TWIN Bachelor Thesis

Hilbert's Tenth Problem

AUTHOR
Jessy Musoko

SUPERVISOR
Jaap van Oosten

Universiteit Utrecht

July 25, 2015

Contents

History and Statement of the Tenth Problem

Most of this introductory chapter is based on [10, 12, 5, 2].

Mathematical logic of the 19th century came to its climax with the consecutive holding of the *First International Congress of Philosophy* and the *Second International Congress of Mathematicians* in Paris, August 1900. At the Second Congress of Mathematicians, David Hilbert, one of the greatest mathematicians of his time, was one of the invited lecturers. In his lecture, he presented to the mathematics community a total of ten of the —in his opinion— most important open problems in mathematics at that time. Later that year, he officially published a list of twenty three problems (including the ones from his lecture) in [6]; these problems have become famously known as *Hilbert's Problems*.

Hilbert's problems have greatly influenced the development of mathematics throughout the 20th century. In particular, they greatly stimulated the development of mathematical logic for decades to come, partly because the first two problems on Hilbert's list (below) are directly about logic:

1. Settle the Continuum Hypothesis, i.e. prove or disprove the existence of a set X with cardinality $|\mathbb{N}| < |X| < |\mathbb{R}|$.

2. Prove that the axioms of arithmetic are consistent, i.e. free of contradiction.

Until the conferences in 1900, one could say that mathematical logic lacked academic recognition in some sense as none of the 19th century logicians held major positions at first-rank universities: for example, Frege and Cantor remained at provincial universities, Peirce never obtained a permanent university position and Dedekind was a high school teacher.

As of this writing, a total of ten of Hilbert's problems have been resolved with a definite answer (including the 10th problem) and four remain unresolved (including the 8th problem, which asks to settle the infamous Riemann Hypothesis); the remaining problems are either partially resolved, too vaguely stated to ever be resolved, or only resolved in certain interpretations of the problem.

The Tenth Problem

In this thesis, we present a full analysis of the 10th problem on Hilbert's list. Many of the problems were quite lengthy in their description and filled one or even multiple pages, but not the 10th problem; it is short enough to restate here in its entirety.

An English translation[1] of Hilbert's problems was first published in [7] in 1902. In this translation, the 10th problem reads as follows.

[1] The problems were first published by Hilbert in [6] in 1900 (in German). Here, the 10th problem reads: "**10. Entscheidung der Lösbarkeit einer Diophantischen Gleichung.** Eine Diophantische Gleichung mit

> **10. Determination of the Solvability of a Diophantine Equation.** Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: *to devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers.*

Let us carefully analyze Hilbert's terminology.

By a *Diophantine equation*, Hilbert meant an equation of the form $F(x_1, \dots, x_m) = 0$, where F is some polynomial with integer coefficients. Examples of Diophantine equations include Pell's equation $x^2 - dy^2 = 1$, where $d > 0$ is a positive non-square integer, and Fermat's equation $x^n + y^n = z^n$, where $n > 2$ is a positive integer.

Because Hilbert speaks of *rational integral numericals* and *rational integrals*, one may think that Hilbert had in mind Diophantine equations with coefficients and solutions in $\mathbb{Q}$, but this is not the case. Hilbert meant nothing more than the familiar integers $\mathbb{Z}$ in both cases. This makes the phrase "*Given a Diophantine equation* [...] *with rational integral coefficients*" pleonastic.

Lastly, Hilbert speaks of *a process according to which it can be determined by a finite number of operations whether* [...]. In modern terminology, such a process would be called an *algorithm*, which leads us to the following modern interpretation of the 10th problem.

> **10. Determination of the Solvability of a Diophantine Equation. [Modernized]** Construct an algorithm which, when given an arbitrary Diophantine equation, determines in a finite number of steps whether the given equation is solvable over $\mathbb{Z}$.

Before Hilbert's lecture at the conference, number theorists have studied the solvability of Diophantine equations since the time of Greek mathematician Diophantus (3rd century) himself. Many (classes of) Diophantine equations had already been proven to be unsolvable over $\mathbb{Z}$, but Hilbert put the 10th problem on his list because he was interested in a *universal* process for determining the solvability of *arbitrary* Diophantine equations.

Note that our modern interpretation still uses the —at this point— informal notion of "algorithm".

Algorithm

Most mathematicians have an intuitive feeling for what an algorithm is, partly due to the increasing importance of computers in most people's everyday lives. Most would agree that an algorithm is something like a finite list of instructions which, at least, satisfies the following requirements[2].

> **Definiteness.** The algorithm's output should be completely determined by a finite amount of initial information (the input). No secret information is attained during its computation.

> **Discreteness.** The algorithm advances in discrete computation steps. At each step, the algorithm is only allowed to use information which has already been calculated in previous steps.

irgend welchen Unbekannten und mit ganzen rationalen Zahlencoefficienten sei vorgelegt: *man soll ein Verfahren angeben, nach welchem sich mittelst einer endlichen Anzahl von Operationen entscheiden läßt, ob die Gleichung in ganzen rationalen Zahlen lösbar ist.*"

[2] taken directly from [2]

Repeatability. No matter how many times the algorithm is repeated on the same input, it will always produce the same output.

Termination. The algorithm is only allowed to terminate (i.e. reach an output) after a finite number of discrete computation steps. At any point, we should be able to tell whether the algorithm has terminated or not; if it has, we should be able to read its output.

This intuitive understanding of algorithm has existed with mathematicians throughout the centuries. Think, for example, of Euclid's Algorithm which computes the greatest common divisor function. This algorithm could be represented as the following scheme.

```
0 : Ask for natural numbers $a > 0$ and $b$. Then go to line 1.
1 : If $b = 0$, go to line 5. If $b > 0$, go to line 2.
2 : If $a > b$, go to line 3. If $a \leq b$, go to line 4.
3 : Redefine $a := a - b$. Then go to line 2.
4 : Redefine $b := b - a$. Then go to line 1.
5 : Output $a$. Then terminate.
```

As an example computation, we can consider the above algorithm on input $(a, b) = (21, 63)$. Since $b > 0$ and $a \leq b$, we must redefine $b := b - a = 42$ and return to line 1 with $(a, b) = (21, 42)$. This is repeated until we arrive at line 1 with $(a, b) = (21, 0)$, in which case the instruction on line 5 is executed. The algorithm then outputs 21, which is exactly the number $\gcd(21, 63)$. Informally, this makes the greatest common divisor function $\gcd : \mathbb{N}^2 \to \mathbb{N}$ an example of an *algorithmically computable function*, i.e. a function for which a computing algorithm exists.

It wasn't until the 1930's when formalizations of this notion of "algorithmically computable function" began to emerge. In 1936, a total of four papers appeared by Church ([1]), Kleene ([8]), Post ([13]) and Turing ([14]), each proposing a way to define the class of computable functions; it was later shown that all four descriptions were in fact equivalent in the sense that they all gave rise to the *same* function class $\mathcal{C}$. Now, it is universally accepted that this class aptly formalizes the mathematical intuition of a computable function. The branch of mathematical logic which studies $\mathcal{C}$ is called *Recursion Theory* or *Computability Theory*; functions of $\mathcal{C}$ are nowadays simply called *recursive* or *(algorithmically) computable.*

The Negative Resolution of the Tenth Problem

Hilbert's 10th problem was solved with a negative answer by Russian mathematician Yuri Matiyasevich in 1970 at the young age of 22, building upon earlier work from the 1950's and 1960's by American logicians Martin Davis, Hilary Putnam and Julia Robinson. He managed to prove what is now known as the *Davis-Putnam-Robinson-Matiyasevich Theorem* (also: *DPRM Theorem* or *Matiyasevich's Theorem*, cf. Theorem 4.1) from which it follows that a universal algorithm, which determines the solvability of arbitrary Diophantine equations, cannot exist.

In the year 2000, Matiyasevich gave a series of lectures at the University of Calgary (Canada) in which he described his resolution of the 10th problem. These lectures have been transcribed into the very readable document [10] on which most of this thesis is based.

Chapter 1

(Exponential) Diophantine Sets

Let us write $\mathbb{N}[X_1, \ldots, X_n]$ for the class of polynomials in n variables with *nonnegative* integer coefficients; it can be defined inductively as the smallest class with the following properties

(P1) The constant polynomials $(x_1, \ldots, x_n) \mapsto 0$ and $(x_1, \ldots, x_n) \mapsto 1$ are contained.

(P2) The projections $(x_1, \ldots, x_n) \mapsto x_i$ are contained for all $i \in \{1, \ldots, n\}$.

(P3) Closure under addition and multiplication: if P and Q are contained, then so are

$$(x_1, \ldots, x_n) \mapsto P(x_1, \ldots, x_n) + Q(x_1, \ldots, x_n)$$

and

$$(x_1, \ldots, x_n) \mapsto P(x_1, \ldots, x_n) \cdot Q(x_1, \ldots, x_n)$$

We are also interested in the following bigger polynomial classes: the class $\mathbb{Z}[X_1, \ldots, X_n]$ of polynomials with *integer* coefficients and the class $\mathbb{N}^*[X_1, \ldots, X_n]$ of *exponential* polynomials with nonnegative integer coefficients. They can be defined as follows.

- The class $\mathbb{Z}[X_1, \ldots, X_n]$ of polynomials in n variables with *integer* coefficients is the smallest class such that (P1), (P2) and (P3) are satisfied, together with the property

  (P4) Closure under subtraction: if P and Q are contained in $\mathbb{Z}[X_1, \ldots, X_n]$, then so is

  $$(x_1, \ldots, x_n) \mapsto P(x_1, \ldots, x_n) - Q(x_1, \ldots, x_n)$$

- The class $\mathbb{N}^*[X_1, \ldots, X_n]$ of *exponential* polynomials in n variables with nonnegative integer coefficients is the smallest class such that (P1), (P2) and (P3) are satisfied, together with the property

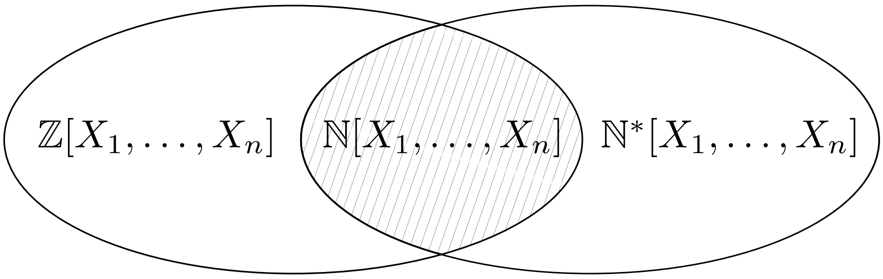
  (P5) Closure under exponentiation: if P and Q are contained in $\mathbb{N}^*[X_1, \ldots, X_n]$, then so is

  $$(x_1, \ldots, x_n) \mapsto P(x_1, \ldots, x_n)^{Q(x_1, \ldots, x_n)}$$

  Throughout this thesis, the number 0^0 shall be treated as 1.

Below are some example polynomials, together with a Venn diagram of these different classes.

$\mathbb{N}[X_1, X_2, X_3]$	$\mathbb{Z}[X_1, X_2, X_3]$	$\mathbb{N}^*[X_1, X_2, X_3]$
$(x, y, z) \mapsto 4xy^7z + 2x$	$(x, y, z) \mapsto 2 - 3y$	$(x, y, z) \mapsto 6^x yz + y^2 + 3$
$(x, y, z) \mapsto (2x + y^3)^{99} + 1$	$(x, y, z) \mapsto (1 - 3xy)^3 - 81y^2z - 3$	$(x, y, z) \mapsto 5 \cdot 2^x y^{(x+3y^2)^{14z}}$


$\mathbb{Z}[X_1, \ldots, X_n]$
$\mathbb{N}[X_1, \ldots, X_n]$
$\mathbb{N}^*[X_1, \ldots, X_n]$

Venn-diagram of the different classes of polynomials.

Evidently, each of the classes $\mathbb{N}[X_1, \ldots, X_n]$, $\mathbb{Z}[X_1, \ldots, X_n]$ and $\mathbb{N}^*[X_1, \ldots, X_n]$ is closed under composition. For example, if the polynomials P and $Q_1, \ldots, Q_n$ all belong to $\mathbb{N}[X_1, \ldots, X_n]$, then the composition function

$$(x_1, \ldots, x_n) \mapsto P(Q_1(x_1, \ldots, x_n), \ldots, Q_n(x_1, \ldots, x_n))$$

belongs to $\mathbb{N}[X_1, \ldots, X_n]$ as well.

Remark. Let F denotes some polynomial in n variables; then the variables $x_1, \ldots, x_n$ in an equation like $F(x_1, \ldots, x_n) = 0$ are always constrained to a certain specified domain. For example, if F denotes the polynomial $(x, y) \mapsto x^2 + y^2 + 1$, then $F(x, y) = 0$ is unsolvable over $\mathbb{Z}$, while it has uncountably many solutions over $\mathbb{C}$. ♦

Definition 1.1. An equation is called *Diophantine* if it is of the form

$$F(x_1, \ldots, x_n) = 0$$

for some $F \in \mathbb{Z}[X_1, \ldots, X_n]$. A Diophantine equation is said to be *solvable* if it is solvable over $\mathbb{Z}$. ♦

Given some polynomial $F \in \mathbb{Z}[X_1, \ldots, X_{k+m}]$, we can consider the problem of determining the solvability the single Diophantine equation

$$F(x_1, \ldots, x_{k+m}) = 0$$

in the variables $x_1, \ldots, x_{k+m}$. However, we can also consider the *family*

$$F(a_1, \ldots, a_k, x_1, \ldots, x_m) = 0 \tag{1.1}$$

of Diophantine equations in the variables $x_1, \ldots, x_m$, where the integers $a_1, \ldots, a_k$ are thought of as *parameters*. The problem, then, is to determine for which choice of parameters $a_1, \ldots, a_k \in \mathbb{Z}$ the Diophantine equation (1.1) is solvable. Diophantine sets are exactly characterized by this idea.

Definition 1.2. Let $A \subseteq \mathbb{N}^k$ be a set. Then A is said to be a *Diophantine* set if there exists some $F \in \mathbb{Z}[X_1, \ldots, X_{k+m}]$ such that A contains exactly those nonnegative parameters for which the Diophantine equation $F = 0$ is solvable, i.e. such that

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \exists x_1 \cdots x_m \in \mathbb{Z}\big(F(a_1, \ldots, a_k, x_1, \ldots, x_m) = 0\big)\}$$

Here, the notation $\exists x_1 \cdots x_m \in \mathbb{Z}(f(x_1, \ldots, x_m) = 0)$ expresses "there is a sequence $x_1, \ldots, x_m$ of integers, such that $f(x_1, \ldots, x_m) = 0$". ♦

Below are some examples of Diophantine sets.

- The set $\{n \in \mathbb{N} \mid \exists x \in \mathbb{Z}(n - x^2 = 0)\}$ of squares.
- The set $\{n \in \mathbb{N} \mid \exists x \in \mathbb{Z}(n - (2x + 1) = 0)\}$ of odd numbers.
- The set $\{(a, b, c) \in \mathbb{N}^3 \mid a^2 + b^2 = c^2\}$ of Pythagorean triples.

If $A \subseteq \mathbb{N}^k$ is a Diophantine set, then, by definition, we have to determine the solvability of some Diophantine equation

$$F(a_1, \ldots, a_k, x_1, \ldots, x_m) = 0$$

over the integers in order to find out whether some given tuple $(a_1, \ldots, a_k)$ lies in A. In this light, one could say that

> "finding an algorithm to determine the solvability of Diophantine equations"

is in some way equivalent to

> "finding an algorithm for determining the membership of tuples of natural numbers in Diophantine sets"

even though we haven't given a definition of "algorithm" yet.

Many times, it will be more convenient to consider the solvability of equations of the form

$$P(a_1, \ldots, a_k, x_1, \ldots, x_m) = Q(a_1, \ldots, a_k, x_1, \ldots, x_m)$$

over $\mathbb{N}$, where $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+m}]$. For this reason we state Theorem 1.4, which says that Diophantine sets can also be characterized by the solvability of such equations over $\mathbb{N}$. Before we prove it, however, we have the following technical lemma.

Lemma 1.3. *Let $F \in \mathbb{Z}[X_1, \ldots, X_{k+m}]$ be some polynomial with integer coefficients.*

a) There is a $G \in \mathbb{Z}[X_1, \ldots, X_{k+\ell}]$ such that

$$\exists z_1 \cdots z_m \in \mathbb{Z}\big(F(a_1, \ldots, a_k, z_1, \ldots, z_m) = 0\big)$$
$$\Longleftrightarrow$$
$$\exists x_1 \cdots x_\ell \in \mathbb{N}\big(G(a_1, \ldots, a_k, x_1, \ldots, x_\ell) = 0\big)$$

holds for all $a_1, \ldots, a_k \in \mathbb{N}$.

b) There is a $G \in \mathbb{Z}[X_1, \ldots, X_{k+\ell}]$ such that

$$\exists x_1 \cdots x_m \in \mathbb{N}\big(F(a_1, \ldots, a_k, x_1, \ldots, x_m) = 0\big)$$
$$\Longleftrightarrow$$
$$\exists z_1 \cdots z_\ell \in \mathbb{Z}\big(G(a_1, \ldots, a_k, z_1, \ldots, z_\ell) = 0\big)$$

holds for all $a_1, \ldots, a_k \in \mathbb{N}$.

Proof. Let $F \in \mathbb{Z}[X_1, \ldots, X_{k+m}]$ and write $\vec{a}$ for some arbitrary tuple $(a_1, \ldots, a_k) \in \mathbb{N}^k$.

For part a), define the function G by

$$G : (\vec{v}, x_1, \ldots, x_m, y_1, \ldots, y_m) \mapsto F(\vec{v}, x_1 - y_1, \ldots, x_m - y_m)$$

where $\vec{v} = (v_1, \ldots, v_k)$. Then it is easily seen that $G \in \mathbb{Z}[X_1, \ldots, X_{k+\ell}]$, where $\ell = 2m$.

Assume that $\exists z_1 \cdots z_m \in \mathbb{Z}\big(F(\vec{a}, z_1, \ldots, z_m) = 0\big)$, i.e. that $F(\vec{a}, z_1, \ldots, z_m) = 0$ for certain $z_1, \ldots, z_m \in \mathbb{Z}$. Because every z_i is of the form $x_i - y_i$ for natural numbers x_i and y_i, there are numbers $x_1, \ldots, x_m, y_1, \ldots, y_m \in \mathbb{N}$ such that $F(\vec{a}, x_1 - y_1, \ldots, x_m - y_m) = 0$, i.e. such that $G(\vec{a}, x_1, \ldots, x_m, y_1, \ldots, y_m) = 0$. So $\exists x_1 \cdots x_\ell \in \mathbb{N}\big(G(\vec{a}, x_1, \ldots, x_\ell) = 0\big)$.

Conversely, assume that $\exists x_1 \cdots x_\ell \in \mathbb{N}\big(G(\vec{a}, x_1, \ldots, x_\ell) = 0\big)$, i.e. that $G(\vec{a}, x_1, \ldots, x_\ell) = 0$ for certain $x_1, \ldots, x_\ell \in \mathbb{N}$. Define the integers z_i by $z_i = x_i - x_{m+i}$. Then $F(\vec{a}, z_1, \ldots, z_m) = 0$ by definition of G, showing that $\exists z_1 \cdots z_m \in \mathbb{Z}\big(F(\vec{a}, z_1, \ldots, z_m) = 0\big)$.

For part b), we shall use Lagrange's Squares Theorem[1] which states that every natural number can be written as the sum of four squares. Define the function G by

$$G : (\vec{v}, x_1, x_1', x_1'', x_1''', x_1'''', \ldots, x_m, x_m', x_m'', x_m''', x_m'''') \mapsto$$
$$F(\vec{v}, x_1, \ldots, x_m)^2 + \sum_{i=1}^{m} \big(x_i - (x_i')^2 - (x_i'')^2 - (x_i''')^2 - (x_i'''')^2)\big)^2$$

where $\vec{v} = (v_1, \ldots, v_k)$. Then it is easily seen that $G \in \mathbb{Z}[X_1, \ldots, X_{k+\ell}]$, where $\ell = 4m$.

Assume that $\exists x_1 \cdots x_m \in \mathbb{N}\big(F(\vec{a}, x_1, \ldots, x_m) = 0\big)$, i.e. that $F(\vec{a}, x_1, \ldots, x_m) = 0$ for certain $x_1, \ldots, x_m \in \mathbb{N}$. By Lagrange's Squares Theorem, every x_i is of the form $(x_i')^2 + (x_i'')^2 + (x_i''')^2 + (x_i'''')^2$ for certain $x_i', x_i'', x_i''', x_i'''' \in \mathbb{N}$. So, it follows that these numbers $x_1, x_1', x_1'', x_1''', x_1'''', \ldots, x_m, x_m', x_m'', x_m''', x_m'''' \in \mathbb{N} \subseteq \mathbb{Z}$ satisfy

$$G(\vec{a}, x_1, x_1', x_1'', x_1''', x_1'''', \ldots, x_m, x_m', x_m'', x_m''', x_m'''') = 0$$

and we see that $\exists z_1 \cdots z_\ell \in \mathbb{Z}\big(G(\vec{a}, z_1, \ldots, z_\ell) = 0\big)$.

Conversely, assume that $\exists z_1 \cdots z_\ell \in \mathbb{Z}\big(G(\vec{a}, z_1, \ldots, z_\ell) = 0\big)$, i.e. that $G(\vec{a}, z_1, \ldots, z_\ell) = 0$ for certain $z_1, \ldots, z_\ell \in \mathbb{Z}$. By definition of G, there are integers $x_1, \ldots, x_m$ among these numbers $z_1, \ldots, z_\ell$ such that $F(\vec{a}, x_1, \ldots, x_m)$ and such that every x_i is the sum of four squares, implying that every x_i is nonnegative. We conclude that $\exists x_1 \cdots x_m \in \mathbb{N}\big(F(\vec{a}, x_1, \ldots, x_m) = 0\big)$.

∎

Now we can now easily give the promised equivalent characterization of Diophantine sets.

Theorem 1.4. *Let $A \subseteq \mathbb{N}^k$ be a set. Then A is Diophantine if and only if there exist some $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+\ell}]$ such that*

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \exists x_1 \cdots x_\ell \in \mathbb{N}\big(P(a_1, \ldots, a_k, x_1, \ldots, x_\ell) = Q(a_1, \ldots, a_k, x_1, \ldots, x_\ell)\big)\}$$

Proof. Let $A \subseteq \mathbb{N}^k$ be a set.

If A is Diophantine, there is, by Definition 1.2, some $F \in \mathbb{Z}[X_1, \ldots, X_{k+m}]$ such that

$$(a_1, \ldots, a_k) \in A \iff \exists z_1 \cdots z_m \in \mathbb{Z}\big(F(a_1, \ldots, a_k, z_1, \ldots, z_m) = 0\big)$$

It then follows from part a) of Lemma 1.3 that there is some $G \in \mathbb{Z}[X_1, \ldots, X_{k+\ell}]$ such that

$$(a_1, \ldots, a_k) \in A \iff \exists x_1 \cdots x_\ell \in \mathbb{N}\big(G(a_1, \ldots, a_k, x_1, \ldots, x_\ell) = 0\big) \tag{1.2}$$

[1] a proof can be found in the appendix

We will now show that G must be of the form $P - Q$ for certain $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+\ell}]$, by induction[2] on the class $\mathbb{Z}[X_1, \ldots, X_{k+\ell}]$.

If G is equal to the zero or unit polynomial, or if G is one of the projections $(x_1, \ldots, x_{k+\ell}) \mapsto x_i$, we can simply let $P = G$ and $Q = 0$. Then $G = P - Q$ and $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+\ell}]$.

If G is of the form $G_1 + G_2$ or $G_1 \cdot G_1$ or $G_1 - G_2$, we may assume, by induction, that there are $P_1, Q_1, P_2, Q_2 \in \mathbb{N}[X_1, \ldots, X_{k+\ell}]$ such that $G_1 = P_1 - Q_1$ and $G_2 = P_2 - Q_2$. If $G = G_1 + G_2$, define $P = P_1 + P_2$ and $Q = Q_1 + Q_2$; then $G = P - Q$ and $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+\ell}]$. If $G = G_1 \cdot G_2$, define $P = P_1 \cdot P_2 + Q_1 \cdot Q_2$ and $Q = P_1 \cdot Q_2 + Q_2 \cdot P_1$; then $G = P - Q$ and $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+\ell}]$. Lastly, if $G = G_1 - G_2$, let $P = P_1 + Q_2$ and $Q = P_2 + Q_1$; then $G = P - Q$ and $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+\ell}]$.

It follows that our function G from (1.2) is of the form $P - Q$ for certain $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+\ell}]$. So, by (1.2), A is of the form

$$\{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \exists x_1 \cdots x_\ell \in \mathbb{N}\big(P(a_1, \ldots, a_k, x_1, \ldots, x_\ell) = Q(a_1, \ldots, a_k, x_1, \ldots, x_\ell)\big)\}$$

For the converse, *assume* that A is of the form above; we show that A must be Diophantine. To begin, we have that

$$\begin{aligned}(a_1, \ldots, a_k) \in A &\iff \exists x_1 \cdots x_\ell \in \mathbb{N}\big(P(a_1, \ldots, a_k, x_1, \ldots, x_\ell) = Q(a_1, \ldots, a_k, x_1, \ldots, x_\ell)\big)\\ &\iff \exists x_1 \cdots x_\ell \in \mathbb{N}\big(F(a_1, \ldots, a_k, x_1, \ldots, x_\ell) = 0\big)\end{aligned}$$

where $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+\ell}]$ and where F is defined as $F = P - Q$ so that $F \in \mathbb{Z}[X_1, \ldots, X_{k+\ell}]$.

Then, by part b) of Lemma 1.3, there is some $G \in \mathbb{Z}[X_1, \ldots, X_{k+m}]$ such that

$$(a_1, \ldots, a_k) \in A \iff \exists z_1 \cdots z_m \in \mathbb{Z}\big(G(a_1, \ldots, a_k, z_1, \ldots, z_m) = 0),$$

directly showing that A is Diophantine by Definition 1.2.

∎

Theorem 1.4 shows us that a set $A \in \mathbb{N}^k$ is Diophantine if and only if

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \exists x_1 \cdots x_m \in \mathbb{N}\big(P(a_1, \ldots, a_k, x_1, \ldots, x_m) = Q(a_1, \ldots, a_k, x_1, \ldots, x_m)\big)\}$$

for some $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+m}]$. For this reason, the *exponential* Diophantine sets are defined as follows.

Definition 1.5. Let $A \subseteq \mathbb{N}^k$ be a set. Then A is said to be an *exponential Diophantine* set if there exist some $E, F \in \mathbb{N}^*[X_1, \ldots, X_{k+m}]$ such that

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \exists x_1 \cdots x_m \in \mathbb{N}\big(E(n_1, \ldots, n_k, x_1, \ldots, x_m) = F(n_1, \ldots, n_k, x_1, \ldots, x_m)\big)\}$$

♦

An example of an exponential Diophantine set is the set $\{n \in \mathbb{N} \mid \exists x(n = 2^x)\}$ of powers of 2.

From Theorem 1.4 and the fact that $\mathbb{N}[X_1, \ldots, X_{k+m}]$ is a subclass of $\mathbb{N}^*[X_1, \ldots, X_{k+m}]$, it is easily seen that every Diophantine set is also exponential Diophantine. What is most remarkable, however, is that the converse holds as well: *the classes of Diophantine sets and exponential Diophantine sets coincide!* A sufficient condition for this remarkable assertion is given at the end of the next section; the main part of the proof, however, will occupy a chapter of its own (cf. Chapter 3).

[2] a proof by induction is possible because, as we recall from the first page of this chapter, the class $\mathbb{Z}[X_1, \ldots, X_{k+\ell}]$ is defined inductively as the smallest class of functions (in $k+\ell$ variables) which contains the zero and unit polynomials and all the projections (cf. properties (P1) and (P2)) and which is closed under addition, multiplication and subtraction (cf. properties (P3) and (P4))

1.1 (Exponential) Diophantine Formulas

Definition 1.6. A formula $\varphi(v_1, \ldots, v_k)$, with free variables $v_1, \ldots, v_k$ ranging over $\mathbb{N}$, is said to be *exponential Diophantine* if it is of the form

$$\exists x_1 \cdots x_m \in \mathbb{N}\Big(P(v_1, \ldots, v_k, x_1, \ldots, x_m) = Q(v_1, \ldots, v_k, x_1, \ldots, x_m)\Big) \tag{1.3}$$

for certain $P, Q \in \mathbb{N}^*[X_1, \ldots, X_{k+m}]$. In particular, if P and Q are non-exponential, i.e. if $P, Q \in \mathbb{N}[X_1, \ldots, X_{k+m}]$, then $\varphi(v_1, \ldots, v_k)$ is simply called *Diophantine.*

Moreover, the formula $\varphi(v_1, \ldots, v_k)$ is said to *represent* its corresponding (exponential) Diophantine set $\{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \varphi(a_1, \ldots, a_k)\}$. ♦

Remark 1.7. It follows immediately from Theorem 1.4 that a formula $\varphi(v_1, \ldots, v_k)$ is Diophantine if and only if it is of the form $\exists z_1 \cdots z_m \in \mathbb{Z}\big(F(v_1, \ldots, v_k, z_1, \ldots, z_m) = 0\big)$ for some $F \in \mathbb{Z}[X_1, \ldots, X_{k+m}]$. ♦

Our next goal is to derive some closure properties of the class of (exponential) Diophantine formulas. For example, given (exponential) Diophantine formulas $\varphi_1(v_1, \ldots, v_k)$ and $\varphi_2(v_1, \ldots, v_k)$, we wonder whether these formulas can be connected by logical symbols like "$\wedge$" for conjunction and "$\vee$" for disjunction to create new (exponential) Diophantine formulas. Theorem 1.9 will show us that this is indeed possible; before we prove it, however, we have the following lemma.

Lemma 1.8.

a) Let $P_1, Q_1 \in \mathbb{N}^*[X_1, \ldots, X_{k+m}]$ and $P_2, Q_2 \in \mathbb{N}^*[X_1, \ldots, X_{k+\ell}]$ be exponential polynomials. Then, for all $\vec{v} \in \mathbb{N}^k$, $\vec{x} \in \mathbb{N}^m$ and $\vec{y} \in \mathbb{N}^\ell$, each of the following two formulas

$$P_1(\vec{v}, \vec{x}) = Q_1(\vec{v}, \vec{x}) \wedge P_2(\vec{v}, \vec{y}) = Q_2(\vec{v}, \vec{y})$$
$$P_1(\vec{v}, \vec{x}) = Q_1(\vec{v}, \vec{x}) \vee P_2(\vec{v}, \vec{y}) = Q_2(\vec{v}, \vec{y})$$

is equivalent to a formula of the form

$$P(\vec{v}, \vec{x}, \vec{y}) = Q(\vec{v}, \vec{x}, \vec{y})$$

for certain $P, Q \in \mathbb{N}^*[X_1, \ldots, X_{k+m+l}]$.

Moreover, if all the polynomials P_1, Q_1, P_2 and Q_2 are non-exponential, then P and Q can be assumed to be non-exponential as well.

b) Let $F \in \mathbb{Z}[X_1, \ldots, X_{k+m}]$ and $G \in \mathbb{Z}[X_1, \ldots, X_{k+\ell}]$ be polynomials with integer coefficients. Then, for all $\vec{v} \in \mathbb{Z}^k$, $\vec{x} \in \mathbb{Z}^m$ and $\vec{y} \in \mathbb{Z}^\ell$, each of the following two formulas

$$F(\vec{v}, \vec{x}) = 0 \wedge G(\vec{v}, \vec{y}) = 0$$
$$F(\vec{v}, \vec{x}) = 0 \vee G(\vec{v}, \vec{y}) = 0$$

is equivalent to a formula of the form

$$H(\vec{v}, \vec{x}, \vec{y}) = 0$$

for some $H \in \mathbb{Z}[X_1, \ldots, X_{k+m+\ell}]$.

Proof. For part a), let P_1, Q_1, P_2 and Q_2 be as in the statement. Let $\vec{v} \in \mathbb{N}^k$, $\vec{x} \in \mathbb{N}^m$ and $\vec{y} \in \mathbb{N}^\ell$ be arbitrary. Then

$$\begin{gathered} P_1(\vec{v},\vec{x}) = Q_1(\vec{v},\vec{x}) \wedge P_2(\vec{v},\vec{y}) = Q_2(\vec{v},\vec{y}) \\ \Longleftrightarrow \\ \left(P_1(\vec{v},\vec{x}) - Q_1(\vec{v},\vec{x})\right)^2 + \left(P_2(\vec{v},\vec{y}) - Q_2(\vec{v},\vec{y})\right)^2 = 0 \\ \Longleftrightarrow \\ P_1(\vec{v},\vec{x})^2 + Q_1(\vec{v},\vec{x})^2 + P_2(\vec{v},\vec{y})^2 + Q_2(\vec{v},\vec{y})^2 = 2P_1(\vec{v},\vec{x})Q_1(\vec{v},\vec{x}) + 2P_2(\vec{v},\vec{y})Q_2(\vec{v},\vec{y}) \end{gathered}$$

so we can define $P(\vec{v},\vec{x},\vec{y})$ and $Q(\vec{v},\vec{x},\vec{y})$ as the left hand side and right hand side of the equation above. Then $P, Q \in \mathbb{N}^*[X_1, \ldots, X_{k+m+l}]$, and if P_1, Q_1, P_2 and Q_2 are non-exponential, we easily see that P and Q are non-exponential as well.

The disjunction case is similar, after noting that

$$\begin{gathered} P_1(\vec{v},\vec{x}) = Q_1(\vec{v},\vec{x}) \vee P_2(\vec{v},\vec{y}) = Q_2(\vec{v},\vec{y}) \\ \Longleftrightarrow \\ \left(P_1(\vec{v},\vec{x}) - Q_1(\vec{v},\vec{x})\right) \cdot \left(P_2(\vec{v},\vec{y}) - Q_2(\vec{v},\vec{y})\right) = 0 \\ \Longleftrightarrow \\ P_1(\vec{v},\vec{x})P_2(\vec{v},\vec{y}) + Q_1(\vec{v},\vec{x})Q_2(\vec{v},\vec{y}) = P_1(\vec{v},\vec{x})Q_2(\vec{v},\vec{y}) + Q_1(\vec{v},\vec{x})P_2(\vec{v},\vec{y}) \end{gathered}$$

Part b) of the lemma is proven in a similar way; simply note that $F = 0 \wedge G = 0$ is equivalent to $F^2 + G^2 = 0$ and that $F = 0 \vee G = 0$ is equivalent to $F \cdot G = 0$.

∎

Theorem 1.9. *Both the class of exponential Diophantine formulas and the class of Diophantine formulas is closed under conjunction, disjunction and existential quantifiers over $\mathbb{N}$. Precisely, if $\varphi_1(v_1, \ldots, v_k)$ and $\varphi_2(v_1, \ldots, v_k)$ are (exponential) Diophantine formulas, then the formulas*

$$\begin{gathered} \varphi_1(v_1, \ldots, v_k) \wedge \varphi_2(v_1, \ldots, v_k) \\ \varphi_1(v_1, \ldots, v_k) \vee \varphi_2(v_1, \ldots, v_k) \\ \exists v_1 \in \mathbb{N}\big(\varphi_1(v_1, \ldots, v_k)\big) \end{gathered}$$

are (exponential) Diophantine as well.

Proof. Assume that the formulas $\varphi_1(v_1, \ldots, v_k)$ and $\varphi_2(v_1, \ldots, v_k)$ are (exponential) Diophantine, say of the form

$$\exists x_1 \cdots x_m \in \mathbb{N}\big(P_1(v_1, \ldots, v_k, x_1, \ldots, x_m) = Q_1(v_1, \ldots, v_k, x_1, \ldots, x_m)\big) \tag{φ_1}$$

$$\exists y_1 \cdots y_\ell \in \mathbb{N}\big(P_2(v_1, \ldots, v_k, y_1, \ldots, y_\ell) = Q_2(v_1, \ldots, v_k, y_1, \ldots, y_\ell)\big) \tag{φ_2}$$

for certain (exponential) polynomials $P_1, Q_1 \in \mathbb{N}^*[X_1, \ldots, X_{k+m}]$ and $P_2, Q_2 \in \mathbb{N}^*[X_1, \ldots, X_{k+\ell}]$.

Let us write $\vec{x} = (x_1, \ldots, x_m)$ and $\vec{y} = (y_1, \ldots, y_\ell)$. Then

$$\begin{aligned} \varphi_1(\vec{v}) \wedge \varphi_2(\vec{v}) &\Longleftrightarrow \exists \vec{x} \in \mathbb{N}^m\, (P_1(\vec{v},\vec{x}) = Q_1(\vec{v},\vec{x})) \wedge \exists \vec{y} \in \mathbb{N}^\ell\, (P_2(\vec{v},\vec{y}) = Q_2(\vec{v},\vec{y})) \\ &\Longleftrightarrow \exists \vec{x}\vec{y} \in \mathbb{N}^{m+\ell}\, (P_1(\vec{v},\vec{x}) = Q_1(\vec{v},\vec{x}) \wedge P_2(\vec{v},\vec{y}) = Q_2(\vec{v},\vec{y})) \end{aligned}$$

and similarly

$$\begin{aligned} \varphi_1(\vec{v}) \vee \varphi_2(\vec{v}) &\Longleftrightarrow \exists \vec{x} \in \mathbb{N}^m\, (P_1(\vec{v},\vec{x}) = Q_1(\vec{v},\vec{x})) \vee \exists \vec{y} \in \mathbb{N}^\ell\, (P_2(\vec{v},\vec{y}) = Q_2(\vec{v},\vec{y})) \\ &\Longleftrightarrow \exists \vec{x}\vec{y} \in \mathbb{N}^{m+\ell}\, (P_1(\vec{v},\vec{x}) = Q_1(\vec{v},\vec{x}) \vee P_2(\vec{v},\vec{y}) = Q_2(\vec{v},\vec{y})) \end{aligned}$$

It remains to apply Lemma 1.8 to transform the formulas $P_1 = Q_1 \wedge P_2 = Q_2$ and $P_1 = Q_1 \wedge P_2 = Q_2$ into formulas of the form $P = Q$.

For the existential quantifier case, we see that $\exists v_1 \in \mathbb{N}\big(\varphi_1(v_1, \dots, v_k)\big)$ is equivalent to

$$\exists v_1 x_1 \cdots x_m \in \mathbb{N}\big(P_1(v_1, \dots, v_k, x_1 \dots, x_m) = Q_1(v_1, \dots, v_k, x_1, \dots, x_m)),$$

which surely is (exponential) Diophantine.

∎

Because every (exponential) Diophantine set is of the form $\{(n_1, \dots, n_k) \in \mathbb{N}^k \mid \varphi(n_1, \dots, n_k)\}$ for some (exponential) Diophantine formula φ, the following corollary is immediate.

Corollary 1.10. *Let A_1 and A_2 be subsets of $\mathbb{N}^k$. If they are both Diophantine, then so are $A_1 \cup A_2$ and $A_1 \cap A_2$; if they are both exponential Diophantine, then so are $A_1 \cup A_2$ and $A_1 \cap A_2$.*

Remark 1.11. One might wonder whether the complement of a Diophantine set is Diophantine as well. This assertion only holds in some cases.

Consider, for example, the Diophantine formula $\mathrm{sq}(v)$, given by $\exists x \in \mathbb{N}(v = x^2)$, which represents the set of squares. Because a natural number n is a *not* a square if and only if $z^2 < n < (z+1)^2$ for some $z \in \mathbb{N}$, it follows that

$$\begin{aligned} \neg\, \mathrm{sq}(v) &\iff \exists z \in \mathbb{N}(z^2 < v < (z+1)^2) \\ &\iff \exists xyz \in \mathbb{N}(z^2 + x + 1 = v \wedge v + y + 1 = (z+1)^2) \end{aligned}$$

where this last formula is transformed into a genuine Diophantine formula by applying part a) of Lemma 1.8, showing that both the set of squares and its complement are Diophantine.

The fact that not every Diophantine set has a Diophantine complement is non-trivial, but, anticipating the results of Chapters 2 and 3, we can try to give a hand-waving argument right now. A *computable* set is a subset of $\mathbb{N}^k$ for which there is a computer program which always tells us in finite time whether some given k-tuple belongs to the set. A *computably enumerable* can be seen[3] as a subset of $\mathbb{N}^k$ for which there is a computer program which eventually lists any member of that set if we let the program run 'long enough' (it never lists tuples which don't belong to the set).

Now, if a set A and its complement A^c are both computably enumerable (say their elements are listed by the programs P and P'), one can show that A must be computable. This is seen by constructing a computer program which combines P and P' and runs them 'at the same time': when some k-tuple is given, we know that either P or P' must list this k-tuple after some finite time, so our program can be made in such a way that it always tells in finite time whether the tuple belongs to A or not (depending on whether the tuple was eventually listed by P or P').

In Chapters 2 and 3, it will be shown that a set is computably enumerable if and only if it is Diophantine. So, if every Diophantine set has a Diophantine complement, it would follow that every computably enumerable set has a computably enumerable complement as well. It would then follow from our discussion above that every computably enumerable set is computable; however, because we will see that there are computably enumerable sets which are not computable (cf. Theorem 2.8), this is a contradiction. So there must be a Diophantine set whose complement is not Diophantine. ♦

We end this section with the following important theorem, which shows that, in order to prove the remarkable assertion that the classes of Diophantine sets and exponential Diophantine sets coincide, it suffices to show that exponentiation is Diophantine.

[3] in Chapter 2, a slightly different definition will be given

Theorem 1.12. *If exponentiation is Diophantine, i.e. if there exists some $W \in \mathbb{Z}[X_1, \dots, X_{m+3}]$ such that*

$$a = b^c \iff \exists x_1 \cdots x_m \in \mathbb{Z}\Big(W(a, b, c, x_1, \dots, x_m) = 0\Big)$$

for any triple $(a, b, c) \in \mathbb{N}^3$, then a set is Diophantine if and only if it is exponential Diophantine.

Proof. We have already argued that every Diophantine set is exponential Diophantine. For the converse, we consider, as an example, the exponential Diophantine set

$$A = \{z \in \mathbb{N} \mid \exists xy \in \mathbb{N}\big(E(x, y, z) = F(x, y, z)\big)\}$$

with the exponential polynomials $E, F \in \mathbb{N}^*[X_1, X_2, X_3]$ given by

$$\begin{aligned} E &: (x, y, z) \mapsto 2^x + 4y^7 + z \\ F &: (x, y, z) \mapsto (2x + y^2)^{(12xyz+3)^{7y}} \end{aligned}$$

Now, let $W \in \mathbb{Z}[X_1, \dots, X_{m+3}]$ be as in the statement of the theorem. Then for all $z \in \mathbb{N}$ we have that $z \in A$ if and only if $\exists xy \in \mathbb{N}\big(2^x + 4y^7 + z = (2x+y^2)^{(12xyz+3)^{7y}}\big)$. Using the polynomial W, this last condition is then equivalent to

$$\begin{aligned} &\exists xy \in \mathbb{N}\ \exists u_0 u_1 \cdots u_m v_0 v_1 \cdots v_m w_0 w_1 \cdots w_m \in \mathbb{Z}\big(\\ &\qquad (u_0 + 4y^7 + z) - v_0 = 0 \\ &\qquad \wedge W(u_0, 2, x, u_1, \dots, u_m) = 0 \\ &\qquad \wedge W(v_0, 2x + y^2, w_0, v_1, \dots, v_m) = 0 \\ &\qquad \wedge W(w_0, 12xyz + 3, 7y, w_1, \dots, w_m) = 0 \\ &\big) \end{aligned} \tag{1.4}$$

I hope that it is clear that we can construct a representing formula like (1.4) for exponential Diophantine sets

$$\{(a_1, \dots, a_k) \in \mathbb{N}^k \mid \exists x_1 \cdots x_m \in \mathbb{N}\big(E(a_1, \dots, a_k, x_1, \dots, x_m) = F(a_1, \dots, a_k, x_1, \dots, x_m)\big)\},$$

in general, with $E, F \in \mathbb{N}^*[X_1, \dots, X_{k+m}]$ arbitrary. One just introduces $m + 1$ new variables for "each level of exponentiation", while making excessive use of the given polynomial W.

To see that formula (1.4) is Diophantine, note that it is equivalent to a formula of the form

$$\begin{aligned} &\exists xy \in \mathbb{N}\ \exists u_0 u_1 \cdots u_m v_0 v_1 \cdots v_m w_0 w_1 \cdots w_m \in \mathbb{Z}\big(\\ &\qquad F(x, y, u_0, \dots, u_m, v_0, \dots, v_m, w_0, \dots, w_m) = 0 \\ &\big) \end{aligned}$$

because, by part b) of Lemma 1.8, the conjunctions in (1.4) can be eliminated in favor of some polynomial $F \in \mathbb{Z}[X_1, \dots, X_{3m+5}]$. Now, because the formula

$$\begin{aligned} &\exists u_0 u_1 \cdots u_m v_0 v_1 \cdots v_m w_0 w_1 \cdots w_m \in \mathbb{Z}\big(\\ &\qquad F(x, y, u_0, \dots, u_m, v_0, \dots, v_m, w_0, \dots, w_m) = 0 \\ &\big) \end{aligned}$$

is Diophantine by Remark 1.7, it follows from closure under existential quantifiers over $\mathbb{N}$ (cf. Theorem 1.9) that (1.4) is equivalent to some Diophantine formula $\psi(z)$. So $A = \{z \in \mathbb{N} \mid \psi(z)\}$ is Diophantine.

∎

1.2 Examples of (Exponential) Diophantine Sets

In this section, we will prove that some relations, which are going to be important later on, are (exponential) Diophantine.

Proposition 1.13 (Diophantine Sets). *The sets*

$$\{(a,b,m) \in \mathbb{N}^3 \mid a \equiv b \mod m\}$$
$$\{(a,b) \in \mathbb{N}^2 \mid a < b\}$$
$$\{(a,b) \in \mathbb{N}^2 \mid a \mid b\}$$

are Diophantine.

Proof. For all $a, b, m \in \mathbb{N}$ we have

$$\begin{aligned} a \equiv b \mod m &\iff \exists x \in \mathbb{Z}\big((a-b) - mx = 0\big) \\ a < b &\iff \exists x \in \mathbb{Z}\big((a+x+1) - b = 0\big) \\ a \mid b &\iff \exists x \in \mathbb{Z}\big(ax - b = 0\big), \end{aligned}$$

showing that each set is represented by a Diophantine formula.

∎

For the remainder of this section, we turn our attention solely to *exponential* Diophantine sets.

We begin by reviewing some basic facts about the representation of natural numbers with respect to a certain *base*, which is simply a natural number greater than 1. If $b \in \mathbb{N}_{\geq 2}$ denotes some base, then, for every $a \in \mathbb{N}$, there is a unique sequence $\{a_k\}_{k \in \mathbb{N}}$ of natural numbers, known as *base-b digits*, such that

$$a = \sum_{k=0}^{\infty} a_k b^k \qquad \text{and} \qquad a_k < b \text{ for all } k \tag{1.5}$$

It follows that every natural number has, at most, finitely many nonzero digits (in any base). We will often use the following notation for the sum in (1.5):

$$\cdots a_2 a_1 a_0{}_{\langle b \rangle} = \sum_{k=0}^{\infty} a_k b^k,$$

Similarly, an expression like $a_N \cdots a_0{}_{\langle b \rangle}$ is shorthand notation for $\sum_{k=0}^{N} a_k b^k$. If (1.5) holds then $\cdots a_2 a_1 a_0{}_{\langle b \rangle}$ is said to *represent* the number a in base-b notation. The k-th digit $a_k \in \{0, \ldots, b-1\}$ of some natural number a in base-b notation will be denoted by $\mathrm{Digit}(a, b, k)$.

Example. The two most familiar bases are the decimal base $\langle 10 \rangle$ and the binary base $\langle 2 \rangle$. For example, if $a \in \mathbb{N}$ represents the number twelve, we may write

$$a = 12_{\langle 10 \rangle} \qquad \text{or} \qquad a = 1100_{\langle 2 \rangle},$$

where the terms $12_{\langle 10 \rangle}$ and $1100_{\langle 2 \rangle}$ should just be seen as abbreviations for the sums $2 \cdot 10^0 + 1 \cdot 10^1$ and $0 \cdot 2^0 + 0 \cdot 2^1 + 1 \cdot 2^2 + 1 \cdot 2^3$ respectively. Note that $\mathrm{Digit}(a, 10, k) = 0$ whenever $k > 1$ and that $\mathrm{Digit}(a, 2, k) = 0$ whenever $k > 3$ in this case.

Whenever we use the familiar symbols 0,1,2,3,4,5,6,7,8 and 9 to represent some natural number in decimal notation, the decimal base-indicator $\cdot_{\langle 10 \rangle}$ may be omitted; so $12 = 12_{\langle 10 \rangle} = 1100_{\langle 2 \rangle}$. ♦

The following lemma gives us some basic properties of the Digit function.

Lemma 1.14. *Let $x, y \in \mathbb{N}$ and $b \in \mathbb{N}_{\geq 2}$.*

a) If $Q \in \mathbb{N}$ and $\mathrm{Digit}(x, b, i) + \mathrm{Digit}(y, b, i) < b$ for all $i \in \{0, \ldots, Q\}$, then

$$\mathrm{Digit}(x + y, b, i) = \mathrm{Digit}(x, b, i) + \mathrm{Digit}(y, b, i)$$

for all $i \in \{0, \ldots, Q\}$.

b) If $i \in \mathbb{N}$, then $\mathrm{Digit}(bx, b, i + 1) = \mathrm{Digit}(x, b, i)$.

Proof. For part a), say $x = \cdots x_2x_1x_{0\langle b\rangle}$ and $y = \cdots y_2y_1y_{0\langle b\rangle}$ and assume $x_i + y_i < b$ for all $i \leq Q$ for some $Q \in \mathbb{N}$. Then we can write $x + y$ as

$$x + y = Nb^{Q+1} + \sum_{i=0}^{Q}(x_i + y_i)b^i$$

for some $N \in \mathbb{N}$. Writing N in base-b notation as $N = \cdots N_2N_1N_{0\langle b\rangle}$, it follows that

$$\begin{aligned} x + y &= b^{Q+1}\sum_{i=0}^{\infty} N_ib^i + \sum_{i=0}^{Q}(x_i + y_i)b^i \\ &= \sum_{i=0}^{Q}(x_i + y_i)b^i + \sum_{i=Q+1}^{\infty} N_{i-(Q+1)}b^i \\ &= \sum_{i=0}^{\infty} z_ib^i \end{aligned}$$

where $z_i = x_i + y_i$ if $i \leq Q$ and $z_i = N_{i-(Q+1)}$ if $i > Q$. Because $z_i < b$ for all i, we see that $\mathrm{Digit}(x + y, b, i) = z_i$ for all $i \in \mathbb{N}$. In particular, we have $\mathrm{Digit}(x + y, b, i) = x_i + y_i$ for all $i \leq Q$.

For part b), say $x = \cdots x_2x_1x_{0\langle b\rangle}$. Then

$$bx = b\sum_{i=0}^{\infty} x_ib^i = \sum_{i=1}^{\infty} x_{i-1}b^i = \sum_{i=0}^{\infty} \widehat{x}_ib^i$$

where $\widehat{x}_0 = 0$ and $\widehat{x}_{i+1} = x_i$. Because $\widehat{x}_i < b$ for all i, we find that $\mathrm{Digit}(bx, b, i + 1) = \widehat{x}_{i+1} = x_i$ for all $i \in \mathbb{N}$.

∎

Surely, part a) of Lemma 1.14 can easily be strengthened for finite sums.

Corollary 1.15. *Let $x_1, \ldots, x_N \in \mathbb{N}$ and $b \in \mathbb{N}_{\geq 2}$. If $Q \in \mathbb{N}$ and $\sum_{n=0}^{N} \mathrm{Digit}(x_n, b, i) < b$ for all $i \in \{0, \ldots, Q\}$, then*

$$\mathrm{Digit}\left(\sum_{n=0}^{N} x_n, b, i\right) = \sum_{n=0}^{N} \mathrm{Digit}(x_n, b, i)$$

for all $i \in \{0, \ldots, Q\}$.

Proof. Repeatedly apply part a) of Lemma 1.14 to find that

$$\begin{aligned}
\operatorname{Digit}\left(\sum_{n=0}^{N} x_n, b, i\right) &= \operatorname{Digit}(x_0, b, i) + \operatorname{Digit}\left(\sum_{n=1}^{N} x_n, b, i\right) \\
&= \operatorname{Digit}(x_0, b, i) + \operatorname{Digit}(x_1, b, i) + \operatorname{Digit}\left(\sum_{n=2}^{N} x_n, b, i\right) \\
&\vdots \\
&= \sum_{n=1}^{N} \operatorname{Digit}(x_n, b, i)
\end{aligned}$$

∎

The next proposition shows that the Digit function is exponential Diophantine.

Proposition 1.16. *The set*

$$\{(a, b, k, d) \in \mathbb{N}^4 \mid d = \operatorname{Digit}(a, b, k)\},$$

is exponential Diophantine.

Proof. Let $a, b, k, d \in \mathbb{N}$ be arbitrary. We show that

$$d = \operatorname{Digit}(a, b, k) \iff \exists xy \in \mathbb{N}\Big(1 < b \wedge a = x + db^k + yb^{k+1} \wedge d < b \wedge x < b^k\Big) \tag{1.6}$$

If $d = \operatorname{Digit}(a, b, k)$, then $b \geq 2$ and we can write $a = a_N \cdots a_{k+1} d a_{k-1} \cdots a_{0\langle b \rangle}$ for certain digits $a_j < b$ and some N, i.e.

$$a = \sum_{j=0}^{k-1} a_j b^j + db^k + \sum_{j=k+1}^{N} a_j b^j = \sum_{j=0}^{k-1} a_j b^j + db^k + b^{k+1} \sum_{j=k+1}^{N} a_j b^{j-(k+1)}$$

So, if we define $x = \sum_{j=0}^{k-1} a_j b^j$ and $y = \sum_{j=k+1}^{N} a_j b^{j-(k+1)}$, then $x, y \in \mathbb{N}$ and $a = x + db^k + yb^{k+1}$. It follows from the definition of Digit that $d < b$. The fact that $x < b^k$ can be seen as follows.

$$\begin{aligned}
x &= \sum_{j=0}^{k-1} a_j b^j && \text{by definition} \\
&\leq \sum_{j=0}^{k-1} (b-1) b^j && \text{because } a_j < b \text{ for all } j \\
&= b^k - b^0 && \text{because we have a telescoping series} \\
&< b^k
\end{aligned}$$

For the converse, let $x, y \in \mathbb{N}$ be such that $a = x + db^k + yb^{k+1}$, $d < b$ and $x < b^k$ with $b \geq 2$. Let us write $x = \cdots x_2 x_1 x_{0\langle b \rangle}$ and $y = \cdots y_2 y_1 y_{0\langle b \rangle}$ for the base-b representations of x and y. Then $x_j = 0$ whenever $j \geq k$ (otherwise we would have $x \geq b^k$), so we can write $x = \sum_{j=0}^{k-1} x_j b^j$. If we define the sequence $\{a_j\}_{j \in \mathbb{N}}$ by

$$a_j = \begin{cases} x_j & \text{if } j < k \\ d & \text{if } j = k \\ y_{j-(k+1)} & \text{if } j > k \end{cases}$$

it follows from our assumptions that $a = \sum_{j=0}^{\infty} a_j b^j$, with $a_j < b$ for all j. So $\text{Digit}(a, b, k) = a_k = d$.

Because "$<$" is Diophantine by Proposition 1.13, it follows that the right hand side of (1.6) is just a conjunction of (exponential) Diophantine formulas, preceded by some existential quantifiers. It then follows from Theorem 1.9 that the formula $d = \text{Digit}(a, b, k)$ is exponential Diophantine.

∎

The next proposition shows that the binomial coefficient is exponential Diophantine as well. Together with Kummer's Theorem (cf. Theorem 1.18), this will allows us to prove the main results of this section, namely that *binary masking* and *binary multiplication* are both exponential Diophantine.

Proposition 1.17. *The set*

$$\{(a, b, c) \in \mathbb{N}^3 \mid c = \binom{a}{b}\}$$

is exponential Diophantine.

Proof. Let $a, b, c \in \mathbb{N}$ be arbitrary. We know from Newton's binomial theorem that

$$(2+1)^a = \binom{a}{0}2^0 + \binom{a}{1}2^1 + \cdots + \binom{a}{a-1}2^{a-1} + \binom{a}{a}2^a \tag{1.7}$$

So, we see that the b-th binary digit of 3^a is exactly the number $\binom{a}{b}$, i.e. that $\text{Digit}(3^a, 2, b) = \binom{a}{b}$. In particular, note that $\text{Digit}(3^a, 2, b) = 0$ whenever $b > a$ according to (1.7), just as $\binom{a}{b} = 0$ whenever $b > a$. We conclude that the set

$$\{(a, b, c) \in \mathbb{N}^3 \mid c = \binom{a}{b}\} = \{(a, b, c) \in \mathbb{N}^3 \mid \exists t \in \mathbb{N}(c = \text{Digit}(t, 2, b) \wedge t = 3^a)\}$$

is exponential Diophantine (by Proposition 1.16 and Theorem 1.9).

∎

Let $a, b \in \mathbb{N}$. Because $\binom{a+b}{b}$ is a natural number, we know that it has a unique prime factorization: for every prime p there is a unique exponent $\delta_p(a, b) \in \mathbb{N}$ such that

$$\binom{a+b}{b} = \prod_{p \text{ prime}} p^{\delta_p(a,b)} \tag{1.8}$$

In 1852, German mathematician Kummer published a paper ([9]) in which he described a surprisingly easy way to calculate these exponents $\delta_p(a, b)$.

Theorem 1.18 (Kummer's Theorem). *Let a and b be natural numbers and, for every prime p, let $\delta_p(a, b) \in \mathbb{N}$ be the highest number such that $p^{\delta_p(a,b)}$ divides $\binom{a+b}{b}$. Then $\delta_p(a, b)$ may be calculated as follows:*

> *Write a and b in base-p notation and add them together. The number of carries which occur during this addition is exactly the number $\delta_p(a, b)$.*

Rather than proving Kummer's Theorem here, we shall only give an example on how to use it; a proof can be found in the appendix.

Example. Let $a = 6$ and $b = 2$. We will calculate the $\delta_p(a,b)$'s using Kummer's Theorem so let us begin by considering the first four primes $p \in \{2,3,5,7\}$ and writing a and b in base-p notation:

	base-2	base-3	base-5	base-7
a	$110_{\langle 2\rangle}$	$20_{\langle 3\rangle}$	$11_{\langle 5\rangle}$	$6_{\langle 7\rangle}$
b	$10_{\langle 2\rangle}$	$2_{\langle 3\rangle}$	$2_{\langle 5\rangle}$	$2_{\langle 7\rangle}$

Next, we consider the addition of a and b in these different bases:

$$\begin{array}{rl} \cancel{1}\cancel{1} & \\ 110_{\langle 2\rangle} & \\ 10_{\langle 2\rangle} & + \\ \hline 1000_{\langle 2\rangle} & \end{array} \qquad \begin{array}{rl} & \\ 20_{\langle 3\rangle} & \\ 2_{\langle 3\rangle} & + \\ \hline 22_{\langle 3\rangle} & \end{array} \qquad \begin{array}{rl} & \\ 11_{\langle 5\rangle} & \\ 2_{\langle 5\rangle} & + \\ \hline 13_{\langle 5\rangle} & \end{array} \qquad \begin{array}{rl} \cancel{1}\phantom{6_{\langle 7\rangle}} & \\ 6_{\langle 7\rangle} & \\ 2_{\langle 7\rangle} & + \\ \hline 11_{\langle 7\rangle} & \end{array}$$

We see that, during these additions, two carries occur with $p = 2$, no carries occur with $p = 3, 5$ and one carry occurs with $p = 7$. According to Kummer's Theorem we have $\delta_2(a,b) = 2$, $\delta_3(a,b) = \delta_5(a,b) = 0$ and $\delta_7(a,b) = 1$. For any prime $p > 7$ we have that $a + b < p$ so that no carry ever occurs during the addition of a and b in base-p notation, implying that $\delta_p(a,b) = 0$ when $p > 7$. It follows that

$$\prod_{p \text{ prime}} p^{\delta_p(a,b)} = 2^2 \cdot 7^1$$

which is exactly the prime factorization of $\binom{a+b}{b} = 28$. ♦

Definition 1.19. Let a and b be natural numbers with $\cdots a_2 a_1 a_{0\langle 2\rangle}$ and $\cdots b_2 b_1 b_{0\langle 2\rangle}$ as binary representations.

- If $a_j b_j = 0$ for all j, then a and b are said to be *binary orthogonal.* This relation will be denoted by $a \perp b$.
- If $a_j \leq b_j$ for all j, then a is said to be *(binary) masked* by b. This relation will be denoted by $a \preccurlyeq b$.
- The *(binary) digit-by-digit multiplication* of a and b gives us the number c whose binary representation $\cdots c_2 c_1 c_{0\langle 2\rangle}$ satisfies $c_j = a_j b_j$ for all j. The (binary) digit-by-digit product of a and b is denoted by $a * b$.

♦

We will now use Kummer's Theorem to show that "$\perp$", "$\preccurlyeq$" and "$*$" are all exponential Diophantine.

Theorem 1.20 (Exponential Diophantine Sets). *The sets*

$$\begin{gathered} \{(a,b) \in \mathbb{N}^2 \mid a \perp b\} \\ \{(a,b) \in \mathbb{N}^2 \mid a \preccurlyeq b\} \\ \{(a,b,c) \in \mathbb{N}^3 \mid c = a * b\} \\ \{(a,b,k,d) \in \mathbb{N}^4 \mid d = \operatorname{Digit}(a,b,k)\} \end{gathered}$$

are exponential Diophantine.

Proof. By Proposition 1.16, we only have to consider the first three sets.

Let $a = \cdots a_2 a_1 a_{0\langle 2\rangle}$, $b = \cdots b_2 b_1 b_{0\langle 2\rangle}$ and $c = \cdots c_2 c_1 c_{0\langle 2\rangle}$ be natural numbers. We first show that

$$a \perp b \iff \delta_2(a, b) = 0 \iff \binom{a+b}{b} \text{ is odd} \tag{1.9}$$

Because the relations "x is odd" and "$x = \binom{a+b}{b}$" are both exponential Diophantine (cf. Proposition 1.17), it would immediately follow that "$\perp$" is exponential Diophantine as well.

If $a \perp b$, then $a_j b_j = 0$ for all j. Because $a_j < 2$ and $b_j < 2$, this implies that $a_j + b_j < 2$ for all j. It follows that there is no carry in the binary addition of a and b, so $\delta_2(a, b) = 0$ by Kummer's Theorem. Conversely, if $\delta_2(a, b) = 0$, we know from Kummer's Theorem that there is no carry in the binary addition of a and b. So $a_j + b_j < 2$ for all j, implying that $a_j b_j = 0$ for all j, i.e. that $a \perp b$.

For the second equivalence, note that $\binom{a+b}{b}$ is odd if and only if the highest power of 2 in the prime factorization of $\binom{a+b}{b}$ is equal to 1, which, by definition, is the case if and only if $\delta_2(a, b) = 0$.

We will now show that

$$b \preccurlyeq c \iff \binom{c}{b} \text{ is odd}$$

from which it would immediately follow that "$\preccurlyeq$" is exponential Diophantine as well. Note that both sides of the above equivalence are trivially false if $b > c$, so we can assume that $b \leq c$ and we can find some $a \in \mathbb{N}$ such that $c = a + b$. Then, in the light of (1.9), it suffices to show that

$$b \preccurlyeq a + b \iff a \perp b$$

If $b \preccurlyeq a + b$, then we must have $a \perp b$; otherwise, let $k \in \mathbb{N}$ be least such that $a_k b_k = 1$. Then $a_k = b_k = 1$, so $a_k + b_k = 2$ and there must be a carry from the k-th binary digit of $a + b$ to the next. It follows that $\mathrm{Digit}(a+b, 2, k) = 0$, which is a contradiction because $\mathrm{Digit}(b, 2, k) = b_k = 1$ and we assumed that $b \preccurlyeq a + b$. So $a \perp b$.

Conversely, if $a \perp b$, then $a_j b_j = 0$ for all j. It follows that $a_j + b_j < 2$ for all j and thus that there is no carry in the binary addition of a and b, implying that $\mathrm{Digit}(a + b, 2, j) = a_j + b_j$ for all j. Because, obviously, $b_j \leq a_j + b_j$ for all j, it follows that $b \preccurlyeq a + b$.

It only remains to show that $c = a * b$ is exponential Diophantine; we will show that

$$c = a * b \iff c \preccurlyeq a \wedge c \preccurlyeq b \wedge (a - c \perp b - c)$$

holds, from which this assertion would immediately follow (by earlier results).

If $c = a * b$, then $c_j = a_j b_j$ for all j. Recalling that binary digits are either 0 or 1, it immediately follows that $c_j \leq a_j$ and $c_j \leq b_j$ for all j, i.e. that $c \preccurlyeq a$ and $c \preccurlyeq b$. Note that these two masking relations imply, in particular, that $a - c \geq 0$ and $b - c \geq 0$. Furthermore, they imply that

$$\mathrm{Digit}(a - c, 2, j) = a_j - c_j = a_j(1 - b_j)$$
$$\mathrm{Digit}(b - c, 2, j) = b_j - c_j = b_j(1 - a_j)$$

Because $a_j, b_j \in \{0, 1\}$, It follows that $\mathrm{Digit}(a - c, 2, j) \cdot \mathrm{Digit}(b - c, 2, j) = 0$ for all j, i.e. that $a - c \perp b - c$.

For the converse, assume that $c \preccurlyeq a$ and $c \preccurlyeq b$ and $a - c \perp b - c$. Then, for all j, we have that $c_j \leq a_j$ and $c_j \leq b_j$ so that $c_j = c_j^2 \leq a_j b_j$, showing that $c_j > a_j b_j$ is impossible. We show that $c_j < a_j b_j$ is impossible as well; assume $k \in \mathbb{N}$ is least such that $c_k < a_k b_k$. Then we must have $c_k = 0$ and $a_k = b_k = 1$, but that would imply that

$$\begin{aligned} \mathrm{Digit}(a - c, 2, k) = a_k - c_k = 1 \\ \mathrm{Digit}(b - c, 2, k) = b_k - c_k = 1 \end{aligned}$$

showing that $\mathrm{Digit}(a - c, 2, k) \cdot \mathrm{Digit}(b - c, 2, k) = 1$ and contradicting our assumption that $a - c \perp b - c$. We conclude that $c_j = a_j b_j$ for all j, i.e. that $c = a * b$.

■

Chapter 2

Computably Enumerable Sets are Exponential Diophantine

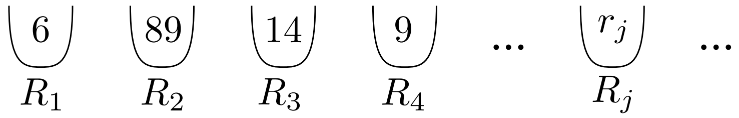
There are several equivalent ways to define the class $\mathcal{C}$ of computable functions. For example, one can follows Kleene's approach in [8] to use a certain inductive definition scheme to construct the *partial recursive functions* or, equivalently, follow Turing's approach in [14] to construct the *Turing-computable functions* as those functions whose values can be computed by an abstract computing device known as a *Turing machine.*

In this chapter, we consider yet another equivalent computation model to define the computable functions: the so-called *Register Machine.*

2.1 Register Machines

We consider an abstract computing device, known as a *Register Machine*. It has a countably infinite number of memory places $R_1, R_2, R_3, \ldots$ known as *registers*, each of which has the ability to store an arbitrary large natural number. The number stored in register R_j is denoted by r_j.

It is assumed that every register stores *some* natural number. Registers which store the number 0 are said to be *empty.*



The registers of a Register Machine.

One can only modify the contents of the registers by giving the Register Machine a *program* P, which is an ordered and non-empty finite list $(I_1, \ldots, I_N)$ of *instructions.* When given a program P, the Register Machine will start by executing the first instruction of P. There are only three types of instructions that the Register Machine can interpret; it reacts to these according to the following scheme.

Instruction	**Action Taken by Register Machine**
$r_j^+ \implies \langle n \rangle$	add 1 to r_j, then go to the n-th instruction of P
$r_j^- \implies \langle n, m \rangle$	if $r_j > 0$: subtract 1 from r_j, then go to the n-th instruction of P; if $r_j = 0$: go to the m-th instruction of P
STOP	terminate the program, i.e. stop the execution of all further instructions

Every program P, say of length N, is assumed to adhere to the following constraints.

- Every instruction of P is of the form '$r_j^+ \implies \langle n \rangle$', '$r_j^- \implies \langle n, m \rangle$' or 'STOP', where $j \in \{1, 2, 3, \dots\}$ and $n, m \in \{1, \dots, N\}$.
- The last instruction (i.e. the N-th instruction) of P is the 'STOP' instruction, and P has exactly one stop instruction.
- The program P is terminated if and only if its 'STOP' instruction is executed.

Note that we only require that *if* a program is ever terminated, that its 'STOP' instruction must have been reached. It is allowed, however, for a valid program to never terminate at all, which can be seen from two of the examples below.

Example. Because the location of the instructions in a program is of great importance, it is many times useful in examples to provide programs with *line-numbers* (these are ignored by the Register Machine). Below are some examples of valid programs.

$1 : \text{STOP}$	The trivial program. Immediately stops.
$1 : r_7^+ \implies \langle 2 \rangle$ $2 : r_3^+ \implies \langle 3 \rangle$ $3 : r_9^+ \implies \langle 4 \rangle$ $4 : \text{STOP}$	Increases the registers R_7, R_3 and R_9 by one. Then stops.
$1 : r_4^- \implies \langle 1, 2 \rangle$ $2 : r_{10}^+ \implies \langle 2 \rangle$ $3 : \text{STOP}$	Empties the fourth register. Then keeps adding to the tenth register indefinitely. Never stops.
$1 : r_j^- \implies \langle 2, 4 \rangle$ $2 : r_{j+1}^+ \implies \langle 3 \rangle$ $3 : r_{j+2}^+ \implies \langle 1 \rangle$ $4 : \text{STOP}$	Moves the content of the j-th register simultaneously to the $(j+1)$-th and the $(j+2)$-th register. Then stops.
$1 : r_3^- \implies \langle 1, 1 \rangle$ $2 : \text{STOP}$	Empties the third register. Then keeps doing nothing forever. Never stops.

♦

It is clear that a program can have very different effects, depending on the initial values of the registers. For example, the program

$$\begin{aligned}
&1 : r_1^- \implies \langle 2, 3\rangle\\
&2 : r_2^+ \implies \langle 2\rangle\\
&3 : \mathrm{STOP}
\end{aligned}$$

terminates after one step if the first register is empty and never halts otherwise. For this very reason, we are always allowed to execute a program on certain *input*, which is simply a tuple $(a_1, \ldots, a_k)$ of natural numbers for some $k \in \mathbb{N}$; if $k = 0$ we speak of the *empty* input $(-)$.

If a program is executed on some input $(a_1, \ldots, a_k)$, then, just before the the first instruction is executed, the first k registers will contain the numbers a_1 through a_k and the remaining registers are empty, i.e.

$$r_j = \begin{cases} a_j & \text{if } j \leq k \\ 0 & \text{otherwise} \end{cases}$$

for all register indices $j \in \{1, 2, 3, \ldots\}$. In particular, *all* registers will initially be empty if the program is executed on the empty input. If a program is executed without a specification of input, the empty input will be assumed.

Before moving to the next section, we remark that every program can be attributed two properties.

Length. The length of a program P, simply denoted $\text{length}(P)$, refers to the total number of instructions that P has. Note that $\text{length}(P) > 0$ for any program P.

Maximum Register Index. Because P contains a finite number of instructions, there is a maximum register index, denoted $\text{mri}(P)$, such that $R_{\text{mri}(P)}$ is the 'last' register which could be modified by P. Precisely, we define

$$\text{mri}(P) = \max\{j \in \mathbb{N} \mid \exists nm \in \mathbb{N}\Big((r_j^+ \implies \langle n\rangle) \in P \vee (r_j^- \implies \langle n, m\rangle) \in P\Big)\}$$

and we define $\text{mri}(P) = 1$ if P is the trivial program.

The only reason for introducing $\text{mri}(P)$ is to know which registers will always be 'ignored' by the program. For example, if P is executed on some input $(a_1, \ldots, a_k)$, where $k > \text{mri}(P)$, we know that 'during the execution' of P, those input values a_κ for which $\text{mri}(P) < \kappa \leq k$, will be ignored because P never interacts with the corresponding registers R_κ.

2.2 Computations and Computable Functions

Definition 2.1. Let P be a program. Write $J = \text{mri}(P)$ and let $(a_1, \ldots, a_k) \in \mathbb{N}^k$ be some input. A *computation* C with program P on input $(a_1, \ldots, a_k)$ is a finite or infinite list

$$C = \Big((\eta^{(0)}; \rho_1^{(0)}, \ldots, \rho_J^{(0)}),\ (\eta^{(1)}; \rho_1^{(1)}, \ldots, \rho_J^{(1)}),\ (\eta^{(2)}; \rho_1^{(2)}, \ldots, \rho_J^{(2)}),\ \ldots\Big)$$

of $(J + 1)$-tuples known as *(computation) states*, which are defined inductively.

The idea is that each state $(\eta^{(i)};\rho_1^{(i)},\ldots,\rho_J^{(i)})$ tells us that, at computation step i, the registers $R_1,\ldots,R_J$ contain the values $\rho_1^{(i)}$ through $\rho_J^{(i)}$ and that the $\eta^{(i)}$-th instruction of P is about to be executed[1]. More precisely, we define the zeroth computation state as

$$(\eta^{(0)};\rho_1^{(0)},\ldots,\rho_J^{(0)}) = \begin{cases} (1;a_1,\ldots,a_k,0,\ldots,0) & \text{if } k < J \\ (1;a_1,\ldots,a_J) & \text{if } k \geq J \end{cases}$$

and if the i-th state $(\eta^{(i)};\rho_1^{(i)},\ldots,\rho_J^{(i)})$ has been defined, we consider three cases.

- If the $\eta^{(i)}$-th instruction of P is of the form '$r_j^+ \implies \langle u\rangle$', then

$$(\eta^{(i+1)};\rho_1^{(i+1)},\ldots,\rho_J^{(i+1)}) = (u;\rho_1^{(i)},\ldots,\rho_{j-1}^{(i)},\rho_j^{(i)}+1,\rho_{j+1}^{(i)},\ldots,\rho_J^{(i)})$$

- If the $\eta^{(i)}$-th instruction of P is of the form '$r_j^- \implies \langle u,v\rangle$', then

$$(\eta^{(i+1)};\rho_1^{(i+1)},\ldots,\rho_J^{(i+1)}) = (u;\rho_1^{(i)},\ldots,\rho_{j-1}^{(i)},\rho_j^{(i)}-1,\rho_{j+1}^{(i)},\ldots,\rho_J^{(i)})$$

  if $r_j^{(i)} > 0$ and

$$(\eta^{(i+1)};\rho_1^{(i+1)},\ldots,\rho_J^{(i+1)}) = (v;\rho_1^{(i)},\ldots,\rho_J^{(i)})$$

  if $r_j^{(i)} = 0$.

- If the $\eta^{(i)}$-th instruction of P is of the form 'STOP', then the computation is finite (i.e. of length $i+1$) and given by

$$C = \Big((\eta^{(0)};\rho_1^{(0)},\ldots,\rho_J^{(0)}),\ldots,(\eta^{(i)};\rho_1^{(i)},\ldots,\rho_J^{(i)})\Big)$$

♦

Let P be a program and let $\vec{a} = (a_1,\ldots,a_k)$ be some input. We see that P and $\vec{a}$ define a unique computation C, i.e. any two copies of the same program, on the same input, always define the same computation. Equivalently, the Register Machine is said to be *deterministic*.

Surely, C is finite if and only if the program P eventually halts on input $\vec{a}$; if C is finite, say of length $Q+1$, so that

$$C = \Big((\eta^{(0)};\rho_1^{(0)},\ldots,\rho_J^{(0)}),\ \ldots,(\eta^{(Q)};\rho_1^{(Q)},\ldots,\rho_J^{(Q)})\Big),$$

we refer to the number $\rho_1^{(Q)}$ as the *output* of C.

We are now ready to define what it means for a function defined on (a subset of) the natural numbers to be *RM-computable*, or simply *computable*.

Definition 2.2. Let X and Y be sets. A *partial function* from X to Y is a function $f : U \to Y$, where U is a subset of X. The set U is called the *domain* of f and denoted by $\mathrm{dom}(f)$. The partial function f is said to be *total* if $\mathrm{dom}(f) = X$.

If we are not interested in the actual domain U, but just want to stress that f is partial, we will write $f : X \rightharpoonup Y$ instead of $f : U \to Y$. ♦

[1] this obviously implies that we must have $\eta^{(i)} \in \{1,\ldots,\mathrm{length}(P)\}$

Definition 2.3. Let $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ be a k-ary partial function. Then f is said to be *computable* (another word is: *recursive*) if there exists a program P such that for every k-tuple $(a_1, \ldots, a_k)$ of natural numbers the following holds.

- If $(a_1, \ldots, a_k) \in \operatorname{dom}(f)$, then the computation of P with input $(a_1, \ldots, a_k)$ is finite and produces the number $f(a_1, \ldots, a_k)$ as output.
- If $(a_1, \ldots, a_k) \notin \operatorname{dom}(f)$, then the computation of P with input $(a_1, \ldots, a_k)$ is infinite.

If such a program exists, it is said to *compute* f and may be called an *algorithm* for f. ⧫

Intuitively, we can think of a computable $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ as a function whose function values can be calculated (depending on the input) on a computing device with infinitely many memory places. This understanding (especially for people who often work with computers in real life) makes it easy to grasp that most simple functions which involve basic arithmetic, such as the functions $n \mapsto n + 5$ and $n \mapsto 2n$, are computable. It may be tedious, however, to actually write Register Machine programs for such functions, especially if we have to take into account that a given function is only defined on a subset of $\mathbb{N}^k$.

Example. The partial functions $f, g : \mathbb{N} \rightharpoonup \mathbb{N}$ given by

$$f : \begin{array}{r} \mathbb{N} \to \mathbb{N} \\ n \mapsto n + 5 \end{array} \qquad \text{and} \qquad g : \begin{array}{r} \mathbb{N} \setminus \{1\} \to \mathbb{N} \\ n \mapsto 2n \end{array}$$

are computable; they are computed by the programs

$$\begin{array}{l} 1 : r_1^+ \implies \langle 2 \rangle \\ 2 : r_1^+ \implies \langle 3 \rangle \\ 3 : r_1^+ \implies \langle 4 \rangle \\ 4 : r_1^+ \implies \langle 5 \rangle \\ 5 : r_1^+ \implies \langle 6 \rangle \\ 6 : \text{STOP} \end{array} \qquad \text{and} \qquad \begin{array}{r} 1 : r_1^- \implies \langle 2, 15 \rangle \\ 2 : r_2^+ \implies \langle 3 \rangle \\ 3 : r_3^+ \implies \langle 4 \rangle \\ 4 : r_1^- \implies \langle 5, 14 \rangle \\ 5 : r_2^+ \implies \langle 6 \rangle \\ 6 : r_3^+ \implies \langle 7 \rangle \\ 7 : r_1^- \implies \langle 8, 10 \rangle \\ 8 : r_2^+ \implies \langle 9 \rangle \\ 9 : r_3^+ \implies \langle 7 \rangle \\ 10 : r_2^- \implies \langle 11, 12 \rangle \\ 11 : r_3^+ \implies \langle 10 \rangle \\ 12 : r_3^- \implies \langle 13, 15 \rangle \\ 13 : r_1^+ \implies \langle 12 \rangle \\ 14 : r_{100}^+ \implies \langle 14 \rangle \\ 15 : \text{STOP} \end{array}$$

respectively.

The algorithm for f is pretty straightforward; if some number $n \in \mathbb{N}$ is given as input, it will reside in the first register R_1 just before execution (all other registers being empty). We simply increase this number by 5 and then terminate the program. The first register will then contain the output $f(n) = n + 5$.

The algorithm for g is more complicated. Let $n \in \mathbb{N}$ be input for this algorithm so that, just before it is executed on the Register Machine, $r_1 = n$ and $r_j = 0$ for $j > 1$.

The first instruction checks whether $n = 0$; if that is the case, we can terminate the program because the first register already contains the output $g(n) = 0$. Otherwise, we decrease r_1 and increase the values r_2 and r_3 (instructions 2 and 3); then we move to the 4th instruction.

At this point we have $(r_1, r_2, r_3) = (n-1, 1, 1)$. Instruction 4 then checks whether $n - 1 = 0$, i.e. $n = 1$. If that is the case, the program must never terminate because $1 \notin \mathrm{dom}(g)$, so we execute the forever-looping 14th instruction. Otherwise, we decrease r_1 by one and increase r_2 and r_3 (instructions 5 and 6); then we move to the 7th instruction.

At this point we have $(r_1, r_2, r_3) = (n-2, 2, 2)$. Lines 7, 8 and 9 then keep decreasing r_1 until it is zero, while simultaneously increasing r_2 and r_3. Then it moves to the 10th instruction.

We now have $(r_1, r_2, r_3) = (0, n, n)$. Instructions 10 and 11 then empty register R_2 while increasing register R_3. We then go to the 12th instruction.

At this point we have $(r_1, r_2, r_3) = (0, 0, 2n)$, so it only remains to move the number stored in register R_3 to R_1. This is done with instructions 12 and 13. Once R_3 has been emptied, the first register will contain the output $g(n) = 2n$ and the program will be terminated. ♦

2.3 Computable and Computably Enumerable Sets

Definition 2.4. A subset A of $\mathbb{N}^k$ is said to be *computable* (also: *recursive*) if its characteristic function $\chi_A : \mathbb{N}^k \to \mathbb{N}$ given by

$$\chi_A(n_1, \ldots, n_k) = \begin{cases} 1 & \text{if } (n_1, \ldots, n_k) \in A \\ 0 & \text{otherwise} \end{cases}$$

is computable. ♦

Two examples of computable sets are $\{(a, b) \in \mathbb{N}^2 \mid a = b\}$ and $\{(a, b) \in \mathbb{N}^2 \mid a < b\}$; their characteristic functions can be computed by the programs

$$\begin{array}{l} 1 : r_1^- \implies \langle 2, 4 \rangle \\ 2 : r_2^- \implies \langle 1, 3 \rangle \\ 3 : r_1^- \implies \langle 3, 6 \rangle \\ 4 : r_2^- \implies \langle 6, 5 \rangle \\ 5 : r_1^+ \implies \langle 6 \rangle \\ 6 : \mathrm{STOP} \end{array} \qquad \text{and} \qquad \begin{array}{l} 1 : r_1^- \implies \langle 2, 4 \rangle \\ 2 : r_2^- \implies \langle 1, 3 \rangle \\ 3 : r_1^- \implies \langle 3, 6 \rangle \\ 4 : r_2^- \implies \langle 5, 6 \rangle \\ 5 : r_1^+ \implies \langle 6 \rangle \\ 6 : \mathrm{STOP} \end{array}$$

respectively.

Definition 2.5. A subset A of $\mathbb{N}^k$ is said to be *computably enumerable* (also: *recursively enumerable*[2] or *listable*) if there exists a computable partial function $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ such that $A = \mathrm{dom}(f)$. ♦

Remark. Let $A \subseteq \mathbb{N}$. In Remark 1.11, I said that A is computably enumerable if there is a program which eventually lists any element of the set if we let it run 'long enough'. This is also the reason why computably enumerable sets may be called listable.

By Definition 2.5, the set A is computably enumerable if $A = \mathrm{dom}(f)$ for some computable *partial* function $f : \mathbb{N} \rightharpoonup \mathbb{N}$. One can show that this is equivalent to the condition that A is the

[2] also commonly abbreviated as *c.e.* or *r.e.*

range of some computable *total* function, i.e. that $A = \mathrm{ran}(g)$ for some computable $g : \mathbb{N} \to \mathbb{N}$. It follows that the elements of A can then be listed as

$$g(0), g(1), g(2), g(3), \ldots$$

Because the function g is total and computable, every value $g(n)$ can be calculated in a finite number of steps. This means that we can make some program which first calculates $g(0)$ and prints its value, then calculates $g(1)$ and prints it value, and so on. Because every $a \in A$ is of the form $g(n)$ for some $n \in \mathbb{N}$, any element of A is eventually printed if we 'wait long enough'. ♦

Computably enumerable sets play an important role in this chapter because, as the title of this chapter suggests, our main goal is to show that these sets are exponential Diophantine.

By definition, a computably enumerable set A is exactly the *domain* of some computable partial function, but the next proposition shows that it is equivalently characterized by the existence of a program which exactly halts on inputs from A.

Proposition 2.6. *Let A be a subset of $\mathbb{N}^k$. Then A is computably enumerable if and only if*

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid P \textit{ halts on input } (a_1, \ldots, a_k)\}$$

for some program P.

Proof. Let $A \subseteq \mathbb{N}^k$ be a set.

If A is computably enumerable, then $A = \mathrm{dom}(f)$ for some computable function f. Say f is computed by the program P. It follows directly from Definition 2.3 that P is such that it halts on input $(a_1, \ldots, a_k) \in \mathbb{N}^k$ if and only if $(a_1, \ldots, a_k) \in \mathrm{dom}(f) = A$.

Conversely, assume that there exists a program P, say of length N, with the property that it terminates on input $(a_1, \ldots, a_k) \in \mathbb{N}^k$ if and only if $(a_1, \ldots, a_k) \in A$. We consider the constant partial function $f : \mathbb{N}^k \rightharpoonup \mathbb{N}$ given by $(n_1, \ldots, n_k) \mapsto 0$ whose domain we *define* as A. Next, we consider the program P' obtained from P by removing its 'STOP' instruction and appending the following two instructions

$$\begin{aligned} N : r_1^- &\implies \langle N, N+1 \rangle \\ N+1 : \mathrm{STOP}& \end{aligned}$$

Then P' computes f because, on input $(a_1, \ldots, a_k) \in \mathbb{N}^k$, the N-th instruction is reached if and only if $(a_1, \ldots, a_k) \in A$, in which case the first register is emptied before halting so that the output is equal to $f(a_1, \ldots, a_k) = 0$. It follows that f is computable and therefore that $A = \mathrm{dom}(f)$ is computably enumerable by definition.

■

Remark 2.7. The main difference between a set $A \subseteq \mathbb{N}^k$ being computable and computably enumerable can be seen from the characterizations

A is computable $\iff$ there is a program P which halts on *every* input $\vec{n} \in \mathbb{N}^k$ and outputs 1 if $\vec{n} \in A$ and 0 otherwise

A is computably enumerable $\iff$ there is a program P which halts on input $\vec{n} \in \mathbb{N}^k$ if and only if $\vec{n} \in A$

which follow immediately from Definition 2.4 and Proposition 2.6. ♦

With Remark 2.7 it can be seen that the computably enumerable sets *include* the computable sets. If $A \subseteq \mathbb{N}^k$ is computable and the program P, say of length N, characterizes A in the sense of Remark 2.7, we can consider the program P' obtained from P by removing its 'STOP' instruction and appending the instructions

$$\begin{aligned} N : r_1^- &\implies \langle N+1, N\rangle \\ N+1 : \text{STOP} & \end{aligned}$$

Then, if P' is executed on some input $\vec{n} \in \mathbb{N}^k$, we know that, once the N-th instruction is reached[3], the register R_1 holds the value 1 if $\vec{n} \in A$ and 0 otherwise. Our appended instructions then make sure that P' halts on input $\vec{n}$ if and only if $\vec{n} \in A$, showing that A is computable enumerable by Proposition 2.6.

Conversely, not every computably enumerable set is computable—a fact which will turn out to be vital for showing that there can be no algorithm for determining the solvability of arbitrary Diophantine equations.

Theorem 2.8. *There is a set $\mathcal{H} \subseteq \mathbb{N}^k$ which is computably enumerable, but not computable.*

For a proof of Theorem 2.8 we refer to ([11], Proposition 3.1.1).

We end this section with the following proposition which easily results from Proposition 2.6.

Proposition 2.9. *Let $A \subseteq \mathbb{N}^k$ be a computably enumerable set. There is a program P such that*

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid P \textit{ halts on input } (a_1, \ldots, a_k) \textit{ and empties all registers before halting}\}$$

Proof. Let $A \subseteq \mathbb{N}^k$ be computably enumerable. Then

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid P \text{ halts on input } (a_1, \ldots, a_k)\} \tag{2.1}$$

for some program P by Proposition 2.6. Say length$(P) = N$ and mri$(P) = J$ and consider the program $\widetilde{P}$ obtained from P by removing its N-th ('STOP') instruction and appending the following $J+1$ instructions

$$\begin{aligned} N : r_0^- &\implies \langle N, N+1\rangle \\ N+1 : r_1^- &\implies \langle N+1, N+2\rangle \\ &\vdots \\ N+J : r_J^- &\implies \langle N+J, N+J+1\rangle \\ N+J+1 : \text{STOP} & \end{aligned}$$

Then $\widetilde{P}$ has the property that it halts on input $(a_1, \ldots, a_k)$ and empties all registers before halting if and only if P halts on input $(a_1, \ldots, a_k)$. With (2.1) we conclude that

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \widetilde{P} \text{ halts on input } (a_1, \ldots, a_k) \text{ and empties its registers before halting}\}$$

∎

[3] this instruction will always be reached because it used to be the 'STOP' instruction

2.4 An Equivalent Characterization of Halting Programs

The main goal of this section is to prove Theorem 2.11, which states that a program halts on some input if and only if there exist certain *sequences* of natural numbers satisfying some inductive, algebraic relations. This result can be seen as the first important step in showing that every computably enumerable set is exponential Diophantine.

By their very nature, exponential Diophantine sets are characterized by the existence of certain natural numbers satisfying some algebraic relation (i.e. being the root of some polynomial). Because a computably enumerable set is characterized by the existence of a program which exactly halts on inputs from that set (cf. Proposition 2.6), Theorem 2.11 will show us that such a set can also be characterized by the existence of certain *sequences* of natural numbers which satisfy a certain algebraic relation, bringing the classes of computably enumerable sets and exponential Diophantine sets a little closer together.

Remark. From now on, we shall always write $\text{length}(P) = N$ and $\text{mri}(P) = J$ whenever P denotes some (generic) program. ⧫

Let P be a program and let us write

$$C = \Big((\eta^{(0)}; \rho_1^{(0)}, \dots, \rho_J^{(0)}),\ (\eta^{(1)}; \rho_1^{(1)}, \dots, \rho_J^{(1)}),\ \dots \Big)$$

for the computation of P on input $(a_1, \dots, a_k)$, which may or may not be finite, where the computation states $(\eta^{(i)}; \rho_1^{(i)}, \dots, \rho_J^{(i)})$ satisfy the inductive relations from Definition 2.1.

We define three sequences $(r_1^{(i)}, \dots, r_J^{(i)})_{i \in \mathbb{N}}$, $(z_1^{(i)}, \dots, z_J^{(i)})_{i \in \mathbb{N}}$ and $(\sigma_1^{(i)}, \dots, \sigma_N^{(i)})_{i \in \mathbb{N}}$ of tuples of natural numbers by a 'simultaneous inductive definition scheme'. Just to be clear on where we are headed, these sequences will be defined by the formulas (2.7)—(2.14) and it is our goal is to show (by induction on i) that they satisfy

$$r_j^{(i)} = \rho_j^{(i)} \qquad \text{for all } j \in \{1, \dots, J\} \tag{2.2}$$

$$z_j^{(i)} = \operatorname{sgn} \rho_j^{(i)} \qquad \text{for all } j \in \{1, \dots, J\} \tag{2.3}$$

$$\sigma_n^{(i)} = \begin{cases} 1 & \text{if } n = \eta^{(i)} \\ 0 & \text{otherwise} \end{cases} \qquad \text{for all } n \in \{1, \dots, N\} \tag{2.4}$$

for all $i \in I$, where

$$I = \begin{cases} \{0, \dots, Q\} & \text{if } C \text{ is of finite length } Q+1 \\ \mathbb{N} & \text{if } C \text{ is infinite} \end{cases}$$

So, we will see that $r_j^{(i)}$ is nothing but the j-th register value $\rho_j^{(i)}$ at computation step i. The numbers $z_j^{(i)}$ and $\sigma_n^{(i)}$ can then be thought of as *zero-indicators* and *state-indicators* because

$$z_j^{(i)} = \begin{cases} 1 & \text{if at computation step } i \text{ the } j\text{-th register is nonempty} \\ 0 & \text{otherwise} \end{cases} \tag{2.5}$$

$$\sigma_n^{(i)} = \begin{cases} 1 & \text{if at computation step } i \text{ the } n\text{-th instruction of } P \text{ is about to be executed} \\ 0 & \text{otherwise} \end{cases} \tag{2.6}$$

In particular, it would follow that, for every i, there is exactly one $n \in \{1, \dots, N\}$ such that $\sigma_n^{(i)}$ is nonzero. We will now show how these three sequences (which carry a dependence on our program P) can be defined in such a way that (2.2)—(2.4) hold for all $i \in I$.

Remark. The symbol 'r_j' currently appears in many places. To clarify: if $j \in \{1, \ldots, J\}$, then

- r_j refers to the natural number stored in the j-th register R_j
- r_j^+ and r_j^- are in itself meaningless; they only appear as the first parts of Register Machine instructions of the form '$r_j^+ \implies \langle n \rangle$' and '$r_j^- \implies \langle n, m \rangle$'
- $\rho_j^{(i)}$ refers to the number stored in register R_j at computation step i
- $r_j^{(i)}$ is a number we are about to define

♦

For $i = 0$ we define

$$(r_1^{(0)}, r_2^{(0)}, \ldots, r_J^{(0)}) = \begin{cases} (a_1, \ldots, a_k, 0, \ldots, 0) & \text{if } k < J \\ (a_1, \ldots, a_J) & \text{if } k \geq J \end{cases} \tag{2.7}$$

$$(z_1^{(0)}, z_2^{(0)}, \ldots, z_J^{(0)}) = (\operatorname{sgn} r_1^{(0)}, \ldots, \operatorname{sgn} r_J^{(0)}) \tag{2.8}$$

$$(\sigma_1^{(0)}, \sigma_2^{(0)}, \ldots, \sigma_N^{(0)}) = (1, 0, \ldots, 0) \tag{2.9}$$

Then (2.2)—(2.4) already hold for $i = 0$ and there is exactly one $n \in \{1, \ldots, N\}$ such that $\sigma_n^{(0)}$ is nonzero.

If C has length 1 we are done. Otherwise, if C has finite length $Q + 1 > 1$, let $i + 1 \leq Q + 1$ be arbitrary and if C is infinite, let $i + 1 \in \mathbb{N}$ be arbitrary[4]. Before continuing our definition of the three sequences, note that we may assume (by induction) that the formulas (2.2)—(2.4) already hold.

We begin by defining $r_j^{(i+1)}$ which we want to do in such a way that $r_j^{(i+1)} = \rho_j^{(i+1)}$. From Definition 2.1 it is easily seen that $\rho_j^{(i+1)}$ is either equal to $\rho_j^{(i)}$ or $\rho_j^{(i)} \pm 1$. The exact value, however, is very much dependent on the value of $\eta^{(i)}$, i.e. which instruction was just about to be executed at the previous computation step i. Therefore, we consider the sets

$$\begin{aligned} \mathcal{N}_j^+ &= \left\{ n \in \{1, \ldots, N\} \;\middle|\; \begin{array}{c} \text{"the } n\text{-th instruction of } P \text{ is of the form '} r_j^+ \implies \langle u \rangle \text{'} \\ \text{for some } u\text{"} \end{array} \right\} \\ \mathcal{N}_j^- &= \left\{ n \in \{1, \ldots, N\} \;\middle|\; \begin{array}{c} \text{"the } n\text{-th instruction of } P \text{ is of the form '} r_j^- \implies \langle u, v \rangle \text{'} \\ \text{for some } u \text{ and } v\text{"} \end{array} \right\} \end{aligned} \tag{2.10}$$

which have the property that they are disjoint for all $j \in \{1, \ldots, J\}$.

Now, for all j, we define $r_j^{(i+1)}$ as follows

$$r_j^{(i+1)} = r_j^{(i)} + \sum_{n \in \mathcal{N}_j^+} \sigma_n^{(i)} - z_j^{(i)} \sum_{n \in \mathcal{N}_j^-} \sigma_n^{(i)} \tag{2.11}$$

and show that this definition implies that $r_j^{(i+1)} = \rho_j^{(i+1)}$.

Let $j \in \{1, \ldots, J\}$ be arbitrary and let $\widetilde{n}$ be the unique element of $\{1, \ldots, N\}$ such that $\sigma_{\widetilde{n}}^{(i)}$ is nonzero. Then we know from the induction hypothesis (2.4) that, at computation step

[4] if $i + 1 \leq Q + 1$ it follows that $i < Q + 1$ and, in particular, that $\eta^{(i)} \neq N$, i.e. that the program has not yet halted; otherwise C would be of length $i < Q + 1$ which is a contradiction

i, the $\widetilde{n}$-th instruction of P was about to be executed (cf. (2.6)). We consider three (mutually exclusive) cases: $\widetilde{n} \notin \mathcal{N}_j^+ \cup \mathcal{N}_j^-$, $\widetilde{n} \in \mathcal{N}_j^+$ and $\widetilde{n} \in \mathcal{N}_j^-$.

Case 1. If $\widetilde{n} \notin \mathcal{N}_j^+ \cup \mathcal{N}_j^-$, then the $\widetilde{n}$-th instruction of P does not involve the j-th register, so we must have $\rho_j^{(i+1)} = \rho_j^{(i)}$ by Definition 2.1. Recalling that $r_j^{(i)} = \rho_j^{(i)}$ by our induction hypothesis (2.2), we see from (2.11) that $r_j^{(i+1)} = \rho_j^{(i+1)}$ because both sums are equal to zero in this case.

Case 2. If $\widetilde{n} \in \mathcal{N}_j^+$ then an instruction of the form '$r_j^+ \implies \langle u \rangle$' was about to be executed, meaning that we will have $\rho_j^{(i+1)} = \rho_j^{(i)} + 1$ by Definition 2.1. Because

$$\sum_{n \in \mathcal{N}_j^+} \sigma_n^{(i)} = 1 \qquad \text{and} \qquad \sum_{n \in \mathcal{N}_j^-} \sigma_n^{(i)} = 0,$$

we see from (2.11) that $r_j^{(i+1)} = \rho_j^{(i)} + 1 = \rho_j^{(i+1)}$.

Case 3. If $\widetilde{n} \in \mathcal{N}_j^-$, then, by Definition 2.1, we have $\rho_j^{(i+1)} = \rho_j^{(i)} - 1$ if $\rho_j^{(i)} > 0$ and $\rho_j^{(i+1)} = \rho_j^{(i)}$ otherwise. Again, it is seen from (2.11) that $r_j^{(i+1)} = \rho_j^{(i+1)}$ because

$$\sum_{n \in \mathcal{N}_j^+} \sigma_n^{(i)} = 0 \qquad \text{and} \qquad z_j^{(i)} \sum_{n \in \mathcal{N}_j^-} \sigma_n^{(i)} = z_j^{(i)}$$

in this case. So

$$\begin{aligned} r_j^{(i+1)} &= r_j^{(i)} - z_j^{(i)} \\ &= \rho_j^{(i)} - \operatorname{sgn} \rho_j^{(i)} \\ &= \rho_j^{(i+1)} \end{aligned}$$

by our induction hypotheses (2.2) and (2.3).

Having defined $(r_j^{(i+1)})_{j=1}^J$ and having showed that $r_j^{(i+1)} = \rho_j^{(i+1)}$ for all j, we easily make sure that $z_j^{(i+1)} = \operatorname{sgn}(\rho_j^{(i+1)})$ holds by just defining

$$z_j^{(i+1)} = \operatorname{sgn} r_j^{(i+1)} \tag{2.12}$$

Our final goal, then, is to define $\sigma_n^{(i+1)}$ in such a way that

$$\sigma_n^{(i+1)} = \begin{cases} 1 & \text{if } n = \eta^{(i+1)} \\ 0 & \text{otherwise} \end{cases}$$

or, equivalently, such that $\sigma_n^{(i+1)} = \delta_{n\eta^{(i+1)}}$ where δ denotes Kronecker's delta. Before we show how this is done, we consider some particular sets, similar to $\mathcal{N}_j^+$ and $\mathcal{N}_j^-$ from (2.10).

Consideration 1. If the $\eta^{(i)}$-th instruction of P was of the form '$r_j^+ \implies \langle n_0 \rangle$' for some j, we have

$$\eta^{(i+1)} = n_0$$

by Definition 2.1. For instructions of this type we must therefore have $\sigma_n^{(i+1)} = \delta_{nn_0}$, motivating us to consider the set of all such instructions.

$$\mathcal{M}_n^+ = \left\{ m \in \{1, \dots, N\} \;\middle|\; \begin{array}{c} \text{“the } m\text{-th instruction of } P \text{ is of the form ‘} r_j^+ \implies \langle n \rangle \text{’} \\ \text{for some } j\text{”} \end{array} \right\} \tag{2.13a}$$

Consideration 2. If the $\eta^{(i)}$-th instruction of P was of the form '$r_j^- \implies \langle n_0, v\rangle$' or '$r_j^- \implies \langle v, n_0\rangle$' for some j and v, we would have

$$\eta^{(i+1)} = \begin{cases} n_0 & \text{if } \rho_j^{(i)} > 0 \\ v & \text{if } \rho_j^{(i)} = 0 \end{cases} \qquad \text{and} \qquad \eta^{(i+1)} = \begin{cases} v & \text{if } \rho_j^{(i)} > 0 \\ n_0 & \text{if } \rho_j^{(i)} = 0 \end{cases}$$

respectively by Definition 2.1. This shows that, in these cases, our number $\sigma_n^{(i+1)}$ must have some extra dependency on the number $\rho_j^{(i)}$ and thus on j. We therefore consider the following sets.

$$\begin{aligned} \mathcal{M}_n^1(j) &= \left\{ m \in \{1,\dots,N\} \;\middle|\; \begin{array}{c} \text{“the } m\text{-th instruction of } P \text{ is of the form} \\ \text{‘} r_j^- \implies \langle n, v\rangle\text{’ for some } v\text{”} \end{array} \right\} \\ \mathcal{M}_n^2(j) &= \left\{ m \in \{1,\dots,N\} \;\middle|\; \begin{array}{c} \text{“the } m\text{-th instruction of } P \text{ is of the form} \\ \text{‘} r_j^- \implies \langle v, n\rangle\text{’ for some } v\text{”} \end{array} \right\} \end{aligned} \tag{2.13b}$$

Note that $\mathcal{M}_n^+$ and $\mathcal{M}_n^1(j) \cup \mathcal{M}_n^2(j)$ are disjoint for all j while $\mathcal{M}_n^1(j)$ and $\mathcal{M}_n^2(j)$ need *not* be disjoint as there may be instructions of the form '$r_j^- \implies \langle n, n\rangle$'.

Now, for all n, we define $\sigma_n^{(i+1)}$ as follows

$$\sigma_n^{(i+1)} = \left(\sum_{m \in \mathcal{M}_n^+} \sigma_m^{(i)} \right) + \left(\sum_{j=1}^{J} z_j^{(i)} \sum_{m \in \mathcal{M}_n^1(j)} \sigma_m^{(i)} \right) + \left(\sum_{j=1}^{J} (1 - z_j^{(i)}) \sum_{m \in \mathcal{M}_n^2(j)} \sigma_m^{(i)} \right) \tag{2.14}$$

and show that this implies that $\sigma_n^{(i+1)} = \delta_{n\eta^{(i+1)}}$.

Let $n \in \{1,\dots,N\}$ be arbitrary and let $\widetilde{m}$ be the unique element of $\{1,\dots,N\}$ such that $\sigma_{\widetilde{m}}^{(i)}$ is nonzero. Then we know from the induction hypothesis (2.4) that, at computation step i, the $\widetilde{m}$-th instruction of P was about to be executed (cf. (2.6)). We consider, again, three (mutually exclusive) cases: $\widetilde{m} \notin \mathcal{M}_n^+ \cup \mathcal{M}_n^1(j) \cup \mathcal{M}_n^2(j)$, $\widetilde{m} \in \mathcal{M}_n^+$ and $\widetilde{m} \in \mathcal{M}_n^1(j) \cup \mathcal{M}_n^2(j)$.

Case 1. If $\widetilde{m} \notin \mathcal{M}_n^+$ and $\widetilde{m} \notin \mathcal{M}_n^1(j) \cup \mathcal{M}_n^2(j)$ for all $j \in \{1,\dots,J\}$, then there are u and v, both unequal to n, such that the $\widetilde{m}$-th instruction of P was of the form '$r_j^+ \implies \langle u\rangle$' or '$r_j^- \implies \langle u, v\rangle$' for some j. It follows (cf. Definition 2.1) that $\eta^{(i+1)} = u$ or $\eta^{(i+1)} = v$. So, because $\eta^{(i+1)} \neq n$ and because

$$\sum_{m \in \mathcal{M}_n^+} \sigma_m^{(i)} = \sum_{m \in \mathcal{M}_n^1(j)} \sigma_m^{(i)} = \sum_{m \in \mathcal{M}_n^2(j)} \sigma_m^{(i)} = 0,$$

for all j, we see from (2.14) that $\sigma_n^{(i+1)} = 0 = \delta_{n\eta^{(i+1)}}$ in this case, as desired.

Case 2. If $\widetilde{m} \in \mathcal{M}_n^+$, then the previous instruction was of the form '$r_j^+ \implies \langle n\rangle$' for some j. According to Definition 2.1, this implies that $\eta^{(i+1)} = n$. Now, because

$$\sum_{m \in \mathcal{M}_n^+} \sigma_m^{(i)} = 1 \qquad \text{and} \qquad \sum_{m \in \mathcal{M}_n^1(j)} \sigma_m^{(i)} = \sum_{m \in \mathcal{M}_n^2(j)} \sigma_m^{(i)} = 0$$

for all j, it follows from (2.14) that $\sigma_n^{(i+1)} = 1 = \delta_{n\eta^{(i+1)}}$ in this case, as desired.

Case 3. If there exists a $j_0 \in \{1,\dots,J\}$ such that $\widetilde{m} \in \mathcal{M}_n^1(j_0) \cup \mathcal{M}_n^2(j_0)$, then such a j_0 is unique and we can already see that (2.14) reduces to

$$\sigma_n^{(i+1)} = z_{j_0}^{(i)} \sum_{m \in \mathcal{M}_n^1(j_0)} \sigma_m^{(i)} + (1 - z_{j_0}^{(i)}) \sum_{m \in \mathcal{M}_n^2(j_0)} \sigma_m^{(i)}$$

Now, if $\widetilde{m} \in \mathcal{M}_n^1(j_0) \setminus \mathcal{M}_n^2(j_0)$, then the previous instruction was of the form '$r_{j_0}^- \implies \langle n, v\rangle$' for some v unequal to n. It follows from Definition 2.1 that we have $\eta^{(i+1)} = n$ if and only if $\rho_{j_0}^{(i)} > 0$ which is the case if and only if $z_{j_0}^{(i)} = 1$ by our induction hypotheses (2.2) and (2.3). Now, because

$$\sum_{m\in\mathcal{M}_n^1(j_0)} \sigma_m^{(i)} = 1 \qquad\qquad \text{and} \qquad\qquad \sum_{m\in\mathcal{M}_n^2(j)} \sigma_m^{(i)} = 0$$

it follows from our reduced version of (2.14) that $\sigma_n^{(i+1)} = 1$ if $z_{j_0}^{(i)} = 1$ and $\sigma_n^{(i+1)} = 0$ otherwise. We conclude that $\sigma_n^{(i+1)} = \delta_{n\eta^{(i+1)}}$ in this (sub)case, which is exactly what we needed to show. In a similar way it is shown that $\sigma_n^{(i+1)} = \delta_{n\eta^{(i+1)}}$ also holds in the remaining (sub)cases $\widetilde{m} \in \mathcal{M}_n^2(j) \setminus \mathcal{M}_n^1(j)$ and $\widetilde{m} \in \mathcal{M}_n^1(j) \cap \mathcal{M}_n^2(j)$.

Our findings are summarized in the following theorem.

Theorem 2.10. *Let P be a program and let*

$$C = \Big((\eta^{(0)}; \rho_1^{(0)}, \dots, \rho_J^{(0)}),\ (\eta^{(1)}; \rho_1^{(1)}, \dots, \rho_J^{(1)}),\ \dots\Big)$$

denote the computation of P on input $(a_1, \dots, a_k) \in \mathbb{N}^k$.

If there are numbers $r_1^{(i)}, \dots, r_J^{(i)}, z_1^{(i)}, \dots, z_J^{(i)}$ and $\sigma_1^{(i)}, \dots, \sigma_N^{(i)}$ satisfying conditions (2.7)—(2.14) *for all $i \in \mathbb{N}$, then they also satisfy formulas* (2.2)—(2.4) *for all $i \in I$, where*

$$I = \begin{cases} \{0, \dots, Q\} & \text{if } C \text{ is of finite length } Q+1 \\ \mathbb{N} & \text{if } C \text{ is infinite} \end{cases}$$

We are now ready to give an equivalent condition for a halting program. We know that a program P halts on input $(a_1, \dots, a_k)$ if and only if its corresponding computation is finite, which is the case if and only if there is some $Q \in \mathbb{N}$ such that $\eta^{(Q)} = N$ by Definition 2.1.

Note that formulas (2.7)—(2.14) allow us to inductively calculate the sequences $(r_1^{(i)}, \dots, r_J^{(i)})$, $(z_1^{(i)}, \dots, z_J^{(i)})$ and $(\sigma_1^{(i)}, \dots, \sigma_N^{(i)})$ for all $i \in \mathbb{N}$. So, if there exists some (least) $Q \in \mathbb{N}$ for which the conditions

$$\sigma_N^{(Q)} = 1 \tag{2.15}$$

$$(r_1^{(Q)}, \dots, r_J^{(Q)}) = (0, \dots, 0) \tag{2.16}$$

are satisfied, it would follow from Theorem 2.10 that $\eta^{(Q)} = N$ and $(\rho_1^{(Q)}, \cdots, \rho_J^{(Q)}) = (0, \dots, 0)$. By Definition 2.1, we see that P has halted on input $(a_1, \dots, a_k)$ and emptied all registers before halting. Conversely, if no $Q \in \mathbb{N}$ exists for which (2.15) and (2.16) holds, it follows from the same theorem that there is no Q for which both $\eta^{(Q)} = N$ and $(\rho_1^{(Q)}, \dots, \rho_J^{(Q)}) = (0, \dots, 0)$ hold, implying by Definition 2.1 that P either does not halt on input $(a_1, \dots, a_k)$, or that it does not empty its registers before halting (if it halts). This equivalence is summarized by the following theorem.

Theorem 2.11. *Let P be a program and $(a_1, \dots, a_k) \in \mathbb{N}^k$ some input. Then*

P halts on input $(a_1, \dots, a_k)$ and empties its registers before halting $\iff \mathcal{R}_P(a_1, \dots, a_k)$

where the predicate $\mathcal{R}_P(a_1, \dots, a_k)$ is defined as:

"there exists some (least) $Q \in \mathbb{N}$ such that there are sequences $(r_1^{(i)}, \ldots, r_J^{(i)})_{i=0}^Q$, $(z_1^{(i)}, \ldots, z_J^{(i)})_{i=0}^Q$ and $(\sigma_1^{(i)}, \ldots, \sigma_N^{(i)})_{i=0}^Q$ of natural numbers which satisfy relations (2.7)—(2.16)"

Moreover, if $\mathcal{R}_P(a_1, \ldots, a_k)$ holds, then the computation of P on input $(a_1, \ldots, a_k)$ is of finite length $Q + 1$.

Note that formulas (2.7)—(2.16) depend on some given program P and input $(a_1, \ldots, a_k) \in \mathbb{N}^k$, which is the reason why the predicate from Theorem 2.11 is denoted as $\mathcal{R}_P(a_1, \ldots, a_k)$.

Remark. Let P be a program and $(a_1, \ldots, a_k) \in \mathbb{N}^k$ some input. If we assume that the predicate $\mathcal{R}_P(a_1, \ldots, a_k)$ from Theorem 2.11 holds, then the sequence $(\sigma_1^{(i)}, \ldots, \sigma_N^{(i)})_{i=0}^Q$ has a few important properties.

First, follows from Theorem 2.11 that the computation of P on input $(a_1, \ldots, a_k)$ is of finite length $Q+1$. Because the $\sigma_n^{(i)}$'s can be thought of as state-indicators by Theorem 2.10 and (2.6), i.e.

$$\sigma_n^{(i)} = \begin{cases} 1 & \text{if at computation step } i \text{ the } n\text{-th instruction of } P \text{ is about to be executed} \\ 0 & \text{otherwise} \end{cases}$$

It follows, in particular, that

$$\sigma_N^{(i)} = \begin{cases} 1 & \text{if } i = Q \\ 0 & \text{otherwise} \end{cases} \tag{2.17}$$

which can be seen as follows. We know $\sigma_N^{(i)} = 1$ if and only if, at computation step i, the N-th instruction (i.e. the 'STOP' instruction) is about to be executed. Because the computation is of length $Q + 1$, this is possible if and only if $i = Q$.

Furthermore, whenever $m \in \mathcal{N}_j^+ \cup \mathcal{N}_j^-$ or $m \in \mathcal{M}_n^+ \cup \mathcal{M}_n^1(j) \cup \mathcal{M}_n^2(j)$, where these sets are defined by (2.10) and (2.13), it follows that the m-th instruction of P is *not* the 'STOP' instruction, i.e. that $m \neq N$. Because at the final (Q-th) computation step, we have that the N-th instruction (i.e. the 'STOP' instruction) is about to be executed, it follows that $\sigma_N^{(Q)} = 1$ and $\sigma_m^{(Q)} = 0$ whenever $m \neq N$. So, in conclusion, we have

$$m \in \mathcal{N}_j^+ \cup \mathcal{N}_j^- \cup \mathcal{M}_n^+ \cup \mathcal{M}_n^1(j) \cup \mathcal{M}_n^2(j) \implies \sigma_m^{(Q)} = 0 \tag{2.18}$$

♦

2.5 Binary Concatenation

Before we get to Theorem 2.17, however, we first have to treat the concept of *(binary) concatenation.*

Definition 2.12. Let $a = a_N \cdots a_1$ and $b = b_M \cdots b_1$ be sequences of 0's and 1's. The *(binary) concatenation* of a and b gives us the natural number $a||b$ whose binary representation is obtained by by placing the sequences a and b after each other, i.e. $a \,||\, b = a_N \cdots a_1 b_M \cdots b_{1\langle 2\rangle}$. ♦

We note that concatenation should be regarded as a function

$$|| \; : \{\text{"finite sequences of binary digits"}\} \times \{\text{"finite sequences of binary digits"}\} \to \mathbb{N}$$

rather than a function $||\ : \mathbb{N}^2 \to \mathbb{N}$. For example, the terms $3\,||\,2$ and $1\,||\,8$ are undefined because $3, 2, 8 \in \mathbb{N}$. However, the term $11\,||\,01$ *is* defined[5] and simply denotes the natural number 13.

The next lemma shows that, whenever some number $a \in \mathbb{N}$ is represented as $\cdots a_2 a_1 a_0{}_{\langle b\rangle}$ in base-b notation, with b some power of 2, the binary representations of the *digits* a_i may be glued together to obtain the binary representation of a itself.

Lemma 2.13 (Gluing Lemma). *Let $a \in \mathbb{N}$ and assume that its base-b representation is given by $a_N \cdots a_0{}_{\langle b\rangle}$, i.e.*

$$a = \sum_{i=0}^{N} a_i b^i$$

for some N, where $b = 2^{c+1}$ for some $c \in \mathbb{N}$.

If, for every $i \in \{0, \ldots, N\}$, the binary representation of the base-b digit a_i is given by

$$a_i = a_{i,M} \cdots a_{i,0}{}_{\langle 2\rangle},$$

for some $M = M(i)$, then the binary representation of a is given by

$$a = \widehat{a}_N \,||\, \widehat{a}_{N-1} \,||\, \ldots \,||\, \widehat{a}_1 \,||\, \widehat{a}_0$$

where $\widehat{a}_i$ denotes the sequence of 0's and 1's obtained by padding the binary digits of a_i with leading zero's until there are $c+1$ digits in total, i.e. where

$$\widehat{a}_i = \overbrace{0 \ldots 0 a_{i,M} \ldots a_{i,0}}^{c+1 \text{ digits}}$$

Let us give an example on how to use Lemma 2.13 before we prove it.

Example. Let $a = 1875$. We choose the hexadecimal base $b = 2^{c+1}$ with $c = 3$. Then, in base-b, our number a is represented by $a = 753_{\langle b\rangle}$. Since

$$\begin{aligned} a_0 &= 3 = 11_{\langle 2\rangle} \\ a_1 &= 5 = 101_{\langle 2\rangle} \\ a_2 &= 7 = 111_{\langle 2\rangle} \end{aligned}$$

it follows from Lemma 2.13 that the binary representation of a must be given by

$$\begin{aligned} a &= 0111 \,||\, 0101 \,||\, 0011 \\ &= 11101010011_{\langle 2\rangle} \end{aligned}$$

If we had chosen $b = 2^{c+1}$ with $c = 4$, we would have found that $a = 1(26)(19)_{\langle b\rangle}$. Since $1 = 1_{\langle 2\rangle}$, $26 = 11010_{\langle 2\rangle}$ and $19 = 10011_{\langle 2\rangle}$, we would have found the same binary representation

$$\begin{aligned} a &= 00001 \,||\, 11010 \,||\, 10011 \\ &= 11101010011_{\langle 2\rangle} \end{aligned}$$

for our number a. ♦

[5] We previously adopted the convention that the decimal base-indicator may be omitted when representing natural numbers, e.g. that $86 = 86_{\langle 10\rangle}$. We now face the problem that a term like 101 can either be seen as the natural number hundred-and-one, or simply as a sequence of 0's and 1's (without an implicit numerical value). For this reason, whenever a term like 101 appears as one of the arguments to the $||$ function, we regard it simply as a (non-numerical) sequence of 0's and 1's.

Proof (Lemma 2.13; Gluing Lemma). Assume that $a = a_N \dots a_{0\langle b \rangle}$ with $b = 2^{c+1}$ for some $c \in \mathbb{N}$. Because every sequence $\widehat{a}_i$ is of the form[6]

$$\widehat{a}_i = \overbrace{0 \dots 0 a_{i,M} \dots a_{i,0}}^{c+1 \text{ digits}}$$

we let $\widehat{a}_{i,m}$ denote the m-th digit in the $\widehat{a}_i$ sequence (right-to-left; zero-based), i.e.

$$\widehat{a}_{i,m} = \begin{cases} a_{i,m} & \text{if } 0 \leq m \leq M \\ 0 & \text{otherwise} \end{cases}$$

Then it is seen from the definition of the $a_{i,m}$'s that

$$\sum_{m=0}^{c} \widehat{a}_{i,m} 2^m = a_i \tag{2.19}$$

for all $i \in \{0, \dots, N\}$. In particular, (2.19) implies that

$$\sum_{m=0}^{c} \widehat{a}_{0,m} 2^m = a_0 b^0$$

In a similar way, it can be seen from (2.19) that

$$\begin{aligned} \sum_{m=c+1}^{2(c+1)-1} \widehat{a}_{1,m-(c+1)} 2^m &= \sum_{m=0}^{c} \widehat{a}_{1,m} 2^{m+(c+1)} \\ &= a_1 2^{c+1} \\ &= a_1 b^1 \end{aligned}$$

or, more generally, that

$$\sum_{m=i(c+1)}^{(i+1)(c+1)-1} \widehat{a}_{i,m-i(c+1)} 2^m = a_i b^i$$

for all $i \in \{0, \dots, N\}$. It then follows that

$$\begin{aligned} \widehat{a}_N \,||\, \widehat{a}_{N-1} \,||\, \dots \,||\, \widehat{a}_1 \,||\, \widehat{a}_0 &= \sum_{i=0}^{N} \left(\sum_{m=i(c+1)}^{(i+1)(c+1)-1} \widehat{a}_{i,m-i(c+1)} 2^m \right) \\ &= \sum_{i=0}^{N} a_i b^i \\ &= a \end{aligned}$$

as desired.

∎

[6] any base-b digit a_i of a can always be binary represented as $a_i = a_{i,M} \cdots a_{i,0\langle 2 \rangle}$ for some $N \leq c$; if a_i had some nonzero n-th binary digit, where $n \geq c+1$, it would follow that $a_i \geq 2^n \geq b$, contradicting that a_i is a base-b digit

The following lemma is an application of the Gluing Lemma. It is only stated for its use in the proof of Theorem 2.17, so it may be skipped for now.

Lemma 2.14. *Let $b = 2^{c+1}$ for some $c \in \mathbb{N}$ and let $\widetilde{z}$ and $\widetilde{\sigma}$ be natural numbers whose base-b representations are given by*

$$\widetilde{z} = \sum_{i=0}^{q} z_i b^i \qquad \text{and} \qquad \widetilde{\sigma} = \sum_{i=0}^{q} \sigma_i b^i$$

If $z_i \in \{0,1\}$ and $\sigma_i \in \{0,1\}$ for all $i \in \{0,\dots,q\}$, then the base-b representation of the binary product $\widetilde{z} * \widetilde{\sigma}$ is given by

$$\widetilde{z} * \widetilde{\sigma} = \sum_{i=0}^{q} z_i \sigma_i b^i$$

Furthermore, if we define $e = \sum_{i=0}^{q} b^i$, then the base-b representation of $(e - \widetilde{z}) * \widetilde{\sigma}$ is given by

$$(e - \widetilde{z}) * \widetilde{\sigma} = \sum_{i=0}^{q} (1 - z_i)\sigma_i b^i$$

Proof. Let $i \in \{0,\dots,q\}$. Because z_i and σ_i both lie in $\{0,1\}$, their binary representations are trivially given by

$$z_i = \overbrace{00\cdots 00z_i}^{c+1 \text{ digits}}{}_{\langle 2\rangle} \qquad \text{and} \qquad \sigma_i = \overbrace{00\cdots 00\sigma_i}^{c+1 \text{ digits}}{}_{\langle 2\rangle}$$

Furthermore, the binary representation of 1 is trivially given by

$$1 = \overbrace{00\cdots 001}^{c+1 \text{ digits}}{}_{\langle 2\rangle}$$

It then follows from the Gluing Lemma that the binary representations of our numbers $\widetilde{z}$, $\widetilde{\sigma}$ and e are given by

$$\widetilde{z} = \overbrace{00\cdots 00z_q \,||\, 00\cdots 00z_{q-1} \,||\, \cdots\cdots \,||\, 00\cdots 00z_1 \,||\, 00\cdots 00z_0}^{(q+1)\times(c+1) \text{ digits}}$$
$$\widetilde{\sigma} = \overbrace{00\cdots 00\sigma_q \,||\, 00\cdots 00\sigma_{q-1} \,||\, \cdots\cdots \,||\, 00\cdots 00\sigma_1 \,||\, 00\cdots 00\sigma_0}^{(q+1)\times(c+1) \text{ digits}}$$
$$e = \overbrace{00\ldots 001 \,||\, 00\cdots 001 \,||\, \cdots\cdots \,||\, 00\cdots 001 \,||\, 00\cdots 001}^{(q+1)\times(c+1) \text{ digits}}$$

so that

$$e - \widetilde{z} = \overbrace{00\cdots 00(1-z_q) \,||\, 00\cdots 00(1-z_{q-1}) \,||\, \cdots\cdots \,||\, 00\cdots 00(1-z_1) \,||\, 00\cdots 00(1-z_0)}^{(q+1)\times(c+1) \text{ digits}}$$

It is now easily seen that the binary products $\widetilde{z} * \widetilde{\sigma}$ and $(e - \widetilde{z}) * \widetilde{\sigma}$ are binary represented by

$$\widetilde{z} * \widetilde{\sigma} = \overbrace{00\cdots 00(z_q\sigma_q) \,||\, \cdots\cdots \,||\, 00\cdots 00(z_0\sigma_0)}^{(q+1)\times(c+1) \text{ digits}}$$
$$(e - \widetilde{z}) * \widetilde{\sigma} = \overbrace{00\cdots 00((1-z_q)\sigma_q) \,||\, \cdots\cdots \,||\, 00\cdots 00((1-z_0)\sigma_0)}^{(q+1)\times(c+1) \text{ digits}}$$

It finally follows from the Gluing Lemma that the binary representations of the base-b digits of $\widetilde{z} * \widetilde{\sigma}$ and $(e - \widetilde{z}) * \widetilde{\sigma}$ must be given by

$$\mathrm{Digit}(\widetilde{z} * \widetilde{\sigma}, b, i) = \overbrace{00 \cdots 00(z_i\sigma_i)}^{c+1 \text{ digits}}{}_{\langle 2 \rangle}$$
$$\mathrm{Digit}((e - \widetilde{z}) * \widetilde{\sigma}, b, i) = \overbrace{00 \cdots 00((1 - z_i)\sigma_i)}^{c+1 \text{ digits}}{}_{\langle 2 \rangle}$$

So, we see that

$$\mathrm{Digit}(\widetilde{z} * \widetilde{\sigma}, b, i) = \begin{cases} z_i\sigma_i & \text{if } i \in \{0, \dots, q\} \\ 0 & \text{otherwise} \end{cases}$$
$$\mathrm{Digit}((e - \widetilde{z}) * \widetilde{\sigma}, b, i) = \begin{cases} (1 - z_i)\sigma_i & \text{if } i \in \{0, \dots, q\} \\ 0 & \text{otherwise} \end{cases}$$

and thus that the base-b representation of $\widetilde{z} * \widetilde{\sigma}$ and $(e - \widetilde{z}) * \widetilde{\sigma}$ are given by

$$\widetilde{z} * \widetilde{\sigma} = \sum_{i=0}^{q} z_i\sigma_i b^i \qquad \text{and} \qquad (e - \widetilde{z}) * \widetilde{\sigma} = \sum_{i=0}^{q} (1 - z_i)\sigma_i b^i$$

∎

2.6 The DPR Theorem

The goal of this final section is to prove Theorem 2.17 from which it will easily follow, in combination with Proposition 2.9, that every computably enumerable set is exponential Diophantine. This theorem (known as the *Davis-Putnam-Robinson Theorem* or simply *DPR Theorem*) was first published in [4] in 1961 and resulted from the combined efforts of American logicians Martin Davis, Hilary Putnam and Julia Robinson. This was nine years before Matiyasevich provided the final step in the resolution of Hilbert's tenth problem in 1970.

Remark 2.15. From now on, if P denotes some (generic) program, we shall attribute to P not only the numbers $N = \mathrm{length}(P)$ and $J = \mathrm{mri}(P)$, but also, for every $n \in \{1, \dots, N\}$ and $j \in \{1, \dots, J\}$, the sets

$$\mathcal{N}_j^+ = \left\{ n \in \{1, \dots, N\} \;\middle|\; \begin{array}{c} \text{“the } n\text{-th instruction of } P \text{ is of the form} \\ \text{‘} r_j^+ \implies \langle u \rangle \text{’ for some } u\text{”} \end{array} \right\}$$
$$\mathcal{N}_j^- = \left\{ n \in \{1, \dots, N\} \;\middle|\; \begin{array}{c} \text{“the } n\text{-th instruction of } P \text{ is of the form} \\ \text{‘} r_j^- \implies \langle u, v \rangle \text{’ for some } u \text{ and } v\text{”} \end{array} \right\}$$

and

$$\mathcal{M}_n^+ = \left\{ m \in \{1, \dots, N\} \;\middle|\; \begin{array}{c} \text{“the } m\text{-th instruction of } P \text{ is of the form} \\ \text{‘} r_j^+ \implies \langle n \rangle \text{’ for some } j\text{”} \end{array} \right\}$$
$$\mathcal{M}_n^1(j) = \left\{ m \in \{1, \dots, N\} \;\middle|\; \begin{array}{c} \text{“the } m\text{-th instruction of } P \text{ is of the form} \\ \text{‘} r_j^- \implies \langle n, v \rangle \text{’ for some } v\text{”} \end{array} \right\}$$
$$\mathcal{M}_n^2(j) = \left\{ m \in \{1, \dots, N\} \;\middle|\; \begin{array}{c} \text{“the } m\text{-th instruction of } P \text{ is of the form} \\ \text{‘} r_j^- \implies \langle v, n \rangle \text{’ for some } v\text{”} \end{array} \right\}$$

♦

For convenience, let us restate the definition of the $\mathcal{R}_P(a_1, \ldots, a_k)$ predicate from Theorem 2.11 here in its entirety; we will be using it a lot.

Definition 2.16. Let P be some program and $(a_1, \ldots, a_k) \in \mathbb{N}^k$ some k-tuple. The predicate $\mathcal{R}_P(a_1, \ldots, a_k)$ is defined to hold if and only if there is some (least) $Q \in \mathbb{N}$ such that there are sequences $(r_1^{(i)}, \ldots, r_J^{(i)})_{i=0}^Q$, $(z_1^{(i)}, \ldots, z_J^{(i)})_{i=0}^Q$ and $(\sigma_1^{(i)}, \ldots, \sigma_N^{(i)})_{i=0}^Q$ of natural numbers which satisfy

$$(r_1^{(0)}, \ldots, r_J^{(0)}) = \begin{cases} (a_1, \ldots, a_k, 0, \ldots, 0) & \text{if } k < J \\ (a_1, \ldots, a_J) & \text{if } k \geq J \end{cases} \tag{2.20}$$

$$(z_1^{(0)}, \ldots, z_J^{(0)}) = (\operatorname{sgn} r_1^{(0)}, \ldots, \operatorname{sgn} r_J^{(0)}) \tag{2.21}$$

$$(\sigma_1^{(0)}, \ldots, \sigma_N^{(0)}) = (1, 0, \ldots, 0) \tag{2.22}$$

together with, for all $j \in \{1, \ldots, J\}$ and $n \in \{1, \ldots, N\}$, the inductive relations

$$r_j^{(i+1)} = r_j^{(i)} + \sum_{n \in \mathcal{N}_j^+} \sigma_n^{(i)} - z_j^{(i)} \sum_{n \in \mathcal{N}_j^-} \sigma_n^{(i)} \tag{2.23}$$

$$z_j^{(i+1)} = \operatorname{sgn} r_j^{(i+1)} \tag{2.24}$$

$$\sigma_n^{(i+1)} = \left(\sum_{m \in \mathcal{M}_n^+} \sigma_m^{(i)} \right) + \left(\sum_{j=1}^J z_j^{(i)} \sum_{m \in \mathcal{M}_n^1(j)} \sigma_m^{(i)} \right) + \left(\sum_{j=1}^J (1 - z_j^{(i)}) \sum_{m \in \mathcal{M}_n^2(j)} \sigma_m^{(i)} \right), \tag{2.25}$$

and the halting relations

$$\sigma_N^{(Q)} = 1 \tag{2.26}$$

$$(r_1^{(Q)}, \ldots, r_J^{(Q)}) = (0, \ldots, 0) \tag{2.27}$$

♦

We now arrive at the main theorem of this section.

Theorem 2.17. *Let P be a program and $(a_1, \ldots, a_k) \in \mathbb{N}^k$ some k-tuple. Then*

$$P \textit{ halts on input } (a_1, \ldots, a_k) \textit{ and empties its registers before halting}$$

$$\Longleftrightarrow$$

$$\exists q b c d e f \widetilde{r}_1 \cdots \widetilde{r}_J \widetilde{z}_1 \cdots \widetilde{z}_J \widetilde{\sigma}_1 \cdots \widetilde{\sigma}_N \in \mathbb{N}\big(\phi_1 \wedge \cdots \wedge \phi_{14}\big)$$

with the formulas $\phi_1, \ldots, \phi_{14}$ given by

$$b = 2^{c+1} \tag{ϕ_1}$$

$$d = \sum_{i=0}^q (2^c - 1) b^i \tag{ϕ_2}$$

$$e = \sum_{i=0}^q b^i \tag{ϕ_3}$$

$$f = \sum_{i=0}^{q} 2^c b^i \tag{ϕ_4}$$

$$\bigwedge_{j=1}^{J} \widetilde{r}_j \preccurlyeq d \tag{ϕ_5}$$

$$\bigwedge_{j=1}^{J} \widetilde{z}_j \preccurlyeq e \tag{ϕ_6}$$

$$\bigwedge_{n=1}^{N} \widetilde{\sigma}_n \preccurlyeq e \tag{ϕ_7}$$

$$\bigwedge_{\ell=1}^{k} a_\ell < 2^c \tag{ϕ_8}$$

$$N(2J+1) < 2^c \tag{ϕ_9}$$

$$\bigwedge_{j=1}^{J} \widetilde{r}_j = b \left(\widetilde{r}_j + \sum_{n \in \mathcal{N}_j^+} \widetilde{\sigma}_n - \sum_{n \in \mathcal{N}_j^-} \widetilde{z}_j * \widetilde{\sigma}_n \right) + \begin{cases} a_j & \textit{if } j \le k \\ 0 & \textit{otherwise} \end{cases} \tag{ϕ_{10}}$$

$$\bigwedge_{j=1}^{J} 2^c \widetilde{z}_j = f * (\widetilde{r}_j + d) \tag{ϕ_{11}}$$

$$\begin{aligned} \bigwedge_{n=1}^{N} \widetilde{\sigma}_n = b \left(\sum_{m \in \mathcal{M}_n^+} \widetilde{\sigma}_m + \sum_{j=1}^{J} \sum_{m \in \mathcal{M}_n^1(j)} \widetilde{z}_j * \widetilde{\sigma}_m + \sum_{j=1}^{J} \sum_{m \in \mathcal{M}_n^2(j)} (e - \widetilde{z}_j) * \widetilde{\sigma}_m \right) \\ + \begin{cases} 1 & \textit{if } n = 1 \\ 0 & \textit{otherwise} \end{cases} \end{aligned} \tag{ϕ_{12}}$$

$$\widetilde{\sigma}_N = b^q \tag{ϕ_{13}}$$

$$\bigwedge_{j=1}^{J} \mathrm{Digit}(\widetilde{r}_j, b, q) = 0 \tag{ϕ_{14}}$$

Proof. In the light of Theorem 2.11, it suffices to prove that

$$\mathcal{R}_P(a_1, \ldots, a_k) \iff \exists qbcdef\widetilde{r}_1 \cdots \widetilde{r}_J \widetilde{z}_1 \cdots \widetilde{z}_J \widetilde{\sigma}_1 \cdots \widetilde{\sigma}_N \in \mathbb{N} \big(\phi_1 \wedge \cdots \wedge \phi_{14} \big) \tag{2.28}$$

where $\mathcal{R}_P(a_1, \ldots, a_k)$ denotes the predicate from Definition 2.16.

Let us first make some remarks regarding the numbers d, e and f defined by formulas ϕ_2, ϕ_3 and ϕ_4. If $c \in \mathbb{N}$, then the binary representation of the number $2^c - 1$ consists of a single block of 1's of length c, i.e. we can write

$$2^c - 1 = \overbrace{011 \cdots 11}^{c+1 \text{ digits}}{}_{\langle 2 \rangle} \tag{2.29}$$

It can then be seen from (2.29) that, for all $x \in \mathbb{N}$, we have

$$x \preccurlyeq 2^c - 1 \iff x \le 2^c - 1 \tag{2.30}$$

Certainly, $x \preccurlyeq 2^c - 1$ implies that $x \le 2^c - 1$. For the converse, say $x = \cdots x_2 x_1 x_{0\langle 2 \rangle}$. If $x \le 2^c - 1$, then we must have $x_n = 0$ whenever $n \ge c$ because, if x had some nonzero n-th binary digit with $n \geq c$, it would follow that $x \geq 2^n \geq 2^c$, which is clearly a contradiction. So $x = x_{c-1} \cdots x_{0\langle 2\rangle}$. Because $x_n \in \{0,1\}$ for all n, and because, in binary, $2^c - 1$ consists of a single block of 1's of length c, cf. (2.29), it follows immediately that x must be masked by $2^c - 1$, i.e. that $x \preccurlyeq 2^c - 1$.

Furthermore, it follows from (2.29) and the Gluing Lemma that the binary representation of d, as defined by ϕ_2, is given by

$$d = \overbrace{011\cdots 11 \,||\, 011\cdots 11 \,||\, \cdots\cdots \,||\, 011\cdots 11 \,||\, 011\cdots 11}^{(q+1)\times(c+1)\text{ digits}} \tag{2.31}$$

Similarly, because the binary representations of the numbers 1 and 2^c are given by

$$1 = \overbrace{00\cdots 001}^{c+1\text{ digits}}{}_{\langle 2\rangle} \qquad \text{and} \qquad 2^c = \overbrace{100\cdots 00}^{c+1\text{ digits}}{}_{\langle 2\rangle}$$

respectively, it follows from the Gluing Lemma that the binary representations of e and f, as defined by ϕ_3 and ϕ_4, are given by

$$e = \overbrace{00\cdots 001 \,||\, 00\cdots 001 \,||\, \cdots\cdots \,||\, 00\cdots 001 \,||\, 00\cdots 001}^{(q+1)\times(c+1)\text{ digits}} \tag{2.32}$$

$$f = \overbrace{100\cdots 00 \,||\, 100\cdots 00 \,||\, \cdots\cdots \,||\, 100\cdots 00 \,||\, 100\cdots 00}^{(q+1)\times(c+1)\text{ digits}} \tag{2.33}$$

The Sufficiency

We begin by showing that the right hand side of (2.28) is sufficient for $\mathcal{R}_P(a_1,\ldots,a_k)$.

Let $q, b, c, d, e, f, \widetilde{r}_1, \ldots, \widetilde{r}_J, \widetilde{z}_1, \ldots, \widetilde{z}_J, \widetilde{\sigma}_1, \ldots, \widetilde{\sigma}_N \in \mathbb{N}$ be such that the formulas $\phi_1, \ldots, \phi_{14}$ hold. We begin by letting $Q = q$ and we shall use q and Q interchangeably. Next, we define the sequences $(r_1^{(i)}, \ldots, r_J^{(i)})_{i=0}^Q$, $(z_1^{(i)}, \ldots, z_J^{(i)})_{i=0}^Q$ and $(\sigma_1^{(i)}, \ldots, \sigma_N^{(i)})_{i=0}^Q$ as follows. For all $i \in \{0, \ldots, Q\}$, let

$$(r_1^{(i)}, \ldots, r_J^{(i)}) = \big(\mathrm{Digit}(\widetilde{r}_1, b, i), \ldots, \mathrm{Digit}(\widetilde{r}_J, b, i)\big) \tag{2.34}$$

$$(z_1^{(i)}, \ldots, z_J^{(i)}) = \big(\mathrm{Digit}(\widetilde{z}_1, b, i), \ldots, \mathrm{Digit}(\widetilde{z}_J, b, i)\big) \tag{2.35}$$

$$(\sigma_1^{(i)}, \ldots, \sigma_N^{(i)}) = \big(\mathrm{Digit}(\widetilde{\sigma}_1, b, i), \ldots, \mathrm{Digit}(\widetilde{\sigma}_N, b, i)\big) \tag{2.36}$$

so that, by definition of Digit, we have

$$\widetilde{r}_j = \lambda_j b^{q+1} + \sum_{i=0}^{q} r_j^{(i)} b^i$$

$$\widetilde{z}_j = \mu_j b^{q+1} + \sum_{i=0}^{q} z_j^{(i)} b^i$$

$$\widetilde{\sigma}_n = \nu_n b^{q+1} + \sum_{i=0}^{q} \sigma_n^{(i)} b^i$$

for all $j \in \{1, \ldots, J\}$ and $n \in \{1, \ldots, N\}$, where obviously $r_j^{(i)}, z_j^{(i)}, \sigma_n^{(i)} < b$ and where λ_j, μ_j and ν_n denote certain (irrelevant) natural numbers.

In fact, we can show that $\lambda_j = \mu_j = \nu_n = 0$. This follows from the fact that $\widetilde{r}_j$ is masked by d and $\widetilde{z}_j$ and $\widetilde{\sigma}_n$ are both masked by e, according to ϕ_5, ϕ_6 and ϕ_7. From the binary representations (2.31) and (2.32) of d and e it can then be seen, together with the Gluing Lemma, that these masking relations can only hold if $\lambda_j = \mu_j = \nu_n = 0$. This is so because, if $\lambda_j > 0$ for example, it would follow that $\widetilde{r}_j$ has some nonzero i-th base-b digit, where $i > q$. It would then follow that $\widetilde{r}_j$ can't be masked by the number d, whose binary representation consists of only $q+1$ blocks of $c+1$ digits by (2.31), because the binary representation of $\widetilde{r}_j$ would have some extra (nonzero) block of digits somewhere by the Gluing Lemma.

So, we must have

$$\widetilde{r}_j = \sum_{i=0}^{q} r_j^{(i)} b^i \tag{2.37}$$

$$\widetilde{z}_j = \sum_{i=0}^{q} z_j^{(i)} b^i \tag{2.38}$$

$$\widetilde{\sigma}_n = \sum_{i=0}^{q} \sigma_n^{(i)} b^i \tag{2.39}$$

We are now required to show that our sequences (2.34)—(2.36) satisfy the characterizing relations (2.20)—(2.27) of a halting program.

We first show that (2.20) holds. It follows from ϕ_{10} that, for all $j \in \{1, \ldots, J\}$, we have

$$\widetilde{r}_j = bA + \begin{cases} a_j & \text{if } j \leq k \\ 0 & \text{otherwise} \end{cases}$$

for some $A \in \mathbb{N}$, where $a_j < b$ by ϕ_8 and ϕ_1. On the other hand, it follows from (2.37) that

$$\widetilde{r}_j = bB + r_j^{(0)}$$

for some $B \in \mathbb{N}$, where $r_j^{(0)} < b$ because $r_j^{(0)}$ is a base-b digit. So, with the Euclidean division theorem we see that $A = B$ and

$$r_j^{(0)} = \begin{cases} a_j & \text{if } j \leq k \\ 0 & \text{otherwise} \end{cases}$$

So (2.20) holds.

To see that (2.21) and (2.24) hold, we first show that $z_j^{(i)} \in \{0, 1\}$ for all i and j. To begin, ϕ_6 tells us that $\widetilde{z}_j \preccurlyeq e$ must hold, where

$$e = \overbrace{00\cdots001 \,||\, 00\cdots001 \,||\, \cdots\cdots \,||\, 00\cdots001 \,||\, 00\cdots001}^{(q+1)\times(c+1)\text{ digits}}$$

by (2.32). Now, because

$$\widetilde{z}_j = \sum_{i=0}^{q} z_j^{(i)} b^i$$

by (2.38), it follows from the Gluing Lemma that $\widetilde{z}_j \preccurlyeq e$ can only hold if the binary representation of each base-b digit $z_j^{(i)}$ is either given by

$$\overbrace{00\cdots001}^{c+1\text{ digits}}{}_{\langle 2\rangle} \qquad \text{or} \qquad \overbrace{00\cdots000}^{c+1\text{ digits}}{}_{\langle 2\rangle},$$

so we see that $z_j^{(i)} \in \{0,1\}$ for all i and j. In exactly the same way, it can be shown with ϕ_7 that $\sigma_n^{(i)} \in \{0,1\}$ for all i and n. So

$$z_j^{(i)} \in \{0,1\} \qquad \text{and} \qquad \sigma_n^{(i)} \in \{0,1\} \tag{2.40}$$

for all $i \in \{0,\ldots,Q\}$, $j \in \{1,\ldots,J\}$ and $n \in \{1,\ldots,N\}$.

We will now show that $z_j^{(i)} = \mathrm{sgn}(r_j^{(i)})$ for all i and j. We begin by considering the number $r_j^{(i)} + 2^c - 1$, which has an interesting property. First note that ϕ_5 tells us that $\widetilde{r}_j \preccurlyeq d$, implying that

$$\sum_{i=0}^{q} r_j^{(i)} b^i \preccurlyeq \overbrace{011\cdots11 \,||\, 011\cdots11 \,||\, \cdots\cdots \,||\, 011\cdots11 \,||\, 011\cdots11}^{(q+1)\times(c+1)\text{ digits}}$$

by (2.37) and (2.31). By the Gluing Lemma, this is only possible if each base-b digit $r_j^{(i)}$ is masked by a block of 1's of length c, i.e. if $r_j^{(i)} \preccurlyeq 11\cdots11_{\langle 2\rangle}$. It then follows from (2.29) and (2.30) that

$$r_j^{(i)} \leq 2^c - 1 \tag{2.41}$$

So, we see with (2.41) that $r_j^{(i)} + 2^c - 1 < 2^{c+1}$, implying that only the first $c+1$ binary digits of $r_j^{(i)} + 2^c - 1$ can be nonzero. Knowing this, it is easily seen that our number $r_j^{(i)} + 2^c - 1$ has the following property.

- If $r_j^{(i)} = 0$, then $r_j^{(i)} + 2^c - 1 = \overbrace{011\cdots11}^{c+1\text{ digits}}{}_{\langle 2\rangle}$.
- If $r_j^{(i)} > 0$, then $r_j^{(i)} + 2^c - 1 = \overbrace{1\delta_{i,c-1}\delta_{1,c-2}\cdots\delta_{i,1}\delta_{i,0}}^{c+1\text{ digits}}{}_{\langle 2\rangle}$ for certain (irrelevant) binary digits $\delta_{i,0},\ldots,\delta_{i,c-1} \in \{0,1\}$.

So, we see that the $(c+1)$-th binary digit of $r_j^{(i)} + 2^c - 1$ is equal to 0 if $r_j^{(i)} = 0$ and equal to 1 otherwise, i.e. that

$$\mathrm{Digit}(r_j^{(i)} + 2^c - 1, 2, c+1) = \mathrm{sgn}\ r_j^{(i)} \tag{2.42}$$

Now, by (2.37) and ϕ_2, we have that

$$\widetilde{r}_j + d = \sum_{i=0}^{q} (r_j^{(i)} + 2^c - 1) b^i \tag{2.43}$$

So, if we take the binary product of $\widetilde{r}_j + d$ and our number f, whose binary representation is given by (2.33), it follows from (2.43) and (2.42) that

$$f * (\widetilde{r}_j + d) = \overbrace{\mathrm{sgn}(r_j^{(q)})00\cdots00 \,||\, \cdots\cdots \,||\, \mathrm{sgn}(r_j^{(0)})00\cdots00}^{(q+1)\times(c+1)\text{ digits}} \tag{2.44}$$

Furthermore, because we have already shown that $z_j^{(i)} \in \{0,1\}$ for all i and j, it is easily seen that the binary representation of $2^c z_j^{(i)}$ is given by

$$2^c z_j^{(i)} = \overbrace{z_j^{(i)}00\cdots00}^{c+1\text{ digits}}{}_{\langle 2\rangle}$$

so that

$$2^c\widetilde{z}_j = \sum_{i=0}^{q} 2^c z_j^{(i)} b^i = \overbrace{z_j^{(q)}00\cdots00 \,||\, \cdots\cdots \,||\, z_j^{(0)}00\cdots00}^{(q+1)\times(c+1)\text{ digits}} \tag{2.45}$$

by the Gluing Lemma. Finally, because $2^c\widetilde{z}_j = f * (\widetilde{r}_j + d)$ by ϕ_{11}, we conclude from (2.45) and (2.44) that $z_j^{(i)} = \operatorname{sgn}(r_j^{(i)})$ for all i and j. So the relations (2.21) and (2.24) hold.

To show that (2.22) holds, we use a familiar argument. If $n \in \{1, \ldots, N\}$, it follows from ϕ_{12} that

$$\widetilde{\sigma}_n = bA + \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

for some $A \in \mathbb{N}$, where $1 < b$. On the other hand, it follows from (2.36) that

$$\widetilde{\sigma}_n = bB + \sigma_n^{(0)}$$

for some $B \in \mathbb{N}$, where $\sigma_n^{(0)} < b$ because $\sigma_n^{(0)}$ is a base-b digit. With the Euclidean division theorem we conclude that $A = B$ and

$$\sigma_n^{(0)} = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$$

i.e. that (2.22) holds as well.

It remains to show that the inductive relations (2.23) and (2.25) and the halting relations (2.26) and (2.27) hold. We begin with the halting relations.

According to ϕ_{13} we have $\widetilde{\sigma}_N = b^q$, showing that the base-$b$ representation of $\widetilde{\sigma}$ is given by

$$\widetilde{\sigma}_N = \overbrace{100\cdots00}^{q+1\text{ digits}}{}_{\langle 2\rangle}$$

showing that $\operatorname{Digit}(\widetilde{\sigma}_N, b, q) = 1$ and $\operatorname{Digit}(\widetilde{\sigma}_N, b, i) = 0$ for all $i \neq q$. It then follows from our definition (2.36) of the $\sigma_N^{(i)}$'s that

$$\sigma_N^{(i)} = \begin{cases} 1 & \text{if } i = Q \\ 0 & \text{otherwise} \end{cases} \tag{2.46}$$

implying that the first halting relation (2.26) holds. The second halting relation (2.27) immediately follows from our definition (2.34) of the $r_j^{(Q)}$'s and formula ϕ_{14}.

It now remains to show that the inductive relations (2.23) and (2.25) hold. We begin by showing how (2.25) follows from ϕ_{12}.

First, note that $\operatorname{Digit}(1, b, i+1) = 0$ for all $i \in \mathbb{N}$ because if $\operatorname{Digit}(1, b, i+1) > 0$ for some i, it would follow that $1 \geq b^{i+1}$, which is clearly a contradiction by ϕ_1. So, with part a) of Lemma 1.14, it follows from ϕ_{12} that

$$\begin{aligned}&\operatorname{Digit}(\widetilde{\sigma}_n, b, i+1) \\ &\qquad = \operatorname{Digit}\left(b\Big(\sum_{m\in\mathcal{M}_n^+} \widetilde{\sigma}_m + \sum_{j=1}^{J} \sum_{m\in\mathcal{M}_n^1(j)} \widetilde{z}_j * \widetilde{\sigma}_m + \sum_{j=1}^{J} \sum_{m\in\mathcal{M}_n^2(j)} (e - \widetilde{z}_j) * \widetilde{\sigma}_m\Big), b, i+1\right)\end{aligned}$$

By part b) of Lemma 1.14 and the definition of $\sigma_n^{(i+1)}$, cf. (2.36), the above equation is then equivalent to

$$\sigma_n^{(i+1)} = \text{Digit}\left(\Big(\sum_{m\in\mathcal{M}_n^+} \widetilde{\sigma}_m + \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^1(j)} \widetilde{z}_j * \widetilde{\sigma}_m + \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^2(j)} (e-\widetilde{z}_j) * \widetilde{\sigma}_m\Big), b, i\right) \tag{2.47}$$

Let $n \in \{1,\dots,N\}$ and $i \in \{0,\dots,q\}$ be arbitrary. We define the number $S(n,i)$ as follows

$$\begin{aligned} S(n,i) = \sum_{m\in\mathcal{M}_n^+} \text{Digit}(\widetilde{\sigma}_m, b, i) + \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^1(j)} \text{Digit}(\widetilde{z}_j * \widetilde{\sigma}_m, b, i) \\ + \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^2(j)} \text{Digit}((e-\widetilde{z}_j) * \widetilde{\sigma}_m, b, i) \end{aligned} \tag{2.48}$$

We want to show that $0 \le S(n,i) < b$ for all $i \in \{0,\dots,q\}$, because it would then follow from Corollary 1.15 that the Digit function in (2.47) can be distributed over the summation, i.e. that

$$\sigma_n^{(i+1)} = S(n,i) \tag{2.49}$$

for all $i \in \{0,\dots,q\}$. However, before we show that $0 \le S(n,i) < b$, let us rewrite this number $S(n,i)$ into a different form. We know that $\text{Digit}(\widetilde{\sigma}, b, i) = \sigma_b^{(i)}$ by (2.36). Furthermore, it follows from (2.38) and (2.39), together with condition (2.40), that we can apply Lemma 2.14 to find that the base-b representations of $\widetilde{z}_j * \widetilde{\sigma}_m$ and $(e-\widetilde{z}_j) * \widetilde{\sigma}_m$ are given by

$$\begin{aligned} \widetilde{z}_j * \widetilde{\sigma}_m &= \sum_{i=0}^{q} z_j^{(i)} \sigma_m^{(i)} b^i \\ (e-\widetilde{z}_j) * \widetilde{\sigma}_m &= \sum_{i=0}^{q} (1-z_j^{(i)}) \sigma_m^{(i)} b^i \end{aligned} \tag{2.50}$$

so that $\text{Digit}(\widetilde{z}_j * \widetilde{\sigma}, b, i) = z_j^{(i)}\sigma_m^{(i)}$ and $\text{Digit}((e-\widetilde{z}_j) * \widetilde{\sigma}_m, b, i) = (1-z_j^{(i)})\sigma_m^{(i)}$. It follows that (2.48) can be rewritten as

$$S(n,i) = \sum_{m\in\mathcal{M}_n^+} \sigma_m^{(i)} + \sum_{j=1}^{J} z_j^{(i)} \sum_{m\in\mathcal{M}_n^1(j)} \sigma_m^{(i)} + \sum_{j=1}^{J} (1-z_j^{(i)}) \sum_{m\in\mathcal{M}_n^2(j)} \sigma_m^{(i)} \tag{2.51}$$

Now, with (2.51) and the definition of the sets $\mathcal{M}_n^+$, $\mathcal{M}_n^1(j)$ and $\mathcal{M}_n^2(j)$, it is easily seen that $0 \le S(n,i) < b$ for all $i \in \{0,\dots,q\}$. From (2.40) it already follows that $0 \le S(n,i)$. Furthermore, we have

$$\begin{aligned} S(n,i) &\le \sum_{m\in\mathcal{M}_n^+} 1 + \sum_{j=1}^{J} 1 \sum_{m\in\mathcal{M}_n^1(j)} 1 + \sum_{j=1}^{J} 1 \sum_{m\in\mathcal{M}_n^2(j)} 1 && \text{by (2.40)} \\ &= |\mathcal{M}_n^+| + J|\mathcal{M}_n^1(j)| + J|\mathcal{M}_n^2(j)| \\ &\le N + 2JN && \text{by Remark 2.15} \\ &< b && \text{by } \phi_9 \text{ and } \phi_1 \end{aligned}$$

Because we have already argued that, according to Corollary 1.15, the condition $0 \leq S(n,i) < b$ is sufficient for (2.49), we conclude that (2.49) and (2.51) both hold. Together, they finally imply the inductive relation (2.25).

Before moving on, we prove a property of our sequence $(\sigma_1^{(i)}, \dots, \sigma_N^{(i)})_{i=0}^{Q}$ which is needed for showing that the final inductive relation (2.23) holds. It is the following property:

$$\text{“there is exactly one } \zeta \in \{1, \dots, N\} \text{ such that } \sigma_\zeta^{(i)} = 1\text{, the other } \sigma_n^{(i)}\text{'s being zero”} \tag{2.52}$$

for all $i \in \{0, \dots, Q\}$

We proceed by induction on i. Clearly (2.52) holds for $i = 0$ because we have already shown that (2.22) holds. For the induction hypothesis, assume (2.52) holds for some arbitrary $i < Q$. We consider the ζ-th instruction of our program P. If it is the 'STOP' instruction, then $\zeta = N$ because the 'STOP' instruction can only be the N-th instruction. However, $\zeta = N$ gives a contradiction because it follows from (2.39) and ϕ_{14} that we must have $\sigma_N^{(i)} = 0$ for all $i < Q$, contradicting our assumption that $\sigma_\zeta^{(i)} = 1$. So, the ζ-th instruction must be of the form '$r_{j_0}^+ \implies \langle w \rangle$' or '$r_{j_0}^- \implies \langle x, y \rangle$'.

Case 1. If the ζ-th instruction is of the form $r_{j_0}^+ \implies \langle w \rangle$ for unique $j_0 \in \{1, \dots, J\}$ and $w \in \{1, \dots, N\}$, then $\zeta \in \mathcal{M}_w^+$ and $\zeta \notin \mathcal{M}_n^1(j) \cup \mathcal{M}_n^2(j)$ for all n and j. It then follows from the inductive relation (2.25) and our induction hypothesis (2.52), which implies that $\sigma_m^{(i)} = 0$ for all $m \in \mathcal{M}_n^1(j) \cup \mathcal{M}_n^2(j)$, that

$$\sigma_n^{(i+1)} = \sum_{m \in \mathcal{M}_n^+} \sigma_m^{(i)}$$

By uniqueness of w we have that $\zeta \notin \mathcal{M}_n^+$ whenever $n \neq w$, showing that $\sigma_n^{(i+1)} = 0$ whenever $n \neq w$ according to (2.52). Because $\zeta \in \mathcal{M}_w^+$ satisfies (2.52), it also follows that $\sigma_w^{(i+1)} = 1$, showing that there is exactly one w such that $\sigma_w^{(i+1)} = 1$.

Case 2. If the ζ-th instruction is of the form $r_{j_0}^- \implies \langle x, y \rangle$ for unique $j_0 \in \{1, \dots, J\}$ and $x, y \in \{1, \dots, N\}$, then

$$\zeta \in \mathcal{M}_x^1(j_0) \qquad \text{and} \qquad \zeta \in \mathcal{M}_y^2(j_0) \tag{2.53}$$

Now $\zeta \notin \mathcal{M}_n^+$ for all n, implying that the inductive relation (2.25) already reduces to

$$\sigma_n^{(i+1)} = \sum_{j=1}^{J} z_j^{(i)} \sum_{m \in \mathcal{M}_n^1(j)} \sigma_m^{(i)} + \sum_{j=1}^{J} (1 - z_j^{(i)}) \sum_{m \in \mathcal{M}_n^2(j)} \sigma_m^{(i)}$$

Because $\zeta \notin \mathcal{M}_n^1(j)$ and $\zeta \notin \mathcal{M}_n^2(j)$ whenever $j \neq j_0$ by uniqueness of j_0, it can be seen that

$$\sigma_n^{(i+1)} = z_{j_0}^{(i)} \sum_{m \in \mathcal{M}_n^1(j_0)} \sigma_m^{(i)} + (1 - z_{j_0}^{(i)}) \sum_{m \in \mathcal{M}_n^2(j_0)} \sigma_m^{(i)}$$

Furthermore, because $\zeta \notin \mathcal{M}_n^1(j_0)$ unless $n = x$ and $\zeta \notin \mathcal{M}_n^2(j_0)$ unless $n = y$ by uniqueness of x and y, it can be seen that

$$\sigma_x^{(i+1)} = z_{j_0}^{(i)} \sum_{m \in \mathcal{M}_x^1(j_0)} \sigma_m^{(i)} + (1 - z_{j_0}^{(i)}) \sum_{m \in \mathcal{M}_x^2(j_0)} \sigma_m^{(i)}$$
$$\sigma_y^{(i+1)} = z_{j_0}^{(i)} \sum_{m \in \mathcal{M}_y^1(j_0)} \sigma_m^{(i)} + (1 - z_{j_0}^{(i)}) \sum_{m \in \mathcal{M}_y^2(j_0)} \sigma_m^{(i)}$$

and $\sigma_n^{(i+1)} = 0$ for all $n \notin \{x, y\}$. If $x = y$, then $\sigma_x^{(i+1)} = \sigma_y^{(i+1)}$ and $\zeta \in \mathcal{M}_x^1(j_0) \cap \mathcal{M}_x^2(j_0)$ by (2.53), showing that $\sigma_x^{(i+1)} = z_{j_0}^{(i)} + (1 - z_{j_0}^{(i)}) = 1$ by (2.52), implying that there is exactly one x such that $\sigma_x^{(i+1)} = 1$. If $x \neq y$, then we see that $\sigma_x^{(i+1)} = z_{j_0}^{(i)}$ and $\sigma_y^{(i+1)} = 1 - z_{j_0}^{(i)}$ by (2.53) and (2.52). Because $z_{j_0}^{(i)} \in \{0, 1\}$ by (2.40), it follows that, in all cases, there is exactly one x such that $\sigma_x^{(i+1)} = 1$.

We see that (2.52) also holds for $i + 1$ in both cases, so it follows that (2.52) holds for all $i \in \{0, \dots, Q\}$ by induction.

It only remains to show that the inductive relation (2.23) holds. Because $a_\ell < b/2$ for all $\ell \in \{1, \dots, k\}$ by ϕ_8 and ϕ_1, we know that $\text{Digit}(a_\ell, b, i+1) = 0$ for all $i \in \mathbb{N}$ because if $\text{Digit}(a_\ell, b, i+1) > 0$ for some i, it would follow that $a_\ell \geq b^{i+1} > b$, contradicting that $a_\ell < b/2$. So, by part a) of Lemma 1.14, it follows from ϕ_{10} that

$$\text{Digit}(\widetilde{r}_j, b, i+1) = \text{Digit}\left(b\Big(\widetilde{r}_j + \sum_{n \in \mathcal{N}_j^+} \widetilde{\sigma}_n - \sum_{n \in \mathcal{N}_j^-} \widetilde{z}_j * \widetilde{\sigma}_n\Big), b, i+1\right)$$

By part b) of Lemma 1.14 and the definition of $r_j^{(i+1)}$, cf. (2.34), the above is then equivalent to

$$r_j^{(i+1)} = \text{Digit}\left(\Big(\widetilde{r}_j + \sum_{n \in \mathcal{N}_j^+} \widetilde{\sigma}_n - \sum_{n \in \mathcal{N}_j^-} \widetilde{z}_j * \widetilde{\sigma}_n\Big), b, i\right) \tag{2.54}$$

Let $j \in \{1, \dots, J\}$ and $i \in \{0, \dots, Q\}$ be arbitrary. We define the number $R(j, i)$ as follows

$$R(j, i) = \text{Digit}(\widetilde{r}_j, b, i) + \sum_{n \in \mathcal{N}_j^+} \text{Digit}(\widetilde{\sigma}_n, b, i) - \sum_{n \in \mathcal{N}_j^-} \text{Digit}(\widetilde{z}_j * \widetilde{\sigma}_n, b, i) \tag{2.55}$$

We want to show that $0 \leq R(j, i) < b$ because it would then follow from Corollary 1.15 that the Digit function in (2.54) can be distributed over the summation, i.e. that

$$r_j^{(i+1)} = R(j, i) \tag{2.56}$$

for all $i \in \{0, \dots, Q\}$. However, before we show that $0 \leq R(j, i) < b$, let us rewrite $R(j, i)$ into a different form. We know that $\text{Digit}(\widetilde{r}_j, b, i) = r_j^{(i)}$ and $\text{Digit}(\widetilde{\sigma}_n, b, i) = \sigma_n^{(i)}$ by (2.34) and (2.36). Furthermore, we have seen that the base-b representation of $\widetilde{z}_j * \widetilde{\sigma}_m$ is given by (2.50), implying that $\text{Digit}(\widetilde{z}_j * \widetilde{\sigma}_n, b, i) = z_j^{(i)} \sigma_n^{(i)}$. This shows that (2.55) can be written as

$$R(j, i) = r_j^{(i)} + \sum_{n \in \mathcal{N}_j^+} \sigma_n^{(i)} - z_j^{(i)} \sum_{n \in \mathcal{N}_j^-} \sigma_n^{(i)} \tag{2.57}$$

To show that $0 \leq R(j, i)$ for all $i \in \{0, \dots, Q\}$, we will use a property of the $(\sigma_1^{(i)}, \dots, \sigma_N^{(i)})_{i=0}^Q$ sequence, namely property (2.52). Let $\zeta \in \{1, \dots, N\}$ be unique such that $\sigma_\zeta^{(i)} = 1$.

Case 1. If $\zeta \notin \mathcal{N}_j^+ \cup \mathcal{N}_j^-$, then $\sigma_n^{(i)} = 0$ for all $n \in \mathcal{N}_j^+ \cup \mathcal{N}_j^-$, showing that $R(j, i) = r_j^{(i)} \geq 0$.

Case 2. If $\zeta \in \mathcal{N}_j^+$, then $\zeta \notin \mathcal{N}_j^-$ because $\mathcal{N}_j^+ \cap \mathcal{N}_j^- = \emptyset$, showing that $R(j, i) = r_j^{(i)} + 1 \geq 0$.

Case 3. If $\zeta \in \mathcal{N}_j^-$, then $\zeta \notin \mathcal{N}_j^+$, showing that $R(j,i) = r_j^{(i)} - z_j^{(i)}$. However, $z_j^{(i)} = \operatorname{sgn}(r_j^{(i)})$ by relations (2.21) and (2.24), showing that $R(j,i) = \max(0, r_j^{(i)} - 1) \geq 0$.

So $R(j,i) \geq 0$ in all cases. To see that $R(j,i) < b$ for all $i \in \{0,\dots,q\}$, note that

$$\begin{aligned}
R(j,i) &\leq r_j^{(i)} + \sum_{n \in \mathcal{N}_j^+} 1 && \text{by (2.40)} \\
&= r_j^{(i)} + |\mathcal{N}_j^+| \\
&\leq (2^c - 1) + N && \text{by (2.41) and Remark 2.15} \\
&< 2^c + 2^c && \text{because } N < 2^c \text{ by } \phi_9 \\
&= b && \text{by } \phi_1
\end{aligned}$$

Because we have already argued that, according to Corollary 1.15, the condition $0 \leq R(j,i) < b$ is sufficient for (2.56), we conclude that (2.56) and (2.57) both hold. Together, they imply the last inductive relation (2.23).

We conclude that $\mathcal{R}_P(a_1,\dots,a_k)$ holds and thus that the right-hand side of (2.28) is sufficient for $\mathcal{R}_P(a_1,\dots,a_k)$.

The Necessity

We will now show that the right hand side of (2.28) is necessary for $\mathcal{R}_P(a_1,\dots,a_k)$, so assume that $\mathcal{R}_P(a_1,\dots,a_k)$ holds. We have to find $q, b, c, d, e, f, \widetilde{r}_1, \dots, \widetilde{r}_J, \widetilde{z}_1, \dots, \widetilde{z}_J, \widetilde{\sigma}_1, \dots, \widetilde{\sigma}_N \in \mathbb{N}$ which satisfy the formulas $\phi_1, \dots, \phi_{14}$, so, for readability, I will place $[\phi_i]$ in the margin whenever we have shown that formula ϕ_i holds.

Let $(r_1^{(i)}, \dots, r_J^{(i)})_{i=0}^Q$, $(z_1^{(i)}, \dots, z_J^{(i)})_{i=0}^Q$ and $(\sigma_1^{(i)}, \dots, \sigma_N^{(i)})_{i=0}^Q$ denote the sequences from our predicate $\mathcal{R}_P(a_1,\dots,a_k)$. We begin by letting $q = Q$ and, as before, we shall use q and Q interchangeably. Next, we define $b = 2^{c+1}$ for some $c \in \mathbb{N}$ which is 'large enough' in the following sense. For all $i \in \{0,\dots,Q\}$, $j \in \{1,\dots,J\}$, $n \in \{1,\dots,N\}$ and $\ell \in \{1,\dots,k\}$, we must have

$$\begin{gathered}
\max(r_j^{(i)}, z_j^{(i)}, \sigma_n^{(i)}, a_\ell) < 2^c \\
N(2J+1) < 2^c
\end{gathered} \tag{2.58}$$

$[\phi_1]$

So, the formulas ϕ_1, ϕ_8 and ϕ_9 already hold. $[\phi_8]$

Furthermore, we define $[\phi_9]$

$$d = \sum_{i=0}^{q} (2^c - 1) b^i, \quad e = \sum_{i=0}^{q} b^i \quad \text{and} \quad f = \sum_{i=0}^{q} 2^c b^i$$

$[\phi_2]$

so that the formulas ϕ_2, ϕ_3 and ϕ_4 hold as well. $[\phi_3]$

Lastly, the natural numbers $\widetilde{r}_1, \dots, \widetilde{r}_J, \widetilde{z}_1, \dots, \widetilde{z}_J, \widetilde{\sigma}_1, \dots, \widetilde{\sigma}_N$ are defined as follows. $[\phi_4]$

$$\widetilde{r}_j = \sum_{i=0}^{q} r_j^{(i)} b^i \tag{2.59}$$

$$\widetilde{z}_j = \sum_{i=0}^{q} z_j^{(i)} b^i \tag{2.60}$$

$$\widetilde{\sigma}_n = \sum_{i=0}^{q} \sigma_n^{(i)} b^i \tag{2.61}$$

In particular, because $r_j^{(i)}, z_j^{(i)}, \sigma_n^{(i)} < b$ by (2.58), it follows from the definitions (2.59)—(2.61) that the numbers $r_j^{(i)}$, $z_j^{(i)}$ and $\sigma_n^{(i)}$ from our sequences are nothing but the base-b digits of our newly defined numbers $\widetilde{r}_j$, $\widetilde{z}_j$ and $\widetilde{\sigma}_n$.

Because $r_j^{(i)} \leq 2^c - 1$ by (2.58), it follows from (2.30) that $r_j^{(i)} \preccurlyeq 2^c - 1$ for all $i \in \{0, \ldots, q\}$. It then follows from the Gluing Lemma that

$$\sum_{i=0}^{q} r_j^{(i)} b^i \preccurlyeq \sum_{i=0}^{q} (2^c - 1) b^i$$

i.e. that $\widetilde{r}_j \preccurlyeq d$. So formula ϕ_5 holds. [ϕ_5]

Furthermore, we have that

$$z_j^{(i)} \in \{0, 1\} \tag{2.62}$$

because $z_j^{(i)} = \operatorname{sgn}(r_j^{(i)})$ by (2.21) and (2.24), and we have that

$$\sigma_n^{(i)} \in \{0, 1\} \tag{2.63}$$

by Theorem 2.10. So, it follows that $z_j^{(i)} \preccurlyeq 1$ and $\sigma_n^{(i)} \preccurlyeq 1$ and we see with the Gluing Lemma that

$$\sum_{i=0}^{q} z_j^{(i)} b^i \preccurlyeq \sum_{i=0}^{q} b^i \qquad \text{and} \qquad \sum_{i=0}^{q} \sigma_n^{(i)} b^i \preccurlyeq \sum_{i=0}^{q} b^i$$

[ϕ_6]

i.e. that $\widetilde{z}_j \preccurlyeq e$ and $\widetilde{\sigma}_n \preccurlyeq e$. So formulas ϕ_6 and ϕ_7 hold as well. [ϕ_7]

Before we show that ϕ_{10} and ϕ_{12} hold, note that it follows from (2.60) and (2.61), together with conditions (2.62) and (2.63), that we can apply Lemma 2.14 to find that

$$\begin{aligned} \sum_{i=0}^{q} z_j^{(i)} \sigma_n^{(i)} b^i &= \widetilde{z}_j * \widetilde{\sigma}_n \\ \sum_{i=0}^{q} (1 - z_j^{(i)}) \sigma_n^{(i)} b^i &= (e - \widetilde{z}_j) * \widetilde{\sigma}_n \end{aligned} \tag{2.64}$$

We will now show how ϕ_{10} follows from the inductive relation (2.23). By definition of $\widetilde{r}_j$, cf. (2.59), and (2.23) we have

$$\begin{aligned} \widetilde{r}_j &= b \sum_{i=0}^{q-1} r_j^{(i+1)} b^i + r_j^{(0)} \\ &= b \sum_{i=0}^{q-1} \left(r_j^{(i)} + \sum_{n \in \mathcal{N}_j^+} \sigma_n^{(i)} - z_j^{(i)} \sum_{n \in \mathcal{N}_j^+} \sigma_n^{(i)} \right) b^i + r_j^{(0)} \\ &= b \left(\sum_{i=0}^{q-1} r_j^{(i)} b^i + \sum_{n \in \mathcal{N}_j^+} \sum_{i=0}^{q-1} \sigma_n^{(i)} b^i - \sum_{n \in \mathcal{N}_j^-} \sum_{i=0}^{q-1} z_j^{(i)} \sigma_n^{(i)} b^i \right) + r_j^{(0)} \end{aligned}$$

so that, by (2.59), (2.61) and (2.64), we have

$$\widetilde{r}_j = b \left(\left(\widetilde{r}_j - r_j^{(q)} b^q \right) + \sum_{n \in \mathcal{N}_j^+} \left(\widetilde{\sigma}_n - \sigma_n^{(q)} b^q \right) - \sum_{n \in \mathcal{N}_j^-} \left(\widetilde{z}_j * \widetilde{\sigma}_n - z_j^{(q)} \sigma_n^{(q)} b^q \right) \right) + r_j^{(0)}$$

Because we know from the halting relation (2.27) that $r_j^{(q)} = 0$ and because we know from (2.18) that $\sigma_n^{(q)} = 0$ for all $n \in \mathcal{N}_j^+ \cup \mathcal{N}_j^-$, it follows that

$$\widetilde{r}_j = b\left(\widetilde{r}_j + \sum_{n\in\mathcal{N}_j^+} \widetilde{\sigma}_n - \sum_{n\in\mathcal{N}_j^-} \widetilde{z}_j * \widetilde{\sigma}_n\right) + r_j^{(0)}$$

Now, since $r_j^{(0)} = a_j$ if $j \leq k$ and $r_j^{(0)} = 0$ otherwise, according to (2.20), we see that ϕ_{10} holds. $[\phi_{10}]$

To show that ϕ_{11} holds, we consider, the number $r_j^{(i)} + 2^c - 1$. We have previously shown that this number satisfies (2.42) on the premise that $r_j^{(i)} \leq 2^c - 1$. So, because $r_j^{(i)} < 2^c$ by (2.58), we conclude that $\text{Digit}(r_j^{(i)} + 2^c - 1, 2, c+1) = \text{sgn}(r_j^{(i)})$, where $\text{sgn}(r_j^{(i)}) = z_j^{(i)}$ by (2.21) and (2.24). So

$$z_j^{(i)} = \text{Digit}(r_j^{(i)} + 2^c - 1, 2, c+1) \tag{2.65}$$

Because $r_j^{(i)} < 2^c$, we have $r_j^{(i+1)} + 2^c - 1 < 2^{c+1}$, implying that only the first $c+1$ binary digits of $r_j^{(i)} + 2^c - 1$ can be nonzero. So, according to (2.65), we must then have

$$r_j^{(i)} + 2^c - 1 = \overbrace{z_j^{(i)}\delta_{i,c-1}\cdots\delta_{i,0}}^{c+1 \text{ digits}}{}_{\langle 2\rangle} \tag{2.66}$$

for certain (irrelevant) binary digits $\delta_{i,0}, \ldots, \delta_{i,c-1} \in \{0,1\}$. Now, by definition of $\widetilde{r}_j$ and d, cf. (2.59) and ϕ_2, we have that the base-b representation of $\widetilde{r}_j + d$ is given by

$$\widetilde{r}_j + d = \sum_{i=0}^{q}(r_j^{(i)} + 2^c - 1)b^i$$

So, because the binary representation of each base-b digit $r_j^{(i)} + 2^c - 1$ is given by (2.65), it follows from the Gluing Lemma that the binary representation of $\widetilde{r}_j + d$ is given by

$$\widetilde{r}_j + d = \overbrace{z_j^{(q)}\delta_{q,c-1}\cdots\delta_{q,0} \,||\, \cdots\cdots \,||\, z_j^{(0)}\delta_{0,c-1}\cdots\delta_{0,0}}^{(q+1)\times(c+1) \text{ digits}}$$

We can then take the binary product of $\widetilde{r}_j + d$ and f, whose binary representation is given by (2.33), to find that

$$\begin{aligned}
f * (\widetilde{r}_j + d) &= \overbrace{z_j^{(q)}00\cdots00 \,||\, z_j^{(q-1)}00\cdots00 \,||\, \cdots\cdots \,||\, z_j^{(1)}00\cdots00 \,||\, z_j^{(0)}00\cdots00}^{(q+1)\times(c+1) \text{ digits}} \\
&= z_j^{(0)}2^{(c+1)-1} + z_j^{(1)}2^{2(c+1)-1} + \cdots + z_j^{(q-1)}2^{((q-1)+1)(c+1)-1} + z_j^{(q)}2^{(q+1)(c+1)-1} \\
&= \sum_{i=0}^{q} z_j^{(i)}2^{(i+1)(c+1)-1} \\
&= \sum_{i=0}^{q} z_j^{(i)}2^{i(c+1)}2^c \\
&= 2^c\sum_{i=0}^{q} z_j^{(i)}b^i \\
&= 2^c\widetilde{z}_j
\end{aligned}$$

and conclude that ϕ_{11} holds as well. [ϕ_{11}]

We will now show how ϕ_{12} follows from the inductive relation (2.25). By definition of $\widetilde{\sigma}_n$, cf. (2.61), and (2.25) we have

$$\begin{aligned}\widetilde{\sigma}_n &= b\sum_{i=0}^{q-1}\sigma_n^{(i+1)}b^i + \sigma_n^{(0)}\\ &= b\sum_{i=0}^{q-1}\left(\sum_{m\in\mathcal{M}_n^+}\sigma_m^{(i)} + \sum_{j=1}^{J}z_j^{(i)}\sum_{m\in\mathcal{M}_n^1(j)}\sigma_m^{(i)} + \sum_{j=1}^{J}(1-z_j^{(i)})\sum_{m\in\mathcal{M}_n^2(j)}\sigma_m^{(i)}\right)b^i + \sigma_n^{(0)}\\ &= b\left(\sum_{m\in\mathcal{M}_n^+}\sum_{i=0}^{q-1}\sigma_m^{(i)} + \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^1(j)}\sum_{i=0}^{q-1}z_j^{(i)}\sigma_m^{(i)} + \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^2(j)}\sum_{i=0}^{q-1}(1-z_j^{(i)})\sigma_m^{(i)}\right) + \sigma_n^{(0)}\end{aligned}$$

so that, by (2.61) and (2.64), we have

$$\begin{aligned}\widetilde{\sigma}_n = b\Bigg(&\sum_{m\in\mathcal{M}_n^+}\left(\widetilde{\sigma}_m - \sigma_m^{(q)}\right) + \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^1(j)}\left(\widetilde{z}_j * \widetilde{\sigma}_m - z_j^{(q)}\sigma_m^{(q)}b^q\right)\\ &+ \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^2(j)}\left((e-\widetilde{z}_j) * \widetilde{\sigma}_m - (1-z_j^{(q)})\sigma_m^{(q)}b^q\right)\Bigg) + \sigma_n^{(0)}\end{aligned}$$

Because $\sigma_m^{(q)} = 0$ for all $m \in \mathcal{M}_n^+ \cup \mathcal{M}_n^1(j) \cup \mathcal{M}_n^2(j)$ by (2.18), it then follows that

$$\widetilde{\sigma}_n = b\left(\sum_{m\in\mathcal{M}_n^+}\widetilde{\sigma}_m + \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^1(j)}\widetilde{z}_j * \widetilde{\sigma}_m + \sum_{j=1}^{J}\sum_{m\in\mathcal{M}_n^2(j)}(e-\widetilde{z}_j) * \widetilde{\sigma}_m\right) + \sigma_n^{(0)}$$

So, because $\sigma_n^{(0)} = 1$ if $n = 1$ and $\sigma_n^{(0)} = 0$ otherwise, according to (2.22), we conclude that formula ϕ_{12} holds as well. [ϕ_{12}]

Now, because $\sigma_N^{(q)} = 1$ and $\sigma_N^{(i)} = 0$ whenever $i \neq q$, according to (2.17), it follows from the definition of $\widetilde{\sigma}_N$, cf. (2.61), that

$$\widetilde{\sigma}_N = \sum_{i=0}^{q}\sigma_N^{(i)}b^i = b^q$$

and thus that ϕ_{13} holds as well. [ϕ_{13}]

Lastly, formula ϕ_{14} follows immediately from the fact that $\text{Digit}(\widetilde{r}_j, b, i) = r_j^{(i)}$ by (2.59), together with our halting relation (2.27). [ϕ_{14}]

We conclude that the formulas $\phi_1, \ldots, \phi_{14}$ all hold, showing that right hand side of (2.28) is not just sufficient, but also necessary. This completes the proof.

∎

We finally arrive at the DPR Theorem

Theorem 2.18 (DPR Theorem; 1961). *Every computably enumerable set is exponential Diophantine.*

Proof. Let $A \subseteq \mathbb{N}^k$ be a computably enumerable set. By Proposition 2.9 and Theorem 2.17, there is some program P such that

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \exists qbcdef\widetilde{r}_1 \cdots \widetilde{r}_J\widetilde{z}_1 \cdots \widetilde{z}_J\widetilde{\sigma}_1 \cdots \widetilde{\sigma}_N \in \mathbb{N}\,(\phi_1 \wedge \cdots \wedge \phi_{14})\}$$

where $\phi_1, \ldots, \phi_{14}$ denotes the formulas from Theorem 2.17. We will show that all the ϕ_i's are exponential Diophantine.

First note that formulas ϕ_1 and ϕ_{13} are exponential Diophantine by themselves. Next, each of the formulas $\phi_5, \phi_6, \phi_7, \phi_{11}, \phi_{14}$ is a conjunction of exponential Diophantine formulas because "$\preccurlyeq$", "$*$" and "Digit" are all exponential Diophantine according to Theorem 1.20. So, by Theorem 1.9, they are exponential Diophantine themselves. Similarly, formulas ϕ_8 and ϕ_9 are Diophantine by Proposition 1.13. To see that ϕ_{10} and ϕ_{12} are exponential Diophantine as well, first note that there are only finite sums involved (sums which depend on the program P which is assumed to be fixed). Because $\widetilde{r}_j$ and $\widetilde{\sigma}_N$ both lie in $\mathbb{N}$, we do not have to worry about the minus signs in ϕ_{10} and ϕ_{12} as the negative terms can easily be transposed to the other side, or we can introduce some extra variables. To be explicit, ϕ_{10} is equivalent to the conjunction over all j of the formula

$$\widetilde{r}_j + b \sum_{n \in \mathcal{N}_j^-} \widetilde{z}_j * \widetilde{\sigma}_n = b \left(\widetilde{r}_j + \sum_{n \in \mathcal{N}_j^+} \widetilde{\sigma}_n \right) + \begin{cases} a_j & \text{if } j \leq k \\ 0 & \text{otherwise} \end{cases}$$

and ϕ_{12} is equivalent to the conjunction over all n of the formula

$$\begin{aligned} &\exists t_1 \cdots t_J \in \mathbb{N}\big(\\ &\qquad \widetilde{\sigma}_n = b \left(\sum_{m \in \mathcal{M}_n^+} \widetilde{\sigma}_m + \sum_{j=1}^{J} \sum_{m \in \mathcal{M}_n^1(j)} \widetilde{z}_j * \widetilde{\sigma}_m + \sum_{j=1}^{J} \sum_{m \in \mathcal{M}_n^2(j)} t_j * \widetilde{\sigma}_m \right) + \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases} \\ &\qquad \wedge t_1 + \widetilde{z}_1 = e \\ &\qquad \wedge t_2 + \widetilde{z}_2 = e \\ &\qquad \vdots \\ &\qquad \wedge t_J + \widetilde{z}_J = e \\ &\big) \end{aligned}$$

Because "$*$" is exponential Diophantine, we see that both ϕ_{10} and ϕ_{12} are (equivalent to) formulas which are built up from exponential Diophantine formulas and connected by conjunctions and existential quantifiers. So, by Theorem 1.9, they are exponential Diophantine themselves.

It remains to show that the formulas ϕ_2, ϕ_3 and ϕ_4 are exponential Diophantine in the variables q, b, c, d, e, f. This is not immediate, because each of these formulas involves a sum where the number of terms depends on the variable q. However, note that $\sum_{i=0}^{q} b^i$ is nothing but the partial sum of the geometric series. Because it is well known that

$$\sum_{i=0}^{q} b^i = \frac{b^{q+1} - 1}{b - 1}$$

it then easily follows that the formulas ϕ_2, ϕ_3 and ϕ_4 are equivalent to the exponential Diophantine formulas

$$\begin{aligned} (b-1)d &= (2^c - 1)(b^{q+1} - 1) \\ (b-1)e &= b^{q+1} - 1 \\ (b-1)f &= 2^c(b^{q+1} - 1) \end{aligned}$$

So ϕ_2, ϕ_3 and ϕ_4 are exponential Diophantine as well and it follows that the formulas $\phi_1, \ldots, \phi_{14}$ are all exponential Diophantine.

Now, let $\phi(a_1, \ldots, a_k)$ be the formula $\exists qbcdef\widetilde{r}_1 \cdots \widetilde{r}_J \widetilde{z}_1 \cdots \widetilde{z}_J \widetilde{\sigma}_1 \cdots \widetilde{\sigma}_N \in \mathbb{N}\,(\phi_1 \wedge \cdots \wedge \phi_{14})$. Then ϕ is a conjunction of exponential Diophantine formulas, preceded by a finite number of existential quantifiers; so ϕ is exponential Diophantine itself by Theorem 1.9. We conclude that our computably enumerable set

$$A = \{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \phi(a_1, \ldots, a_k)\}$$

is exponential Diophantine.

∎

Chapter 3

Exponentiation is Diophantine

The main object of study in this chapter is a recurrent sequence $\{\alpha_b(n)\}_{n\in\mathbb{N}}$ which we will come to refer to as the α_b*-sequence*. It is parametrized by a natural number $b \geq 2$ and defined as follows.

$$\begin{aligned} \alpha_b(0) &= 0 \\ \alpha_b(1) &= 1 \\ \alpha_b(n+2) &= b\alpha_b(n+1) - \alpha_b(n) \end{aligned} \tag{3.1}$$

We will find that, in order to prove that exponentiation is Diophantine, it suffices to show that the α_b-sequence is Diophantine, i.e. that the set of triples $(a, b, c) \in \mathbb{N}^3$ such that $a = \alpha_b(c)$ is Diophantine. The next proposition shows some basic properties of the α_b-sequence.

Proposition 3.1. *The α_b-sequence increases strictly and grows faster than its index. Furthermore, it is linear for $b = 2$ and increases exponentially for $b > 2$. Precisely, if $b \geq 2$, then*

- $\alpha_b(n) < \alpha_b(n+1)$
- $n \leq \alpha_b(n)$
- $\alpha_2(n) = n$
- $(b-1)^n \leq \alpha_b(n+1) \leq b^n$

for all $n \in \mathbb{N}$.

Proof. All properties are proven by induction on n.

- It follows from the definition that $\alpha_b(0) < \alpha_b(1)$. Assume that $\alpha_b(n) < \alpha_b(n+1)$ for some arbitrary n. Then $\alpha_b(n+1) < \alpha_b(n+2)$ can be seen as follows.

$$\begin{aligned} \alpha_b(n+1) &< \alpha_b(n+1) + (\alpha_b(n+1) - \alpha_b(n)) \\ &= 2\alpha_b(n+1) - \alpha_b(n) \\ &\leq b\alpha_b(n+1) - \alpha_b(n) \\ &= \alpha_b(n+2) \end{aligned}$$

- By definition $0 \leq \alpha_b(0)$ and $1 \leq \alpha_b(1)$ are easily seen to hold. Assume that $n \leq \alpha_b(n)$ and $n+1 \leq \alpha_b(n+1)$ for some arbitrary $n \in \mathbb{N}$. Then

  $$\begin{aligned} \alpha_b(n+2) &= b\alpha_b(n+1) - \alpha_b(n) \\ &> b\alpha_b(n+1) - \alpha_b(n+1) \\ &\geq (n+1)(b-1) \\ &\geq n+1 \end{aligned}$$

  where the second line follows from $\alpha_b(n) < \alpha_b(n+1)$. Because $\alpha_b(n+2) > n+1$ we conclude that $n+2 \leq \alpha_b(n+2)$.

- We have $\alpha_2(0) = 0$ and $\alpha_2(1) = 1$ by definition. If we assume that $\alpha_2(n) = n$ and $\alpha_2(n+1) = n+1$ for some arbitrary n, then

  $$\alpha_2(n+2) = 2\alpha_2(n+1) - \alpha_2(n) = 2(n+1) - n = n+2 \tag{3.2}$$

- It is easily seen that $(b-1)^0 \leq \alpha_b(1) \leq b^0$ because $(b-1)^0 = \alpha_b(1) = b^0 = 1$. If we assume that $(b-1)^n \leq \alpha_b(n+1) \leq b^n$ for some arbitrary n, then

  $$\begin{aligned} \alpha_b((n+1)+1) &= b\alpha_b(n+1) - a_b(n) \\ &\leq b\alpha_b(n+1) \\ &\leq b^{n+1} \end{aligned}$$

  and

  $$\begin{aligned} \alpha_b((n+1)+1) &= b\alpha_b(n+1) - \alpha_b(n) \\ &> b\alpha_b(n+1) - \alpha_b(n+1) \\ &= (b-1)\alpha_b(n+1) \\ &\geq (b-1)^{n+1} \end{aligned}$$

  which shows that $(b-1)^{n+1} \leq \alpha_b\left((n+1)+1\right) \leq b^{n+1}$.

■

3.1 The α_b-sequence in Matrix Form

Let us extend the definition of the α_b-sequence by letting $\alpha_b(-1) = -1$ so that the recurrent definition $\alpha_b(n+2) = b\alpha_b(n+1) - \alpha_b(n)$ also holds for $n = -1$. Consider then, for $n \in \mathbb{N}$, the following matrices

$$A_b(n) = \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix}, \qquad B_b = \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \tag{3.3}$$

It is easily seen from the definition of the α_b-sequence that

$$A_b(0) = \begin{pmatrix} \alpha_b(1) & -\alpha_b(0) \\ \alpha_b(0) & -\alpha_b(-1) \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

and

$$\begin{aligned} A_b(n+1) &= \begin{pmatrix} \alpha_b(n+2) & -\alpha_b(n+1) \\ \alpha_b(n+1) & -\alpha_b(n) \end{pmatrix} \\ &= \begin{pmatrix} b\alpha_b(n+1)-\alpha_b(n) & -\alpha_b(n+1) \\ b\alpha_b(n)-\alpha_b(n-1) & -\alpha_b(n) \end{pmatrix} \\ &= \begin{pmatrix} \alpha_b(n+1) & -\alpha_b(n) \\ \alpha_b(n) & -\alpha_b(n-1) \end{pmatrix} \begin{pmatrix} b & -1 \\ 1 & 0 \end{pmatrix} \\ &= A_b(n)B_b \end{aligned}$$

for all $n \in \mathbb{N}$. These matrix relations can be written more compactly as

$$A_b(n) = B_b^n \tag{3.4}$$

where $B_b^0 = \mathrm{Id}$ denotes the 2×2 identity matrix. Now, because $\det(B_b) = 1$, it follows from (3.4) that

$$\det A_b(n) = 1 \tag{3.5}$$

and thus that $\alpha_b(n)^2 - \alpha_b(n+1)\alpha_b(n-1) = 1$ by definition of $A_b(n)$. Substituting $\alpha_b(n+1) = b\alpha_b(n) - \alpha_b(n-1)$, we find that the equation

$$\alpha_b(n-1)^2 - b\alpha_b(n-1)\alpha_b(n) + \alpha_b(n)^2 = 1 \tag{3.6}$$

holds for all $n \in \mathbb{N}$.

Proposition 3.2. *Let $k \in \mathbb{N}$. Then $\alpha_b(k)$ and $\alpha_b(k+1)$ are coprime.*

Proof. Assume $d \in \mathbb{N}$ divides both $\alpha_b(k)$ and $d\alpha_b(k+1)$. Then $\alpha_b(k) = Nd$ and $\alpha_b(k+1) = Md$ for certain $M, N \in \mathbb{N}$. According to (3.6) we have $\alpha_b(k)^2 - b\alpha_b(k)\alpha_b(k+1) + \alpha_b(k+1)^2 = 1$, so it follows that $N^2d^2 - bNMd^2 + M^2d^2 = 1$, i.e. $(N^2 - bNM + M^2)d^2 = 1$. We conclude that $d^2 = 1$ and thus that $d = 1$.

∎

Before we can prove that the α_b-sequence is Diophantine, we must first show that the α_b-sequence satisfies a total of five properties. Two of these are divisibility properties and two of these are congruence properties. The remaining property we will prove right now.

Theorem 3.3. *For all $x, y \in \mathbb{N}$ and $b \in \mathbb{N}_{\geq 2}$ it holds that*

$$x^2 - bxy + y^2 = 1$$
$$\iff$$
$$\exists m \in \mathbb{N}\Big((x = \alpha_b(m) \wedge y = \alpha_b(m+1)) \vee (y = \alpha_b(m) \wedge x = \alpha_b(m+1))\Big)$$

Proof. If $x = \alpha_b(m)$ and $y = \alpha_b(m+1)$ for some $m \in \mathbb{N}$, then it follows directly from (3.6) that $x^2 - bxy + y^2 = 1$. By symmetry, the same holds if $y = \alpha_b(m)$ and $x = \alpha_b(m+1)$.

For the converse, we note that it suffices to show that

$$x^2 - bxy + y^2 = 1 \wedge x < y \implies \exists m \in \mathbb{N}(x = \alpha_b(m) \wedge y = \alpha_b(m+1)) \tag{3.7}$$

because, if $x^2 - bxy + y^2 = 1$ for some x and y, then either $x < y$ or $x \geq y$. The case $y < x$ is equivalent to the case $x < y$ by symmetry and the case $x = y$ is impossible because it would imply that $(2-b)x^2 = 1$ for some $b \geq 2$.

We will prove that (3.7) holds by using the principle of strong induction (on x). If $x = 0$ and $y \in \mathbb{N}$ is such that $x < y$ and $x^2 - bxy + y^2 = 1$ it follows that $y^2 = 1$ i.e. $y = 1$. This shows that we can choose $m = 0$ because then $x = \alpha_b(m) = 0$ and $y = \alpha_b(m+1) = 1$.

For the strong induction hypothesis, assume that there is some arbitrary $N \in \mathbb{N}$ such that whenever $\widetilde{x} \in \{0, \dots, N\}$ and $\widetilde{y} \in \mathbb{N}$ satisfy $\widetilde{x} < \widetilde{y}$ and $\widetilde{x}^2 - b\widetilde{x}\widetilde{y} + \widetilde{y}^2 = 1$, there is an $\widetilde{m}$ for which $\widetilde{x} = \alpha_b(\widetilde{m})$ and $\widetilde{y} = \alpha_b(\widetilde{m}+1)$.

Let $x = N+1$ and assume that $y \in \mathbb{N}$ is such that $x < y$ and $x^2 - bxy + y^2 = 1$. It follows that

$$bx - y = \frac{x^2 - 1}{y} \geq 0$$

and

$$bx - y = \frac{x^2-1}{y} < \frac{x^2}{y} < x$$

So we see that $0 \leq bx - y < x$. If we define $\widetilde{x} = bx - y$ and $\widetilde{y} = x$, then $\widetilde{x} < \widetilde{y}$ and

$$\begin{aligned}
\widetilde{x}^2 - b\widetilde{x}\widetilde{y} + \widetilde{y}^2 &= (bx-y)^2 - b(bx-y)x + x^2 \\
&= b^2x^2 - 2bxy + y^2 - b^2x^2 + byx + x^2 \\
&= x^2 - bxy + y^2 \\
&= 1
\end{aligned}$$

Because $\widetilde{x} < \widetilde{y}$, where $\widetilde{y} = x = N+1$, it follows that $\widetilde{x} \leq N$. So, by our induction hypothesis, there exists an $\widetilde{m}$ such that $\widetilde{x} = \alpha_b(\widetilde{m})$ and $\widetilde{y} = \alpha_b(\widetilde{m}+1)$. By definition of $\widetilde{x}$ and $\widetilde{y}$ this implies that $x = \widetilde{y} = \alpha_b(\widetilde{m}+1)$ and

$$\begin{aligned}
y &= bx - \widetilde{x} \\
&= b\widetilde{y} - \widetilde{x} \\
&= b\alpha_b(\widetilde{m}+1) - \alpha_b(\widetilde{m}) \\
&= \alpha_b(\widetilde{m}+2)
\end{aligned}$$

So if we let $m = \widetilde{m}+1$, then $x = \alpha_b(m)$ and $y = \alpha_b(m+1)$. By the principle of strong induction, we conclude that (3.7) holds for all $x \in \mathbb{N}$, which completes the proof.

■

3.2 Divisibility Properties

This section is devoted to the proof of the following theorems.

Theorem 3.4 (First Divisibility Property). *Let $b \in \mathbb{N}_{\geq 2}$ and $k, m \in \mathbb{N}$. Then*

$$k \mid m \iff \alpha_b(k) \mid \alpha_b(m)$$

Theorem 3.5 (Second Divisibility Property). *Let $b \in \mathbb{N}_{\geq 2}$ and $k, m \in \mathbb{N}$. Then*

$$\alpha_b(k)^2 \mid \alpha_b(m) \iff k\alpha_b(k) \mid m$$

Before we prove these divisibility properties, let us do some groundwork first. If $k, m \in \mathbb{N}$ are arbitrary with $k > 0$, there exist, by the Euclidean division theorem, unique natural numbers ℓ and n such that

$$m = k\ell + n \qquad \text{and} \qquad 0 \leq n < k$$

Using the matrix relation (3.4) it can then be seen that

$$\begin{aligned} A_b(m) &= B_b^{k\ell+n} \\ &= B_b^n (B_b^k)^\ell \\ &= A_b(n)(A_b(k))^\ell \end{aligned} \tag{3.8}$$

Let $\widetilde{A}_b(k)$ denote the matrix

$$\widetilde{A}_b(k) = \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}$$

and let us define the congruence relation "$\equiv$" for two $n \times m$ matrices, or vectors, $A = (a_{ij})$ and $B = (b_{ij})$ element-wise. That is: $A \equiv B \mod q$ holds if and only if $a_{ij} \equiv b_{ij} \mod q$ for all i, j.

Lemma 3.6. *For every $\ell \in \mathbb{N}$ it holds that $A_b(k)^\ell \equiv \widetilde{A}_b(k)^\ell \mod \alpha_b(k)$.*

Proof. We proceed by induction on ℓ. If $\ell = 0$ then $A_b(k)^\ell = \widetilde{A}_b(k)^\ell = \mathrm{Id}$, where Id denotes the 2×2 identity matrix, showing that $A_b(k) \equiv \widetilde{A}_b(k) \mod \alpha_b(k)$ holds trivially.

For the induction hypothesis, assume that $A_b(k)^\ell \equiv \widetilde{A}_b(k)^\ell \mod \alpha_b(k)$ for some arbitrary $\ell \in \mathbb{N}$ and let the integers M, N, P and Q be such that

$$\begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix}^\ell - \begin{pmatrix} \alpha_b(k+1) & 0 \\ 0 & -\alpha_b(k-1) \end{pmatrix}^\ell = \alpha_b(k) \begin{pmatrix} M & N \\ P & Q \end{pmatrix}$$

Then we have for $A_b(k)^{\ell+1}$ that

$$\begin{aligned} A_b(k)^{\ell+1} &= A_b(k) A_b(k)^\ell \\ &= A_b(k) \left(\alpha_b(k) \begin{pmatrix} M & N \\ P & Q \end{pmatrix} + \widetilde{A}_b(k)^\ell \right) \\ &= A_b(k) \left(\alpha_b(k) \begin{pmatrix} M & N \\ P & Q \end{pmatrix} + \begin{pmatrix} \alpha_b(k+1)^\ell & 0 \\ 0 & (-1)^\ell \alpha_b(k-1)^\ell \end{pmatrix} \right) \\ &= \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix} \begin{pmatrix} M\alpha_b(k) + \alpha_b(k+1)^\ell & N\alpha_b(k) \\ P\alpha_b(k) & Q\alpha_b(k) + (-1)^\ell \alpha_b(k-1)^\ell \end{pmatrix} \\ &= \begin{pmatrix} \widetilde{M}\alpha_b(k) + \alpha_b(k+1)^{\ell+1} & \widetilde{N}\alpha_b(k) \\ \widetilde{P}\alpha_b(k) & \widetilde{Q}\alpha_b(k) + (-1)^{\ell+1}\alpha_b(k-1)^{\ell+1} \end{pmatrix} \\ &= \begin{pmatrix} \widetilde{M}\alpha_b(k) & \widetilde{N}\alpha_b(k) \\ \widetilde{P}\alpha_b(k) & \widetilde{Q}\alpha_b(k) \end{pmatrix} + \begin{pmatrix} a_b(k+1)^{\ell+1} & 0 \\ 0 & (-1)^{\ell+1}\alpha_b(k-1)^{\ell+1} \end{pmatrix} \end{aligned}$$

$$= \begin{pmatrix} \widetilde{M} & \widetilde{N} \\ \widetilde{P} & \widetilde{Q} \end{pmatrix} \alpha_b(k) + \widetilde{A}_b(k)^{\ell+1}$$

where the integers $\widetilde{M}, \widetilde{N}, \widetilde{P}$ and $\widetilde{Q}$ are given by

$$\begin{aligned} \widetilde{M} &= M\alpha_b(k+1) - P\alpha_b(k) \\ \widetilde{N} &= N\alpha_b(k+1) - Q\alpha_b(k) - (-\alpha_b(k-1))^\ell \\ \widetilde{P} &= M\alpha_b(k) + \alpha_b(k+1)^\ell - P\alpha_b(k-1) \\ \widetilde{Q} &= N\alpha_b(k) - Q\alpha_b(k-1) \end{aligned}$$

This shows that

$$A_b(k)^{\ell+1} - \widetilde{A}_b(k)^{\ell+1} = \alpha_b(k) \begin{pmatrix} \widetilde{M} & \widetilde{N} \\ \widetilde{P} & \widetilde{Q} \end{pmatrix}$$

and thus that $A_b(k)^{\ell+1} \equiv \widetilde{A}_b(k)^{\ell+1} \mod \alpha_b(k)$, which completes the proof.

∎

Because $A_b(m) = A_b(n)A_b(k)^\ell$ by (3.8), it follows from Lemma 3.6 that

$$A_b(m) \equiv A_b(n)\widetilde{A}_b(k)^\ell \mod \alpha_b(k)$$

Using the definitions of $A_b(m)$, $A_b(n)$ and $\widetilde{A}_b(k)$, this translates to

$$\begin{pmatrix} \alpha_b(m+1) & -\alpha_b(m) \\ \alpha_b(m) & -\alpha_b(m-1) \end{pmatrix} \equiv \begin{pmatrix} \alpha_b(n+1)\alpha_b(k+1)^\ell & \alpha_b(n)\alpha_b(k-1)^\ell \\ \alpha_b(n)\alpha_b(k+1)^\ell & \alpha_b(n-1)\alpha_b(k-1)^\ell \end{pmatrix} \mod \alpha_b(k)$$

So, if we apply this congruence element-wise, we arrive at the following formula

$$\alpha_b(m) \equiv \alpha_b(n)\alpha_b(k+1)^\ell \mod \alpha_b(k) \tag{3.9}$$

We are now ready to prove the divisibility properties; the following number-theoretical lemma is only stated for convenience.

Lemma 3.7. *Let $a, b, c \in \mathbb{N}$ and assume that a and b are coprime. Then*

$$a \mid b^n c \implies a \mid c$$

for all $n \in \mathbb{N}$.

Proof. The assertion holds trivially for $n = 0$, so let $n > 0$. Because a and b are coprime, it follows from the well known Bézout's lemma that there are integers x and y such that

$$ax + by = 1$$

Multiplying both sides with $b^{n-1}c$ we find that

$$ab^{n-1}cx + b^n cy = b^{n-1}c \tag{3.10}$$

Because $a \mid ab^{n-1}cx$ holds trivially and because $a \mid b^n cy$ follows from the assumption that $a \mid b^n c$, it follows that a must also divide the right side of (3.10), i.e. that $a \mid b^{n-1}c$.

We can now let $n' = n - 1$ and repeat the previous argument finitely many times until we can conclude that $a \mid c$.

∎

Proof (Theorem 3.4; First Divisibility Property). We exclude the case $k = 0$ because then $\alpha_b(k) = 0$ and

$$k \mid m \iff m = 0 \iff \alpha_b(m) = 0 \iff \alpha_b(k) \mid \alpha_b(m)$$

holds for all $m \in \mathbb{N}$, showing that the theorem holds for $k = 0$. Now let $k, m \in \mathbb{N}$ be arbitrary with $k > 0$ and let $\ell, n \in \mathbb{N}$ be the unique natural numbers with the property that

$$\begin{aligned} m &= k\ell + n \\ 0 \leq n &< k \end{aligned} \tag{3.11}$$

Our previous discussion then shows that (3.9) holds.

If $k \mid m$, then we must have $n = 0$ by (3.11) and thus $\alpha_b(n) = 0$. By (3.9) we have $\alpha_b(m) \equiv 0 \mod \alpha_b(k)$, i.e. $\alpha_b(k) \mid \alpha_b(m)$.

Conversely, if $\alpha_b(k) \mid \alpha_b(m)$, then it follows from (3.9) that

$$\alpha_b(k) \mid \alpha_b(n)\alpha_b(k+1)^\ell$$

Since we know that $\alpha_b(k)$ and $\alpha_b(k+1)$ are coprime (cf. Proposition 3.2), it follows from Lemma 3.7 that $\alpha_b(k) \mid \alpha_b(n)$. Because $n < k$ according to (3.11) it follows from the increasing property of the α_b-sequence (cf. Proposition 3.1) that $\alpha_b(n) < \alpha_b(k)$, showing that $\alpha_b(k) \mid \alpha_b(n)$ is only possible if $\alpha_b(n) = 0$. We conclude that $n = 0$ and by (3.11) we have $m = k\ell$, i.e. $k \mid m$.

∎

Proof (Theorem 3.5; Second Divisibility Property). Let $k, m \in \mathbb{N}$ be arbitrary. We exclude the case $k = 0$ because then $\alpha_b(k) = 0$ and

$$\alpha_b(k)^2 \mid \alpha_b(m) \iff \alpha_b(m) = 0 \iff m = 0 \iff k\alpha_b(k) \mid m$$

We also exclude the case $k \nmid m$ because then $k\alpha_b(k) \nmid m$ and, by the first divisibility property, $\alpha_b(k) \nmid \alpha_b(m)$ and thus $\alpha_b(k)^2 \nmid \alpha_b(m)$. So we trivially have

$$\alpha_b(k)^2 \mid \alpha_b(m) \iff k\alpha_b(k) \mid m,$$

because neither $k\alpha_b(k) \mid m$ nor $\alpha_b(k)^2 \mid \alpha_b(m)$ holds in this case.

Assume $k \mid m$ and let $\ell \in \mathbb{N}$ be such that $m = k\ell$. We consider the cases $\ell = 0$, $\ell = 1$ and $\ell \geq 2$ separately.

If $\ell = 0$, then $m = 0$ and $\alpha_b(m) = 0$; so our property holds trivially because both $\alpha_b(k)^2|\alpha_b(m)$ and $k\alpha_b(k) \mid m$ hold in this case.

If $\ell = 1$, then $m = k$ and thus $\alpha_b(m) = \alpha_b(k)$. It follows that

$$\begin{aligned} \alpha_b(k)^2 \mid \alpha_b(m) &\iff \alpha_b(k)^2 \mid \alpha_b(k) \\ &\iff \alpha_b(k) = 0 \vee \alpha_b(k) = 1 \\ &\iff k\alpha_b(k) \mid k \\ &\iff k\alpha_b(k) \mid m, \end{aligned}$$

showing that the property also holds in this case.

If $\ell \geq 2$ we have by matrix relation (3.4) that $A_b(m) = B_b^{k\ell} = A_b(k)^\ell$. Now, a direct computation shows that $A_b(k) = \alpha_b(k)B_b - \alpha_b(k-1)\mathrm{Id}$ because

$$\begin{aligned}\alpha_b(k)B_b - \alpha_b(k-1)\mathrm{Id} &= \begin{pmatrix} b\alpha_b(k) & -\alpha_b(k) \\ \alpha_b(k) & 0 \end{pmatrix} - \begin{pmatrix} \alpha_b(k-1) & 0 \\ 0 & \alpha_b(k-1) \end{pmatrix} \\ &= \begin{pmatrix} \alpha_b(k+1) & -\alpha_b(k) \\ \alpha_b(k) & -\alpha_b(k-1) \end{pmatrix} \\ &= A_b(k)\end{aligned}$$

By using Newton's binomial theorem, which states that $(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}$ for any two commuting elements x and y of some ring, we then find that

$$\begin{aligned}A_b(m) &= A_b(k)^\ell \\ &= \Big(\alpha_b(k)B_b - \alpha_b(k-1)\mathrm{Id}\Big)^\ell \\ &= \sum_{j=0}^{\ell} \binom{\ell}{j} \alpha_b(k)^j B_b^j (-1)^{\ell-j} \alpha_b(k-1)^{\ell-j} \mathrm{Id}^{\ell-j} \\ &= \sum_{j=0}^{\ell} \binom{\ell}{j} \alpha_b(k)^j (-1)^{\ell-j} \alpha_b(k-1)^{\ell-j} B_b^j \\ &= (-1)^\ell \alpha_b(k-1)^\ell \mathrm{Id} + \ell\alpha_b(k)(-1)^{\ell-1}\alpha_b(k-1)^{\ell-1}B_b + \alpha_b(k)^2 \sum_{j=2}^{\ell} \widetilde{B}_j\end{aligned}$$

for some irrelevant integer-valued matrices $\widetilde{B}_2, \ldots, \widetilde{B}_\ell$. This shows that we can pass to a congruence modulo $\alpha_b(k)^2$ to find that

$$A_b(m) \equiv (-1)^\ell \alpha_b(k-1)^\ell \mathrm{Id} + \ell\alpha_b(k)(-1)^{\ell-1}\alpha_b(k-1)^{\ell-1}B_b \mod \alpha_b(k)^2$$

If we apply this congruence element-wise, using the definitions of $A_b(m)$ and B_b, it follows that

$$\alpha_b(m) \equiv \ell\alpha_b(k)(-1)^{\ell-1}\alpha_b(k-1)^{\ell-1} \mod \alpha_b(k)^2 \tag{3.12}$$

We are now ready to show that $\alpha_b(k)^2 \mid \alpha_b(m) \iff k\alpha_b(k) \mid m$ also holds in the $\ell \geq 2$ case.

Assume that $\alpha_b(k)^2 \mid \alpha_b(m)$. Then we have by (3.12) that $\alpha_b(k)^2 \mid \ell\alpha_b(k)(-1)^{\ell-1}\alpha_b(k-1)^{\ell-1}$ from which it follows that $\alpha_b(k) \mid \ell(-1)^{\ell-1}\alpha_b(k-1)^{\ell-1}$. Now, noting that $k-1 \geq 0$ because we excluded $k=0$, we have that $\alpha_b(k)$ and $\alpha_b(k-1)$ are coprime by Proposition 3.2, so we can apply Lemma 3.7 to find that $\alpha_b(k) \mid (-1)^{\ell-1}l$, from which it follows that $\alpha_b(k) \mid \ell$. We conclude that $k\alpha_b(k) \mid k\ell$ and thus that $k\alpha_b(k) \mid m$ by definition of ℓ.

For the converse, assume that $k\alpha_b(k) \mid m$. Then $k\alpha_b(k) \mid k\ell$, showing that $\alpha_b(k) \mid \ell$, i.e. that $\ell = M\alpha_b(k)$ for some $M \in \mathbb{N}$. By (3.12) there is an $N \in \mathbb{Z}$ such that

$$\begin{aligned}\alpha_b(m) &= \ell\alpha_b(k)(-1)^{\ell-1}\alpha_b(k-1)^{\ell-1} + N\alpha_b(k)^2 \\ &= \left(M(-1)^{\ell-1}\alpha_b(k-1)^{\ell-1} + N\right)\alpha_b(k)^2,\end{aligned}$$

showing that $\alpha_b(k)^2 \mid \alpha_b(m)$.

∎

3.3 Congruence Properties

In this section, we prove the following congruence properties. They are much easier to prove than the divisibility properties.

Theorem 3.8 (First Congruence Property). *Let $b_1, b_2 \in \mathbb{N}_{\geq 2}$ and $q \in \mathbb{N}$. Then it holds for all $n \in \mathbb{N}$ that*

$$b_1 \equiv b_2 \mod q \implies \alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \mod q$$

Theorem 3.9 (Second Congruence Property). *Let $b \in \mathbb{N}_{\geq 2}$ and let $n, \ell, m, j \in \mathbb{N}$. Then*

$$n = 2\ell m \pm j \implies \alpha_b(n) \equiv \pm\alpha_b(j) \mod v$$

with v defined as $v = \alpha_b(m+1) - \alpha_b(m-1)$.

Here, the choices of "+" and "−" do not have to coincide, i.e. the formula should be read as: "if either $n = 2\ell m + j$ or $n = 2\ell m - j$, then either $\alpha_b(n) \equiv \alpha_b(j) \mod v$ or $\alpha_b(n) \equiv -\alpha_b(j) \mod v$".

Both proofs can be given immediately.

Proof (Theorem 3.8; First Congruence Property). The assertion will be proven by induction of n. If $n = 0$ or $n = 1$ then the implication holds trivially because $\alpha_b(0) = 0$ and $\alpha_b(1) = 1$ for all $b \in \mathbb{N}_{\geq 2}$.

For the induction hypothesis, assume that the implications

$$\begin{aligned} b_1 \equiv b_2 \mod q &\implies \alpha_{b_1}(n) \equiv \alpha_{b_2}(n) \mod q \\ b_1 \equiv b_2 \mod q &\implies \alpha_{b_1}(n+1) \equiv \alpha_{b_2}(n+1) \mod q \end{aligned}$$

hold for some arbitrary $n \in \mathbb{N}$. Then, if $b_1 \equiv b_2 \mod q$, there are integers M, N and P such that

$$\begin{aligned} b_1 - b_2 &= Mq \\ \alpha_{b_1}(n) - \alpha_{b_2}(n) &= Nq \\ \alpha_{b_1}(n+1) - \alpha_{b_2}(n+1) &= Pq \end{aligned}$$

A direct computation (using the definition of the α_b-sequence) then shows that

$$\begin{aligned} \alpha_{b_1}(n+2) - \alpha_{b_2}(n+2) &= b_1\alpha_{b_1}(n+1) - b_2\alpha_{b_2}(n+1) + \alpha_{b_1}(n) - \alpha_{b_2}(n) \\ &= b_1\alpha_{b_1}(n+1) - b_2\alpha_{b_2}(n+1) + Nq \\ &= b_1(Pq + \alpha_{b_2}(n+1)) - b_2\alpha_{b_2}(n+1) + Nq \\ &= (b_1 - b_2)\alpha_{b_2}(n+1) + b_1Pq + Nq \\ &= Mq\alpha_{b_2}(n+1) + (b_1P + N)q \\ &= (M\alpha_{b_2}(n+1) + b_1P + N)q, \end{aligned}$$

from which we see that $\alpha_{b_1}(n+2) \equiv \alpha_{b_2}(n+2) \mod q$.

∎

Remark 3.10. Before we prove the second property, let us quickly note that our matrix $A_b(n)$ from (3.3) is invertible because $\det(A_b(n)) = 1$ for all $n \in \mathbb{N}$, as we have seen in (3.5). Its inverse is given by

$$A_b(n)^{-1} = \begin{pmatrix} -\alpha_b(n-1) & \alpha_b(n) \\ -\alpha_b(n) & \alpha_b(n+1) \end{pmatrix}$$

♦

Proof (Theorem 3.9; Second Congruence Property). Let $n, \ell, m, j \in \mathbb{N}$ be such that $n = 2\ell m + j \vee n = 2\ell m - j$, which we denote by $n = 2\ell m \pm j$.

We exclude the case $\ell = 0$ because then $n = 2\ell m \pm j$ implies that $n = j$, showing that we trivially have $\alpha_b(n) \equiv \alpha_b(j) \mod v$.

Assume $\ell \geq 1$. Then it follows, as before, from our matrix relation (3.4) that

$$\begin{aligned} A_b(n) &= B_b^{2\ell m \pm j} \\ &= \left((B_b^m)^2\right)^\ell B_b^{\pm j} \\ &= \left(A_b(m)^2\right)^\ell A_b(j)^{\pm 1} \end{aligned} \tag{3.13}$$

As stated in the theorem, let $v = \alpha_b(m+1) - \alpha_b(m-1)$. It is directly seen from the definition of $A_b(m)$ that

$$A_b(m) + A_b(m)^{-1} = \begin{pmatrix} v & 0 \\ 0 & -v \end{pmatrix}$$

which shows that $A_b(m) \equiv -A_b(m)^{-1} \mod v$. If we multiply both sides with $A_b(m)$ we find that $A_b(m)^2 \equiv -\mathrm{Id} \mod v$, i.e.

$$A_b(m)^2 = vD - \mathrm{Id}$$

for some integer valued matrix D. Continuing our previous calculation (3.13) and applying Newton's binomial theorem, we find that

$$\begin{aligned} A_b(n) &= (vD - \mathrm{Id})^\ell A_b(j)^{\pm 1} \\ &= \left(\sum_{i=0}^{\ell} \binom{\ell}{i} v^i D^i (-1)^{\ell-i} \mathrm{Id}^{\ell-i}\right) A_b(j)^{\pm 1} \\ &= \left(\sum_{i=0}^{\ell} \binom{\ell}{i} (-1)^{\ell-i} v^i D^i\right) A_b(j)^{\pm 1} \\ &= \left((-1)^\ell \mathrm{Id} + v \sum_{i=1}^{\ell} \widetilde{D}_i\right) A_b(j)^{\pm 1} \end{aligned}$$

for some irrelevant integer valued matrices $\widetilde{D}_1, \ldots, \widetilde{D}_\ell$. According to this last formula, we can then pass to a congruence modulo v to find that

$$A_b(n) \equiv (-1)^\ell A_b(j)^{\pm 1} \mod v$$

Since the element in row 2 column 1 of the matrix $A_b(j)^{\pm 1}$ is equal to $\pm\alpha_b(j)$, cf. Remark 3.10, we can apply the above congruence element-wise to find that

$$\alpha_b(n) \equiv \pm(-1)^\ell \alpha_b(j) \mod v$$

Obviously $\pm(-1)^\ell \in \{-1, 1\}$ for all ℓ, so we conclude that either $\alpha_b(n) \equiv \alpha_b(j) \mod v$ or $\alpha_b(n) \equiv -\alpha_b(j) \mod v$ holds, i.e. $\alpha_b(n) \equiv \pm\alpha_b(j) \mod v$.

■

3.4 The α_b-sequence is Diophantine

In this section we show that the α_b-sequence is Diophantine for $b > 3$ by proving that, for all triples $(a, b, c) \in \mathbb{N}^3$, the following equivalence holds.

$$3 < b \wedge a = \alpha_b(c) \iff \exists rstuvwxy \in \mathbb{N}(\varphi_1 \wedge \cdots \wedge \varphi_{15}), \tag{3.14}$$

Here, the formulas $\varphi_1, \ldots, \varphi_{15}$ are given by

$$3 < b \tag{φ_1}$$
$$u^2 - but + t^2 = 1 \tag{φ_2}$$
$$s^2 - bsr + r^2 = 1 \tag{φ_3}$$
$$r < s \tag{φ_4}$$
$$u^2 \mid s \tag{φ_5}$$
$$v = bs - 2r \tag{φ_6}$$
$$w \equiv b \mod v \tag{φ_7}$$
$$w \equiv 2 \mod u \tag{φ_8}$$
$$2 < w \tag{φ_9}$$
$$x^2 - wxy + y^2 = 1 \tag{φ_{10}}$$
$$2a < u \tag{φ_{11}}$$
$$2a < v \tag{φ_{12}}$$
$$a \equiv x \mod v \tag{φ_{13}}$$
$$2c < u \tag{φ_{14}}$$
$$c \equiv x \mod u \tag{φ_{15}}$$

The Sufficiency

We will first show that the right hand side of (3.14) is sufficient. Let $(a, b, c) \in \mathbb{N}^3$ be arbitrary and let $s, r, t, u, v, w, x, y \in \mathbb{N}$ be such that the formulas $\varphi_1, \ldots, \varphi_{15}$ hold.

It follows trivially from φ_1 that $3 < b$, so it remains to prove that $a = \alpha_b(c)$. We begin by applying Theorem 3.3 to φ_2 to find that

$$u = \alpha_b(k) \tag{3.15}$$

for some $k \in \mathbb{N}$. The same theorem can be applied to φ_3 to find that

$$\begin{aligned} r &= \alpha_b(m-1) \\ s &= \alpha_b(m) \end{aligned} \tag{3.16}$$

for some $m \in \mathbb{N}_{\geq 1}$, where we have taken into account that the case $r = \alpha_b(m) \wedge s = \alpha_b(m-1)$ is impossible by φ_4.

It follows from φ_5 that $u^2 \mid s$, i.e. that $\alpha_b(k)^2 \mid \alpha_b(m)$, so we can apply the second divisibility property (Theorem 3.5) to find that $k\alpha_b(k) \mid m$, i.e. that $ku \mid m$ and thus that

$$u \mid m \tag{3.17}$$

Now, because $w > 2$ according to φ_9, we can also apply Theorem 3.3 to φ_{10} to find that

$$x = \alpha_w(n) \tag{3.18}$$

for some $n \in \mathbb{N}$. This fixes the numbers k, m and n.

Because $m \in \mathbb{N}_{\geq 1}$ we can consider the division of n by m to find unique $\ell', j' \in \mathbb{N}$ with $j' < m$ such that

$$n = \ell' m + j'$$

We want to show that there are natural numbers $\ell, j \in \mathbb{N}$, not necessarily unique, such that $j \leq m$ and either $n = 2\ell m + j$ or $n = 2\ell m - j$, i.e. $n = 2\ell m \pm j$.

- If ℓ' is even, let $\ell = \ell'/2$ and $j = j'$. Then $0 \leq j \leq m$ and

$$\begin{aligned} 2\ell m + j &= \ell' m + j' \\ &= n \end{aligned}$$

- If ℓ' is odd, let $\ell = (\ell' + 1)/2$ and $j = (m - j')$. Then $0 \leq j \leq m$ and

$$\begin{aligned} 2\ell m - j &= (\ell' + 1)m - (m - j') \\ &= \ell' m + j' \\ &= n \end{aligned}$$

By the above, let $\ell, j \in \mathbb{N}$ be such that

$$\begin{aligned} n &= 2\ell m \pm j \\ j &\leq m \end{aligned} \tag{3.19}$$

According to φ_6 we have a number $v = bs - 2r$, so it follows from (3.16) and the definition of our sequence that

$$\begin{aligned} v &= b\alpha_b(m) - 2\alpha_b(m-1) \\ &= \alpha_b(m+1) - \alpha_b(m-1) \end{aligned} \tag{3.20}$$

We will now show, using both of our congruence properties (Theorems 3.8 and 3.9), that $a \equiv \pm\alpha_b(j) \mod v$. Note that

$$\begin{aligned} a &\equiv x \mod v && \text{by } \varphi_{13} \\ x &\equiv \alpha_w(n) \mod v && \text{by (3.18)} \\ \alpha_w(n) &\equiv \alpha_b(n) \mod v && \text{by applying Theorem 3.8 to } \varphi_7 \\ \alpha_b(n) &\equiv \pm\alpha_b(j) \mod v && \text{by applying Theorem 3.9 to (3.19) and (3.20)} \end{aligned}$$

By transitivity of the congruence relation, we conclude that $a \equiv \pm\alpha_b(j) \mod v$.

From φ_{12} we already know that $2a < v$. Our goal is to show that $2\alpha_b(j) < v$ holds also, which can be seen as follows.

$$\begin{aligned} 2\alpha_b(j) &\leq 2\alpha_b(m) && \text{because } j \leq m \text{ by (3.19)} \\ &\leq (b-2)\alpha_b(m) && \text{because } b > 3 \text{ by } \varphi_1 \\ &< b\alpha_b(m) - 2\alpha_b(m-1) && \text{because } \alpha_b(m) > \alpha_b(m-1) \\ &= v && \text{by (3.20)} \end{aligned}$$

So far, we conclude that $a \equiv \pm\alpha_b(j) \mod v$, where $0 \leq 2a < v$ and $0 \leq 2\alpha_b(j) < v$. According to the following lemma, this is only possible if $a = \alpha_b(j)$.

Lemma 3.11. *Let $a, b, v \in \mathbb{N}$ be such that $a \equiv \pm b \mod v$, where $0 \leq 2a < v$ and $0 \leq 2b < v$. Then $a = b$.*

Proof. If $a \equiv b \mod v$, let $k \in \mathbb{Z}$ be such that $a - b = kv$. If $k \geq 1$, then $a = b + kv \geq v$ and thus $2a \geq v$, quod non. Similarly, if $k \leq -1$, then $b = a + (-k)v \geq v$ and thus $2\alpha_b(j) \geq v$, quod non. It follows that we must have $k = 0$ and therefore $a = b$.

If $a \equiv -b \mod v$ we can write $a + b = kv$ for some $k \in \mathbb{N}$. It follows that $2kv = 2(a+b) < 2v$, which is only possibly if $k = 0$. So $a = b = 0$.

∎

By the preceding lemma, we have

$$a = \alpha_b(j) \tag{3.21}$$

In the remainder of this proof, it will be shown that $j = c$. First, note that

$$\begin{aligned} c &\equiv x \mod u && \text{by } \varphi_{15} \\ x &\equiv \alpha_w(n) \mod u && \text{by (3.18)} \\ \alpha_w(n) &\equiv \alpha_2(n) \mod u && \text{by applying Theorem 3.8 to } \varphi_8 \\ \alpha_2(n) &\equiv n \mod u && \text{because } \alpha_2(n) = n \text{ by linearity of } \alpha_2 \end{aligned}$$

The above then shows that $c \equiv n \mod u$. Now, because $n = 2\ell m \pm j$ by (3.19) and because $u \mid m$ by (3.17), it is easily seen that

$$c \equiv \pm j \mod u \tag{3.22}$$

We already know that $2c < u$ by φ_{14}. It can be seen that $2j < u$ also holds because $2j \leq 2\alpha_b(j)$ by Proposition 3.1 and $2\alpha_b(j) = 2a$ by (3.21), where $2a < u$ by φ_{11}.

This shows that the conditions of Lemma 3.11 are satisfied, from which it follows that $j = c$. Together with (3.21), this implies that $a = \alpha_b(c)$, which proves the sufficiency.

The Necessity

We will now show that the right hand side of (3.14) is necessary, so let $(a, b, c) \in \mathbb{N}^3$ be such that $3 < b$ and $a = \alpha_b(c)$. We have to find natural numbers s, r, t, u, v, w, x, y satisfying formulas $\varphi_1, \ldots, \varphi_{15}$, so, for readability, I will place $[\varphi_i]$ in the margin whenever we have shown that formula φ_i holds.

Obviously, φ_1 holds trivially. Let $k \in \mathbb{N}$ be any number such that $\alpha_b(k) > \max(2a, 2c)$ and such that $\alpha_b(k)$ is odd[1]. We define [φ_1]

$$u = \alpha_b(k)$$

so that φ_{11} and φ_{14} hold. Next, we define [φ_{11}] [φ_{14}]

$$t = \alpha_b(k+1)$$

so that it follows from Theorem 3.3 that $u^2 - but + t^2 = 1$, i.e. that φ_2 holds. [φ_2]

With the numbers k and $u = \alpha_b(k)$ defined, we let $m = ku$. Then $m \geq 1$, for if $m = 0$ we would have $k = \alpha_b(k) = 0$, which is a contradiction since $\alpha_b(k)$ was assumed odd. With this in mind, we define $r, s \in \mathbb{N}$ as follows.

$$\begin{aligned} r &= \alpha_b(m-1) \\ s &= \alpha_b(m) \end{aligned}$$

Then it follows from Theorem 3.3 and the increasing property of our sequence that φ_3 and φ_4 hold. Furthermore, since we trivially have $ku \mid m$ by definition of m, where $u = \alpha_b(k)$, it follows [φ_3] [φ_4]

from the second divisibility property (Theorem 3.5) that $\alpha_b(k)^2 \mid \alpha_b(m)$, i.e. that $u^2 \mid s$. So φ_5 [φ_5]
holds as well.

We now define the number $v \in \mathbb{N}$ as

$$v = bs - 2r,$$

so that φ_6 holds trivially. It can then be seen that [φ_6]

$$\begin{aligned} v &= b\alpha_b(m) - 2\alpha_b(m-1) && \text{by definition of } s \text{ and } r \\ &\geq 4\alpha_b(m) - 2\alpha_b(m-1) && \text{because } b > 3 \\ &> 2\alpha_b(m) && \text{because } \alpha_b(m) - \alpha_b(m-1) > 0 \\ &\geq 2m && \text{by Proposition 3.1} \\ &\geq 2u && \text{because } m = ku \text{ and } m \geq 1 \\ &> 4a && \text{by } \varphi_{11} \end{aligned}$$

We conclude that $2a < v$ and thus that φ_{12} holds as well. [φ_{12}]

Next, we show that $u = \alpha_b(k)$ and $v = bs - 2r$ are coprime. Assume $d \in \mathbb{N}$ is such that $d \mid u$ and $d \mid v$. Then, because $u = \alpha_b(k)$ was assumed to be odd, it follows that d must be odd as well. Furthermore we have $2r = bs - v$ by definition of v. Because $d \mid v$ holds by assumption and because $d \mid s$ follows from the assumption $d \mid u$, together with the fact $u^2 \mid s$, which follows from φ_5, we conclude that $d \mid (v - bs)$, i.e. $d \mid 2r$, must hold as well.

The above shows that $2r = \ell' d$ for some $\ell' \in \mathbb{N}$, but, because d is odd, we must have $\ell' = 2\ell$ for some $\ell \in \mathbb{N}$. It follows that $r = \ell d$ and thus that $d \mid r$. We have shown that $d \mid r$ and $d \mid s$, so, because $r = \alpha_b(m-1)$ and $s = \alpha_b(m)$ are coprime by Proposition 3.2 we conclude that $d = 1$.

Because u and v are coprime we can use the Chinese remainder theorem to find an integer $w \in \mathbb{Z}$ such that

$$\begin{aligned} w &\equiv 2 \mod u \\ w &\equiv b \mod v \end{aligned}$$

We can assume that $w > 2$ for if it is not, we can replace it by $w' = w + \ell uv$ for some suffi-
ciently large $\ell \in \mathbb{N}$, where $u, v \geq 1$ according to φ_{11} and φ_{12}. Then w' would also satisfy both [φ_7]
congruences. We conclude that φ_7, φ_8 and φ_9 hold. [φ_8]

Having defined w, we are ready for the last part. Define [φ_9]

$$\begin{aligned} x &= \alpha_w(c) \\ y &= \alpha_w(c+1) \end{aligned}$$

where we recall that the c refers to the third element of our tuple $(a, b, c) \in \mathbb{N}^3$. Then it already
follows from Theorem 3.3 that φ_{10} holds. [φ_{10}]

Since $w \equiv b \mod v$ by φ_7, where $w, b \geq 2$, it follows from the first congruence property
(Theorem 3.8) that $\alpha_w(c) \equiv \alpha_b(c) \mod v$. Because $x = \alpha_w(c)$ by definition and because $a =$
$\alpha_b(c)$ follows from our main assumption, we see that $x \equiv a \mod v$, i.e. that φ_{13} holds. [φ_{13}]

Now, obviously $w \equiv 2 \mod (w-2)$ holds for any number w, so it follows from the first
congruence property that $\alpha_w(c) \equiv \alpha_2(c) \mod (w-2)$. Linearity of the α_2-sequence together
with the definition of x then implies that $x \equiv c \mod (w-2)$. Because $w \equiv 2 \mod u$ by φ_8, we
conclude that $x \equiv c \mod u$, which shows that φ_{15} holds as well. This proves the necessity. [φ_{15}]

[1] it follows from (3.6) that, for all $k \in \mathbb{N}$, either $\alpha_b(k)$ or $\alpha_b(k+1)$ is odd; if they were both even it would follow that $(2m)^2 - b(2m)(2n) + (2n)^2 = 1$, i.e. that $2(2m^2 - 2bmn + 2n^2) = 1$ for certain $n, m \in \mathbb{N}$, showing that 1 is an even number

Conclusion

Let us summarize the main result of this section in a theorem for future reference.

Theorem 3.12. *The α_b-sequence is Diophantine for $b > 3$, i.e. the set*

$$\{(a,b,c) \in \mathbb{N}^3 \mid 3 < b \wedge a = \alpha_b(c)\}$$

is Diophantine.

Proof. We have shown that

$$\{(a,b,c) \in \mathbb{N}^3 \mid 3 < b \wedge a = \alpha_b(c)\} = \{(a,b,c) \in \mathbb{N}^3 \mid \exists rstuvwxy \in \mathbb{N}(\varphi_1 \wedge \cdots \wedge \varphi_{15})\},$$

with the formulas $\varphi_1, \ldots, \varphi_{15}$ given at the beginning of this section.

From Proposition 1.13 we know that each of the φ_i's is a Diophantine formula. It follows that $\exists rstuvwxy \in \mathbb{N}(\varphi_1 \wedge \cdots \wedge \varphi_{15})$ is a conjunction of Diophantine formulas, preceded by existential quantifiers; therefore, by Theorem 1.9, it is Diophantine.

■

3.5 From the α_b-sequence to Exponentiation

We start this final section with a lemma.

Lemma 3.13. *Let $q, r \in \mathbb{N}$ be natural numbers with $q > 0$. If $b, m \in \mathbb{N}$ satisfy*

$$\begin{aligned} b &= \alpha_{q+4}(r+1) + q^2 + 2 \\ m &= bq - q^2 - 1 \end{aligned}$$

then

$$\begin{aligned} q\alpha_b(r) - \alpha_b(r-1) &\equiv q^r \mod m \\ q^r &< m \end{aligned}$$

Proof. We first show that $q\alpha_b(r) - \alpha_b(r-1) \equiv q^r \mod m$. Let B_b denote the matrix from (3.3). A direct computation then shows that

$$\begin{aligned} B_b \begin{pmatrix} q \\ 1 \end{pmatrix} &= \begin{pmatrix} bq-1 \\ q \end{pmatrix} \\ &= \begin{pmatrix} q^2+m \\ q \end{pmatrix} \\ &= q\begin{pmatrix} q \\ 1 \end{pmatrix} + \begin{pmatrix} m \\ 0 \end{pmatrix} \end{aligned}$$

from which we see that

$$B_b \begin{pmatrix} q \\ 1 \end{pmatrix} \equiv q \begin{pmatrix} q \\ 1 \end{pmatrix} \mod m$$

Because $A_b(r) = B_b^r$, it follows that

$$\begin{aligned} A_b(r)\begin{pmatrix} q \\ 1 \end{pmatrix} &= B_b^r \begin{pmatrix} q \\ 1 \end{pmatrix} \\ &\equiv q^r \begin{pmatrix} q \\ 1 \end{pmatrix} \mod m \end{aligned} \tag{3.23}$$

If we write out the left side of the above congruence, i.e.

$$\begin{aligned} A_b(r)\begin{pmatrix} q \\ 1 \end{pmatrix} &= \begin{pmatrix} \alpha_b(r+1) & -\alpha_b(r) \\ \alpha_b(r) & -\alpha_b(r-1) \end{pmatrix} \begin{pmatrix} q \\ 1 \end{pmatrix} \\ &= \begin{pmatrix} q\alpha_b(r+1) - \alpha_b(r) \\ q\alpha_b(r) - \alpha_b(r-1) \end{pmatrix} \end{aligned}$$

and apply the congruence element-wise, it follows that $q\alpha_b(r) - \alpha_b(r-1) \equiv q^r \mod m$.

To show that $q^r < m$, note that $\alpha_{q+4}(r+1) \geq (q+3)^r$ by Proposition 3.1 so that

$$\begin{aligned} b &= \alpha_{q+4}(r+1) + q^2 + 2 \\ &\geq (q+3)^{r+1} + q^2 + 2 \\ &> q^r + q + 1 \end{aligned}$$

With this, we see that

$$\begin{aligned} m &= bq - q^2 - 1 \\ &> (q^r + q + 1)q - q^2 - 1 \\ &= q^{r+1} + (q-1) \\ &\geq q^r \end{aligned}$$

∎

We are now ready to prove a most remarkable theorem.

Theorem 3.14 (Exponentiation is Diophantine). *The set*

$$\{(p, q, r) \in \mathbb{N}^3 \mid p = q^r\}$$

is Diophantine.

Proof. We will show that

$$\begin{aligned} p = q^r \iff & (q = 0 \wedge r = 0 \wedge p = 1) \\ & \vee (q = 0 \wedge 0 < r \wedge p = 0) \\ & \vee \exists bm \in \mathbb{N}\big(\\ & \qquad 0 < q \\ & \qquad \wedge b = \alpha_{q+4}(r+1) + q^2 + 2 \\ & \qquad \wedge m = bq - q^2 - 1 \\ & \qquad \wedge q\alpha_b(r) - \alpha_b(r-1) \equiv p \mod m \\ & \qquad \wedge p < m \\ & \big) \end{aligned} \tag{3.24}$$

holds for all $(p, q, r) \in \mathbb{N}^3$, where we recall that $\alpha_b(-1) = -1$ so that the formula $q\alpha_b(r) - \alpha_b(r-1) \equiv p \mod m$ is interpreted as $1 \equiv p \mod m$ whenever $r = 0$.

Assume $p, q, r \in \mathbb{N}$ satisfy $p = q^r$. If $q = 0$, we must have $p = 1$ if $r = 0$ and $p = 0$ otherwise. If $q > 0$, we define $b = \alpha_{q+4}(r+1) + q^2 + 2$ and $m = bq - q^2 - 1$. Then it follows from Lemma 3.13 that $q\alpha_b(r) - \alpha_b(r-1) \equiv q^r \mod m$ and $q^r < m$. Because $p = q^r$ by assumption, we see that the right hand side of (3.24) holds.

For the converse, let $p, q, r \in \mathbb{N}$ be such that the right hand side of (3.24) holds. If $q = 0$, then either $(q = 0 \wedge r = 0 \wedge p = 1)$ or $(q = 0 \wedge 0 < r \wedge p = 0)$ must hold, in which case we already have $p = q^r$. If $q > 0$, there must be $b, m \in \mathbb{N}$ such that

$$\begin{aligned} b &= \alpha_{q+4}(r+1) + q^2 + 2 \\ m &= bq - q^2 - 1 \\ q\alpha_b(r) - \alpha_b(r-1) &\equiv p \mod m \\ p &< m \end{aligned}$$

For such b and m, however, we have by Lemma 3.13 that $q\alpha_b(r) - \alpha_b(r-1) \equiv q^r \mod m$ with $q^r < m$. We conclude that there are integers $N, M \in \mathbb{Z}$ such that

$$\begin{aligned} q\alpha_b(r) - \alpha_b(r-1) &= Nm + p, &\qquad 0 \le p < m \\ q\alpha_b(r) - \alpha_b(r-1) &= Mm + q^r, &\qquad 0 \le q^r < m \end{aligned}$$

By the Euclidean division theorem (note that $m > 0$), we see that $N = M$ and $p = q^r$. This proves that (3.24) holds for all $p, q, r \in \mathbb{N}$.

From (3.24) it can be seen that

$$\begin{aligned} p = q^r \iff & (q = 0 \wedge r = 0 \wedge p = 1) \\ & \vee (q = 0 \wedge 0 < r \wedge p = 0) \\ & \vee \exists bmt_1t_2t_3 \in \mathbb{N}\big(\\ & \qquad 0 < q \\ & \qquad \wedge b = t_1 + q^2 + 2 \\ & \qquad \wedge t_1 = \alpha_{q+4}(r+1) \\ & \qquad \wedge m = bq - q^2 - 1 \\ & \qquad \wedge \begin{pmatrix} \big(qt_2 - t_3 \equiv p \mod m \wedge t_2 = \alpha_b(r) \wedge t_3 = \alpha_b(r-1) \wedge 0 < r\big) \\ \vee \\ \big(1 \equiv p \mod m \wedge r = 0\big) \end{pmatrix} \\ & \qquad \wedge p < m \\ & \big) \end{aligned}$$

Here, the formulas

$$\begin{aligned} t_1 &= \alpha_{q+4}(r+1) \\ t_2 &= \alpha_b(r) \\ t_3 &= \alpha_b(r-1), \end{aligned}$$

are all Diophantine by Theorem 3.12, where we note that $q+4 > 3$ and $b = \alpha_{q+4}(r+1)+q^2+2 > 3$ whenever $q > 0$. The remaining formulas are all Diophantine by Proposition 1.13, so the formula

$p = q^r$ is equivalent to a formula $\psi(p, q, r)$, where ψ is built up from Diophantine formulas and connected by conjunctions, disjunctions and existential quantifiers. It then follows from Theorem 1.9 that the set

$$\{(p, q, r) \in \mathbb{N}^3 \mid p = q^r\} = \{(p, q, r) \in \mathbb{N}^3 \mid \psi(p, q, r)\}$$

is Diophantine.

∎

Chapter 4

The Negative Resolution

We are finally ready to present the negative resolution of Hilbert's tenth problem as a corollary of the DPRM theorem.

Theorem 4.1 (DPRM Theorem; 1970). *Every computably enumerable set is Diophantine.*

Proof. We know from the DPR Theorem (cf. Theorem 2.18) that every computable enumerable set is exponential Diophantine and we know from Theorem 1.12 that every exponential Diophantine set is Diophantine on the premise that exponentiation is Diophantine. The result then follows from Theorem 3.14.

∎

Corollary 4.2 (Negative Resolution of Hilbert's Tenth Problem). *There is no algorithm which determines for an arbitrary Diophantine equation whether it has a solution over $\mathbb{Z}$.*

Proof. Assume that the described algorithm exists. Then for an arbitrary Diophantine equation, say of the form

$$F(x_1, \ldots, x_{k+m}) = 0 \tag{4.1}$$

where $F \in \mathbb{Z}[X_1, \ldots, X_{k+m}]$, we have some program which tells us after some finite computation whether (4.1) has a solution over $\mathbb{Z}$ in the unknowns $x_1, \ldots, x_{k+m}$. In particular, for every list $a_1, \ldots, a_k \in \mathbb{N}$ of parameters, the program would be able to tell us after some finite computation whether the Diophantine equation

$$F(a_1, \ldots, a_k, x_1, \ldots, x_m) = 0$$

has a solution over $\mathbb{Z}$ in the unknowns $x_1, \ldots, x_n$.

Put differently, such a program would always tell us after some finite computation whether some arbitrary k-tuple $(a_1, \ldots, a_k) \in \mathbb{N}^k$ lies in the Diophantine set

$$\{(a_1, \ldots, a_k) \in \mathbb{N}^k \mid \exists x_1 \cdots x_k \in \mathbb{N}\, (F(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0)\} \tag{4.2}$$

In the light of Remark 2.7, it follows that every set of the form (4.2) is computable. Because *every* Diophantine set is of the form (4.2) for some $F \in \mathbb{Z}[X_1, \ldots, X_{k+n}]$, we conclude that every Diophantine set must be computable. According to the DPRM Theorem (cf. Theorem 4.1), every computably enumerable set must then be computable. Because this gives a contradiction with the set $\mathcal{H} \subseteq \mathbb{N}^k$ from Theorem 2.8, the algorithm cannot exist.

∎

Chapter 5

Appendix

5.1 Lagrange's Squares Theorem

We begin with some lemma's.

Lemma 5.1 (Euler's Squares Identity). *Let $a, b, c, d, w, x, y, z \in \mathbb{N}$. Then*

$$\begin{aligned}(a^2+b^2+c^2+d^2)(w^2+x^2+y^2+z^2) &= (aw+bx+cy+dz)^2+(ax-bw-cz+dy)^2 \\ &\quad + (ay+bz-cw-dx)^2+(az-by+cx-dw)^2\end{aligned}$$

Proof. If we write out the left-hand side, there are 16 terms in total, i.e. the terms a^2w^2, b^2x^2, a^2z^2, etc. If we write out the right-hand side, we certainly find these 16 necessary terms as well. So, we only have to show that the extra terms on the right-hand side (i.e. terms which are not of the form $\lambda^2\xi^2$ for $\lambda \in \{a, b, c, d\}$ and $\xi \in \{w, x, y, z\}$) all cancel out against each other. It is easily seen that these extra terms are exactly the following terms.

$$\begin{array}{llllll}
+2(aw)(bx) & +2(aw)(cy) & +2(aw)(dz) & +2(bx)(cy) & +2(bx)(dz) & +2(cy)(dz) \\
-2(ax)(bw) & -2(ax)(cz) & +2(ax)(dy) & +2(bw)(cz) & -2(bw)(dy) & -2(cz)(dy) \\
+2(ay)(bz) & -2(ay)(cw) & -2(ay)(dx) & -2(bz)(cw) & -2(bz)(dx) & +2(cw)(dx) \\
-2(az)(by) & +2(az)(cx) & -2(az)(dw) & -2(by)(cx) & +2(by)(dw) & -2(cx)(dw)
\end{array}$$

Because in each of these 6 columns, the 4 terms always sum to zero, the extra terms all cancel out against each other.

∎

Lemma 5.2. *Let $m \in \mathbb{N}$. If $2m$ is the sum of two squares, then so is m.*

Proof. Say $2m = x^2 + y^2$ for some $x, y \in \mathbb{N}$. It is easily seen that either both x and y are odd, or both x and y are even. In any of these cases, the numbers $x - y$ and $x + y$ are both even, so

$$\frac{x+y}{2}, \frac{x-y}{2} \in \mathbb{N}$$

and we see that m is the sum of two squares because

$$\begin{aligned}\left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2 &= \frac{x^2-2xy+y^2}{4}+\frac{x^2+2xy+y^2}{4}\\ &= \frac{x^2+y^2}{2}\\ &= m\end{aligned}$$

■

Lemma 5.3. *Let p be an odd prime. There are $a, b \in \mathbb{Z}$ such that*

$$kp = a^2 + b^2 + 1$$

for some $k \in \mathbb{N}$ with $0 < k < p$.

Proof. Let p be an odd prime, say $p = 2n + 1$. We define two sets $A, B \subseteq \mathbb{Z}$ as follows

$$\begin{aligned}A &= \{a^2 \mid a \in \{0, \ldots, n\}\}\\ B &= \{-(b^2+1) \mid b \in \{0, \ldots, n\}\}\end{aligned}$$

We will show that there are no two distinct elements $a_1, a_2 \in A$ such that $a_1 \equiv a_2 \mod p$. If $a_1, a_2 \in A$, say $a_1 = x^2$ and $a_2 = y^2$ for $x, y \in \{0, \ldots, n\}$, then $a_1 \equiv a_2 \mod p$ would imply that $p \mid x^2 - y^2$, i.e. that $p \mid (x + y)(x - y)$. Because p is prime, it follows that

$$p \mid (x+y) \qquad \text{or} \qquad p \mid (x-y) \tag{5.1}$$

However, because $|x + y| < p$ and $|x - y| < p$, we see that (5.1) can only hold if either $x + y = 0$ or $x - y = 0$. It follows that $x = y$ in all cases, i.e. $a_1 = a_2$, and we conclude that A has no two distinct elements which are congruent modulo p. In the same way it is shown that B contains no two distinct elements which are congruent modulo p either.

Now, because A and B are disjoint, the set $A \cup B$ has $p+1$ elements. Because every element of $A \cup B$ belongs to one of the p residue classes $[0]_p, [1]_p, \ldots, [p-1]_p$, it follows from the pigeonhole principle that there are two distinct elements of $A \cup B$ which belong to the same residue class, i.e. there are two distinct $w_1, w_2 \in A \cup B$ such that $w_1 \equiv w_2 \mod p$. It follows from our previous discussion that w_1 and w_2 can't both lie in A or B. So, there must be $a, b \in \{0, \ldots, n\}$ such that

$$a^2 + b^2 + 1 = kp$$

for some $k \in \mathbb{Z}$. Obviously, this k satisfies $k > 0$. Furthermore, since $p^2 = (2n+1)^2 > 2n^2 + 1 \geq a^2 + b^2 + 1 = kp$, it follows that $p > k$. So $0 < k < p$.

■

We are now ready for the main theorem.

Theorem (Lagrange's Squares Theorem). *Every natural number is a sum of four squares.*

Proof. Let $n \in \mathbb{N}$. We exclude the cases $n = 0$ and $n = 1$ since

$$\begin{aligned}0 &= 0^2 + 0^2 + 0^2 + 0^2\\ 1 &= 1^2 + 0^2 + 0^2 + 0^2\end{aligned}$$

So, assume $n \geq 2$. Because n can be written as a finite (non-empty) product of primes, it suffices by Lemma 5.1 to show that every prime can be written as the sum of four squares (because, if a and b in $\mathbb{N}$ are both a sum of four squares, then so is ab). Because $2 = 1^2 + 1^2 + 0^2 + 0^2$, it suffices to show that every *odd* prime can be written as the sum of four squares.

Let p be an odd prime. By Lemma 5.3, there exist $a, b, c, d, k \in \mathbb{N}$ such that

$$kp = a^2 + b^2 + c^2 + d^2 \tag{5.2}$$

with $0 < k < p$. If $k = 1$ then it already follows that p is the sum of four squares, so we shall assume that $1 < k < p$.

Let $\mathrm{fsq}(n)$ denote the predicate "n is the sum of four squares". We shall prove the following theorem.

$$\forall k \in \mathbb{N}\Big(\big(1 < k < p \wedge \mathrm{fsq}(kp)\big) \to \exists m \in \mathbb{N}\big(1 \leq m < k \wedge \mathrm{fsq}(mp)\big)\Big) \tag{5.3}$$

In words, (5.3) tells us that, whenever kp is the sum of four squares, with $1 < k < p$, there is some m with $1 \leq m < k$ such that mp is the sum of four squares. Because kp is the sum of four squares by (5.2), with $1 < k < p$, we could repeatedly apply (5.3) to find that our odd prime p must be a sum of four squares as well, which is exactly what we needed to show. So, it suffices to prove (5.3).

Assume that $k \in \mathbb{N}$ satisfies both $1 < k < p$ and (5.2) for certain $a, b, c, d \in \mathbb{N}$. We will assume that k is odd because if k is even we can write

$$2mp = a^2 + b^2 + c^2 + d^2$$

for some $m \in \mathbb{N}$ with $1 \leq m < k$. It then follows from Lemma 5.2 that mp is a sum of four squares, already showing that (5.3) holds. So, assume k is odd. We want to find integers w, x, y and z satisfying

$$\begin{aligned} w &\equiv a \mod k \\ x &\equiv b \mod k \\ y &\equiv c \mod k \\ z &\equiv d \mod k \end{aligned} \tag{5.4}$$

and

$$w, x, y, z \in (-k/2, k/2) \tag{5.5}$$

To show that such a w exists, we must find some $Z \in \mathbb{Z}$ so that we can define $w = Zk + a$, where $w \in (-k/2, k/2)$. This is equivalent to finding some $Z \in \mathbb{Z}$ such that

$$Z + \frac{a}{k} \in (-1/2, 1/2)$$

Since $a/k \in \mathbb{R}_{\geq 0}$, we can write $a/k = X + r$ for some $X \in \mathbb{N}$ and some $r \in [0, 1)$. If $r < 1/2$, we choose $Z = -X$ so that $Z + a/k = r \in (-1/2, 1/2)$. If $r > 1/2$ we choose $Z = -X - 1$ so that $Z + a/k = r - 1 \in (-1/2, 1/2)$. The case $r = 1/2$ is impossible because it would imply that $a/k = X + 1/2$, i.e. that $2a = (2X + 1)k$, which is only possible if k is even, contradicting our assumption that k is odd. In exactly the same way we can find $x, y, z \in \mathbb{Z}$ such that the corresponding conditions (5.4) and (5.5) are satisfied.

By the above, let $w, x, y, z \in \mathbb{Z}$ be such that (5.4) and (5.5) hold. Then we see from (5.5) that

$$w^2 + x^2 + y^2 + z^2 < k^2 \tag{5.6}$$

Furthermore, it is easily seen from the congruences (5.4), together with condition (5.2), that $w^2 + x^2 + y^2 + z^2 \equiv 0 \mod k$, i.e. that

$$mk = w^2 + x^2 + y^2 + z^2 \tag{5.7}$$

for some $m \in \mathbb{N}$, where $m < k$ according to (5.6).

We will show that $1 \leq m < k$. If $m = 0$, then $w = x = y = z = 0$ by (5.7). So, $a \equiv b \equiv c \equiv d \equiv 0 \mod k$ by (5.4), showing that a^2, b^2, c^2 and d^2 are all multiples of k^2. But then it follows from (5.2) that $kp = Nk^2$ for some $N \in \mathbb{N}$, implying that $p = Nk$ and contradicting our assumption that p is a prime.

So, we have found integers $w, x, y, z \in \mathbb{Z}$ and $n \in \mathbb{N}$ such that

$$\begin{aligned} mk &= w^2 + x^2 + y^2 + z^2 \\ 1 &\leq m < k \end{aligned} \tag{5.8}$$

Together with (5.2), this implies that

$$(a^2 + b^2 + c^2 + d^2)(w^2 + x^2 + y^2 + z^2) = k^2 mp \tag{5.9}$$

Now, consider the four squares on the right hand side of Euler's squares identity in Lemma 5.1. With (5.4) and (5.2), it is easily seen that the first square, i.e. the term $(aw + bx + cy + dz)^2$, is a multiple of k^2. To be explicit, according to (5.4) we can write $w = N_1 k + a$ for some $N_1 \in \mathbb{Z}$, showing that $aw = (aN_1)k + a^2$. Similarly, $bx = (bN_2)k + b^2$, $cy = (cN_3)k + c^2$ and $dz = (dN_4)k + d^2$, showing that

$$\begin{aligned} aw + bx + cy + dz &= (aN_1 + bN_2 + cN_3 + dN_4)k + a^2 + b^2 + c^2 + d^2 \\ &= (aN_1 + bN_2 + cN_3 + dN_4 + p)k \end{aligned}$$

and thus that

$$aw + bx + cy + dz \equiv 0 \mod k \tag{5.10}$$

The same conclusion holds for the three remaining squares. Note that, according to (5.4), we have $N_1, N_2, N_3, N_4 \in \mathbb{Z}$ such that

$$\begin{aligned} ax - bw - cz + dy &= (ax - wx + xw - bw) + (dy - dc + cd - cz) \\ &= (a - w)x + (x - b)w + d(y - c) + c(d - z) \\ &= (N_1 x + N_2 w + dN_3 + cN_4)k \end{aligned}$$

showing that

$$ax - bw - cz + dy \equiv 0 \mod k \tag{5.11}$$

In exactly the same way as above, it can be seen from the congruences (5.4) that

$$ay + bz - cw - dx \equiv 0 \mod k \tag{5.12}$$

and

$$az - by + cx - dw \equiv 0 \mod k \tag{5.13}$$

Now, it follows from equation (5.9), Euler's squares identity (cf. Lemma 5.1) and the congruences (5.10)—(5.13) that there are natural numbers M_1, M_2, M_3 and M_4 such that

$$k^2 mp = (M_1^2 + M_2^2 + M_3^2 + M_4^2)k^2$$

i.e. that $mp = M_1^2 + M_2^2 + M_3^2 + M_4^2$. Because $1 \leq m < k$ according to (5.8), we finally conclude that (5.3) holds. Because we have argued that this result is sufficient for Lagrange's squares theorem, this completes the proof.

∎

5.2 Kummer's Theorem

Theorem (Kummer's Theorem). *Let a and b be natural numbers and, for every prime p, let $\delta_p(a,b) \in \mathbb{N}$ be the highest number such that $p^{\delta_p(a,b)}$ divides $\binom{a+b}{b}$. Then $\delta_p(a,b)$ may be calculated as follows:*

> *Write a and b in base-p notation and add them together. The number of carries which occur during this addition is exactly the number $\delta_p(a,b)$.*

Proof. Throughout this proof, let p denote some prime. If $n \in \mathbb{N}$ we shall write $\varepsilon_p(n) \in \mathbb{N}$ for the highest number such that $p^{\varepsilon_p(n)}$ divides $n!$, i.e. such that

$$n! = \prod_{p \text{ prime}} p^{\varepsilon_p(n)}$$

We shall use a counting argument to show that

$$\varepsilon_p(n) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor \tag{5.14}$$

where $\lfloor \cdot \rfloor : \mathbb{R} \to \mathbb{Z}$ denotes the floor function.

The list $1, 2, \ldots, n$ contains exactly $\lfloor n/p \rfloor$ multiples of p, so we could say that $\varepsilon_p(n)$ is simply equal to $\lfloor n/p \rfloor$. However, if the list also contains multiples of p^2, then these would only be counted once, while they *should* be counted twice. Therefore, it would be better to say that $\varepsilon_p(n)$ is equal to $\lfloor n/p \rfloor + \lfloor n/p^2 \rfloor$ because then every multiple of p is counted once and every multiple of p^2 is *also* counted once. However, every multiple of p^3 is only counted twice in this approach, so we should add the correcting term $\lfloor n/p^3 \rfloor$ to $\varepsilon_p(n)$. By taking into account all powers of p, we find that (5.14) must hold.

For the remainder of this proof, let a and b be some natural numbers. The familiar definition

$$\binom{a+b}{b} = \frac{(a+b)!}{a!b!}$$

now allows us to express $\delta_p(a,b)$ in terms of $\varepsilon_p(a+b)$, $\varepsilon_p(a)$ and $\varepsilon_p(b)$. By definition of the δ_p's and the ε_p's we have

$$\begin{aligned}
\prod_{p \text{ prime}} p^{\delta_p(a,b)} &= \binom{a+b}{b} \\
&= \frac{(a+b)!}{a!b!} \\
&= \frac{\prod_{p \text{ prime}} p^{\varepsilon_p(a+b)}}{\left(\prod_{p \text{ prime}} p^{\varepsilon_p(a)}\right)\left(\prod_{p \text{ prime}} p^{\varepsilon_p(b)}\right)} \\
&= \prod_{p \text{ prime}} p^{\varepsilon_p(a,b)-\varepsilon_p(a)-\varepsilon_p(b)},
\end{aligned}$$

implying that $\delta_p(a,b) = \varepsilon_p(a+b) - \varepsilon_p(a) - \varepsilon_p(b)$. By (5.14), this result is then equivalent to

$$\delta_p(a,b) = \sum_{k=1}^{\infty} S_k \tag{5.15}$$

with S_k defined as

$$S_k = \left\lfloor \frac{a+b}{p^k} \right\rfloor - \left\lfloor \frac{a}{p^k} \right\rfloor - \left\lfloor \frac{b}{p^k} \right\rfloor \tag{5.16}$$

Let us write $\cdots a_2 a_1 a_{0\langle p \rangle}$ and $\cdots b_2 b_1 b_{0\langle p \rangle}$ for the base-p digits of a and b respectively. Because $a = \sum_{j=0}^{\infty} a_j p^j$, it then follows that

$$\frac{a}{p^k} = \frac{\sum_{j=0}^{k-1} a_j p^j}{p^k} + \sum_{j=k}^{\infty} a_j p^{j-k}$$

where $\sum_{j=k}^{\infty} a_j p^{j-k} \in \mathbb{N}$. So, by a basic property of the floor function, we have that

$$\left\lfloor \frac{a}{p^k} \right\rfloor = \left\lfloor \frac{\sum_{j=0}^{k-1} a_j p^j}{p^k} \right\rfloor + \sum_{j=k}^{\infty} a_j p^{j-k}$$

Now, because $a_j < p$ for all j (by definition of base-p representation), i.e. $a_j \leq p-1$ for all j, it follows that

$$\begin{aligned} \sum_{j=0}^{k-1} a_j p^j &\leq \sum_{j=0}^{k-1} (p-1) p^j \\ &= \sum_{j=0}^{k-1} (p^{j+1} - p^j) \\ &= p^k - 1 \\ &< p^k \end{aligned}$$

so that $\left(\sum_{j=0}^{k-1} a_j p^j \right) / p^k < 1$, implying that $\left\lfloor \left(\sum_{j=0}^{k-1} a_j p^j \right) / p^k \right\rfloor = 0$ and thus that

$$\left\lfloor \frac{a}{p^k} \right\rfloor = \sum_{j=k}^{\infty} a_j p^{j-k}$$

By analyzing $\lfloor b/p^k \rfloor$ and $\lfloor (a+b)/p^k \rfloor$ in a similar way, it is easily seen that certain terms cancel, causing (5.16) to reduce to the following form

$$S_k = \left\lfloor \frac{\sum_{j=0}^{k-1} (a_j + b_j) p^j}{p^k} \right\rfloor \tag{5.17}$$

Since $0 \leq a_j < p$ and $0 \leq b_j < p$ for all j, it is easily seen that $S_k \in \{0, 1\}$ for all k because

$$\begin{aligned} 0 \leq \sum_{j=0}^{k-1} (a_j + b_j) p^j &\leq 2 \sum_{j=0}^{k-1} (p-1) p^j \\ &= 2p^k - 2 \\ &< 2p^k \end{aligned}$$

Considering the base-p addition of natural numbers $a = \cdots a_2 a_1 a_{0\langle p \rangle}$ and $b = \cdots b_2 b_1 b_{0\langle p \rangle}$, we are now ready to prove that

$$S_{k+1} = \begin{cases} 1 & \text{if there is a carry from the } k\text{-th digit (to the } (k+1)\text{-th digit)} \\ 0 & \text{otherwise} \end{cases} \tag{5.18}$$

holds for all $k \in \mathbb{N}$. Note that Kummer's Theorem would immediately follow from this because $\delta_p(a,b) = \sum_{k=1}^{\infty} S_k$ by (5.15).

Before we prove that (5.18) holds for all $k \in \mathbb{N}$, let Carry(k) denote the predicate "there is a carry from the k-th digit (to the next digit)". Because $S_k \in \{0,1\}$ for all k, it is easily seen that (5.18) is then equivalent to

$$\text{Carry}(k) \iff S_{k+1} = 1 \tag{5.19}$$

Using the principle of induction, we shall prove that (5.19) holds for all $k \in \mathbb{N}$.

For the induction basis, note that

$$\text{Carry}(0) \iff a_0 + b_0 \geq p \iff 1 \leq \frac{a_0 + b_0}{p} < 2 \iff \left\lfloor \frac{a_0 + b_0}{p} \right\rfloor = 1 \iff S_1 = 1,$$

where, again, we used that $a_j < p$ and $b_j < p$ for all $j \in \mathbb{N}$.

For the induction hypothesis, assume that (5.19) holds. We have to show that

$$\text{Carry}(k+1) \iff S_{k+2} = 1 \tag{5.20}$$

holds as well. However, because $k + 1 > 0$ we need to think a bit more carefully about when Carry($k+1$) exactly holds, i.e. when a carry from the $(k+1)$-th digit to the next digit exactly occurs.

Certainly, a carry from the $(k+1)$-th digit to the next occurs if $a_{k+1} + b_{k+1} \geq p$. However, if $a_{k+1} + b_{k+1} = p - 1$ and a carry from the k-th digit to the $(k+1)$-th digit has *already* occurred, we will also get a carry from the $(k+1)$-th digit to the next, even though $a_{k+1} + b_{k+1} < p$. For example, in the binary addition of $1 = 01_{\langle 2 \rangle}$ and $3 = 11_{\langle 2 \rangle}$, there is also a carry from the first digit to the second, even though $0 + 1 < 2$, because a carry from the zeroth to the first digit has already occurred. This means that we have the following inductive relation.

$$\text{Carry}(k+1) \iff \Big(a_{k+1} + b_{k+1} \geq p \lor \big(a_{k+1} + b_{k+1} = p - 1 \land \text{Carry}(k)\big)\Big)$$

Because Carry(k) $\iff$ $S_{k+1} = 1$ by our induction hypothesis (5.19), it follows that (5.20) is equivalent to

$$\Big(a_{k+1} + b_{k+1} \geq p \lor \big(a_{k+1} + b_{k+1} = p - 1 \land S_{k+1} = 1\big)\Big) \iff S_{k+2} = 1 \tag{5.21}$$

so that, instead of proving (5.20), we can also prove (5.21). Before we do this, let us quickly note that

$$S_n = 1 \iff \sum_{j=0}^{n-1} (a_j + b_j) p^j \geq p^n \ , \qquad \text{for all } n \in \mathbb{N} \tag{5.22}$$

which follows (almost) immediately from (5.17).

Assume that the left hand side of (5.21) holds. If $a_{k+1} + b_{k+1} \geq p$, we immediately see that

$$\begin{aligned}
\sum_{j=0}^{k+1} (a_j + b_j) p^j &= (a_{k+1} + b_{k+1}) p^{k+1} + \sum_{j=0}^{k} (a_j + b_j) p^j \\
&\geq p^{k+2} + \sum_{j=0}^{k} (a_j + b_j) p^j \\
&\geq p^{k+2}
\end{aligned}$$

so that $S_{k+2} = 1$ by (5.22), as desired. If $a_{k+1} + b_{k+1} = p - 1$ and $S_{k+1} = 1$, we know from (5.22) that

$$\sum_{j=0}^{k} (a_j + b_j)p^j \geq p^{k+1}$$

so that

$$\begin{aligned}\sum_{j=0}^{k+1} (a_j + b_j)p^j &= \sum_{j=0}^{k} (a_j + b_j)p^j + (a_{k+1} + b_{k+1})p^{k+1} \\ &\geq p^{k+1} + (a_{k+1} + b_{k+1})p^{k+1} \\ &= (1 + a_{k+1} + b_{k+1})p^{k+1} \\ &= p^{k+2}\end{aligned}$$

It then follows from (5.22) again that $S_{k+2} = 1$, as desired.

For the converse, assume that the right hand side of (5.21) holds. By (5.22), we have that

$$\sum_{j=0}^{k+1} (a_j + b_j)p^j \geq p^{k+2} \tag{5.23}$$

We first show that (5.23) already implies that $a_{k+1} + b_{k+1} \geq p - 1$. If $a_{k+1} + b_{k+1} < p - 1$, it would follow that $a_{k+1} + b_{k+1} \leq p - 2$; together with the fact that $a_j + b_j \leq 2(p - 1)$ for all j, this would imply that

$$\begin{aligned}\sum_{j=0}^{k+1} (a_j + b_j)p^j &= \sum_{j=0}^{k} (a_j + b_j)p^j + (a_{k+1} + b_{k+1})p^{k+1} \\ &\leq 2\sum_{j=0}^{k} (p - 1)p^j + (p - 2)p^{k+1} \\ &= 2(p^{k+1} - 1) + p^{k+2} - 2p^{k+1} \\ &< p^{k+2},\end{aligned}$$

which is a contradiction. So, there are only two cases two consider: $a_{k+1} + b_{k+1} > p - 1$ and $a_{k+1} + b_{k+1} = p - 1$.

Case 1. If $a_{k+1} + b_{k+1} > p - 1$ it follows that $a_{k+1} + b_{k+1} \geq p$, showing that the left hand side of (5.21) already holds.

Case 2. If $a_{k+1} + b_{k+1} = p - 1$, the left hand side of (5.21) almost holds; it remains to show that $S_{k+1} = 1$. From (5.23) it follows that

$$\begin{aligned}\sum_{j=0}^{k} (a_j + b_j)p^j &\geq p^{k+2} - (a_{k+1} + b_{k+1})p^{k+1} \\ &= p^{k+2} - (p - 1)p^{k+1} \\ &= p^{k+1}\end{aligned}$$

so that $S_{k+1} = 1$ by (5.22), as desired.

∎

References

[1] A. Church. *An Unsolvable Problem of Elementary Number Theory*, American Journal of Mathematics, vol. 58(2), pp. 345-363, 1936.

[2] J.D. Clemens. *Math 459; Computability and Unsolvability Lecture Notes*, 2003.

[3] M. Davis. *Arithmetical problems and recursively enumerable predicates*, Journal of Symbolic Logic, vol. 18(1), pp. 33-41, 1953.

[4] M. Davis, H. Putnam, J. Robinson. *The Decision Problem for Exponential Diophantine Equations*, Annals of Mathematics, vol. 74(3), pp. 425-436, 1961.

[5] R.R. Dipert, J.J. Hintikka, P.V. Spade. *History of logic*, August 2014. Article retrieved from `http://www.britannica.com/`.

[6] D. Hilbert. *Mathematische Probleme*, Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, pp. 253-297, 1900.

[7] D. Hilbert. *Mathematical problems*, Bulletin of the American Mathematical Society, vol. 8(10), pp. 437-479, 1902.

[8] S.C. Kleene. *General recursive functions of natural numbers*, Mathematische Annalen, vol. 112, pp. 727-742, 1936.

[9] E.E. Kummer. *Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen*, Journal für die reine und angewandte Mathematik, pp. 93-146, 1852.

[10] Y. Matiyasevich. *On Hilbert's Tenth Problem*, PIMS Distinguished Chair Lectures, Edited by M.P. Lamoureux, 2000.

[11] J. van Oosten. *Basic Computability Theory*, Revised 2013.

[12] J. van Oosten. *Gödel's Incompleteness Theorems*, 2015.

[13] E.L. Post. *Finitary Combinatory Processes—Formulation I*, Journal of Symbolic Logic, vol. 1(3), pp. 103-105, 1936.

[14] A.M. Turing. *On Computable Numbers, With An Application To The Entscheidungsproblem*, Proceedings of the London Mathematical Society, series 2(42), pp. 230-265, 1937.

Index