Introduction to the Theory of Computation
Computability, Complexity,
And the Lambda Calculus
Some Notes for CIS262

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 20, 2020
## Contents

1 RAM Programs, Turing Machines .......................... 5
   1.1 Partial Functions and RAM Programs .......................... 6
   1.2 Definition of a Turing Machine .......................... 11
   1.3 Computations of Turing Machines .......................... 13
   1.4 RAM-computable functions are Turing-computable .......................... 16
   1.5 Turing-computable functions are RAM-computable .......................... 17
   1.6 Computably Enumerable and Computable Languages .......................... 18
   1.7 The Primitive Recursive Functions .......................... 19
   1.8 The Partial Computable Functions .......................... 25

2 Universal RAM Programs and the Halting Problem 31
   2.1 Pairing Functions .......................... 31
   2.2 Equivalence of Alphabets .......................... 34
   2.3 Coding of RAM Programs .......................... 38
   2.4 Kleene’s $T$-Predicate .......................... 46
   2.5 A Simple Function Not Known to be Computable .......................... 48
   2.6 A Non-Computable Function; Busy Beavers .......................... 50

3 Elementary Recursive Function Theory 55
   3.1 Acceptable Indexings .......................... 55
   3.2 Undecidable Problems .......................... 58
   3.3 Listable (Recursively Enumerable) Sets .......................... 63
   3.4 Reducibility and Complete Sets .......................... 68
   3.5 The Recursion Theorem .......................... 72
   3.6 Extended Rice Theorem .......................... 76
   3.7 Creative and Productive Sets .......................... 79

4 The Lambda-Calculus 83
   4.1 Syntax of the Lambda-Calculus .......................... 85
   4.2 $\beta$-Reduction and $\beta$-Conversion; the Church–Rosser Theorem .......................... 90
   4.3 Some Useful Combinators .......................... 94
<table>
<thead>
<tr>
<th>Section</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.4</td>
<td>Representing the Natural Numbers</td>
<td>96</td>
</tr>
<tr>
<td>4.5</td>
<td>Fixed-Point Combinators and Recursively Defined Functions</td>
<td>102</td>
</tr>
<tr>
<td>4.6</td>
<td>λ-Definability of the Computable Functions</td>
<td>104</td>
</tr>
<tr>
<td>4.7</td>
<td>Definability of Functions in Typed Lambda-Calculi</td>
<td>110</td>
</tr>
<tr>
<td>4.8</td>
<td>Head Normal-Forms and the Partial Computable Functions</td>
<td>117</td>
</tr>
<tr>
<td>5</td>
<td>Listable and Diophantine Sets; Hilbert’s Tenth</td>
<td>123</td>
</tr>
<tr>
<td>5.1</td>
<td>Diophantine Equations; Hilbert’s Tenth Problem</td>
<td>123</td>
</tr>
<tr>
<td>5.2</td>
<td>Diophantine Sets and Listable Sets</td>
<td>126</td>
</tr>
<tr>
<td>5.3</td>
<td>Some Applications of the DPRM Theorem</td>
<td>130</td>
</tr>
<tr>
<td>5.4</td>
<td>Gödel’s Incompleteness Theorem</td>
<td>133</td>
</tr>
<tr>
<td>6</td>
<td>The Post Correspondence Problem; Applications</td>
<td>139</td>
</tr>
<tr>
<td>6.1</td>
<td>The Post Correspondence Problem</td>
<td>139</td>
</tr>
<tr>
<td>6.2</td>
<td>Some Undecidability Results for CFG’s</td>
<td>140</td>
</tr>
<tr>
<td>6.3</td>
<td>More Undecidable Properties of Languages</td>
<td>143</td>
</tr>
<tr>
<td>7</td>
<td>Computational Complexity; $\mathcal{P}$ and $\mathcal{NP}$</td>
<td>145</td>
</tr>
<tr>
<td>7.1</td>
<td>The Class $\mathcal{P}$</td>
<td>145</td>
</tr>
<tr>
<td>7.2</td>
<td>Directed Graphs, Paths</td>
<td>147</td>
</tr>
<tr>
<td>7.3</td>
<td>Eulerian Cycles</td>
<td>148</td>
</tr>
<tr>
<td>7.4</td>
<td>Hamiltonian Cycles</td>
<td>149</td>
</tr>
<tr>
<td>7.5</td>
<td>Propositional Logic and Satisfiability</td>
<td>150</td>
</tr>
<tr>
<td>7.6</td>
<td>The Class $\mathcal{NP}$, $\mathcal{NP}$-Completeness</td>
<td>155</td>
</tr>
<tr>
<td>7.7</td>
<td>The Cook-Levin Theorem</td>
<td>159</td>
</tr>
<tr>
<td>8</td>
<td>Some $\mathcal{NP}$-Complete Problems</td>
<td>171</td>
</tr>
<tr>
<td>8.1</td>
<td>Statements of the Problems</td>
<td>171</td>
</tr>
<tr>
<td>8.2</td>
<td>Proofs of $\mathcal{NP}$-Completeness</td>
<td>182</td>
</tr>
<tr>
<td>8.3</td>
<td>Succinct Certificates, $\text{coNP}$, and $\mathcal{EXP}$</td>
<td>196</td>
</tr>
<tr>
<td>9</td>
<td>Primality Testing is in $\mathcal{NP}$</td>
<td>201</td>
</tr>
<tr>
<td>9.1</td>
<td>Prime Numbers and Composite Numbers</td>
<td>201</td>
</tr>
<tr>
<td>9.2</td>
<td>Methods for Primality Testing</td>
<td>202</td>
</tr>
<tr>
<td>9.3</td>
<td>Modular Arithmetic, the Groups $\mathbb{Z}/n\mathbb{Z}$, $(\mathbb{Z}/n\mathbb{Z})^*$</td>
<td>205</td>
</tr>
<tr>
<td>9.4</td>
<td>The Lucas Theorem; Lucas Trees</td>
<td>213</td>
</tr>
<tr>
<td>9.5</td>
<td>Algorithms for Computing Powers Modulo $m$</td>
<td>218</td>
</tr>
<tr>
<td>9.6</td>
<td>PRIMES is in $\mathcal{NP}$</td>
<td>220</td>
</tr>
</tbody>
</table>

Bibliography 225

Symbol Index 227

Index 229
Chapter 1

RAM Programs, Turing Machines, and the Partial Computable Functions

See the scanned version of this chapter found in the web page for CIS511:

1.1 Partial Functions and RAM Programs

We define an abstract machine model for computing functions

\[ f : \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_n \rightarrow \Sigma^*, \]

where \( \Sigma = \{a_1, \ldots, a_k\} \) is some input alphabet.

Numerical functions \( f : \mathbb{N}^n \rightarrow \mathbb{N} \) 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 1.1.** A binary relation \( R \subseteq A \times B \) between two sets \( A \) and \( B \) is \textit{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 \textit{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 \textit{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 \( f : A \rightarrow B \).

The \textit{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 \( f(x) \) \textit{converges}, also denoted as \( f(x) \downarrow \).

If \( x \in A \) and \( x \notin \text{dom}(f) \), we say that \( f(x) \) \textit{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 \( f : A \rightarrow B \) is a \textit{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 \textit{RAM programs}, or \textit{Post machines}.

RAM programs are written in a sort of assembly language involving simple instructions manipulating strings stored into registers.
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 \( x_2 \).

\[
\begin{align*}
R3 & \leftarrow R1 \\
R4 & \leftarrow R2 \\
N0 & N4 \text{ jmp}_a N1b \\
N4 & \text{ jmp}_b N2b \\
 & \text{ jmp N3b} \\
N1 & \text{ add}_a R3 \\
 & \text{ tail R4} \\
 & \text{ jmp N0a} \\
N2 & \text{ add}_b R3 \\
 & \text{ tail R4} \\
 & \text{ jmp N0a} \\
N3 & R1 \leftarrow R3 \\
\end{align*}
\]

**Definition 1.2.** *RAM programs* are constructed from seven types of *instructions* shown below:

\[
\begin{align*}
(1_j) & \text{ } N \text{ add}_j Y \\
(2) & \text{ } N \text{ tail } Y \\
(3) & \text{ } N \text{ clr } Y \\
(4) & \text{ } N Y \leftarrow X \\
(5a) & \text{ } N \text{ jmp N1a} \\
(5b) & \text{ } N \text{ jmp N1b} \\
(6Ja) & \text{ } N Y \text{ jmp}_j N1a \\
(6Jb) & \text{ } N Y \text{ jmp}_j N1b \\
(7) & \text{ } N \text{ continue}
\end{align*}
\]
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 $tail$, defined such that

$$tail(\epsilon) = \epsilon,$$
$$tail(a_ju) = u.$$ 

The effect is the assignment

$$Y := tail(Y).$$ 

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 $N_1$ occurring above the instruction being executed, and the effect of (5b) is to jump to the closest line number $N_1$ occurring below the instruction being executed.

6. An instruction of type $(6_ja)$ or $(6_jb)$ is a conditional jump. Let $head$ be the function defined as follows:

$$head(\epsilon) = \epsilon,$$
$$head(a_ju) = a_j.$$ 

The effect of $(6_ja)$ is to jump to the closest line number $N_1$ occurring above the instruction being executed iff $head(Y) = a_j$, else to execute the next instruction (the one immediately following the instruction being executed).
1.1. *PARTIAL FUNCTIONS AND RAM PROGRAMS*

The effect of $(6_j b)$ is to jump to the closest line number $N1$ occurring below the instruction being executed iff $\text{head}(Y) = a_j$, else to execute the next instruction.

When computing over $\mathbb{N}$, instructions of type $(6_j b)$ jump to the closest $N1$ 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 1.3.** A *RAM program* $P$ is a finite sequence of instructions as in Definition 1.2, 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 $N1$ 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 $R1, \ldots, Rn$ are initialized with the input values of the function $f$.

We also assume that the output is returned in register $R1$.

The following RAM program concatenates two strings $x_1$ and $x_2$ held in registers $R1$ and $R2$.

$$
\begin{align*}
R3 & \leftarrow R1 \\
R4 & \leftarrow R2 \\
N0 & R4 \text{ jmp}_a N1b \\
R4 & \text{ jmp}_b N2b \\
        & \text{ jmp } N3b \\
N1 & \text{ add}_a R3 \\
        & \text{ tail } R4 \\
        & \text{ jmp } N0a \\
N2 & \text{ add}_b R3 \\
        & \text{ tail } R4 \\
        & \text{ jmp } N0a \\
N3 & R1 \leftarrow R3 \\
        & \text{ continue }
\end{align*}
$$
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 1.4.** 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 *iff 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 $u \in \Sigma^*$:

\[
\begin{align*}
\text{clr} & \quad R_1 \\
\text{continue} & \quad \text{R1}
\end{align*}
\]

The following program computes the *$j$th successor function* $S_j$ defined such that

$$S_j(u) = ua_j$$

for all $u \in \Sigma^*$:

\[
\begin{align*}
\text{add}_j & \quad R_1 \\
\text{continue} & \quad \text{R1}
\end{align*}
\]

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 $1 \leq i \leq n$:

\[
\begin{align*}
R_1 & \leftarrow \quad R_i \\
\text{continue} & \quad \text{Ri}
\end{align*}
\]

Note that $P^n_1$ 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-fashion.

This class can be given several other definitions. We will present the definition of the so-called \( \mu \)-recursive functions (due to Kleene).

The following proposition will be needed to simplify the encoding of RAM programs as numbers.

**Proposition 1.1.** Every RAM program can be converted to an equivalent program only using the following type of instructions:

<table>
<thead>
<tr>
<th>Instruction</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) ( j )</td>
<td>( N ), add ( j ), Y</td>
</tr>
<tr>
<td>(2)</td>
<td>( N ), tail, Y</td>
</tr>
<tr>
<td>(6, a)</td>
<td>( N ), Y, ( \text{jmp}_j ), N1a</td>
</tr>
<tr>
<td>(6, b)</td>
<td>( N ), Y, ( \text{jmp}_j ), N1b</td>
</tr>
<tr>
<td>(7)</td>
<td>( N ), continue</td>
</tr>
</tbody>
</table>

The proof is fairly simple. For example, instructions of the form

\[ R_i \leftarrow R_j \]

can be eliminated by transferring the contents of \( R_j \) into an auxiliary register \( R_k \), and then by transferring the contents of \( R_k \) into \( R_i \) and \( R_j \).

### 1.2 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 1.5.** 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:
1.3 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 1.6.** 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 1.7.** 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

$$q_0, B \rightarrow B, R, q_3,$$

$$q_0, a \rightarrow b, R, q_1,$$

$$q_0, b \rightarrow a, R, q_1,$$

$$q_1, a \rightarrow b, R, q_1,$$

$$q_1, b \rightarrow a, R, q_1,$$

$$q_1, B \rightarrow B, L, q_2,$$

$$q_2, a \rightarrow a, L, q_2,$$

$$q_2, b \rightarrow b, L, q_2,$$

$$q_2, B \rightarrow B, R, q_3.$$
(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 \( \vdash^\ast \) denote the reflexive and transitive closure of \( \vdash. \)

We can now explain how a Turing machine computes a partial function

\[
\begin{align*}
  f &: \prod_{i=1}^{n} \Sigma^* \to \Sigma^*.
\end{align*}
\]

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 1.8.** 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 \( q_0w \) \( w \in \Sigma^+, \) 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 1.9. 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 1.10. 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

\[ ID_0 = q_0 w_1, w_2, \ldots, w_n \]

or \( q_0 w \) with \( w \in \Sigma^+ \), or \( q_0 B \), 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:

$q_0, B \rightarrow B, R, q_3$,

$q_0, a \rightarrow b, R, q_1$,

$q_0, b \rightarrow a, R, q_1$,

$q_1, a \rightarrow b, R, q_1$,

$q_1, b \rightarrow a, R, q_1$,

$q_1, B \rightarrow B, L, q_2$,

$q_2, a \rightarrow a, L, q_2$,

$q_2, b \rightarrow b, L, q_2$,

$q_2, B \rightarrow B, R, q_3$.

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 $bbbabaa$.

### 1.4 RAM-computable functions are Turing-computable

Turing machines can simulate RAM programs, and as a result, we have the following Theorem.

**Theorem 1.2.** 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 $R_1, \ldots, R_p$ on the Turing machine tape by the string

$\#r_1#r_2# \cdots #r_p#$,
1.5 Turing-computable functions are RAM-computable

RAM programs can also simulate Turing machines.

**Theorem 1.3.** 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 1.7.

**Definition 1.11.** 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.
1.6 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 1.12. 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).

### 1.7 The Primitive Recursive Functions

The class of primitive recursive functions is defined in terms of base functions and closure operations.

**Definition 1.13.** 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 1.14.** 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 1.15.** Let \( \Sigma = \{a_1, \ldots, a_N\} \). For any function
\[
g : \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{m-1} \to \Sigma^*,
\]
where \( m \geq 2 \), and any \( N \) functions
\[
h_i : \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_{m+1} \to \Sigma^*,
\]
the function
\[
f : \underbrace{\Sigma^* \times \cdots \times \Sigma^*}_m \to \Sigma^*,
\]
is defined by **primitive recursion from** \( g \) **and** \( h_1, \ldots, h_N \), if
\[
f(\epsilon, w_2, \ldots, w_m) = g(w_2, \ldots, w_m),
f(ua_1, w_2, \ldots, w_m) = h_1(u, f(u, w_2, \ldots, w_m), w_2, \ldots, w_m),
\]
\[
\vdots = \ldots
\]
\[
f(ua_N, w_2, \ldots, w_m) = h_N(u, f(u, w_2, \ldots, w_m), w_2, \ldots, w_m),
\]
for all \( u, w_2, \ldots, w_m \in \Sigma^* \).

When \( m = 1 \), for some fixed \( w \in \Sigma^* \), we have
\[
f(\epsilon) = w,
f(ua_1) = h_1(u, f(u)),
\]
\[
\vdots = \ldots
\]
\[
f(ua_N) = h_N(u, f(u)),
\]
for all \( u \in \Sigma^* \).

For numerical functions (i.e., when \( \Sigma = \{a_1\} \)), the scheme of primitive recursion is simpler:
\[
f(0, x_2, \ldots, x_m) = g(x_2, \ldots, x_m),
f(x + 1, x_2, \ldots, x_m) = h_1(x, f(x, x_2, \ldots, x_m), x_2, \ldots, x_m),
\]
for all \( x, x_2, \ldots, x_m \in \mathbb{N} \).

The \textit{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 ...):

\[
\begin{align*}
text{add}(0,n) &= P^1_1(n) = n, \\
\text{add}(m+1,n) &= S \circ P^3_2(m, \text{add}(m,n), n) \\
&= S(\text{add}(m,n)) \\
\text{mult}(0,n) &= E(n) = 0, \\
\text{mult}(m+1,n) &= \text{add} \circ (P^3_2, P^3_3)(m, \text{mult}(m,n), n) \\
&= \text{add}(\text{mult}(m,n), n), \\
\text{rexp}(0,n) &= S \circ E(n) = 1, \\
\text{rexp}(m+1,n) &= \text{mult}(\text{rexp}(m,n), n), \\
\text{exp}(m,n) &= \text{rexp} \circ (P^2_2, P^2_1)(m,n), \\
\text{supexp}(0,n) &= 1, \\
\text{supexp}(m+1,n) &= \text{exp}(n, \text{supexp}(m,n)).
\end{align*}
\]

We usually write \( m + n \) for \( \text{add}(m,n) \), \( m \ast n \) or even \( mn \) for \( \text{mult}(m,n) \), and \( m^n \) for \( \text{exp}(m,n) \).

There is a minus operation on \( \mathbb{N} \) named \textit{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 \textit{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 \textit{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 \textit{monus}.
As an example over \( \{a, b\}^* \), the following function
\( g: \Sigma^* \times \Sigma^* \to \Sigma^* \), is defined by primitive recursion:

\[
g(\epsilon, v) = P_1^1(v),
\]
\[
g(ua_i, v) = S_i \circ P_2^3(u, g(u, v), v),
\]

where \( 1 \leq i \leq N \). It is easily verified that \( g(u, v) = vu \). Then,

\[
f = g \circ (P_2^1, P_1^2)
\]

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

\[
abs(m, n) = |m - m| = m \cdot n + n \cdot m,
\]

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

\[
\text{cond}(m, n, p, q) = eq(m, n) \ast p + \overline{sg}(eq(m, n)) \ast q.
\]
We can also design more general version of \textit{cond}. For example, define \textit{compare} 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
\[
\text{compare}_\leq (m, n) = 1 - \text{sg}(m - n).
\]
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
\[
\text{cond}_\leq (m, n, n, p) = \text{compare}_\leq (m, n) \ast p + \overline{\text{sg}}(\text{compare}_\leq (m, n)) \ast q.
\]
The above allows to define functions by cases.

\textbf{Definition 1.16.} Let $\Sigma = \{a_1, \ldots, a_N\}$. The class of \textit{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.

\textbf{Theorem 1.4.} 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 1.2 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.

\textbf{Definition 1.17.} An \textit{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 \textit{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 \textit{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 $(\Sigma^\ast)^n$), 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 1.5.** 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:

$$g(x) = \begin{cases} f_1(x) & \text{iff } P_1(x) \\ \vdots \\ f_n(x) & \text{iff } P_n(x) \\ f_{n+1}(x) & \text{otherwise.} \end{cases}$$

(writing $\bar{x}$ for $(x_1, \ldots, x_n)$.)

It is also useful to have bounded quantification and bounded minimization.

**Definition 1.18.** 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 1.6.** 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 1.19.** If $P$ is an $(n+1)$-ary predicate, then the bounded minimization of $P$, $\min y/x P(y, z)$, is the function defined such that $\min y/x P(y, z)$ is the shortest prefix of $x$ such that $P(y, z)$ if such a $y$ exists, $xa_1$ otherwise.

The bounded maximization of $P$, $\max y/x P(y, z)$, is the function defined such that $\max y/x P(y, z)$ is the longest prefix of $x$ such that $P(y, z)$ if such a $y$ exists, $xa_1$ otherwise.
Proposition 1.7. 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.

1.8 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

$$g(u, w_1, \ldots, w_m) = \epsilon :$$

$$u := \epsilon;$$
while $g(u, w_1, \ldots, w_m) \neq \epsilon$ do
$$u := ua_j;$$
endwhile
let $f(w_1, \ldots, w_m) = u$

The operation of minimization (sometimes called minimalization) is defined as follows.

Definition 1.20. 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 minimization over $\{a_j\}^*$ 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 1.21. 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.
1.8. THE PARTIAL COMPUTABLE FUNCTIONS

Theorem 1.8. 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 1.2, 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 $A: \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ which is defined by the following recursive clauses:

\[
\begin{align*}
A(0, y) &= y + 1, \\
A(x + 1, 0) &= A(x, 1), \\
A(x + 1, y + 1) &= A(x, A(x + 1, y)).
\end{align*}
\]

It turns out that $A$ is a computable function which is not primitive recursive.

It can be shown that:

\[
\begin{align*}
A(0, x) &= x + 1, \\
A(1, x) &= x + 2, \\
A(2, x) &= 2x + 3, \\
A(3, x) &= 2^{x+3} - 3,
\end{align*}
\]

and

\[
A(4, x) = 2^{2^{2^{\cdots^{2^{16}}}}} - 3,
\]

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 \( \leq \) on \( \mathbb{N} \times \mathbb{N} \), which is defined as follows:

\[
(m, n) \leq (m', n') \quad \text{iff either}
\begin{align*}
& m = m' \text{ and } n = n', \\
& m < m', \\
& m = m' \text{ and } n < n'.
\end{align*}
\]

We write \( (m, n) \prec (m', n') \) when \( (m, n) \leq (m', n') \) 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).
1.8. THE PARTIAL COMPUTABLE FUNCTIONS

**Definition 1.22.** We say that a function \( f : \Sigma^* \times \Sigma^* \rightarrow \Sigma^* \) is universal for the one-argument functions in \( \mathcal{F} \) iff for every function \( g : \Sigma^* \rightarrow \Sigma^* \) in \( \mathcal{F} \), there is some \( n \in \mathbb{N} \) such that
\[
 f(a_1^n, u) = g(u)
\]
for all \( u \in \Sigma^* \).

**Proposition 1.9.** 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 \( g : \Sigma^* \rightarrow \Sigma^* \) 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
\[
 g(u) = f(a_1^{|u|}, u) a_1
\]
for all \( u \in \Sigma^* \). We claim that \( g \in \mathcal{F} \). It is enough to prove that the function \( h \) such that
\[
 h(u) = a_1^{|u|}
\]
is primitive recursive, which is easily shown.

Then, because \( f \) is universal, there is some \( m \) such that
\[
 g(u) = f(a_1^m, u)
\]
for all \( u \in \Sigma^* \). Letting \( u = a_1^m \), we get
\[
 g(a_1^m) = f(a_1^m, a_1^m) = f(a_1^m, a_1^m) a_1,
\]
a contradiction. \( \square \)

Thus, either a universal function for \( \mathcal{F} \) is partial, or it is not in \( \mathcal{F} \).
Chapter 2

Universal RAM Programs and Undecidability of the Halting Problem

2.1 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 $J: \mathbb{N}^2 \to \mathbb{N}$. The function $J$ has the graph partially showed below:

```
   y
  4 10
  |  \
  3 6 11
  |  \
  2 3 7 12
  |  \
  1 1 4 8 13
  |  \
  0 0 2 5 9 14
  |  \
  0 1 2 3 4
```

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

$$K(J(a,b)) = a \text{ and } L(J(a,b)) = b,$$

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 $J$,

$$x \leq J(x,y) \text{ and } y \leq J(x,y),$$

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

$$Q_1(z) = \left\lceil \left(\lfloor \sqrt{8z + 1} \rfloor + 1 \right)/2 \right\rceil - 1,$$

$$Q_2(z) = 2z - (Q_1(z))^2,$$

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.

\[ \langle x_1, x_2, x_3 \rangle_3 = \langle x_1, \langle x_2, x_3 \rangle \rangle_2 \]

\[ = \langle x_1, x_2, x_3 \rangle \]

\[ \langle x_1, x_2, x_3, x_4 \rangle_4 = \langle x_1, x_2, \langle x_3, x_4 \rangle \rangle_3 \]

\[ = \langle x_1, x_2, x_3, x_4 \rangle \]

\[ \langle x_1, x_2, x_3, x_4, x_5 \rangle_5 = \langle x_1, x_2, x_3, \langle x_4, x_5 \rangle \rangle_4 \]

\[ = \langle x_1, x_2, x_3, \langle x_4, x_5 \rangle \rangle \]

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 \( \text{Large} \), 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 \( \varphi: \mathbb{N}^n \rightarrow \mathbb{N} \) 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 \( \mathbb{N} \).

### 2.2 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 \( a_1 \) 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

\[ a, b, c, aa, ab, ac, ba, bb, bc, ca, cb, cc, \]

\[ aaaa, aab, aac, aba, abb, abc, \ldots. \]

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 \( f: \Sigma^* \rightarrow \mathbb{N} \) 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*. 
Since we also want a decoding function, we define the coding function \( C_k : \Sigma^* \rightarrow \Sigma^* \) as follows:

\[
C_k(\epsilon) = \epsilon, \text{ and if } u = a_{i_1} \cdots a_{i_n}, \text{ then }
C_k(u) = a_{i_1 k^{n-1} + i_2 k^{n-2} + \cdots + i_n - 1} a_{i_n}.
\]

The function \( C_k \) is primitive recursive, because

\[
C_k(\epsilon) = \epsilon, \quad C_k(xa_i) = C_k(x) a_i.
\]

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

\[
D_k(x) = D_k(a_1|x|)
\]

for all \( x \in \Sigma^* \). It remains to define \( D_k \) by primitive recursion over \( \{a_1\}^* \). For this, we introduce three auxiliary functions \( p, q, r \), defined as follows. Let

\[
p(\epsilon) = \epsilon, \quad p(xa_i) = xa_i, \text{ if } i \neq k, \quad p(xa_k) = p(x).
\]

Note that \( p(x) \) is the result of deleting consecutive \( a_k \)'s in the tail of \( x \). Let

\[
q(\epsilon) = \epsilon, \quad q(xa_i) = q(x)a_1.
\]

Note that \( q(x) = a_1|x| \). Finally, let

\[
r(\epsilon) = a_1, \quad r(xa_i) = xa_{i+1}, \text{ if } i \neq k, \quad r(xa_k) = xa_k.
\]

The function \( r \) is almost the successor function, for the ordering. Then, the trick is that \( D_k(xa_i) \) is the successor of \( D_k(x) \) in the ordering, and if

\[
D_k(x) = ya_ja_k^n
\]

with \( j \neq k \), since the successor of \( ya_ja_k^n \) is \( ya_{j+1}a_k^n \), we can use \( r \). Thus, we have

\[
D_k(\epsilon) = \epsilon, \quad D_k(xa_i) = r(p(D_k(x)))q(D_k(x) - p(D_k(x))).
\]
Then, both $C_k$ and $D_k$ are primitive recursive, and $C_k \circ D_k = D_k \circ C_k = \text{id}$.

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 $\psi^+$ 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:

$$f(0) = 1,$$

$$f(1) = 1,$$

$$f(n + 2) = f(n + 1) + f(n),$$

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, $g(y + 1, \overline{x})$ is only allowed to depend upon $g(y, \overline{x})$.

**Definition 2.1.** Given any function $f: \mathbb{N}^n \to \mathbb{N}$, the function $\overline{f}: \mathbb{N}^{n+1} \to \mathbb{N}$ defined such that

$$\overline{f}(y, \overline{x}) = (f(0, \overline{x}), \ldots, f(y, \overline{x}))_{y+1}$$

is called the course-of-value function for $f$.

The following lemma holds.

**Proposition 2.1.** Given any function $f: \mathbb{N}^n \to \mathbb{N}$, if $f$ is primitive recursive, then so is $\overline{f}$. 

2.2. EQUIVALENCE OF ALPHABETS

Proof. First, it is necessary to define a function \( con \) 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
\[
con(m, x, y) = \langle x_1, \ldots, x_m, y_1, \ldots, y_n \rangle.
\]
This fact is left as an exercise. Now, if \( f \) is primitive recursive, let
\[
\overline{f}(0, x) = f(0, x),
\]
\[
\overline{f}(y + 1, x) = con(y + 1, \overline{f}(y, x), f(y + 1, x)),
\]
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.

Remark: Why is it that
\[
\overline{f}(y + 1, x) = \langle \overline{f}(y, x), f(y + 1, x) \rangle
\]
do not work?

We define \textit{course-of-value recursion} as follows.

\textbf{Definition 2.2.} Given any two functions \( g : \mathbb{N}^n \to \mathbb{N} \) and \( h : \mathbb{N}^{n+2} \to \mathbb{N} \), the function \( f : \mathbb{N}^{n+1} \to \mathbb{N} \) is defined by \textit{course-of-value recursion} from \( g \) and \( h \) if
\[
f(0, x) = g(x),
\]
\[
f(y + 1, x) = h(y, \overline{f}(y, x), x).
\]

The following lemma holds.

\textbf{Proposition 2.2.} If \( f : \mathbb{N}^{n+1} \to \mathbb{N} \) is defined by course-of-value recursion from \( g \) and \( h \) and \( g, h \) are primitive recursive, then \( f \) is primitive recursive.

\textit{Proof.} We prove that \( \overline{f} \) is primitive recursive. Then, by Proposition 2.1, \( f \) is also primitive recursive. To prove that \( \overline{f} \) is primitive recursive, observe that
\[
\overline{f}(0, x) = g(x),
\]
\[
\overline{f}(y + 1, x) = con(y + 1, \overline{f}(y, x), h(y, \overline{f}(y, x), x)).
\]

When we use Proposition 2.2 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 \( f(y + 1, x) \) can be obtained in a primitive recursive manner from \( f(0, x) \) through \( f(y, x) \). Thus, an informal use of Proposition 2.2 shows that the Fibonacci function is primitive recursive. A rigorous proof of this fact is left as an exercise.
2.3 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 add and jmp (and add increments by 1 the contents of the specified register \( R_j \)).

\[
\begin{align*}
Ni \, \text{add} \, R_j \quad & \text{code} = \langle 1, i, j, 0 \rangle \\
Ni \, \text{tail} \, R_j \quad & \text{code} = \langle 2, i, j, 0 \rangle \\
Ni \, \text{continue} \quad & \text{code} = \langle 3, i, 1, 0 \rangle \\
Ni \, R_j \, \text{jmp} \, Nka \quad & \text{code} = \langle 4, i, j, k \rangle \\
Ni \, R_j \, \text{jmp} \, Nkb \quad & \text{code} = \langle 5, i, j, k \rangle
\end{align*}
\]

Recall that a conditional jump causes a jump to the closest address \( Nk \) above or below iff \( R_j \) is nonzero, and if \( R_j \) 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 Typ, Nam, Reg, and Jmp, defined as follows:

\[
\begin{align*}
\text{Typ}(x) &= \Pi(1, 4, x), \\
\text{Nam}(x) &= \Pi(2, 4, x), \\
\text{Reg}(x) &= \Pi(3, 4, x), \\
\text{Jmp}(x) &= \Pi(4, 4, x).
\end{align*}
\]

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

\[
\langle x, y \rangle = ((x + y)^2 + 3x + y)/2.
\]

Consider the following program \( \text{Padd2} \) computing the function \( \text{add2} : \mathbb{N} \to \mathbb{N} \) given by

\[
\text{add2}(n) = n + 2.
\]

\[
I_1 : 1 \quad \text{add} \quad R1 \\
I_2 : 2 \quad \text{add} \quad R1 \\
I_3 : 3 \quad \text{continue}
\]

We have

\[
\#I_1 = \langle 1, 1, 1, 0 \rangle_4 = \langle 1, \langle 1, 1, 0 \rangle \rangle = 37 \\
\#I_2 = \langle 1, 2, 1, 0 \rangle_4 = \langle 1, \langle 2, 1, 0 \rangle \rangle = 92 \\
\#I_3 = \langle 3, 3, 1, 0 \rangle_4 = \langle 3, \langle 3, 1, 0 \rangle \rangle = 234
\]

and

\[
\#\text{Padd2} = \langle 3, \#I_1, \#I_2, \#I_3 \rangle_4 = \langle 3, \langle 37, \langle 92, 234 \rangle \rangle \rangle \\
= 1018748519973070618.
\]

The codes get big fast!

We define the primitive recursive functions \( \text{Ln}, \text{Pg}, \) and \( \text{Line} \), such that:

\[
\text{Ln}(x) = \Pi(1, 2, x),
\text{Pg}(x) = \Pi(2, 2, x),
\text{Line}(i, x) = \Pi(i, \text{Ln}(x), \text{Pg}(x)).
\]
The function Ln yields the length of the program (the number of instructions), Pg yields the sequence of instructions in the program (really, a code for the sequence), and Line(i, x) yields the code of the ith 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

\[
\text{Line}(0, x) = \text{Line}(1, x), \quad \text{and} \\
\text{Line}(\text{Ln}(x), x) = \text{Line}(i, x), \quad \text{for all } i \geq x.
\]

The primitive recursive predicate PROG is defined such that PROG(x) holds iff x codes a program. Thus, 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

\[
\forall i \leq \text{Ln}(x)[i \geq 1 \supset [\text{INST(Line}(i, x)) \land \text{Typ(Line(Ln(x), x))} = 3
\land \text{Typ(Line}(i, x)) = 4 \supset \\
\exists j \leq i - 1[j \geq 1 \land \text{Nam(Line}(j, x)) = \text{Jmp(Line}(i, x))]]\land
\text{Typ(Line}(i, x)) = 5 \supset \\
\exists j \leq \text{Ln}(x)[j > i \land \text{Nam(Line}(j, x)) = \text{Jmp(Line}(i, x))]].
\]

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 2.3. (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 R1 and with input i in register R2 (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 R1 iff i codes a program that runs forever when started on input x in R1 (all other registers set to zero).
3. If i does not code a program, then Decider halts with output 2 in R1.

**Proof.** Assume that Decider is such a RAM program, and let Q be the following program with a single input:

\[
\text{Program Q (code q)} \begin{cases}
R2 \leftarrow R1 \\
P \quad N1 \text{ continue} \\
R1 \quad \text{jmp} \quad N1a \\
\end{cases}
\]
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 \( \text{Decider} \) on input \( i \) and code \( i \).*

1. If \( \text{Decider} \) says that program \( P \) coded by \( i \) halts on input \( i \), then \( R1 \) just after the `continue` in line \( N1 \) contains 1, and \( Q \) loops forever.

2. If \( \text{Decider} \) says that program \( P \) coded by \( i \) loops forever on input \( i \), then \( R1 \) just after `continue` in line \( N1 \) 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:

\[
\text{Reg(Line}(i, x)) \leq \text{Line}(i, x) \leq \text{Pg}(x)
\]
for all \( i, x \in \mathbb{N} \). Then, if \( x \) codes a program, then \( R_1, \ldots, R_x \) 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 2.3.** Let \( x \) code a program and let \( i \) be such that \( 1 \leq i \leq \text{Ln}(x) \). The following functions are defined:

1. \( \text{Nextline}(i, x, y) \) 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. \( \text{Nextcont}(i, x, y) \) 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 2.4.** The functions Nextline, Nextcont, and Comp, are primitive recursive.

**Proof.** (1) \( \text{Nextline}(i, x, y) = i + 1 \), unless the \( i \)th instruction is a jump and the contents of the register being tested is nonzero:

\[
\text{Nextline}(i, x, y) = \\
\max j \leq \text{Ln}(x)[j < i \land \text{Nam(Line}(j, x)) = \text{Jmp(Line}(i, x))] \\
\text{if Typ(Line}(i, x)) = 4 \land \Pi(\text{Reg(Line}(j, x)), x, y) \neq 0 \\
\min j \leq \text{Ln}(x)[j > i \land \text{Nam(Line}(j, x)) = \text{Jmp(Line}(i, x))] \\
\text{if Typ(Line}(i, x)) = 5 \land \Pi(\text{Reg(Line}(j, x)), x, y) \neq 0 \\
i + 1 \text{ otherwise}.
\]

Note that according to this definition, if the \( i \)th line is the final \texttt{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.

\( \text{Add}(j, x, y) \) is the number coding the contents of the registers used by the program coded by \( x \) after register \( R_j \) coded by \( \Pi(j, x, y) \) has been increased by 1, and
2.3. CODING OF RAM PROGRAMS

Sub\((j, x, y)\) codes the contents of the registers after register \(R_j\) has been decremented by 1 (\(y\) codes the previous contents of the registers). It is easy to see that

\[
\text{Sub}(j, x, y) = \min z \leq y [\Pi(j, x, z) = \Pi(j, x, y) - 1 \\
\land \forall k \leq x [0 < k \neq j \lor \Pi(k, x, z) = \Pi(k, x, y)]].
\]

The definition of Add is slightly more tricky. We leave as an exercise to the reader to prove that:

\[
\text{Add}(j, x, y) = \min z \leq \text{Large}(x, y + 1) [\Pi(j, x, z) = \Pi(j, x, y) + 1 \land \forall k \leq x [0 < k \neq j \lor \Pi(k, x, z) = \Pi(k, x, y)]],
\]

where the function Large is the function defined in an earlier exercise. Then

\[
\text{Nextcont}(i, x, y) = \begin{cases} 
\text{Add}(\text{Reg(Line}(i, x), x, y)) & \text{if } \text{Typ(Line}(i, x)) = 1 \\
\text{Sub}(\text{Reg(Line}(i, x), x, y)) & \text{if } \text{Typ(Line}(i, x)) = 2 \\
y & \text{if } \text{Typ(Line}(i, x)) \geq 3.
\end{cases}
\]

(3) Recall that \(\Pi_1(z) = \Pi(1, 2, z)\) and \(\Pi_2(z) = \Pi(2, 2, z)\). The function Comp is defined by primitive recursion as follows:

\[
\text{Comp}(x, y, 0) = \langle 1, y \rangle \\
\text{Comp}(x, y, m + 1) = \langle \text{Nextline}(\Pi_1(\text{Comp}(x, y, m)), x, \Pi_2(\text{Comp}(x, y, m))), 
\text{Nextcont}(\Pi_1(\text{Comp}(x, y, m)), x, \Pi_2(\text{Comp}(x, y, m))) \rangle.
\]

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 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

\[
z = \Pi_2(\text{Comp}(x, \langle y, 0 \rangle, m))
\]

\[
z = \Pi_2(\text{Comp}(x, \langle y, 0 \rangle, \text{End}(x, \langle y, 0 \rangle))).
\]

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 1.9, the partial function $\varphi_{\text{univ}}$ is not computable (recursive). 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:

```
N1      add   R1
N1     jmp   N1a
N1    continue
```

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 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 UNIV that has a code 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 2.4.** 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 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 $\varphi_x$.

---

\[\text{The term recursive function is now considered old-fashion. Many researchers have switched to the term computable function.}\]
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 $\varphi_{univ}$ is sufficiently important to be recorded in the following proposition.

**Proposition 2.5.** For the indexing of RAM programs defined earlier, there is a universal partial computable function $\varphi_{univ}$ such that, for all $x,y \in \mathbb{N}$, if $\varphi_x$ is the partial computable function computed by $P_x$, then

$$
\varphi_x(y) = \varphi_{univ}(\langle x, y \rangle).
$$

The program UNIV computing $\varphi_{univ}$ 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 2.3 and Proposition 2.5, 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.

### 2.4 Kleene’s $T$-Predicate

In Section 2.3, 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

$$
z = \langle n + 2, \langle 1, y_0 \rangle, \langle i_1, y_1 \rangle, \dots, \langle i_n, y_n \rangle \rangle,
$$

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 2.5.** The $T$-predicate is the primitive recursive predicate defined as follows:

$$T(x,y,z) \text{ iff } \text{PROG}(x) \text{ and } (\text{Ln}(z) \geq 3) \text{ and }$$

$$\forall j \leq \text{Ln}(z) - 3 [0 \leq j \supset \text{Nextline}(\Pi_1(\Pi(j + 2, \text{Ln}(z), z)), x, \Pi_2(\Pi(j + 2, \text{Ln}(z), z))) = \Pi_1(\Pi(j + 3, \text{Ln}(z), z)) \text{ and }$$

$$\text{Nextcont}(\Pi_1(\Pi(j + 2, \text{Ln}(z), z)), x, \Pi_2(\Pi(j + 2, \text{Ln}(z), z))) = \Pi_2(\Pi(j + 3, \text{Ln}(z), z)) \text{ and }$$

$$\Pi_1(\Pi(\text{Ln}(z) - 1, \text{Ln}(z), z)) = \text{Ln}(x) \text{ and }$$

$$\Pi_1(\Pi(2, \text{Ln}(z), z)) = 1 \text{ and }$$

$$y = \Pi_1(\Pi_2(\Pi(2, \text{Ln}(z), z))) \text{ and } \Pi_2(\Pi_2(\Pi(2, \text{Ln}(z), z))) = 0]$$

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 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 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 2.6.** (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 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 Conprogs creates the code of the program obtained by concatenating the programs $P_x$ and $P_y$, and for $i \geq 2$, Cumclr($i$) is the code of the program which clears registers $R2, \ldots, Ri$. To get Cumclr, we can use the function clr($i$) such that clr($i$) is the code of the program

\[
\begin{array}{ccc}
N1 & \text{tail} & Ri \\
N1 & Ri & \text{jmp} \\
N & \text{continue} & N1a
\end{array}
\]

We leave it as an exercise to prove that clr, Conprogs, and Cumclr, are primitive recursive.
Theorem 2.7. There is a primitive recursive function \( c \) such that
\[
\varphi_{c(x,y)} = \varphi_x \circ \varphi_y.
\]

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:
\[
c(x, y) = \begin{cases} 
\text{Conprogs}(y, \text{Conprogs}(\text{Cumclr}(y), x)) & \text{if PROG}(x) \text{ and } \text{PROG}(y) \\
\text{loop} & \text{otherwise}.
\end{cases}
\]

\[\square\]

2.5 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 2.1.

![Figure 2.1: Graph of the sequence for $n = 8400511$.](image)

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 2.2.

So far, the conjecture remains open. It has been checked by computer for all integers less than or equal to $87 \times 2^{60}$.

### 2.6 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 2.6.** 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 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 \( (4(n + 1))^{2n} \). 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^{18,267} )</td>
<td>( \geq 7.412 \times 10^{36,534} )</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:

<table>
<thead>
<tr>
<th></th>
<th>( A )</th>
<th>( B )</th>
<th>( C )</th>
<th>( D )</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \Delta )</td>
<td>(1, ( R ), ( B ))</td>
<td>(1, ( L ), ( A ))</td>
<td>(1, ( R ), ( H ))</td>
<td>(1, ( R ), ( D ))</td>
</tr>
<tr>
<td>1</td>
<td>(1, ( L ), ( B ))</td>
<td>(( \Delta ), ( L ), ( C ))</td>
<td>(1, ( L ), ( D ))</td>
<td>(( \Delta ), ( R ), ( A ))</td>
</tr>
</tbody>
</table>

The above machine output 13 ones in 107 steps. In fact, the output is

\[ \Delta \Delta 1 \Delta 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 \Delta \Delta. \]

5-state best contender:
The above machine output 4098 ones in 47,176,870 steps.

6-state contender (Heiner Marxen):

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>∆</td>
<td>(1, R, B)</td>
<td>(1, R, C)</td>
<td>(1, R, D)</td>
<td>(1, L, A)</td>
<td>(1, R, H)</td>
</tr>
<tr>
<td>1</td>
<td>(1, L, C)</td>
<td>(1, R, B)</td>
<td>(∆, L, E)</td>
<td>(1, L, D)</td>
<td>(∆, L, A)</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></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>∆</td>
<td>(1, R, B)</td>
<td>(1, L, C)</td>
<td>(∆, R, F)</td>
<td>(1, R, A)</td>
<td>(1, L, H)</td>
<td>(∆, L, A)</td>
</tr>
<tr>
<td>1</td>
<td>(1, R, A)</td>
<td>(1, L, B)</td>
<td>(1, L, D)</td>
<td>(∆, L, E)</td>
<td>(1, L, F)</td>
<td>(∆, L, 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 2.8.** 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

$$\Sigma(n + k_f) \geq f(n) \text{ for all } n \geq 0.$$  

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

$$\Sigma(n + k_f) \geq f(n) \text{ for all } n \geq 0.$$  

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

$$\Sigma(n + k_g) \geq g(n) = \Sigma(2n) \text{ for all } n \geq 0,$$
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 2.3.
Chapter 3

Elementary Recursive Function Theory

3.1 Acceptable Indexings

In Chapter 2, 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 3.1.** 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 $\varphi_{\text{univ}}$.
CHAPTER 3. ELEMENTARY RECURSIVE FUNCTION THEORY

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 2, 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 2.3 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 \( \varphi((x_1, \ldots, x_n)) \), 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 \( \psi \).

**Theorem 3.1.** (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
\[ \varphi_{s(i, m, x_1, \ldots, x_m)}(y_1, \ldots, y_n) = \varphi_i(x_1, \ldots, x_m, y_1, \ldots, y_n). \]

**Proof.** First, note that the above identity is really
\[ \varphi_{s(i, m, x_1, \ldots, x_m)}((y_1, \ldots, y_n)) = \varphi_i((x_1, \ldots, x_m, y_1, \ldots, y_n)). \]

Recall that there is a primitive recursive function \( \text{Con} \) such that
\[ \text{Con}(m, (x_1, \ldots, x_m), (y_1, \ldots, y_n)) = (x_1, \ldots, x_m, y_1, \ldots, y_n) \]
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
\[
\begin{align*}
R(0) &= p, \\
R(x + 1) &= c(q, R(x)),
\end{align*}
\]
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 \( \text{Con} \), 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 2.3, 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 3.2.** 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
\[
\psi_{s(i, x)}(y) = \psi_i(x, y)
\]
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
\[
\psi_{s(k, i)}(x) = \psi_k(i, x) = \varphi_{\text{univ}}(i, x) = \varphi_i(x),
\]
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 \( i \in \mathbb{N} \).
Using Theorem 3.2, 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 $s$-$m$-$n$ 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 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 undecidable, problems.

3.2 Undecidable Problems

We saw in Section 2.3 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 any indexing of the partial computable functions.

**Theorem 3.3.** (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. \qed
Observe that the proof of Theorem 3.3 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 3.3 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 3.2.** 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 3.2, Theorem 3.3 can be restated as follows.

**Proposition 3.4.** 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 2.3 and Section 2.4, where a set of objects, the RAM programs, is encoded into a set of natural numbers, using a coding scheme.

**Definition 3.3.** 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 3.5.** 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 \( f : A \rightarrow \text{TOTAL} \), so that
\[
x \in A \text{ iff } f(x) \in \text{TOTAL}.
\]
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 \( f : K \rightarrow \text{TOTAL} \), we use the s-m-n Theorem. Let \( \theta \) be the function defined below: for all \( x, y \in \mathbb{N} \),
\[
\theta(x, y) = \begin{cases} 
\varphi_x(x) & \text{if } x \in K, \\
\text{undefined} & \text{if } x \notin K.
\end{cases}
\]
Note that \( \theta \) does not depend on \( y \). The function \( \theta \) is partial computable. Indeed, we have
\[
\theta(x, y) = \varphi_x(x) = \varphi_{\text{univ}}(x, x).
\]
Thus, \( \theta \) has some index \( j \), so that \( \theta = \varphi_j \), and by the s-m-n Theorem, we have
\[
\varphi_{s(j,1,x)}(y) = \varphi_j(x,y) = \theta(x,y).
\]
3.2. 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 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 3.6. (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

$$x \in K \text{ iff } f(x) \in P_C,$$

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 3.7.** 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.
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.

### 3.3 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 3.4.** 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 \textit{partially decidable} or \textit{semidecidable} set.

**Remark:** It should be noted that the definition of a \textit{listable set} \( (r.e \text{ set or } c.e. \text{ set}) \) given in Definition 3.4 is \textit{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 3.9 \((1) \iff (4)\).

The following proposition relates computable sets and listable sets (recursive sets and recursively enumerable sets).

**Proposition 3.8.** 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. \( \square \)

Our next goal is to show that the listable (recursively enumerable) sets can be given several equivalent definitions.

**Proposition 3.9.** 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.
3.3. LISTABLE (RECURSIVELY ENUMERABLE) SETS

Proof. The implication (1) ⇒ (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) ⇒ (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) ⇒ (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) ⇒ (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) ⇒ (4) and (4) ⇒ (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 3.9.

**Proposition 3.10.** (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 3.10 is left as an exercise. Using Proposition 3.9, 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 3.11.** 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 3.12. 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 3.8, the set \( K \) would be computable, a contradiction. \( \square \)

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 3.13. (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 3.14. 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 3.15. For every unary partial function \( f \), the following properties are equivalent:

(1) \( f \) is partial computable.

(2) The set 
\[
\{(x, f(x)) \mid x \in \text{dom}(f)\}
\]
is c.e. (r.e.).

Proof. Let \( g(x) = (x, f(x)) \). Clearly, \( g \) is partial computable, and 
\[
\text{range}(g) = \{(x, f(x)) \mid x \in \text{dom}(f)\}.
\]
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 3.9, we obtain an indexing of the c.e. sets. (r.e. sets).

**Definition 3.5.** 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.

### 3.4 Reducibility and Complete Sets

We already used the notion of reducibility in the proof of Proposition 3.5 to show that TOTAL is not computable (not recursive).

**Definition 3.6.** 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) \( f: \mathbb{N} \rightarrow \mathbb{N} \) (or \( f: \Sigma^* \rightarrow \Sigma^* \)) 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.
Proposition 3.16. Let $A, B, C$ be subsets of $\mathbb{N}$ (or $\Sigma^*$). 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 3.7. 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 3.17. 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

$$y \in W_x \text{ iff } \langle x, y \rangle \in K_0,$$

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 $z \in \mathbb{N}$,

$$z \in K_0 \text{ iff } \varphi_{\Pi_1(z)}(\Pi_2(z)) \text{ converges},$$
iff $\varphi_{f(z)}(y) = 1$ for all $y \in \mathbb{N}$. However,

$$\varphi_{f(z)}(y) = 1 \iff \varphi_{f(z)}(f(z)) = 1,$$

since $\varphi_{f(z)}$ is a constant function. This means that

$$z \in K_0 \iff f(z) \in K,$$

and $f$ is the desired function.

As a corollary of Theorem 3.17, the set $K$ is also complete.

**Definition 3.8.** 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 3.18.** We have $K_0 \leq \text{EMPTY}$.

The proof of Proposition 3.18 follows from the proof of Theorem 3.17. We also have the following proposition.

**Proposition 3.19.** 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.
3.4. REDUCIBILITY AND COMPLETE SETS

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 \( \overline{K} \leq \text{EMPTY} \). By the s-m-n Theorem, there exists a computable function \( f \) such that
\[
\varphi_{\varphi(x)}(y) = \begin{cases} 
\varphi_x(x) & \text{if } \varphi_x(x) \text{ converges}, \\
\text{undefined} & \text{if } \varphi_x(x) \text{ diverges},
\end{cases}
\]
for all \( x, y \in \mathbb{N} \). Note that for all \( x \in \mathbb{N} \),
\[
x \in \overline{K} \iff f(x) \in \text{EMPTY},
\]
and thus, \( \overline{K} \leq \text{EMPTY} \). Since \( \overline{K} \) is not c.e., \( \text{EMPTY} \) is not c.e.

By the s-m-n Theorem, there is a computable function \( g \) such that
\[
\varphi_{\varphi(x)}(y) = \min z[T(x, \Pi_1(z), \Pi_2(z))],
\]
for all \( x, y \in \mathbb{N} \). Note that
\[
x \in \text{EMPTY} \iff g(x) \in \overline{K}
\]
for all \( x \in \mathbb{N} \). Therefore, \( \text{EMPTY} \leq \overline{K} \), and since we just showed that \( \overline{K} \leq \text{EMPTY} \), the sets \( \overline{K} \) and \( \text{EMPTY} \) are equivalent. \( \square \)

**Proposition 3.20.** The following properties hold:

1. TOTAL and \( \overline{\text{TOTAL}} \) are not c.e. (not r.e.).
2. FINITE and \( \overline{\text{FINITE}} \) are not c.e (not r.e.).

Proof. Checking the proof of Theorem 3.17, we note that \( K_0 \leq \text{TOTAL} \) and \( K_0 \leq \overline{\text{FINITE}} \). Hence, we get \( \overline{K_0} \leq \text{TOTAL} \) and \( \overline{K_0} \leq \overline{\text{FINITE}} \), and neither \( \text{TOTAL} \) nor \( \text{FINITE} \) is c.e. If \( \text{TOTAL} \) was c.e., then there would be a computable function \( f \) such that \( \text{TOTAL} = \text{range}(f) \). Define \( g \) as follows:
\[
g(x) = \varphi_{\varphi(x)}(x) + 1 = \varphi_{\text{univ}}(f(x), x) + 1
\]
for all \( x \in \mathbb{N} \). Since \( f \) is total and \( \varphi_{\varphi(x)} \) is total for all \( x \in \mathbb{N} \), the function \( g \) is total computable. Let \( e \) be an index such that
\[
g = \varphi_{\varphi(e)}.
\]
Since \( g \) is total, \( g(e) \) is defined. Then, we have
\[
g(e) = \varphi_{\varphi(e)}(e) + 1 = g(e) + 1,
\]
a contradiction. Hence, \( \text{TOTAL} \) is not c.e. Finally, we show that \( \text{TOTAL} \leq \overline{\text{FINITE}} \). This also shows that \( \overline{\text{FINITE}} \) is not c.e. By the s-m-n Theorem, there is a computable function \( f \) such that
\[
\varphi_{\varphi(x)}(y) = \begin{cases} 
1 & \text{if } \forall z \leq y(\varphi_x(z) \downarrow), \\
\text{undefined} & \text{otherwise},
\end{cases}
\]
for all $x, y \in \mathbb{N}$. It is easily seen that
\[
x \in \text{TOTAL} \iff f(x) \in \text{FINITE}
\]
for all $x \in \mathbb{N}$.

From Proposition 3.20, 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 3.21.** 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 $x \in \mathbb{N}$.

We now turn to the recursion Theorem.

### 3.5 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 3.22.** (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

\[
\varphi_n(y) = \varphi_{g(m)}(y) = \theta(m, y) = \varphi_{\text{univ}}(\varphi_{\text{univ}}(m, m), y) = \varphi_{\varphi_{\text{univ}}(m, m)}(y)
= \varphi_{\varphi_m}(y) = \varphi_{f \circ g}(y) = \varphi_{f(g(m))}(y) = \varphi_f(n)(y),
\]

for all \( y \in \mathbb{N} \). Therefore, \( \varphi_n = \varphi_{f(n)} \), as desired. \( \square \)

The recursion Theorem can be strengthened as follows.

**Theorem 3.23.** (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 3.22 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. \( \square \)

A third version of the recursion Theorem is given below.

**Theorem 3.24.** (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

\[
\varphi_{c(i,j)}(x, x_1, \ldots, x_n) = \varphi_i(\varphi_{j}(x, x_1, \ldots, x_n), x_1, \ldots, x_n)
\]

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

\[
\varphi_{h(x,x_1,\ldots,x_n)} = \varphi_{g(c(x,i),x_1,\ldots,x_n)} = \varphi_{\varphi_{c(i)}(c(x,i),x_1,\ldots,x_n)},
\]

and

\[
\varphi_{\varphi_{c(i)}(c(x,i),x_1,\ldots,x_n)} = \varphi_{\varphi_x(c(x,i),x_1,\ldots,x_n),x_1,\ldots,x_n)} = \varphi_{\varphi_x(g(c(x,i),x_1,\ldots,x_n),x_1,\ldots,x_n)} = \varphi_{\varphi_x(h(x,x_1,\ldots,x_n),x_1,\ldots,x_n)}.
\]

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 3.22, 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 \(\overline{P_C} \neq \mathbb{N}\), 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 3.22, there is some \( n \) such that
\[
\varphi_{f(n)} = \varphi_n.
\]
But then, we have
\[
n \in P_C \quad \text{iff} \quad f(n) \notin P_C
\]
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 3.25.** 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
\[
x \in A \quad \text{iff} \quad f(x) \in \overline{A}
\]
for all \( x \in \mathbb{N} \). By the recursion Theorem, there is some \( n \) such that
\[
\varphi_{f(n)} = \varphi_n.
\]
But then,
\[
\varphi_n \in C \quad \text{iff} \quad n \in A \quad \text{iff} \quad f(n) \in \overline{A} \quad \text{iff} \quad \varphi_{f(n)} \in \overline{C},
\]
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:

$$
g(n, 0, y) = y + 1, \\
g(n, x + 1, 0) = \varphi_{\text{univ}}(n, x, 1), \\
g(n, x + 1, y + 1) = \varphi_{\text{univ}}(n, x, \varphi_{\text{univ}}(n, x + 1, y)).
$$

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.

### 3.6 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 3.26.** 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 3.27. 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 3.27 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:

\[
\psi(z) = \begin{cases} 
\Pi_1(z) & \text{if } P_{f(z)} \subseteq \varphi_{z}, \\
\text{undefined} & \text{otherwise}.
\end{cases}
\]

It is clear that

\[
P_C = \text{range}(\psi).
\]

To see that \( \psi \) is partial computable, write \( \psi(z) \) as follows:

\[
\psi(z) = \begin{cases} 
\Pi_1(z) & \text{if } \forall w \leq \Pi_1(f(z))[F(f(z),w) > 0 \\
\varphi_{z}(w) = F(f(z),w) - 1, & \text{undefined otherwise}.
\end{cases}
\]

To establish the converse of Proposition 3.27, we need two propositions.

Proposition 3.28. 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,

\[
x \in K \iff g(x) \in P_C
\]

for all \( x \in \mathbb{N} \), that is, \( K \leq P_C \). Since \( P_C \) is c.e., \( K \) would also be c.e., a contradiction. 

As a corollary of Proposition 3.28, we note that TOTAL is not c.e.
Proposition 3.29. 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

\[
\varphi_{h(x)}(y) = \begin{cases} 
\psi(y) & \text{if } x \in K, \\
\varphi(y) & \text{if } x \notin K,
\end{cases}
\]

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

\[
\theta(x, y) = \begin{cases} 
\psi(y) & \text{if } x \in K, \\
\varphi(y) & \text{if } x \notin K,
\end{cases}
\]

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 \( x, y \in \mathbb{N} \). \( \square \)

Observe that Proposition 3.29 yields a new proof that \( \text{TOTAL} \) is not c.e. (not r.e.). Finally, we can prove the extended Rice Theorem.

Theorem 3.30. (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

\[
\varphi_x \in C \iff \exists y \in A (P_y \subseteq \varphi_x).
\]
3.7. 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 3.28 and Proposition 3.29, 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 3.28, 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 3.29, since \( \varphi_x \) extends \( P_y \), we get
\[
\varphi_x \in C.
\]

3.7 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
\[
W_x \subseteq \overline{K}
\]
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.
Definition 3.9. 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 3.31. 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 3.32.** 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 3.24), 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, $\overline{K} \leq A$. 

Using Proposition 3.32, the following results can be shown.

**Proposition 3.33.** 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 4

The Lambda-Calculus

The original motivation of Alonzo Church for inventing the λ-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 λ-calculus as a formalism for defining the notion of computability (1932,1933,1935). The λ-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 λ-calculus, showing that the λ-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 λ-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 λ-calculus. In fact, it is also true that all the partial computable functions (partial recursive functions) are definable in the λ-calculus but this requires more care.

Since the λ-calculus does not have any notion of tape, register, or any other means of storing data, it quite amazing that the λ-calculus has so much computing power.

The λ-calculus is based on three concepts:

(1) Application.

(2) Abstraction (also called λ-abstraction).

(3) β-reduction (and β-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.\(^1\) 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,
\[
(\lambda x. M)N \xrightarrow{\beta} M\left[x := N\right],
\]
where \( M\left[x := N\right] \) 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 \(\text{OCaml, ML, Miranda and Haskell} \), 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.
4.1 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 4.1.** 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 4.1 and the raw simply-typed \( \lambda \)-terms of Definition ?? 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 4.5).

**Definition 4.2.** 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 4.3.** 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 4.3 is illustrated in Figure 4.1.

![Figure 4.1: 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
   \[\lambda x_1\cdots x_n. M.\]
4.1. SYNTAX OF THE LAMBDA-CALCULUS

Matching parentheses may be dropped or added for convenience. Here are some examples
of \( \lambda \)-terms (and their abbreviation):

\[
\begin{array}{ll}
y & \lambda x. yx \\
(yx) & (\lambda x. (yx))z \\
\lambda x. (yx) & ((\lambda x. (yx))z)w \\
\end{array}
\]

Note that \( \lambda x. yx \) is an abbreviation for \( (\lambda x. (yx)) \), not \( ((\lambda x. y)x) \).
The variables occurring in a \( \lambda \)-term are free of bound.

**Definition 4.4.** For any \( \lambda \)-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 \( M = (M_1 M_2) \), 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 \( \lambda \)-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 4.3. 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 4.2 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 4.5.** 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:
4.1. 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 4.6.** The binary relation $\rightarrow_{\alpha}$ on $\lambda$-terms called immediate $\alpha$-conversion is the smallest relation satisfying the following properties: for all $\lambda$-terms $M, N, P, Q$:

$$\lambda x. M \rightarrow_{\alpha} \lambda y. M[x := y], \quad \text{for all } y \notin FV(M) \cup BV(M)$$

if $M \rightarrow_{\alpha} N$ then $MQ \rightarrow_{\alpha} NQ$ and $PM \rightarrow_{\alpha} PN$

if $M \rightarrow_{\alpha} N$ then $\lambda x. M \rightarrow_{\alpha} \lambda x. N$.

The least equivalence relation $\equiv_{\alpha} = (\rightarrow_{\alpha} \cup \rightarrow_{\alpha}^{-1})^*$ containing $\rightarrow_{\alpha}$ (the reflexive and transitive closure of $\rightarrow_{\alpha} \cup \rightarrow_{\alpha}^{-1}$) is called $\alpha$-conversion. Here $\rightarrow_{\alpha}^{-1}$ denotes the converse of the relation $\rightarrow_{\alpha}$, that is, $M \rightarrow_{\alpha}^{-1} N$ iff $N \rightarrow_{\alpha} M$.

For example,

$$\lambda f.x. f(f(x)) = \lambda f. \lambda x. f(f(x)) \rightarrow_{\alpha} \lambda f. \lambda y. f(f(y)) \rightarrow_{\alpha} \lambda g. \lambda y. g(g(y)) = \lambda g.y. g(g(y)).$$

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,

$$(\lambda xyz.(xy)z)(yz) \equiv_{\alpha} (\lambda xuv.(xu)v)(yz) \rightarrow_{\beta} (\lambda uv.(xu)v)[x := yz] = \lambda uv.((yz)uv).$$

---

2We told you that Church was fond of Greek letters.
CHAPTER 4. THE LAMBDA-CALCULUS

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.

4.2 $\beta$-Reduction and $\beta$-Conversion; the Church–Rosser Theorem

The computational engine of the $\lambda$-calculus is $\beta$-reduction.

**Definition 4.7.** The relation $\to_\beta$, called immediate $\beta$-reduction, is the smallest relation satisfying the following properties for all $\lambda$-terms $M, N, P, Q$:

$$(\lambda x. M)N \to_\beta M[x := N], \quad \text{where } M \text{ is safe for } [x := N]$$

if $M \to_\beta N$ then $MQ \to_\beta NQ$ and $PM \to_\beta PN$

if $M \to_\beta N$ then $\lambda x. M \to_\beta \lambda x. N$.

The transitive closure of $\to_\beta$ is denoted by $\pm_\beta$, the reflexive and transitive closure of $\to_\beta$ is denoted by $\ast_\beta$, and we define $\beta$-conversion, denoted by $\leftrightarrow_\beta$, as the smallest equivalence relation $\leftrightarrow_\beta = (\to_\beta \cup \to_\beta^{-1})^\ast$ containing $\to_\beta$. 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 $M \to_\beta N$, equivalently if $M$ contains no $\beta$-redex.

For example,

$$(\lambda xy. x)uv = ((\lambda x. (\lambda y. x)u)v \to_\beta ((\lambda y. x)[x := u])v = (\lambda y. u)v \to_\beta u[y := v] = u$$

and

$$(\lambda xy. y)uv = ((\lambda x. (\lambda y. y)u)v \to_\beta ((\lambda y. y)[x := u])v = (\lambda y. y)v \to_\beta y[y := v] = v.$$  

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

$$\Omega = \omega \omega = (\lambda x. (xx))(\lambda x. (xx)) \to_\beta (xx)[x := \lambda x. (xx)] = \omega \omega = \Omega.$$  

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 β-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 λ-term contains many different β-redex. One then might wonder if there is any sort of relationship between any two terms \(M_1\) and \(M_2\) arising through two β-reduction sequences \(M \xrightarrow{+\beta} M_1\) and \(M \xrightarrow{+\beta} M_2\) starting with the same term \(M\). The answer is given by the following famous theorem.

**Theorem 4.1.** (Church–Rosser Theorem) The following two properties hold:

1. The λ-calculus is **confluent**: for any three λ-terms \(M, M_1, M_2\), if \(M \xrightarrow{+\beta} M_1\) and \(M \xrightarrow{+\beta} M_2\), then there is some λ-term \(M_3\) such that \(M_1 \xrightarrow{+\beta} M_3\) and \(M_2 \xrightarrow{+\beta} M_3\). See Figure 4.3.

![Figure 4.3: The confluence property](image)

2. The λ-calculus has the **Church–Rosser property**: for any two λ-terms \(M_1, M_2\), if \(M_1 \xleftrightarrow{+\beta} M_2\), then there is some λ-term \(M_3\) such that \(M_1 \xrightarrow{+\beta} M_3\) and \(M_2 \xrightarrow{+\beta} M_3\). See Figure 4.4.

Furthermore (1) and (2) are equivalent, and if a λ-term \(M\) β-reduces to a β-normal form \(N\), then \(N\) is unique (up to α-conversion).

**Proof.** I am not aware of any easy proof of Part (1) or Part (2) of Theorem 4.1, but the equivalence of (1) and (2) is easily shown by induction.
Given

\[
M_1 \xrightarrow{\ast} \quad M_2
\]

\[
M_1 \xrightarrow{\ast} M_2
\]

\[
\ast
\]

\[
M_3
\]

\[
\text{Church-Rosser}
\]

Figure 4.4: The Church–Rosser property.

Assume that (2) holds. Since \(\rightarrow_\beta^*\) is contained in \(\leftarrow_\beta^*\), if \(M \rightarrow_\beta^* M_1\) and \(M \rightarrow_\beta^* M_2\), then \(M_1 \leftarrow_\beta M_2\), and since (2) holds, then there is some \(\lambda\)-term \(M_3\) such that \(M_1 \rightarrow_\beta^* M_3\) and \(M_2 \rightarrow_\beta^* M_3\), which is (1).

To prove that (1) implies (2) we need the following observation.

Since \(\leftarrow_\beta^* = (\rightarrow_\beta \cup \rightarrow_\beta^{-1})^*\), we see immediately that \(M_1 \leftarrow_\beta M_2\) iff either

(a) \(M_1 = M_2\), or

(b) there is some \(M_3\) such that \(M_1 \rightarrow_\beta M_3\) and \(M_3 \leftarrow_\beta M_2\), or

(c) there is some \(M_3\) such that \(M_3 \rightarrow_\beta M_1\) and \(M_3 \leftarrow_\beta M_2\).

Assume (1). We proceed by induction on the number of steps in \(M_1 \leftarrow_\beta M_2\). If \(M_1 \leftarrow_\beta^* M_2\), 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 \(M_3 \leftarrow_\beta M_2\). Since \(M_3 \leftarrow_\beta^* M_2\) contains one less step than \(M_1 \leftarrow_\beta M_2\), by the induction hypothesis there is some \(M_4\) such that \(M_3 \rightarrow_\beta^* M_4\) and \(M_2 \rightarrow_\beta^* M_4\), and then \(M_1 \rightarrow_\beta M_3 \rightarrow_\beta M_4\) and \(M_2 \rightarrow_\beta M_4\), proving (2). See Figure 4.5.

**Case c.** There is some \(M_3\) such that \(M_3 \rightarrow_\beta M_1\) and \(M_3 \leftarrow_\beta M_2\). Since \(M_3 \leftarrow_\beta^* M_2\) contains one less step than \(M_1 \leftarrow_\beta M_2\), by the induction hypothesis there is some \(M_4\) such that \(M_3 \rightarrow_\beta^* M_4\) and \(M_2 \rightarrow_\beta^* M_4\). Now \(M_3 \rightarrow_\beta M_1\) and \(M_3 \rightarrow_\beta M_4\), so by (1) there is some \(M_5\) such that \(M_1 \rightarrow_\beta M_5\) and \(M_4 \rightarrow_\beta M_5\). Putting derivations together we get \(M_1 \rightarrow_\beta^* M_5\) and \(M_2 \rightarrow_\beta^* M_4 \rightarrow_\beta^* M_5\), which proves (2). See Figure 4.6.
4.2. \(\beta\)-REDUCTION AND \(\beta\)-CONVERSION; THE CHURCH–ROSSER THEOREM

Suppose \(M \xrightarrow{\ast} \beta N_1\) and \(M \xrightarrow{\ast} \beta N_2\) where \(N_1\) and \(N_2\) are both \(\beta\)-normal forms. Then by confluence there is some \(N\) such that \(N_1 \xrightarrow{\ast} \beta N\) and \(N_2 \xrightarrow{\ast} \beta N\). 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 \(M \xleftarrow{\ast} \beta N\) and if \(N\) is a \(\beta\)-normal form, then in fact \(M \xrightarrow{\ast} \beta N\). We leave this fact as an exercise.

This fact will be useful in showing that the recursive functions are computable in the \(\lambda\)-calculus.
4.3 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 4.2.** If \( I, K, K_\ast, \) and \( S \) are the combinators defined by

\[
I = \lambda x. x
\]

\[
K = \lambda xy. x
\]

\[
K_\ast = \lambda xy. y
\]

\[
S = \lambda xyz. (xz)(yz),
\]

then...
4.3. SOME USEFUL COMBINATORS

then for all $\lambda$-terms $M, N, P$, we have

\[
\begin{align*}
IM & \rightarrow_{\beta} M \\
KMN & \rightarrow_{\beta} M \\
K_{\ast}MN & \rightarrow_{\beta} N \\
SMNP & \rightarrow_{\beta} (MP)(NP) \\
KI & \rightarrow_{\beta} K_{\ast} \\
SKK & \rightarrow_{\beta} I.
\end{align*}
\]

The proof is left as an easy exercise. For example,

\[
SMNP = (\lambda xyz. (xz)(yz))MNP \rightarrow_{\beta} ((\lambda z. (Mz)(yz))[x := M])NP
\]

\[
= (\lambda z. (Mz)(yz))NP \\
\rightarrow_{\beta} ((\lambda z. (Mz)(yz))[y := N])P \\
= (\lambda z. (Mz)(Nz))P \\
\rightarrow_{\beta} ((Mz)(Nz))[z := P] = (MP)(NP).
\]

The need for a conditional construct if then else such that if $T$ then $P$ else $Q$ yields $P$ and if $F$ then $P$ else $Q$ yields $Q$ is indispensable to write nontrivial programs. There is a trick to encode the boolean values $T$ and $F$ in the $\lambda$-calculus to mimic the above behavior of if $B$ then $P$ else $Q$, provided that $B$ is a truth value. Since everything in the $\lambda$-calculus is a function, the booleans values $T$ and $F$ are encoded as $\lambda$-terms. At first, this seems quite odd, but what counts is the behavior of if $B$ then $P$ else $Q$, and it works!

The truth values $T, F$ and the conditional construct if $B$ then $P$ else $Q$ can be encoded in the $\lambda$-calculus as follows.

**Proposition 4.3.** Consider the combinators given by $T = K, F = K_{\ast},$ and 

\[
\text{if then else } = \lambda bxy.bxy.
\]

Then for all $\lambda$-terms we have

\[
\begin{align*}
\text{if } T \text{ then } P \text{ else } Q & \rightarrow_{\beta} P \\
\text{if } F \text{ then } P \text{ else } Q & \rightarrow_{\beta} Q.
\end{align*}
\]

The proof is left as an easy exercise. For example,

\[
\begin{align*}
\text{if } T \text{ then } P \text{ else } Q = (\text{if then else})TPQ \\
& = (\lambda bxy. bxy)TPQ \\
& \rightarrow_{\beta} ((\lambda bxy. bxy)[b := T])PQ = (\lambda yx. Txy)PQ \\
& \rightarrow_{\beta} ((\lambda yx. Txy)[x := P])Q = (\lambda y. TPy)Q \\
& \rightarrow_{\beta} (TPy)[y := Q] = TPQ \\
& = KPQ \rightarrow_{\beta} P,
\end{align*}
\]
by Proposition 4.2.

The boolean operations $\land, \lor, \neg$ can be defined in terms of if then else. For example,

$$\text{And } b_1 b_2 = \text{if } b_1 \text{ then } (\text{if } b_2 \text{ then } T \text{ else } F) \text{ else } F.$$

**Remark:** If $B$ is a term different from $T$ or $F$, then if $B$ then $P$ 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 4.4.** 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

$$\langle M, N \rangle = \lambda z. z MN = \lambda z. \text{if } z \text{ then } M \text{ else } N$$

$$\pi_1 = \lambda z. z K$$

$$\pi_2 = \lambda z. z K_\ast.$$

Then

$$\pi_1 (M, N) \xrightarrow{+}^\beta M$$

$$\pi_2 (M, N) \xrightarrow{+}^\beta N$$

$$\langle M, N \rangle T \xrightarrow{+}^\beta M$$

$$\langle M, N \rangle F \xrightarrow{+}^\beta N.$$

The proof is left as an easy exercise. For example,

$$\pi_1 (M, N) = (\lambda z. z K)(\lambda z. z MN)$$

$$\xrightarrow{+}^\beta (z K)[z := \lambda z. z MN] = (\lambda z. z MN)K$$

$$\xrightarrow{+}^\beta (z MN)[z := K] = KMN \xrightarrow{+}^\beta M,$$

by Proposition 4.2.

In the next section we show how to encode the natural numbers in the $\lambda$-calculus and how to compute various arithmetical functions.

### 4.4 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 \( \lambda \)-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 4.8.** (Church Numerals) The *Church numerals* \( c_0, c_1, c_2, \ldots \) are defined by

\[
c_n = \lambda fx. f^n(x).
\]

So \( c_0 = \lambda fx. x = K_x \), \( c_1 = \lambda fx. fx \), \( c_2 = \lambda fx. f(fx) \), etc. The Church numerals are \( \beta \)-normal forms.

Observe that

\[
c_n F z = (\lambda fx. f^n(x))Fz \xrightarrow{+} \beta F^n(z).
\]

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 4.9.** The *iteration combinator* \( \text{Iter} \) is given by

\[
\text{Iter} = \lambda nfx. nfx.
\]

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

\[
\text{Succ}_c c_n = (\lambda nx. f(nfx))c_n \\
\xrightarrow{+} \beta (\lambda fx. f(nfx))[n := c_n] = \lambda f x. f(c_nfx) \\
\xrightarrow{+} \beta \lambda fx. f(f^n(x)) \\
= \lambda f x. f^{n+1}(x) = c_{n+1}.
\]
The function IsZero which tests whether a natural number is equal to 0 is defined by the combinator
\[
\text{IsZero}_c = \lambda x. x(KF)T.
\]
The proof that it works is left as an exercise.
Addition and multiplication are a little more tricky to define.

**Proposition 4.5.** (J.B. Rosser) Define Add and Mult as the combinators given by
\[
\text{Add} = \lambda mnfx. mf(nfx) \\
\text{Mult} = \lambda xyz. x(yz).
\]
We have
\[
\text{Add } c_m c_n \xrightarrow{+} \beta c_{m+n} \\
\text{Mult } c_m c_n \xrightarrow{+} \beta c_{m*n}
\]
for all \(m, n \in \mathbb{N}\).

**Proof.** We have
\[
\text{Add } c_m c_n = (\lambda mnfx. mf(nfx))c_m c_n \\
\xrightarrow{+} \beta (\lambda fx. c_m f(c_n f x)) \\
\xrightarrow{+} \beta \lambda fx. f^m(f^n(x)) \\
= \lambda fx. f^{m+n}(x) = c_{m+n}.
\]

For multiplication we need to prove by induction on \(m\) that
\[
(c_n x)^m(y) \xrightarrow{\star} \beta x^{m*n}(y). \tag{*}
\]
If \(m = 0\) then both sides are equal to \(y\).
For the induction step we have
\[
(c_n x)^{m+1}(y) = c_n x((c_n x)^m(y)) \\
\xrightarrow{\star} \beta c_n x(x^{m*n}(y)) \quad \text{by induction} \\
\xrightarrow{\star} \beta x^n(x^{m*n}(y)) \\
= x^{n+m*n}(y) = x^{(m+1)*n}(y).
\]
We now have
\[
\text{Mult } c_m c_n = (\lambda xyz. x(yz))c_m c_n \\
\xrightarrow{+} \beta \lambda z. (c_m(c_n z)) \\
= \lambda z. ((\lambda fy. f^m(y))(c_n z)) \\
\xrightarrow{+} \beta \lambda zy. (c_n z)^m(y),
\]
and since we proved in (*) that
\[(c_n z)^m(y) \rightarrow^\beta z^{m+n}(y),\]
we get
\[\text{Mult } c_m c_n \rightarrow^\beta \lambda z y. (c_n z)^m(y) \rightarrow^\beta \lambda z y. z^{m+n}(y) = c_{m+n},\]
which completes the proof.

As an exercise the reader should prove that addition and multiplication can also be defined in terms of \textit{Iter} (see Definition 4.9) by
\[
\text{Add} = \lambda m n. \text{Iter } m \text{ Succ}_e n
\]
\[
\text{Mult} = \lambda m n. \text{Iter } m (\text{Add } n) c_0.
\]
The above expressions are close matches to the primitive recursive definitions of addition and multiplication. To check that they work, prove that
\[
\text{Add } c_m c_n \rightarrow^\beta (\text{Succ}_e)^m(c_n) \rightarrow^\beta c_{m+n}
\]
and
\[
\text{Mult } c_m c_n \rightarrow^\beta (\text{Add } n)^m(c_0) \rightarrow^\beta c_{m+n}.
\]

A version of the exponential function can also be defined. A function that plays an important technical role is the predecessor function \textit{Pred} defined such that
\[
\text{Pred}(0) = 0
\]
\[
\text{Pred}(n + 1) = n.
\]

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
\[
\text{Pred}_K = \lambda n. \pi_2(\text{Iter } n \lambda z. \langle \text{Succ}_e(\pi_1 z), \pi_1 z \rangle \langle c_0, c_0 \rangle).
\]
The reason this works is that we can prove that
\[
(\lambda z. \langle \text{Succ}_e(\pi_1 z), \pi_1 z \rangle)^0 \langle c_0, c_0 \rangle \rightarrow^\beta \langle c_0, c_0 \rangle,
\]
and by induction that
\[
(\lambda z. \langle \text{Succ}_e(\pi_1 z), \pi_1 z \rangle)^{n+1} \langle c_0, c_0 \rangle \rightarrow^\beta \langle c_{n+1}, c_n \rangle.
\]
For the base case \(n = 0\) we get
\[
(\lambda z. \langle \text{Succ}_e(\pi_1 z), \pi_1 z \rangle) \langle c_0, c_0 \rangle \rightarrow^\beta \langle c_1, c_0 \rangle.
\]
For the induction step we have

\[(\lambda z. \langle \text{Succ}_c(\pi_1 z), \pi_1 z \rangle)^{n+2}(c_0, c_0) =
(\lambda z. \langle \text{Succ}_c(\pi_1 z), \pi_1 z \rangle)((\lambda z. \langle \text{Succ}_c(\pi_1 z), \pi_1 z \rangle)^{n+1}(c_0, c_0))
\]

\[\vdash \beta (\lambda z. \langle \text{Succ}_c(\pi_1 z), \pi_1 z \rangle)(c_{n+1}, c_n) \rightharpoonup \beta (c_{n+2}, c_{n+1}).\]

Here is another tricky solution due to J. Velmans (according to H. Barendregt):

\[\text{Pred}_c = \lambda xyz. x(\lambda pq. q(py))(Kz)I.\]

We leave it to the reader to verify that it works.

The ability to construct pairs together with the Iter combinators allows the definition of a large class of functions, because 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

\[h = \lambda xn. \text{Mult} \text{Succ}_c n x\]

and then

\[\text{fact} = \lambda n. \pi_1(\text{Iter} n \lambda z. \langle h(\pi_1 z)(\pi_2 z), \text{Succ}_c(\pi_2 z) \rangle (c_1, c_0)).\]

The above term works because

\[(\lambda z. \langle h(\pi_1 z)(\pi_2 z), \text{Succ}_c(\pi_2 z) \rangle)^0(c_1, c_0) \rightharpoonup \beta (c_1, c_0) = (c_{0!}, c_0),\]

and

\[(\lambda z. \langle h(\pi_1 z)(\pi_2 z), \text{Succ}_c(\pi_2 z) \rangle)^{n+1}(c_1, c_0) \rightharpoonup \beta (c_{(n+1)!}, c_{n+1}) = (c_{(n+1)!}, c_{n+1}).\]

We leave the details as an exercise.

Barendregt came up with another way of representing the natural numbers that makes things easier.

**Definition 4.10. (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 \(\ulcorner n \urcorner\) 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 4.6. The functions Succ, Pred and IsZero are defined in terms of the Barendregt numerals by the combinators

\[
\text{Succ}_b = \lambda x. (F, x)
\]
\[
\text{Pred}_b = \lambda x. (xF)
\]
\[
\text{IsZero}_b = \lambda x. (xT),
\]

and we have

\[
\text{Succ}_b b_n \xrightarrow{\beta} b_{n+1}
\]
\[
\text{Pred}_b b_0 \xrightarrow{\beta} b_0
\]
\[
\text{Pred}_b b_{n+1} \xrightarrow{\beta} b_n
\]
\[
\text{IsZero}_b b_0 \xrightarrow{\beta} T
\]
\[
\text{IsZero}_b b_{n+1} \xrightarrow{\beta} F.
\]

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 4.7. The combinator \( T \) given by

\[
T = \lambda x. (x\text{Succ}_b)b_0
\]

has the property that

\[
T c_n \xrightarrow{\beta} b_n \quad \text{for all } n \in \mathbb{N}.
\]

Proof. We proceed by induction on \( n \). For the base case

\[
T c_0 = (\lambda x. (x\text{Succ}_b)b_0)c_0
\]
\[
\xrightarrow{\beta} c_0(\text{Succ}_b)b_0
\]
\[
\xrightarrow{\beta} b_0.
\]

For the induction step,

\[
T c_n = (\lambda x. (x\text{Succ}_b)b_0)c_n
\]
\[
\xrightarrow{\beta} (c_n\text{Succ}_b)b_0
\]
\[
\xrightarrow{\beta} \text{Succ}_b^n(b_0).
\]

Thus we need to prove that

\[
\text{Succ}_b^n(b_0) \xrightarrow{\beta} b_n. \quad (\ast)
\]
For the base case $n = 0$, the left-hand side reduces to $b_0$.

For the induction step, we have

\[
\begin{align*}
\text{Succ}_b^{n+1}(b_0) &= \text{Succ}_b(\text{Succ}_b^n(b_0)) \\
&\xrightarrow{\beta} \text{Succ}_b(b_n) \quad \text{by induction} \\
&\xrightarrow{\beta} b_{n+1},
\end{align*}
\]

which concludes the proof. $\square$

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.

## 4.5 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 4.8. (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

\[
F(YF) \xrightarrow{\beta} YF.
\]

**Proof.** Write $W = \lambda x. F(xx)$. We have

\[
F(YF) = F\left( (\lambda f. (\lambda x. f(xx))(\lambda x. f(xx)))F \right) \xrightarrow{\beta} F( (\lambda x. F(xx))(\lambda x. F(xx))) = F(WW),
\]

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 $F(YF) \xrightarrow{\beta} YF$, as claimed. $\square$

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 4.9. (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. \qed

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
$$
GX \xrightarrow{\beta} X(XG) \quad \text{for all } X.
$$
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 4.9 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

\[ F = \lambda g. n. \text{if } \text{IsZero}_c n \text{ then } c_1 \text{ else } \text{Mult} n g(\text{Pred}_c n). \]

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

\[ F = \lambda g. n. \text{if } \text{IsZero}_c n \text{ then } c_1 \text{ else } \text{Mult} n g(\text{Succ}_c n) \]

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.

4.6 \( \lambda \)-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 4.11.** The base functions are the functions \( Z, S, P^*_n \) 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 $P^n_i$ such that

$$P^n_i(x_1, \ldots, x_n) = x_i, \quad x_1, \ldots, x_n \in \mathbb{N}.$$ 

Next comes (extended) composition.

**Definition 4.12.** Given any partial or total function $g: \mathbb{N}^m \to \mathbb{N}$ $(m \geq 1)$ and any $m$ partial or total functions $h_i: \mathbb{N}^n \to \mathbb{N}$ $(n \geq 1)$, 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 $f: \mathbb{N}^n \to \mathbb{N}$ 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 4.13.** Given any partial or total functions $g: \mathbb{N}^m \to \mathbb{N}$ and $h: \mathbb{N}^{m+2} \to \mathbb{N}$ $(m \geq 1)$, the partial or total function function $f: \mathbb{N}^{m+1} \to \mathbb{N}$ is defined by primitive recursion from $g$ and $h$ if $f$ is given by:

$$f(0, x_1, \ldots, x_m) = g(x_1, \ldots, x_m)$$

$$f(n + 1, x_1, \ldots, x_m) = h(f(n, x_1, \ldots, x_m), n, x_1, \ldots, x_m)$$

for all $n, x_1, \ldots, x_m \in \mathbb{N}$. If $m = 0$, then $g$ is some fixed natural number and we have

$$f(0) = g$$

$$f(n + 1) = h(f(n), n).$$

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

$$f(n + 1, x_1, \ldots, x_m) = h(f(n, x_1, \ldots, x_m), n, x_1, \ldots, x_m)$$

(*)

but in an earlier definition it was

$$f(n + 1, x_1, \ldots, x_m) = h(n, f(n, x_1, \ldots, x_m), x_1, \ldots, x_m),$$

(∗2)

with the first two arguments of $h$ permuted. Since

$$h \circ (P_2^{m+2}, P_1^{m+2}, P_3^{m+2}, \ldots, P_{m+2}^{m+2})(n, f(n, x_1, \ldots, x_m), x_1, \ldots, x_m) = h(f(n, x_1, \ldots, x_m), n, x_1, \ldots, x_m)$$
and
\[ h \circ (P^{m+2}_2, P^{m+2}_1, P^{m+2}_3, \ldots, P^{m+2}_{m+2})(f(n, x_1, \ldots, x_m), n, x_1, \ldots, x_m) = h(n, f(n, x_1, \ldots, x_m), x_1, \ldots, x_m), \]
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 4.14.** 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 4.15.** (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.
(3) Minimization.
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 4.16. 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

\[
Fc_{m_1} \cdots c_{m_n} \xrightarrow{\beta} c_{f(m_1, \ldots, m_n)}.
\]

In view of the Church–Rosser theorem (Theorem 4.1) and the fact that \( c_{f(m_1, \ldots, m_n)} \) is a \( \beta \)-normal form, we can replace

\[
Fc_{m_1} \cdots c_{m_n} \xrightarrow{\beta} c_{f(m_1, \ldots, m_n)}
\]

by

\[
Fc_{m_1} \cdots c_{m_n} \xrightarrow{\beta} Fc_{m_1} \cdots c_{m_n}.
\]

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 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 4.7.

We have the following remarkable theorems.

Theorem 4.10. 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 4.10 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 4.11. (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. The base functions are \( \lambda \)-definable.
We already showed that $Z_c$ computes $Z$ and that $\text{Succ}_c$ computes $S$. Observe that $U^n_i$ given by
\[ U^n_i = \lambda x_1 \cdots x_i \]
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 $\text{Iter}$ 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
\[ F = \lambda n x_1 \cdots x_m. \pi_1(\text{Iter} n \lambda z. \langle H \pi_1 z \pi_2 z x_1 \cdots x_m, \text{Succ}_c(\pi_2 z) \rangle \langle G x_1 \cdots x_m, c_0 \rangle). \]

The reason $F$ works is that we can prove by induction that
\[ (\lambda z. \langle H \pi_1 z \pi_2 z c_{n_1} \cdots c_{n_m}, \text{Succ}_c(\pi_2 z) \rangle)^n \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle \xrightarrow{+\beta} \langle c_{f(n,n_1,\ldots,n_m)}, c_n \rangle. \]

For the base case $n = 0$,
\[ (\lambda z. \langle H \pi_1 z \pi_2 z c_{n_1} \cdots c_{n_m}, \text{Succ}_c(\pi_2 z) \rangle)^0 \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle \xrightarrow{+\beta} \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle = \langle c_{g(0,n_1,\ldots,n_m)}, c_0 \rangle = \langle c_{f(0,n_1,\ldots,n_m)}, c_0 \rangle. \]

For the induction step,
\[ (\lambda z. \langle H \pi_1 z \pi_2 z c_{n_1} \cdots c_{n_m}, \text{Succ}_c(\pi_2 z) \rangle)^{n+1} \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle \]
\[ = (\lambda z. \langle H \pi_1 z \pi_2 z c_{n_1} \cdots c_{n_m}, \text{Succ}_c(\pi_2 z) \rangle) \]
\[ (\lambda z. \langle H \pi_1 z \pi_2 z c_{n_1} \cdots c_{n_m}, \text{Succ}_c(\pi_2 z) \rangle)^n \langle G c_{n_1} \cdots c_{n_m}, c_0 \rangle) \xrightarrow{+\beta} \langle \lambda z. \langle H \pi_1 z \pi_2 z c_{n_1} \cdots c_{n_m}, \text{Succ}_c(\pi_2 z) \rangle \rangle \langle c_{f(n,n_1,\ldots,n_m)}, c_n \rangle \]
\[ \xrightarrow{+\beta} \langle H c_{f(n,n_1,\ldots,n_m)} c_n c_{n_1} \cdots c_{n_m}, \text{Succ}_c c_n \rangle \]
\[ \xrightarrow{+\beta} \langle c_{h(f(n,n_1,\ldots,n_m),n_1,\ldots,n_m)}, c_{n+1} \rangle = \langle c_{f(n+1,n_1,\ldots,n_m)}, c_{n+1} \rangle. \]

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
\[ J = \lambda f x_1 \cdots x_m. \text{if IsZero}_c x \text{ then } G x_1 \cdots x_m \text{ else } H(f(\text{Pred}_c x) x_1 \cdots x_m)(\text{Pred}_c x) x_1 \cdots x_m, \]

\[ F = \lambda n x_1 \cdots x_m. \pi_1(\text{Iter} n \lambda z. \langle H \pi_1 z \pi_2 z x_1 \cdots x_m, \text{Succ}_c(\pi_2 z) \rangle \langle G x_1 \cdots x_m, c_0 \rangle). \]
4.6. \( \lambda \)-DEFINABILITY OF THE COMPUTABLE FUNCTIONS

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.


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

\[
F c_n c_{n_1} \cdots c_{n_m} \rightarrow^\beta \begin{cases} c_n & \text{if } g(n, n_1, \ldots, n_m) = 0 \\ F c_{n+1} c_{n_1} \cdots c_{n_m} & \text{otherwise,} \end{cases}
\]

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 \( f : \mathbb{N}^m \rightarrow \mathbb{N} \) is computable as

\[
f = g \circ \mu h,
\]

for some primitive recursive functions \( g : \mathbb{N} \rightarrow \mathbb{N} \) and \( h : \mathbb{N}^{m+1} \rightarrow \mathbb{N} \). 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 4.10 and Theorem 4.11 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 4.12. (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 4.12 is proven in Barendregt [3] (Chapter 6, Theorem 6.6.2) and Barendregt [4].

As a corollary of Theorem 4.12 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.

4.7 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 ??, 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 \( \text{Nat}_\sigma = (\sigma \to \sigma) \to (\sigma \to \sigma) \), by

\[
    c_n = \lambda f : (\sigma \to \sigma). \lambda x : \sigma. f^n(x).
\]

The notion of \( \lambda \)-definable function is defined just as before. Then we can define \( \text{Add} \) and \( \text{Mult} \) as terms of type \( \text{Nat}_\sigma \to (\text{Nat}_\sigma \to \text{Nat}_\sigma) \) 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
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

\[
\frac{\Gamma \vdash M : \forall X. \sigma}{\Gamma \vdash (\forall \tau). M \tau : \sigma[X := \tau]} \quad \text{(type application)}
\]

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.
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

$$
A_\sigma = \lambda x: \sigma. \lambda f: (\sigma \rightarrow \sigma). f x,
$$

of type $\sigma \rightarrow ((\sigma \rightarrow \sigma) \rightarrow \sigma)$, such that for every term $F$ of type $\sigma \rightarrow \sigma$ 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

$$
A = \Lambda X. \lambda x: X. \lambda f: (X \rightarrow X). f x,
$$

which has type $\forall X. (X \rightarrow ((X \rightarrow X) \rightarrow X))$, 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 $\vdash M: \sigma$ is provable is a hard problem. Indeed Statman proved that this problem is 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 $\vdash M: \sigma$ 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 Löb 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 \( \text{Nat} \). Inspired by the definition of \( \text{Succ} \) given in Section 4.4, we can define the successor function on the natural numbers as

\[
\text{Succ } c_n = \lambda n: \text{Nat}. \Lambda X. \lambda x: X. \lambda f: (X \to X). f(nX xf).
\]

Note how \( n \), which is of type \( \text{Nat} = \forall X. (X \to ((X \to X) \to X)) \), 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

\[
c_n\sigma aF = (\Lambda X. \lambda x: X. \lambda f: (X \to X). f^n(x))\sigma aF
\]

\[
\overset{\to}{\to}_{\lambda 2} (\lambda x: \sigma. \lambda f: (\sigma \to \sigma). f^n(x)) aF
\]

\[
\overset{\to}{\to}_{\lambda 2} F^n(a);
\]

that is,

\[
c_n\sigma aF \overset{\to}{\to}_{\lambda 2} F^n(a).
\]

\( \ast_{c2} \)

So \( c_n\sigma \) iterates \( F \) \( n \) times starting with \( a \). As a consequence,

\[
\text{Succ } c_n = (\lambda n: \text{Nat}. \Lambda X. \lambda x: X. \lambda f: (X \to X). f(nX xf)) c_n
\]

\[
\overset{\to}{\to}_{\lambda 2} \Lambda X. \lambda x: X. \lambda f: (X \to X). f(c_nX x f)
\]

\[
\overset{\to}{\to}_{\lambda 2} \Lambda X. \lambda x: X. \lambda f: (X \to X). f(f^n(x))
\]

\[
= \Lambda X. \lambda x: X. \lambda f: (X \to X). f^{n+1}(x) = c_{n+1}.
\]
We can also define addition of natural numbers as

\[ \text{Add} = \lambda m : \text{Nat}. \lambda n : \text{Nat}. \lambda X : X. \lambda f : (X \to X). (mX f(nX f))f. \]

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 \( X \), thus \( f(nXxf) \) also has type \( X \), and \( mXf(nXxf) \) has type \( (X \to X) \to X \), and finally \( (mXf(nXxf))f \) 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

\[ \langle -, - \rangle = \lambda u : \sigma. \lambda v : \tau. \lambda X : X. \lambda f : \sigma \to (\tau \to X). fuv, \]

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

\[ \langle -, - \rangle_{\sigma,\tau} MN \xrightarrow{\lambda 2} \lambda X. \lambda f : \sigma \to (\tau \to X). fMN. \]

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 \( \land, \lor, \neg, \bot \) and \( \exists \) are definable in terms of \( \to \) (as a logical connective, \( \Rightarrow \)) and \( \forall \).

**Proposition 4.13.** 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 \( \tau \):

\[
\begin{align*}
\sigma \land \tau & \equiv \forall X. ((\sigma \to (\tau \to X)) \to X) \\
\sigma \lor \tau & \equiv \forall X. ((\sigma \to X) \to ((\tau \to X) \to X)) \\
\neg \sigma & \equiv \sigma \to \forall X. X \\
\exists Y. \sigma & \equiv \forall X. ((\forall Y. (\sigma \to X)) \to X).
\end{align*}
\]
4.7. DEFINABILITY OF FUNCTIONS IN TYPED LAMBDA-CALCULI

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

$$
\pi_1 = \lambda g: \sigma \times \tau. g\sigma(\lambda x: \sigma. \lambda y: \tau. x)
$$

$$
\pi_2 = \lambda g: \sigma \times \tau. g\tau(\lambda x: \sigma. \lambda y: \tau. y).
$$

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

$$
\pi_1(M, N) \xrightarrow{+}^\lambda M \quad \text{and} \quad \pi_2(M, N) \xrightarrow{+}^\lambda N.
$$

For example, we have

$$
\pi_1(M, N) = (\lambda g: \sigma \times \tau. g\sigma(\lambda x: \sigma. \lambda y: \tau. x))(\Lambda X. \lambda f: \sigma \rightarrow (\tau \rightarrow X). f MN)
$$

$$
\xrightarrow{+}^\lambda (\Lambda X. \lambda f: \sigma \rightarrow (\tau \rightarrow X). f MN)\sigma(\lambda x: \sigma. \lambda y: \tau. x)
$$

$$
\xrightarrow{+}^\lambda (\lambda f: \sigma \rightarrow (\tau \rightarrow \sigma). f MN)(\lambda x: \sigma. \lambda y: \tau. x)
$$

$$
\xrightarrow{+}^\lambda (\lambda x: \sigma. \lambda y: \tau. x)MN
$$

$$
\xrightarrow{+}^\lambda (\lambda y: \tau. M)N
$$

$$
\xrightarrow{+}^\lambda M.
$$

The booleans can be defined as

$$
T = \Lambda X. \lambda x: X. \lambda y: X. x
$$

$$
F = \Lambda X. \lambda x: X. \lambda y: X. y,
$$

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

$$
(\text{if } T \text{ then } M \text{ else } N)\sigma \xrightarrow{+}^\lambda M
$$

$$
(\text{if } F \text{ then } M \text{ else } N)\sigma \xrightarrow{+}^\lambda N,
$$
where we write \((\text{if } T \text{ then } M \text{ else } N)\sigma\) instead of \((\text{if then else})\sigma TMN\) (and similarly for the other term). For example, we have
\[
(\text{if } T \text{ then } M \text{ else } N)\sigma = (\Lambda X. \lambda z: \text{Bool}. zX)\sigma TMN
\]
\[
\xrightarrow{\lambda_2} (\lambda z: \text{Bool}. z\sigma) TMN
\]
\[
\xrightarrow{\lambda_2} (T\sigma) MN
\]
\[
= ((\Lambda X. \lambda x: X. \lambda y: X. x)\sigma) MN
\]
\[
\xrightarrow{\lambda_2} (\lambda x: \sigma. \lambda y: \sigma. x) MN
\]
\[
\xrightarrow{\lambda_2} M.
\]

Lists, trees, and other inductively data structures are also representable in system F; see Girard–Lafond–Taylor [13].

We can also define an iterator \(\text{Iter}\) given by
\[
\text{Iter} = \Lambda X. \lambda u: X. \lambda f: (X \rightarrow X). \lambda z: \text{Nat}. zX uf
\]
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 \(\text{Iter} \sigma uf c_n\) iterates \(f \ n\) times over the input \(u\). It is easy to show that for any term \(t\) of type \(\text{Nat}\) we have
\[
\text{Iter} \sigma uf c_0 \xrightarrow{\lambda_2} u
\]
\[
\text{Iter} \sigma uf (\text{Succ}_c t) \xrightarrow{\lambda_2} f(\text{Iter} \sigma utf),
\]
and that
\[
\text{Iter} \sigma uf c_n \xrightarrow{\lambda_2} f^n(u).
\]

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 intutionistic 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 calculus of constructions due to Huet and Coquand, but these topics are beyond the scope of these notes.
4.8 HEAD NORMAL-FORMS AND THE PARTIAL COMPUTABLE FUNCTIONS

One last comment has to do with the use of the simply-typed λ-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 λ-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.

4.8 Head Normal-Forms and the Partial Computable Functions

One defect of the proof of Theorem 4.11 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 $g$ λ-defined by a closed term $G$ and a partial computable function $h$ λ-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 λ-defined by $G = \text{K}\Omega$ and $h$ is λ-defined by $H = \text{K}c_0$, with $\Omega = (\lambda x. (xx))(\lambda x. (xx))$. We have

$$\lambda x. H(Gx) = \lambda x. \text{K}c_0(\Omega x) \xrightarrow{+} \beta \lambda x. \text{K}c_0\Omega \xrightarrow{+} \beta \lambda x. c_0,$$

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 λ-define $h \circ g$.

It turns out that the λ-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 β-normal form. As a consequence, there a fewer λ-terms having no head normal form than λ-terms having no β-normal form, and we capture a stronger form of divergence.

Recall that a λ-term is either a variable $x$, or an application $(MN)$, or a λ-abstraction $(\lambda x. M)$. We can sharpen this characterization as follows.

**Proposition 4.14.** 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:

$$M = \lambda x_1 \cdots x_n. xM_1 \cdots M_m, \quad m, n \geq 0 \quad (a)$$

$$M = \lambda x_1 \cdots x_n. (\lambda x. M_0)M_1 \cdots M_m, \quad m \geq 1, n \geq 0, \quad (b)$$

where $x$ is a variable.

Proof. (1) Suppose that $M$ is an application $M = M_1M_2$. 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

$$M_1 = (N_1N_2 \cdots N_{n-1})N_n, \quad n \geq 2,$$

where $N_1$ is not an application term, and then

$$M = M_1M_2 = ((N_1N_2 \cdots N_{n-1})N_n)M_2 \quad n \geq 2,$$

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 $M = N_1N_2 \cdots N_p$ 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. \qed

The terms, $I, K, K_\ast, S$, the Church numerals $c_n$, if then else, $(M, N), \pi_1, \pi_2, \text{Iter}, \text{Succ}_e, \text{Add}$ and $\text{Mult}$ as in Proposition 4.5, are $\lambda$-terms of type (a). However, $\text{Pred}_K, \Omega = (\lambda x.(xx))(\lambda x.(xx)), Y$ (the Curry $Y$-combinator), $\Theta$ (the Turing $\Theta$-combinator) are of type (b).

Proposition 4.14 motivates the following definition.

**Definition 4.17.** 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 \( M \xrightarrow{\beta} N \).

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 4.14, the term \( \lambda x. x \Omega \) is a head normal form. It is the head normal form of the term \( \lambda x. (I x) \Omega \), which has no \( \beta \)-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 \( \beta \)-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 \( \beta \)-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 4.18.** The relation \( \xrightarrow{h} \), 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 \( M \xrightarrow{h} N \) with
\[
N = \lambda x_1 \cdots x_n. (M_0[x := M_1]) M_2 \cdots M_m.
\]
We denote by \( \xrightarrow{+} h \) the transitive closure of \( \xrightarrow{h} \) and by \( \xrightarrow{*} h \) the reflexive and transitive closure of \( \xrightarrow{h} \).

Given a term \( M \) containing a head redex, the head reduction sequence of \( M \) is the uniquely determined sequence of one-step head reductions
\[
M = M_0 \xrightarrow{h} M_1 \xrightarrow{h} \cdots \xrightarrow{h} M_n \xrightarrow{h} \cdots.
\]
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 4.15. (Wadsworth) A λ-term $M$ has a head normal form if and only if the head reduction sequence terminates.

In some intuitive sense, a λ-term $M$ that does not have any head normal form has a strong divergence behavior with respect to β-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 λ-term $M$ is a weak head normal form if it of one of the two forms

$$\lambda x. N \quad \text{or} \quad y N_1 \cdots N_m$$

where $y$ is a variable. These are exactly the terms that do not have a redex of the form $(\lambda x. M_0) M_1 N_1 \cdots N_m$. 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 4.19. A closed λ-term $M$ is solvable if there are closed terms $N_1, \ldots, N_n$ such that

$$MN_1 \cdots N_n \xrightarrow{\ast} \beta I.$$

A λ-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 4.16. (Wadsworth) A λ-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 λ-definability of numerical functions.

Definition 4.20. A function (partial or total) $f: \mathbb{N}^n \rightarrow \mathbb{N}$ is strongly λ-definable if for all $m_1, \ldots, m_n \in \mathbb{N}$, there is a combinator (a closed λ-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 β-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 4.16. Not only $Fc_{m_1} \cdots c_{m_n}$ has no β-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 $KII$. 


4.8. HEAD NORMAL-FORMS AND THE PARTIAL COMPUTABLE FUNCTIONS

**Theorem 4.17.** 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 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 5

Listable Sets and Diophantine Sets; Hilbert’s Tenth Problem

5.1 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. \( 3x_1, -2x_2 \), are monomials of degree 1.
3. \( x_1x_2, 2x_1^2, 3x_1x_3, -5x_2^2 \), are monomials of degree 2.
4. \( x_1x_2x_3, x_1^2x_3, -x_2^3 \), are monomials of degree 3.
5. \( x_1^4, -x_1^2x_3^2, x_1x_2^2x_3 \), 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 \( n = 3 \),

\[
x^{(1,2,1)} = x_1x_2^2x_3, \ x^{(0,2,2)} = x_2^2x_3^2.
\]

123
Definition 5.1. 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

$$x = t^2 - 1, \quad y = 2t, \quad z = t^2 + 1$$

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

\[(x, y, z) = (-283059965, -2218888517, 2220422932),\]
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.

5.2 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 5.1.** 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

\[ Q = P(u_1^2 + v_1^2 + z_1^2, \ldots, u_n^2 + v_n^2 + y_n^2 + z_n^2) \]

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 \( \mathbb{N} \). \( \square \)

As consequence, the contrapositive of Proposition 5.1 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 5.2. A set $S \subseteq \mathbb{N}$ of natural numbers is Diophantine (or Diophantine definable) if there is a polynomial $P(a, x_1, \ldots, x_n) \in \mathbb{Z}[a, x_1, \ldots, x_n]$, with $n \geq 0^1$ 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 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 $x_1, \ldots, x_n$,

$$P_1 = 0, \ P_2 = 0, \ldots, \ P_m = 0,$$  \hspace{1cm} (\ast)

observe that (\ast) 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

$$P_1^2 + P_2^2 + \cdots + P_m^2 = 0$$  \hspace{1cm} (\ast\ast)

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.

\(^1\)We have to allow $n = 0$. Otherwise singleton sets would not be Diophantine.
5.2. DIOPHANTINE SETS AND LISTABLE SETS

Definition 5.3. 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 2.1 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 5.2.** 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 \( \langle x_1, \ldots, x_n \rangle \) of Section 2.1, 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 5.3.** (Davis-Putnam-Robinson-Matiyasevich, 1970) Every listable subset of \( \mathbb{N} \) is Diophantine. Every partial computable function is Diophantine.

Theorem 5.3 is often referred to as the DPRM theorem. A complete proof of Theorem 5.3 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 3.11 that \( K = \{ x \in \mathbb{N} \mid \varphi_x(x) \text{ is defined} \} \) is listable but not computable. Since \( K \) is listable, by Theorem 5.3, 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 5.4.** 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 5.3.

### 5.3 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 5.5.** For every listable subset \( S \) of \( \mathbb{N} \), there is some polynomial \( Q(x, x_1, \ldots, x_n) \) with integer coefficients such that

\[
S = \{ Q(a, b_1, \ldots, b_n) \mid Q(a, b_1, \ldots, b_n) \in \mathbb{N}, a, b_1, \ldots, b_n \in \mathbb{N} \}.
\]
5.3. SOME APPLICATIONS OF THE DPRM THEOREM

Proof. By the DPRM theorem (Theorem 5.3), 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 \( a \in S \). \( \Box \)

Remark: It should be noted that in general, the polynomials \( Q \) arising in Theorem 5.5 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 5.5, \( S_3 \) 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 5.5, 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 $a, b, s, r, q \in \mathbb{N}$:

\[
\begin{align*}
    p &= s + 1 \\
    p &= r + 2 \\
    q &= s! \\
    ap - bq &= 1
\end{align*}
\]

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:

\[(k + 2)\left[1 - ((wz + h + j - q)^2 + [(gk + 2g + k + 1)(h + j) + h - z]^2 \\
+ 16(k + 1)^3(k + 2)(n + 1)^2 + 1 - f^2]^2 \\
+ 2(n + p + q + z - e)^2 + [e^3(e + 2)(a + 1)^2 + 1 - o^2]^2 \\
+ [(a^2 - 1)y^2 + 1 - x^2]^2 + [16r^2y^4(a^2 - 1) + 1 - u^2]^2 \\
+ [((a + u^2 - a))^2 - 1)(n + 4dy)^2 + 1 - (x + cu)^2]^2 \\
+ [(a^2 - 1)^2l^2 + 1 - m^2]^2 + [ai + k + 1 - l - i]^2 + [n + l + v - y]^2 \\
+ [p + l(a - n - 1) + b(2an + 2a - n^2 - 2n - 2) - m]^2 \\
+ [q + y(a - p - 1) + b(2ap + 2a - p^2 - 2p - 2) - x]^2 \\
+ [z + pl(a - p) + t(2ap - p^2 - 1) - pm]^2]\]
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.

5.4 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 2.5), 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 3.5 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 5.6. (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 5.3), 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.

The Diophantine equation \( U(n,a,x_1,\ldots,x_n) = 0 \) is called a \textit{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
\[ S(S(\cdots(S(0))\cdots)) \]
is denoted by \( S^n(0) \), and represents the natural number \( n \).

For example,
\[ \exists x(S(S(S(0))) < (S(S(0)) + x)), \]
\[ \exists x \exists y \exists z((x > 0) \land (y > 0) \land (z > 0) \land ((x \cdot x + y \cdot y) = z \cdot z)), \]
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 \( x = S^3(0), y = S^4(0) \) 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 \textit{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
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

$$S^m(0) + S^n(0) = S^{m+n}(0)$$

$$S^m(0) \cdot S^n(0) = S^{mn}(0)$$

$$S^m(0) < S^n(0) \quad \text{iff} \quad m < n,$$

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 $S^{m_1}(0), \ldots,$
$S^{m_m}(0)$ in $P_{\text{neg}}(x_1, \ldots, x_m)$, and evaluate using the formulae for the addition and multipli-
cation 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:

\[ \forall x \neg (S(x) = 0) \]
\[ \forall x \forall y ((S(x) = S(y)) \Rightarrow (x = y)) \]
\[ \forall y ((y = 0) \lor \exists x (S(x) = y)) \]
\[ \forall x (x + 0 = x) \]
\[ \forall x \forall y (x + S(y) = S(x + y)) \]
\[ \forall x (x \cdot 0 = 0) \]
\[ \forall x \forall y (x \cdot S(y) = x \cdot y + x). \]

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

\[ S^m(0) + S^n(0) = S^{m+n}(0) \]
\[ S^m(0) \cdot S^n(0) = S^{mn}(0) \]
\[ S^m(0) < S^n(0) \text{ iff } m < n, \]

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 5.7.** (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

\[
\neg(\exists x_1, \ldots, x_m)(F(x_1, \ldots, x_m) = 0) \tag{\ast}
\]

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:

\[
A = \{ a \in \mathbb{N} \mid \neg(\exists x_1, \ldots, x_n)(P_a(a, x_1, \ldots, x_n) = 0) \text{ is provable from } A \}, \tag{\ast\ast}
\]

where \( P_n(a, x_1, \ldots, x_n) \) is defined just after Proposition 5.6. 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 5.6, 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

\[
(\exists x_1, \ldots, x_n)(P_k(k, x_1, \ldots, x_n) = 0), \quad \tag{\dagger_1}
\]

and since \( A = W_k \), by (\ast\ast), that

\[
\neg(\exists x_1, \ldots, x_n)(P_k(k, x_1, \ldots, x_n) = 0) \text{ is provable from } A. \quad \tag{\dagger_2}
\]

By (\dagger_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 (\dagger_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 \( A \). \(\square\)
As a corollary of Theorem 5.7, 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 \( \mathcal{A} \) 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 6

The Post Correspondence Problem; Applications to Undecidability Results

6.1 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:

\[
    abab\, aaabbb\, aab\, ba\, ab\, ab\, aa = ababaaa\, bb\, baab\, baa\, ba\, ba\, a.
\]

We are beginning to suspect that this is a hard problem. Indeed, it is undecidable!
Theorem 6.1. (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 6.1, 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.

6.2 Some Undecidability Results for CFG’s

Theorem 6.2. 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:

- $S \rightarrow S_U$
- $S \rightarrow S_V$
- $S_U \rightarrow u_is_Uc_i$
- $S_U \rightarrow u_ic_i$
- $S_V \rightarrow v_is_Vc_i$
- $S_V \rightarrow v_ic_i$.

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 6.4).

Recall that the computations of a Turing Machine, $M$, can be described in terms of instantaneous descriptions, $upav$.

We can encode computations

$$ID_0 \vdash ID_1 \vdash \cdots \vdash ID_n$$

halting in a proper ID, as the language, $L_M$, consisting all of strings

$$w_0 \# w_1^R \# w_2 \# w_2^R \# \cdots \# w_{2k} \# w_{2k+1}^R,$$

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 $L_0^M$ and $L_1^M$ defined as follows:

1. The strings in $L_0^M$ 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 $L_1^M$ 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 6.3.** Given any Turing machine $M$, the languages $L_0^M$ and $L_1^M$ are context-free, and $L_M = L_0^M \cap L_1^M$.

**Proof.** We can construct PDA’s accepting $L_0^M$ and $L_1^M$. It is easily checked that $L_M = L_0^M \cap L_1^M$. \hfill \square

As a corollary, we obtain the following undecidability result:
**Theorem 6.4.** 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 6.3, the languages $L_M^0$ and $L_M^1$ are context-free. Thus, we can construct context-free grammars $G_1$ and $G_2$ so that $L_M^0 = L(G_1)$ and $L_M^1 = L(G_2)$. Then, $M$ never halts in a proper ID iff $L_M = \emptyset$ iff (by Theorem 6.3), $L_M = L(G_1) \cap L(G_2) = \emptyset$. \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 6.5.** 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 6.6.** 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 6.5, 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 6.7.** 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!
6.3 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 $c: \mathcal{L} \rightarrow \mathbb{N}$ 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 $L_1R \in \mathcal{L}$, $RL_1 \in \mathcal{L}$, and $c(RL_1)$ and $c(L_1R)$ 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 6.8.** (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. \qed

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 7

Computational Complexity; \( \mathcal{P} \) and \( \mathcal{NP} \)

7.1 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 7.1. 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

$$ID_0 \vdash ID_1 \vdash^* ID_{n-1} \vdash ID_n, \text{ with } n > p(|x|),$$

where $ID_0 = q_0x$ 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 7.1 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 7.1.** 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 $\mathcal{P}$.

### 7.2 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 7.2.** 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 $G$?
7.3 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.

![Figure 7.1: A 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 7.2.** 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 7.2 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 7.2 is know for Hamiltonian cycles.

### 7.4 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 7.2 is a plane projection of a regular dodecahedron and we want to know if there is a Hamiltonian cycle in this directed graph.

![Figure 7.2: A tour “around the world.”](image)
Finding a Hamiltonian cycle in this graph does not appear to be so easy!
A solution is shown in Figure 7.3 below.

![Figure 7.3: A Hamiltonian cycle in D.](image)

**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.

### 7.5 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 \emph{propositional (or boolean) variables}, say

\[
PV = \{x_1, x_2, \ldots, \},
\]

using the connectives \( \land \) (and), \( \lor \) (or) and \( \neg \) (negation).

We define a \emph{literal (or atomic proposition)}, \( L \), as \( L = x \) or \( L = \neg x \), also denoted by \( \overline{x} \), where \( x \in PV \).

A \emph{clause}, \( C \), is a disjunction of pairwise distinct literals,

\[
C = (L_1 \lor L_2 \lor \cdots \lor L_m).
\]

Thus, a clause may also be viewed as a nonempty \emph{set}

\[
C = \{L_1, L_2, \ldots, L_m\}.
\]

We also have a special clause, the \emph{empty clause}, denoted \( \perp \) or \( \Box \) (or \( \{\} \)). It corresponds to the truth value false.

A \emph{proposition in CNF, or boolean formula}, \( P \), is a conjunction of pairwise distinct clauses

\[
P = C_1 \land C_2 \land \cdots \land C_n.
\]

Thus, a boolean formula may also be viewed as a nonempty \emph{set}

\[
P = \{C_1, \ldots, C_n\},
\]

but this time, the comma is interpreted as conjunction. We also allow the proposition \( \perp \), and sometimes the proposition \( \top \) (corresponding to the truth value true).

For example, here is a boolean formula:

\[
P = \{(x_1 \lor x_2 \lor x_3), (\overline{x_1} \lor x_2), (\overline{x_2} \lor x_3), (\overline{x_3} \lor x_1), (\overline{x_1} \lor \overline{x_2} \lor \overline{x_3})\}.
\]

In order to interpret boolean formulae, 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 \emph{truth assignment (or valuation)}, \( v \), is any function \( v: PV \to BOOL \).

For example, the function \( v_F: PV \to BOOL \) 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

\[
\begin{align*}
v(x_1) &= T \\
v(x_2) &= F \\
v(x_3) &= T \\
v(x_i) &= T \quad \text{for all } i \geq 4
\end{align*}
\]

is also a truth assignment.

Given a truth assignment \( v : PV \rightarrow BOOL \), we define the truth value \( \widehat{v}(X) \) of a literal, clause, and boolean formula, \( X \), using the following recursive definition:

1. \( \widehat{v}(\bot) = F, \widehat{v}(\top) = T \).
2. \( \widehat{v}(x) = v(x), \) if \( x \in PV \).
3. \( \widehat{v}(\overline{x}) = \overline{v(x)}, \) if \( x \in PV \), where \( \overline{v(x)} = F \) if \( v(x) = T \) and \( \overline{v(x)} = T \) if \( v(x) = F \).
4. \( \widehat{v}(C) = F \) if \( C \) is a clause and \( \widehat{v}(L_i) = F \) for all literals \( L_i \) in \( C \), otherwise \( T \).
5. \( \widehat{v}(P) = T \) if \( P \) is a boolean formula and \( \widehat{v}(C_j) = T \) 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 \( \widehat{v}(P) \) 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 7.3.** 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 \( \widehat{v_1}(P) = \widehat{v_2}(P) \).

In view of Proposition 7.3, 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

\[
P = \{(x_1 \lor x_2 \lor x_3), (\overline{x_1} \lor x_2), (x_2 \lor x_3), (x_3 \lor x_1), (x_1 \lor x_2 \lor x_3)\},
\]
we only need to specify \(v(x_1), v(x_2), v(x_3)\). Thus there are \(2^3 = 8\) distinct truth assignments:

\[
\begin{array}{ccc}
F, F, F & T, F, F \\
F, F, T & T, F, T \\
F, T, F & T, T, F \\
F, T, T & T, T, T.
\end{array}
\]

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

\[
P = (x_1 \lor x_2 \lor x_3) \land (\overline{x_1} \lor x_2) \land (\overline{x_2} \lor x_3) \land (\overline{x_3} \lor x_1) \land (\overline{x_1} \lor \overline{x_2} \lor \overline{x_3})
\]

\[
= \{(x_1 \lor x_2 \lor x_3), (\overline{x_1} \lor x_2), (\overline{x_2} \lor x_3), (\overline{x_3} \lor x_1), (\overline{x_1} \lor \overline{x_2} \lor \overline{x_3})\},
\]

and the truth assignment

\[
v(x_1) = T, \quad v(x_2) = F, \quad v(x_3) = F.
\]

For the literals, we have

\[
\hat{v}(x_1) = T, \quad \hat{v}(x_2) = F, \quad \hat{v}(x_3) = F, \quad \hat{v}(\overline{x_1}) = F, \quad \hat{v}(x_2) = T \quad \hat{v}(\overline{x_3}) = T,
\]

for the clauses

\[
\hat{v}(x_1 \lor x_2 \lor x_3) = \hat{v}(x_1) \lor \hat{v}(x_2) \lor \hat{v}(x_3) = T \lor F \lor F = T,
\]

\[
\hat{v}(\overline{x_1} \lor x_2) = \hat{v}(\overline{x_1}) \lor \hat{v}(x_2) = F \lor F = F,
\]

\[
\hat{v}(\overline{x_2} \lor x_3) = \hat{v}(\overline{x_2}) \lor \hat{v}(x_3) = T \lor F = T,
\]

\[
\hat{v}(\overline{x_3} \lor x_1) = \hat{v}(\overline{x_3}) \lor \hat{v}(x_1) = T \lor T = T,
\]

\[
\hat{v}(\overline{x_1} \lor \overline{x_2} \lor \overline{x_3}) = \hat{v}(\overline{x_1}) \lor \hat{v}(\overline{x_2}) \lor \hat{v}(\overline{x_3}) = F \lor T \lor T = T,
\]

and for the conjunction of the clauses,

\[
\hat{v}(P) = \hat{v}(x_1 \lor x_2 \lor x_3) \land \hat{v}(\overline{x_1} \lor x_2) \land \hat{v}(\overline{x_2} \lor x_3) \land \hat{v}(\overline{x_3} \lor x_1) \land \hat{v}(\overline{x_1} \lor \overline{x_2} \lor \overline{x_3})
\]

\[
= T \land F \land T \land T \land T = T.
\]

Therefore, \(\hat{v}(P) = F\).

**Definition 7.3.** 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 \( \mathcal{P} \).
7.6 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 7.4.** 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

$$ID_0 \vdash ID_1 \vdash \ldots \vdash ID_{n-1} \vdash ID_n,$$

with $n > p(|x|)$, 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

$$\mathcal{P} \subseteq \mathcal{NP},$$

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 $\mathcal{P} \neq \mathcal{NP}$ 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 7.5.** 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

$$ID_0 \vdash ID_1 \vdash \ldots \vdash ID_{n-1} \vdash ID_n,$$

with $n > p(|x|)$, 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 $f: \Sigma^* \to \Sigma^*$ so that for all $u \in \Sigma^*$, 

$$u \in L_1 \iff f(u) \in L_2.$$ 

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 $f: \Sigma^* \to \Sigma^*$ 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 3.16 for polynomial-time reducibility is easy to prove.

**Proposition 7.4.** 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

$$ (x_{1j} \lor x_{2j} \lor \cdots \lor x_{nj}), \quad 1 \leq j \leq n. \quad (1) $$

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

$$ (\overline{x_{ij}} \lor \overline{x_{kj}}), \quad 1 \leq i, j, k \leq n, \; i \neq k. \quad (2) $$

Since $(\overline{x_{ij}} \lor \overline{x_{kj}})$ is equivalent to $(\overline{x_{ij}} \land \overline{x_{kj}})$, 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

$$ (x_{i1} \lor x_{i2} \lor \cdots \lor x_{in}), \quad 1 \leq i \leq n, \quad (3) $$

and

$$ (\overline{x_{ij}} \lor \overline{x_{ik}}), \quad 1 \leq i, j, k \leq n, \; j \neq k. \quad (4) $$

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 assignation $v$ 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 $(\overline{x_{ij}} \lor \overline{x_{kj+1}})$.

Therefore, for all $(i, k)$ such that $(i, k) \notin E$ (with $i, k \in \{1, 2, \ldots, n\}$), we have the clauses

$$ (\overline{x_{ij}} \lor \overline{x_{kj+1}} \text{(mod } n)), \quad j = 1, \ldots, n. \quad (5) $$

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 $F = \tau(G)$. 

7.6. THE CLASS $\mathcal{NP}$, $\mathcal{NP}$-COMPLETENESS
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 8.2.

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 7.6.** 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 nondeterministically 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 3.17 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 7.6.

The importance of \( \mathcal{NP} \)-complete problems stems from the following theorem which follows immediately from Proposition 7.4.

**Theorem 7.5.** 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

\[
\text{co}\mathcal{NP} = \{ \overline{L} \mid L \in \mathcal{NP} \},
\]
7.7. THE COOK-LEVIN THEOREM

that is, $\text{coNP}$ consists of all complements of languages in $\text{NP}$. Since $\mathcal{P} \subseteq \text{NP}$ and $\mathcal{P}$ is closed under complementation,

$$\mathcal{P} \subseteq \text{coNP},$$

and thus

$$\mathcal{P} \subseteq \text{NP} \cap \text{coNP},$$

but nobody knows whether the inclusion is proper. There are problems in $\text{NP} \cap \text{coNP}$ not known to be in $\mathcal{P}$; see Section 8.3. It is unknown whether $\text{NP}$ is closed under complementation, that is, nobody knows whether $\mathcal{P} = \text{coNP}$. This is considered unlikely. We will come back to $\text{coNP}$ in Section 8.3.

Next, we prove a famous theorem of Steve Cook and Leonid Levin (proved independently): SAT is $\text{NP}$-complete.

### 7.7 The Cook–Levin Theorem: SAT is $\text{NP}$-Complete

Instead of showing directly that SAT is $\text{NP}$-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 $\text{NP}$-complete.

2. We show that the tiling problem can be reduced to SAT.

We are given a finite set $\mathcal{T} = \{t_1, \ldots, t_p\}$ 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 $H \subseteq \mathcal{T} \times \mathcal{T}$, and the vertical constraints are given by a relation $V \subseteq \mathcal{T} \times \mathcal{T}$.

Thus, a tiling system is a triple $T = (\mathcal{T}, V, H)$ 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:

\[
\begin{array}{c|c|c|c|c}
| a & e & | a & c & | c & e & | e & e |
\end{array}
\]
\[
\begin{array}{c|c|c|c|c}
| b & d & | b & d & | c & e & | d & e |
\end{array}
\]
\[
\begin{array}{c|c|c|c|c}
| c & d & | b & c & | c & d & | e & e |
\end{array}
\]
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

```
 a   b   c   d   e   e   e
  c   c   d   d   e   e   e
  c   b   c   d   e   e   e
```

we have the tiling shown below:

```
  a   b   c   d   e   e   e
   c   c   d   d   e   e   e
    c   b   c   d   e   e   e
     c   b   c   d   e   e   e
```

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 \((T, V, H, \hat{s}, \sigma_0)\), where \((T, V, H)\) is a tiling system, \(\hat{s}\) 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 \(\hat{s} = 1000000001\). The length of \(\hat{s}\) 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 \(((T, V, H), \hat{s}, \sigma_0)\) 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 \(((T, V, H), \hat{s}, \sigma_0)\). 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 7.6. 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, \(((T, V, H)_L, \hat{s}, \sigma_0)\), where \(s = p(|u|) + 2\), and where the bottom row encodes the starting ID, so that \(u \in L\) iff the tiling problem \(((T, V, H)_L, \hat{s}, \sigma_0)\) 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 the size of the input \(((T, V, H), \hat{s}, \sigma_0)\), 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

\[
\begin{array}{c}
\text{a} \\
\text{a}
\end{array}
\]
(2) For every \( a \in \Gamma \), the bottom row uses tiles

\[
\begin{array}{c}
\text{a} \\
\hline
\end{array} \quad \begin{array}{c}
q_0, a \\
\hline
\end{array}
\]

where \( q_0 \) is the start state.

(3) For every instruction \((p, a, b, R, q) \in \delta\), for every \( c \in \Gamma \), tiles

\[
\begin{array}{c}
b \\
q, R \\
p, a \\
\hline
\end{array} \quad \begin{array}{c}
q, c \\
q, R \\
c \\
\hline
\end{array}
\]

(4) For every instruction \((p, a, b, L, q) \in \delta\), for every \( c \in \Gamma \), tiles

\[
\begin{array}{c}
q, c \\
q, L \\
c \\
\hline
\end{array} \quad \begin{array}{c}
b \\
q, L \\
p, a \\
\hline
\end{array}
\]

(5) For every halting state, \( p \), tiles

\[
\begin{array}{c}
p, 1 \\
\hline
\end{array}
\begin{array}{c}
p, 1 \\
\hline
\end{array}
\]

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:

\[
\begin{array}{c}
B \\
\hline
\end{array} \quad \cdots \quad \begin{array}{c}
q_0, u_1 \\
\hline
\end{array} \quad \cdots \quad \begin{array}{c}
u_k \\
\hline
\end{array} \quad \cdots \quad \begin{array}{c}
B \\
\hline
\end{array}
\]

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 \( i \) steps the upper horizontal edge of the \((i+1)\)th row of tiles represents the current ID 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 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 \( p 1 \) 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 \( \mathcal{NE}XP \)-complete! The class \( \mathcal{NE}XP \) 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 8.4. By the time hierarchy theorem (Cook, Seiferas, Fischer, Meyer, Zak), it is known that \( \mathcal{NP} \) is properly contained in \( \mathcal{NE}XP \); 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 7.7. (Cook, 1971, Levin, 1973) The satisfiability problem SAT is \( \mathcal{NP} \)-complete.

Proof. We reduce the tiling problem to SAT. Given a tiling problem, \(((T, V, H), \hat{s}, \sigma_0)\), 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 \( t \in T \).

The intuition is that \( x_{mnt} = T \) 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,

\[ (x_{mnt_1} \lor x_{mnt_2} \lor \cdots \lor x_{mnt_p}), \]

for all \( p \) tiles in \( T \).

This clause states that every position in \( \sigma \) is tiled.

2. For any two distinct tiles \( t \neq t' \in T \), 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 \( (t, t') \in T \times T - H \), for all \( m \) with \( 1 \leq m \leq 2s - 1 \), and all \( n \), with \( 1 \leq n \leq s \),

\[ (\overline{x_{mnt}} \lor \overline{x_{m+1nt'}}). \]

This clause enforces the horizontal adjacency constraints.

4. For every pair of tiles \( (t, t') \in T \times T - V \), for all \( m \) with \( 1 \leq m \leq 2s \), and all \( n \), with \( 1 \leq n \leq s - 1 \),

\[ (\overline{x_{mnt}} \lor \overline{x_{mn+1t'}}). \]

This clause enforces the vertical adjacency constraints.

5. For all \( m \) with \( 1 \leq m \leq 2s \),

\[ (x_{m_1\sigma_0(m)}). \]

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 7.7 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 7.8.** *(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 \( v \), \( v(L_i) = F \), for \( i = 1, 2, \ldots, 6 \). To satisfy the first clause, we must have \( v(y_1) = T \). Then to satisfy the second clause, we must have \( v(y_2) = T \), and similarly satisfy the third clause, we must have \( v(y_3) = T \). However, since \( v(L_5) = F \) and \( v(L_6) = F \), the only way to satisfy the fourth clause is to have \( v(y_3) = F \), contradicting that \( v(y_3) = T \). 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 \( v(L_1) = T \). Then if we let \( v(y_1) = v(y_2) = v(y_3) = F \), we see that \( C' \) is satisfied.

Say \( i = 2 \), so \( v(L_1) = F \) and \( v(L_2) = T \). Again if we let \( v(y_1) = v(y_2) = v(y_3) = F \), we see that \( C' \) is satisfied.

Say \( i = 3 \), so \( v(L_1) = F, v(L_2) = F, \) and \( v(L_3) = T \). If we let \( v(y_1) = T \) and \( v(y_2) = v(y_3) = F \), we see that \( C' \) is satisfied.

Say \( i = 4 \), so \( v(L_1) = F, v(L_2) = F, v(L_3) = F, \) and \( v(L_4) = T \). If we let \( v(y_1) = T, v(y_2) = T \) and \( v(y_3) = F \), we see that \( C' \) is satisfied.

Say \( i = 5 \), so \( v(L_1) = F, v(L_2) = F, v(L_3) = F, v(L_4) = F, \) and \( v(L_5) = T \). If we let \( v(y_1) = T, v(y_2) = T \) and \( v(y_3) = T \), we see that \( C' \) is satisfied.
Say $i = 6$, so $v(L_1) = F$, $v(L_2) = F$, $v(L_3) = F$, $v(L_4) = F$, $v(L_5) = F$, and $v(L_6) = T$. Again, if we let $v(y_1) = T$, $v(y_2) = T$ and $v(y_3) = T$, 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

$$(L_1 \lor L_2 \lor y_1), (\overline{y_1} \lor L_3 \lor y_2), (y_2 \lor L_4 \lor y_3), \ldots, (\overline{y}_{k-4} \lor L_{k-2} \lor y_{k-3}), (\overline{y}_{k-3} \lor L_{k-1} \lor L_k).$$

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 $v(L_i) = F$, for $i = 1, \ldots, k$.

However, $C'$ is satisfied by some $v$, and the only way this can happen is that $v(y_1) = T$, to satisfy the first clause. Then, $v(\overline{y_1}) = F$, and we must have $v(y_2) = T$, to satisfy the second clause.

By induction, we must have $v(y_{k-3}) = T$, 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 $v(C) = T$, and thus, there is a smallest index $i$, with $1 \leq i \leq k$, so that $v(L_i) = T$ (and so, $v(L_j) = F$ for all $j < i$).

Let $v'$ be the assignment extending $v$ defined so that

$$v'(y_j) = F \quad \text{if } \max\{1, i - 1\} \leq j \leq k - 3,$$

and $v'(y_j) = T$, otherwise.

It is easily checked that $v'(C') = T$. \hfill $\Box$

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 7.9.** (Cook, 1971) The satisfiability problem for exact 3-SAT is $NP$-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. \hfill $\Box$
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, \( x \in \text{PV} \), 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 \( \text{nff} \). A proposition is in \( \text{nff} \) 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 \( \text{nff} \) by using the de Morgan laws:

\[
\neg (A \lor B) \equiv (\neg A \land \neg B)\\
\neg (A \land B) \equiv (\neg A \lor \neg B)\\
\neg A \equiv A.
\]

Then, a proposition in \( \text{nff} \) 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 \( \text{nnf} \) to CNF is to construct a tree whose nodes are labeled with sets of propositions using the following (Gentzen-style) rules:

\[
\frac{P, \Delta}{(P \land Q), \Delta} \quad Q, \Delta
\]
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 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 8

Some $\mathcal{NP}$-Complete Problems

8.1 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 so 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.
8.1. 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 8.1.** 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 8.1?

Finding a Hamiltonian cycle in this graph does not appear to be so easy! A solution is shown in Figure 8.2 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 8.1: A tour "around the world."

Figure 8.2: 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 8.2. 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 8.1 to an undirected edge. The directed Hamiltonian cycle given in Figure 8.1 is also an undirected Hamiltonian cycle of the undirected graph of Figure 8.3.

We see immediately that Hamiltonian Cycle (for Undirected Graphs) is in $\mathcal{NP}$. To prove that it is $\mathcal{NP}$-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 8.1.** 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 8.4. A maximal solution 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 8.5. A maximal solution corresponds to the largest feasible value of $K$. The problem Clique is obviously in $NP$. To show that it is $NP$-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.

(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 8.6. A minimal solution corresponds to the smallest feasible value of $B$. The problem Node Cover is obviously in $NP$. To show that it is $NP$-complete, we reduce Independent Set to it. This means that we provide a method running in polynomial time that converts every instance of
8.1. STATEMENTS OF THE PROBLEMS

**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 $\ast$-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 $\ast$-free regular expressions are the right candidate. A $\ast$-free regular expression is a regular expression which is built up from the atomic expressions using only $+$ and $\cdot$, but not $\ast$. 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

$$a_{11}x_1 + \cdots + a_{1q}x_q = b_1$$
$$\vdots \quad \vdots$$
$$a_{i1}x_1 + \cdots + a_{iq}x_q = b_i$$
$$\vdots \quad \vdots$$
$$a_{p1}x_1 + \cdots + a_{pq}x_q = b_p$$

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.

8.2 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 8.2.** 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

\[
\begin{align*}
\{p_{11}\}, \{p_{12}\}, \{p_{21}\}, \{p_{22}\}, \{p_{23}\}, \{p_{31}\}, \{p_{41}\}, \{p_{42}\} \\
T_{1,F} &= \{x_1, p_{11}\} \\
T_{1,T} &= \{x_1, p_{21}\} \\
T_{2,F} &= \{x_2, p_{22}, p_{31}\} \\
T_{2,T} &= \{x_2, p_{12}, p_{41}\} \\
T_{3,F} &= \{x_3, p_{23}\} \\
T_{3,T} &= \{x_3, p_{42}\} \\
\{C_1, p_{11}\}, \{C_1, p_{12}\}, \{C_2, p_{21}\}, \{C_2, p_{22}\}, \{C_2, p_{23}\}, \{C_3, p_{31}\}, \{C_4, p_{41}\}, \{C_4, p_{42}\}.
\end{align*}
\]

It is easy to check that the set \( C \) consisting of the following subsets is an exact cover:

\[
\begin{align*}
T_{1,T} &= \{x_1, p_{21}\}, T_{2,T} = \{x_2, p_{12}, p_{41}\}, T_{3,F} = \{x_3, p_{23}\}, \\
\{C_1, p_{11}\}, \{C_2, p_{22}\}, \{C_3, p_{31}\}, \{C_4, p_{42}\}.
\end{align*}
\]
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 \(\mathcal{F}\):
\[
T_{i,T} = \{x_i\} \cup \{p_{jk} \mid L_{jk} = \overline{x}_i\}
\]
which contains \(x_i\) and all negative occurrences of \(x_i\), and
\[
T_{i,F} = \{x_i\} \cup \{p_{jk} \mid L_{jk} = x_i\}
\]
which contains \(x_i\) and all its positive occurrences. Note carefully that \(T_{i,T}\) involves negative occurrences of \(x_i\) whereas \(T_{i,F}\) 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 \(\mathcal{C}\) as follows:

For each \(x_i\), we put the subset \(T_{i,T}\) in \(\mathcal{C}\) iff \(v(x_i) = T\), else we we put the subset \(T_{i,F}\) in \(\mathcal{C}\) iff \(v(x_i) = F\). Also, for every clause \(C_j\), we put some subset \(\{C_j, p_{jk}\}\) in \(\mathcal{C}\) for a literal \(L_{jk}\) which is made true by \(v\). By construction of \(T_{i,T}\) and \(T_{i,F}\), this \(p_{jk}\) is not in any set in \(\mathcal{C}\) 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 \(\mathcal{C}\) for every remaining \(p_{jk}\) which has not yet been covered by the sets already in \(\mathcal{C}\).

Going back to Example 8.2, 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 \(\mathcal{C}\).

We leave as an exercise to check that the above procedure works.

Conversely, if \(\mathcal{C}\) is an exact cover of \(\tau(F)\), we define a truth assignment as follows:

For every \(x_i\), if \(T_{i,T}\) is in \(\mathcal{C}\), then we set \(v(x_i) = T\), else if \(T_{i,F}\) is in \(\mathcal{C}\), then we set \(v(x_i) = F\). We leave it as an exercise to check that this procedure works.
Example 8.3. 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

\[ F_2 = \{C_1 = (x_1 \lor \overline{x_2}), C_2 = (x_1 \lor x_2 \lor x_3), C_3 = (x_2), C_4 = (x_2 \lor \overline{x_3} \lor x_4)\} \]

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 \((U, F)\) of Exact Cover to a directed graph \( G = \tau(U, F) \) such that \( G \) has a Hamiltonian cycle iff \((U, F)\) has an exact cover.

The construction of the graph \( G \) uses a trick involving a small subgraph \( Gad \) with 7 (distinct) nodes known as a gadget shown in Figure 8.7.
The crucial property of the graph $G_{ad}$ is that if $G_{ad}$ is a subgraph of a bigger graph $G$ in such a way that no edge of $G$ is incident to any of the nodes $u,v,w$ unless it is one of the eight edges of $G_{ad}$ incident to the nodes $u,v,w$, then for any Hamiltonian cycle in $G$, 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 8.8.

Whenever such a figure occurs, the actual graph is obtained by substituting a copy of the graph $G_{ad}$ (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 8.9.

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 8.9: 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 8.4. The above construction is illustrated in Figure 8.10 for the instance of the exact cover problem given by

\[ U = \{u_1, u_2, u_3, u_4\}, \quad F = \{S_1 = \{u_3, u_4\}, S_2 = \{u_2, u_3, u_4\}, S_3 = \{u_1, u_2\}\}. \]

It remains to prove that \((U, F)\) has an exact cover iff the graph \(G = \tau(U, F)\) 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 \((S_{i-1}, S_i)\) can’t be traversed, which means that the short edge \((S_{i-1}, S_i)\) is traversed. Consequently, if \(C\) consists of those subsets \(S_i\) such that the short edge \((S_{i-1}, S_i)\) is traversed, then \(C\) consists of pairwise disjoint subsets whose union is \(U\), namely \(C\) 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

$$\text{short } (S_0, S_1), \text{ long } (S_1, S_2), \text{ short } (S_2, S_3), (S_3, u_0),$$

$$ (u_0, u_1)_3, (u_1, u_2)_3, (u_2, u_3)_1, (u_3, u_4)_1, (u_4, S_0).$$

The subsets corresponding to the short ($S_{i-1}, S_i$) edges are $S_1$ and $S_3$, and indeed $C = \{S_1, S_3\}$ 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 $C$ 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 $S_i \in C$, each edge $(u_{j-1}, u_j)_i$ such that $u_j \in S_i$, 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 $(u_n, S_0)$ and $(S_m, u_0)$, then we obtain a Hamiltonian cycle.

In our example, the exact cover $C = \{S_1, S_3\}$ yields the Hamiltonian

$$\text{short } (S_0, S_1), \text{ long } (S_1, S_2), \text{ short } (S_2, S_3), (S_3, u_0),$$

$$ (u_0, u_1)_3, (u_1, u_2)_3, (u_2, u_3)_1, (u_3, u_4)_1, (u_4, S_0)$$

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) \(\leq_{P}\) 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 8.11.

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 $\{u_1, u_2\}$.
8.2. PROOFS OF NP-COMPLETENESS

Figure 8.11: Conversion of a directed graph into an undirected graph

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 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 \textit{NP}-complete, we reduce Exact 3-Satisfiability to it:

\textbf{Exact 3-Satisfiability} $\leq_p \text{Independent Set}$

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.

\textbf{Example 8.5.} 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 8.12.

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
Figure 8.12: The graph constructed from the clauses of Example 8.5

we assign an arbitrary truth value to the unassigned variables. This yields a satisfying assignment for $F$.

In Example 8.5, the set $C = \{c_{11}, c_{22}, c_{32}, c_{41}\}$ corresponding to the nodes shown in red in Figure 8.12 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 8.13, 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.
(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 8.14 where an independent set is shown in blue and a node cover is shown in red.

![Figure 8.14: An independent set (left) and a node cover (right)](image)

(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 $(U, F)$ of set cover with $U = \{u_1, \ldots, u_n\}$ and $F = \{S_1, \ldots, S_m\}$, a family of subsets of $U$, we need to produce in polynomial time an instance $\tau(U, F)$ 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 $\mathcal{F}$.

The trick here is the relationship between set union and integer addition.

**Example 8.6.** Consider the exact cover problem given by $U = \{u_1, u_2, u_3, u_4\}$ and

$$\mathcal{F} = \{S_1 = \{u_3, u_4\}, S_2 = \{u_2, u_3, u_4\}, S_3 = \{u_1, u_2\}\}.$$ 

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

$$a_1 = 0011 \quad a_2 = 0111 \quad a_3 = 1100.$$ 

Then, the trick is that some family $\mathcal{C}$ 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,

$$\mathcal{C} = \{S_1 = \{u_3, u_4\}, S_3 = \{u_1, u_2\}\}$$

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

$$S_1 = \{u_3, u_5, u_6\} \quad S_2 = \{u_3, u_4, u_6\} \quad S_3 = \{u_3, u_4, u_5, u_6\} \quad S_4 = \{u_2, u_3\},$$

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 $\mathcal{F}$) instead of base 2.
Example 8.7. 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 \(*\)-free Regular Expressions

To show that Inequivalence of \(*\)-free Regular Expressions is \( \mathcal{NP} \)-complete, we reduce the Satisfiability Problem to it:
8.2. 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 \( w \in L[R] \) we have \( |w| \leq |R| \). The above observation shows that if \( R_1 \) and \( R_2 \) are \(*\)-free and if there is a string \( w \in (L[R_1] - L[R_2]) \cup (L[R_2] - L[R_1]) \), 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

\[
S = (0 + 1)(0 + 1) \cdots (0 + 1)^n.
\]

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

\[
R_i = R_i^1 \cdot R_i^2 \cdots R_i^n,
\]

where \( R_i^j \) is defined by

\[
R_i^j = \begin{cases} 
0 & \text{if } x_j \text{ is a literal of } C_i \\
1 & \text{if } \overline{x}_j \text{ is a literal of } C_i \\
(0 + 1) & \text{if } x_j \text{ does not occur in } C_i.
\end{cases}
\]

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 $NP$.

To prove that the is $NP$-complete we reduce the bounded-tiling problem to it:

bounded-tiling problem $\leq_P$ 0-1 integer programming problem

Given a tiling problem, $((T, V, H), \hat{s}, s_0)$, 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.

8.3 Succinct Certificates, $coNP$, and $EXP$ All the problems considered in Section 8.1 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 $NP$ 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 $NP$ 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 8.3. 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
\[
L = \{ x \in \Sigma^* \mid (\exists y \in \Sigma^*)(x; y \in L') \}.
\]
The intuition is that for each $x \in L$, the set
\[
\{ y \in \Sigma^* \mid x; y \in L' \}
\]
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
\[
L = \{ x \in \Sigma^* \mid (\exists y \in \Sigma^*)(x; y \in L') \}.
\]
The details of this construction are left as an exercise. In summary, we obtain the following theorem.

**Theorem 8.1.** 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
\[
L = \{ x \in \Sigma^* \mid (\exists y \in \Sigma^*)(x; y \in L') \}.
\]

A striking illustration of the notion of succinct 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 $\mathcal{EXP}$.

By definition,
\[
\text{coNP} = \{ L \mid L \in \mathcal{NP} \},
\]
that is, \( \text{coNP} \) consists of all complements of languages in \( \mathcal{NP} \). Since \( \mathcal{P} \subseteq \mathcal{NP} \) and \( \mathcal{P} \) is closed under complementation,

\[ \mathcal{P} \subseteq \text{coNP}, \]

but nobody knows whether \( \mathcal{NP} \) is closed under complementation, that is, nobody knows whether \( \mathcal{NP} = \text{coNP} \).

What can be shown is that if \( \mathcal{NP} \neq \text{coNP} \) then \( \mathcal{P} \neq \mathcal{NP} \). However it is possible that \( \mathcal{P} = \mathcal{NP} \) and yet \( \mathcal{NP} = \text{coNP} \), although this is considered unlikely.

Of course, \( \mathcal{P} \subseteq \mathcal{NP} \cap \text{coNP} \). There are problems in \( \mathcal{NP} \cap \text{coNP} \) not known to be in \( \mathcal{P} \).

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 \( \mathcal{NP} \) is clear. To show that **Integer factorization** is in \( \text{coNP} \), we can guess a factorization of \( N \) into distinct factors all greater than \( M \), check that they are prime using the results of Chapter 9 showing that testing primality is in \( \mathcal{NP} \) (even in \( \mathcal{P} \), 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 \( \mathcal{P} \), 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 \( \mathcal{NP} \)-complete or \( \text{coNP} \)-complete, then we would have \( \mathcal{NP} = \text{coNP} \), 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 \( \text{coNP} \) 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 \( \hat{v}(P) = F \). It is obvious that the set of falsifiable propositions is in \( \mathcal{NP} \). Since a proposition \( P \) is valid iff \( P \) is not falsifiable, the **validity (or tautology) problem** \( \text{TAUT} \) for propositions is in \( \text{coNP} \). In fact, \( \text{TAUT} \) is \( \text{coNP} \)-complete; see Papadimitriou [19].

This is easy to prove. Since \( \text{SAT} \) is \( \mathcal{NP} \)-complete, for every language \( L \in \mathcal{NP} \), 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 \( f(x) \in \neg \text{SAT} \), which means that every language \( L \in \text{coNP} \) 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 \( \text{coNP} \)-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 \( \text{coNP} \)-complete can also be used to show the following interesting result.
Proposition 8.2. If a language $L$ is $\text{NP}$-complete, then its complement $\overline{L}$ is $\text{coNP}$-complete.

Proof. By definition, since $L \in \text{NP}$, we have $\overline{L} \in \text{coNP}$. Since $L$ is $\text{NP}$-complete, for every language $L_2 \in \text{NP}$, 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.

The class $\text{EXP}$ is defined as follows.

Definition 8.4. 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 $ID_0 \vdash ID_1 \vdash \ldots \vdash ID_{n-1} \vdash ID_n$, with $n > 2^{p(|x|)}$.

The class $\text{EXP}$ is the class of all languages that are accepted by some exponentially bounded deterministic Turing machine.

Remark: We can also define the class $\text{NEXP}$ as in Definition 8.4, except that we allow nondeterministic Turing machines.

One of the interesting features of $\text{EXP}$ is that it contains $\text{NP}$.

Theorem 8.3. We have the inclusion $\text{NP} \subseteq \text{EXP}$.

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 $2^{q(|x|)}$.

It is also immediate to see that $\text{EXP}$ is closed under complementation. Furthermore the strict inclusion $\text{P} \subset \text{EXP}$ holds.
Theorem 8.4. We have the strict inclusion $\mathcal{P} \subset \mathcal{E}\mathcal{X}\mathcal{P}$.

Sketch of proof. We use a diagonalization argument to produce a language $E$ such that $E \notin \mathcal{P}$, yet $E \in \mathcal{E}\mathcal{X}\mathcal{P}$. We need to code a Turing machine as a string, but this can certainly be done using the techniques of Chapter 2. 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 $E \in \mathcal{E}\mathcal{X}\mathcal{P}$. 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

$$\mathcal{P} \subseteq \mathcal{N}\mathcal{P} \subseteq \mathcal{E}\mathcal{X}\mathcal{P},$$

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

$$\mathcal{P} \subseteq \mathcal{N}\mathcal{P} \subseteq \mathcal{E}\mathcal{X}\mathcal{P} \subseteq \mathcal{N}\mathcal{E}\mathcal{X}\mathcal{P}.$$  

Nobody knows whether $\mathcal{E}\mathcal{X}\mathcal{P} = \mathcal{N}\mathcal{E}\mathcal{X}\mathcal{P}$, but it can be shown that if $\mathcal{E}\mathcal{X}\mathcal{P} \neq \mathcal{N}\mathcal{E}\mathcal{X}\mathcal{P}$, then $\mathcal{P} \neq \mathcal{N}\mathcal{P}$; see Papadimitriou [19].
Chapter 9

Primality Testing is in \( \mathcal{NP} \)

9.1 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 9.1. 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 \( 3215\,031\,751 \) 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 9.1. 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 9.1. 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 9.2.** 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, ..., $n$, since otherwise $p$ would divide $N - n! = 1$, a contradiction. □

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.

### 9.2 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 9.2 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 9.7.

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 countexample. 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

\[
a^{90-1} = 3^{90} \equiv 1 \pmod{91},
\]

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 \( \mathbb{P} \)” 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].
(2) Randomized algorithms. To avoid having problems with infinite events, we assume that we are testing numbers in some large finite interval \( I \). Given any positive integer \( m \in I \), 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 \textit{Monte Carlo} algorithm, which means the following:

(1) \textit{If the test is positive, then} \( m \in I \) \textit{is composite.} In terms of probabilities, this is expressed by saying that the conditional probability that \( m \in I \) is composite given that the test is positive is equal to 1. If we denote the event that some positive integer \( m \in I \) is composite by \( C \), then we can express the above as

\[
\Pr(C \mid \text{test is positive}) = 1.
\]

(2) \textit{If} \( m \in I \) \textit{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 \( m \in I \) is prime, then the test is negative. If we denote by \( P \) the event that some positive integer \( m \in I \) 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 \( \Pr(\text{test is negative} \ell \text{ times} \mid C) \), is given by

\[
\Pr(\text{test is negative} \ell \text{ times} \mid C) = \Pr(\text{test is negative} \mid C)^\ell
= (1 - \Pr(\text{test is positive} \mid C))^\ell
\leq \left(1 - \frac{1}{2}\right)^\ell
= \left(\frac{1}{2}\right)^\ell,
\]

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. \textit{This confirms that if we run the algorithm} \( \ell \text{ times, then} \ \Pr(\text{test is negative} \ell \text{ times} \mid C) \text{ is very small.} \) In other words, it is very unlikely that the test will lie \( \ell \) times (is negative) given that the number \( m \in I \) is composite.
9.3 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 \( I \), 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.

9.3 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 9.2.** 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 9.3.** 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 9.3 allows us to define addition, subtraction, and multiplication on equivalence classes modulo \( m \).

**Definition 9.3.** 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.

<table>
<thead>
<tr>
<th>( n = 2 )</th>
<th>( n = 3 )</th>
<th>( n = 4 )</th>
<th>( n = 5 )</th>
<th>( n = 6 )</th>
<th>( n = 7 )</th>
</tr>
</thead>
<tbody>
<tr>
<td>+</td>
<td>0</td>
<td>1</td>
<td>+</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>0</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
</tr>
<tr>
<td>1</td>
<td>1</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>0</td>
<td>1</td>
<td>2</td>
<td>2</td>
</tr>
<tr>
<td>3</td>
<td>3</td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>4</td>
<td>4</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>5</td>
</tr>
</tbody>
</table>
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 $\bar{a} \bar{b}$ instead of $\bar{a} \cdot \bar{b}$. 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.
Examine 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 9.4.** Given any integer \( n \geq 1 \), for any \( a \in \mathbb{Z} \), the residue class \( \overline{a} \in \mathbb{Z}/n\mathbb{Z} \) is invertible with respect to multiplication iff \( \gcd(a, n) = 1 \).

**Proof.** If \( \overline{a} \) has inverse \( \overline{b} \) in \( \mathbb{Z}/n\mathbb{Z} \), then \( \overline{a} \overline{b} = 1 \), 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 \( \overline{a} \overline{u} = 1 \), so \( \overline{a} \) is invertible in \( \mathbb{Z}/n\mathbb{Z} \). \qed

We have alluded to the notion of a group. Here is the formal definition.

**Definition 9.4.** 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 \( a, b, c \in G \):
\[ \begin{align*}
(G1) \quad & a \cdot (b \cdot c) = (a \cdot b) \cdot c. & \text{(associativity);} \\
(G2) \quad & a \cdot e = e \cdot a = a. & \text{(identity;)}
\end{align*} \]
(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

$$a \cdot b = b \cdot a \text{ for all } a, b \in G.$$ 

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 9.5.** 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 9.6.** 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 9.4 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 accomodate the special case $n = 1$. 
Definition 9.7. If $G$ is a finite group, the number of elements in $G$ is called the *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 9.8.** Given a group $G$ with identity element $e$, for any nonnegative integer $n$, it is natural to define the *power* $g^n$ of $g$ as follows:

\[
\begin{align*}
g^0 &= e \\
g^{n+1} &= g \cdot g^n.
\end{align*}
\]

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

\[
\begin{align*}
g^i \cdot g^j &= g^{i+j} \\
(g^i)^{-1} &= g^{-i} \\
g^i \cdot g^j &= g^j \cdot g^i
\end{align*}
\]

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 9.5.** 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 $m$. 

9.3. 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 

$$e = a^i(a^i)^{-1} = a^2(a^i)^{-1} = a^ia^{-i} = a^{j-i}.$$ 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

$$a^i a^j = a^{i+j} = a^{sq + r} = a^{sq}a^r = (a^s)^qa^r = e^qa^r = a^r,$$

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

$$a^i \langle a \rangle = \langle a \rangle.$$ 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 $m$. 

$\square$
Definition 9.9. 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 9.5 is called the order of $a$.

For any integer $n \geq 2$, let $(\mathbb{Z}/n\mathbb{Z})^\ast$ be the group of invertible elements of the ring $\mathbb{Z}/n\mathbb{Z}$. This is a group of order $\varphi(n)$. Then Proposition 9.5 yields the following result.

Theorem 9.6. (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 9.7. (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 $200^{250} \equiv 1 \pmod{251}$, without making any computations.

Proposition 9.5 suggests considering groups of the form $\langle g \rangle$.

Definition 9.10. 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 $(\mathbb{Z}/p\mathbb{Z})^\ast$ is a cyclic group when $p$ is prime, but no efficient method for finding a generator for $(\mathbb{Z}/p\mathbb{Z})^\ast$ is known (besides a brute-force search).

Examining the multiplication tables for $(\mathbb{Z}/n\mathbb{Z})^\ast$ for $n = 3, 4, \ldots, 9$, we can check the following facts:

1. 2 is a generator for $(\mathbb{Z}/3\mathbb{Z})^\ast$.
2. 3 is a generator for $(\mathbb{Z}/4\mathbb{Z})^\ast$.
3. 2 is a generator for $(\mathbb{Z}/5\mathbb{Z})^\ast$.
4. 5 is a generator for $(\mathbb{Z}/6\mathbb{Z})^\ast$.
5. 3 is a generator for $(\mathbb{Z}/7\mathbb{Z})^\ast$.
6. Every element of $(\mathbb{Z}/8\mathbb{Z})^\ast$ satisfies the equation $a^2 = 1 \pmod{8}$, thus $(\mathbb{Z}/8\mathbb{Z})^\ast$ has no generators.
7. 2 is a generator for $(\mathbb{Z}/9\mathbb{Z})^\ast$. 
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 9.11.** 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 9.8.** *(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* \(p\).

### 9.4 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 \(2\log_2^2 n\).

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 that or equal to \(x\), and the *ceiling of* \(x\) is the least integer \([x]\) that is greater that 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

\[
\log_2 x = \frac{\ln 10}{\ln 2} \ln_{10} x.
\]

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.
Since the Lucas test yields a tree such that the number of modular multiplications involved in checking the congruences is bounded by $2 \log^2_2 n$, 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 9.9. (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 9.6),

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

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 9.10. 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:

1. $a^{(n-1)/2} \equiv -1 \pmod{n}$.
2. 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 9.10 hold. Then we claim that Conditions (1) and (2) of Theorem 9.9 hold. By squaring the congruence $a^{(n-1)/2} \equiv -1 \pmod{n}$, we get $a^{n-1} \equiv 1 \pmod{n}$, which is Condition (1) of Theorem 9.9. Since $a^{(n-1)/2} \equiv -1 \pmod{n}$, Condition (2) of Theorem 9.9 holds for $q = 2$. Next, if $q$ is an odd prime divisor of $n - 1$, let $m = a^{(n-1)/2q}$. Condition (1b) means that $m^q \equiv a^{(n-1)/2} \equiv -1 \pmod{n}$.

Now if $m^2 \equiv a^{(n-1)/q} \equiv 1 \pmod{n}$, since $q$ is an odd prime, we can write $q = 2k + 1$ for some $k \geq 1$, and then

$$m^q \equiv m^{2k+1} \equiv (m^2)^k m \equiv 1^k m \equiv m \pmod{n},$$

and since $m^q \equiv -1 \pmod{n}$, we get

$$m \equiv -1 \pmod{n}$$

(regardless of whether $n$ is prime or not). Thus we proved that if $m^q \equiv -1 \pmod{n}$ and $m^2 \equiv 1 \pmod{n}$, then $m \equiv -1 \pmod{n}$. By contrapositive, we see that if $m \not\equiv -1 \pmod{n}$, then $m^2 \not\equiv 1 \pmod{n}$ or $m^q \not\equiv -1 \pmod{n}$, but since $m^q \equiv a^{(n-1)/2} \equiv -1 \pmod{n}$ by Condition (1a), we conclude that $m^q \equiv a^{(n-1)/q} \not\equiv 1 \pmod{n}$, which is Condition (2) of Theorem 9.9. But then, Theorem 9.9 implies that $n$ is prime.

Conversely, assume that $n$ is an odd prime, and let $a$ be any primitive root modulo $n$. Then by little Fermat we know that

$$a^{n-1} \equiv 1 \pmod{n},$$

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. \qed
If \( n \) is an odd prime, we can use Theorem 9.10 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 9.1.** 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 numbers 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:

\[
\begin{align*}
(1279, ((2, 1), (3, 2), (71, 1)), 3) \\
(3, ((2, 1)), 2) & \rightarrow (71, ((2, 1), (5, 1), (7, 1)), 7) \\
(5, ((2, 2)), 2) & \rightarrow (7, ((2, 1), (3, 1)), 3) \\
& \quad \downarrow \quad \downarrow \\
& \quad (3, ((2, 1)), 2)
\end{align*}
\]

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

\[
\begin{align*}
3^{1278/2} & \equiv 3^{864} \equiv -1 \pmod{1279} \quad (1b) \\
3^{1278/(2 \cdot 3)} & \equiv 3^{213} \equiv 775 \pmod{1279} \quad (2b) \\
3^{1278/(2 \cdot 71)} & \equiv 3^9 \equiv 498 \pmod{1279}. \quad (2b)
\end{align*}
\]
Assuming that 3 and 71 are prime, the above congruences check that Conditions (1a) and (2b) are satisfied, and by Theorem 9.10 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 9.12.** 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 9.12 are Conditions (1b) and (2b) of Theorem 9.10, we see that Definition 9.12 has been designed in such a way that Theorem 9.10 yields the following result.

**Theorem 9.11.** 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 \( x^n \mod n \) in polynomial time in \( \log_2 n \). This is the object of the next section.

### 9.5 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 \( 999^{179} \mod 1763 \). 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 repeated squaring method.

An Algorithm to Compute $x^n \mod m$ 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.

9.6 PRIMES is in $\mathcal{NP}$

Exponentiation modulo $n$ can performed by repeated squaring, as explained in Section 9.5. 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.

**Proposition 9.12.** 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 \( p - 1 = 2^{i_0} \), then any Lucas tree has a single node, and \( 1 < \log_2 3 < \log_2 p \). If \( p - 1 \) has the prime factorization \( p - 1 = 2^{i_0} q_1^{i_1} \cdots q_k^{i_k} \),

then by the induction hypothesis, each pre-Lucas tree \( L_j \) for \( q_j \) has less than \( \log_2 q_j \) nodes, so

\[
N(p) = 1 + \sum_{j=1}^{k} N(q_j) < 1 + \sum_{j=1}^{k} \log_2 q_j = 1 + \log_2 (q_1 \cdots q_k) \leq 1 + \log_2 \left( \frac{p - 1}{2} \right) < \log_2 p,
\]

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, \( a^{(q-1)/2r} \not\equiv -1 \pmod q \) 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. \( \square \)

The following impressive example is from Pratt [21].

**Example 9.2.** Let \( n = 474397531 \). It is easy to check that \( n - 1 = 474397531 - 1 = 474397530 = 2 \cdot 3 \cdot 5 \cdot 251^3 \). We claim that the following is a Lucas tree for \( n = 474397531 \):

\[
(474397531, ((2, 1), (3, 1), (5, 1), (251, 3)), 2) \rightarrow (3, ((2, 1)), 2) \rightarrow (5, ((2, 2)), 2) \rightarrow (251, ((2, 1), (5, 3)), 6) \rightarrow (5, ((2, 2)), 2)
\]
To verify that the above pre-Lucas tree is a Lucas tree, we check that 2 is indeed a primitive root modulo 474,397,531 by computing (using Mathematica) that
\[ 2^{474,397,530}/2 \equiv 2^{237,198,765} \equiv -1 \pmod{474,397,531} \] (1)
\[ 2^{474,397,530}/(2 \cdot 3) \equiv 2^{79,066,255} \equiv 9,583,569 \pmod{474,397,531} \] (2)
\[ 2^{474,397,530}/(2 \cdot 5) \equiv 2^{47,439,753} \equiv 91,151,207 \pmod{474,397,531} \] (3)
\[ 2^{474,397,530}/(2 \cdot 251) \equiv 2^{945,015} \equiv 282,211,150 \pmod{474,397,531} \] (4)

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:
\[ 6^{250}/2 \equiv 6^{125} \equiv -1 \pmod{251} \] (5)
\[ 6^{250}/(2 \cdot 5) \equiv 6^{10} \equiv 175 \pmod{251} \] (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, 474,397,531 is prime.

As nice as it is, Proposition 9.12 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 9.9, instead of the improved version, Theorem 9.10, so his proof trees have at least twice as many nodes as ours.

As nice as it is, Proposition 9.12 is deceiving, because finding a Lucas tree is hard.

The following nice result was first shown by V. Pratt in 1975 [21].

Theorem 9.13. The problem PRIMES (testing whether an integer is prime) is in NP.
Proof. Since all even integers besides 2 are composite, we can restrict out attention to odd integers \( n \geq 3 \). By Theorem 9.11, 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 9.12, checking that it is a Lucas tree can be done in \( O(\log^2_2 n) \). 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 \( \varphi(\varphi(p)) \). 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 9. PRIMALITY TESTING IS IN $\mathcal{NP}$
Bibliography


Symbol Index

(MN), 85
M[ϕ], 89
[x₁ := N₁, ..., xₙ := Nₙ], 88
←→₂β, 90
→₂β, 90
λx. M, 85
←₂β, 90
→₂β, 90
→₂β, 90
Index

α-conversion, 89
    immediate, 89
α-reduction, 89
    immediate, 89
β-conversion, 90
β-redex, 90
β-reduction, 90
    immediate, 90
λ-abstraction, 85
λ-calculus, 85
    pure, 85
    untyped, 85
λ-term
    closed, 87
    raw simply-typed, 85
application, 85
combinator, 87
congruent, 205

modular arithmetic, 205, 206

redex, 90
repeated squaring, 220

substitution, 88

type, 111
    second order, 111
    polymorphic, 111

variable, 85
    bound, 87
    capture, 89
    free, 87