in the $\lambda$-calculus.

### 6.6 $\lambda$-Definability of the Computable Functions

Let us begin by reviewing the definition of the computable functions (recursive functions) (à la Herbrand–Gödel–Kleene). For our purposes it suffices to consider functions (partial or total) $f : \mathbb{N}^n \rightarrow \mathbb{N}$ as opposed to the more general case of functions $f : (\Sigma^*)^n \rightarrow \Sigma^*$ defined on strings.

**Definition 6.11.** The **base functions** are the functions $Z, S, P^n_1$ defined as follows:

1. The constant **zero function** $Z$ such that
   
   $$ Z(n) = 0, \quad \text{for all } n \in \mathbb{N}. $$

2. The **successor function** $S$ such that
   
   $$ S(n) = n + 1, \quad \text{for all } n \in \mathbb{N}. $$
(3) For every \( n \geq 1 \) and every \( i \) with \( 1 \leq i \leq n \), the projection function \( P^m_i \) such that
\[
P^m_i(x_1, \ldots, x_n) = x_i, \quad x_1, \ldots, x_n \in \mathbb{N}.
\]

Next comes (extended) composition.

**Definition 6.12.** Given any partial or total function \( g: \mathbb{N}^m \rightarrow \mathbb{N} \) \( (m \geq 1) \) and any \( m \) partial or total functions \( h_i: \mathbb{N}^n \rightarrow \mathbb{N} \) \( (n \geq 1) \), the composition of \( g \) and \( h_1, \ldots, h_m \), denoted \( g \circ (h_1, \ldots, h_m) \), is the partial or total function function \( f: \mathbb{N}^n \rightarrow \mathbb{N} \) given by
\[
f(x_1, \ldots, x_n) = g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)), \quad x_1, \ldots, x_n \in \mathbb{N}.
\]

If \( g \) or any of the \( h_i \) are partial functions, then \( f(x_1, \ldots, x_n) \) is defined if and only if all \( h_i(x_1, \ldots, x_n) \) are defined and \( g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)) \) is defined.

Note that even if \( g \) “ignores” one of its arguments, say the \( i \)th one, \( g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n)) \) is undefined if \( h_i(x_1, \ldots, x_n) \) is undefined.

**Definition 6.13.** Given any partial or total functions \( g: \mathbb{N}^m \rightarrow \mathbb{N} \) and \( h: \mathbb{N}^{m+2} \rightarrow \mathbb{N} \) \( (m \geq 1) \), the partial or total function function \( f: \mathbb{N}^{m+1} \rightarrow \mathbb{N} \) is defined by primitive recursion from \( g \) and \( h \) if \( f \) is given by:
\[
\begin{align*}
f(0, x_1, \ldots, x_m) &= g(x_1, \ldots, x_m) \\
f(n + 1, x_1, \ldots, x_m) &= h(f(n, x_1, \ldots, x_m), n, x_1, \ldots, x_m)
\end{align*}
\]
for all \( n, x_1, \ldots, x_m \in \mathbb{N} \). If \( m = 0 \), then \( g \) is some fixed natural number and we have
\[
\begin{align*}
f(0) &= g \\
f(n + 1) &= h(f(n), n).
\end{align*}
\]

It can be shown that if \( g \) and \( h \) are total functions, then so if \( f \).

Note that the second clause of the definition of primitive recursion is
\[
f(n + 1, x_1, \ldots, x_m) = h(f(n, x_1, \ldots, x_m), n, x_1, \ldots, x_m) \quad \text{(1)}
\]
but in an earlier definition it was
\[
f(n + 1, x_1, \ldots, x_m) = h(n, f(n, x_1, \ldots, x_m), x_1, \ldots, x_m), \quad \text{(2)}
\]
with the first two arguments of \( h \) permuted. Since
\[
h \circ (P^m_{m+2}, P^m_{m+2}, P^m_{m+2}, \ldots, P^m_{m+2})(n, f(n, x_1, \ldots, x_m), x_1, \ldots, x_m)
\]
\[
= h(f(n, x_1, \ldots, x_m), n, x_1, \ldots, x_m)
\]
and
\[
    h \circ (P^{m+2}, P^{m+2}, P^{m+2}, \ldots, P^{m+2})(f(n, x_1, \ldots, x_m), n, x_1, \ldots, x_m)
    = h(n, f(n, x_1, \ldots, x_m), x_1, \ldots, x_m),
\]
the two definitions are equivalent. In this section we chose version \((\ast_1)\) because it matches
the treatment in Barendregt [3] and will make it easier for the reader to follow Barendregt
[3] if they wish.

The last operation is minimization (sometimes called minimalization).

**Definition 6.14.** Given any partial or total function \(g : \mathbb{N}^{m+1} \to \mathbb{N} (m \geq 0)\), the partial or
total function function \(f : \mathbb{N}^m \to \mathbb{N}\) is defined as follows: for all \(x_1, \ldots, x_m \in \mathbb{N}\),
\[
f(x_1, \ldots, x_m) = \text{the least } n \in \mathbb{N} \text{ such that } g(n, x_1, \ldots, x_m) = 0,
\]
and undefined if there is no \(n\) such that \(g(n, x_1, \ldots, x_m) = 0\). We say that \(f\) is defined by
minimization from \(g\), and we write
\[
f(x_1, \ldots, x_m) = \mu x[g(x, x_1, \ldots, x_m) = 0].
\]
For short, we write \(f = \mu g\).

Even if \(g\) is a total function, \(f\) may be undefined for some (or all) of its inputs.

**Definition 6.15.** (Herbrand–Gödel–Kleene) The set of partial computable (or partial recur-
sive) functions is the smallest set of partial functions (defined on \(\mathbb{N}^n\) for some \(n \geq 1\)) which
contains the base functions and is closed under

1. Composition.
2. Primitive recursion.

The set of computable (or recursive) functions is the subset of partial computable functions
that are total functions (that is, defined for all input).

We proved earlier the Kleene normal form, which says that every partial computable
function \(f : \mathbb{N}^m \to \mathbb{N}\) is computable as
\[
f = g \circ \mu h,
\]
for some primitive recursive functions \(g : \mathbb{N} \to \mathbb{N}\) and \(h : \mathbb{N}^{m+1} \to \mathbb{N}\). The significance of this
result is that \(f\) is built up from total functions using composition and primitive recursion,
and only a single minimization is needed at the end.

Before stating our main theorem, we need to define what it means for a (numerical)
function in the \(\lambda\)-calculus. This requires some care to handle partial functions.

Since there are combinators for translating Church numerals to Barendregt numerals and
vice-versa, it does not matter which numerals we pick. We pick the Church numerals because
primitive recursion is definable without using a fixed-point combinator.
Definition 6.16. A function (partial or total) \( f : \mathbb{N}^n \to \mathbb{N} \) is \( \lambda \)-definable if for all \( m_1, \ldots, m_n \in \mathbb{N} \), there is a combinator (a closed \( \lambda \)-term) \( F \) with the following properties:

1. The value \( f(m_1, \ldots, m_n) \) is defined if and only if \( Fc_{m_1} \cdots c_{m_n} \) reduces to a \( \beta \)-normal form (necessarily unique by the Church–Rosser theorem).

2. If \( f(m_1, \ldots, m_n) \) is defined, then

\[
Fc_{m_1} \cdots c_{m_n} \leftrightarrow_\beta c_{f(m_1, \ldots, m_n)}
\]

In view of the Church–Rosser theorem (Theorem 6.1) and the fact that \( c_{f(m_1, \ldots, m_n)} \) is a \( \beta \)-normal form, we can replace

\[
Fc_{m_1} \cdots c_{m_n} \leftrightarrow_\beta c_{f(m_1, \ldots, m_n)}
\]

by

\[
Fc_{m_1} \cdots c_{m_n} \Rightarrow_\beta c_{f(m_1, \ldots, m_n)}
\]

Note that the termination behavior of \( f \) on inputs \( m_1, \ldots, m_n \) has to match the reduction behavior of \( Fc_{m_1} \cdots c_{m_n} \), namely \( f(m_1, \ldots, m_n) \) is undefined if no reduction sequence from \( Fc_{m_1} \cdots c_{m_n} \) reaches a \( \beta \)-normal form. Condition (2) ensures that if \( f(m_1, \ldots, m_n) \) is defined, then the correct value \( c_{f(m_1, \ldots, m_n)} \) is computed by some reduction sequence from \( Fc_{m_1} \cdots c_{m_n} \).

If we only care about total functions then we require that \( Fc_{m_1} \cdots c_{m_n} \) reduces to a \( \beta \)-normal form for all \( m_1, \ldots, m_n \) and (2). A stronger and more elegant version of \( \lambda \)-definability that better captures when a function is undefined for some input is considered in Section 6.7.

We have the following remarkable theorems.

Theorem 6.10. If a total function \( f : \mathbb{N}^n \to \mathbb{N} \) is \( \lambda \)-definable, then it is (total) computable. If a partial function \( f : \mathbb{N}^n \to \mathbb{N} \) is \( \lambda \)-definable, then it is partial computable.

Although Theorem 6.10 is intuitively obvious since computation by \( \beta \)-reduction sequences are “clearly” computable, a detailed proof is long and very tedious. One has to define primitive recursive functions to mimic \( \beta \)-conversion, etc. Most books sweep this issue under the rug. Barendregt observes that the “\( \lambda \)-calculus is recursively axiomatized,” which implies that the graph of the function being defined is recursively enumerable, but no details are provided; see Barendregt [3] (Chapter 6, Theorem 6.3.13). Kleene (1936) provides a detailed and very tedious proof. This is an amazing paper, but very hard to read. If the reader is not content she/he should work out the details over many long lonely evenings.

Theorem 6.11. (Kleene, 1936) If a (total) function \( f : \mathbb{N}^n \to \mathbb{N} \) is computable, then it is \( \lambda \)-definable. If a (partial) function \( f : \mathbb{N}^n \to \mathbb{N} \) is partial computable, then it is \( \lambda \)-definable.

Proof. First we assume all functions to be total. There are several steps.

1. **Step 1.** The base functions are \( \lambda \)-definable.
CHAPTER 6. THE LAMBDA-CALCULUS

We already showed that $Z_c$ computes $Z$ and that $Succ_c$ computes $S$. Observe that $U^n_i$ given by

$$U^n_i = \lambda x_1 \cdots x_n. x_i$$

computes $P^n_i$.

**Step 2.** Closure under composition.

If $g$ is $\lambda$-defined by the combinator $G$ and $h_1, \ldots, h_m$ are $\lambda$-defined by the combinators $H_1, \ldots, H_m$, then $g \circ (h_1, \ldots, h_m)$ is $\lambda$-defined by

$$F = \lambda x_1 \cdots x_n. G(H_1 x_1 \cdots x_n) \cdots (H_m x_1 \cdots x_n).$$

Since the functions are total, there is no problem.

**Step 3.** Closure under primitive recursion.

We could use a fixed-point combinator but the combinator $Iter$ and pairing do the job. If $f$ is defined by primitive recursion from $g$ and $h$, and if $G$ $\lambda$-defines $g$ and $H$ $\lambda$-defines $h$, then $f$ is $\lambda$-defined by

$$F = \lambda n x_1 \cdots x_m. \pi_1(Iter \ n \ \lambda z. \langle H_1 \pi_2 z x_1 \cdots x_m, Succ_c(\pi_2 z) \rangle \langle G x_1 \cdots x_m, c_0 \rangle).$$

The reason $F$ works is that we can prove by induction that

$$(\lambda z. \langle H_1 \pi_2 z c_{n_1} \cdots c_{n_m}, Succ_c(\pi_2 z) \rangle)^n \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle \rightarrow_\beta \langle c_{f(n_1, \ldots, n_m)}, c_n \rangle.$$

For the base case $n = 0$,

$$(\lambda z. \langle H_1 \pi_2 z c_{n_1} \cdots c_{n_m}, Succ_c(\pi_2 z) \rangle)^0 \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle$$

$$\rightarrow_\beta \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle = \langle c_{g(n_1, \ldots, n_m)}, c_0 \rangle = \langle c_{f(0, n_1, \ldots, n_m)}, c_0 \rangle.$$

For the induction step,

$$(\lambda z. \langle H_1 \pi_2 z c_{n_1} \cdots c_{n_m}, Succ_c(\pi_2 z) \rangle)^{n+1} \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle$$

$$= (\lambda z. \langle H_1 \pi_2 z c_{n_1} \cdots c_{n_m}, Succ_c(\pi_2 z) \rangle)$$

$$\rightarrow_\beta (\lambda z. \langle H_1 \pi_2 z c_{n_1} \cdots c_{n_m}, Succ_c(\pi_2 z) \rangle)^n \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle$$

$$\rightarrow_\beta \langle H_{c_{f(n_1, \ldots, n_m)}} c_n c_{n_1} \cdots c_{n_m}, Succ_c c_n \rangle$$

$$\rightarrow_\beta \langle c_{h(f(n_1, \ldots, n_m), n_1, \ldots, n_m)}, c_{n+1} \rangle = \langle c_{f(n+1, n_1, \ldots, n_m)}, c_{n+1} \rangle.$$

Since the functions are total, there is no problem.

We can also show that primitive recursion can be achieved using a fixed-point combinator.

Define the combinators $J$ and $F$ by

$$J = \lambda f x_1 \cdots x_m. \text{if } IsZero_c x \text{ then } G x_1 \cdots x_m \text{ else } H(f(Pred_c x) x_1 \cdots x_m)(\text{Pred}_c x) x_1 \cdots x_m,$$
and

\[ F = \Theta J. \]

Then \( F \) \( \lambda \)-defines \( f \), and since the functions are total, there is no problem. This method must be used if we use the Barendregt numerals.

**Step 4.** Closure under minimization.

Suppose \( f \) is total and defined by minimization from \( g \) and that \( g \) is \( \lambda \)-defined by \( G \).

Define the combinators \( J \) and \( F \) by

\[ J = \lambda f x_1 \cdots x_m. \text{if IsZero}_c G x_1 \cdots x_m \text{ then } x \text{ else } f(\text{Succ}_c x) x_1 \cdots x_m \]

and

\[ F = \Theta J. \]

It is not hard to check that

\[ F c_n c_{n_1} \cdots c_{n_n} \rightarrow_{\beta} \begin{cases} c_n & \text{if } g(n, n_1, \ldots, n_m) = 0 \\ F c_n+1 c_{n_1} \cdots c_{n_n} & \text{otherwise,} \end{cases} \]

and we can use this to prove that \( F \) \( \lambda \)-defines \( f \). Since we assumed that \( f \) is total, some least \( n \) will be found. We leave the details as an exercise.

This finishes the proof that every total computable function is \( \lambda \)-definable.

To prove the result for the partial computable functions we appeal to the Kleene normal form: every partial computable function \( f : \mathbb{N}^m \to \mathbb{N} \) is computable as

\[ f = g \circ \mu h, \]

for some primitive recursive functions \( g : \mathbb{N} \to \mathbb{N} \) and \( h : \mathbb{N}^{m+1} \to \mathbb{N} \). Then our previous proof yields combinators \( G \) and \( H \) that \( \lambda \)-define \( g \) and \( h \). The minimization of \( h \) may fail but since \( g \) is a total function of a single argument, \( f(n_1, \ldots, n_m) \) is defined iff \( g(\mu_n[h(n, n_1, \ldots, n_m) = 0]) \) is defined so it should be clear that \( F \) computes \( f \), but the reader may want to provide a rigorous argument. A detailed proof is given in Hindley and Seldin [16] (Chapter 4, Theorem 4.18).

Combining Theorem 6.10 and Theorem 6.11 we have established the remarkable result that the set of \( \lambda \)-definable total functions is exactly the set of (total) computable functions, and similarly for partial functions. So the \( \lambda \)-calculus has universal computing power.

**Remark:** With some work, it is possible to show that lists can be represented in the \( \lambda \)-calculus. Since a Turing machine tape can be viewed as a list, it should be possible (but very tedious) to simulate a Turing machine in the \( \lambda \)-calculus. This simulation should be somewhat analogous to the proof that a Turing machine computes a computable function (defined à la Herbrand–Gödel–Kleene).

Since the \( \lambda \)-calculus has the same power as Turing machines we should expect some undecidability results analogous to the undecidability of the halting problem or Rice’s theorem. We state the following analog of Rice’s theorem without proof. It is a corollary of a theorem known as the Scott–Curry theorem.
Theorem 6.12. (D. Scott) Let $A$ be any nonempty set of $\lambda$-terms not equal to the set of all $\lambda$-terms. If $A$ is closed under $\beta$-reduction, then it is not computable (not recursive).

Theorem 6.12 is proven in Barendregt [3] (Chapter 6, Theorem 6.6.2) and Barendregt [4].

As a corollary of Theorem 6.12 it is undecidable whether a $\lambda$-term has a $\beta$-normal form, a result originally proved by Church. This is an analog of the undecidability of the halting problem, but it seems more spectacular because the syntax of $\lambda$-terms is really very simple. The problem is that $\beta$-reduction is very powerful and elusive.

### 6.7 Definability of Functions in Typed Lambda-Calculi

In the pure $\lambda$-calculus, some $\lambda$-terms have no $\beta$-normal form, and worse, it is undecidable whether a $\lambda$-term has a $\beta$-normal form. In contrast, by Theorem 2.12, every raw $\lambda$-term that type-checks in the simply-typed $\lambda$-calculus has a $\beta$-normal form. Thus it is natural to ask whether the natural numbers are definable in the simply-typed $\lambda$-calculus because if the answer is positive, then the numerical functions definable in the simply-typed $\lambda$-calculus are guaranteed to be total.

This indeed possible. If we pick any base type $\sigma$, then we can define typed Church numerals $c_n$ as terms of type $\text{Nat}_\sigma = (\sigma \rightarrow \sigma) \rightarrow (\sigma \rightarrow \sigma)$, by

$$c_n = \lambda f : (\sigma \rightarrow \sigma). \lambda x : \sigma. f^n(x).$$

The notion of $\lambda$-definable function is defined just as before. Then we can define $\text{Add}$ and $\text{Mult}$ as terms of type $\text{Nat}_\sigma \rightarrow (\text{Nat}_\sigma \rightarrow \text{Nat}_\sigma)$ essentially as before, but surprise, not much more is definable. Among other things, strong typing of terms restricts the iterator combinator too much. It was shown by Schwichtenberg and Statman that the numerical functions definable in the simply-typed $\lambda$-calculus are the extended polynomials; see Statman [24] and Troelstra and Schwichtenberg [25]. The extended polynomials are the smallest class of numerical functions closed under composition containing

1. The constant functions 0 and 1.
2. The projections.
3. Addition and multiplication.
4. The function $\text{IsZero}_c$.

Is there a way to get a larger class of total functions?

There are indeed various ways of doing this. One method is to add the natural numbers and the booleans as data types to the simply-typed $\lambda$-calculus, and to also add product types, an iterator combinator, and some new reduction rules. This way we obtain a system equivalent to Gödel’s system $T$. A large class of numerical total functions containing the
6.7. DEFINABILITY OF FUNCTIONS IN TYPED LAMBDA-CALCULI

primitive recursive functions is definable in this system; see Girard–Lafond–Taylor [13]. Although theoretically interesting, this is not a practical system.

Another wilder method is to allow more general types to the simply-typed \( \lambda \)-calculus, the so-called second-order types or polymorphic types. In addition to base types, we allow type variables (often denoted \( X, Y, \ldots \)) ranging over simple types and new types of the form \( \forall X. \sigma \).\(^3\) For example, \( \forall X. (X \to X) \) is such a new type, and so is

\[
\forall X. (X \to ((X \to X) \to X)).
\]

Actually, the second-order types that we just defined are special cases of the QBF (quantified boolean formulae) arising in complexity theory restricted to implication and universal quantifiers. Remarkably, the other connectives \( \land, \lor, \neg \) and \( \exists \) are definable in terms of \( \to \) (as a logical connective, \( \Rightarrow \)) and \( \forall \); see Troelstra and Schwichtenberg [25] (Chapter 11).

**Remark:** The type

\[
\text{Nat} = \forall X. (X \to ((X \to X) \to X))
\]

can be chosen to represent the type of the natural numbers. The type of the natural numbers can also be chosen to be

\[
\forall X. (X \to X) \to (X \to X).
\]

This makes essentially no difference but the first choice has some technical advantages.

There is also a new form of type abstraction, \( \Lambda X. M \), and of type application, \( M \sigma \), where \( M \) is a \( \lambda \)-term and \( \sigma \) is a type. There are two new typing rules:

\[
\frac{\Gamma \vdash M : \sigma}{\Gamma \vdash (\Lambda X. M) : \forall X. \sigma} \quad \text{(type abstraction)}
\]

provided that \( X \) does not occur free in any of the types in \( \Gamma \), and

\[
\frac{\Gamma \vdash M : \forall X. \sigma}{\Gamma \vdash (M \tau) : \sigma[X := \tau]} \quad \text{(type application)}
\]

where \( \tau \) is any type (and no capture of variable takes place).

From the point of view where types are viewed as propositions and \( \lambda \)-terms are viewed as proofs, type abstraction is an introduction rule and type application is an elimination rule, both for the second-order quantifier \( \forall \).

We also have a new reduction rule

\[
(\Lambda X. M)\sigma \to_{\beta\forall} M[X := \sigma]
\]

that corresponds to a new form of redundancy in proofs having to do with a \( \forall \)-elimination immediately following a \( \forall \)-introduction. Here in the substitution \( M[X := \tau] \), all free occurrences of \( X \) in \( M \) and the types in \( M \) are replaced by \( \tau \). For example,

\[
(\Lambda X. \lambda f : (X \to X). \lambda x : X. \lambda g : \forall Y. (Y \to Y). g X f x)[X := \tau] = \lambda f : (\tau \to \tau). \lambda x : \tau. \lambda g : \forall Y. (Y \to Y). g \tau x f.
\]

\(^3\)Barendregt and others used Greek variables to denote type variables but we find this confusing.
For technical details, see Gallier [10].

This new typed $\lambda$-calculus is the second-order polymorphic lambda calculus. It was invented by Girard (1972) who named it system $F$; see Girard [14, 15], and it is denoted $\lambda 2$ by Barendregt. From the point of view of logic, Girard’s system is a proof system for intuitionistic second-order propositional logic. We define $\rightarrow_{\lambda 2}^+$ and $\rightarrow_{\lambda 2}^*$ as the relations

$$
\rightarrow_{\lambda 2}^+ = (\rightarrow_{\beta} \cup \rightarrow_{\beta\forall})^+
$$

$$
\rightarrow_{\lambda 2}^* = (\rightarrow_{\beta} \cup \rightarrow_{\beta\forall})^*.
$$

A variant of system $F$ was also introduced independently by John Reynolds (1974) but for very different reasons.

The intuition behind terms of type $\forall X.\sigma$ is that a term $M$ of type $\forall X.\sigma$ is a sort of generic function such that for any type $\tau$, the function $M\tau$ is a specialized version of type $\sigma[X := \tau]$ of $M$. For example, $M$ could be the function that appends an element to a list, and for specific types such as the natural numbers $\text{Nat}$, strings $\text{String}$, trees $\text{Tree}$, etc., the functions $M\text{Nat}$, $M\text{String}$, $M\text{Tree}$, are the specialized versions of $M$ to lists of elements having the specific data types $\text{Nat}$, $\text{String}$, $\text{Tree}$.

For example, if $\sigma$ is any type, we have the closed term

$$
A_\sigma = \lambda x : \sigma. \lambda f : (\sigma \to \sigma). f x,
$$

of type $\sigma \to ((\sigma \to \sigma) \to \sigma)$, such that for every term $F$ of type $\sigma \to \sigma$ and every term $a$ of type $\sigma$,

$$
A_\sigma Fa \rightarrow_{\lambda 2}^+ Fa.
$$

Since $A_\sigma$ has the same behavior for all types $\sigma$, it is natural to define the generic function $A$ given by

$$
A = \Lambda X. \lambda x : X. \lambda f : (X \to X). f x,
$$

which has type $\forall X. (X \to ((X \to X) \to X))$, and then $A\sigma$ has the same behavior as $A_\sigma$.

We will see shortly that $A$ is the Church numeral $c_1$ in $\lambda 2$.

Remarkably, system F is strongly normalizing, which means that every $\lambda$-term typable in system F has a $\beta$-normal form. The proof of this theorem is hard and was one of Girard’s accomplishments in his dissertation, Girard [15]. The Church–Rosser property also holds for system F. The proof technique used to prove that system F is strongly normalizing is thoroughly analyzed in Gallier [10].

We stated earlier that deciding whether a simple type $\sigma$ is provable, that is, whether there is a closed $\lambda$-term $M$ that type-checks in the simply-typed $\lambda$-calculus such that the judgement $\triangleright M : \sigma$ is provable is a hard problem. Indeed Statman proved that this problem is $\text{P}$-space complete; see Statman [23].

It is natural so ask whether it is decidable whether given any second-order type $\sigma$, there is a closed $\lambda$-term $M$ that type-checks in system F such that the judgement $\triangleright M : \sigma$ is provable (if $\sigma$ is viewed as a second-order logical formula, the problem is to decide whether $\sigma$
is provable). Surprisingly the answer is no; this problem (called *inhabitation*) is undecidable. This result was proven by L"ob around 1976, see Barendregt [4].

This undecidability result is troubling and at first glance seems paradoxical. Indeed, viewed as a logical formula, a second-order type $\sigma$ is a QBF (a quantified boolean formula), and if we assign the truth values $F$ and $T$ to the boolean variables in it, we can decide whether such a proposition is valid in exponential time and polynomial space (in fact, we will see that later QBF validity is P-space complete). This seems in contradiction with the fact that provability is undecidable.

But the proof system corresponding to system F is an *intuitionistic* proof system, so there are (non-quantified) propositions that are valid in the truth-value semantics but not provable in intuitionistic propositional logic. The set of second-order propositions provable in intuitionistic second-order logic is a *proper* subset of the set of valid QBF (under the truth-value semantics), and it is *not computable*. So there is no paradox after all.

Going back to the issue of computability of numerical functions, a version of the *Church numerals* can be defined as

$$c_n = \Lambda X. \lambda x: X. \lambda f: (X \to X). f^n(x).$$

Observe that $c_n$ has type $Nat$. Inspired by the definition of $Succ$ given in Section 6.4, we can define the successor function on the natural numbers as

$$Succ = \lambda n: Nat. \Lambda X. \lambda x: X. \lambda f: (X \to X). f(nX xf).$$

Note how $n$, which is of type $Nat = \forall X. (X \to ((X \to X) \to X))$, is applied to the type variable $X$ in order to become a term $nX$ of type $X \to ((X \to X) \to X)$, so that $nX xf$ has type $X$, thus $f(nX xf)$ also has type $X$.

For every type $\sigma$, every term $F$ of type $\sigma \to \sigma$ and every term $a$ of type $\sigma$, we have

$$c_n \sigma a F = (\Lambda X. \lambda x: X. \lambda f: (X \to X). f^n(x)) a F \xrightarrow{\lambda_2} (\lambda x: \sigma. \lambda f: (\sigma \to \sigma). f^n(x)) a F \xrightarrow{\lambda_2} F^n(a);$$

that is,

$$c_n \sigma a F \xrightarrow{\lambda_2} F^n(a). \quad (\ast_{c2})$$

So $c_n \sigma$ iterates $F$ $n$ times starting with $a$. As a consequence,

$$Succ \ c_n = (\lambda n: Nat. \Lambda X. \lambda x: X. \lambda f: (X \to X). f(nX xf)) c_n \xrightarrow{\lambda_2} \Lambda X. \lambda x: X. \lambda f: (X \to X). f(c_n X xf) \xrightarrow{\lambda_2} \Lambda X. \lambda x: X. \lambda f: (X \to X). f(f^n(x))$$

$$= \Lambda X. \lambda x: X. \lambda f: (X \to X). f^{n+1}(x) = c_{n+1}.$$
We can also define addition of natural numbers as

\[
\text{Add} = \lambda m : \text{Nat}. \lambda n : \text{Nat}. \Lambda X. \lambda x : X. \lambda f : (X \to X). (mX f(nX x)f).
\]

Note how \( m \) and \( n \), which are of type \( \text{Nat} = \forall X. (X \to (X \to X) \to X) \), are applied to the type variable \( X \) in order to become terms \( mX \) and \( nX \) of type \( X \to (X \to X) \to X \), so that \( nXxf \) has type \( X \) and \( f(nXxf) \) has type \( X \to X \), and finally \( (mX f(nX x)f)f \) has type \( X \).

Many of the constructions that can be performed in the pure \( \lambda \)-calculus can be mimicked in system F, which explains its expressive power. For example, for any two second-order types \( \sigma \) and \( \tau \), we can define a pairing function \( \langle -, - \rangle \) (to be very precise, \( \langle -, - \rangle_{\sigma,\tau} \)) given by

\[
\langle -, - \rangle = \lambda u : \sigma. \lambda v : \tau. \Lambda X. \lambda f : \sigma \to (\tau \to X). fuv,
\]

of type \( \sigma \to (\tau \to (\forall X. ((\sigma \to (\tau \to X)) \to X)) \). Given any term \( M \) of type \( \sigma \) and any term \( N \) of type \( \tau \), we have

\[
\langle -, - \rangle_{\sigma,\tau} MN \xrightarrow{\lambda2} \Lambda X. \lambda f : \sigma \to (\tau \to X). fMN.
\]

Thus we define \( \langle M, N \rangle \) as

\[
\langle M, N \rangle = \Lambda X. \lambda f : \sigma \to (\tau \to X). fMN,
\]

and the type

\[
\forall X. ((\sigma \to (\tau \to X)) \to X)
\]

of \( \langle M, N \rangle \) is denoted by \( \sigma \times \tau \). As a logical formula it is equivalent to \( \sigma \land \tau \), which means that if we view \( \sigma \) and \( \tau \) as (second-order) propositions, then

\[
\sigma \land \tau \equiv \forall X. ((\sigma \to (\tau \to X)) \to X)
\]

is provable intuitionistically. This is a special case of the result that we mentioned earlier: the connectives \( \land, \lor, \neg \) and \( \exists \) are definable in terms of \( \to \) (as a logical connective, \( \Rightarrow \)) and \( \forall \).

**Proposition 6.13.** The connectives \( \land, \lor, \neg, \bot \) and \( \exists \) are definable in terms of \( \to \) and \( \forall \), which means that the following equivalences are provable intuitionistically, where \( X \) is not free in \( \sigma \) or \( \tau \):

\[
\sigma \land \tau \equiv \forall X. ((\sigma \to (\tau \to X)) \to X)
\]
\[
\sigma \lor \tau \equiv \forall X. ((\sigma \to X) \to ((\tau \to X) \to X))
\]
\[
\bot \equiv \forall X. X
\]
\[
\neg \sigma \equiv \sigma \to \forall X. X
\]
\[
\exists Y. \sigma \equiv \forall X. ((\forall Y. (\sigma \to X)) \to X).
\]
We leave the proof as an exercise, or see Troelstra and Schwichtenberg [25] (Chapter 11).

Remark: The rule of type application implies that \( \bot \rightarrow \sigma \) is intuitionistically provable for all propositions (types) \( \sigma \). So in second-order logic there is no difference between minimal and intuitionistic logic.

We also have two projections \( \pi_1 \) and \( \pi_2 \) (to be very precise \( \pi_1^{\sigma \times \tau} \) and \( \pi_2^{\sigma \times \tau} \)) given by

\[
\begin{align*}
\pi_1 &= \lambda g : \sigma \times \tau. g \sigma(\lambda x : \sigma. \lambda y : \tau. x) \\
\pi_2 &= \lambda g : \sigma \times \tau. g \tau(\lambda x : \sigma. \lambda y : \tau. y).
\end{align*}
\]

It is easy to check that \( \pi_1 \) has type \( (\sigma \times \tau) \rightarrow \sigma \) and that \( \pi_2 \) has type \( (\sigma \times \tau) \rightarrow \tau \). The reader should check that for any \( M \) of type \( \sigma \) and any \( N \) of type \( \tau \) we have

\[
\begin{align*}
\pi_1(M, N) &\xrightarrow{+} \lambda_2 M \quad \text{and} \quad \pi_2(M, N) \xrightarrow{+} \lambda_2 N.
\end{align*}
\]

For example, we have

\[
\begin{align*}
\pi_1(M, N) &= (\lambda g : \sigma \times \tau. g \sigma(\lambda x : \sigma. \lambda y : \tau. x))(\Lambda X. \lambda f : \sigma \rightarrow (\tau \rightarrow X). f MN) \\
&\xrightarrow{+} \lambda_2 (\Lambda X. \lambda f : \sigma \rightarrow (\tau \rightarrow X). f MN)\sigma(\lambda x : \sigma. \lambda y : \tau. x) \\
&\xrightarrow{+} \lambda_2 (\lambda f : \sigma \rightarrow (\tau \rightarrow \sigma). f MN)(\lambda x : \sigma. \lambda y : \tau. x) \\
&\xrightarrow{+} \lambda_2 (\lambda x : \sigma. \lambda y : \tau. x)MN \\
&\xrightarrow{+} \lambda_2 (\lambda y : \tau. M)N \\
&\xrightarrow{+} \lambda_2 M.
\end{align*}
\]

The booleans can be defined as

\[
\begin{align*}
T &= \Lambda X. \lambda x : X. \lambda y : X. x \\
F &= \Lambda X. \lambda x : X. \lambda y : X. y,
\end{align*}
\]

both of type \( \text{Bool} = \forall X. (X \rightarrow (X \rightarrow X)) \). We also define if then else as

\[
\text{if then else} = \Lambda X. \lambda z : \text{Bool}. z X
\]

of type \( \forall X. \text{Bool} \rightarrow (X \rightarrow (X \rightarrow X)) \). It is easy that for any type \( \sigma \) and any two terms \( M \) and \( N \) of type \( \sigma \) we have

\[
\begin{align*}
(\text{if } T \text{ then } M \text{ else } N) \sigma &\xrightarrow{+} \lambda_2 M \\
(\text{if } F \text{ then } M \text{ else } N) \sigma &\xrightarrow{+} \lambda_2 N,
\end{align*}
\]
where we write \((\text{if } T \text{ then } M \text{ else } N)\)\(\sigma\) instead of \((\text{if then else } \sigma) T M N\) (and similarly for the other term). For example, we have

\[
(if \; T \; then \; M \; else \; N)\; \sigma = (\Lambda X. \lambda z : \text{Bool}. z X)\; \sigma \; T M N
\]

\[
\overset{\lambda 2}{\rightarrow} (\lambda z : \text{Bool}. z \sigma) T M N
\]

\[
\overset{\lambda 2}{\rightarrow} (T \sigma) M N
\]

\[
= ((\Lambda X. \lambda x : X. \lambda y : X. x)\sigma) M N
\]

\[
\overset{\lambda 2}{\rightarrow} (\lambda x : \sigma. \lambda y : \sigma. x) M N
\]

\[
\overset{\lambda 2}{\rightarrow} M.
\]

Lists, trees, and other inductively data structures are also representable in system F; see Girard–Lafond–Taylor [13].

We can also define an iterator \textbf{Iter} given by

\[
\text{Iter} = \Lambda X. \lambda u : X. \lambda f : (X \rightarrow X). \lambda z : \text{Nat}. z X u f
\]

of type \(\forall X. (X \rightarrow ((X \rightarrow X) \rightarrow (\text{Nat} \rightarrow X)))\). The idea is that given \(f\) of type \(\sigma \rightarrow \sigma\) and \(u\) of type \(\sigma\), the term \textbf{Iter} \(\sigma u f c_n\) iterates \(f\) \(n\) times over the input \(u\). It is easy to show that for any term \(t\) of type \text{Nat} we have

\[
\text{Iter} \sigma u f c_0 \overset{\lambda 2}{\rightarrow} u
\]

\[
\text{Iter} \sigma u f (\text{Succ}_c t) \overset{\lambda 2}{\rightarrow} f(\text{Iter} \sigma u f t),
\]

and that

\[
\text{Iter} \sigma u f c_n \overset{\lambda 2}{\rightarrow} f^n(u).
\]

Then mimicking what we did in the pure \(\lambda\)-calculus, we can show that the primitive recursive functions are \(\lambda\)-definable in system \(F\). Actually, higher-order primitive recursion is definable. So, for example, Ackermann’s function is definable.

Remarkably, the class of numerical functions definable in system F is a class of (total) computable functions much bigger than the class of primitive recursive functions. This class of functions was characterized by Girard as the functions that are provably-recursive in a formalization of arithmetic known as \textit{intuitionistic second-order arithmetic}; see Girard [15], Troelstra and Schwichtenberg [25] and Girard–Lafond–Taylor [13]. It can also be shown (using a diagonal argument) that there are (total) computable functions not definable in system F.

From a theoretical point of view, every (total) function that we will ever want to compute is definable in system F. However, from a practical point of view, programming in system F is very tedious and usually leads to very inefficient programs. Nevertheless polymorphism is an interesting paradigm which had made its way in certain programming languages.

Type systems even more powerful than system F have been designed, the ultimate system being the \textit{calculus of constructions} due to Huet and Coquand, but these topics are beyond the scope of these notes.
One last comment has to do with the use of the simply-typed \( \lambda \)-calculus as a the core of a programming language. In the early 1970's Dana Scott defined a system named LCF based on the the simply-typed \( \lambda \)-calculus and obtained by adding the natural numbers and the booleans as data types, product types, and a fixed-point operator. Robin Milner then extended LCF, and as a by-product, defined a programming language known as ML, which is the ancestor of most functional programming languages. A masterful and thorough exposition of type theory and its use in programming language design is given in Pierce [20].

We now revisit the problem of defining the partial computable functions.

### 6.8 Head Normal-Forms and the Partial Computable Functions

One defect of the proof of Theorem 6.11 in the case where a computable function is partial is the use of the Kleene normal form. The difficulty has to do with composition. Given a partial computable function \( g \) \( \lambda \)-defined by a closed term \( G \) and a partial computable function \( h \) \( \lambda \)-defined by a closed term \( H \) (for simplicity we assume that both \( g \) and \( h \) have a single argument), it would be nice if the composition \( h \circ g \) was represented by \( \lambda x. H(Gx) \). This is true if both \( g \) and \( h \) are total, but false if either \( g \) or \( h \) is partial as shown by the following example from Barendregt [3] (Chapter 2, §2). If \( g \) is the function undefined everywhere and \( h \) is the constant function 0, then \( g \) is \( \lambda \)-defined by \( G = K \Omega \) and \( h \) is \( \lambda \)-defined by \( H = K c_0 \), with \( \Omega = (\lambda x.(xx))(\lambda x.(xx)) \). We have

\[
\lambda x. H(Gx) = \lambda x. K c_0(K \Omega x) \xrightarrow{+} \beta \lambda x. K c_0 \Omega \xrightarrow{+} \beta \lambda x. c_0,
\]

but \( h \circ g = g \) is the function undefined everywhere, and \( \lambda x. c_0 \) represents the total function \( h \), so \( \lambda x. H(Gx) \) does not \( \lambda \)-define \( h \circ g \).

It turns out that the \( \lambda \)-definability of the partial computable functions can be obtained in a more elegant fashion without having recourse to the Kleene normal form by capturing the fact that a function is undefined for some input is a more subtle way. The key notion is the notion of head normal form, which is more general than the notion of \( \beta \)-normal form. As a consequence, there a fewer \( \lambda \)-terms having no head normal form than \( \lambda \)-terms having no \( \beta \)-normal form, and we capture a stronger form of divergence.

Recall that a \( \lambda \)-term is either a variable \( x \), or an application \( (MN) \), or a \( \lambda \)-abstraction \( (\lambda x.M) \). We can sharpen this characterization as follows.

**Proposition 6.14.** The following properties hold:

1. Every application term \( M \) is of the form

\[
M = (N_1N_2 \cdots N_{n-1})N_n, \quad n \geq 2,
\]

where \( N_1 \) is not an application term.
(2) Every abstraction term $M$ is of the form
\[ M = \lambda x_1 \cdots x_n. N, \quad n \geq 1, \]
where $N$ is not an abstraction term.

(3) Every $\lambda$-term $M$ is of one of the following two forms:
\[ M = \lambda x_1 \cdots x_n. xM_1 \cdots M_m, \quad m, n \geq 0 \]  
\[ M = \lambda x_1 \cdots x_n. (\lambda x. M_0)M_1 \cdots M_m, \quad m \geq 1, n \geq 0, \]
where $x$ is a variable.

Proof. (1) Suppose that $M$ is an application $M = M_1 M_2$. We proceed by induction on the depth of $M_1$. For the base case $M_1$ must be variables and we are done. For the induction step, if $M_1$ is a $\lambda$-abstraction, we are done. If $M_1$ is an application, then by the induction hypothesis it is of the form
\[ M_1 = (N_1 N_2 \cdots N_{n-1})N_n, \quad n \geq 2, \]
where $N_1$ is not an application term, and then
\[ M = M_1 M_2 = ((N_1 N_2 \cdots N_{n-1})N_n)M_2 \quad n \geq 2, \]
where $N_1$ is not an application term.

The proof of (2) is similar.

(3) We proceed by induction on the depth of $M$. If $M$ is a variable, then we are in Case (a) with $m = n = 0$.

If $M$ is an application, then by (1) it is of the form $M = N_1 N_2 \cdots N_p$ with $N_1$ not an application term. This means that either $N_1$ is a variable, in which case we are in Case (a) with $n = 0$, or $N_1$ is an abstraction, in which case we are in Case (b) also with $n = 0$.

If $M$ is an abstraction $\lambda x. N$, then by the induction hypothesis $N$ is of the form (a) or (b), and by adding one more binder $\lambda x$ in front of these expressions we preserve the shape of (a) and (b) by increasing $n$ by 1.

Proposition 6.14 motivates the following definition.

**Definition 6.17.** A $\lambda$-term $M$ is a **head normal form** (for short *hnf*) if it is of the form (a), namely
\[ M = \lambda x_1 \cdots x_n. xM_1 \cdots M_m, \quad m, n \geq 0, \]
where $x$ is a variable called the **head variable**.
A λ-term $M$ has a head normal form if there is some head normal form $N$ such that $M \overset{*}{\rightarrow}_\beta N$.

In a term $M$ of the form (b),

$$M = \lambda x_1 \cdots x_n. (\lambda x. M_0)M_1 \cdots M_m, \quad m \geq 1, n \geq 0,$$

the subterm $(\lambda x. M_0)M_1$ is called the head redex of $M$.

In addition to the terms of type (a) that we listed after Proposition 6.14, the term $\lambda x. x\Omega$ is a head normal form. It is the head normal form of the term $\lambda x. (Ix)\Omega$, which has no β-normal form.

Not every term has a head normal form. For example, the term

$$\Omega = (\lambda x. (xx))(\lambda x. (xx))$$

has no head normal form. Every β-normal form must be a head normal form, but the converse is false as we saw with

$$M = \lambda x. x\Omega,$$

which is a head normal form but has no β-normal form.

Note that a head redex of a term is a leftmost redex, but not conversely, as shown by the term $\lambda x. x((\lambda y. y)x)$.

A term may have more than one head normal form but here is a way of obtaining a head normal form (if there is one) in a systematic fashion.

**Definition 6.18.** The relation $\rightarrow_h$, called one-step head reduction, is defined as follows: For any two terms $M$ and $N$, if $M$ contains a head redex $(\lambda x. M_0)M_1$, which means that $M$ is of the form

$$M = \lambda x_1 \cdots x_n. (\lambda x. M_0)M_1 \cdots M_m, \quad m \geq 1, n \geq 0,$$

then $M \rightarrow_h N$ with

$$N = \lambda x_1 \cdots x_n. (M_0[x := M_1])M_2 \cdots M_m.$$

We denote by $\overset{+}{\rightarrow}_h$ the transitive closure of $\rightarrow_h$ and by $\overset{*}{\rightarrow}_h$ the reflexive and transitive closure of $\rightarrow_h$.

Given a term $M$ containing a head redex, the head reduction sequence of $M$ is the uniquely determined sequence of one-step head reductions

$$M = M_0 \rightarrow_h M_1 \rightarrow_h \cdots \rightarrow_h M_n \rightarrow_h \cdots.$$

If the head reduction sequence reaches a term $M_n$ which is a head normal form we say that the sequence terminates, and otherwise we say that $M$ has an infinite head reduction.

The following result is shown in Barendregt [3] (Chapter 8, §3).
Theorem 6.15. (Wadsworth) A $\lambda$-term $M$ has a head normal form if and only if the head reduction sequence terminates.

In some intuitive sense, a $\lambda$-term $M$ that does not have any head normal form has a strong divergence behavior with respect to $\beta$-reduction.

Remark: There is a notion more general than the notion of head normal form which comes up in functional languages (for example, Haskell). A $\lambda$-term $M$ is a weak head normal form if it of one of the two forms

$$\lambda x. N \text{ or } y N_1 \cdots N_m$$

where $y$ is a variable. These are exactly the terms that do not have a redex of the form $(\lambda x. M_0) M_1 N_1 \cdots N_m$. Every head normal form is a weak head normal form, but there are many more weak head normal forms than there are head normal forms since a term of the form $\lambda x. N$ where $N$ is arbitrary is a weak head normal form, but not a head normal form unless $N$ is of the form $\lambda x_1 \cdots x_n. x M_1 \cdots M_m$, with $m, n \geq 0$.

Reducing to a weak head normal form is a lazy evaluation strategy.

There is also another useful notion which turns out to be equivalent to having a head normal form.

Definition 6.19. A closed $\lambda$-term $M$ is solvable if there are closed terms $N_1, \ldots, N_n$ such that

$$MN_1 \cdots N_n \overset{*}{\to} \beta I.$$ 

A $\lambda$-term $M$ with free variables $x_1, \ldots, x_m$ is solvable if the closed term $\lambda x_1 \cdots x_m. M$ is solvable. A term is unsolvable if it is not solvable.

The following result is shown in Barendregt [3] (Chapter 8, §3).

Theorem 6.16. (Wadsworth) A $\lambda$-term $M$ has a head normal form if and only if is it solvable.

Actually, the proof that having a head normal form implies solvable is not hard.

We are now ready to revise the notion of $\lambda$-definability of numerical functions.

Definition 6.20. A function (partial or total) $f: \mathbb{N}^n \to \mathbb{N}$ is strongly $\lambda$-definable if for all $m_1, \ldots, m_n \in \mathbb{N}$, there is a combinator (a closed $\lambda$-term) $F$ with the following properties:

1. If the value $f(m_1, \ldots, m_n)$ is defined, then $Fc_{m_1} \cdots c_{m_n}$ reduces to the $\beta$-normal form $c_{f(m_1, \ldots, m_n)}$.

2. If $f(m_1, \ldots, m_n)$ is undefined, then $Fc_{m_1} \cdots c_{m_n}$ has no head normal form, or equivalently, is unsolvable.

Observe that in Case (2), when the value $f(m_1, \ldots, m_n)$ is undefined, the divergence behavior of $Fc_{m_1} \cdots c_{m_n}$ is stronger than in Definition 6.16. Not only $Fc_{m_1} \cdots c_{m_n}$ has no $\beta$-normal form, but actually it has no head normal form.

The following result is proven in Barendregt [3] (Chapter 8, §4). The proof does not use the Kleene normal form. Instead, it makes clever use of the term $\text{KII}$.
Theorem 6.17. Every partial or total computable function is strongly $\lambda$-definable. Conversely, every strongly $\lambda$-definable function is partial computable.

Making sure that a composition $g \circ (h_1, \ldots, h_m)$ is defined for some input $x_1, \ldots, x_n$ iff all the $h_i(x_1, \ldots, x_n)$ and $g(h_1(x_1, \ldots, x_n), \ldots, h_m(x_1, \ldots, x_n))$ are defined is tricky. The term $\text{KII}$ comes to the rescue! If $g$ is strongly $\lambda$-definable by $G$ and the $h_i$ are strongly $\lambda$-definable by $H_i$, then it can be shown that the combinator $F$ given by

$$F = \lambda x_1 \cdots x_n. (H_1 x_1 \cdots x_n \text{KII}) \cdots (H_m x_1 \cdots x_n \text{KII})(G(H_1 x_1 \cdots x_n) \cdots (G(H_m x_1 \cdots x_n))$$

strongly $\lambda$-defines $F$; see Barendregt [3] (Chapter 8, Lemma 8.4.6).
Chapter 7

Listable Sets and Diophantine Sets; Hilbert’s Tenth Problem

7.1 Diophantine Equations and Hilbert’s Tenth Problem

There is a deep and a priori unexpected connection between the theory of computable and listable sets and the solutions of polynomial equations involving polynomials in several variables with integer coefficients. These are polynomials in \( n \geq 1 \) variables \( x_1, \ldots, x_n \) which are finite sums of monomials of the form

\[
a x_1^{k_1} \cdots x_n^{k_n},
\]

where \( k_1, \ldots, k_n \in \mathbb{N} \) are nonnegative integers, and \( a \in \mathbb{Z} \) is an integer (possibly negative). The natural number \( k_1 + \cdots + k_n \) is called the degree of the monomial \( a x_1^{k_1} \cdots x_n^{k_n} \).

For example, if \( n = 3 \), then

1. 5, -7, are monomials of degree 0.
2. 3\( x_1 \), -2\( x_2 \), are monomials of degree 1.
3. \( x_1 x_2 \), 2\( x_1^2 \), 3\( x_1 x_3 \), -5\( x_2^2 \), are monomials of degree 2.
4. \( x_1 x_2 x_3 \), \( x_1^2 x_3 \), -\( x_2^3 \), are monomials of degree 3.
5. \( x_1^4 \), -\( x_1^2 x_3^2 \), \( x_1 x_2^2 x_3 \), are monomials of degree 4.

It is convenient to introduce multi-indices, where an \( n \)-dimensional multi-index is an \( n \)-tuple \( \alpha = (k_1, \ldots, k_n) \) with \( n \geq 1 \) and \( k_i \in \mathbb{N} \). Let \( |\alpha| = k_1 + \cdots + k_n \). Then we can write

\[
x^\alpha = x_1^{k_1} \cdots x_n^{k_n}.
\]

For example, for \( n = 3 \),

\[
x^{(1,2,1)} = x_1 x_2^2 x_3, \quad x^{(0,2,2)} = x_2^2 x_3^2.
\]
Definition 7.1. A polynomial \( P(x_1, \ldots, x_n) \) in the variables \( x_1, \ldots, x_n \) with integer coefficients is a finite sum of monomials of the form

\[
P(x_1, \ldots, x_n) = \sum_{\alpha} a_{\alpha} x_{\alpha},
\]

where the \( \alpha \)'s are \( n \)-dimensional multi-indices, and with \( a_{\alpha} \in \mathbb{Z} \). The maximum of the degrees \( |\alpha| \) of the monomials \( a_{\alpha} x_{\alpha} \) is called the total degree of the polynomial \( P(x_1, \ldots, x_n) \). The set of all such polynomials is denoted by \( \mathbb{Z}[x_1, \ldots, x_n] \).

Sometimes, we write \( P \) instead of \( P(x_1, \ldots, x_n) \). We also use variables \( x, y, z \) etc. instead of \( x_1, x_2, x_3, \ldots \).

For example, \( 2x - 3y - 1 \) is a polynomial of total degree 1, \( x^2 + y^2 - z^2 \) is a polynomial of total degree 2, and \( x^3 + y^3 + z^3 - 29 \) is a polynomial of total degree 3.

Mathematicians have been interested for a long time in the problem of solving equations of the form

\[
P(x_1, \ldots, x_n) = 0,
\]

with \( P \in \mathbb{Z}[x_1, \ldots, x_n] \), seeking only integer solutions for \( x_1, \ldots, x_n \).

Diophantus of Alexandria, a Greek mathematician of the 3rd century, was one of the first to investigate such equations. For this reason, seeking integer solutions of polynomials in \( \mathbb{Z}[x_1, \ldots, x_n] \) is referred to as solving Diophantine equations.

This problem is not as simple as it looks. The equation

\[
2x - 3y - 1 = 0
\]

obviously has the solution \( x = 2, y = 1 \), and more generally \( x = -1 + 3a, y = -1 + 2a \), for any integer \( a \in \mathbb{Z} \).

The equation

\[
x^2 + y^2 - z^2 = 0
\]

has the solution \( x = 3, y = 4, z = 5 \), since \( 3^2 + 4^2 = 9 + 16 = 25 = 5^2 \). More generally, the reader should check that

\[
x = t^2 - 1, \ y = 2t, \ z = t^2 + 1
\]

is a solution for all \( t \in \mathbb{Z} \).

The equation

\[
x^3 + y^3 + z^3 - 29 = 0
\]

has the solution \( x = 3, y = 1, z = 1 \).

What about the equation

\[
x^3 + y^3 + z^3 - 30 = 0?
\]
Amazingly, the only known integer solution is 
\[(x, y, z) = (-283059965, -221888517, 2220422932),\]
discovered in 1999 by E. Pine, K. Yarbrough, W. Tarrant, and M. Beck, following an approach suggested by N. Elkies.

And what about solutions of the equation
\[x^3 + y^3 + z^3 - 33 = 0?\]
Well, nobody knows whether this equation is solvable in integers!

In 1900, at the International Congress of Mathematicians held in Paris, the famous mathematician David Hilbert presented a list of ten open mathematical problems. Soon after, Hilbert published a list of 23 problems. The tenth problem is this:

**Hilbert’s tenth problem (H10)**

Find an algorithm that solves the following problem:

Given as input a polynomial \( P \in \mathbb{Z}[x_1, \ldots, x_n] \) with integer coefficients, return YES or NO, according to whether there exist integers \( a_1, \ldots, a_n \in \mathbb{Z} \) so that \( P(a_1, \ldots, a_n) = 0 \); that is, the Diophantine equation \( P(x_1, \ldots, x_n) = 0 \) has a solution.

It is important to note that at the time Hilbert proposed his tenth problem, a rigorous mathematical definition of the notion of algorithm did not exist. In fact, the machinery needed to even define the notion of algorithm did not exist. It is only around 1930 that precise definitions of the notion of computability due to Turing, Church, and Kleene, were formulated, and soon after shown to be all equivalent.

So to be precise, the above statement of Hilbert’s tenth should say: find a RAM program (or equivalently a Turing machine) that solves the following problem: ...

In 1970, the following somewhat surprising resolution of Hilbert’s tenth problem was reached:

**Theorem** (Davis-Putnam-Robinson-Matiyasevich)

*Hilbert’s tenth problem is undecidable; that is, there is no algorithm for solving Hilbert’s tenth problem.*

In 1962, Davis, Putnam and Robinson had shown that if a fact known as Julia Robinson hypothesis could be proved, then Hilbert’s tenth problem would be undecidable. At the time, the Julia Robinson hypothesis seemed implausible to many, so it was a surprise when in 1970 Matiyasevich found a set satisfying the Julia Robinson hypothesis, thus completing the proof of the undecidability of Hilbert’s tenth problem. It is also a bit startling that Matiyasevich’ set involves the Fibonacci numbers.

A detailed account of the history of the proof of the undecidability of Hilbert’s tenth problem can be found in Martin Davis’ classical paper Davis [6].
Even though Hilbert’s tenth problem turned out to have a negative solution, the knowledge gained in developing the methods to prove this result is very significant. What was revealed is that polynomials have considerable expressive powers. This is what we discuss in the next section.

7.2 Diophantine Sets and Listable Sets

We begin by showing that if we can prove that the version of Hilbert’s tenth problem with solutions restricted to belong to \( \mathbb{N} \) is undecidable, then Hilbert’s tenth problem (with solutions in \( \mathbb{Z} \) is undecidable).

Proposition 7.1. If we had an algorithm for solving Hilbert’s tenth problem (with solutions in \( \mathbb{Z} \)), then we would have an algorithm for solving Hilbert’s tenth problem with solutions restricted to belong to \( \mathbb{N} \) (that is, nonnegative integers).

Proof. The above statement is not at all obvious, although its proof is short with the help of some number theory. Indeed, by a theorem of Lagrange (Lagrange’s four square theorem), every natural number \( m \) can be represented as the sum of four squares,

\[
m = a_0^2 + a_1^2 + a_2^2 + a_3^2, \quad a_0, a_1, a_2, a_3 \in \mathbb{Z}.
\]

We reduce Hilbert’s tenth problem restricted to solutions in \( \mathbb{N} \) to Hilbert’s tenth problem (with solutions in \( \mathbb{Z} \)). Given a Diophantine equation \( P(x_1, \ldots, x_n) = 0 \), we can form the polynomial

\[
Q = P(u_1^2 + v_1^2 + y_1^2 + z_1^2, \ldots, u_n^2 + v_n^2 + y_n^2 + z_n^2)
\]

in the \( 4n \) variables \( u_i, v_i, y_i, z_i \) (1 \( \leq \) \( i \) \( \leq \) \( n \)) obtained by replacing \( x_i \) by \( u_i^2 + v_i^2 + y_i^2 + z_i^2 \) for \( i = 1, \ldots, n \). If \( Q = 0 \) has a solution \( (p_1, q_1, r_1, s_1, \ldots, p_n, q_n, r_n, s_n) \) with \( p_i, q_i, r_i, s_i \in \mathbb{Z} \), then if we set \( a_i = p_i^2 + q_i^2 + r_i^2 + s_i^2 \), obviously \( P(a_1, \ldots, a_n) = 0 \) with \( a_i \in \mathbb{N} \). Conversely, if \( P(a_1, \ldots, a_n) = 0 \) with \( a_i \in \mathbb{N} \), then by Lagrange’s theorem there exist some \( p_i, q_i, r_i, s_i \in \mathbb{Z} \) (in fact \( \mathbb{N} \)) such that \( a_i = p_i^2 + q_i^2 + r_i^2 + s_i^2 \) for \( i = 1, \ldots, n \), and the equation \( Q = 0 \) has the solution \( (p_1, q_1, r_1, s_1, \ldots, p_n, q_n, r_n, s_n) \) with \( p_i, q_i, r_i, s_i \in \mathbb{Z} \). Therefore \( Q = 0 \) has a solution \( (p_1, q_1, r_1, s_1, \ldots, p_n, q_n, r_n, s_n) \) with \( p_i, q_i, r_i, s_i \in \mathbb{Z} \) iff \( P = 0 \) has a solution \( (a_1, \ldots, a_n) \) with \( a_i \in \mathbb{N} \). If we had an algorithm to decide whether \( Q \) has a solution with its components in \( \mathbb{Z} \), then we would have an algorithm to decide whether \( P = 0 \) has a solution with its components in \( \mathbb{N} \).

As consequence, the contrapositive of Proposition 7.1 shows that if the version of Hilbert’s tenth problem restricted to solutions in \( \mathbb{N} \) is undecidable, so is Hilbert’s original problem (with solutions in \( \mathbb{Z} \)).

In fact, the Davis-Putnam-Robinson-Matiyasevich theorem establishes the undecidability of the version of Hilbert’s tenth problem restricted to solutions in \( \mathbb{N} \). From now on, we restrict our attention to this version of Hilbert’s tenth problem.
A key idea is to use Diophantine equations with parameters, to define sets of numbers. For example, consider the polynomial

\[ P_1(a, y, z) = (y + 2)(z + 2) - a. \]

For \( a \in \mathbb{N} \) fixed, the equation \((y + 2)(z + 2) - a = 0\), equivalently

\[ a = (y + 2)(z + 2), \]

has a solution with \( y, z \in \mathbb{N} \) iff \( a \) is composite.

If we now consider the polynomial

\[ P_2(a, y, z) = y(2z + 3) - a, \]

for \( a \in \mathbb{N} \) fixed, the equation \( y(2z + 3) - a = 0 \), equivalently

\[ a = y(2z + 3), \]

has a solution with \( y, z \in \mathbb{N} \) iff \( a \) is not a power of 2.

For a slightly more complicated example, consider the polynomial

\[ P_3(a, y) = 3y + 1 - a^2. \]

We leave it as an exercise to show that the natural numbers \( a \) that satisfy the equation \( 3y + 1 - a^2 = 0 \), equivalently

\[ a^2 = 3y + 1, \]

or \((a - 1)(a + 1) = 3y\), are of the form \( a = 3k + 1 \) or \( a = 3k + 2 \), for any \( k \in \mathbb{N} \).

In the first case, if we let \( S_1 \) be the set of composite natural numbers, then we can write

\[ S_1 = \{ a \in \mathbb{N} \mid (\exists y, z)((y + 2)(z + 2) - a = 0) \}, \]

where it is understood that the existentially quantified variables \( y, z \) take their values in \( \mathbb{N} \).

In the second case, if we let \( S_2 \) be the set of natural numbers that are not powers of 2, then we can write

\[ S_2 = \{ a \in \mathbb{N} \mid (\exists y, z)(y(2z + 3) - a = 0) \}. \]

In the third case, if we let \( S_3 \) be the set of natural numbers that are congruent to 1 or 2 modulo 3, then we can write

\[ S_3 = \{ a \in \mathbb{N} \mid (\exists y)(3y + 1 - a^2 = 0) \}. \]

A more explicit Diophantine definition for \( S_3 \) is

\[ S_3 = \{ a \in \mathbb{N} \mid (\exists y)((a - 3y - 1)(a - 3y - 2) = 0) \}. \]

The natural generalization is as follows.
Definition 7.2. A set \( S \subseteq \mathbb{N} \) of natural numbers is \textit{Diophantine} (or \textit{Diophantine definable}) if there is a polynomial \( P(a, x_1, \ldots, x_n) \in \mathbb{Z}[a, x_1, \ldots, x_n] \), with \( n \geq 0 \) such that

\[
S = \{ a \in \mathbb{N} \mid (\exists x_1, \ldots, x_n)(P(a, x_1, \ldots, x_n) = 0) \},
\]

where it is understood that the existentially quantified variables \( x_1, \ldots, x_n \) take their values in \( \mathbb{N} \). More generally, a relation \( R \subseteq \mathbb{N}^m \) is \textit{Diophantine} (\( m \geq 2 \)) if there is a polynomial \( P(a_1, \ldots, a_m, x_1, \ldots, x_n) \in \mathbb{Z}[a_1, \ldots, a_m, x_1, \ldots, x_n] \), with \( n \geq 0 \), such that

\[
R = \{ (a_1, \ldots, a_m) \in \mathbb{N}^m \mid (\exists x_1, \ldots, x_n)(P(a_1, \ldots, a_m, x_1, \ldots, x_n) = 0) \},
\]

where it is understood that the existentially quantified variables \( x_1, \ldots, x_n \) take their values in \( \mathbb{N} \).

For example, the strict order relation \( a_1 < a_2 \) is defined as follows:

\[
a_1 < a_2 \iff (\exists x)(a_1 + 1 + x - a_2 = 0),
\]

and the divisibility relation \( a_1 \mid a_2 \) (\( a_1 \) divides \( a_2 \)) is defined as follows:

\[
a_1 \mid a_2 \iff (\exists x)(a_1 x - a_2 = 0).
\]

What about the ternary relation \( R \subseteq \mathbb{N}^3 \) given by

\[
(a_1, a_2, a_3) \in R \text{ if } a_1 \mid a_2 \text{ and } a_1 < a_3?
\]

At first glance it is not obvious how to “convert” a conjunction of Diophantine definitions into a single Diophantine definition, but we can do this using the following trick: given any finite number of Diophantine equations in the variables \( x_1, \ldots, x_n \),

\[
P_1 = 0, \ P_2 = 0, \ldots, \ P_m = 0,
\]

observe that (*) has a solution \((a_1, \ldots, a_n)\), which means that \( P_i(a_1, \ldots, a_n) = 0 \) for \( i = 1, \ldots, m \), iff the single equation

\[
P_1^2 + P_2^2 + \cdots + P_m^2 = 0\]

also has the solution \((a_1, \ldots, a_n)\). This is because, since \( P_1^2, P_2^2, \ldots, P_m^2 \) are all nonnegative, their sum is equal to zero iff they are all equal to zero, that is \( P_i^2 = 0 \) for \( i = 1 \ldots, m \), which is equivalent to \( P_i = 0 \) for \( i = 1 \ldots, m \).

Using this trick, we see that

\[
(a_1, a_2, a_3) \in R \iff (\exists u, v)((a_1 u - a_2)^2 + (a_1 + 1 + v - a_3)^2 = 0).
\]

We can also define the notion of Diophantine function.

---

1We have to allow \( n = 0 \). Otherwise singleton sets would not be Diophantine.
Definition 7.3. A function $f : \mathbb{N}^n \to \mathbb{N}$ is Diophantine iff its graph $\{(a_1, \ldots, a_n, b) \subseteq \mathbb{N}^{n+1} \mid b = f(a_1, \ldots, a_n)\}$ is Diophantine.

For example, the pairing function $J$ and the projection functions $K, L$ due to Cantor introduced in Section 4.1 are Diophantine, since

$$
\begin{align*}
    z = J(x, y) & \iff (x + y - 1)(x + y) + 2x - 2z = 0 \\
    x = K(z) & \iff (\exists y)((x + y - 1)(x + y) + 2x - 2z = 0) \\
    y = L(z) & \iff (\exists x)((x + y - 1)(x + y) + 2x - 2z = 0).
\end{align*}
$$

How extensive is the family of Diophantine sets? The remarkable fact proved by Davis-Putnam-Robinson-Matiyasevich is that they coincide with the listable sets (the recursively enumerable sets). This is a highly nontrivial result.

The easy direction is the following result.

Proposition 7.2. Every Diophantine set is listable (recursively enumerable).

Proof sketch. Suppose $S$ is given as

$$
S = \{a \in \mathbb{N} \mid (\exists x_1, \ldots, x_n)(P(a, x_1, \ldots, x_n) = 0)\},
$$

Using the extended pairing function $\langle x_1, \ldots, x_n \rangle_n$ of Section 4.1, we enumerate all $n$-tuples $(x_1, \ldots, x_n) \in \mathbb{N}^n$, and during this process we compute $P(a, x_1, \ldots, x_n)$. If $P(a, x_1, \ldots, x_n)$ is zero, then we output $a$, else we go on. This way, $S$ is the range of a computable function, and it is listable.

It is also easy to see that every Diophantine function is partial computable. The main theorem of the theory of Diophantine sets is the following deep result.

Theorem 7.3. (Davis-Putnam-Robinson-Matiyasevich, 1970) Every listable subset of $\mathbb{N}$ is Diophantine. Every partial computable function is Diophantine.

Theorem 7.3 is often referred to as the DPRM theorem. A complete proof of Theorem 7.3 is provided in Davis [6]. As noted by Davis, although the proof is certainly long and nontrivial, it only uses elementary facts of number theory, nothing more sophisticated than the Chinese remainder theorem. Nevertheless, the proof is a tour de force.

One of the most difficult steps is to show that the exponential function $h(n, k) = n^k$ is Diophantine. This is done using the Pell equation. According to Martin Davis, the proof given in Davis [6] uses a combination of ideas from Matiyasevich and Julia Robinson. Matiyasevich’s proof used the Fibonacci numbers.

Using some results from the theory of computation it is now easy to deduce that Hilbert’s tenth problem is undecidable. To achieve this, recall that there are listable sets that are not
computable. For example, it is shown in Lemma 5.11 that \( K = \{ x \in \mathbb{N} \mid \varphi_x(x) \text{ is defined} \} \) is listable but not computable. Since \( K \) is listable, by Theorem 7.3, it is defined by some Diophantine equation

\[
P(a, x_1, \ldots, x_n) = 0,
\]

which means that

\[
K = \{ a \in \mathbb{N} \mid (\exists x_1 \ldots, x_n)(P(a, x_1, \ldots, x_n) = 0) \}.
\]

We have the following strong form of the undecidability of Hilbert’s tenth problem, in the sense that it shows that Hilbert’s tenth problem is already undecidable for a fixed Diophantine equation in one parameter.

**Theorem 7.4.** There is no algorithm which takes as input the polynomial \( P(a, x_1, \ldots, x_n) \) defining \( K \) and any natural number \( a \in \mathbb{N} \) and decides whether

\[
P(a, x_1, \ldots, x_n) = 0.
\]

Consequently, Hilbert’s tenth problem is undecidable.

**Proof.** If there was such an algorithm, then \( K \) would be decidable, a contradiction.

Any algorithm for solving Hilbert’s tenth problem could be used to decide whether or not \( P(a, x_1, \ldots, x_n) = 0 \), but we just showed that there is no such algorithm. \(\square\)

It is an open problem whether Hilbert’s tenth problem is undecidable if we allow rational solutions (that is, \( x_1, \ldots, x_n \in \mathbb{Q} \)).

Alexandra Shlapentokh proved that various extensions of Hilbert’s tenth problem are undecidable. These results deal with some algebraic number theory beyond the scope of these notes. Incidentally, Alexandra was an undergraduate at Penn and she worked on a logic project for me (finding a Gentzen system for a subset of temporal logic).

Having now settled once and for all the undecidability of Hilbert’s tenth problem, we now briefly explore some interesting consequences of Theorem 7.3.

### 7.3 Some Applications of the DPRM Theorem

The first application of the DPRM theorem is a particularly striking way of defining the listable subsets of \( \mathbb{N} \) as the nonnegative ranges of polynomials with integer coefficients. This result is due to Hilary Putnam.

**Theorem 7.5.** For every listable subset \( S \) of \( \mathbb{N} \), there is some polynomial \( Q(x, x_1, \ldots, x_n) \) with integer coefficients such that

\[
S = \{ Q(a, b_1, \ldots, b_n) \mid Q(a, b_1, \ldots, b_n) \in \mathbb{N}, a, b_1, \ldots, b_n \in \mathbb{N} \}.
\]
Proof. By the DPRM theorem (Theorem 7.3), there is some polynomial \( P(x, x_1, \ldots, x_n) \) with integer coefficients such that

\[
S = \{a \in \mathbb{N} \mid (\exists x_1, \ldots, x_n)(P(a, x_1, \ldots, x_n) = 0)\}.
\]

Let \( Q(x, x_1, \ldots, x_n) \) be given by

\[
Q(x, x_1, \ldots, x_n) = (x + 1)(1 - P^2(x, x_1, \ldots, x_n)) - 1.
\]

We claim that \( Q \) satisfies the statement of the theorem. If \( a \in S \), then \( P(a, b_1, \ldots, b_n) = 0 \) for some \( b_1, \ldots, b_n \in \mathbb{N} \), so

\[
Q(a, b_1, \ldots, b_n) = (a + 1)(1 - 0) - 1 = a.
\]

This shows that all \( a \in S \) show up the the nonnegative range of \( Q \). Conversely, assume that \( Q(a, b_1, \ldots, b_n) \geq 0 \) for some \( a, b_1, \ldots, b_n \in \mathbb{N} \). Then by definition of \( Q \) we must have

\[
(a + 1)(1 - P^2(a, b_1, \ldots, b_n)) - 1 \geq 0,
\]

that is,

\[
(a + 1)(1 - P^2(a, b_1, \ldots, b_n)) \geq 1,
\]

and since \( a \in \mathbb{N} \), this implies that \( P^2(a, b_1, \ldots, b_n) < 1 \), but since \( P \) is a polynomial with integer coefficients and \( a, b_1, \ldots, b_n \in \mathbb{N} \), the expression \( P^2(a, b_1, \ldots, b_n) \) must be a nonnegative integer, so we must have

\[
P(a, b_1, \ldots, b_n) = 0,
\]

which shows that \( a \in S \).

Remark: It should be noted that in general, the polynomials \( Q \) arising in Theorem 7.5 may take on negative integer values, and to obtain all listable sets, we must restrict ourself to their nonnegative range.

As an example, the set \( S_3 \) of natural numbers that are congruent to 1 or 2 modulo 3 is given by

\[
S_3 = \{a \in \mathbb{N} \mid (\exists y)(3y + 1 - a^2 = 0)\}.
\]

so by Theorem 7.5, \( S_3 \) is the nonnegative range of the polynomial

\[
Q(x, y) = (x + 1)(1 - (3y + 1 - x^2))^2 - 1
\]

\[
= -(x + 1)((3y - x^2)^2 + 2(3y - x^2))) - 1
\]

\[
= (x + 1)(x^2 - 3y)(2 - (x^2 - 3y)) - 1.
\]

Observe that \( Q(x, y) \) takes on negative values. For example, \( Q(0, 0) = -1 \). Also, in order for \( Q(x, y) \) to be nonnegative, \( (x^2 - 3y)(2 - (x^2 - 3y)) \) must be positive, but this can only happen if \( x^2 - 3y = 1 \), that is, \( x^2 = 3y + 1 \), which is the original equation defining \( S_3 \).
There is no miracle. The nonnegativity of \( Q(x, x_1, \ldots, x_n) \) must subsume the solvability of the equation \( P(x, x_1, \ldots, x_n) = 0 \).

A particularly interesting listable set is the set of primes. By Theorem 7.5, in theory, the set of primes is the positive range of some polynomial with integer coefficients.

Remarkably, some explicit polynomials have been found. This is a nontrivial task. In particular, the process involves showing that the exponential function is definable, which was the stumbling block of the completion of the DPRM theorem for many years.

To give the reader an idea of how the proof begins, observe by the Bezout identity, if \( p = s + 1 \) and \( q = s! \), then we can assert that \( p \) and \( q \) are relatively prime (\( \gcd(p, q) = 1 \)) as the fact that the Diophantine equation

\[
ap - bq = 1
\]

is satisfied for some \( a, b \in \mathbb{N} \). Then, it is not hard to see that \( p \in \mathbb{N} \) is prime iff the following set of equations has a solution for \( a, b, s, r, q \in \mathbb{N} \):

\[
p = s + 1 \\
p = r + 2 \\
q = s! \\
ap - bq = 1.
\]

The problem with the above is that the equation \( q = s! \) is not Diophantine. The next step is to show that the factorial function is Diophantine, and this involves a lot of work. One way to proceed is to show that the above system is equivalent to a system allowing the use of the exponential function. The final step is to show that the exponential function can be eliminated in favor of polynomial equations.

We refer the interested reader to the remarkable expository paper by Davis, Matiyasevich and Robinson [7] for details. Here is a polynomial of total degree 25 in 26 variables (due to J. Jones, D. Sato, H. Wada, D. Wiens) which produces the primes as its positive range:

\[
(k + 2) \left[ 1 - ([wz + h + j - q]^2 + [(gk + 2g + k + 1)(h + j) + h - z]^2 \\
+ [16(k + 1)^3(k + 2)(n + 1)^2 + 1 - f]^2 \\
+ [2n + p + q + z - e]^2 + [e^3(e + 2)(a + 1)^2 + 1 - o]^2 \\
+ [(a^2 - 1)y^2 + 1 - x]^2 + [16n^2y^4(a^2 - 1) + 1 - u]^2 \\
+ [(a + u^2(u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 \\
+ [(a^2 - 1)l^2 + 1 - m]^2 + [ai + k + 1 - l - i]^2 + [n + l + v - y]^2 \\
+ [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 \\
+ [q + y(a + p - 1) + s(2ap + 2a - p^2 - 2p - 2) - x]^2 \\
+ [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2 \right].
\]
Around 2004, Nachi Gupta, an undergraduate student at Penn, and I, tried to produce
the prime 2 as one of the values of the positive range of the above polynomial. It turns out
that this leads to values of the variables that are so large that we never succeeded!

Other interesting applications of the DPRM theorem are the re-statements of famous
open problems, such as the Riemann hypothesis, as the unsolvability of certain Diophantine
equations. For all this, see Davis, Matiyasevich and Robinson [7]. One may also obtain a
nice variant of Gödel’s incompleteness theorem.

## 7.4 Gödel’s Incompleteness Theorem

Gödel published his famous incompleteness theorem in 1931. At the time, his result rocked
the mathematical world, and certainly the community of logicians.

In order to understand why his result had such impact one needs to step back in time.
In the late eighteen hundreds, Hilbert had advanced the thesis that it should be possible
to completely formalize mathematics in such a way that every true statement should be
provable “mechanically.” In modern terminology, Hilbert believed that one could design
a theorem prover that should be complete. His quest is known as Hilbert’s program. In
order to achieve his goal, Hilbert was led to investigate the notion of proof, and with some
collaborators including Ackerman, Hilbert developed a significant amount of what is known
as proof theory. When the young Gödel announced his incompleteness theorem, Hilbert’s
program came to an abrupt halt. Even the quest for a complete proof system for arithmetic
was impossible.

It should be noted that when Gödel proved his incompleteness theorem, computability
theory basically did not exist, so Gödel had to start from scratch. His proof is really a tour
de force. Gödel’s theorem also triggered extensive research on the notion of computability
and undecidability between 1931 and 1936, the major players being Church, Gödel himself,
Herbrand, Kleene, Rosser, Turing, and Post.

In this section we will give a (deceptively) short proof that relies on the DPRM and the
existence of universal functions. The proof is short because the hard work lies in the proof
of the DPRM!

The first step is to translate the fact that there is a universal partial computable function
$\varphi_{\text{univ}}$ (see Proposition 4.5), such that for all $x, y \in \mathbb{N}$, if $\varphi_x$ is the $x$th partial computable
function, then

$$\varphi_x(y) = \varphi_{\text{univ}}(x, y).$$

Also recall from Definition 5.5 that for any acceptable indexing of the partial computable
functions, the c.e sets $W_x$ are given by

$$W_x = \text{dom}(\varphi_x), \quad x \in \mathbb{N}.$$

Since $\varphi_{\text{univ}}$ is a partial computable function, it can be converted into a Diophantine
equation so that we have the following result.
**Theorem 7.6.** (Universal Equation Theorem) There is a Diophantine equation $U(n,a,x_1,\ldots,x_n) = 0$ such that for every c.e. set $W_n$ ($n \in \mathbb{N}$) we have

$$a \in W_n \iff (\exists x_1,\ldots,x_n)(U(n,a,x_1,\ldots,x_n) = 0).$$

**Proof.** We have

$$W_n = \{a \in \mathbb{N} \mid (\exists x_1)(\varphi_{univ}(n,a) = x_1)\},$$

and since $\varphi_{univ}$ is partial computable, by the DPRM (Theorem 7.3), there is Diophantine polynomial $U(n,a,x_1,\ldots,x_n)$ such that

$$x_1 = \varphi_{univ}(n,a) \iff (\exists x_2,\ldots,x_n)(U(n,a,x_1,\ldots,x_n) = 0),$$

and so

$$W_n = \{a \in \mathbb{N} \mid (\exists x_1,\ldots,x_n)(U(n,a,x_1,\ldots,x_n) = 0)\},$$

as claimed. \(\square\)

The Diophantine equation $U(n,a,x_1,\ldots,x_n) = 0$ is called a *universal Diophantine equation*. It is customary to denote $U(n,a,x_1,\ldots,x_n)$ by $P_n(a,x_1,\ldots,x_n)$.

Gödel’s incompleteness theorem applies to sets of logical (first-order) formulae of arithmetic built from the mathematical symbols $0, S, +, \cdot, <$ and the logical connectives $\land, \lor, \neg, \Rightarrow, =, \forall, \exists$. Recall that logical equivalence, $\equiv$, is defined by

$$P \equiv Q \iff (P \Rightarrow Q) \land (Q \Rightarrow P).$$

The term

$$S(S(\cdots(S(0))\cdots))_n$$

is denoted by $S^n(0)$, and represents the natural number $n$.

For example,

$$\exists x(S(S(0))) < (S(S(0)) + x),$$

$$\exists x \exists y \exists z((x > 0) \land (y > 0) \land (z > 0) \land ((x \cdot x + y \cdot y) = z \cdot z)),$$

and

$$\forall x \forall y \forall z((x > 0) \land (y > 0) \land (z > 0) \Rightarrow \neg((x \cdot x \cdot x + y \cdot y \cdot y) = z \cdot z \cdot z))$$

are formulae in the language of arithmetic. All three are true. The first formula is satisfied by $x = S(0)$, the second by $x = S^2(0), y = S^4(0)$ and $z = S^5(0)$ (since $3^2 + 4^2 = 9 + 16 = 25 = 5^2$), and the third formula asserts a special case of Fermat’s famous theorem: for every $n \geq 3$, the equation $x^n + y^n = z^n$ has no solution with $x, y, z \in \mathbb{N}$ and $x > 0, y > 0, z > 0$. The third formula correspond to $n = 4$. Even for this case, the proof is hard.

To be completely rigorous we should explain precisely what is a formal proof. Roughly speaking, a proof system consists of axioms and inference rule. A proof is a certain kind of
7.4. Gödel’s Incompleteness Theorem

tree whose nodes are labeled with formulae, and this tree is constructed in such a way that for every node some inference rule is applied. Such proof systems are presented in Gallier [12, 11]. Here, we rely on an intuitive notion of proof.

Given a polynomial \( P(x_1, \ldots, x_m) \) in \( \mathbb{Z}[x_1, \ldots, x_m] \), we need a way to “prove” that some natural numbers \( n_1, \ldots, n_m \in \mathbb{N} \) are a solution of the Diophantine equation

\[
P(x_1, \ldots, x_m) = 0,
\]

which means that we need to have enough formulae of arithmetic to allow us to simplify the expression \( P(n_1, \ldots, n_m) \) and check whether or not it is equal to zero.

For example, if \( P(x, y) = 2x - 3y - 1 \), we have the solution \( x = 2 \) and \( y = 1 \). What we do is to group all monomials with positive signs, \( 2x \), and all monomials with negative signs, \( 3y + 1 \), plug in the values for \( x \) and \( y \), simplify using the arithmetic tables for + and \( \cdot \), and then compare the results. If they are equal, then we proved that the equation has a solution.

In our language, \( x = S^2(0) \), \( 2x = S^2(0) \cdot x \), and \( y = S^1(0) \), \( 3y + 1 = S^3(0) \cdot y + S(0) \). We need to simplify the expressions

\[
2x = S^2(0) \cdot S^2(0) \quad \text{and} \quad 3y + 1 = S^3(0) \cdot S(0) + S(0).
\]

Using the formulae

\[
S^m(0) + S^n(0) = S^{m+n}(0) \\
S^m(0) \cdot S^n(0) = S^{mn}(0) \\
S^m(0) < S^n(0) \iff m < n,
\]

with \( m, n \in \mathbb{N} \), we simplify \( S^2(0) \cdot S^2(0) \) to \( S^4(0) \), \( S^3(0) \cdot S(0) + S(0) \) to \( S^4(0) \), and we see that the results are equal.

In general, given a polynomial \( P(x_1, \ldots, x_m) \) in \( \mathbb{Z}[x_1, \ldots, x_m] \), we write it as

\[
P(x_1, \ldots, x_m) = P_{\text{pos}}(x_1, \ldots, x_m) - P_{\text{neg}}(x_1, \ldots, x_m),
\]

where \( P_{\text{pos}}(x_1, \ldots, x_m) \) consists of the monomials with positive coefficients, and \( -P_{\text{neg}}(x_1, \ldots, x_m) \) consists of the monomials with negative coefficients. Next we plug in \( S^{n_1}(0), \ldots, S^{n_m}(0) \) in \( P_{\text{pos}}(x_1, \ldots, x_m) \), and evaluate using the formulae for the addition and multiplication tables obtaining a term of the form \( S^p(0) \). Similarly, we plug in \( S^{n_1}(0), \ldots, S^{n_m}(0) \) in \( P_{\text{neg}}(x_1, \ldots, x_m) \), and evaluate using the formulae for the addition and multiplication tables obtaining a term of the form \( S^q(0) \). Then we test in parallel (using the above formulae) whether

\[
S^p(0) = S^q(0), \quad \text{or} \quad S^p(0) < S^q(0), \quad \text{or} \quad S^q(0) < S^p(0).
\]

Only one outcome is possible, and we obtain a proof that either \( P(n_1, \ldots, n_m) = 0 \) or \( P(n_1, \ldots, n_m) \neq 0 \).
A more economical way that does not an infinite number of formulae expressing the addition and multiplication tables is to use various axiomatizations of arithmetic.

One axiomatization known as Robinson arithmetic (R. M. Robinson (1950)) consists of the following seven axioms:

\[
\begin{align*}
\forall x & \neg (S(x) = 0) \\
\forall x \forall y & ((S(x) = S(y)) \Rightarrow (x = y)) \\
\forall y & ((y = 0) \lor \exists x (S(x) = y)) \\
\forall x & (x + 0 = x) \\
\forall x \forall y & (x + S(y) = S(x + y)) \\
\forall x & (x \cdot 0 = 0) \\
\forall x \forall y & (x \cdot S(y) = x \cdot y + x).
\end{align*}
\]

Peano arithmetic is obtained from Robinson arithmetic by adding a rule schema expressing induction:

\[
[\varphi(0) \land \forall n (\varphi(n) \Rightarrow \varphi(n + 1))] \Rightarrow \forall m \varphi(m),
\]

where \(\varphi(x)\) is any (first-order) formula of arithmetic. To deal with \(<\), we also have the axiom

\[
\forall x \forall y (x < y \equiv \exists z (S(z) + x = y)).
\]

It is easy to prove that the formulae

\[
\begin{align*}
S^m(0) + S^n(0) &= S^{m+n}(0) \\
S^m(0) \cdot S^n(0) &= S^{mn}(0) \\
S^m(0) &= S^n(0) \text{ iff } m < n,
\end{align*}
\]

are provable in Robinson arithmetic, and thus in Peano arithmetic (with \(m, n \in \mathbb{N}\)).

Gödel’s incompleteness applies to sets \(\mathcal{A}\) of formulae of arithmetic that are “nice” and strong enough. A set \(\mathcal{A}\) of formulae is nice if it is listable and consistent, which means that it is impossible to prove \(\varphi\) and \(\neg \varphi\) from \(\mathcal{A}\) for some formula \(\varphi\). In other words, \(\mathcal{A}\) is free of contradictions.

Since the axioms of Peano arithmetic are obviously true statements about \(\mathbb{N}\) and since the induction principle holds for \(\mathbb{N}\), the set of all formulae provable in Robinson arithmetic and in Peano arithmetic is consistent. It can also be shown that they are listable.

Here is a rather strong version of Gödel’s incompleteness from Davis, Matiyasevich and Robinson [7].

**Theorem 7.7.** (Gödel’s Incompleteness Theorem) Let \(\mathcal{A}\) be a set of formulae of arithmetic satisfying the following properties:

(a) The set \(\mathcal{A}\) is consistent.
(b) The set $A$ is listable (c.e.)

(c) The set $A$ is strong enough to prove all formulae

\[ S^m(0) + S^n(0) = S^{m+n}(0) \]
\[ S^m(0) \cdot S^n(0) = S^{mn}(0) \]
\[ S^m(0) < S^n(0) \quad \text{iff} \quad m < n, \]

for all $m, n \in \mathbb{N}$.

Then we can construct a Diophantine equation $F(x_1, \ldots, x_m) = 0$ corresponding to $A$ such that $F(x_1, \ldots, x_m) = 0$ has no solution with $x_1, \ldots, x_m \in \mathbb{N}$ but the formula

\[ \neg(\exists x_1, \ldots, x_m)(F(x_1, \ldots, x_m) = 0) \]

is not provable from $A$. In other words, there is a true statement of arithmetic not provable from $A$; that is, $A$ is incomplete.

**Proof.** Define the subset $A \subseteq \mathbb{N}$ as follows:

\[ A = \{ a \in \mathbb{N} \mid \neg(\exists x_1, \ldots, x_n)(P_a(a, x_1, \ldots, x_n) = 0) \text{ is provable from } A \}, \]  

where $P_n(a, x_1, \ldots, x_n)$ is defined just after Proposition 7.6. Because by (b) $A$ is listable, it is easy to see (because the set of formulae provable from a listable set is listable) that $A$ is listable, so by the DPRM $A$ is Diophantine, and by Proposition 7.6, there is some $k \in \mathbb{N}$ such that

\[ A = W_k = \{ a \in \mathbb{N} \mid (\exists x_1, \ldots, x_n)(P_k(a, x_1, \ldots, x_n) = 0) \}. \]

The trick is now to see whether $k \in W_k$ or not.

We claim that $k \notin W_k$.

We proceed by contradiction. Assume that $k \in W_k$. This means that

\[ (\exists x_1, \ldots, x_n)(P_k(k, x_1, \ldots, x_n) = 0), \]  

and since $A = W_k$, by (**), that

\[ \neg(\exists x_1, \ldots, x_n)(P_k(k, x_1, \ldots, x_n) = 0) \text{ is provable from } A. \]  

By (†1) and (c), since the equation $P_k(k, x_1, \ldots, x_n) = 0$ has a solution, we can prove the formula

\[ (\exists x_1, \ldots, x_n)(P_k(k, x_1, \ldots, x_n) = 0) \]

from $A$. By (†2), the formula $\neg(\exists x_1, \ldots, x_n)(P_k(k, x_1, \ldots, x_n) = 0)$ is provable from $A$, but since $(\exists x_1, \ldots, x_n)(P_k(k, x_1, \ldots, x_n) = 0)$ is also provable from $A$, this contradicts the fact that $A$ is consistent (which is hypothesis (a)).

Therefore we must have $k \notin W_k$. This means that $P_k(k, x_1, \ldots, x_n) = 0$ has no solution with $x_1, \ldots, x_n \in \mathbb{N}$, and since $A = W_k$, the formula

\[ \neg(\exists x_1, \ldots, x_n)(P_a(a, x_1, \ldots, x_n) = 0) \]

is not provable from $A$. \qed
As a corollary of Theorem 7.7, since the theorems provable in Robinson arithmetic satisfy (a), (b), (c), we deduce that there are true theorems of arithmetic not provable in Robinson arithmetic; in short, Robinson arithmetic is incomplete. Since Robinson arithmetic does not have induction axioms, this shows that induction is not the culprit behind incompleteness. Since Peano arithmetic is an extension (consistent) of Robinson arithmetic, it is also incomplete. This is Gödel’s original incompleteness theorem, but Gödel had to develop from scratch the tools needed to prove his result, so his proof is very different (and a tour de force).

But the situation is even more dramatic. Adding a true unprovable statement to a set $A$ satisfying (a), (b), (c) preserves properties (a), (b), (c), so there is no escape from incompleteness (unless perhaps we allow unreasonable sets of formulae violating (b)).

Gödel’s incompleteness theorem is a negative result, in the sense that it shows that there is no hope of obtaining proof systems capable of proving all true statements for various mathematical theories such as arithmetic. We can also view Gödel’s incompleteness theorem positively as evidence that mathematicians will never be replaced by computers! There is always room for creativity.

The true but unprovable formulae arising in Gödel’s incompleteness theorem are rather contrived and by no means “natural.” For many years after Gödel’s proof was published logicians looked for natural incompleteness phenomena. In the early 1980’s such results were found, starting with a result of Kirby and Paris. Harvey Friedman then found more spectacular instances of natural incompleteness, one of which involves a finite miniaturization of Kruskal’s tree theorem. The proof of such results uses some deep methods of proof theory involving a tool known as ordinal notations. A survey of such results can be found in Gallier [8].
Chapter 8

The Post Correspondence Problem; Applications to Undecidability Results

8.1 The Post Correspondence Problem

The Post correspondence problem (due to Emil Post) is another undecidable problem that turns out to be a very helpful tool for proving problems in logic or in formal language theory to be undecidable.

Let $\Sigma$ be an alphabet with at least two letters. An instance of the Post Correspondence problem (for short, PCP) is given by two sequences $U = (u_1, \ldots, u_m)$ and $V = (v_1, \ldots, v_m)$, of strings $u_i, v_i \in \Sigma^*$.

The problem is to find whether there is a (finite) sequence $(i_1, \ldots, i_p)$, with $i_j \in \{1, \ldots, m\}$ for $j = 1, \ldots, p$, so that

$$u_{i_1} u_{i_2} \cdots u_{i_p} = v_{i_1} v_{i_2} \cdots v_{i_p}.$$ 

Equivalently, an instance of the PCP is a sequence of pairs

$$(u_1, v_1), \ldots, (u_m, v_m).$$

For example, consider the following problem:

$$(abab, ababaa), (aaabbb, bb), (aab, baab), (ba, baa), (ab, ba), (aa, a).$$

There is a solution for the string 1234556:

$$abab aababb aab ba ab ab a = ababaa bb baab baa ba ba a.$$ 

We are beginning to suspect that this is a hard problem. Indeed, it is undecidable!
Theorem 8.1. (Emil Post, 1946) The Post correspondence problem is undecidable, provided that the alphabet $\Sigma$ has at least two symbols.

There are several ways of proving Theorem 8.1, but the strategy is more or less the same: Reduce the halting problem to the PCP, by encoding sequences of ID’s as partial solutions of the PCP.

For instance, this can be done for RAM programs. The first step is to show that every RAM program can be simulated by a single register RAM program.

Then, the halting problem for RAM programs with one register is reduced to the PCP (using the fact that only four kinds of instructions are needed). A proof along these lines was given by Dana Scott.

8.2 Some Undecidability Results for CFG’s

Theorem 8.2. It is undecidable whether a context-free grammar is ambiguous.

Proof. We reduce the PCP to the ambiguity problem for CFG’s. Given any instance $U = (u_1, \ldots, u_m)$ and $V = (v_1, \ldots, v_m)$ of the PCP, let $c_1, \ldots, c_m$ be $m$ new symbols, and consider the following languages:

\[
L_U = \{u_{i_1} \cdots u_{i_p} c_{i_p} \cdots c_{i_1} \mid 1 \leq i_j \leq m, \\
1 \leq j \leq p, p \geq 1\}, \\
L_V = \{v_{i_1} \cdots v_{i_p} c_{i_p} \cdots c_{i_1} \mid 1 \leq i_j \leq m, \\
1 \leq j \leq p, p \geq 1\},
\]

and $L_{U,V} = L_U \cup L_V$.

We can easily construct a CFG, $G_{U,V}$, generating $L_{U,V}$. The productions are:

\[
S \rightarrow S_U \\
S \rightarrow S_V \\
S_U \rightarrow u_i S_U c_i \\
S_U \rightarrow u_i c_i \\
S_V \rightarrow v_i S_V c_i \\
S_V \rightarrow v_i c_i.
\]

It is easily seen that the PCP for $(U, V)$ has a solution iff $L_U \cap L_V \neq \emptyset$ iff $G$ is ambiguous. \qed
Remark: As a corollary, we also obtain the following result: It is undecidable for arbitrary context-free grammars $G_1$ and $G_2$ whether $L(G_1) \cap L(G_2) = \emptyset$ (see also Theorem 8.4).

Recall that the computations of a Turing Machine, $M$, can be described in terms of instantaneous descriptions, upav.

We can encode computations

$$ID_0 \vdash ID_1 \vdots \vdash ID_n$$

halting in a proper ID, as the language, $L_M$, consisting all of strings

$$w_0 \# w_1^R \# w_2 \# w_3^R \# \cdots \# w_{2k} \# w_{2k+1}^R,$$

or

$$w_0 \# w_1^R \# w_2 \# w_3^R \# \cdots \# w_{2k-2} \# w_{2k-1}^R \# w_{2k},$$

where $k \geq 0$, $w_0$ is a starting ID, $w_i \vdash w_{i+1}$ for all $i$ with $0 \leq i < 2k + 1$ and $w_{2k+1}$ is proper halting ID in the first case, $0 \leq i < 2k$ and $w_{2k}$ is proper halting ID in the second case.

The language $L_M$ turns out to be the intersection of two context-free languages $L_0^0_M$ and $L_1^1_M$ defined as follows:

1. The strings in $L_0^0_M$ are of the form

$$w_0 \# w_1^R \# w_2 \# w_3^R \# \cdots \# w_{2k} \# w_{2k+1}^R$$

or

$$w_0 \# w_1^R \# w_2 \# w_3^R \# \cdots \# w_{2k-2} \# w_{2k-1}^R \# w_{2k},$$

where $w_{2i} \vdash w_{2i+1}$ for all $i \geq 0$, and $w_{2k}$ is a proper halting ID in the second case.

2. The strings in $L_1^1_M$ are of the form

$$w_0 \# w_1^R \# w_2 \# w_3^R \# \cdots \# w_{2k} \# w_{2k+1}^R$$

or

$$w_0 \# w_1^R \# w_2 \# w_3^R \# \cdots \# w_{2k-2} \# w_{2k-1}^R \# w_{2k},$$

where $w_{2i+1} \vdash w_{2i+2}$ for all $i \geq 0$, $w_0$ is a starting ID, and $w_{2k+1}$ is a proper halting ID in the first case.

Theorem 8.3. Given any Turing machine $M$, the languages $L_0^0_M$ and $L_1^1_M$ are context-free, and $L_M = L_0^0_M \cap L_1^1_M$.

Proof. We can construct PDA’s accepting $L_0^0_M$ and $L_1^1_M$. It is easily checked that $L_M = L_0^0_M \cap L_1^1_M$.

As a corollary, we obtain the following undecidability result:
Theorem 8.4. It is undecidable for arbitrary context-free grammars $G_1$ and $G_2$ whether $L(G_1) \cap L(G_2) = \emptyset$.

Proof. We can reduce the problem of deciding whether a partial recursive function is undefined everywhere to the above problem. By Rice’s theorem, the first problem is undecidable.

However, this problem is equivalent to deciding whether a Turing machine never halts in a proper ID. By Theorem 8.3, the languages $L^0_M$ and $L^1_M$ are context-free. Thus, we can construct context-free grammars $G_1$ and $G_2$ so that $L^0_M = L(G_1)$ and $L^1_M = L(G_2)$. Then, $M$ never halts in a proper ID iff $L_M = \emptyset$ iff (by Theorem 8.3), $L_M = L(G_1) \cap L(G_2) = \emptyset$. \qed

Given a Turing machine $M$, the language $L_M$ is defined over the alphabet $\Delta = \Gamma \cup Q \cup \{\#\}$. The following fact is also useful to prove undecidability:

Theorem 8.5. Given any Turing machine $M$, the language $\Delta^* - L_M$ is context-free.

Proof. One can easily check that the conditions for not belonging to $L_M$ can be checked by a PDA. \qed

As a corollary, we obtain:

Theorem 8.6. Given any context-free grammar, $G = (V, \Sigma, P, S)$, it is undecidable whether $L(G) = \Sigma^*$.

Proof. We can reduce the problem of deciding whether a Turing machine never halts in a proper ID to the above problem.

Indeed, given $M$, by Theorem 8.5, the language $\Delta^* - L_M$ is context-free. Thus, there is a CFG, $G$, so that $L(G) = \Delta^* - L_M$. However, $M$ never halts in a proper ID iff $L_M = \emptyset$ iff $L(G) = \Delta^*$. \qed

As a consequence, we also obtain the following:

Theorem 8.7. Given any two context-free grammar, $G_1$ and $G_2$, and any regular language, $R$, the following facts hold:

1. $L(G_1) = L(G_2)$ is undecidable.
2. $L(G_1) \subseteq L(G_2)$ is undecidable.
3. $L(G_1) = R$ is undecidable.
4. $R \subseteq L(G_2)$ is undecidable.

In contrast to (4), the property $L(G_1) \subseteq R$ is decidable!
8.3 More Undecidable Properties of Languages; Greibach’s Theorem

We conclude with a nice theorem of S. Greibach, which is a sort of version of Rice’s theorem for families of languages.

Let $\mathcal{L}$ be a countable family of languages. We assume that there is a coding function $c: \mathcal{L} \to \mathbb{N}$ and that this function can be extended to code the regular languages (all alphabets are subsets of some given countably infinite set).

We also assume that $\mathcal{L}$ is effectively closed under union, and concatenation with the regular languages.

This means that given any two languages $L_1$ and $L_2$ in $\mathcal{L}$, we have $L_1 \cup L_2 \in \mathcal{L}$, and $c(L_1 \cup L_2)$ is given by a recursive function of $c(L_1)$ and $c(L_2)$, and that for every regular language $R$, we have $L_1 R \in \mathcal{L}$, $RL_1 \in \mathcal{L}$, and $c(RL_1)$ and $c(L_1 R)$ are recursive functions of $c(R)$ and $c(L_1)$.

Given any language, $L \subseteq \Sigma^*$, and any string, $w \in \Sigma^*$, we define $L/w$ by

$$L/w = \{u \in \Sigma^* | uw \in L\}.$$  

**Theorem 8.8.** (Greibach) Let $\mathcal{L}$ be a countable family of languages that is effectively closed under union, and concatenation with the regular languages, and assume that the problem $L = \Sigma^*$ is undecidable for $L \in \mathcal{L}$ and any given sufficiently large alphabet $\Sigma$. Let $P$ be any nontrivial property of languages that is true for the regular languages, and so that if $P(L)$ holds for any $L \in \mathcal{L}$, then $P(L/a)$ also holds for any letter $a$. Then, $P$ is undecidable for $\mathcal{L}$.

**Proof.** Since $P$ is nontrivial for $\mathcal{L}$, there is some $L_0 \in \mathcal{L}$ so that $P(L_0)$ is false.

Let $\Sigma$ be large enough, so that $L_0 \subseteq \Sigma^*$, and the problem $L = \Sigma^*$ is undecidable for $L \in \mathcal{L}$.

We show that given any $L \in \mathcal{L}$, with $L \subseteq \Sigma^*$, we can construct a language $L_1 \in \mathcal{L}$, so that $L = \Sigma^*$ iff $P(L_1)$ holds. Thus, the problem $L = \Sigma^*$ for $L \in \mathcal{L}$ reduces to property $P$ for $\mathcal{L}$, and since for $\Sigma$ big enough, the first problem is undecidable, so is the second.

For any $L \in \mathcal{L}$, with $L \subseteq \Sigma^*$, let

$$L_1 = L_0 \# \Sigma^* \cup \Sigma^* \# L.$$ 

Since $\mathcal{L}$ is effectively closed under union and concatenation with the regular languages, we have $L_1 \in \mathcal{L}$.

If $L = \Sigma^*$, then $L_1 = \Sigma^* \# \Sigma^*$, a regular language, and thus, $P(L_1)$ holds, since $P$ holds for the regular languages.

Conversely, we would like to prove that if $L \neq \Sigma^*$, then $P(L_1)$ is false.
Since \( L \neq \Sigma^* \), there is some \( w \notin L \). But then,
\[
L_1/\#w = L_0.
\]
Since \( P \) is preserved under quotient by a single letter, by a trivial induction, if \( P(L_1) \) holds, then \( P(L_0) \) also holds. However, \( P(L_0) \) is false, so \( P(L_1) \) must be false.

Thus, we proved that \( L = \Sigma^* \) iff \( P(L_1) \) holds, as claimed.

Greibach’s theorem can be used to show that it is undecidable whether a context-free grammar generates a regular language.

It can also be used to show that it is undecidable whether a context-free language is inherently ambiguous.
Chapter 9

Computational Complexity; \( \mathcal{P} \) and \( \mathcal{NP} \)

9.1 The Class \( \mathcal{P} \)

In the previous two chapters, we clarified what it means for a problem to be decidable or undecidable. This chapter is heavily inspired by Lewis and Papadimitriou’s excellent treatment [17].

In principle, if a problem is decidable, then there is an algorithm (i.e., a procedure that halts for every input) that decides every instance of the problem.

However, from a practical point of view, knowing that a problem is decidable may be useless, if the number of steps (time complexity) required by the algorithm is excessive, for example, exponential in the size of the input, or worse.

For instance, consider the traveling salesman problem, which can be formulated as follows:

We have a set \( \{c_1, \ldots, c_n\} \) of cities, and an \( n \times n \) matrix \( D = (d_{ij}) \) of nonnegative integers, the distance matrix, where \( d_{ij} \) denotes the distance between \( c_i \) and \( c_j \), which means that \( d_{ii} = 0 \) and \( d_{ij} = d_{ji} \) for all \( i \neq j \).

The problem is to find a shortest tour of the cities, that is, a permutation \( \pi \) of \( \{1, \ldots, n\} \) so that the cost

\[
C(\pi) = d_{\pi(1)\pi(2)} + d_{\pi(2)\pi(3)} + \cdots + d_{\pi(n-1)\pi(n)} + d_{\pi(n)\pi(1)}
\]

is as small as possible (minimal).

One way to solve the problem is to consider all possible tours, i.e., \( n! \) permutations.

Actually, since the starting point is irrelevant, we need only consider \( (n-1)! \) tours, but this still grows very fast. For example, when \( n = 40 \), it turns out that \( 39! \) exceeds \( 10^{45} \), a huge number.
Consider the $4 \times 4$ symmetric matrix given by
\[
D = \begin{pmatrix}
0 & 2 & 1 & 1 \\
2 & 0 & 1 & 1 \\
1 & 1 & 0 & 3 \\
1 & 1 & 3 & 0
\end{pmatrix},
\]
and the budget $B = 4$. The tour specified by the permutation
\[
\pi = \begin{pmatrix}
1 & 2 & 3 & 4 \\
1 & 4 & 2 & 3
\end{pmatrix}
\]
has cost 4, since
\[
c(\pi) = d_{\pi(1)\pi(2)} + d_{\pi(2)\pi(3)} + d_{\pi(3)\pi(4)} + d_{\pi(4)\pi(1)} \\
= d_{14} + d_{42} + d_{23} + d_{31} \\
= 1 + 1 + 1 + 1 = 4.
\]
The cities in this tour are traversed in the order
\[
(1, 4, 2, 3, 1).
\]

**Remark:** The permutation $\pi$ shown above is described in Cauchy’s *two-line notation*,
\[
\pi = \begin{pmatrix}
1 & 2 & 3 & 4 \\
1 & 4 & 2 & 3
\end{pmatrix}
\]
where every element in the second row is the image of the element immediately above it in the first row: thus
\[
\pi(1) = 1, \ \pi(2) = 4, \ \pi(3) = 2, \ \pi(4) = 3.
\]

Thus, to capture the essence of practically feasible algorithms, we must limit our computational devices to run only for a number of steps that is bounded by a *polynomial* in the length of the input.

We are led to the definition of polynomially bounded computational models.

**Definition 9.1.** A deterministic Turing machine $M$ is said to be *polynomially bounded* if there is a polynomial $p(X)$ so that the following holds: For every input $x \in \Sigma^*$, there is no ID $ID_n$ so that
\[
ID_0 \vdash ID_1 \vdash^* ID_{n-1} \vdash ID_n, \quad \text{with} \quad n > p(|x|),
\]
where $ID_0 = q_0 x$ is the starting ID.

A language $L \subseteq \Sigma^*$ is *polynomially decidable* if there is a polynomially bounded Turing machine that accepts $L$. The family of all polynomially decidable languages is denoted by $\mathcal{P}$. 
Remark: Even though Definition 9.1 is formulated for Turing machines, it can also be formulated for other models, such as RAM programs.

The reason is that the conversion of a Turing machine into a RAM program (and vice versa) produces a program (or a machine) whose size is polynomial in the original device.

The following proposition, although trivial, is useful:

**Proposition 9.1.** The class \( \mathcal{P} \) is closed under complementation.

Of course, many languages do not belong to \( \mathcal{P} \). One way to obtain such languages is to use a diagonal argument. But there are also many natural languages that are not in \( \mathcal{P} \), although this may be very hard to prove for some of these languages.

Let us consider a few more problems in order to get a better feeling for the family \( \mathcal{P} \).

### 9.2 Directed Graphs, Paths

Recall that a **directed graph**, \( G \), is a pair \( G = (V, E) \), where \( E \subseteq V \times V \). Every \( u \in V \) is called a **node** (or **vertex**) and a pair \( (u, v) \in E \) is called an **edge** of \( G \).

We will restrict ourselves to **simple graphs**, that is, graphs without edges of the form \( (u, u) \); equivalently, \( G = (V, E) \) is a simple graph if whenever \( (u, v) \in E \), then \( u \neq v \).

Given any two nodes \( u, v \in V \), a **path from \( u \) to \( v \)** is any sequence of \( n + 1 \) edges \((n \geq 0)\)

\[(u, v_1), (v_1, v_2), \ldots, (v_n, v).\]

(If \( n = 0 \), a path from \( u \) to \( v \) is simply a single edge, \((u, v)\).)

A graph \( G \) is **strongly connected** if for every pair \( (u, v) \in V \times V \), there is a path from \( u \) to \( v \). A **closed path, or cycle**, is a path from some node \( u \) to itself.

We will restrict our attention to finite graphs, i.e. graphs \((V, E)\) where \( V \) is a finite set.

**Definition 9.2.** Given a graph \( G \), an **Eulerian cycle** is a cycle in \( G \) that passes through all the nodes (possibly more than once) and every edge of \( G \) exactly once. A **Hamiltonian cycle** is a cycle that passes through all the nodes exactly once (note, some edges may not be traversed at all).

**Eulerian Cycle Problem:** Given a graph \( G \), is there an Eulerian cycle in \( G \)?

**Hamiltonian Cycle Problem:** Given a graph \( G \), is there an Hamiltonian cycle in \( G \)?
9.3 Eulerian Cycles

The following graph is a directed graph version of the Königsberg bridge problem, solved by Euler in 1736.

The nodes $A, B, C, D$ correspond to four areas of land in Königsberg and the edges to the seven bridges joining these areas of land.

![Directed graph modeling the Königsberg bridge problem](image)

The problem is to find a closed path that crosses every bridge exactly once and returns to the starting point.

In fact, the problem is unsolvable, as shown by Euler, because some nodes do not have the same number of incoming and outgoing edges (in the undirected version of the problem, some nodes do not have an even degree.)

It may come as a surprise that the Eulerian Cycle Problem does have a polynomial time algorithm, but that so far, not such algorithm is known for the Hamiltonian Cycle Problem.

The reason why the Eulerian Cycle Problem is decidable in polynomial time is the following theorem due to Euler:

**Theorem 9.2.** A graph $G = (V, E)$ has an Eulerian cycle iff the following properties hold:

1. The graph $G$ is strongly connected.
2. Every node has the same number of incoming and outgoing edges.

Proving that properties (1) and (2) hold if $G$ has an Eulerian cycle is fairly easy. The converse is harder, but not that bad (try!).
Theorem 9.2 shows that it is necessary to check whether a graph is strongly connected. This can be done by computing the transitive closure of $E$, which can be done in polynomial time (in fact, $O(n^3)$).

Checking property (2) can clearly be done in polynomial time. Thus, the Eulerian cycle problem is in $\mathcal{P}$.

Unfortunately, no theorem analogous to Theorem 9.2 is known for Hamiltonian cycles.

## 9.4 Hamiltonian Cycles

A game invented by Sir William Hamilton in 1859 uses a regular solid dodecahedron whose twenty vertices are labeled with the names of famous cities.

The player is challenged to “travel around the world” by finding a closed cycle along the edges of the dodecahedron which passes through every city exactly once (this is the undirected version of the Hamiltonian cycle problem).

In graphical terms, assuming an orientation of the edges between cities, the graph $D$ shown in Figure 9.2 is a plane projection of a regular dodecahedron and we want to know if there is a Hamiltonian cycle in this directed graph.

![Figure 9.2: A tour “around the world.”](image-url)
Finding a Hamiltonian cycle in this graph does not appear to be so easy!
A solution is shown in Figure 9.3 below.

Figure 9.3: A Hamiltonian cycle in $D$.

Remark: We talked about problems being decidable in polynomial time. Obviously, this is equivalent to deciding some property of a certain class of objects, for example, finite graphs.

Our framework requires that we first encode these classes of objects as strings (or numbers), since $\mathcal{P}$ consists of languages.

Thus, when we say that a property is decidable in polynomial time, we are really talking about the encoding of this property as a language. Thus, we have to be careful about these encodings, but it is rare that encodings cause problems.

9.5 Propositional Logic and Satisfiability

We define the syntax and the semantics of propositions in conjunctive normal form (CNF).
The syntax has to do with the legal form of propositions in CNF. Such propositions are interpreted as truth functions, by assigning truth values to their variables.

We begin by defining propositions in CNF. Such propositions are constructed from a countable set, \( PV \), of propositional (or boolean) variables, say

\[
PV = \{ x_1, x_2, \ldots \},
\]

using the connectives \( \wedge \) (and), \( \vee \) (or) and \( \neg \) (negation).

We define a literal (or atomic proposition), \( L \), as \( L = x \) or \( L = \neg x \), also denoted by \( \overline{x} \), where \( x \in PV \).

A clause, \( C \), is a disjunction of pairwise distinct literals,

\[
C = (L_1 \vee L_2 \vee \cdots \vee L_m).
\]

Thus, a clause may also be viewed as a nonempty set

\[
C = \{ L_1, L_2, \ldots, L_m \}.
\]

We also have a special clause, the empty clause, denoted \( \bot \) or \( \square \) (or \( \{ \} \)). It corresponds to the truth value false.

A proposition in CNF, or boolean formula, \( P \), is a conjunction of pairwise distinct clauses

\[
P = C_1 \wedge C_2 \wedge \cdots \wedge C_n.
\]

Thus, a boolean formula may also be viewed as a nonempty set

\[
P = \{ C_1, \ldots, C_n \},
\]

but this time, the comma is interpreted as conjunction. We also allow the proposition \( \bot \), and sometimes the proposition \( \top \) (corresponding to the truth value true).

For example, here is a boolean formula:

\[
P = \{ (x_1 \vee x_2 \vee x_3), (\overline{x_1} \vee x_2), (\overline{x_2} \vee x_3), (\overline{x_3} \vee x_1), (\overline{x_1} \vee \overline{x_2} \vee \overline{x_3}) \}.
\]

In order to interpret boolean formulæ, we use truth assignments.

We let \( BOOL = \{ F, T \} \), the set of truth values, where \( F \) stands for false and \( T \) stands for true.

A truth assignment (or valuation), \( v \), is any function \( v : PV \rightarrow BOOL \).

For example, the function \( v_F : PV \rightarrow BOOL \) given by

\[
v_F(x_i) = F \quad \text{for all } i \geq 1
\]
is a truth assignment, and so is the function $v_T: PV \rightarrow BOOL$ given by

$$v_T(x_i) = T \quad \text{for all } i \geq 1.$$ 

The function $v: PV \rightarrow BOOL$ given by

$$v(x_1) = T,$$
$$v(x_2) = F,$$
$$v(x_3) = T,$$
$$v(x_i) = T \quad \text{for all } i \geq 4$$

is also a truth assignment.

Given a truth assignment $v: PV \rightarrow BOOL$, we define the truth value $\hat{v}(X)$ of a literal, clause, and boolean formula, $X$, using the following recursive definition:

1. $\hat{v}(\bot) = F$, $\hat{v}(\top) = T$.
2. $\hat{v}(x) = v(x)$, if $x \in PV$.
3. $\hat{v}(\overline{x}) = \overline{v(x)}$, where $\overline{v(x)} = F$ if $v(x) = T$ and $\overline{v(x)} = T$ if $v(x) = F$.
4. $\hat{v}(C) = F$ if $C$ is a clause and iff $\hat{v}(L_i) = F$ for all literals $L_i$ in $C$, otherwise $T$.
5. $\hat{v}(P) = T$ if $P$ is a boolean formula and iff $\hat{v}(C_j) = T$ for all clauses $C_j$ in $P$, otherwise $F$.

Since a boolean formula $P$ only contains a finite number of variables, say $\{x_{i_1}, \ldots, x_{i_n}\}$, one should expect that its truth value $\hat{v}(P)$ depends only on the truth values assigned by the truth assignment $v$ to the variables in the set $\{x_{i_1}, \ldots, x_{i_n}\}$, and this is indeed the case. The following proposition is easily shown by induction on the depth of $P$ (viewed as a tree).

**Proposition 9.3.** Let $P$ be a boolean formula containing the set of variables $\{x_{i_1}, \ldots, x_{i_n}\}$. If $v_1: PV \rightarrow BOOL$ and $v_2: PV \rightarrow BOOL$ are any truth assignments agreeing on the set of variables $\{x_{i_1}, \ldots, x_{i_n}\}$, which means that

$$v_1(x_{i_j}) = v_2(x_{i_j}) \quad \text{for } j = 1, \ldots, n,$$

then $\hat{v}_1(P) = \hat{v}_2(P)$.

In view of Proposition 9.3, given any boolean formula $P$, we only need to specify the values of a truth assignment $v$ for the variables occurring on $P$. For example, given the boolean formula

$$P = \{(x_1 \lor x_2 \lor x_3), (\overline{x_1} \lor x_2), (x_2 \lor x_3), (x_3 \lor x_1), (\overline{x_1} \lor x_2 \lor \overline{x_3})\},$$
we only need to specify \( v(x_1), v(x_2), v(x_3) \). Thus there are \( 2^3 = 8 \) distinct truth assignments:

\[
\begin{array}{c|c|c}
F, F, F & T, F, F \\
F, F, T & T, F, T \\
F, T, F & T, T, F \\
F, T, T & T, T, T \\
\end{array}
\]

In general, there are \( 2^n \) distinct truth assignments to \( n \) distinct variables.

Here is an example showing the evaluation of the truth value \( \hat{v}(P) \) for the boolean formula

\[
P = (x_1 \lor x_2 \lor x_3) \land (\overline{x_1} \lor x_2) \land (x_2 \lor x_3) \land (\overline{x_3} \lor x_1) \land (\overline{x_1} \lor \overline{x_2} \lor \overline{x_3})
\]

\[
= \{(x_1 \lor x_2 \lor x_3), (\overline{x_1} \lor x_2), (x_2 \lor x_3), (\overline{x_3} \lor x_1), (\overline{x_1} \lor \overline{x_2} \lor \overline{x_3})\},
\]

and the truth assignment

\[
v(x_1) = T, \quad v(x_2) = F, \quad v(x_3) = F.
\]

For the literals, we have

\[
\hat{v}(x_1) = T, \quad \hat{v}(x_2) = F, \quad \hat{v}(x_3) = F, \quad \hat{v}(\overline{x_1}) = F, \quad \hat{v}(\overline{x_2}) = T, \quad \hat{v}(\overline{x_3}) = T,
\]

for the clauses

\[
\hat{v}(x_1 \lor x_2 \lor x_3) = \hat{v}(x_1) \lor \hat{v}(x_2) \lor \hat{v}(x_3) = T \lor F \lor F = T,
\]

\[
\hat{v}(\overline{x_1} \lor x_2) = \hat{v}(\overline{x_1}) \lor \hat{v}(x_2) = F \lor F = F,
\]

\[
\hat{v}(x_2 \lor x_3) = \hat{v}(x_2) \lor \hat{v}(x_3) = T \lor F = T,
\]

\[
\hat{v}(\overline{x_3} \lor x_1) = \hat{v}(\overline{x_3}) \lor \hat{v}(x_1) = T \lor T = T,
\]

\[
\hat{v}(\overline{x_1} \lor \overline{x_2} \lor \overline{x_3}) = \hat{v}(\overline{x_1}) \lor \hat{v}(\overline{x_2}) \lor \hat{v}(\overline{x_3}) = F \lor T \lor T = T,
\]

and for the conjunction of the clauses,

\[
\hat{v}(P) = \hat{v}(x_1 \lor x_2 \lor x_3) \land \hat{v}(\overline{x_1} \lor x_2) \land \hat{v}(x_2 \lor x_3) \land \hat{v}(\overline{x_3} \lor x_1) \land \hat{v}(\overline{x_1} \lor \overline{x_2} \lor \overline{x_3})
\]

\[
= T \land F \land T \land T \land T = F.
\]

Therefore, \( \hat{v}(P) = F \).

**Definition 9.3.** We say that a truth assignment \( v \) satisfies a boolean formula \( P \), if \( \hat{v}(P) = T \). In this case, we also write

\[
v \models P.
\]

A boolean formula \( P \) is satisfiable if \( v \models P \) for some truth assignment \( v \), otherwise, it is unsatisfiable. A boolean formula \( P \) is valid (or a tautology) if \( v \models P \) for all truth assignments \( v \), in which case we write

\[
\models P.
\]
One should check that the boolean formula

\[ P = \{(x_1 \lor x_2 \lor x_3), (\overline{x_1} \lor x_2), (\overline{x_2} \lor x_3), (\overline{x_3} \lor x_1), (x_1 \lor x_2 \lor \overline{x_3})\} \]

is unsatisfiable.

One may think that it is easy to test whether a proposition is satisfiable or not. Try it, it is not that easy!

As a matter of fact, the satisfiability problem, testing whether a boolean formula is satisfiable, also denoted SAT, is not known to be in \( \mathcal{P} \).

Moreover, it is an NP-complete problem. Most people believe that the satisfiability problem is not in \( \mathcal{P} \), but a proof still eludes us!

Before we explain what is the class \( \mathcal{NP} \), let us remark that the satisfiability problem for clauses containing at most two literals (2-satisfiability, or 2-SAT) is solvable in polynomial time.

The first step consists in observing that if every clause in \( P \) contains at most two literals, then we can reduce the problem to testing satisfiability when every clause has exactly two literals.

Indeed, if \( P \) contains some clause \( \{x\} \), then any valuation satisfying \( P \) must make \( x \) true. Then, all clauses containing \( x \) will be true, and we can delete them, whereas we can delete \( \overline{x} \) from every clause containing it, since \( \overline{x} \) is false.

Similarly, if \( P \) contains some clause \( \{\overline{x}\} \), then any valuation satisfying \( P \) must make \( x \) false.

Thus, in a finite number of steps, either we get the empty clause, and \( P \) is unsatisfiable, or we get a set of clauses with exactly two literals.

The number of steps is clearly linear in the number of literals in \( P \).

For the second step, we construct a directed graph from \( P \). The nodes of this graph are the literals in \( P \), and edges are defined as follows:

1. For every clause \( \{\overline{x} \lor y\} \), there is an edge from \( x \) to \( y \) and an edge from \( \overline{y} \) to \( \overline{x} \).
2. For every clause \( \{x \lor y\} \), there is an edge from \( \overline{x} \) to \( y \) and an edge from \( \overline{y} \) to \( x \).
3. For every clause \( \{\overline{x} \lor \overline{y}\} \), there is an edge from \( x \) to \( \overline{y} \) and an edge from \( y \) to \( \overline{x} \).

Then, it can be shown that \( P \) is unsatisfiable iff there is some \( x \) so that there is a cycle containing \( x \) and \( \overline{x} \).

As a consequence, 2-satisfiability is in \( \mathcal{P} \).
9.6 The Class \( \mathcal{NP} \), Polynomial Reducibility, \( \mathcal{NP} \)-Completeness

One will observe that the hard part in trying to solve either the Hamiltonian cycle problem or the satisfiability problem, SAT, is to *find* a solution, but that *checking* that a candidate solution is indeed a solution can be done easily in polynomial time.

This is the essence of problems that can be solved *nondeterministically* in polynomial time: A solution can be guessed and then checked in polynomial time.

**Definition 9.4.** A nondeterministic Turing machine \( M \) is said to be *polynomially bounded* if there is a polynomial \( p(X) \) so that the following holds: For every input \( x \in \Sigma^* \), there is no ID \( ID_n \) so that

\[
ID_0 \vdash ID_1 \vdash^* ID_{n-1} \vdash ID_n, \quad \text{with} \quad n > p(|x|),
\]

where \( ID_0 = q_0x \) is the starting ID.

A language \( L \subseteq \Sigma^* \) is *nondeterministic polynomially decidable* if there is a polynomially bounded nondeterministic Turing machine that accepts \( L \). The family of all nondeterministic polynomially decidable languages is denoted by \( \mathcal{NP} \).

Of course, we have the inclusion

\[
P \subseteq \mathcal{NP},
\]

but whether or not we have equality is one of the most famous open problems of theoretical computer science and mathematics.

In fact, the question \( P \neq \mathcal{NP} \) is one of the open problems listed by the CLAY Institute, together with the Poincaré conjecture and the Riemann hypothesis, among other problems, and for which *one million dollar* is offered as a reward!

It is easy to check that SAT is in \( \mathcal{NP} \), and so is the Hamiltonian cycle problem.

As we saw in recursion theory, where we introduced the notion of many-one reducibility, in order to compare the “degree of difficulty” of problems, it is useful to introduce the notion of reducibility and the notion of a complete set.

**Definition 9.5.** A function \( f : \Sigma^* \rightarrow \Sigma^* \) is *polynomial-time computable* if there is a polynomial \( p(X) \) so that the following holds: There is a deterministic Turing machine \( M \) computing it so that for every input \( x \in \Sigma^* \), there is no ID \( ID_n \) so that

\[
ID_0 \vdash ID_1 \vdash^* ID_{n-1} \vdash ID_n, \quad \text{with} \quad n > p(|x|),
\]

where \( ID_0 = q_0x \) is the starting ID.
Given two languages $L_1, L_2 \subseteq \Sigma^*$, a polynomial-time reduction from $L_1$ to $L_2$ is a polynomial-time computable function $f : \Sigma^* \rightarrow \Sigma^*$ so that for all $u \in \Sigma^*$,

$$u \in L_1 \text{ iff } f(u) \in L_2.$$ 

The notation $L_1 \leq_P L_2$ is often used to denote the fact that there is polynomial-time reduction from $L_1$ to $L_2$. Sometimes, the notation $L_1 \leq_{P^m} L_2$ is used to stress that this is a many-to-one reduction (that is, $f$ is not necessarily injective). This type of reduction is also known as a Karp reduction.

A polynomial reduction $f : \Sigma^* \rightarrow \Sigma^*$ from a language $L_1$ to a language $L_2$ is a method that converts in polynomial time every string $u \in \Sigma^*$ (viewed as an instance of a problem $A$ encoded by language $L_1$) to a string $f(u) \in \Sigma^*$ (viewed as an instance of a problem $B$ encoded by language $L_2$) in such way that membership in $L_1$, that is $u \in L_1$, is equivalent to membership in $L_2$, that is $f(u) \in L_2$.

As a consequence, if we have a procedure to decide membership in $L_2$ (to solve every instance of problem $B$), then we have a procedure for solving membership in $L_1$ (to solve every instance of problem $A$), since given any $u \in L_1$, we can first apply $f$ to $u$ to produce $f(u)$, and then apply our procedure to decide whether $f(u) \in L_2$; the defining property of $f$ says that this is equivalent to deciding whether $u \in L_1$. Furthermore, if the procedure for deciding membership in $L_2$ runs deterministically in polynomial time, since $f$ runs deterministically in polynomial time, so does the procedure for deciding membership in $L_1$, and similarly if the procedure for deciding membership in $L_2$ runs non deterministically in polynomial time.

For the above reason, we see that membership in $L_2$ can be considered at least as hard as membership in $L_1$, since any method for deciding membership in $L_2$ yields a method for deciding membership in $L_1$. Thus, if we view $L_1$ an encoding a problem $A$ and $L_2$ as encoding a problem $B$, then $B$ is at least as hard as $A$.

The following version of Proposition 5.16 for polynomial-time reducibility is easy to prove.

**Proposition 9.4.** Let $A, B, C$ be subsets of $\mathbb{N}$ (or $\Sigma^*$). The following properties hold:

1. If $A \leq_P B$ and $B \leq_P C$, then $A \leq_P C$.
2. If $A \leq_P B$ then $\overline{A} \leq_P \overline{B}$.
3. If $A \leq_P B$ and $B \in \mathcal{NP}$, then $A \in \mathcal{NP}$.
4. If $A \leq_P B$ and $A \notin \mathcal{NP}$, then $B \notin \mathcal{NP}$.
5. If $A \leq_P B$ and $B \in \mathcal{P}$, then $A \in \mathcal{P}$.
6. If $A \leq_P B$ and $A \notin \mathcal{P}$, then $B \notin \mathcal{P}$.

Intuitively, we see that if $L_1$ is a hard problem and $L_1$ can be reduced to $L_2$ in polynomial time, then $L_2$ is also a hard problem.
For example, one can construct a polynomial reduction from the Hamiltonian cycle problem to the satisfiability problem SAT. Given a directed graph \( G = (V, E) \) with \( n \) nodes, say \( V = \{1, \ldots, n\} \), we need to construct in polynomial time a set \( F = \tau(G) \) of clauses such that \( G \) has a Hamiltonian cycle iff \( \tau(G) \) is satisfiable. We need to describe a permutation of the nodes that forms a Hamiltonian cycle. For this we introduce \( n^2 \) boolean variables \( x_{ij} \), with the intended interpretation that \( x_{ij} \) is true iff node \( i \) is the \( j \)th node in a Hamiltonian cycle.

To express that at least one node must appear as the \( j \)th node in a Hamiltonian cycle, we have the \( n \) clauses
\[
(x_{1j} \lor x_{2j} \lor \cdots \lor x_{nj}), \quad 1 \leq j \leq n.
\]
(1)
The conjunction of these clauses is satisfied iff for every \( j = 1, \ldots, n \) there is some node \( i \) which is the \( j \)th node in the cycle.

To express that only one node appears in the cycle, we have the clauses
\[
(x_{ij} \lor x_{kj}), \quad 1 \leq i,j,k \leq n, \ i \neq k.
\]
(2)
Since \( (x_{ij} \lor x_{kj}) \) is equivalent to \( (x_{ij} \land x_{kj}) \), each such clause asserts that no two distinct nodes may appear as the \( j \)th node in the cycle. Let \( S_1 \) be the set of all clauses of type (1) or (2).

The conjunction of the clauses in \( S_1 \) assert that exactly one node appear at the \( j \)th node in the Hamiltonian cycle. We still need to assert that each node \( i \) appears exactly once in the cycle. For this, we have the clauses
\[
(x_{i1} \lor x_{i2} \lor \cdots \lor x_{in}), \quad 1 \leq i \leq n,
\]
(3)
and
\[
(x_{ij} \lor x_{ik}), \quad 1 \leq i,j,k \leq n, \ j \neq k.
\]
(4)
Let \( S_2 \) be the set of all clauses of type (3) or (4).

The conjunction of the clauses in \( S_1 \cup S_2 \) asserts that the \( x_{ij} \) represents a bijection of \( \{1,2,\ldots,n\} \), in the sense that for any truth assignment \( v \) satisfying all these clauses, \( i \mapsto j \) iff \( v(x_{ij}) = T \) defines a bijection of \( \{1,2,\ldots,n\} \).

It remains to assert that this permutation of the nodes is a Hamiltonian cycle, which means that if \( x_{ij} \) and \( x_{kj+1} \) are both true then there there must be an edge \( (i,k) \). By contrapositive, this equivalent to saying that if \( (i,k) \) is not an edge of \( G \), then \( \overline{x_{ij} \land x_{kj+1}} \) is true, which as a clause is equivalent to \( (x_{ij} \lor x_{kj+1}) \).

Therefore, for all \( (i,k) \) such that \( (i,k) \notin E \) (with \( i,k \in \{1,2,\ldots,n\} \)), we have the clauses
\[
(x_{ij} \lor x_{k,j+1}), \quad j = 1, \ldots, n.
\]
(5)
Let \( S_3 \) be the set of clauses of type (5). The conjunction of all the clauses in \( S_1 \cup S_2 \cup S_3 \) is the boolean formula \( F = \tau(G) \).
We leave it as an exercise to prove that $G$ has a Hamiltonian cycle iff $F = \tau(G)$ is satisfiable.

It is also possible to construct a reduction of the satisfiability problem to the Hamiltonian cycle problem but this is harder. It is easier to construct this reduction in two steps by introducing an intermediate problem, the exact cover problem, and to provide a polynomial reduction from the satisfiability problem to the exact cover problem, and a polynomial reduction from the exact cover problem to the Hamiltonian cycle problem. These reductions are carried out in Section 10.2.

The above construction of a set $F = \tau(G)$ of clauses from a graph $G$ asserting that $G$ has a Hamiltonian cycle iff $F$ is satisfiable illustrates the expressive power of propositional logic.

Remarkably, every language in $\mathcal{NP}$ can be reduced to SAT. Thus, SAT is a hardest problem in $\mathcal{NP}$ (Since it is in $\mathcal{NP}$).

**Definition 9.6.** A language $L$ is $\mathcal{NP}$-hard if there is a polynomial reduction from every language $L_1 \in \mathcal{NP}$ to $L$. A language $L$ is $\mathcal{NP}$-complete if $L \in \mathcal{NP}$ and $L$ is $\mathcal{NP}$-hard.

Thus, an $\mathcal{NP}$-hard language is as hard to decide as any language in $\mathcal{NP}$.

**Remark:** There are $\mathcal{NP}$-hard languages that do not belong to $\mathcal{NP}$. Such problems are really hard. Two standard examples are $K_0$ and $K$, which encode the halting problem. Since $K_0$ and $K$ are not computable, they can’t be in $\mathcal{NP}$. Furthermore, since every language $L$ in $\mathcal{NP}$ is accepted nondeterminstically in polynomial time $p(X)$, for some polynomial $p(X)$, for every input $w$ we can try all computations of length at most $p(|w|)$ (there can be exponentially many, but only a finite number), so every language in $\mathcal{NP}$ is computable. Finally, it is shown in Theorem 5.17 that $K_0$ and $K$ are complete with respect to many-one reducibility, so in particular they are $\mathcal{NP}$-hard. An example of a computable $\mathcal{NP}$-hard language not in $\mathcal{NP}$ will be described after Theorem 9.6.

The importance of $\mathcal{NP}$-complete problems stems from the following theorem which follows immediately from Proposition 9.4.

**Theorem 9.5.** Let $L$ be an $\mathcal{NP}$-complete language. Then, $\mathcal{P} = \mathcal{NP}$ iff $L \in \mathcal{P}$.

There are analogies between $\mathcal{P}$ and the class of computable sets, and $\mathcal{NP}$ and the class of listable sets, but there are also important differences. One major difference is that the family of computable sets is properly contained in the family of listable sets, but it is an open problem whether $\mathcal{P}$ is properly contained in $\mathcal{NP}$. We also know that a set $L$ is computable iff both $L$ and $\overline{L}$ are listable, but it is also an open problem whether if both $L \in \mathcal{NP}$ and $\overline{L} \in \mathcal{NP}$, then $L \in \mathcal{P}$. This suggests defining $$
\text{co}\mathcal{NP} = \{\overline{L} \mid L \in \mathcal{NP}\},$$
that is, co\(NP\) consists of all complements of languages in \(NP\). Since \(P \subseteq NP\) and \(P\) is closed under complementation,
\[
P \subseteq \text{co}NP,
\]
and thus
\[
P \subseteq NP \cap \text{co}NP,
\]
but nobody knows whether the inclusion is proper. There are problems in \(NP \cap \text{co}NP\) not known to be in \(P\); see Section 10.3. It is unknown whether \(NP\) is closed under complementation, that is, nobody knows whether \(NP = \text{co}NP\). This is considered unlikely. We will come back to \(\text{co}NP\) in Section 10.3.

Next, we prove a famous theorem of Steve Cook and Leonid Levin (proved independently): SAT is \(NP\)-complete.

### 9.7 The Cook–Levin Theorem: SAT is \(NP\)-Complete

Instead of showing directly that SAT is \(NP\)-complete, which is rather complicated, we proceed in two steps, as suggested by Lewis and Papadimitriou.

1. First, we define a tiling problem adapted from H. Wang (1961) by Harry Lewis, and we prove that it is \(NP\)-complete.

2. We show that the tiling problem can be reduced to SAT.

We are given a finite set \(T = \{t_1, \ldots, t_p\}\) of tile patterns, for short, tiles. Copies of these tile patterns may be used to tile a rectangle of predetermined size \(2s \times s\) (\(s > 1\)). However, there are constraints on the way that these tiles may be adjacent horizontally and vertically.

The horizontal constraints are given by a relation \(H \subseteq T \times T\), and the vertical constraints are given by a relation \(V \subseteq T \times T\).

Thus, a tiling system is a triple \(T = (T, V, H)\) with \(V\) and \(H\) as above.

The bottom row of the rectangle of tiles is specified before the tiling process begins.

For example, consider the following tile patterns:

\[
\begin{array}{cccc}
  a & e & a & c \\
  c & a & c & e \\
  b & c & d & e \\
  c & d & e & e \\
\end{array}
\]
The horizontal and the vertical constraints are that the letters on adjacent edges match (blank edges do not match).

For \( s = 3 \), given the bottom row

\[
\begin{array}{cccccccc}
  a & b & c & d & e & e & e & e \\
  c & c & d & d & e & e & e & e \\
  d & c & e & e & e & e & e & e \\
\end{array}
\]

we have the tiling shown below:

\[
\begin{array}{cccccccccccc}
  a & b & c & d & e & e & e & e & e & e & e & e \\
  a & b & c & d & e & e & e & e & e & e & e & e \\
  a & b & c & d & e & e & e & e & e & e & e & e \\
  a & b & c & d & e & e & e & e & e & e & e & e \\
  a & b & c & d & e & e & e & e & e & e & e & e \\
  a & b & c & d & e & e & e & e & e & e & e & e \\
  a & b & c & d & e & e & e & e & e & e & e & e \\
  a & b & c & d & e & e & e & e & e & e & e & e \\
\end{array}
\]

Formally, the problem is then as follows:

**The Bounded Tiling Problem**

Given any tiling system \((T, V, H)\), any integer \( s > 1 \), and any initial row of tiles \( \sigma_0 \) (of length \( 2s \))

\[
\sigma_0 : \{1, 2, \ldots, s, s + 1, \ldots, 2s\} \to T,
\]

find a \( 2s \times s \)-tiling \( \sigma \) extending \( \sigma_0 \), i.e., a function

\[
\sigma : \{1, 2, \ldots, s, s + 1, \ldots, 2s\} \times \{1, \ldots, s\} \to T
\]

so that

1. \( \sigma(m, 1) = \sigma_0(m) \), for all \( m \) with \( 1 \leq m \leq 2s \).
2. \((\sigma(m, n), \sigma(m + 1, n)) \in H\), for all \( m \) with \( 1 \leq m \leq 2s - 1 \), and all \( n \), with \( 1 \leq n \leq s \).
3. \((\sigma(m, n), \sigma(m, n + 1)) \in V\), for all \( m \) with \( 1 \leq m \leq 2s \), and all \( n \), with \( 1 \leq n \leq s - 1 \).
Formally, an *instance of the tiling problem* is a triple \((T, V, H, \tilde{s}, \sigma_0)\), where \((T, V, H)\) is a tiling system, \(\tilde{s}\) is the string representation of the number \(s \geq 2\), in binary and \(\sigma_0\) is an initial row of tiles (the bottom row).

For example, if \(s = 1025\) (as a decimal number), then its binary representation is \(\tilde{s} = 1000000001\). The length of \(\tilde{s}\) is \(\log_2 s + 1\).

Recall that the input must be a string. This is why the number \(s\) is represented by a string in binary.

If we only included a *single* tile \(\sigma_0\) in position \((s + 1, 1)\), then the length of the input \(((T, V, H), \tilde{s}, \sigma_0)\) would be \(\log_2 s + C + 2\) for some constant \(C\) corresponding to the length of the string encoding \((T, V, H)\).

However, the rectangular grid has size \(2s^2\), which is *exponential* in the length \(\log_2 s + C + 2\) of the input \(((T, V, H), \tilde{s}, \sigma_0)\). Thus, it is impossible to check in polynomial time that a proposed solution is a tiling.

However, if we include in the input the bottom row \(\sigma_0\) of length \(2s\), then the size of the grid is indeed polynomial in the size of the input.

**Theorem 9.6.** The tiling problem defined earlier is \(\mathcal{NP}\)-complete.

**Proof.** Let \(L \subseteq \Sigma^*\) be any language in \(\mathcal{NP}\) and let \(u\) be any string in \(\Sigma^*\). Assume that \(L\) is accepted in polynomial time bounded by \(p(|u|)\).

We show how to construct an instance of the tiling problem, \(((T, V, H)_L, \tilde{s}, \sigma_0)\), where \(s = p(|u|) + 2\), and where the bottom row encodes the starting ID, so that \(u \in L\) iff the tiling problem \(((T, V, H)_L, \tilde{s}, \sigma_0)\) has a solution.

First, note that the problem is indeed in \(\mathcal{NP}\), since we have to guess a rectangle of size \(2s^2\), and that checking that a tiling is legal can indeed be done in \(O(s^2)\), where \(s\) is *bounded by the size of the input* \(((T, V, H), \tilde{s}, \sigma_0)\), since the input contains the bottom row of \(2s\) symbols (this is the reason for including the bottom row of \(2s\) tiles in the input!).

The idea behind the definition of the tiles is that, in a solution of the tiling problem, the labels on the horizontal edges between two adjacent rows represent a legal ID, \(upav\).

In a given row, the labels on vertical edges of adjacent tiles keep track of the change of state and direction.

Let \(\Gamma\) be the tape alphabet of the TM, \(M\). As before, we assume that \(M\) signals that it accepts \(u\) by halting with the output 1 (true).

From \(M\), we create the following tiles:

(1) For every \(a \in \Gamma\), tiles

\[
\begin{array}{c}
a\\
\end{array}
\]
(2) For every $a \in \Gamma$, the bottom row uses tiles

\[
\begin{array}{c}
\text{a} \\
\end{array}
\quad
\begin{array}{c}
\text{q}_0, a \\
\end{array}
\]

where $q_0$ is the start state.

(3) For every instruction $(p, a, b, R, q) \in \delta$, for every $c \in \Gamma$, tiles

\[
\begin{array}{c}
\text{b} \\
\text{q}, R \\
\text{p}, a \\
\end{array}
\quad
\begin{array}{c}
\text{q}, c \\
\text{q}, R \\
\text{c} \\
\end{array}
\]

(4) For every instruction $(p, a, b, L, q) \in \delta$, for every $c \in \Gamma$, tiles

\[
\begin{array}{c}
\text{q}, c \\
\text{q}, L \\
\text{c} \\
\end{array}
\quad
\begin{array}{c}
\text{b} \\
\text{q}, L \\
\text{p}, a \\
\end{array}
\]

(5) For every halting state, $p$, tiles

\[
\begin{array}{c}
p, 1 \\
\end{array}
\quad
\begin{array}{c}
p, 1 \\
\end{array}
\]

The purpose of tiles of type (5) is to fill the $2s \times s$ rectangle iff $M$ accepts $u$. Since $s = p(|u|) + 2$ and the machine runs for at most $p(|u|)$ steps, the $2s \times s$ rectangle can be tiled iff $u \in L$.

The vertical and the horizontal constraints are that adjacent edges have the same label (or no label).

If $u = u_1 \cdots u_k$, the initial bottom row $\sigma_0$, of length $2s$, is:

\[
\begin{array}{c}
\text{B} \\
\text{...} \\
\text{q}_0, u_1 \\
\text{...} \\
\text{u}_k \\
\text{...} \\
\text{B} \\
\end{array}
\]

where the tile labeled $q_0, u_1$ is in position $s + 1$.

The example below illustrates the construction:
We claim that \( u = u_1 \cdots u_k \) is accepted by \( M \) iff the tiling problem just constructed has a solution.

The upper horizontal edge of the first (bottom) row of tiles represents the starting configuration \( B^s q_0 u B^{s-|u|} \). By induction, we see that after \( i \) \( (i \leq p(|u|) = s - 2) \) steps the upper horizontal edge of the \((i+1)\)th row of tiles represents the current ID \( \text{upav} \) reached by the Turing machine. Since the machine runs for at most \( p(|u|) \) steps and since \( s = p(|u|) + 2 \), when the computation stops, at most the lowest \( p(|u|) + 1 = s - 1 \) rows of the \( 2s \times s \) rectangle have been tiled. Assume the machine \( M \) stops after \( r \leq s - 2 \) steps. Then the lowest \( r + 1 \) rows have been tiled, and since no further instruction can be executed (since the machine entered a halting state), the remaining \( s - r - 1 \) rows can be filled iff tiles of type (5) can be used iff the machine stopped in an ID containing a pair \( p1 \) where \( p \) is a halting state. Therefore, the machine \( M \) accepts \( u \) iff the \( 2s \times s \) rectangle can be tiled. \( \square \)

**(Remarks.**

(1) The problem becomes harder if we only specify a single tile \( \sigma_0 \) as input, instead of a row of length \( 2s \). If \( s \) is specified in binary (or any other base, but not in tally notation), then the \( 2s^2 \) grid has size exponential in the length \( \log_2 s + C + 2 \) of the input \( ((T, V, H), \hat{s}, \sigma_0) \), and this tiling problem is actually \( \mathcal{NEXP}-complete! \) The class \( \mathcal{NEXP} \) is the family of languages that can be accepted by a nondeterministic Turing machine that runs in time bounded by \( 2^{p(|x|)} \), for every \( x \), where \( p \) is a polynomial; see the remark after Definition 10.4. By the time hierarchy theorem (Cook, Seiferas, Fischer, Meyer, Zak), it is known that \( \mathcal{NP} \) is properly contained in \( \mathcal{NEXP} \); see Papadimitriou [19] (Chapters 7 and 20) and Arora and Barak [2] (Chapter 3, Section 3.2). Then the tiling problem with a single tile as input is a computable \( \mathcal{NP} \)-hard problem not in \( \mathcal{NP} \).

(2) If we relax the finiteness condition and require that the entire upper half-plane be tiled, i.e., for every \( s > 1 \), there is a solution to the \( 2s \times s \)-tiling problem, then the problem is undecidable.

In 1972, Richard Karp published a list of 21 \( \mathcal{NP} \)-complete problems.

We finally prove the Cook-Levin theorem.
Theorem 9.7. (*Cook, 1971, Levin, 1973*) The satisfiability problem SAT is \( \mathcal{NP} \)-complete.

Proof. We reduce the tiling problem to SAT. Given a tiling problem, \(((\mathcal{T}, V, H), \hat{s}, \sigma_0)\), we introduce boolean variables

\[ x_{mnt}, \]

for all \( m \) with \( 1 \leq m \leq 2s \), all \( n \) with \( 1 \leq n \leq s \), and all tiles \( t \in \mathcal{T} \).

The intuition is that \( x_{mnt} = 1 \) iff tile \( t \) occurs in some tiling \( \sigma \) so that \( \sigma(m, n) = t \).

We define the following clauses:

1. For all \( m, n \) in the correct range, as above,
   \[ (x_{m \sigma_0(m)} \lor x_{m \sigma_0(m) + 1} \lor \cdots \lor x_{m \sigma_0(m)}), \]
   for all \( p \) tiles in \( \mathcal{T} \).
   This clause states that every position in \( \sigma \) is tiled.

2. For any two distinct tiles \( t \neq t' \in \mathcal{T} \), for all \( m, n \) in the correct range, as above,
   \[ (\overline{x_{mnt}} \lor \overline{x_{mnt'}}). \]
   This clause states that a position may not be occupied by more than one tile.

3. For every pair of tiles \((t, t') \in \mathcal{T} \times \mathcal{T} - H\), for all \( m \) with \( 1 \leq m \leq 2s - 1 \), and all \( n \), with \( 1 \leq n \leq s \),
   \[ (\overline{x_{mnt}} \lor \overline{x_{m+1 n t'}}). \]
   This clause enforces the horizontal adjacency constraints.

4. For every pair of tiles \((t, t') \in \mathcal{T} \times \mathcal{T} - V\), for all \( m \) with \( 1 \leq m \leq 2s \), and all \( n \), with \( 1 \leq n \leq s - 1 \),
   \[ (\overline{x_{mnt}} \lor \overline{x_{m n+1 t'}}). \]
   This clause enforces the vertical adjacency constraints.

5. For all \( m \) with \( 1 \leq m \leq 2s \),
   \[ (x_{m \sigma_0(m)}). \]
   This clause states that the bottom row is correctly tiled with \( \sigma_0 \).

It is easily checked that the tiling problem has a solution iff the conjunction of the clauses just defined is satisfiable. Thus, SAT is \( \mathcal{NP} \)-complete. \( \square \)
We sharpen Theorem 9.7 to prove that 3-SAT is also \( \mathcal{NP} \)-complete. This is the satisfiability problem for clauses containing at most three literals.

We know that we can’t go further and retain \( \mathcal{NP} \)-completeness, since 2-SAT is in \( \mathcal{P} \).

**Theorem 9.8.** (Cook, 1971) The satisfiability problem 3-SAT is \( \mathcal{NP} \)-complete.

**Proof.** We have to break “long clauses”

\[
C = (L_1 \lor \cdots \lor L_k),
\]

i.e., clauses containing \( k \geq 4 \) literals, into clauses with at most three literals, in such a way that satisfiability is preserved.

For example, consider the following clause with \( k = 6 \) literals:

\[
C = (L_1 \lor L_2 \lor L_3 \lor L_4 \lor L_5 \lor L_6).
\]

We create 3 new boolean variables \( y_1, y_2, y_3 \), and the 4 clauses

\[
(L_1 \lor L_2 \lor y_1), \ (\overline{y}_1 \lor L_3 \lor y_2), \ (\overline{y}_2 \lor L_4 \lor y_3), \ (\overline{y}_3 \lor L_5 \lor L_6).
\]

Let \( C' \) be the conjunction of these clauses. We claim that \( C \) is satisfiable iff \( C' \) is.

Assume that \( C' \) is satisfiable but \( C \) is not. If so, in any truth assignment \( v \), \( v(L_i) = \text{F} \), for \( i = 1, 2, \ldots, 6 \). To satisfy the first clause, we must have \( v(y_1) = \text{T} \). Then to satisfy the second clause, we must have \( v(y_2) = \text{T} \), and similarly satisfy the third clause, we must have \( v(y_3) = \text{T} \). However, since \( v(L_5) = \text{F} \) and \( v(L_6) = \text{F} \), the only way to satisfy the fourth clause is to have \( v(y_3) = \text{F} \), contradicting that \( v(y_3) = \text{T} \). Thus, \( C \) is indeed satisfiable.

Let us now assume that \( C \) is satisfiable. This means that there is a smallest index \( i \) such that \( L_i \) is satisfied.

Say \( i = 1 \), so \( v(L_1) = \text{T} \). Then if we let \( v(y_1) = v(y_2) = v(y_3) = \text{F} \), we see that \( C' \) is satisfied.

Say \( i = 2 \), so \( v(L_1) = \text{F} \) and \( v(L_2) = \text{T} \). Again if we let \( v(y_1) = v(y_2) = v(y_3) = \text{F} \), we see that \( C' \) is satisfied.

Say \( i = 3 \), so \( v(L_1) = \text{F} \), \( v(L_2) = \text{F} \), and \( v(L_3) = \text{T} \). If we let \( v(y_1) = \text{T} \) and \( v(y_2) = v(y_3) = \text{F} \), we see that \( C' \) is satisfied.

Say \( i = 4 \), so \( v(L_1) = \text{F} \), \( v(L_2) = \text{F} \), \( v(L_3) = \text{F} \), and \( v(L_4) = \text{T} \). If we let \( v(y_1) = \text{T} \), \( v(y_2) = \text{T} \) and \( v(y_3) = \text{F} \), we see that \( C' \) is satisfied.

Say \( i = 5 \), so \( v(L_1) = \text{F} \), \( v(L_2) = \text{F} \), \( v(L_3) = \text{F} \), \( v(L_4) = \text{F} \), and \( v(L_5) = \text{T} \). If we let \( v(y_1) = \text{T} \), \( v(y_2) = \text{T} \) and \( v(y_3) = \text{T} \), we see that \( C' \) is satisfied.
CHAPTER 9. COMPUTATIONAL COMPLEXITY; \( \mathcal{P} \) AND \( \mathcal{NP} \)

Say \( i = 6 \), so \( v(L_1) = \mathbf{F} \), \( v(L_2) = \mathbf{F} \), \( v(L_3) = \mathbf{F} \), \( v(L_4) = \mathbf{F} \), \( v(L_5) = \mathbf{F} \), and \( v(L_6) = \mathbf{T} \).

Again, if we let \( v(y_1) = \mathbf{T} \), \( v(y_2) = \mathbf{T} \) and \( v(y_3) = \mathbf{T} \), we see that \( C' \) is satisfied.

Therefore if \( C \) is satisfied, then \( C' \) is satisfied in all cases.

In general, for every long clause, create \( k - 3 \) new boolean variables \( y_1, \ldots, y_{k-3} \), and the \( k - 2 \) clauses

\[
(L_1 \lor L_2 \lor y_1), (\overline{y_1} \lor L_3 \lor y_2), (\overline{y_2} \lor L_4 \lor y_3), \ldots, \\
(\overline{y}_{k-4} \lor L_{k-2} \lor y_{k-3}), (\overline{y}_{k-3} \lor L_{k-1} \lor L_k).
\]

Let \( C' \) be the conjunction of these clauses. We claim that \( C \) is satisfiable iff \( C' \) is.

Assume that \( C' \) is satisfiable, but that \( C \) is not. Then, for every truth assignment \( v \), we have \( v(L_i) = \mathbf{F} \), for \( i = 1, \ldots, k \).

However, \( C' \) is satisfied by some \( v \), and the only way this can happen is that \( v(y_1) = \mathbf{T} \), to satisfy the first clause. Then, \( v(\overline{y_1}) = \mathbf{F} \), and we must have \( v(y_2) = \mathbf{T} \), to satisfy the second clause.

By induction, we must have \( v(y_{k-3}) = \mathbf{T} \), to satisfy the next to the last clause. However, the last clause is now false, a contradiction.

Thus, if \( C' \) is satisfiable, then so is \( C \).

Conversely, assume that \( C \) is satisfiable. If so, there is some truth assignment, \( v \), so that \( v(C) = \mathbf{T} \), and thus, there is a smallest index \( i \), with \( 1 \leq i \leq k \), so that \( v(L_i) = \mathbf{T} \) (and so, \( v(L_j) = \mathbf{F} \) for all \( j < i \)).

Let \( v' \) be the assignment extending \( v \) defined so that

\[
v'(y_j) = \mathbf{F} \quad \text{if} \quad \max\{1, i-1\} \leq j \leq k-3,
\]

and \( v'(y_j) = \mathbf{T} \), otherwise.

It is easily checked that \( v'(C') = \mathbf{T} \). \( \square \)

Another version of 3-SAT can be considered, in which every clause has exactly three literals. We will call this the problem exact 3-SAT.

**Theorem 9.9. (Cook, 1971)** The satisfiability problem for exact 3-SAT is \( \mathcal{NP} \)-complete.

**Proof.** A clause of the form \( (L) \) is satisfiable iff the following four clauses are satisfiable:

\[
(L \lor u \lor v), (L \lor \overline{u} \lor v), (L \lor u \lor \overline{v}), (L \lor \overline{u} \lor \overline{v}).
\]

A clause of the form \( (L_1 \lor L_2) \) is satisfiable iff the following two clauses are satisfiable:

\[
(L_1 \lor L_2 \lor u), (L_1 \lor L_2 \lor \overline{u}).
\]

Thus, we have a reduction of 3-SAT to exact 3-SAT. \( \square \)
We now make some remarks on the conversion of propositions to CNF.

Recall that the set of propositions (over the connectives $\lor$, $\land$, and $\neg$) is defined inductively as follows:

1. Every propositional letter, $x \in \mathbf{PV}$, is a proposition (an *atomic* proposition).
2. If $A$ is a proposition, then $\neg A$ is a proposition.
3. If $A$ and $B$ are propositions, then $(A \lor B)$ is a proposition.
4. If $A$ and $B$ are propositions, then $(A \land B)$ is a proposition.

Two propositions $A$ and $B$ are *equivalent*, denoted $A \equiv B$, if

$$v \models A \iff v \models B$$

for all truth assignments, $v$.

It is easy to show that $A \equiv B$ iff the proposition

$$(\neg A \lor B) \land (\neg B \lor A)$$

is valid.

Every proposition, $A$, is equivalent to a proposition, $A'$, in CNF.

There are several ways of proving this fact. One method is algebraic, and consists in using the algebraic laws of boolean algebra.

First, one may convert a proposition to *negation normal form*, or *nnf*. A proposition is in nnf if occurrences of $\neg$ only appear in front of propositional variables, but not in front of compound propositions.

Any proposition can be converted to an equivalent one in nnf by using the de Morgan laws:

$$\neg(A \lor B) \equiv (\neg A \land \neg B)$$

$$\neg(A \land B) \equiv (\neg A \lor \neg B)$$

$$\neg\neg A \equiv A.$$

Then, a proposition in nnf can be converted to CNF, but the question of uniqueness of the CNF is a bit tricky.

For example, the proposition

$$A = (u \land (x \lor y)) \lor (\neg u \land (x \lor y))$$
has

\[ A_1 = (u \lor x \lor y) \land (\neg u \lor x \lor y) \]
\[ A_2 = (u \lor \neg u) \land (x \lor y) \]
\[ A_3 = x \lor y, \]

as equivalent propositions in CNF!

We can get a unique CNF equivalent to a given proposition if we do the following:

(1) Let \( \text{Var}(A) = \{x_1, \ldots, x_m\} \) be the set of variables occurring in \( A \).

(2) Define a maxterm w.r.t. \( \text{Var}(A) \) as any disjunction of \( m \) pairwise distinct literals formed from \( \text{Var}(A) \), and not containing both some variable \( x_i \) and its negation \( \neg x_i \).

(3) Then, it can be shown that for any proposition \( A \) that is not a tautology, there is a unique proposition in CNF equivalent to \( A \), whose clauses consist of maxterms formed from \( \text{Var}(A) \).

The above definition can yield strange results. For instance, the CNF of any unsatisfiable proposition with \( m \) distinct variables is the conjunction of all of its \( 2^m \) maxterms!

The above notion does not cope well with minimality.

For example, according to the above, the CNF of

\[ A = (u \land (x \lor y)) \lor (\neg u \land (x \lor y)) \]

should be

\[ A_1 = (u \lor x \lor y) \land (\neg u \lor x \lor y). \]

There are also propositions such that any equivalent proposition in CNF has size exponential in terms of the original proposition.

Here is such an example:

\[ A = (x_1 \land x_2) \lor (x_3 \land x_4) \lor \cdots \lor (x_{2n-1} \land x_{2n}). \]

Observe that it is in DNF.

We will prove a little later that any CNF for \( A \) contains \( 2^n \) occurrences of variables.

A nice method to convert a proposition in nnf to CNF is to construct a tree whose nodes are labeled with sets of propositions using the following (Gentzen-style) rules:

\[
\frac{P, \Delta}{(P \land Q), \Delta} \quad \frac{Q, \Delta}{(P \land Q), \Delta}
\]
and

\[
\frac{P, Q, \Delta}{(P \lor Q), \Delta}
\]

where \( \Delta \) stands for any set of propositions (even empty), and the comma stands for union. Thus, it is assumed that \((P \land Q) \notin \Delta\) in the first case, and that \((P \lor Q) \notin \Delta\) in the second case.

Since we interpret a set, \( \Gamma \), of propositions as a disjunction, a valuation, \( v \), satisfies \( \Gamma \) iff it satisfies some proposition in \( \Gamma \).

Observe that a valuation \( v \) satisfies the conclusion of a rule iff it satisfies both premises in the first case, and the single premise in the second case.

Using these rules, we can build a finite tree whose leaves are labeled with sets of literals.

By the above observation, a valuation \( v \) satisfies the proposition labeling the root of the tree iff it satisfies all the propositions labeling the leaves of the tree.

But then, a CNF for the original proposition \( A \) (in \( \text{nnf} \), at the root of the tree) is the conjunction of the clauses appearing as the leaves of the tree.

We may exclude the clauses that are tautologies, and we may discover in the process that \( A \) is a tautology (when all leaves are tautologies).

Going back to our “bad” proposition, \( A \), by induction, we see that any tree for \( A \) has \( 2^n \) leaves.

However, it should be noted that for any proposition, \( A \), we can construct in polynomial time a formula, \( A' \), in CNF, so that \( A \) is satisfiable iff \( A' \) is satisfiable, by creating new variables.

We proceed recursively. The trick is that we replace

\[
(C_1 \land \cdots \land C_m) \lor (D_1 \land \cdots \land D_n)
\]

by

\[
(C_1 \lor y) \land \cdots \land (C_m \lor y) \land (D_1 \lor \overline{y}) \land \cdots \land (D_n \lor \overline{y}),
\]

where the \( C_i \)'s and the \( D_j \)'s are clauses, and \( y \) is a new variable.

It can be shown that the number of new variables required is at most quadratic in the size of \( A \).

Warning: In general, the proposition \( A' \) is not equivalent to the proposition \( A \).

Rules for dealing for \( \neg \) can also be created. In this case, we work with pairs of sets of propositions,

\[
\Gamma \rightarrow \Delta,
\]
where, the propositions in $\Gamma$ are interpreted conjunctively, and the propositions in $\Delta$ are interpreted disjunctively.

We obtain a sound and complete proof system for propositional logic (a “Gentzen-style” proof system, see Gallier’s *Logic for Computer Science*).
Chapter 10

Some $\mathcal{NP}$-Complete Problems

10.1 Statements of the Problems

In this chapter we will show that certain classical algorithmic problems are $\mathcal{NP}$-complete. This chapter is heavily inspired by Lewis and Papadimitriou’s excellent treatment [17]. In order to study the complexity of these problems in terms of resource (time or space) bounded Turing machines (or RAM programs), it is crucial to be able to encode instances of a problem $P$ as strings in a language $L_P$. Then an instance of a problem $P$ is solvable iff the corresponding string belongs to the language $L_P$. This implies that our problems must have a yes–no answer, which is not always the usual formulation of optimization problems where what is required is to find some optimal solution, that is, a solution minimizing or maximizing some objective (cost) function $F$. For example the standard formulation of the traveling salesman problem asks for a tour (of the cities) of minimal cost.

Fortunately, there is a trick to reformulate an optimization problem as a yes–no answer problem, which is to explicitly incorporate a budget (or cost) term $B$ into the problem, and instead of asking whether some objective function $F$ has a minimum or a maximum $w$, we ask whether there is a solution $w$ such that $F(w) \leq B$ in the case of a minimum solution, or $F(w) \geq B$ in the case of a maximum solution.

If we are looking for a minimum of $F$, we try to guess the minimum value $B$ of $F$ and then we solve the problem of finding $w$ such that $F(w) \leq B$. If our guess for $B$ is too small, then we fail. In this case, we try again with a larger value of $B$. Otherwise, if $B$ was not too small we find some $w$ such that $F(w) \leq B$, but $w$ may not correspond to a minimum of $F$, so we try again with a smaller value of $B$, and so on. This yields an approximation method to find a minimum of $F$.

Similarly, if we are looking for a maximum of $F$, we try to guess the maximum value $B$ of $F$ and then we solve the problem of finding $w$ such that $F(w) \geq B$. If our guess for $B$ is too large, then we fail. In this case, we try again with a smaller value of $B$. Otherwise, if $B$ was not too large we find some $w$ such that $F(w) \geq B$, but $w$ may not correspond to a maximum of $F$, so we try again with a greater value of $B$, and so on. This yields an
approximation method to find a maximum of $F$.

We will see several examples of this technique in Problems 5–8 listed below.

The problems that will consider are

(1) Exact Cover

(2) Hamiltonian Cycle for directed graphs

(3) Hamiltonian Cycle for undirected graphs

(4) The Traveling Salesman Problem

(5) Independent Set

(6) Clique

(7) Node Cover

(8) Knapsack, also called subset sum

(9) Inequivalence of $*$-free Regular Expressions

(10) The 0-1-integer programming problem

We begin by describing each of these problems.

(1) **Exact Cover**

We are given a finite nonempty set $U = \{u_1, \ldots, u_n\}$ (the universe), and a family $\mathcal{F} = \{S_1, \ldots, S_m\}$ of $m \geq 1$ nonempty subsets of $U$. The question is whether there is an exact cover, that is, a subfamily $\mathcal{C} \subseteq \mathcal{F}$ of subsets in $\mathcal{F}$ such that the sets in $\mathcal{C}$ are disjoint and their union is equal to $U$.

For example, let $U = \{u_1, u_2, u_3, u_4, u_5, u_6\}$, and let $\mathcal{F}$ be the family

$$\mathcal{F} = \{\{u_1, u_3\}, \{u_2, u_3, u_6\}, \{u_1, u_5\}, \{u_2, u_3, u_4\}, \{u_5, u_6\}, \{u_2, u_4\}\}.$$  

The subfamily

$$\mathcal{C} = \{\{u_1, u_3\}, \{u_5, u_6\}, \{u_2, u_4\}\}$$

is an exact cover.

It is easy to see that **Exact Cover** is in $\mathcal{NP}$. To prove that it is $\mathcal{NP}$-complete, we will reduce the **Satisfiability Problem** to it. This means that we provide a method running in polynomial time that converts every instance of the **Satisfiability Problem** to an instance of **Exact Cover**, such that the first problem has a solution iff the converted problem has a solution.
10.1. STATEMENTS OF THE PROBLEMS

(2) Hamiltonian Cycle (for Directed Graphs)

Recall that a *directed graph* $G$ is a pair $G = (V, E)$, where $E \subseteq V \times V$. Elements of $V$ are called *nodes* (or *vertices*). A pair $(u, v) \in E$ is called an *edge* of $G$. We will restrict ourselves to *simple graphs*, that is, graphs without edges of the form $(u, u)$; equivalently, $G = (V, E)$ is a simple graph if whenever $(u, v) \in E$, then $u \neq v$.

Given any two nodes $u, v \in V$, a *path from $u$ to $v$* is any sequence of $n+1$ edges ($n \geq 0$)

$$(u, v_1), (v_1, v_2), \ldots, (v_n, v).$$

(If $n = 0$, a path from $u$ to $v$ is simply a single edge, $(u, v)$.)

A directed graph $G$ is *strongly connected* if for every pair $(u, v) \in V \times V$, there is a path from $u$ to $v$. A *closed path, or cycle*, is a path from some node $u$ to itself. We will restrict our attention to finite graphs, i.e. graphs $(V, E)$ where $V$ is a finite set.

**Definition 10.1.** Given a directed graph $G$, a *Hamiltonian cycle* is a cycle that passes through all the nodes exactly once (note, some edges may not be traversed at all).

**Hamiltonian Cycle Problem (for Directed Graphs):** Given a directed graph $G$, is there an Hamiltonian cycle in $G$?

Is there is a Hamiltonian cycle in the directed graph $D$ shown in Figure 10.1?

Finding a Hamiltonian cycle in this graph does not appear to be so easy! A solution is shown in Figure 10.2 below.

It is easy to see that *Hamiltonian Cycle (for Directed Graphs)* is in $\mathcal{NP}$. To prove that it is $\mathcal{NP}$-complete, we will reduce *Exact Cover* to it. This means that we provide a method running in polynomial time that converts every instance of *Exact Cover* to an instance of *Hamiltonian Cycle (for Directed Graphs)* such that the first problem has a solution iff the converted problem has a solution. This is perhaps the hardest reduction.
Figure 10.1: A tour “around the world.”

Figure 10.2: A Hamiltonian cycle in $D$. 
(3) Hamiltonian Cycle (for Undirected Graphs)

Recall that an undirected graph $G$ is a pair $G = (V, E)$, where $E$ is a set of subsets $\{u, v\}$ of $V$ consisting of exactly two distinct elements. Elements of $V$ are called nodes (or vertices). A pair $\{u, v\} \in E$ is called an edge of $G$.

Given any two nodes $u, v \in V$, a path from $u$ to $v$ is any sequence of $n$ nodes ($n \geq 2$)

$$u = u_1, u_2, \ldots, u_n = v$$

such that $\{u_i, u_{i+1}\} \in E$ for $i = 1, \ldots, n - 1$. (If $n = 2$, a path from $u$ to $v$ is simply a single edge, $\{u, v\}$.)

An undirected graph $G$ is connected if for every pair $(u, v) \in V \times V$, there is a path from $u$ to $v$. A closed path, or cycle, is a path from some node $u$ to itself.

**Definition 10.2.** Given an undirected graph $G$, a Hamiltonian cycle is a cycle that passes through all the nodes exactly once (note, some edges may not be traversed at all).

**Hamiltonian Cycle Problem (for Undirected Graphs):** Given an undirected graph $G$, is there an Hamiltonian cycle in $G$?

An instance of this problem is obtained by changing every directed edge in the directed graph of Figure 10.1 to an undirected edge. The directed Hamiltonian cycle given in Figure 10.1 is also an undirected Hamiltonian cycle of the undirected graph of Figure 10.3.

We see immediately that Hamiltonian Cycle (for Undirected Graphs) is in $NP$. To prove that it is $NP$-complete, we will reduce Hamiltonian Cycle (for Directed Graphs) to it. This means that we provide a method running in polynomial time that converts every instance of Hamiltonian Cycle (for Directed Graphs) to an instance of Hamiltonian Cycle (for Undirected Graphs) such that the first problem has a solution iff the converted problem has a solution. This is an easy reduction.

(4) Traveling Salesman Problem

We are given a set $\{c_1, c_2, \ldots, c_n\}$ of $n \geq 2$ cities, and an $n \times n$ matrix $D = (d_{ij})$ of nonnegative integers, where $d_{ij}$ is the distance (or cost) of traveling from city $c_i$ to city $c_j$. We assume that $d_{ii} = 0$ and $d_{ij} = d_{ji}$ for all $i, j$, so that the matrix $D$ is symmetric and has zero diagonal.

**Traveling Salesman Problem:** Given some $n \times n$ matrix $D = (d_{ij})$ as above and some integer $B \geq 0$ (the budget of the traveling salesman), find a permutation $\pi$ of $\{1, 2, \ldots, n\}$ such that

$$c(\pi) = d_{\pi(1)\pi(2)} + d_{\pi(2)\pi(3)} + \cdots + d_{\pi(n-1)\pi(n)} + d_{\pi(n)\pi(1)} \leq B.$$
The quantity $c(\pi)$ is the cost of the trip specified by $\pi$. The Traveling Salesman Problem has been stated in terms of a budget so that it has a yes or no answer, which allows us to convert it into a language. A minimal solution corresponds to the smallest feasible value of $B$.

**Example 10.1.** Consider the $4 \times 4$ symmetric matrix given by

$$D = \begin{pmatrix}
0 & 2 & 1 & 1 \\
2 & 0 & 1 & 1 \\
1 & 1 & 0 & 3 \\
1 & 1 & 3 & 0
\end{pmatrix},$$

and the budget $B = 4$. The tour specified by the permutation

$$\pi = \begin{pmatrix}
1 & 2 & 3 & 4 \\
1 & 4 & 2 & 3
\end{pmatrix}$$

has cost 4, since

$$c(\pi) = d_{\pi(1)\pi(2)} + d_{\pi(2)\pi(3)} + d_{\pi(3)\pi(4)} + d_{\pi(4)\pi(1)}$$

$$= d_{14} + d_{42} + d_{23} + d_{31}$$

$$= 1 + 1 + 1 + 1 = 4.$$
The cities in this tour are traversed in the order

\[(1, 4, 2, 3, 1)\].

It is clear that the **Traveling Salesman Problem** is in \(\mathcal{NP}\). To show that it is \(\mathcal{NP}\)-complete, we reduce the **Hamiltonian Cycle Problem (Undirected Graphs)** to it. This means that we provide a method running in polynomial time that converts every instance of **Hamiltonian Cycle Problem (Undirected Graphs)** to an instance of the **Traveling Salesman Problem** such that the first problem has a solution iff the converted problem has a solution.

(5) **Independent Set**

The problem is this: Given an undirected graph \(G = (V, E)\) and an integer \(K \geq 2\), is there a set \(C\) of nodes with \(|C| \geq K\) such that for all \(v_i, v_j \in C\), there is no edge \(\{v_i, v_j\} \in E\)?

A maximal independent set with 3 nodes is shown in Figure 10.4. A maximal solution

![Figure 10.4: A maximal Independent Set in a graph](image)

corresponds to the largest feasible value of \(K\). The problem **Independent Set** is obviously in \(\mathcal{NP}\). To show that it is \(\mathcal{NP}\)-complete, we reduce **Exact 3-Satisfiability** to it. This means that we provide a method running in polynomial time that converts every instance of **Exact 3-Satisfiability** to an instance of **Independent Set** such that the first problem has a solution iff the converted problem has a solution.
(6) **Clique**

The problem is this: Given an undirected graph $G = (V, E)$ and an integer $K \geq 2$, is there a set $C$ of nodes with $|C| \geq K$ such that for all $v_i, v_j \in C$, there is some edge $\{v_i, v_j\} \in E$? Equivalently, does $G$ contain a complete subgraph with at least $K$ nodes?

A maximal clique with 4 nodes is shown in Figure 10.5. A maximal solution corresponds to the largest feasible value of $K$. The problem Clique is obviously in $\text{NP}$. To show that it is $\text{NP}$-complete, we reduce Independent Set to it. This means that we provide a method running in polynomial time that converts every instance of Independent Set to an instance of Clique such that the first problem has a solution iff the converted problem has a solution.

Figure 10.5: A maximal Clique in a graph

(7) **Node Cover**

The problem is this: Given an undirected graph $G = (V, E)$ and an integer $B \geq 2$, is there a set $C$ of nodes with $|C| \leq B$ such that $C$ covers all edges in $G$, which means that for every edge $\{v_i, v_j\} \in E$, either $v_i \in C$ or $v_j \in C$?

A minimal node cover with 6 nodes is shown in Figure 10.6. A minimal solution corresponds to the smallest feasible value of $B$. The problem Node Cover is obviously in $\text{NP}$. To show that it is $\text{NP}$-complete, we reduce Independent Set to it. This means that we provide a method running in polynomial time that converts every instance of
10.1. STATEMENTS OF THE PROBLEMS

Figure 10.6: A minimal Node Cover in a graph

**Independent Set** to an instance of **Node Cover** such that the first problem has a solution iff the converted problem has a solution.

The Node Cover problem has the following interesting interpretation: think of the nodes of the graph as rooms of a museum (or art gallery *etc.*), and each edge as a straight corridor that joins two rooms. Then Node Cover may be useful in assigning as few as possible guards to the rooms, so that all corridors can be seen by a guard.

(8) **Knapsack** (also called **Subset sum**)

The problem is this: Given a finite nonempty set $S = \{a_1, a_2, \ldots, a_n\}$ of nonnegative integers, and some integer $K \geq 0$, all represented in binary, is there a nonempty subset $I \subseteq \{1, 2, \ldots, n\}$ such that

$$\sum_{i \in I} a_i = K?$$

A “concrete” realization of this problem is that of a hiker who is trying to fill her/his backpack to its maximum capacity with items of varying weights or values.

It is easy to see that the **Knapsack** Problem is in $\mathcal{NP}$. To show that it is $\mathcal{NP}$-complete, we reduce **Exact Cover** to it. This means that we provide a method running in polynomial time that converts every instance of **Exact Cover** to an instance of **Knapsack** Problem such that the first problem has a solution iff the converted problem has a solution.
Remark: The 0-1 Knapsack Problem is defined as the following problem. Given a set of $n$ items, numbered from 1 to $n$, each with a weight $w_i \in \mathbb{N}$ and a value $v_i \in \mathbb{N}$, given a maximum capacity $W \in \mathbb{N}$ and a budget $B \in \mathbb{N}$, is there a set of $n$ variables $x_1, \ldots, x_n$ with $x_i \in \{0, 1\}$ such that

\[
\sum_{i=1}^{n} x_i v_i \geq B,
\]

\[
\sum_{i=1}^{n} x_i w_i \leq W.
\]

Informally, the problem is to pick items to include in the knapsack so that the sum of the values exceeds a given minimum $B$ (the goal is to maximize this sum), and the sum of the weights is less than or equal to the capacity $W$ of the knapsack. A maximal solution corresponds to the largest feasible value of $B$.

The Knapsack Problem as we defined it (which is how Lewis and Papadimitriou define it) is the special case where $v_i = w_i = 1$ for $i = 1, \ldots, n$ and $W = B$. For this reason, it is also called the Subset Sum Problem. Clearly, the Knapsack (Subset Sum) Problem reduces to the 0-1 Knapsack Problem, and thus the 0-1 Knapsack Problem is also NP-complete.

(9) Inequivalence of ∗-free Regular Expressions

Recall that the problem of deciding the equivalence $R_1 \cong R_2$ of two regular expressions $R_1$ and $R_2$ is the problem of deciding whether $R_1$ and $R_2$ define the same language, that is, $L[R_1] = L[R_2]$. Is this problem in $\mathcal{NP}$?

In order to show that the equivalence problem for regular expressions is in $\mathcal{NP}$ we would have to be able to somehow check in polynomial time that two expressions define the same language, but this is still an open problem.

What might be easier is to decide whether two regular expressions $R_1$ and $R_2$ are inequivalent. For this, we just have to find a string $w$ such that either $w \in L[R_1] - L[R_2]$ or $w \in L[R_2] - L[R_1]$. The problem is that if we can guess such a string $w$, we still have to check in polynomial time that $w \in (L[R_1] - L[R_2]) \cup (L[R_2] - L[R_1])$, and this implies that there is a bound on the length of $w$ which is polynomial in the sizes of $R_1$ and $R_2$. Again, this is an open problem.

To obtain a problem in $\mathcal{NP}$ we have to consider a restricted type of regular expressions, and it turns out that ∗-free regular expressions are the right candidate. A ∗-free regular expression is a regular expression which is built up from the atomic expressions using only + and ·, but not ∗. For example,

\[
R = ((a + b)aa(a + b) + aba(a + b)b)
\]
is such an expression.

It is easy to see that if $R$ is a $\ast$-free regular expression, then for every string $w \in \mathcal{L}[R]$ we have $|w| \leq |R|$. In particular, $\mathcal{L}[R]$ is finite. The above observation shows that if $R_1$ and $R_2$ are $\ast$-free and if there is a string $w \in (\mathcal{L}[R_1] - \mathcal{L}[R_2]) \cup (\mathcal{L}[R_2] - \mathcal{L}[R_1])$, then $|w| \leq |R_1| + |R_2|$, so we can indeed check this in polynomial time. It follows that the inequivalence problem for $\ast$-free regular expressions is in $\mathcal{NP}$. To show that it is $\mathcal{NP}$-complete, we reduce the Satisfiability Problem to it. This means that we provide a method running in polynomial time that converts every instance of Satisfiability Problem to an instance of Inequivalence of Regular Expressions such that the first problem has a solution iff the converted problem has a solution.

Observe that both problems of Inequivalence of Regular Expressions and Equivalence of Regular Expressions are as hard as Inequivalence of $\ast$-free Regular Expressions, since if we could solve the first two problems in polynomial time, then we we could solve Inequivalence of $\ast$-free Regular Expressions in polynomial time, but since this problem is $\mathcal{NP}$-complete, we would have $\mathcal{P} = \mathcal{NP}$. This is very unlikely, so the complexity of Equivalence of Regular Expressions remains open.

(10) 0-1 integer programming problem

Let $A$ be any $p \times q$ matrix with integer coefficients and let $b \in \mathbb{Z}^p$ be any vector with integer coefficients. The 0-1 integer programming problem is to find whether a system of $p$ linear equations in $q$ variables

\[
\begin{align*}
    a_{11}x_1 + \cdots + a_{1q}x_q &= b_1 \\
    \vdots & \quad \vdots \\
    a_{i1}x_1 + \cdots + a_{iq}x_q &= b_i \\
    \vdots & \quad \vdots \\
    a_{p1}x_1 + \cdots + a_{pq}x_q &= b_p
\end{align*}
\]

with $a_{ij}, b_i \in \mathbb{Z}$ has any solution $x \in \{0, 1\}^q$, that is, with $x_i \in \{0, 1\}$. In matrix form, if we let

\[
A = \begin{pmatrix}
    a_{11} & \cdots & a_{1q} \\
    \vdots & \ddots & \vdots \\
    a_{p1} & \cdots & a_{pq}
\end{pmatrix}, \quad b = \begin{pmatrix}
    b_1 \\
    \vdots \\
    b_p
\end{pmatrix}, \quad x = \begin{pmatrix}
    x_1 \\
    \vdots \\
    x_q
\end{pmatrix},
\]

then we write the above system as

\[
Ax = b.
\]

It is immediate that 0-1 integer programming problem is in $\mathcal{NP}$. To prove that it is $\mathcal{NP}$-complete we reduce the bounded tiling problem to it. This means that
we provide a method running in polynomial time that converts every instance of the bounded tiling problem to an instance of the 0-1 integer programming problem such that the first problem has a solution iff the converted problem has a solution.

10.2 Proofs of \( \mathcal{NP} \)-Completeness

(1) Exact Cover

To prove that Exact Cover is \( \mathcal{NP} \)-complete, we reduce the Satisfiability Problem to it:

Satisfiability Problem \( \leq_p \) Exact Cover

Given a set \( F = \{C_1, \ldots, C_\ell\} \) of \( \ell \) clauses constructed from \( n \) propositional variables \( x_1, \ldots, x_n \), we must construct in polynomial time an instance \( \tau(F) = (U, F) \) of Exact Cover such that \( F \) is satisfiable iff \( \tau(F) \) has a solution.

Example 10.2. If

\[
F = \{C_1 = (x_1 \lor \overline{x}_2), C_2 = (\overline{x}_1 \lor x_2 \lor x_3), C_3 = (x_2), C_4 = (\overline{x}_2 \lor \overline{x}_3)\},
\]

then the universe \( U \) is given by

\[
U = \{x_1, x_2, x_3, C_1, C_2, C_3, C_4, p_{11}, p_{12}, p_{21}, p_{22}, p_{23}, p_{31}, p_{41}, p_{42}\},
\]

and the family \( F \) consists of the subsets

\[
\begin{align*}
T_{1,F} &= \{x_1, p_{11}\} \\
T_{1,T} &= \{x_1, p_{21}\} \\
T_{2,F} &= \{x_2, p_{22}, p_{31}\} \\
T_{2,T} &= \{x_2, p_{12}, p_{41}\} \\
T_{3,F} &= \{x_3, p_{23}\} \\
T_{3,T} &= \{x_3, p_{42}\} \\
\{C_1, p_{11}\}, \{C_1, p_{12}\}, \{C_2, p_{21}\}, \{C_2, p_{22}\}, \{C_2, p_{23}\}, \\
\{C_3, p_{31}\}, \{C_4, p_{41}\}, \{C_4, p_{42}\}.
\end{align*}
\]

It is easy to check that the set \( \mathcal{C} \) consisting of the following subsets is an exact cover:

\[
\begin{align*}
T_{1,T} &= \{x_1, p_{21}\}, T_{2,T} = \{x_2, p_{12}, p_{41}\}, T_{3,F} = \{x_3, p_{23}\}, \\
\{C_1, p_{11}\}, \{C_2, p_{22}\}, \{C_3, p_{31}\}, \{C_4, p_{42}\}.
\end{align*}
\]
10.2. PROOFS OF N\(\mathcal{P}\)-COMPLETENESS

The general method to construct \((U, \mathcal{F})\) from \(F = \{C_1, \ldots, C_\ell\}\) proceeds as follows. Say

\[ C_j = (L_{j1} \lor \cdots \lor L_{jm_j}) \]

is the \(j\)th clause in \(F\), where \(L_{jk}\) denotes the \(k\)th literal in \(C_j\) and \(m_j \geq 1\). The universe of \(\tau(F)\) is the set

\[ U = \{x_i \mid 1 \leq i \leq n\} \cup \{C_j \mid 1 \leq j \leq \ell\} \cup \{p_{jk} \mid 1 \leq j \leq \ell, 1 \leq k \leq m_j\} \]

where in the third set \(p_{jk}\) corresponds to the \(k\)th literal in \(C_j\).

The following subsets are included in \(\mathcal{F}\):

(a) There is a set \(\{p_{jk}\}\) for every \(p_{jk}\).

(b) For every boolean variable \(x_i\), the following two sets are in \(\mathcal{F}\):

\[ T_{i,\overline{T}} = \{x_i\} \cup \{p_{jk} \mid L_{jk} = \overline{x_i}\} \]

which contains \(x_i\) and all negative occurrences of \(x_i\), and

\[ T_{i,T} = \{x_i\} \cup \{p_{jk} \mid L_{jk} = x_i\} \]

which contains \(x_i\) and all its positive occurrences. Note carefully that \(T_{i,\overline{T}}\) involves negative occurrences of \(x_i\) whereas \(T_{i,T}\) involves positive occurrences of \(x_i\).

(c) For every clause \(C_j\), the \(m_j\) sets \(\{C_j, p_{jk}\}\) are in \(\mathcal{F}\).

It remains to prove that \(F\) is satisfiable iff \(\tau(F)\) has a solution. We claim that if \(v\) is a truth assignment that satisfies \(F\), then we can make an exact cover \(C\) as follows:

For each \(x_i\), we put the subset \(T_{i,\overline{T}}\) in \(C\) iff \(v(x_i) = \overline{T}\), else we we put the subset \(T_{i,T}\) in \(C\) iff \(v(x_i) = T\). Also, for every clause \(C_j\), we put some subset \(\{C_j, p_{jk}\}\) in \(C\) for a literal \(L_{jk}\) which is made true by \(v\). By construction of \(T_{i,\overline{T}}\) and \(T_{i,T}\), this \(p_{jk}\) is not in any set in \(C\) selected so far. Since by hypothesis \(F\) is satisfiable, such a literal exists for every clause. Having covered all \(x_i\) and \(C_j\), we put a set \(\{p_{jk}\}\) in \(C\) for every remaining \(p_{jk}\) which has not yet been covered by the sets already in \(C\).

Going back to Example 10.2, the truth assignment \(v(x_1) = T, v(x_2) = T, v(x_3) = F\) satisfies \(F\), so we put

\[ T_{1,T} = \{x_1, p_{21}\}, T_{2,T} = \{x_2, p_{12}, p_{41}\}, T_{3,F} = \{x_3, p_{23}\}, \{C_1, p_{11}\}, \{C_2, p_{22}\}, \{C_3, p_{31}\}, \{C_4, p_{42}\} \]

in \(C\).

We leave as an exercise to check that the above procedure works.

Conversely, if \(C\) is an exact cover of \(\tau(F)\), we define a truth assignment as follows:

For every \(x_i\), if \(T_{i,T}\) is in \(C\), then we set \(v(x_i) = T\), else if \(T_{i,F}\) is in \(C\), then we set \(v(x_i) = F\). We leave it as an exercise to check that this procedure works.
Example 10.3. Given the exact cover

\[ T_1, T = \{ x_1, p_{21} \}, T_2, T = \{ x_2, p_{12}, p_{41} \}, T_3, F = \{ x_3, p_{23} \}, \]
\[ \{ C_1, p_{11} \}, \{ C_2, p_{22} \}, \{ C_3, p_{31} \}, \{ C_4, p_{42} \}, \]

we get the satisfying assignment \( v(x_1) = T, v(x_2) = T, v(x_3) = F \).

If we now consider the proposition is CNF given by

\[ F_2 = \{ C_1 = (x_1 \lor x_2), C_2 = (x_1 \lor x_2 \lor x_3), C_3 = (x_2), C_4 = (x_2 \lor x_3 \lor x_4) \} \]

where we have added the boolean variable \( x_4 \) to clause \( C_4 \), then \( U \) also contains \( x_4 \) and \( p_{43} \) so we need to add the following subsets to \( F \):

\[ T_4, F = \{ x_4, p_{43} \}, T_4, T = \{ x_4 \}, \{ C_4, p_{43} \}, \{ p_{43} \}. \]

The truth assignment \( v(x_1) = T, v(x_2) = T, v(x_3) = F, v(x_4) = T \) satisfies \( F_2 \), so an exact cover \( C \) is

\[ T_1, T = \{ x_1, p_{21} \}, T_2, T = \{ x_2, p_{12}, p_{41} \}, T_3, F = \{ x_3, p_{23} \}, T_4, T = \{ x_4 \}, \]
\[ \{ C_1, p_{11} \}, \{ C_2, p_{22} \}, \{ C_3, p_{31} \}, \{ C_4, p_{42} \}, \{ p_{43} \}. \]

Observe that this time, because the truth assignment \( v \) makes both literals corresponding to \( p_{42} \) and \( p_{43} \) true and since we picked \( p_{42} \) to form the subset \( \{ C_4, p_{42} \} \), we need to add the singleton \( \{ p_{43} \} \) to \( C \) to cover all elements of \( U \).

(2) Hamiltonian Cycle (for Directed Graphs)

To prove that Hamiltonian Cycle (for Directed Graphs) is \( \mathcal{NP} \)-complete, we will reduce Exact Cover to it:

Exact Cover \( \leq_P \) Hamiltonian Cycle (for Directed Graphs)

We need to find an algorithm working in polynomial time that converts an instance \( (U, \mathcal{F}) \) of Exact Cover to a directed graph \( G = \tau(U, \mathcal{F}) \) such that \( G \) has a Hamiltonian cycle iff \( (U, \mathcal{F}) \) has an exact cover.

The construction of the graph \( G \) uses a trick involving a small subgraph \( \text{Gad} \) with 7 (distinct) nodes known as a gadget shown in Figure 10.7.
The crucial property of the graph \textit{Gad} is that if \textit{Gad} is a subgraph of a bigger graph \textit{G} in such a way that no edge of \textit{G} is incident to any of the nodes \(u, v, w\) unless it is one of the eight edges of \textit{Gad} incident to the nodes \(u, v, w\), then for any Hamiltonian cycle in \textit{G}, either the path \((a,u),(u,v),(v,w),(w,b)\) is traversed or the path \((c,w),(w,v),(v,u),(u,d)\) is traversed, but not both.

The reader should convince herself/himself that indeed, any Hamiltonian cycle that does not traverse either the subpath \((a,u),(u,v),(v,w),(w,b)\) from \(a\) to \(b\) or the subpath \((c,w),(w,v),(v,u),(u,d)\) from \(c\) to \(d\) will not traverse one of the nodes \(u, v, w\).

Also, the fact that node \(v\) is traversed exactly once forces only one of the two paths to be traversed but not both. The reader should also convince herself/himself that a smaller graph does not guarantee the desired property.

It is convenient to use the simplified notation with a special type of edge labeled with the exclusive or sign \(\oplus\) between the “edges” between \(a\) and \(b\) and between \(d\) and \(c\), as shown in Figure 10.8.

Whenever such a figure occurs, the actual graph is obtained by substituting a copy of the graph \textit{Gad} (the four nodes \(a, b, c, d\) must be distinct). This abbreviating device
can be extended to the situation where we build gadgets between a given pair \((a, b)\) and several other pairs \((c_1, d_1), \ldots, (c_m, d_m)\), all nodes being distinct, as illustrated in Figure 10.9.

Either all three edges \((c_1, d_1), (c_2, d_2), (c_3, d_3)\) are traversed or the edge \((a, b)\) is traversed, and these possibilities are mutually exclusive.

![Figure 10.9: A shorthand notation for several gadgets](image)

The graph \(G = \tau(U, F)\) where \(U = \{u_1, \ldots, u_n\}\) (with \(n \geq 1\)) and \(F = \{S_1, \ldots, S_m\}\) (with \(m \geq 1\)) is constructed as follows:

The graph \(G\) has \(m + n + 2\) nodes \(\{u_0, u_1, \ldots, u_n, S_0, S_1, \ldots, S_m\}\). Note that we have added two extra nodes \(u_0\) and \(S_0\). For \(i = 1, \ldots, m\), there are two edges \((S_{i-1}, S_i)_1\) and \((S_{i-1}, S_i)_2\) from \(S_{i-1}\) to \(S_i\). For \(j = 1, \ldots, n\), from \(u_{j-1}\) to \(u_j\), there are as many edges as there are sets \(S_i \in F\) containing the element \(u_j\). We can think of each edge between \(u_{j-1}\) and \(u_j\) as an occurrence of \(u_j\) in a uniquely determined set \(S_i \in F\); we denote this edge by \((u_{j-1}, u_j)_i\). We also have an edge from \(u_n\) to \(S_0\) and an edge from \(S_m\) to \(u_0\), thus “closing the cycle.”

What we have constructed so far is not a legal graph since it may have many parallel edges, but are going to turn it into a legal graph by pairing edges between the \(u_j\)’s and edges between the \(S_i\)’s. Indeed, since each edge \((u_{j-1}, u_j)_i\) between \(u_{j-1}\) and \(u_j\) corresponds to an occurrence of \(u_j\) in some uniquely determined set \(S_i \in F\) (that is, \(u_j \in S_i\)), we put an exclusive-or edge between the edge \((u_{j-1}, u_j)_i\) and the edge \((S_{i-1}, S_i)_2\) between \(S_{i-1}\) and \(S_i\), which we call the long edge. The other edge \((S_{i-1}, S_i)_1\) between \(S_{i-1}\) and \(S_i\) (not paired with any other edge) is called the short edge. Effectively, we put a copy of the gadget graph \(Gad\) with \(a = u_{j-1}, b = u_j, c = S_{i-1}, d = S_i\) for any pair \((u_j, S_i)\) such that \(u_j \in S_i\). The resulting object is indeed a directed graph with no parallel edges.
Example 10.4. The above construction is illustrated in Figure 10.10 for the instance of the exact cover problem given by

\[ U = \{u_1, u_2, u_3, u_4\}, \quad \mathcal{F} = \{S_1 = \{u_3, u_4\}, \quad S_2 = \{u_2, u_3, u_4\}, \quad S_3 = \{u_1, u_2\}\}. \]

It remains to prove that \((U, \mathcal{F})\) has an exact cover iff the graph \(G = \tau(U, \mathcal{F})\) has a Hamiltonian cycle. First, assume that \(G\) has a Hamiltonian cycle. If so, for every \(j\) some unique “edge” \((u_{j-1}, u_j)\) is traversed once (since every \(u_j\) is traversed once), and by the exclusive-or nature of the gadget graphs, the corresponding long edge \((S_{i-1}, S_i)_{2}\) can’t be traversed, which means that the short edge \((S_{i-1}, S_i)_{1}\) is traversed. Consequently, if \(\mathcal{C}\) consists of those subsets \(S_i\) such that the short edge \((S_{i-1}, S_i)_{1}\) is traversed, then \(\mathcal{C}\) consists of pairwise disjoint subsets whose union is \(U\), namely \(\mathcal{C}\) is an exact cover.
In our example, there is a Hamiltonian where the blue edges are traversed between the $S_i$ nodes, and the red edges are traversed between the $u_j$ nodes, namely

$$\text{short } (S_0, S_1), \text{ long } (S_1, S_2), \text{ short } (S_2, S_3), \text{ (}S_3, u_0\text{)},$$

$$(u_0, u_1)_3, (u_1, u_2)_3, (u_2, u_3)_1, (u_3, u_4)_1, (u_4, S_0).$$

The subsets corresponding to the short $(S_{i-1}, S_i)$ edges are $S_1$ and $S_3$, and indeed $\mathcal{C} = \{S_1, S_3\}$ is an exact cover.

Note that the exclusive-or property of the gadgets implies the following: since the edge $(u_0, u_1)_3$ must be chosen to obtain a Hamiltonian, the long edge $(S_2, S_3)$ can’t be chosen, so the edge $(u_1, u_2)_3$ must be chosen, but then the edge $(u_1, u_2)_2$ is not chosen so the long edge $(S_1, S_2)$ must be chosen, so the edges $(u_2, u_3)_2$ and $(u_3, u_4)_2$ can’t be chosen, and thus edges $(u_2, u_3)_1$ and $(u_3, u_4)_1$ must be chosen.

Conversely, if $\mathcal{C}$ is an exact cover for $(U, \mathcal{F})$, then consider the path in $G$ obtained by traversing each short edge $(S_{i-1}, S_i)_1$ for which $S_i \in \mathcal{C}$, each edge $(u_{j-1}, u_j)_i$ such that $u_j \in S_j$, which means that this edge is connected by a $\oplus$-sign to the long edge $(S_{i-1}, S_i)_2$ (by construction, for each $u_j$ there is a unique such $S_i$), and the edges $(u_0, S_0)$ and $(S_m, u_0)$, then we obtain a Hamiltonian cycle.

In our example, the exact cover $\mathcal{C} = \{S_1, S_3\}$ yields the Hamiltonian

$$\text{short } (S_0, S_1), \text{ long } (S_1, S_2), \text{ short } (S_2, S_3), \text{ (}S_3, u_0\text{)},$$

$$(u_0, u_1)_3, (u_1, u_2)_3, (u_2, u_3)_1, (u_3, u_4)_1, (u_4, S_0)$$

that we encountered earlier.

(3) **Hamiltonian Cycle (for Undirected Graphs)**

To show that **Hamiltonian Cycle (for Undirected Graphs)** is $\mathcal{NP}$-complete we reduce **Hamiltonian Cycle (for Directed Graphs)** to it:

**Hamiltonian Cycle (for Directed Graphs) $\leq_F$ Hamiltonian Cycle (for Undirected Graphs)**

Given any directed graph $G = (V, E)$ we need to construct in polynomial time an undirected graph $\tau(G) = G' = (V', E')$ such that $G$ has a (directed) Hamiltonian cycle iff $G'$ has a (undirected) Hamiltonian cycle. This is easy. We make three distinct copies $v_0, v_1, v_2$ of every node $v \in V$ which we put in $V'$, and for every edge $(u, v) \in E$ we create five edges $\{u_0, u_1\}, \{u_1, u_2\}, \{u_2, v_0\}, \{v_0, v_1\}, \{v_1, v_2\}$ which we put in $E'$, as illustrated in the diagram shown in Figure 10.11.

The crucial point about the graph $G'$ is that although there may be several edges adjacent to a node $u_0$ or a node $u_2$, the only way to reach $u_1$ from $u_0$ is through the edge $\{u_0, u_1\}$ and the only way to reach $u_1$ from $u_2$ is through the edge $\{u_1, u_2\}$. 
10.2. PROOFS OF $\mathcal{NP}$-COMPLETENESS

Suppose there is a Hamiltonian cycle in $G'$. If this cycle arrives at a node $u_0$ from the node $u_1$, then by the above remark, the previous node in the cycle must be $u_2$. Then, the predecessor of $u_2$ in the cycle must be a node $v_0$ such that there is an edge $\{u_2, v_0\}$ in $G'$ arising from an edge $(u, v)$ in $G$. The nodes in the cycle in $G'$ are traversed in the order $(v_0, u_2, u_1, u_0)$ where $v_0$ and $u_2$ are traversed in the opposite order in which they occur as the endpoints of the edge $(u, v)$ in $G$. If so, consider the reverse of our Hamiltonian cycle in $G'$, which is also a Hamiltonian cycle since $G'$ is unoriented. In this cycle, we go from $u_0$ to $u_1$, then to $u_2$, and finally to $v_0$. In $G$, we traverse the edge from $u$ to $v$. In order for the cycle in $G'$ to be Hamiltonian, we must continue by visiting $v_1$ and $v_2$, since otherwise $v_1$ is never traversed. Now, the next node $w_0$ in the Hamiltonian cycle in $G'$ corresponds to an edge $(v, w)$ in $G$, and by repeating our reasoning we see that our Hamiltonian cycle in $G'$ determines a Hamiltonian cycle in $G$. We leave it as an easy exercise to check that a Hamiltonian cycle in $G$ yields a Hamiltonian cycle in $G'$.

(4) Traveling Salesman Problem

To show that the Traveling Salesman Problem is $\mathcal{NP}$-complete, we reduce the Hamiltonian Cycle Problem (Undirected Graphs) to it:

Hamiltonian Cycle Problem (Undirected Graphs) $\leq_P$ Traveling Salesman Problem

This is a fairly easy reduction.

Given an undirected graph $G = (V, E)$, we construct an instance $\tau(G) = (D, B)$ of the traveling salesman problem so that $G$ has a Hamiltonian cycle iff the traveling salesman problem has a solution. If we let $n = |V|$, we have $n$ cities and the matrix $D = (d_{ij})$ is defined as follows:

$$d_{ij} = \begin{cases} 
0 & \text{if } i = j \\
1 & \text{if } \{v_i, v_j\} \in E \\
2 & \text{otherwise.}
\end{cases}$$

We also set the budget $B$ as $B = n$. 
Any tour of the cities has cost equal to \( n \) plus the number of pairs \((v_i, v_j)\) such that \( i \neq j \) and \( \{v_i, v_j\} \) is not an edge of \( G \). It follows that a tour of cost \( n \) exists iff there are no pairs \((v_i, v_j)\) of the second kind iff the tour is a Hamiltonian cycle.

The reduction from Hamiltonian Cycle Problem (Undirected Graphs) to the Traveling Salesman Problem is quite simple, but a direct reduction of say Satisfiability to the Traveling Salesman Problem is hard. By breaking this reduction into several steps made it simpler to achieve.

(5) **Independent Set**

To show that Independent Set is \( \mathcal{NP} \)-complete, we reduce Exact 3-Satisfiability to it:

**Exact 3-Satisfiability \( \leq_p \) Independent Set**

Recall that in Exact 3-Satisfiability every clause \( C_i \) has exactly three literals \( L_{i1}, L_{i2}, L_{i3} \).

Given a set \( F = \{C_1, \ldots, C_m\} \) of \( m \geq 2 \) such clauses, we construct in polynomial time an undirected graph \( G = (V, E) \) such that \( F \) is satisfiable iff \( G \) has an independent set \( C \) with at least \( K = m \) nodes.

For every \( i \) \((1 \leq i \leq m)\), we have three nodes \( c_{i1}, c_{i2}, c_{i3} \) corresponding to the three literals \( L_{i1}, L_{i2}, L_{i3} \) in clause \( C_i \), so there are \( 3m \) nodes in \( V \). The “core” of \( G \) consists of \( m \) triangles, one for each set \( \{c_{i1}, c_{i2}, c_{i3}\} \). We also have an edge \( \{c_{ik}, c_{j\ell}\} \) iff \( L_{ik} \) and \( L_{j\ell} \) are complementary literals.

**Example 10.5.** Let \( F \) be the set of clauses

\[
F = \{C_1 = (x_1 \lor \overline{x}_2 \lor x_3), \ C_2 = (\overline{x}_1 \lor \overline{x}_2 \lor x_3), \ C_3 = (\overline{x}_1 \lor \overline{x}_2 \lor \overline{x}_3), \ C_4 = (x_1 \lor x_2 \lor x_3)\}.
\]

The graph \( G \) associated with \( F \) is shown in Figure 10.12.

It remains to show that the construction works. Since any three nodes in a triangle are connected, an independent set \( C \) can have at most one node per triangle and thus has at most \( m \) nodes. Since the budget is \( K = m \), we may assume that there is an independent set with \( m \) nodes. Define a (partial) truth assignment by

\[
v(x_i) = \begin{cases} 
T & \text{if } L_{jk} = x_i \text{ and } c_{jk} \in C \\
F & \text{if } L_{jk} = \overline{x}_i \text{ and } c_{jk} \in C.
\end{cases}
\]

Since the non-triangle edges in \( G \) link nodes corresponding to complementary literals and nodes in \( C \) are not connected, our truth assignment does not assign clashing truth values to the variables \( x_i \). Not all variables may receive a truth value, in which case
we assign an arbitrary truth value to the unassigned variables. This yields a satisfying assignment for $F$.

In Example 10.5, the set $C = \{c_{11}, c_{22}, c_{32}, c_{41}\}$ corresponding to the nodes shown in red in Figure 10.12 form an independent set, and they induce the partial truth assignment $v(x_1) = T, v(x_2) = F$. The variable $x_3$ can be assigned an arbitrary value, say $v(x_3) = F$, and $v$ is indeed a satisfying truth assignment for $F$.

Conversely, if $v$ is a truth assignment for $F$, then we obtain an independent set $C$ of size $m$ by picking for each clause $C_i$ a node $c_{ik}$ corresponding to a literal $L_{ik}$ whose value under $v$ is $T$.

(6) **Clique**

To show that **Clique** is $\mathcal{NP}$-complete, we reduce **Independent Set** to it:

**Independent Set $\leq_P$ Clique**

The key the reduction is the notion of the complement of an undirected graph $G = (V, E)$. The complement $G^c = (V, E^c)$ of the graph $G = (V, E)$ is the graph with the same set of nodes $V$ as $G$ but there is an edge $\{u, v\}$ (with $u \neq v$) in $E^c$ iff $\{u, v\} \notin E$. Then, it is not hard to check that there is a bijection between maximum independent sets in $G$ and maximum cliques in $G^c$. The reduction consists in constructing from a graph $G$ its complement $G^c$, and then $G$ has an independent set iff $G^c$ has a clique.

This construction is illustrated in Figure 10.13, where a maximum independent set in the graph $G$ is shown in blue and a maximum clique in the graph $G^c$ is shown in red.

Figure 10.12: The graph constructed from the clauses of Example 10.5
(7) **Node Cover**

To show that **Node Cover** is \( \mathcal{NP} \)-complete, we reduce **Independent Set** to it:

**Independent Set \( \leq_P \) Node Cover**

This time the crucial observation is that if \( N \) is an independent set in \( G \), then the complement \( C = V - N \) of \( N \) in \( V \) is a node cover in \( G \). Thus there is an independent set of size at least \( K \) iff there is a node cover of size at most \( n - K \) where \( n = |V| \) is the number of nodes in \( V \). The reduction leaves the graph unchanged and replaces \( K \) by \( n - K \). An example is shown in Figure 10.14 where an independent set is shown in blue and a node cover is shown in red.

(8) **Knapsack (also called Subset sum)**

To show that **Knapsack** is \( \mathcal{NP} \)-complete, we reduce **Exact Cover** to it:

**Exact Cover \( \leq_P \) Knapsack**

Given an instance \((U, \mathcal{F})\) of set cover with \( U = \{u_1, \ldots, u_n\} \) and \( \mathcal{F} = \{S_1, \ldots, S_m\} \), a family of subsets of \( U \), we need to produce in polynomial time an instance \( \tau(U, \mathcal{F}) \) of the knapsack problem consisting of \( k \) nonnegative integers \( a_1, \ldots, a_k \) and another
integer $K > 0$ such that there is a subset $I \subseteq \{1, \ldots, k\}$ such that $\sum_{i \in I} a_i = K$ iff there is an exact cover of $U$ using subsets in $F$.

The trick here is the relationship between set union and integer addition.

**Example 10.6.** Consider the exact cover problem given by $U = \{u_1, u_2, u_3, u_4\}$ and $F = \{S_1 = \{u_3, u_4\}, S_2 = \{u_2, u_3, u_4\}, S_3 = \{u_1, u_2\}\}$.

We can represent each subset $S_j$ by a binary string $a_j$ of length 4, where the $i$th bit from the left is 1 iff $u_i \in S_j$, and 0 otherwise. In our example

\[
\begin{align*}
  a_1 &= 0011 \\
  a_2 &= 0111 \\
  a_3 &= 1100.
\end{align*}
\]

Then, the trick is that some family $C$ of subsets $S_j$ is an exact cover if the sum of the corresponding numbers $a_j$ adds up to $1111 = 2^4 - 1 = K$. For example,

\[
C = \{S_1 = \{u_3, u_4\}, S_3 = \{u_1, u_2\}\}
\]

is an exact cover and

\[
a_1 + a_3 = 0011 + 1100 = 1111.
\]

Unfortunately, there is a problem with this encoding which has to do with the fact that addition may involve carry. For example, assuming four subsets and the universe $U = \{u_1, \ldots, u_6\}$,

\[
11 + 13 + 15 + 24 = 63,
\]

in binary

\[
001011 + 001101 + 001111 + 011000 = 111111,
\]

but if we convert these binary strings to the corresponding subsets we get the subsets

\[
\begin{align*}
  S_1 &= \{u_3, u_5, u_6\} \\
  S_2 &= \{u_3, u_4, u_6\} \\
  S_3 &= \{u_3, u_4, u_5, u_6\} \\
  S_4 &= \{u_2, u_3\},
\end{align*}
\]

which are not disjoint and do not cover $U$.

The fix is surprisingly simple: use base $m$ (where $m$ is the number of subsets in $F$) instead of base 2.
Example 10.7. Consider the exact cover problem given by \( U = \{u_1, u_2, u_3, u_4, u_5, u_6\} \) and \( F \) given by

\[
\begin{align*}
S_1 &= \{u_3, u_5, u_6\} \\
S_2 &= \{u_3, u_4, u_6\} \\
S_3 &= \{u_3, u_4, u_5, u_6\} \\
S_4 &= \{u_2, u_3\} \\
S_5 &= \{u_1, u_2, u_4\}.
\end{align*}
\]

In base \( m = 5 \), the numbers corresponding to \( S_1, \ldots, S_5 \) are

\[
\begin{align*}
a_1 &= 001011 \\
a_2 &= 001101 \\
a_3 &= 001111 \\
a_4 &= 011000 \\
a_5 &= 110100.
\end{align*}
\]

This time,

\[
a_1 + a_2 + a_3 + a_4 = 001011 + 001101 + 001111 + 011000 = 014223 \neq 111111,
\]

so \( \{S_1, S_2, S_3, S_4\} \) is not a solution. However

\[
a_1 + a_5 = 001011 + 110100 = 111111,
\]

and \( C = \{S_1, S_5\} \) is an exact cover.

Thus, given an instance \((U, F)\) of **Exact Cover** where \( U = \{u_1, \ldots, u_n\} \) and \( F = \{S_1, \ldots, S_m\} \) the reduction to **Knapsack** consists in forming the \( m \) numbers \( a_1, \ldots, a_m \) (each of \( n \) bits) encoding the subsets \( S_j \), namely \( a_{ji} = 1 \) iff \( u_i \in S_j \), else 0, and to let \( K = 1 + m^2 + \cdots + m^{n-1} \), which is represented in base \( m \) by the string \( 11 \cdots 11 \). In testing whether \( \sum_{i \in I} a_i = K \) for some subset \( I \subseteq \{1, \ldots, m\} \), we use arithmetic in base \( m \).

If a candidate solution \( C \) involves at most \( m - 1 \) subsets, then since the corresponding numbers are added in base \( m \), a carry can never happen. If the candidate solution involves all \( m \) subsets, then \( a_1 + \cdots + a_m = K \) iff \( F \) is a partition of \( U \), since otherwise some bit in the result of adding up these \( m \) numbers in base \( m \) is not equal to 1, even if a carry occurs.

(9) Inequivalence of \( \ast \)-free Regular Expressions

To show that **Inequivalence of \( \ast \)-free Regular Expressions** is \( \mathcal{NP} \)-complete, we reduce the **Satisfiability Problem** to it:
10.2. PROOFS OF $\mathcal{NP}$-COMPLETENESS

Satisfiability Problem $\leq_P$ Inequivalence of $*$-free Regular Expressions

We already argued that Inequivalence of $*$-free Regular Expressions is in $\mathcal{NP}$ because if $R$ is a $*$-free regular expression, then for every string $w \in \mathcal{L}[R]$ we have $|w| \leq |R|$. The above observation shows that if $R_1$ and $R_2$ are $*$-free and if there is a string $w \in (\mathcal{L}[R_1] - \mathcal{L}[R_2]) \cup (\mathcal{L}[R_2] - \mathcal{L}[R_1])$, then $|w| \leq |R_1| + |R_2|$, so we can indeed check this in polynomial time. It follows that the inequivalence problem for $*$-free regular expressions is in $\mathcal{NP}$.

We reduce the Satisfiability Problem to the Inequivalence of $*$-free Regular Expressions as follows. For any set of clauses $P = C_1 \land \cdots \land C_p$, if the propositional variables occurring in $P$ are $x_1, \ldots, x_n$, we produce two $*$-free regular expressions $R, S$ over $\Sigma = \{0, 1\}$, such that $P$ is satisfiable iff $L_R \neq L_S$. The expression $S$ is actually

$$S = (0 + 1)(0 + 1) \cdots (0 + 1).$$

The expression $R$ is of the form

$$R = R_1 + \cdots + R_p,$$

where $R_i$ is constructed from the clause $C_i$ in such a way that $L_{R_i}$ corresponds precisely to the set of truth assignments that falsify $C_i$; see below.

Given any clause $C_i$, let $R_i$ be the $*$-free regular expression defined such that, if $x_j$ and $\overline{x}_j$ both belong to $C_i$ (for some $j$), then $R_i = \emptyset$, else

$$R_i = R^1_i \cdot R^2_i \cdots R^n_i,$$

where $R^j_i$ is defined by

$$R^j_i = \begin{cases} 
0 & \text{if } x_j \text{ is a literal of } C_i \\
1 & \text{if } \overline{x}_j \text{ is a literal of } C_i \\
(0 + 1) & \text{if } x_j \text{ does not occur in } C_i.
\end{cases}$$

Clearly, all truth assignments that falsify $C_i$ must assign $\mathbf{F}$ to $x_j$ if $x_j \in C_i$ or assign $\mathbf{T}$ to $x_j$ if $\overline{x}_j \in C_i$. Therefore, $L_{R_i}$ corresponds to the set of truth assignments that falsify $C_i$ (where 1 stands for $\mathbf{T}$ and 0 stands for $\mathbf{F}$) and thus, if we let

$$R = R_1 + \cdots + R_p,$$

then $L_R$ corresponds to the set of truth assignments that falsify $P = C_1 \land \cdots \land C_p$. Since $L_S = \{0, 1\}^n$ (all binary strings of length $n$), we conclude that $L_R \neq L_S$ iff $P$ is satisfiable. Therefore, we have reduced the Satisfiability Problem to our problem and the reduction clearly runs in polynomial time. This proves that the problem of deciding whether $L_R \neq L_S$, for any two $*$-free regular expressions $R$ and $S$ is $\mathcal{NP}$-complete.
(10) 0-1 integer programming problem

It is easy to check that the problem is in \(N^P\).

To prove that the is \(N^P\)-complete we reduce the bounded-tiling problem to it:

**bounded-tiling problem \(\leq_P\) 0-1 integer programming problem**

Given a tiling problem, \(((T, V, H), \hat{\sigma}, \sigma_0)\), we create a 0-1-valued variable \(x_{mnt}\), such that \(x_{mnt} = 1\) iff tile \(t\) occurs in position \((m, n)\) in some tiling. Write equations or inequalities expressing that a tiling exists and then use “slack variables” to convert inequalities to equations. For example, to express the fact that every position is tiled by a single tile, use the equation

\[
\sum_{t \in T} x_{mnt} = 1,
\]

for all \(m, n\) with \(1 \leq m \leq 2s\) and \(1 \leq n \leq s\). We leave the rest as as exercise.

### 10.3 Succinct Certificates, co\(N^P\), and \(\mathcal{E}X^P\)

All the problems considered in Section 10.1 share a common feature, which is that for each problem, a solution is produced nondeterministically (an exact cover, a directed Hamiltonian cycle, a tour of cities, an independent set, a node cover, a clique etc.), and then this candidate solution is checked deterministically and in polynomial time. The candidate solution is a string called a certificate (or witness).

It turns out that membership on \(N^P\) can be defined in terms of certificates. To be a certificate, a string must satisfy two conditions:

1. It must be polynomially succinct, which means that its length is at most a polynomial in the length of the input.
2. It must be checkable in polynomial time.

All “yes” inputs to a problem in \(N^P\) must have at least one certificate, while all “no” inputs must have none.

The notion of certificate can be formalized using the notion of a polynomially balanced language.

**Definition 10.3.** Let \(\Sigma\) be an alphabet, and let “;” be a symbol not in \(\Sigma\). A language \(L' \subseteq \Sigma^*;\Sigma^*\) is said to be polynomially balanced if there exists a polynomial \(p(X)\) such that for all \(x, y \in \Sigma^*\), if \(x; y \in L'\) then \(|y| \leq p(|x|)\).
Suppose $L'$ is a polynomially balanced language and that $L' \in \mathcal{P}$. Then we can consider the language

$$L = \{ x \in \Sigma^* | (\exists y \in \Sigma^*)(x; y \in L') \}.$$ 

The intuition is that for each $x \in L$, the set

$$\{ y \in \Sigma^* | x; y \in L' \}$$

is the set of certificates of $x$. For every $x \in L$, a Turing machine can nondeterministically guess one of its certificates $y$, and then use the deterministic Turing machine for $L'$ to check in polynomial time that $x; y \in L'$. Note that, by definition, strings not in $L$ have no certificate. It follows that $L \in \mathcal{NP}$.

Conversely, if $L \in \mathcal{NP}$ and the alphabet $\Sigma$ has at least two symbols, we can encode the paths in the computation tree for every input $x \in L$, and we obtain a polynomially balanced language $L' \subseteq \Sigma^*; \Sigma^*$ in $\mathcal{P}$ such that

$$L = \{ x \in \Sigma^* | (\exists y \in \Sigma^*)(x; y \in L') \}.$$ 

The details of this construction are left as an exercise. In summary, we obtain the following theorem.

**Theorem 10.1.** Let $L \subseteq \Sigma^*$ be a language over an alphabet $\Sigma$ with at least two symbols, and let ";" be a symbol not in $\Sigma$. Then $L \in \mathcal{NP}$ iff there is a polynomially balanced language $L' \subseteq \Sigma^*; \Sigma^*$ in $\mathcal{P}$ such that

$$L = \{ x \in \Sigma^* | (\exists y \in \Sigma^*)(x; y \in L') \}.$$ 

A striking illustration of the notion of succint certificate is illustrated by the set of composite integers, namely those natural numbers $n \in \mathbb{N}$ that can be written as the product $pq$ of two numbers $p, q \geq 2$ with $p, q \in \mathbb{N}$. For example, the number

$$4, 294, 967, 297$$

is a composite!

This is far from obvious, but if an oracle gives us the certificate $\{6, 700, 417, 641\}$, it is easy to carry out in polynomial time the multiplication of these two numbers and check that it is equal to $4, 294, 967, 297$. Finding a certificate is usually (very) hard, but checking that it works is easy. This is the point of certificates.

We conclude this section with a brief discussion of the complexity classes $\text{coNP}$ and $\text{EXP}$.

By definition,

$$\text{coNP} = \{ \overline{L} | L \in \mathcal{NP} \},$$

where $\overline{L}$ is the complement of $L$.
that is, coNP consists of all complements of languages in NP. Since \( P \subseteq NP \) and \( P \) is closed under complementation,
\[
P \subseteq \text{co}NP,
\]
but nobody knows whether \( NP \) is closed under complementation, that is, nobody knows whether \( NP = \text{co}NP \).

What can be shown is that if \( NP \neq \text{co}NP \) then \( P \neq NP \). However it is possible that \( P \neq NP \) and yet \( NP = \text{co}NP \), although this is considered unlikely.

Of course, \( P \subseteq NP \cap \text{co}NP \). There are problems in \( NP \cap \text{co}NP \) not known to be in \( P \).

One of the most famous in the following problem:

**Integer factorization problem:**

Given an integer \( N \geq 3 \), and another integer \( M \) (a budget) such that \( 1 < M < N \), does \( N \) have a factor \( d \) with \( 1 < d \leq M \)?

That **Integer factorization** is in \( NP \) is clear. To show that **Integer factorization** is in \( \text{co}NP \), we can guess a factorization of \( N \) into distinct factors all greater than \( M \), check that they are prime using the results of Chapter 11 showing that testing primality is in \( NP \) (even in \( P \), but that’s much harder to prove), and then check that the product of these factors is \( N \).

It is widely believed that **Integer factorization** does not belong to \( P \), which is the technical justification for saying that this problem is hard. Most cryptographic algorithms rely on this unproven fact. If **Integer factorization** was either \( NP \)-complete or \( \text{co}NP \)-complete, then we would have \( NP = \text{co}NP \), which is considered very unlikely.

**Remark:** If \( \sqrt{N} \leq M < N \), the above problem is equivalent to asking whether \( N \) is prime.

A natural instance of a problem in \( \text{co}NP \) is the **unsatisfiability problem** for propositions \( \text{UNSAT} = \neg \text{SAT} \), namely deciding that a proposition \( P \) has no satisfying assignment.

A proposition \( P \) (in CNF) is **falsifiable** if there is some truth assignment \( v \) such that \( \hat{v}(P) = \mathbf{F} \). It is obvious that the set of falsifiable propositions is in \( NP \). Since a proposition \( P \) is valid iff \( P \) is not falsifiable, the **validity (or tautology) problem** TAUT for propositions is in \( \text{co}NP \). In fact, TAUT is \( \text{co}NP \)-complete; see Papadimitriou [19].

This is easy to prove. Since SAT is \( NP \)-complete, for every language \( L \in NP \), there is a polynomial-time computable function \( f : \Sigma^* \rightarrow \Sigma^* \) such that \( x \in L \) iff \( f(x) \in \text{SAT} \). Then \( x \notin L \) iff \( f(x) \notin \text{SAT} \), that is, \( x \notin L \) iff \( f(x) \notin \neg \text{SAT} \), which means that every language \( L \in \text{co}NP \) is polynomial-time reducible to \( \neg \text{SAT} = \text{UNSAT} \). But \( \text{TAUT} = \{ \neg P \mid P \in \text{UNSAT} \} \), so we have the polynomial-time computable function \( g \) given by \( g(x) = \neg f(x) \) which gives us the reduction \( x \in L \) iff \( g(x) \in \text{TAUT} \), which shows that \( \text{TAUT} \) is \( \text{co}NP \)-complete.

Despite the fact that this problem has been extensively studied, not much is known about its exact complexity.

The reasoning used to show that \( \text{TAUT} \) is \( \text{co}NP \)-complete can also be used to show the following interesting result.
10.3. SUCCINCT CERTIFICATES, coNP, AND EXP

**Proposition 10.2.** If a language \( L \) is \( \mathcal{NP} \)-complete, then its complement \( \overline{L} \) is \( \text{coNP} \)-complete.

**Proof.** By definition, since \( L \in \mathcal{NP} \), we have \( \overline{L} \in \text{coNP} \). Since \( L \) is \( \mathcal{NP} \)-complete, for every language \( L_2 \in \mathcal{NP} \), there is a polynomial-time computable function \( f: \Sigma^* \rightarrow \Sigma^* \) such that \( x \in L_2 \) iff \( f(x) \in L \). Then \( x \notin L_2 \) iff \( f(x) \notin L \), that is, \( x \in \overline{L_2} \) iff \( f(x) \in \overline{L} \), which means that \( \overline{L} \) is \( \text{coNP} \)-hard as well, thus \( \text{coNP} \)-complete. \( \square \)

The class \( \mathcal{EXP} \) is defined as follows.

**Definition 10.4.** A deterministic Turing machine \( M \) is said to be exponentially bounded if there is a polynomial \( p(X) \) such that for every input \( x \in \Sigma^* \), there is no ID \( ID_n \) such that

\[
ID_0 \vdash ID_1 \vdash \ldots \vdash ID_{n-1} \vdash ID_n, \quad \text{with} \quad n > 2^{p(|x|)}.
\]

The class \( \mathcal{EXP} \) is the class of all languages that are accepted by some exponentially bounded deterministic Turing machine.

**Remark:** We can also define the class \( \mathcal{NEXP} \) as in Definition 10.4, except that we allow nondeterministic Turing machines.

One of the interesting features of \( \mathcal{EXP} \) is that it contains \( \mathcal{NP} \).

**Theorem 10.3.** We have the inclusion \( \mathcal{NP} \subseteq \mathcal{EXP} \).

**Sketch of proof.** Let \( M \) be some nondeterministic Turing machine accepting \( L \) in polynomial time bounded by \( p(X) \). We can construct a deterministic Turing machine \( M' \) that operates as follows: for every input \( x \), \( M' \) simulates \( M \) on all computations of length 1, then on all possible computations of length 2, and so on, up to all possible computations of length \( p(|x|) + 1 \). At this point, either an accepting computation has been discovered or all computations have halted rejecting. We claim that \( M' \) operates in time bounded by \( 2^{q(|x|)} \) for some polynomial \( q(X) \). First, let \( r \) be the degree of nondeterminism of \( M \), that is, the maximum number of triples \((b,m,q)\) such that a quintuple \((p,q,b,m,q)\) is an instructions of \( M \). Then to simulate a computation of \( M \) of length \( \ell \), \( M' \) needs \( O(\ell) \) steps—to copy the input, to produce a string \( c \in \{1,\ldots,r\}^\ell \), and so simulate \( M \) according to the choices specified by \( c \). It follows that \( M' \) can carry out the simulation of \( M \) on an input \( x \) in

\[
\sum_{\ell=1}^{p(|x|)+1} r^\ell \leq (r + 1)^{p(|x|)+1}
\]

steps. Including the \( O(\ell) \) extra steps for each \( \ell \), we obtain the bound \( (r + 2)^{p(|x|)+1} \). Then, we can pick a constant \( k \) such that \( 2^k > r + 2 \), and with \( q(X) = k(p(X) + 1) \), we see that \( M' \) operates in time bounded by \( 2^{q(|x|)} \). \( \square \)
It is also immediate to see that $\mathcal{E}\times\mathcal{P}$ is closed under complementation. Furthermore the strict inclusion $\mathcal{P} \subset \mathcal{E}\times\mathcal{P}$ holds.

**Theorem 10.4.** We have the strict inclusion $\mathcal{P} \subset \mathcal{E}\times\mathcal{P}$.

*Sketch of proof.* We use a diagonalization argument to produce a language $E$ such that $E \notin \mathcal{P}$, yet $E \in \mathcal{E}\times\mathcal{P}$. We need to code a Turing machine as a string, but this can certainly be done using the techniques of Chapter 4. Let $\#(M)$ be the code of Turing machine $M$. Define $E$ as

$$E = \{\#(M)x \mid M \text{ accepts input } x \text{ after at most } 2^{|x|} \text{ steps}\}.$$ 

We claim that $E \notin \mathcal{P}$. We proceed by contradiction. If $E \in \mathcal{P}$, then so is the language $E_1$ given by

$$E_1 = \{\#(M) \mid M \text{ accepts } \#(M) \text{ after at most } 2^{|\#(M)|} \text{ steps}\}.$$ 

Since $\mathcal{P}$ is closed under complementation, we also have $\overline{E_1} \in \mathcal{P}$. Let $M^*$ be a deterministic Turing machine accepting $\overline{E_1}$ in time $p(X)$, for some polynomial $p(X)$. Since $p(X)$ is a polynomial, there is some $n_0$ such that $p(n) \leq 2^n$ for all $n \geq n_0$. We may also assume that $|\#(M^*)| \geq n_0$, since if not we can add $n_0$ “dead states” to $M^*$.

Now, what happens if we run $M^*$ on its own code $\#(M^*)$? It is easy to see that we get a contradiction, namely $M^*$ accepts $\#(M^*)$ iff $M^*$ rejects $\#(M^*)$. We leave this verification as an exercise.

In conclusion, $\overline{E_1} \notin \mathcal{P}$, which in turn implies that $E \notin \mathcal{P}$.

It remains to prove that $E \in \mathcal{E}\times\mathcal{P}$. This is because we can construct a Turing machine that can in exponential time simulate any Turing machine $M$ on input $x$ for $2^{|x|}$ steps. \qed

In summary, we have the chain of inclusions

$$\mathcal{P} \subseteq \mathcal{NP} \subseteq \mathcal{E}\times\mathcal{P},$$ 

where the left inclusion and the right inclusion are both open problems, but we know that at least one of these two inclusions is strict.

We also have the inclusions

$$\mathcal{P} \subseteq \mathcal{NP} \subseteq \mathcal{E}\times\mathcal{P} \subseteq \mathcal{N}\mathcal{E}\times\mathcal{P}.$$ 

Nobody knows whether $\mathcal{E}\times\mathcal{P} = \mathcal{N}\mathcal{E}\times\mathcal{P}$, but it can be shown that if $\mathcal{E}\times\mathcal{P} \neq \mathcal{N}\mathcal{E}\times\mathcal{P}$, then $\mathcal{P} \neq \mathcal{NP}$; see Papadimitriou [19].
Chapter 11

Primality Testing is in \( \mathcal{NP} \)

11.1 Prime Numbers and Composite Numbers

Prime numbers have fascinated mathematicians and more generally curious minds for thousands of years. What is a prime number? Well, \( 2, 3, 5, 7, 11, 13, \ldots, 9973 \) are prime numbers.

**Definition 11.1.** A positive integer \( p \) is prime if \( p \geq 2 \) and if \( p \) is only divisible by 1 and \( p \). Equivalently, \( p \) is prime if and only if \( p \) is a positive integer \( p \geq 2 \) that is not divisible by any integer \( m \) such that \( 2 \leq m < p \). A positive integer \( n \geq 2 \) which is not prime is called composite.

Observe that the number 1 is considered neither a prime nor a composite. For example, \( 6 = 2 \cdot 3 \) is composite. Is \( 3 215 031 751 \) composite? Yes, because

\[
3 215 031 751 = 151 \cdot 751 \cdot 28351.
\]

Even though the definition of primality is very simple, the structure of the set of prime numbers is highly nontrivial. The prime numbers are the basic building blocks of the natural numbers because of the following theorem bearing the impressive name of fundamental theorem of arithmetic.

**Theorem 11.1.** Every natural number \( n \geq 2 \) has a unique factorization

\[
 n = p_1^{i_1} p_2^{i_2} \cdots p_k^{i_k},
\]

where the exponents \( i_1, \ldots, i_k \) are positive integers and \( p_1 < p_2 < \cdots < p_k \) are primes.

Every book on number theory has a proof of Theorem 11.1. The proof is not difficult and uses induction. It has two parts. The first part shows the existence of a factorization. The second part shows its uniqueness. For example, see Apostol [1] (Chapter 1, Theorem 1.10).

How many prime numbers are there? Many! In fact, infinitely many.
Theorem 11.2. The set of prime numbers is infinite.

Proof. The following proof attributed to Hermite only use the fact that every integer greater than 1 has some prime divisor. We prove that for every natural number \( n \geq 2 \), there is some prime \( p > n \). Consider \( N = n! + 1 \). The number \( N \) must be divisible by some prime \( p \) (\( p = N \) is possible). Any prime \( p \) dividing \( N \) is distinct from \( 2, 3, \ldots, n \), since otherwise \( p \) would divide \( N - n! = 1 \), a contradiction. \( \square \)

The problem of determining whether a given integer is prime is one of the better known and most easily understood problems of pure mathematics. This problem has caught the interest of mathematicians again and again for centuries. However, it was not until the 20th century that questions about primality testing and factoring were recognized as problems of practical importance, and a central part of applied mathematics. The advent of cryptographic systems that use large primes, such as RSA, was the main driving force for the development of fast and reliable methods for primality testing. Indeed, in order to create RSA keys, one needs to produce large prime numbers.

### 11.2 Methods for Primality Testing

The general strategy to test whether an integer \( n > 2 \) is prime or composite is to choose some property, say \( A \), implied by primality, and to search for a counterexample \( a \) to this property for the number \( n \), namely some \( a \) for which property \( A \) fails. We look for properties for which checking that a candidate \( a \) is indeed a counterexample can be done quickly.

Is simple property that is the basis of several primality testing algorithms is the Fermat test, namely

\[
a^{n-1} \equiv 1 \pmod{n},
\]

which means that \( a^{n-1} - 1 \) is divisible by \( n \) (see Definition 11.2 for the meaning of the notation \( a \equiv b \pmod{n} \)). If \( n \) is prime, and if gcd\((a, n)=1\), then the above test is indeed satisfied; this is Fermat’s little theorem, Theorem 11.7.

Typically, together with the number \( n \) being tested for primality, some candidate counterexample \( a \) is supplied to an algorithm which runs a test to determine whether \( a \) is really a counterexample to property \( A \) for \( n \). If the test says that \( a \) is a counterexample, also called a witness, then we know for sure that \( n \) is composite.

For example, using the Fermat test, if \( n = 10 \) and \( a = 3 \), we check that

\[
3^9 = 19683 = 10 \cdot 1968 + 3,
\]

so \( 3^9 - 1 \) is not divisible by 10, which means that

\[
a^{n-1} = 3^9 \not\equiv 1 \pmod{10},
\]
and the Fermat test fails. This shows that 10 is not prime and that \( a = 3 \) is a witness of this fact.

If the algorithm reports that \( a \) is not a witness to the fact that \( n \) is composite, does this imply that \( n \) is prime? Unfortunately, no. This is because, there may be some composite number \( n \) and some candidate counterexample \( a \) for which the test says that \( a \) is not a counterexample. Such a number \( a \) is called a liar.

For example, using the Fermat test for \( n = 91 = 7 \cdot 13 \) and \( a = 3 \), we can check that

\[
3^{90} \equiv 1 \pmod{91},
\]

so the Fermat test succeeds even though 91 is not prime. The number \( a = 3 \) is a liar.

The other reason is that we haven’t tested all the candidate counterexamples \( a \) for \( n \). In the case where \( n = 91 \), it can be shown that \( 2^{90} - 64 \) is divisible by 91, so the Fermat test fails for \( a = 2 \), which confirms that 91 is not prime, and \( a = 2 \) is a witness of this fact.

Unfortunately, the Fermat test has the property that it may succeed for all candidate counterexamples, even though \( n \) is composite. The number \( n = 561 = 3 \cdot 11 \cdot 17 \) is such a devious number. It can be shown that for all \( a \in \{2, \ldots, 560\} \) such that \( \gcd(a, 561) = 1 \), we have

\[
a^{560} \equiv 1 \pmod{561},
\]

so all these \( a \) are liars.

Such composite numbers for which the Fermat test succeeds for all candidate counterexamples are called Carmichael numbers, and unfortunately there are infinitely many of them. Thus the Fermat test is doomed. There are various ways of strengthening the Fermat test, but we will not discuss this here. We refer the interested reader to Crandall and Pomerance [5] and Gallier and Quaintance [9].

The remedy is to make sure that we pick a property \( A \) such that if \( n \) is composite, then at least some candidate \( a \) is not a liar, and to test all potential counterexamples \( a \). The difficulty is that trying all candidate counterexamples can be too expensive to be practical.

There are two classes of primality testing algorithms:

1. Algorithms that try all possible counterexamples, and for which the test does not lie. These algorithms give a definite answer: \( n \) is prime or \( n \) is composite. Until 2002, no algorithms running in polynomial time, were known. The situation changed in 2002 when a paper with the title “PRIMES is in \( P \),” by Agrawal, Kayal and Saxena, appeared on the website of the Indian Institute of Technology at Kanpur, India. In this paper, it was shown that testing for primality has a deterministic (nonrandomized) algorithm that runs in polynomial time.

We will not discuss algorithms of this type here, and instead refer the reader to Crandall and Pomerance [5] and Ribenboim [22].
Randomized algorithms. To avoid having problems with infinite events, we assume that we are testing numbers in some large finite interval $\mathcal{I}$. Given any positive integer $m \in \mathcal{I}$, some candidate witness $a$ is chosen at random. We have a test which, given $m$ and a potential witness $a$, determines whether or not $a$ is indeed a witness to the fact that $m$ is composite. Such an algorithm is a *Monte Carlo* algorithm, which means the following:

1. If the test is positive, then $m \in \mathcal{I}$ is composite. In terms of probabilities, this is expressed by saying that the conditional probability that $m \in \mathcal{I}$ is composite given that the test is positive is equal to 1. If we denote the event that some positive integer $m \in \mathcal{I}$ is composite by $C$, then we can express the above as

$$\Pr(C \mid \text{test is positive}) = 1.$$  

2. If $m \in \mathcal{I}$ is composite, then the test is positive for at least 50% of the choices for $a$. We can express the above as

$$\Pr(\text{test is positive} \mid C) \geq \frac{1}{2}.$$  

This gives us a degree of confidence in the test.

The contrapositive of (1) says that if $m \in \mathcal{I}$ is prime, then the test is negative. If we denote by $P$ the event that some positive integer $m \in \mathcal{I}$ is prime, then this is expressed as

$$\Pr(\text{test is negative} \mid P) = 1.$$  

If we repeat the test $\ell$ times by picking independent potential witnesses, then the conditional probability that the test is negative $\ell$ times given that $n$ is composite, written $\Pr(\text{test is negative $\ell$ times} \mid C)$, is given by

$$\Pr(\text{test is negative $\ell$ times} \mid C) = \Pr(\text{test is negative} \mid C)^\ell = (1 - \Pr(\text{test is positive} \mid C))^\ell \leq \left(1 - \frac{1}{2}\right)^\ell = \left(\frac{1}{2}\right)^\ell,$$

where we used Property (2) of a Monte Carlo algorithm that

$$\Pr(\text{test is positive} \mid C) \geq \frac{1}{2}$$

and the independence of the trials. *This confirms that if we run the algorithm $\ell$ times, then $\Pr(\text{test is negative $\ell$ times} \mid C)$ is very small.* In other words, it is very unlikely that the test will lie $\ell$ times (is negative) given that the number $m \in \mathcal{I}$ is composite.
11.3 MODULAR ARITHMETIC, THE GROUPS \( \mathbb{Z}/n\mathbb{Z}, (\mathbb{Z}/n\mathbb{Z})^* \)

If the probability \( \Pr(P) \) of the event \( P \) is known, which requires knowledge of the distribution of the primes in the interval \( \mathcal{I} \), then the conditional probability

\[
\Pr(P \mid \text{test is negative } \ell \text{ times})
\]

can be determined using Bayes’s rule.

A Monte Carlo algorithm does not give a definite answer. However, if \( \ell \) is large enough (say \( \ell = 100 \)), then the conditional probability that the number \( n \) being tested is prime given that the test is negative \( \ell \) times, is very close to 1.

Two of the best known randomized algorithms for primality testing are the Miller–Rabin test and the Solovay–Strassen test. We will not discuss these methods here, and we refer the reader to Gallier and Quaintance [9].

However, what we will discuss is a nondeterministic algorithm that checks that a number \( n \) is prime by guessing a certain kind of tree that we call a Lucas tree (because this algorithm is based on a method due to E. Lucas), and then verifies in polynomial time (in the length \( \log_2 n \) of the input given in binary) that this tree constitutes a “proof” that \( n \) is indeed prime. This shows that primality testing is in \( \mathcal{NP} \), a fact that is not obvious at all. Of course, this is a much weaker result than the AKS algorithm, but the proof that the AKS works in polynomial time (in \( \log_2 n \)) is much harder.

The Lucas test, and basically all of the primality-testing algorithms, use modular arithmetic and some elementary facts of number theory such as the Euler-Fermat theorem, so we proceed with a review of these concepts.

11.3 MODULAR ARITHMETIC, THE GROUPS \( \mathbb{Z}/n\mathbb{Z}, (\mathbb{Z}/n\mathbb{Z})^* \)

Recall the fundamental notion of congruence modulo \( n \) and its notation due to Gauss (circa 1802).

**Definition 11.2.** For any \( a, b \in \mathbb{Z} \), we write \( a \equiv b \pmod{m} \) iff \( a - b = km \), for some \( k \in \mathbb{Z} \) (in other words, \( a - b \) is divisible by \( m \)), and we say that \( a \) and \( b \) are congruent modulo \( m \).

For example, \( 37 \equiv 1 \pmod{9} \), since \( 37 - 1 = 36 = 4 \cdot 9 \). It can also be shown that \( 200^{250} \equiv 1 \pmod{251} \), but this is impossible to do by brute force, so we will develop some tools to either avoid such computations, or to make them tractable.

It is easy to check that congruence is an equivalence relation but it also satisfies the following properties.

**Proposition 11.3.** For any positive integer \( m \), for all \( a_1, a_2, b_1, b_2 \in \mathbb{Z} \), the following properties hold. If \( a_1 \equiv b_1 \pmod{m} \) and \( a_2 \equiv b_2 \pmod{m} \), then

1. \( a_1 + a_2 \equiv b_1 + b_2 \pmod{m} \).
(2) \( a_1 - a_2 \equiv b_1 - b_2 \pmod{m} \).

(3) \( a_1a_2 \equiv b_1b_2 \pmod{m} \).

**Proof.** We only check (3), leaving (1) and (2) as easy exercises. Because \( a_1 \equiv b_1 \pmod{m} \) and \( a_2 \equiv b_2 \pmod{m} \), we have \( a_1 = b_1 + k_1m \) and \( a_2 = b_2 + k_2m \), for some \( k_1, k_2 \in \mathbb{Z} \), so we obtain

\[
a_1a_2 - b_1b_2 = a_1(a_2 - b_2) + (a_1 - b_1)b_2 \\
= (a_1k_2 + k_1b_2)m.
\]

Proposition 11.3 allows us to define addition, subtraction, and multiplication on equivalence classes modulo \( m \).

**Definition 11.3.** Given any positive integer \( m \), we denote by \( \mathbb{Z}/m\mathbb{Z} \) the set of equivalence classes modulo \( m \). If we write \( \overline{a} \) for the equivalence class of \( a \in \mathbb{Z} \), then we define addition, subtraction, and multiplication on residue classes as follows:

\[
\begin{align*}
\overline{a} + \overline{b} &= \overline{a + b} \\
\overline{a} - \overline{b} &= \overline{a - b} \\
\overline{a} \cdot \overline{b} &= \overline{ab}.
\end{align*}
\]

The above operations make sense because \( \overline{a + b} \) does not depend on the representatives chosen in the equivalence classes \( \overline{a} \) and \( \overline{b} \), and similarly for \( \overline{a - b} \) and \( \overline{ab} \). Each equivalence class \( \overline{a} \) contains a unique representative from the set of remainders \( \{0, 1, \ldots, m-1\} \), modulo \( m \), so the above operations are completely determined by \( m \times m \) tables. Using the arithmetic operations of \( \mathbb{Z}/m\mathbb{Z} \) is called **modular arithmetic**.

The additions tables of \( \mathbb{Z}/n\mathbb{Z} \) for \( n = 2, 3, 4, 5, 6, 7 \) are shown below.

\[
\begin{array}{c|cc}
\hline
n = 2 & + & \overline{0} & \overline{1} \\
\hline
\overline{0} & \overline{0} & \overline{1} \\
\overline{1} & \overline{1} & \overline{0} \\
\hline
\end{array}
\quad
\begin{array}{c|cccc}
\hline
n = 3 & + & \overline{0} & \overline{1} & \overline{2} \\
\hline
\overline{0} & \overline{0} & \overline{1} & \overline{2} \\
\overline{1} & \overline{1} & \overline{2} & \overline{0} \\
\overline{2} & \overline{2} & \overline{3} & \overline{0} \\
\hline
\end{array}
\quad
\begin{array}{c|cccc}
\hline
n = 4 & + & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\hline
\overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{0} \\
\overline{2} & \overline{2} & \overline{3} & \overline{0} & \overline{1} \\
\overline{3} & \overline{3} & \overline{0} & \overline{1} & \overline{2} \\
\hline
\end{array}
\quad
\begin{array}{c|cccc}
\hline
n = 5 & + & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\
\hline
\overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\
\overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{0} \\
\overline{2} & \overline{2} & \overline{3} & \overline{0} & \overline{1} & \overline{2} \\
\overline{3} & \overline{3} & \overline{4} & \overline{0} & \overline{1} & \overline{2} \\
\overline{4} & \overline{4} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\hline
\end{array}
\quad
\begin{array}{c|cccc}
\hline
n = 6 & + & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\
\hline
\overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\
\overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{0} \\
\overline{2} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{0} & \overline{1} \\
\overline{3} & \overline{3} & \overline{4} & \overline{5} & \overline{0} & \overline{1} & \overline{2} \\
\overline{4} & \overline{4} & \overline{5} & \overline{0} & \overline{1} & \overline{2} & \overline{3} \\
\overline{5} & \overline{5} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\
\hline
\end{array}
\quad
\begin{array}{c|cccc}
\hline
n = 7 & + & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} \\
\hline
\overline{0} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} \\
\overline{1} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} & \overline{0} \\
\overline{2} & \overline{2} & \overline{3} & \overline{4} & \overline{5} & \overline{6} & \overline{0} & \overline{1} \\
\overline{3} & \overline{3} & \overline{4} & \overline{5} & \overline{6} & \overline{0} & \overline{1} & \overline{2} \\
\overline{4} & \overline{4} & \overline{5} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\
\overline{5} & \overline{5} & \overline{6} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} \\
\overline{6} & \overline{6} & \overline{0} & \overline{1} & \overline{2} & \overline{3} & \overline{4} & \overline{5} \\
\hline
\end{array}
\]
It is easy to check that the addition operation \(+\) is commutative (abelian), associative, that 0 is an identity element for \(+\), and that every element \(a\) has \(-a\) as additive inverse, which means that 
\[ a + (-a) = (-a) + a = 0. \]

It is easy to check that the multiplication operation \(\cdot\) is commutative (abelian), associative, that 1 is an identity element for \(\cdot\), and that \(\cdot\) is distributive on the left and on the right with respect to addition. We usually suppress the dot and write \(\overline{\alpha \beta}\) instead of \(\overline{\alpha \cdot \beta}\). The multiplication tables of \(\mathbb{Z}/n\mathbb{Z}\) for \(n = 2, 3, \ldots, 9\) are shown below. Since \(0 \cdot m = m \cdot 0 = 0\) for all \(m\), these tables are only given for nonzero arguments.
Examining the above tables, we observe that for \( n = 2, 3, 5, 7 \), which are primes, every element has an inverse, which means that for every nonzero element \( a \), there is some (actually, unique) element \( b \) such that
\[
a \cdot b = b \cdot a = 1.
\]
For \( n = 2, 3, 5, 7 \), we say that \( \mathbb{Z}/n\mathbb{Z} - \{0\} \) is an abelian group under multiplication. When \( n \) is composite, there exist nonzero elements whose product is zero. For example, when \( n = 6 \), we have \( 3 \cdot 2 = 0 \), when \( n = 8 \), we have \( 4 \cdot 4 = 0 \), when \( n = 9 \), we have \( 6 \cdot 6 = 0 \).

For \( n = 4, 6, 8, 9 \), the elements \( a \) that have an inverse are precisely those that are relatively prime to the modulus \( n \) (that is, \( \gcd(a, n) = 1 \)).

These observations hold in general. Recall the Bezout theorem: two nonzero integers \( m, n \in \mathbb{Z} \) are relatively prime (\( \gcd(m, n) = 1 \)) iff there are integers \( a, b \in \mathbb{Z} \) such that
\[
am + bn = 1.
\]

**Proposition 11.4.** Given any integer \( n \geq 1 \), for any \( a \in \mathbb{Z} \), the residue class \( \bar{a} \in \mathbb{Z}/n\mathbb{Z} \) is invertible with respect to multiplication iff \( \gcd(a, n) = 1 \).

**Proof.** If \( \bar{a} \) has inverse \( \bar{b} \) in \( \mathbb{Z}/n\mathbb{Z} \), then \( \bar{a} \bar{b} = 1 \), which means that
\[
ab \equiv 1 \pmod{n},
\]
that is \( ab = 1 + nk \) for some \( k \in \mathbb{Z} \), which is the Bezout identity
\[
ab - nk = 1
\]
and implies that \( \gcd(a, n) = 1 \). Conversely, if \( \gcd(a, n) = 1 \), then by Bezout’s identity there exist \( u, v \in \mathbb{Z} \) such that
\[
au + nv = 1,
\]
so \( au = 1 - nv \), that is,
\[
au \equiv 1 \pmod{n},
\]
which means that \( \bar{a} \bar{u} = 1 \), so \( \bar{a} \) is invertible in \( \mathbb{Z}/n\mathbb{Z} \). \(\square\)

We have alluded to the notion of a group. Here is the formal definition.

**Definition 11.4.** A group is a set \( G \) equipped with a binary operation \( \cdot : G \times G \to G \) that associates an element \( a \cdot b \in G \) to every pair of elements \( a, b \in G \), and having the following properties: \( \cdot \) is associative, has an identity element \( e \in G \), and every element in \( G \) is invertible (w.r.t. \( \cdot \)). More explicitly, this means that the following equations hold for all \( a, b, c \in G \):

\[
\begin{align*}
(G1) \quad a \cdot (b \cdot c) &= (a \cdot b) \cdot c. \quad \text{(associativity);} \\
(G2) \quad a \cdot e &= e \cdot a = a. \quad \text{(identity);}
\end{align*}
\]
11.3. MODULAR ARITHMETIC, THE GROUPS $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^*$

(G3) For every $a \in G$, there is some $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$. (inverse).

A group $G$ is abelian (or commutative) if

$$a \cdot b = b \cdot a \quad \text{for all } a, b \in G.$$  

It is easy to show that the element $e$ satisfying property (G2) is unique, and for any $a \in G$, the element $a^{-1} \in G$ satisfying $a \cdot a^{-1} = a^{-1} \cdot a = e$ required to exist by (G3) is actually unique. This element is called the inverse of $a$.

The set of integers $\mathbb{Z}$ with the addition operation is an abelian group with identity element 0. The set $\mathbb{Z}/n\mathbb{Z}$ of residues modulo $m$ is an abelian group under addition with identity element 0. In general, $\mathbb{Z}/n\mathbb{Z} - \{0\}$ is not a group under multiplication, because some nonzero elements may not have an inverse.

The subset of elements, shown in boldface in the multiplication tables, forms an abelian group under multiplication.

**Definition 11.5.** The group (under multiplication) of invertible elements of the ring $\mathbb{Z}/n\mathbb{Z}$ is denoted by $(\mathbb{Z}/n\mathbb{Z})^*$. Note that this group is abelian and only defined if $n \geq 2$.

The Euler $\varphi$-function plays an important role in the theory of the groups $(\mathbb{Z}/n\mathbb{Z})^*$.

**Definition 11.6.** Given any positive integer $n \geq 1$, the Euler $\varphi$-function (or Euler totient function) is defined such that $\varphi(n)$ is the number of integers $a$, with $1 \leq a \leq n$, which are relatively prime to $n$; that is, with $\gcd(a, n) = 1$.

If $p$ is prime, then by definition

$$\varphi(p) = p - 1.$$  

We leave it as an exercise to show that if $p$ is prime and if $k \geq 1$, then

$$\varphi(p^k) = p^{k-1}(p - 1).$$  

It can also be shown that if $\gcd(m, n) = 1$, then

$$\varphi(mn) = \varphi(m)\varphi(n).$$  

The above properties yield a method for computing $\varphi(n)$, based on its prime factorization. If $n = p_1^{i_1} \cdots p_k^{i_k}$, then

$$\varphi(n) = p_1^{i_1-1} \cdots p_k^{i_k-1}(p_1 - 1) \cdots (p_k - 1).$$  

For example, $\varphi(17) = 16$, $\varphi(49) = 7 \cdot 6 = 42$,

$$\varphi(900) = \varphi(2^2 \cdot 3^2 \cdot 5^2) = 2 \cdot 3 \cdot 5 \cdot 1 \cdot 2 \cdot 4 = 240.$$  

Proposition 11.4 shows that $(\mathbb{Z}/n\mathbb{Z})^*$ has $\varphi(n)$ elements. It also shows that $\mathbb{Z}/n\mathbb{Z} - \{0\}$ is a group (under multiplication) iff $n$ is prime.

---

1We allow $a = n$ to accommodate the special case $n = 1$. 

Definition 11.7. If $G$ is a finite group, the number of elements in $G$ is called the \textit{order} of $G$.

Given a group $G$ with identity element $e$, and any element $g \in G$, we often need to consider the powers of $g$ defined as follows.

Definition 11.8. Given a group $G$ with identity element $e$, for any nonnegative integer $n$, it is natural to define the \textit{power} $g^n$ of $g$ as follows:

$$
g^0 = e
$$
$$
g^{n+1} = g \cdot g^n.
$$

Using induction, it is easy to show that

$$
g^m g^n = g^{n+m}
$$

for all $m, n \in \mathbb{N}$.

Since $g$ has an inverse $g^{-1}$, we can extend the definition of $g^n$ to negative powers. For $n \in \mathbb{Z}$, with $n < 0$, let

$$
g^n = (g^{-1})^{-n}.
$$

Then, it is easy to prove that

$$
g^i \cdot g^j = g^{i+j}
$$
$$
(g^i)^{-1} = g^{-i}
$$
$$
g^i \cdot g^j = g^j \cdot g^i
$$

for all $i, j \in \mathbb{Z}$.

Given a finite group $G$ of order $n$, for any element $a \in G$, it is natural to consider the set of powers $\{e, a^1, a^2, \ldots, a^k, \ldots\}$. A crucial fact is that there is a smallest positive $s \in \mathbb{N}$ such that $a^s = e$, and that $s$ divides $n$.

Proposition 11.5. Let $G$ be a finite group of order $n$. For every element $a \in G$, the following facts hold:

(1) There is a smallest positive integer $s \leq n$ such that $a^s = e$.

(2) The set $\{e, a, \ldots, a^{s-1}\}$ is an abelian group denoted $\langle a \rangle$.

(3) We have $a^n = e$, and the positive integer $s$ divides $n$. More generally, for any positive integer $m$, if $a^m = e$, then $s$ divides $m$. 

11.3. MODULAR ARITHMETIC, THE GROUPS $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^*$

Proof. (1) Consider the sequence of $n + 1$ elements

$$(e, a^1, a^2, \ldots, a^n).$$

Since $G$ only has $n$ distinct elements, by the pigeonhole principle, there exist $i, j$ such that $0 \leq i < j \leq n$ such that

$$a^i = a^j.$$

By multiplying both sides by $(a^i)^{-1} = a^{-i}$, we get

$$e = a^i(a^i)^{-1} = a^j(a^i)^{-1} = a^ia^{-i} = a^{j-i}.$$ 

Since $0 \leq i < j \leq n$, we have $0 \leq j-i \leq n$ with $a^{j-i} = e$. Thus there is some $s$ with $0 < s \leq n$ such that $a^s = e$, and thus a smallest such $s$.

(2) Since $a^s = e$, for any $i, j \in \{0, \ldots, s-1\}$ if we write $i+j = sq+r$ with $0 \leq r \leq s-1$, we have

$$a^i a^j = a^{i+j} = a^{sq+r} = a^{sq}a^r = (a^s)^q a^r = e^q a^r = a^r,$$

so $\langle a \rangle$ is closed under multiplication. We have $e \in \langle a \rangle$ and the inverse of $a^i$ is $a^{s-i}$, so $\langle a \rangle$ is a group. This group is obviously abelian.

(3) For any element $g \in G$, let $g\langle a \rangle = \{ga^k \mid 0 \leq k \leq s-1\}$. Observe that for any $i \in \mathbb{N}$, we have

$$a^1 \langle a \rangle = \langle a \rangle.$$

We claim that for any two elements $g_1, g_2 \in G$, if $g_1\langle a \rangle \cap g_2\langle a \rangle \neq \emptyset$, then $g_1\langle a \rangle = g_2\langle a \rangle$.

Proof of the claim. If $g \in g_1\langle a \rangle \cap g_2\langle a \rangle$, then there exist $i, j \in \{0, \ldots, s-1\}$ such that

$$g_1 a^i = g_2 a^j.$$ 

Without loss of generality, we may assume that $i \geq j$. By multiplying both sides by $(a^j)^{-1}$, we get

$$g_2 = g_1 a^{i-j}.$$ 

Consequently

$$g_2\langle a \rangle = g_1 a^{i-j}\langle a \rangle = g_1\langle a \rangle,$$

as claimed. 

It follows that the pairwise disjoint nonempty subsets of the form $g\langle a \rangle$, for $g \in G$, form a partition of $G$. However, the map $\varphi_g$ from $\langle a \rangle$ to $g\langle a \rangle$ given by $\varphi_g(a^i) = ga^i$ has for inverse the map $\varphi_{g^{-1}}$, so $\varphi_g$ is a bijection, and thus the subsets $g\langle a \rangle$ all have the same number of elements, $s$. Since these subsets form a partition of $G$, we must have $n = sq$ for some $q \in \mathbb{N}$, which implies that $a^n = e$.

If $g^m = 1$, then writing $m = sq + r$, with $0 \leq r < s$, we get

$$1 = g^m = g^{sq+r} = (g^s)^q \cdot g^r = g^r,$$

so $g^r = 1$ with $0 \leq r < s$, contradicting the minimality of $s$, so $r = 0$ and $s$ divides $m$. \qed
Definition 11.9. Given a finite group $G$ of order $n$, for any $a \in G$, the smallest positive integer $s \leq n$ such that $a^s = e$ in (1) of Proposition 11.5 is called the order of $a$.

For any integer $n \geq 2$, let $(\mathbb{Z}/n\mathbb{Z})^*$ be the group of invertible elements of the ring $\mathbb{Z}/n\mathbb{Z}$. This is a group of order $\varphi(n)$. Then Proposition 11.5 yields the following result.

Theorem 11.6. (Euler) For any integer $n \geq 2$ and any $a \in \{1, \ldots, n-1\}$ such that $\gcd(a, n) = 1$, we have

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$  

In particular, if $n$ is a prime, then $\varphi(n) = n-1$, and we get Fermat’s little theorem.

Theorem 11.7. (Fermat’s little theorem) For any prime $p$ and any $a \in \{1, \ldots, p-1\}$, we have

$$a^{p-1} \equiv 1 \pmod{p}.$$  

Since 251 is prime, and since $\gcd(200, 252) = 1$, Fermat’s little theorem implies our earlier claim that $200^{200} \equiv 1 \pmod{251}$, without making any computations.

Proposition 11.5 suggests considering groups of the form $\langle g \rangle$.

Definition 11.10. A finite group $G$ is cyclic iff there is some element $g \in G$ such that $G = \langle g \rangle$. An element $g \in G$ with this property is called a generator of $G$.

Even though, in principle, a finite cyclic group has a very simple structure, finding a generator for a finite cyclic group is generally hard. For example, it turns out that the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^*$ is a cyclic group when $p$ is prime, but no efficient method for finding a generator for $(\mathbb{Z}/p\mathbb{Z})^*$ is known (besides a brute-force search).

Examining the multiplication tables for $(\mathbb{Z}/n\mathbb{Z})^*$ for $n = 3, 4, \ldots, 9$, we can check the following facts:

1. $2$ is a generator for $(\mathbb{Z}/3\mathbb{Z})^*$.
2. $3$ is a generator for $(\mathbb{Z}/4\mathbb{Z})^*$.
3. $2$ is a generator for $(\mathbb{Z}/5\mathbb{Z})^*$.
4. $5$ is a generator for $(\mathbb{Z}/6\mathbb{Z})^*$.
5. $3$ is a generator for $(\mathbb{Z}/7\mathbb{Z})^*$.
6. Every element of $(\mathbb{Z}/8\mathbb{Z})^*$ satisfies the equation $a^2 = 1 \pmod{8}$, thus $(\mathbb{Z}/8\mathbb{Z})^*$ has no generators.
7. $2$ is a generator for $(\mathbb{Z}/9\mathbb{Z})^*$.
More generally, it can be shown that the multiplicative groups \((\mathbb{Z}/p^k\mathbb{Z})^*\) and \((\mathbb{Z}/2p^k\mathbb{Z})^*\) are cyclic groups when \(p\) is an odd prime and \(k \geq 1\).

**Definition 11.11.** A generator of the group \((\mathbb{Z}/n\mathbb{Z})^*\) (when there is one), is called a *primitive root modulo \(n\).*

As an exercise, the reader should check that the next value of \(n\) for which \((\mathbb{Z}/n\mathbb{Z})^*\) has no generator is \(n = 12\).

The following theorem due to Gauss can be shown. For a proof, see Apostol [1] or Gallier and Quaintance [9].

**Theorem 11.8.** (*Gauss*) For every odd prime \(p\), the group \((\mathbb{Z}/p\mathbb{Z})^*\) is cyclic of order \(p - 1\). It has \(\varphi(p - 1)\) generators.

The generators of \((\mathbb{Z}/p\mathbb{Z})^*\) are the *primitive roots modulo \(p\).*

### 11.4 The Lucas Theorem; Lucas Trees

In this section we discuss an application of the existence of primitive roots in \((\mathbb{Z}/p\mathbb{Z})^*\) where \(p\) is an odd prime, known as the \(n - 1\) test. This test due to E. Lucas determines whether a positive odd integer \(n\) is prime or not by examining the prime factors of \(n - 1\) and checking some congruences.

The \(n - 1\) test can be described as the construction of a certain kind of tree rooted with \(n\), and it turns out that the number of nodes in this tree is bounded by \(2\log_2 n\), and that the number of modular multiplications involved in checking the congruences is bounded by \(2\log^2 n\).

When we talk about the complexity of algorithms dealing with numbers, we assume that all inputs (to a Turing machine) are strings representing these numbers, typically in base 2. Since the length of the binary representation of a natural number \(n \geq 1\) is \([\log_2 n] + 1\) (or \([\log_2(n + 1)]\), which allows \(n = 0\)), the complexity of algorithms dealing with (nonzero) numbers \(m, n, \text{ etc.}\) is expressed in terms of \(\log_2 m, \log_2 n, \text{ etc.}\) Recall that for any real number \(x \in \mathbb{R}\), the *floor of \(x\)* is the greatest integer \([x]\) that is less than or equal to \(x\), and the *ceiling of \(x\)* is the least integer \(\lceil x \rceil\) that is greater than or equal to \(x\).

If we choose to represent numbers in base 10, since for any base \(b\) we have \(\log_b x = \ln x / \ln b\), we have

\[
\log_2 x = \frac{\ln 10}{\ln 2} \log_{10} x.
\]

Since \((\ln 10)/(\ln 2) \approx 3.322 \approx 10/3\), we see that the number of decimal digits needed to represent the integer \(n\) in base 10 is approximately 30% of the number of bits needed to represent \(n\) in base 2.
CHAPTER 11. PRIMALITY TESTING IS IN $\mathcal{NP}$

Since the Lucas test yields a tree such that the number of modular multiplications involved in checking the congruences is bounded by $2 \log_2 n$, it is not hard to show that testing whether or not a positive integer $n$ is prime, a problem denoted PRIMES, belongs to the complexity class $\mathcal{NP}$. This result was shown by V. Pratt [21] (1975), but Peter Freyd told me that it was “folklore.” Since 2002, thanks to the AKS algorithm, we know that PRIMES actually belongs to the class $\mathcal{P}$, but this is a much harder result.

Here is Lehmer’s version of the Lucas result, from 1876.

**Theorem 11.9. (Lucas theorem)** Let $n$ be a positive integer with $n \geq 2$. Then $n$ is prime iff there is some integer $a \in \{1, 2, \ldots, n - 1\}$ such that the following two conditions hold:

1. $a^{n-1} \equiv 1 \pmod{n}$.
2. If $n > 2$, then $a^{(n-1)/q} \not\equiv 1 \pmod{n}$ for all prime divisors $q$ of $n - 1$.

**Proof.** First, assume that Conditions (1) and (2) hold. If $n = 2$, since 2 is prime, we are done. Thus assume that $n \geq 3$, and let $r$ be the order of $a$. We claim that $r = n - 1$. The condition $a^{n-1} \equiv 1 \pmod{n}$ implies that $r$ divides $n - 1$. Suppose that $r < n - 1$, and let $q$ be a prime divisor of $(n - 1)/r$ (so $q$ divides $n - 1$). Since $r$ is the order of $a$ we have $a^r \equiv 1 \pmod{n}$, so we get

$$a^{(n-1)/q} \equiv a^{(n-1)/(rq)} \equiv (a^r)^{(n-1)/(rq)} \equiv 1^{(n-1)/(rq)} \equiv 1 \pmod{n},$$

contradicting Condition (2). Therefore, $r = n - 1$, as claimed.

We now show that $n$ must be prime. Now $a^{n-1} \equiv 1 \pmod{n}$ implies that $a$ and $n$ are relatively prime so by Euler’s Theorem (Theorem 11.6),

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$  

Since the order of $a$ is $n - 1$, we have $n - 1 \leq \varphi(n)$. If $n \geq 3$ is not prime, then $n$ has some prime divisor $p$, but $n$ and $p$ are integers in $\{1, 2, \ldots, n\}$ that are not relatively prime to $n$, so by definition of $\varphi(n)$, we have $\varphi(n) \leq n - 2$, contradicting the fact that $n - 1 \leq \varphi(n)$. Therefore, $n$ must be prime.

Conversely, assume that $n$ is prime. If $n = 2$, then we set $a = 1$. Otherwise, pick $a$ to be any primitive root modulo $p$. Clearly, if $n > 2$ then we may assume that $a \geq 2$. The main difficulty with the $n - 1$ test is not so much guessing the primitive root $a$, but finding a complete prime factorization of $n - 1$. However, as a nondeterministic algorithm, the $n - 1$ test yields a “proof” that a number $n$ is indeed prime which can be represented as a tree, and the number of operations needed to check the required conditions (the congruences) is bounded by $c \log_2^2 n$ for some positive constant $c$, and this implies that testing primality is in $\mathcal{NP}$.

Before explaining the details of this method, we sharpen slightly Lucas theorem to deal only with odd prime divisors.
Theorem 11.10. Let \( n \) be a positive odd integer with \( n \geq 3 \). Then \( n \) is prime iff there is some integer \( a \in \{2, \ldots, n-1\} \) (a guess for a primitive root modulo \( n \)) such that the following two conditions hold:

(1b) \( a^{(n-1)/2} \equiv -1 \pmod{n} \).

(2b) If \( n-1 \) is not a power of 2, then \( a^{(n-1)/2q} \not\equiv -1 \pmod{n} \) for all odd prime divisors \( q \) of \( n-1 \).

Proof. Assume that Conditions (1b) and (2b) of Theorem 11.10 hold. Then we claim that Conditions (1) and (2) of Theorem 11.9 hold. By squaring the congruence \( a^{(n-1)/2} \equiv -1 \pmod{n} \), we get

\[
a^{n-1} \equiv 1 \pmod{n},
\]

so

\[
(a^{(n-1)/2} - 1)(a^{(n-1)/2} + 1) \equiv 0 \pmod{n}.
\]

Since \( n \) is prime, either \( a^{(n-1)/2} \equiv 1 \pmod{n} \) or \( a^{(n-1)/2} \equiv -1 \pmod{n} \), but since \( a \) generates \((\mathbb{Z}/n\mathbb{Z})^*\), it has order \( n-1 \), so the congruence \( a^{(n-1)/2} \equiv 1 \pmod{n} \) is impossible, and Condition (1b) must hold. Similarly, if we had \( a^{(n-1)/2q} \equiv -1 \pmod{n} \) for some odd prime divisor \( q \) of \( n-1 \), then by squaring we would have

\[
a^{(n-1)/q} \equiv 1 \pmod{n},
\]

and \( a \) would have order at most \((n-1)/q < n-1\), which is absurd. \( \square \)
If \( n \) is an odd prime, we can use Theorem 11.10 to build recursively a tree which is a proof, or certificate, of the fact that \( n \) is indeed prime. We first illustrate this process with the prime \( n = 1279 \).

**Example 11.1.** If \( n = 1279 \), then we easily check that \( n - 1 = 1278 = 2 \cdot 3^2 \cdot 71 \). We build a tree whose root node contains the triple \((1279, ((2, 1), (3, 2), (71, 1)), 3)\), where \( a = 3 \) is the guess for a primitive root modulo 1279. In this simple example, it is clear that 3 and 71 are prime, but we must supply proofs that these number are prime, so we recursively apply the process to the odd divisors 3 and 71.

Since \( 3 - 1 = 2^1 \) is a power of 2, we create a one-node tree \((3, ((2, 1)), 2)\), where \( a = 2 \) is a guess for a primitive root modulo 3. This is a leaf node.

Since \( 71 - 1 = 70 = 2 \cdot 5 \cdot 7 \), we create a tree whose root node is \((71, ((2, 1), (5, 1), (7, 1)), 7)\), where \( a = 7 \) is the guess for a primitive root modulo 71. Since \( 5 - 1 = 4 = 2^2 \), and \( 7 - 1 = 6 = 2 \cdot 3 \), this node has two successors \((5, ((2, 2)), 2)\) and \((7, ((2, 1), (3, 1)), 3)\), where 2 is the guess for a primitive root modulo 5, and 3 is the guess for a primitive root modulo 7.

Since \( 4 = 2^2 \) is a power of 2, the node \((5, ((2, 2)), 2)\) is a leaf node.

Since \( 3 - 1 = 2^1 \), the node \((7, ((2, 1), (3, 1)), 3)\) has a single successor, \((3, ((2, 1)), 2)\), where \( a = 2 \) is a guess for a primitive root modulo 3. Since \( 2 = 2^1 \) is a power of 2, the node \((3, ((2, 1)), 2)\) is a leaf node.

To recap, we obtain the following tree:

\[
(1279, ((2, 1), (3, 2), (71, 1)), 3)
\]

\[
(3, ((2, 1)), 2) \quad (71, ((2, 1), (5, 1), (7, 1)), 7)
\]

\[
(5, ((2, 2)), 2) \quad (7, ((2, 1), (3, 1)), 3)
\]

\[
(3, ((2, 1)), 2)
\]

We still have to check that the relevant congruences hold at every node. For the root node \((1279, ((2, 1), (3, 2), (71, 1)), 3)\), we check that

\[
3^{1278/2} \equiv 3^{864} \equiv -1 \pmod{1279} \quad (1b)
\]

\[
3^{1278/(2 \cdot 3)} \equiv 3^{213} \equiv 775 \pmod{1279} \quad (2b)
\]

\[
3^{1278/(2 \cdot 71)} \equiv 3^9 \equiv 498 \pmod{1279}. \quad (2b)
\]
Assuming that 3 and 71 are prime, the above congruences check that Conditions (1a) and (2b) are satisfied, and by Theorem 11.10 this proves that 1279 is prime. We still have to certify that 3 and 71 are prime, and we do this recursively.

For the leaf node \((3, ((2, 1)), 2)\), we check that

\[ 2^{2/2} \equiv -1 \pmod{3}. \] (1b)

For the node \((71, ((2, 1), (5, 1), (7, 1)), 7)\), we check that

\[ 7^{70/2} \equiv 7^{35} \equiv -1 \pmod{71} \] (1b)
\[ 7^{70/(2 \cdot 5)} \equiv 7^7 \equiv 14 \pmod{71} \] (2b)
\[ 7^{70/(2 \cdot 7)} \equiv 7^5 \equiv 51 \pmod{71}. \] (2b)

Now, we certified that 3 and 71 are prime, assuming that 5 and 7 are prime, which we now establish.

For the leaf node \((5, ((2, 2)), 2)\), we check that

\[ 2^{4/2} \equiv 2^2 \equiv -1 \pmod{5}. \] (1b)

For the node \((7, ((2, 1), (3, 1)), 3)\), we check that

\[ 3^{6/2} \equiv 3^3 \equiv -1 \pmod{7} \] (1b)
\[ 3^{6/(2 \cdot 3)} \equiv 3^1 \equiv 3 \pmod{7}. \] (2b)

We have certified that 5 and 7 are prime, given that 3 is prime, which we finally verify.

At last, for the leaf node \((3, ((2, 1)), 2)\), we check that

\[ 2^{2/2} \equiv -1 \pmod{3}. \] (1b)

The above example suggests the following definition.

**Definition 11.12.** Given any odd integer \(n \geq 3\), a *pre-Lucas tree for n* is defined inductively as follows:

1. It is a one-node tree labeled with \((n, ((2, i_0)), a)\), such that \(n - 1 = 2^{i_0}\), for some \(i_0 \geq 1\) and some \(a \in \{2, \ldots, n - 1\}\).

2. If \(L_1, \ldots, L_k\) are \(k\) pre-Lucas (with \(k \geq 1\)), where the tree \(L_j\) is a pre-Lucas tree for some odd integer \(q_j \geq 3\), then the tree \(L\) whose root is labeled with \((n, ((2, i_0), (q_1, i_1), \ldots, (q_k, i_k)), a)\) and whose \(j\)th subtree is \(L_j\) is a *pre-Lucas tree for n* if

\[ n - 1 = 2^{i_0} q_1^{i_1} \cdots q_k^{i_k}, \]

for some \(i_0, i_1, \ldots, i_k \geq 1\), and some \(a \in \{2, \ldots, n - 1\}\).
Both in (1) and (2), the number $a$ is a guess for a primitive root modulo $n$.

A pre-Lucas tree for $n$ is a Lucas tree for $n$ if the following conditions are satisfied:

(3) If $L$ is a one-node tree labeled with $(n, ((2, i_0), a)$, then
\[ a^{(n-1)/2} \equiv -1 \pmod{n}. \]

(4) If $L$ is a pre-Lucas tree whose root is labeled with $(n, ((2, i_0), (q_1, i_1), \ldots, (q_k, i_k), a)$, and whose $j$th subtree $L_j$ is a pre-Lucas tree for $q_j$, then $L_j$ is a Lucas tree for $q_j$ for $j = 1, \ldots, k$, and
(a) $a^{(n-1)/2} \equiv -1 \pmod{n}$.
(b) $a^{(n-1)/2q_j} \not\equiv -1 \pmod{n}$ for $j = 1, \ldots, k$.

Since Conditions (3) and (4) of Definition 11.12 are Conditions (1b) and (2b) of Theorem 11.10, we see that Definition 11.12 has been designed in such a way that Theorem 11.10 yields the following result.

**Theorem 11.11.** An odd integer $n \geq 3$ is prime iff it has some Lucas tree.

The issue is now to see how long it takes to check that a pre-Lucas tree is a Lucas tree. For this, we need a method for computing $x^n \pmod{n}$ in polynomial time in $\log_2 n$. This is the object of the next section.

### 11.5 Algorithms for Computing Powers Modulo $m$

Let us first consider computing the $n$th power $x^n$ of some positive integer. The idea is to look at the parity of $n$ and to proceed recursively. If $n$ is even, say $n = 2k$, then
\[ x^n = x^{2k} = (x^k)^2, \]
so, compute $x^k$ recursively and then square the result. If $n$ is odd, say $n = 2k + 1$, then
\[ x^n = x^{2k+1} = (x^k)^2 \cdot x, \]
so, compute $x^k$ recursively, square it, and multiply the result by $x$.

What this suggests is to write $n \geq 1$ in binary, say
\[ n = b_\ell \cdot 2^\ell + b_{\ell-1} \cdot 2^{\ell-1} + \cdots + b_1 \cdot 2^1 + b_0, \]
where $b_i \in \{0, 1\}$ with $b_\ell = 1$ or, if we let $J = \{j \mid b_j = 1\}$, as
\[ n = \sum_{j \in J} 2^j. \]
Then we have
\[ x^n \equiv x^{\sum_{j \in J} 2^j} = \prod_{j \in J} x^{2^j} \mod m. \]

This suggests computing the residues \( r_j \) such that
\[ x^{2^j} \equiv r_j \pmod{m}, \]
because then,
\[ x^n \equiv \prod_{j \in J} r_j \pmod{m}, \]
where we can compute this latter product modulo \( m \) two terms at a time.

For example, say we want to compute \( 999^{179} \pmod{1763} \). First, we observe that
\[ 179 = 2^7 + 2^5 + 2^4 + 2^1 + 1, \]
and we compute the powers modulo 1763:
\[
\begin{align*}
999^{2^1} &\equiv 143 \pmod{1763} \\
999^{2^2} &\equiv 143^2 \equiv 1056 \pmod{1763} \\
999^{2^3} &\equiv 1056^2 \equiv 920 \pmod{1763} \\
999^{2^4} &\equiv 920^2 \equiv 160 \pmod{1763} \\
999^{2^5} &\equiv 160^2 \equiv 918 \pmod{1763} \\
999^{2^6} &\equiv 918^2 \equiv 10 \pmod{1763} \\
999^{2^7} &\equiv 10^2 \equiv 100 \pmod{1763}.
\end{align*}
\]

Consequently,
\[
\begin{align*}
999^{179} &\equiv 999 \cdot 143 \cdot 160 \cdot 918 \cdot 100 \pmod{1763} \\
&\equiv 54 \cdot 160 \cdot 918 \cdot 100 \pmod{1763} \\
&\equiv 1588 \cdot 918 \cdot 100 \pmod{1763} \\
&\equiv 1546 \cdot 100 \pmod{1763} \\
&\equiv 1219 \pmod{1763},
\end{align*}
\]
and we find that
\[ 999^{179} \equiv 1219 \pmod{1763}. \]
Of course, it would be impossible to exponentiate \( 999^{179} \) first and then reduce modulo 1763. As we can see, the number of multiplications needed is bounded by \( 2 \log_2 n \), which is quite good.
The above method can be implemented without actually converting \( n \) to base 2. If \( n \) is even, say \( n = 2k \), then \( n/2 = k \) and if \( n \) is odd, say \( n = 2k + 1 \), then \( (n - 1)/2 = k \), so we have a way of dropping the unit digit in the binary expansion of \( n \) and shifting the remaining digits one place to the right without explicitly computing this binary expansion. Here is an algorithm for computing \( x^n \mod m \), with \( n \geq 1 \), using the \textit{repeated squaring} method.

\textbf{An Algorithm to Compute} \( x^n \mod m \) \textit{Using Repeated Squaring}

\begin{verbatim}
begin
    u := 1; a := x;
    while n > 1 do
        if even(n) then e := 0 else e := 1;
        if e = 1 then u := a \cdot u \mod m;
            a := a^2 \mod m; n := (n - e)/2
    endwhile;
    u := a \cdot u \mod m
end
\end{verbatim}

The final value of \( u \) is the result. The reason why the algorithm is correct is that after \( j \) rounds through the while loop, \( a = x^{2^j} \mod m \) and

\[ u = \prod_{i \in J \mid i < j} x^{2^i} \mod m, \]

with this product interpreted as 1 when \( j = 0 \).

Observe that the while loop is only executed \( n - 1 \) times to avoid squaring once more unnecessarily and the last multiplication \( a \cdot u \) is performed outside of the while loop. Also, if we delete the reductions modulo \( m \), the above algorithm is a fast method for computing the \( n \)th power of an integer \( x \) and the time speed-up of not performing the last squaring step is more significant. We leave the details of the proof that the above algorithm is correct as an exercise.

\section{PRIMES is in \textit{NP}}

Exponentiation modulo \( n \) can performed by repeated squaring, as explained in Section 11.5. In that section, we observed that computing \( x^m \mod n \) requires at most \( 2 \log_2 m \) modular multiplications. Using this fact, we obtain the following result.

\textbf{Proposition 11.12.} If \( p \) is any odd prime, then any pre-Lucas tree \( L \) for \( p \) has at most \( \log_2 p \) nodes, and the number \( M(p) \) of modular multiplications required to check that the pre-Lucas tree \( L \) is a Lucas tree is less than \( 2 \log_2^2 p \).
Proof. Let \( N(p) \) be the number of nodes in a pre-Lucas tree for \( p \). We proceed by complete induction. If \( p = 3 \), then \( p - 1 = 2^1 \), any pre-Lucas tree has a single node, and \( 1 < \log_2 3 \).

Suppose the results holds for any odd prime less than \( p \). If \( p - 1 = 2^i \), then any Lucas tree has a single node, and \( 1 < \log_2 3 < \log_2 p \). If \( p - 1 \) has the prime factorization

\[
p - 1 = 2^i q_1^{i_1} \cdots q_k^{i_k},
\]

then by the induction hypothesis, each pre-Lucas tree \( L_j \) for \( q_j \) has less than \( \log_2 q_j \) nodes, so

\[
N(p) = 1 + \sum_{j=1}^k N(q_j) < 1 + \log_2 q_1 + \cdots + \log_2 q_k 
= 1 + \log_2 (q_1 \cdots q_k) 
< 1 + \log_2 \left( \frac{p - 1}{2} \right) < \log_2 p,
\]

establishing the induction hypothesis.

If \( r \) is one of the odd primes in the pre-Lucas tree for \( p \), and \( r < p \), then there is some other odd prime \( q \) in this pre-Lucas tree such that \( r \) divides \( q - 1 \) and \( q \leq p \). We also have to show that at some point, \( a^{(q-1)/2r} \equiv -1 \pmod q \) for some \( a \), and at another point, that \( b^{(r-1)/2} \equiv -1 \pmod r \) for some \( b \). Using the fact that the number of modular multiplications required to exponentiate to the power \( m \) is at most \( 2 \log_2 m \), we see that the number of multiplications required by the above two exponentiations does not exceed

\[
2 \log_2 \left( \frac{q - 1}{2r} \right) + 2 \log_2 \left( \frac{r - 1}{2} \right) < 2 \log_2 q - 4 < 2 \log_2 p.
\]

As a consequence, we have

\[
M(p) < 2 \log_2 \left( \frac{p - 1}{2} \right) + (N(p) - 1)2 \log_2 p < 2 \log_2 p + (\log_2 p - 1)2 \log_2 p = 2 \log_2^2 p,
\]

as claimed.

The following impressive example is from Pratt [21].

**Example 11.2.** Let \( n = 474\,397\,531 \). It is easy to check that \( n - 1 = 474\,397\,531 - 1 = 474\,397\,530 = 2 \cdot 3 \cdot 5 \cdot 251^3 \). We claim that the following is a Lucas tree for \( n = 474\,397\,531 \):

\[
\begin{align*}
(474\,397\,531, ((2, 1), (3, 1), (5, 1), (251, 3)), 2) \\
(3, ((2, 1)), 2) & \quad (5, ((2, 2)), 2) & \quad (251, ((2, 1), (5, 3)), 6) \\
& \quad (5, ((2, 2)), 2)
\end{align*}
\]
To verify that the above pre-Lucas tree is a Lucas tree, we check that 2 is indeed a primitive root modulo \(474397531\) by computing (using Mathematica) that

\[
\begin{align*}
2^{474397530/2} &\equiv 2^{237198765} \equiv -1 \pmod{474397531} \\
2^{474397530/(2\cdot3)} &\equiv 2^{79066255} \equiv 9583569 \pmod{474397531} \\
2^{474397530/(2\cdot5)} &\equiv 2^{47439753} \equiv 91151207 \pmod{474397531} \\
2^{474397530/(2\cdot251)} &\equiv 2^{945015} \equiv 282211150 \pmod{474397531}.
\end{align*}
\]

(1)

The number of modular multiplications is: 27 in (1), 26 in (2), 25 in (3) and 19 in (4).

We have \(251 - 1 = 250 = 2 \cdot 5^3\), and we verify that 6 is a primitive root modulo 251 by computing:

\[
\begin{align*}
6^{250/2} &\equiv 6^{125} \equiv -1 \pmod{251} \\
6^{250/(2\cdot5)} &\equiv 6^{10} \equiv 175 \pmod{251}.
\end{align*}
\]

(5)

(6)

The number of modular multiplications is: 6 in (5), and 3 in (6).

We have \(5 - 1 = 4 = 2^2\), and 2 is a primitive root modulo 5, since

\[
2^{4/2} \equiv 2^2 \equiv -1 \pmod{5}.
\]

(7)

This takes one multiplication.

We have \(3 - 1 = 2 = 2^1\), and 2 is a primitive root modulo 3, since

\[
2^{2/2} \equiv 2^1 \equiv -1 \pmod{3}.
\]

(8)

This takes 0 multiplications.

Therefore, \(474397531\) is prime.

As nice as it is, Proposition 11.12 is deceiving, because finding a Lucas tree is hard.

Remark: Pratt [21] presents his method for finding a certificate of primality in terms of a proof system. Although quite elegant, we feel that this method is not as transparent as the method using Lucas trees, which we adapted from Crandall and Pomerance [5]. Pratt’s proofs can be represented as trees, as Pratt sketches in Section 3 of his paper. However, Pratt uses the basic version of Lucas’ theorem, Theorem 11.9, instead of the improved version, Theorem 11.10, so his proof trees have at least twice as many nodes as ours.

As nice as it is, Proposition 11.12 is deceiving, because finding a Lucas tree is hard.

The following nice result was first shown by V. Pratt in 1975 [21].

Theorem 11.13. The problem \textsc{PRIMES} (testing whether an integer is prime) is in \(\mathcal{NP}\).
11.6. PRIMES IS IN $\mathcal{NP}$

Proof. Since all even integers besides 2 are composite, we can restrict out attention to odd integers $n \geq 3$. By Theorem 11.11, an odd integer $n \geq 3$ is prime iff it has a Lucas tree. Given any odd integer $n \geq 3$, since all the numbers involved in the definition of a pre-Lucas tree are less than $n$, there is a finite (very large) number of pre-Lucas trees for $n$. Given a guess of a Lucas tree for $n$, checking that this tree is a pre-Lucas tree can be performed in $O(\log_2 n)$, and by Proposition 11.12, checking that it is a Lucas tree can be done in $O(\log^2 n)$. Therefore PRIMES is in $\mathcal{NP}$.  

Of course, checking whether a number $n$ is composite is in $\mathcal{NP}$, since it suffices to guess to factors $n_1, n_2$ and to check that $n = n_1 n_2$, which can be done in polynomial time in $\log_2 n$. Therefore, PRIMES $\in \mathcal{NP} \cap \text{co} \mathcal{NP}$. As we said earlier, this was the situation until the discovery of the AKS algorithm, which places PRIMES in $\mathcal{P}$.

Remark: Altough finding a primitive root modulo $p$ is hard, we know that the number of primitive roots modulo $p$ is $\phi(\phi(p))$. If $p$ is large enough, this number is actually quite large. According to Crandal and Pomerance [5] (Chapter 4, Section 4.1.1), if $p$ is a prime and if $p > 200560490131$, then $p$ has more than $p/(2 \ln \ln p)$ primitive roots.
CHAPTER 11. PRIMALITY TESTING IS IN $\mathbb{NP}$
Bibliography


Symbol Index

(MN), 105, 245
(W, ϕ), 99
0, 115
2^A, 50, 135
=, 115
A − B, 48, 136
A ∩ B, 47
A ∪ B, 47, 135
A ⊆ B, 47, 135
A ⊂ B, 47, 135
A^+, 49, 135, 140
M[φ], 109, 249
M[x := N], 109
P(τ_1, ..., τ_n), 115, 116
P[τ/t], 117
P[τ_1/t_1, ..., τ_n/t_n], 41, 116
P[u/t], 117, 118
P ≡ Q, 116
P ⇒ Q, 9, 63, 116
P ∧ Q, 9, 63, 116
S, 115
S^n(0), 128
[x_1 := N_1, ..., x_n := N_n], 108, 248
Δ, 68
Γ ⊨ P, 83
Γ, 67, 68
Γ, P, 66, 67
Γ, P^x, 68
Π, 68
∩, 51, 138
∩ X, 51, 138
∪ X, 50, 137
∪, 50, 137
∩, 47, 136
→ β, 110, 250
∪, 47, 135
∅, 47, 134
≡, 10, 29, 64, 83
≡_α, 109
∀tP, 116
∃, 9, 39, 63, 114, 117, 118
∀tP, 116
∀, 9, 39, 63, 117
⇒, 9, 36, 62, 63, 68, 79, 96
→ β, 109, 250
∈, 46, 133, 134, 142
Z, 32
Γ ⊨ M: σ, 106
λx: σ. M, 105
λx. M, 245
∧, 9, 36, 63, 80, 96
∨, 9, 36, 63, 80, 96
φ(u): PS → BOOL, 99
BOOL, 36, 95
CS, 115
FS, 115
L, 115
PS, 12, 67, 115
false, 9, 36, 63, 95
ture, 9, 36, 63, 95
pred, 131
N, 32
¬P, 9, 63, 116
→, 9, 36, 63, 81, 82, 96
⊕, 152
\(\overline{A}\), 136
\(\bot\), 9, 63, 81, 116
\(\mathbb{Q}\), 33
\(\mathbb{R}\), 33
\(\ast\rightarrow_{\beta}\), 110, 250
\(\ast\rightarrow_{\beta}\), 110, 250
\(P_1, \ldots, P_m \rightarrow Q_1, \ldots, Q_n\), 155
\(\Gamma \rightarrow P\), 77, 82
\(\Gamma \rightarrow \Delta\), 155
\(\sqrt{2}\), 34
\(\subseteq\), 47, 135
\(\subseteq\), 47, 135
\(\mathcal{D}\), 66, 68
\(\mathcal{D}_1[\mathcal{D}_2/x]\), 103
\(\mathcal{N}g^\Rightarrow_{\mathcal{E}}\cong, \land, \lor, \bot\), 82
\(\mathcal{N}g^\Rightarrow_{\mathcal{I}}\cong, \land, \lor, \bot\), 83, 100
\(\mathcal{N}g^\Rightarrow_{\mathcal{M}}\cong, \land, \lor, \bot\), 83
\(\mathcal{N}g^\Rightarrow_{\mathcal{E}}\cong, \lor, \land, \bot, \exists\), 119
\(\mathcal{N}g^\Rightarrow_{\mathcal{I}}\cong, \lor, \land, \bot, \exists\), 119
\(\mathcal{N}g^\Rightarrow_{\mathcal{M}}\cong, 77\)
\(\mathcal{N}g^\Rightarrow_{\mathcal{E}}\cong, \land, \lor, \bot\), 82
\(\mathcal{N}g^\Rightarrow_{\mathcal{I}}\cong, \land, \lor, \bot\), 82, 100
\(\mathcal{N}g^\Rightarrow_{\mathcal{M}}\cong, \land, \lor, \bot\), 82
\(\mathcal{N}g^\Rightarrow_{\mathcal{E}}\cong, \lor, \land, \bot, \exists\), 118
\(\mathcal{N}g^\Rightarrow_{\mathcal{I}}\cong, \lor, \land, \bot, \exists\), 118
\(\mathcal{N}g^\Rightarrow_{\mathcal{M}}\cong, 68\)
\(\mathcal{P}(A)\), 50, 135
\(\tau_1 = \tau_2\), 115, 116
\(\top\), 9, 63, 116, 151
\(\vdash P\), 83
\(\vdash \Gamma \triangleright M: \sigma\), 107
\(\vdash \Gamma \rightarrow P\), 83
\(\{a, b\}\), 134
\(\{a\}\), 134
\(\{x \mid x \notin x\}\), 133
\(\{x \in A \mid P\}\), 136
\(a \in A\), 46, 134
\(a \notin A\), 46, 134
\(a^b\), 35
\(f(\tau_1, \ldots, \tau_n)\), 115
\(n^+\), 140
Index

α-conversion, 109, 249
   immediate, 249
α-reduction, 249
   immediate, 249
β-conversion, 110, 250
β-normal form, 110
β-redex, 250
β-reduction, 109, 250
   immediate, 109, 250
∃-elimination, 118
∃-introduction, 117
∀-elimination, 117
∀-introduction, 117
⇒-elimination rule, 66, 68, 79
⇒-introduction rule, 66, 68, 79
λ-abstraction, 105, 245
λ-calculus, 104, 245
   pure, 245
   simply-typed, 104, 106
   untyped, 245
λ-term, 105
   β-irreducible, 110
   closed, 105, 247
   raw, 105
   raw simply-typed, 105, 245
   simply-typed, 105
∧-elimination rule, 80
∧-introduction rule, 80
∨-elimination rule, 80
∨-introduction rule, 80
¬-elimination rule, 82
¬-introduction rule, 81, 88
¬¬-elimination rule, 89
⊥-elimination rule, 81, 89
absurdity, 9, 63
absurdum, 9, 63
alphabet, 40, 114
And–Elim, 22
And–Intro, 22
Andrews, P., 61, 111
application, 105, 245
associativity, 31, 49, 56, 94, 137, 148
assumption, 14, 64
atomic propositions, 12, 67
auxiliary lemmas, 15, 32, 69, 94, 103
axiom of choice, 141
axiom of infinity, 139, 140, 145
axioms, 7, 14, 65, 67, 79, 156
   of separation, 136
   of set theory, 134
Bernays, P., 132
bound variable, 39, 114
Brouwer, L., 85
Cantor, G., 132
capture of variables, 41, 117
cardinal
   number, 139
Church’s theorem, 101, 145
Church, A., 101, 104
classical logic, 83
classical propositional logic, 30
closed, 66
combinator, 247
complement, 136
INDEX

of a set, 48
completeness, 37, 38, 54, 97, 98, 100, 112, 144
complexity, 7
theory, 111
composite, 12
compound statement, 9, 63
comprehension axioms, 136
computation, 61, 104
conclusion, 14
confluence, 110
congruent, 365
conjunction, 8, 9, 62, 63
consistency, 37, 54, 97, 112, 132, 144
consistent contexts, 77
constant symbols, 40, 114
constructivists, 86
constructivity, 85
context, 77, 106
counterexample, 38, 54, 98, 112, 144
Curry, H., 104
Curry–Howard isomorphism, 104, 145
cut-elimination theorem, 103
de Morgan laws, 26, 30, 54, 55, 91, 137, 144, 146
for quantifiers, 45, 121
deduction, 7, 14, 53, 64, 143, 156
tree, 68, 77, 82, 83, 119
definition, 11
derivation, 7
discharged, 66, 69, 77, 82, 143
disjoint sets, 48
disjunction, 8, 9, 62, 63
distributivity, 31, 49, 56, 94, 137, 148
divisor, 11
double-negation
elimination, 89, 143
rule, 86, 143
translation, 125
dynamic logic, 113
eigenvariable, 118, 119

restriction, 144
empty, 47, 134
set, 47, 134, 145
set axiom, 134
Enderton, H., 132, 141
equality predicate, 115
equation, 115
equivalence
logical, 10, 29, 64, 83
Equivalence–Intro, 29
even, 11, 128, 146
exclusive or, 152
Exist–Elim, 42
Exist–Intro, 42
extensionality, 46
extensionality axiom, 46, 134
falsity, 9, 63
falsum, 9, 63
finite
tree, 101
first-order, 115
classical logic, 118
formulae, 116
intuitionistic logic, 118
language, 115
logic, 54, 144
structures, 112
theories, 145
theory, 126
variables, 115
Forall–Elim, 41
Forall–Intro, 41
formulae, 40
formulae-as-types principle, 104
Fraenkel, A., 132
free variable, 39, 114
function
operator, 40, 114
symbols, 40, 114
Gödel’s completeness theorem, 112, 145
Gödel’s incompleteness theorem, 127, 145
<table>
<thead>
<tr>
<th>Term</th>
<th>Page Numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gödel, K.</td>
<td>125</td>
</tr>
<tr>
<td>Gallier, J.</td>
<td>38, 62, 98, 111, 112, 116, 126</td>
</tr>
<tr>
<td>GB</td>
<td>132</td>
</tr>
<tr>
<td>gcd</td>
<td>35</td>
</tr>
<tr>
<td>Gentzen</td>
<td></td>
</tr>
<tr>
<td>sequent</td>
<td>76, 82, 155</td>
</tr>
<tr>
<td>sequent-calculus</td>
<td>155</td>
</tr>
<tr>
<td>system</td>
<td>143</td>
</tr>
<tr>
<td>Gentzen, G.</td>
<td>65, 76, 103, 125, 155</td>
</tr>
<tr>
<td>Girard, J.Y.</td>
<td>113, 126</td>
</tr>
<tr>
<td>Glivenko, V.</td>
<td>125</td>
</tr>
<tr>
<td>Gowers, T.</td>
<td>31, 62, 94</td>
</tr>
<tr>
<td>Halmos, P.</td>
<td>132</td>
</tr>
<tr>
<td>Hilbert, D.</td>
<td>65, 134</td>
</tr>
<tr>
<td>Howard, W.</td>
<td>104</td>
</tr>
<tr>
<td>hypotheses</td>
<td>7, 14, 64</td>
</tr>
<tr>
<td>if and only if</td>
<td>10, 64</td>
</tr>
<tr>
<td>iff</td>
<td>10, 64</td>
</tr>
<tr>
<td>implication</td>
<td>8, 9, 53, 62, 63, 143</td>
</tr>
<tr>
<td>Implication–Elim</td>
<td>14</td>
</tr>
<tr>
<td>Implication–Intro</td>
<td>14</td>
</tr>
<tr>
<td>implicational logic</td>
<td>67</td>
</tr>
<tr>
<td>inconsistent</td>
<td>88</td>
</tr>
<tr>
<td>induction</td>
<td>33, 93</td>
</tr>
<tr>
<td>induction principle</td>
<td>52, 141</td>
</tr>
<tr>
<td>for (\mathbb{N})</td>
<td>52, 55, 141, 146</td>
</tr>
<tr>
<td>inductive</td>
<td>51, 140</td>
</tr>
<tr>
<td>set</td>
<td>51, 140, 145</td>
</tr>
<tr>
<td>inference rules</td>
<td>8, 53, 62, 65, 143, 156</td>
</tr>
<tr>
<td>for the quantifiers</td>
<td>117</td>
</tr>
<tr>
<td>for the quantifiers in Gentzen-sequent style</td>
<td>118</td>
</tr>
<tr>
<td>infinite</td>
<td></td>
</tr>
<tr>
<td>intersections</td>
<td>51, 138</td>
</tr>
<tr>
<td>integer</td>
<td>32</td>
</tr>
<tr>
<td>intersection</td>
<td>47, 136, 145</td>
</tr>
<tr>
<td>of sets</td>
<td>47, 136</td>
</tr>
<tr>
<td>intuitionistic logic</td>
<td>82, 90</td>
</tr>
<tr>
<td>intuitionistically</td>
<td></td>
</tr>
<tr>
<td>provable</td>
<td>83, 119</td>
</tr>
<tr>
<td>valid</td>
<td>100</td>
</tr>
<tr>
<td>intuitionists</td>
<td>86</td>
</tr>
<tr>
<td>irrational</td>
<td>33, 34</td>
</tr>
<tr>
<td>number</td>
<td>33</td>
</tr>
<tr>
<td>judgement</td>
<td>106</td>
</tr>
<tr>
<td>Kleene, S.</td>
<td>111</td>
</tr>
<tr>
<td>Kolmogorov, A.</td>
<td>125</td>
</tr>
<tr>
<td>Kripke</td>
<td>90</td>
</tr>
<tr>
<td>models</td>
<td>90, 98, 99, 112, 144</td>
</tr>
<tr>
<td>semantics</td>
<td>90, 98</td>
</tr>
<tr>
<td>Kripke, S.</td>
<td>98</td>
</tr>
<tr>
<td>law of the excluded middle</td>
<td>86, 143</td>
</tr>
<tr>
<td>linear</td>
<td></td>
</tr>
<tr>
<td>logic</td>
<td>113</td>
</tr>
<tr>
<td>classical</td>
<td>82, 90, 118, 119</td>
</tr>
<tr>
<td>intuitionistic</td>
<td>82, 83, 118, 119</td>
</tr>
<tr>
<td>mathematical</td>
<td>61</td>
</tr>
<tr>
<td>logical</td>
<td></td>
</tr>
<tr>
<td>connectives</td>
<td>8, 62</td>
</tr>
<tr>
<td>equivalence</td>
<td>29, 83</td>
</tr>
<tr>
<td>formula</td>
<td>9, 63</td>
</tr>
<tr>
<td>language</td>
<td>40, 115</td>
</tr>
<tr>
<td>mathematical</td>
<td>7</td>
</tr>
<tr>
<td>minimal</td>
<td></td>
</tr>
<tr>
<td>logic</td>
<td>68, 82</td>
</tr>
<tr>
<td>modular arithmetic</td>
<td>365, 366</td>
</tr>
<tr>
<td>modus ponens</td>
<td>14, 32, 66, 68, 79</td>
</tr>
<tr>
<td>multiple</td>
<td>11</td>
</tr>
<tr>
<td>multiset</td>
<td>66, 77</td>
</tr>
<tr>
<td>natural</td>
<td></td>
</tr>
<tr>
<td>deduction</td>
<td>30, 142</td>
</tr>
<tr>
<td>deduction system</td>
<td>61, 65, 143</td>
</tr>
<tr>
<td>numbers</td>
<td>32, 140, 145, 161</td>
</tr>
<tr>
<td>negation</td>
<td>8, 9, 62, 63</td>
</tr>
<tr>
<td>Negation–Elim</td>
<td>19</td>
</tr>
<tr>
<td>Negation–Intro</td>
<td>18</td>
</tr>
<tr>
<td>nonconstructive proofs</td>
<td>35, 45, 90, 120</td>
</tr>
<tr>
<td>nonlogical symbols</td>
<td>115</td>
</tr>
</tbody>
</table>
normal form, 90, 103, 104
normalization step, 103
NP-complete, 97
NP-completeness, 144
number
  even, 11, 13
  odd, 11, 13
odd, 11, 128, 146
Or–Elim, 24
Or–Intro, 24
PA, 126
pairing axiom, 134
Peano arithmetic, 115, 126, 145, 154
Peano, G., 126
Peirce’s law, 93, 97, 151
Perp–Elim, 19
power set, 50, 135, 145
power set axiom, 135
Prawitz, D., 65, 103
predicate, 11
  symbols, 40, 114
  terms, 40, 115
premise, 14
premises, 7, 14, 53, 64, 66, 143
  closed, 66
  discharged, 66, 68
prenex-form, 154
prime, 12
principle, 7
  of proof by contradiction, 61
  of the excluded middle, 86
  reasoning, 7
proof, 7, 14, 142, 143, 156
  by-contrapositive rule, 54, 93, 144
  checkers, 8
  classical, 61, 143
  constructive, 61, 86, 90, 143
  direct, 12
  formal, 8, 31, 94
  indirect, 12
  informal, 8, 31, 94
  intuitionistic, 143
  mathematical, 7
  minimal, 78
  nonconstructive, 35, 45, 54, 90, 120, 143, 144
  normalization, 75, 98, 103, 104, 145
  principles, 62
  rules, 8, 62, 65
  substitution, 75
  system, 8, 62, 65
  template, 12
  templates, 7, 53
  tree, 68, 77, 82, 83, 119
  proof–by–cases, 24, 84
  proof–by–contradiction, 54, 143
    for negated propositions, 22
    rule, 19, 81
  Proof–By–Contradiction Principle, 19
  proof–by–contrapositive, 29
    principle, 29
  proper
    subset, 47, 135
propositional
  intuitionistic logic, 83
  logic, 53, 143
  minimal logic, 83
  symbols, 12, 67, 115
propositions, 9, 12, 63, 67
  atomic, 12, 67
provability, 64
provable, 83
  in classical logic, 119
quantified formulae, 115, 116
quantifier
  existential, 39
  universal, 39
quantifiers, 8, 38, 62, 113
RAA, 19, 54, 81, 88–90, 143
rank, 115
rational, 33
  number, 33
real, 33
  number, 33
redex, 250
reductio ad absurdum rule, 19, 81
reduction step, 103
regularity axioms, 141
relative complement, 48, 136, 145
relatively prime, 35
repeated squaring, 380
replacement axioms, 141
rules, 7, 68
  logical, 7, 142
  of logic, 7
Russell’s paradox, 133, 145
Russell, B., 133, 138
SAT, 96
satisfiability, 144
  problem, 96, 144
satisfiable, 96
semantics, 35, 95
  truth-value, 35, 54, 95, 144
sequent, 76, 77
  Gentzen, 77
sequents, 143, 155
set, 46, 134
  of integers, 10
  of natural numbers, 10
  of worlds, 99
  theory, 132
singleton set, 134
soundness, 37, 54, 97, 100, 112, 144
standard model, 132
statements, 8, 62
  atomic, 8, 62
  compound, 8, 62
Statman, R., 111
strong
  normalization, 104, 145
strongly normalizing, 110
subset, 47, 135
  axioms, 136, 145
substitution, 40, 108, 116, 248
  safe, 109
Suppes, P., 132
Takeuti, G., 101
tautology, 37, 54, 96, 144
temporal logic, 113
terms, 40, 114, 115
theorem provers, 8, 101
type, 126
  of computation, 101
  of equality, 126
transitive
  set, 161
tree, 66
truth, 9, 35, 63, 64, 95
  tables, 36, 37, 54, 95, 96, 144
  value, 35, 95
  of a proposition, 36, 96
truth-value semantics, 54, 144
Turing machines, 101
Turing, A., 101
type, 104, 271
  second order, 271
  atomic, 104
  base, 104
  polymorphic, 271
  simple, 104
type-assignment, 106
type-checking, 106
  rules, 106
undecidability, 101
  of the decision problem, 101, 145
  of the halting problem, 101
  of the Post correspondence problem, 101
union, 47, 135, 145
  of sets, 47, 135
union axiom, 134, 137
unsatisfiability, 144
unsatisfiable, 96
valid, 37, 96
validity, 54, 144
   problem, 96, 144
van Dalen, D., 38, 62, 90, 98, 100, 112, 113, 116
variable, 105, 245
   bound, 105, 247
   capture, 109, 249
   free, 105, 247
variables
   bound, 54, 144
   free, 54, 144
VNB, 132
von Neumann, J., 132, 140, 161
weakening rule, 72
well-ordering
   of N, 53
witness, 119
   property, 119
Zermelo, E., 132
Zermelo–Fraenkel set theory, 132, 141, 145
ZF, 132, 141, 145