MTHA7029Y Mathematics Dissertation 2021/22

Goodstein's Theorem

Shay Anthony Jordan

100238811

Abstract

Goodstein's Theorem claims that every Goodstein Sequence converges to 0, despite each such sequence seemingly growing very large, very quickly – suggesting that perhaps they behave quite opposite to the claim of Goodstein's Theorem. The theorem is interesting in its own right, and can be proven using arithmetic of transfinite ordinals. What is more interesting though is that it *must* be proven using arithmetic of transfinite ordinals – as Goodstein's Theorem is (and can be proven to be) undecidable in Peano Arithmetic if Peano Arithmetic is consistent. This result thus extends to a purely number theoretic testament to Gödel's Incompleteness Theorems, proving the incompleteness of Peano Arithmetic.

Supervised by Dr David Asperó

Contents

Introduction

The late nineteenth century and early twentieth century saw an increasing interest in the axiomatisation of arithmetic by mathematicians, and in 1889, Italian mathematician Giuseppe Peano (1858-1932) published *Arithmetices principia nova methodo exposita* – translating from Latin as *The principles of arithmetic presented by a new method.* Within, Peano stated his now famous first-order axioms of number theory (*Peano Arithmetic*), which axiomatise the theory of arithmetic over the natural numbers. As such, Peano is widely regarded as the founder of symbolic logic, and modernised variants of his axioms of arithmetic are still commonly referred to today – in the twenty-first century.

Almost half a century after Peano's axiomatisation of arithmetic, Austro-Hungarian mathematician Kurt Gödel (1906-1978) published his Incompleteness Theorems, which are hugely influential and key to our present understanding of symbolic logic and mathematical theories. Whilst Gödel's Incompleteness Theorems were largely influential, the examples presented alongside them were metamathematical; thus, Barwise (1977) notes that ever since Kurt Gödel published his Incompleteness Theorems in 1931, many sought to find a purely mathematical application of the theorems.

Thirteen years after Gödel's theorems were published, English mathematician Reuben Goodstein (1912-1985) introduced concepts now known as Goodstein Sequences and Goodstein's Theorem in *The Journal of Symbolic Logic* (Goodstein, 1944). Goodstein's Theorem is a statement about natural numbers which claims that for all $a \in \mathbb{N}$, the Goodstein Sequence $(G_i(a))_{i\in\mathbb{N}}$ terminates – meaning that it converges to 0 after a finite number of steps. Goodstein's Theorem is interesting in its own right, as it provides a surprising and unexpected result about the sequences (which seemingly grow extremely fast for most values of $a \in \mathbb{N}$); however, what is more interesting is that Goodstein's Theorem can actually be proven to be independent of (undecidable in) Peano Arithmetic, if Peano Arithmetic is consistent.

The implications of the undecidability/unprovability of Goodstein's Theorem in Peano Arithmetic bear huge significance in the field of symbolic logic and our understanding of incompleteness. Goodstein's Theorem acts precisely as a vehicle for proving the incompleteness of Peano Arithmetic, giving the first ever number theoretic example of Gödel's First Incompleteness Theorem, by appeal to Gödel's Second Incompleteness Theorem (Miller, 2001).

Both Goodstein's Theorem and its unprovability in Peano Arithmetic have a number of consequences. Whilst they most prominently give us a better understanding of the incompleteness of Peano Arithmetic, they also inspire research interests in a number of other areas of mathematics. For example, the nature of Goodstein Sequences growing very large, very fast cultivates interest in its own right, and makes for interesting consideration within other areas of mathematics – including as a dynamical system.

In this report, we shall first introduce Goodstein Sequences and Goodstein's Theorem (Part I) through summary of Goodstein's original work (Goodstein, 1944), and construct a proof of Goodstein's Theorem using ordinal arithmetic in Part II. In Section 5, we will then develop the foundations to begin to understand what it means for something to be unprovable in a given system of axioms. We shall introduce many logical concepts, and then use these as a basis to give a detailed analysis of precisely why Goodstein's Theorem is unprovable in Peano Arithmetic in Section 6. With this, we shall consider the implications and consequences of its unprovability in Peano Arithmetic, including its relevance to Gödel's Incompleteness Theorems and the idea of *truth* in arithmetic, in Section 7.

Part I

Goodstein's Theorem

"*Cut off one head, two more shall take its place.*"

- Johann Schmidt, *Captain America: The First Avenger.*

1 Goodstein Sequences

Goodstein Sequences are sequences of natural numbers, which seemingly grow at an incredible rate; so much so that their behaviour has been compared with that of a hydra – as shall be discussed in subsection 2.2. Despite each step of the sequence involving subtracting 1 from the previous value, most Goodstein Sequences still appear to grow exponentially at every step. However, we shall see that there is more to Goodstein Sequences than what one may expect, and – similarly – there is more to the behaviour of a hydra too, as an equivalent construction of Goodstein Sequences.

1.1 Hereditary Base-b Notation

The key concept used in Goodstein Sequences is the idea of *hereditary base-b* notation of natural numbers, whereby a number $a \in \mathbb{N}$ is expressed as the sum of powers of $b \in \mathbb{N}$, and all exponents also expressed as the sum of powers of b recursively. To understand *hereditary base-b* notation, we first introduce the conversion of standard base-10 natural numbers to alternate bases.

Definition 1.1. Let $n \in \mathbb{Z}$ be an integer. To convert n to base b, we compute $d_0, d_1, \dots, d_k \in \mathbb{N}$, with $0 \leq d_i < b$ for every d_i, such that

$$n = \pm(d_k b^k + d_{k-1} b^{k-1} + \cdots + d_1 b + d_0).$$

Remark 1.2 (A method for writing n in base b)**.**

1. First, compute k such that $b^k \leq n < b^{k+1}$.
2. Next, write $n = d_k b^k + r_k$ – with $d_k, r_k \in \mathbb{N}$, where d_k is maximal, and r_k is the remainder when n is divided by b^k. By construction, we have $0 \leq d_k < b$.
3. If $b \leq r$, return to step 1 to write r_k in base-b notation (using $n = r_k$). Otherwise, if $r_k < b$, proceed to step 4.

4. We now have expressions in the form $a = qb + r$, for $a = n$, and $a = r_k$ for all applicable k. We can then obtain an expression for n in base-b by substituting our expressions for r_k into our expression for n recursively, until we reach an expression equal to n, with $r < b$.

Using this definition and method, we now present some examples:

Example 1.3. Writing 81 in base-3 notation, we have:

$$3^4 = 81 \leq 81 < 243 = 3^5,$$

so $81 = q \cdot 3^4 + r$, where $q = 1$ and $r = 0$. So, in base-3 notation, we have

$$81 = 3^4.$$

Example 1.4. Writing 2021 in base-2 notation, we have:

$$2^{10} = 1024 \leq 2021 < 2048 = 2^{11}.$$

So we write $2021 = q \cdot 2^{10} + r$. In this case, we have $q = 1$, and $r = 997$. That is:

$$2021 = 2^{10} + 997. \tag{1.1}$$

We now convert $r = 997$ into base-2 notation, by finding k such that $b^k \leq 997 < b^{k+1}$. $k = 9$ satisfies this, so we write $997 = q \cdot 2^9 + r$, where $q = 1$, and $r = 485$.

Having obtained that $997 = 2^9 + 485$, we can substitute this into equation 1.1 to derive

$$2021 = 2^{10} + 2^9 + 485,$$

and repeat the process again for $r = 485$ to obtain

$$2021 = 2^{10} + 2^9 + 2^8 + 229,$$

and again for $r = 229$. We continue this for each subsequent value for r obtained by repeatedly performing the algorithm, until a value of r is found which satisfies $r < b$. This eventually arrives at the following base-2 notation way of writing 2021:

$$2021 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^2 + 1.$$

We now extend the concept of base-b notation to *hereditary* base-b notation; the key element from which Goodstein Sequences are constructed.

Definition 1.5. Let $n \in \mathbb{N}$ be a natural number. To write n in *hereditary base-b* notation, we first write n in base-b notation (as in Definition 1.1), and then write all exponents in base-b – and recursively, all exponents of exponents – until the expression is formed solely of integers less than or equal to b.

Example 1.6 (Extending from Example 1.3)**.** Writing 81 in base-3 notation, we have:

$$81 = 3^4$$

So converting this to *hereditary* base-3 notation, this is:

$$81 = 3^{3+1}$$

Example 1.7 (Extending from Example 1.4)**.** Writing 2021 in base-2 notation, we have:

$$2021 = 2^{10} + 2^9 + 2^8 + 2^7 + 2^6 + 2^5 + 2^2 + 1.$$

Converting this to *hereditary* base-2 notation, we write all of the powers (and subsequently, powers of powers) in base 2 notation until our expression for 2021 is made entirely of integers less than or equal to 2 – as such:

$$2021 = 2^{2^{2+1}+2} + 2^{2^{2+1}+1} + 2^{2^{2+1}} + 2^{2^2+2+1} + 2^{2^2+2} + 2^{2^2+1} + 2^2 + 1.$$

1.2 Goodstein Sequences

In his 1944 article, *On the Restricted Ordinal Theorem* (Goodstein, 1944), Reuben Goodstein defined sequences of natural numbers which became widely known as *Goodstein Sequences*. These sequences rely on first writing a natural number $a \in \mathbb{N}$ in hereditary base-b notation before performing two actions to the hereditary base-b representation of a, to obtain the succeeding entry of the sequence. The following definition details how a Goodstein Sequence is obtained for any natural number a.

Definition 1.8. The *Goodstein Sequence* for a natural number $a \in \mathbb{N}$ is a sequence $(G_i(a))_{i\in\mathbb{N}}$ of natural numbers, defined as such:

- The first term of the Goodstein Sequence $G_1(a) = a$.
- Each subsequent i^{th} term $G_i(a)$ is computed as such:
  1. Write $G_{i-1}(a)$ in hereditary base-i notation (as in Definition 1.5). $\left(\xrightarrow{\textbf{h base-}i}\right)$
  2. Substitute each i with $i+1$. $\left(\xrightarrow{i\,\mapsto\,i+1}\right)$
  3. Subtract 1 from the result. $\left(\xrightarrow{\textbf{cut}}\right)$

We now see some examples of the construction of Goodstein Sequences:

Example 1.9. To find the second term of the Goodstein Sequence for $a \in \mathbb{N}$, we must:

1. Write $G_1(a) = a$ in hereditary base-2 notation. $\left(\xrightarrow{\textbf{h base-2}}\right)$
2. Substitute each 2 with a 3. $\left(\xrightarrow{2 \mapsto 3}\right)$
3. Subtract 1 from the result. $\left(\xrightarrow{\textbf{cut}}\right)$

Example 1.10. The Goodstein Sequence for $a = 2$, $(G_i(2))_{i \in \mathbb{N}}$, is as follows:

$$
\begin{aligned}
&G_1(2) = 2. \\
&G_2(2) = 2 \xrightarrow{\textbf{h base-2}} 2 \xrightarrow{2 \mapsto 3} 3 \xrightarrow{\textbf{cut}} 3 - 1 = 2. \\
&G_3(2) = 2 \xrightarrow{\textbf{h base-3}} 2 \xrightarrow{3 \mapsto 4} 2 \xrightarrow{\textbf{cut}} 2 - 1 = 1. \\
&G_4(2) = 1 \xrightarrow{\textbf{h base-4}} 1 \xrightarrow{4 \mapsto 5} 1 \xrightarrow{\textbf{cut}} 1 - 1 = 0. \\
&G_5(2) = 0 \xrightarrow{\textbf{h base-5}} 0 \xrightarrow{5 \mapsto 6} 0 \xrightarrow{\textbf{cut}} 0 - 1 = -1 \notin \mathbb{N}. \\
&\quad\vdots \qquad \vdots
\end{aligned}
$$

We see that the fifth term of the Goodstein Sequence for $a = 2$ is $G_5(2) = -1$, but Goodstein Sequences are sequences of natural numbers, and $-1 \notin \mathbb{N}$. Thus, we say that the Goodstein Sequence $(G_i(2))_{i \in \mathbb{N}}$ *terminates* at the fourth term of the sequence. In fact, we can see that any Goodstein Sequence will terminate at the first term equal to 0, due to the following proposition.

Proposition 1.11. The Goodstein Sequence for $a \in \mathbb{N}$ terminates at the i^{th} term if and only if $G_i(a) = 0$.

Proof. We begin by proving the backwards direction. That is, $G_i(a) = 0$ implies that the sequence terminates at $G_i(a)$.

($\leftarrow$) Suppose $G_i(a) = 0$. By Definition 1.8, to obtain $G_{i+1}(a)$, we must write $G_i(a) = 0$ in hereditary base-$(i+1)$ notation, then substitute each $i+1$ for $i+2$, and subtract 1 from the result. For any $b \in \mathbb{N}$, we have that 0 is equal to 0 in base b, and so the hereditary base-$(i+1)$ notation for 0 is 0. There are no occurrences of $i+1$ in 0, so there is nothing to replace with $i+2$, and finally we subtract 1 from our 0. Thus, $G_{i+1}(a) = -1$, which is not a natural number and hence is not part of the sequence. So the sequence must terminate at $G_i(n)$, the i^{th} term.

($\rightarrow$) Conversely, suppose the sequence terminates at $G_i(a)$. Then, if we computed what would be the $(i+1)^{th}$ term, we would have $G_{i+1}(a) \notin \mathbb{N}$, so $G_{i+1}(a) < 0$. We have two cases:

1. $\mathbf{G_{i+1}(a) = -1}$: in this case, to get back to $G_i(a)$, we must perform the inverse operations specified in Definition 1.8 in reverse order to $G_{i+1}(a)$. That is,

$$\begin{aligned} G_{i+1} + 1 &= 0 \text{ (add 1)} \\ &= 0 \text{ (substitute each } i+2 \text{ with } i+1) \\ &= 0 \text{ (evaluate the expression as a natural number)} \end{aligned}$$

   So $G_i(a) = 0$, as required.

2. $\mathbf{G_{i+1}(a) < -1}$: by performing the same inverse operations as in case 1, we see that $G_i(a)$ must also be negative, thus meaning that $G_i(a)$ is also not a natural number and thus not part of the Goodstein Sequence – which is a contradiction, meaning that this case is not possible.

□

Corollary 1.12. For every $a \in \mathbb{N}$, the Goodstein Sequence $(G_i(a))_{i\in\mathbb{N}}$ terminates at the k^{th} term, where $k \in \mathbb{N}$ is the minimum natural number such that $G_k(a) = 0$.

Definition 1.13. We define the *Goodstein Function* $\mathcal{G}(a)$ as the length of the Goodstein Sequence $(G_i(a))_{i\in\mathbb{N}}$ for $a \in \mathbb{N}$. That is, $\mathcal{G}(a) = k$, where $G_k(a) = 0$.

Example 1.14. We saw in Example 1.10 that $(G_i(2))_{i\in\mathbb{N}}$ terminates at the fourth term, so it has length 4. Thus,

$$\mathcal{G}(2) = 4.$$

We now see another example of a Goodstein Sequence, but for a larger value of a:

Example 1.15. The Goodstein Sequence for $a = 5$ begins as follows:

$$\begin{aligned}
&G_1(5) = 5. \\
&G_2(5) = 5 \xrightarrow{\textbf{h base-2}} 2^2 + 1 \xrightarrow{2 \mapsto 3} 3^3 + 1 \xrightarrow{\textbf{cut}} 3^3 = 27. \\
&G_3(5) = 27 \xrightarrow{\textbf{h base-3}} 3^3 \xrightarrow{3 \mapsto 4} 4^4 \xrightarrow{\textbf{cut}} 4^4 - 1 = 256 - 1 = 255. \\
&G_4(5) = 255 \xrightarrow{\textbf{h base-4}} 3\cdot 4^3 + 3\cdot 4^2 + 3\cdot 4 + 3 \xrightarrow{4 \mapsto 5} 3\cdot 5^3 + 3\cdot 5^2 + 3\cdot 5 + 3 \\
&\qquad\qquad\qquad \xrightarrow{\textbf{cut}} 468 - 1 = 467. \\
&G_5(5) = 467 \xrightarrow{\textbf{h base-5}} 3\cdot 5^3 + 3\cdot 5^2 + 3\cdot 5 + 2 \xrightarrow{5 \mapsto 6} 3\cdot 6^3 + 3\cdot 6^2 + 3\cdot 6 + 2 \\
&\qquad\qquad\qquad \xrightarrow{\textbf{cut}} 776 - 1 = 775. \\
&\quad \vdots \qquad \vdots
\end{aligned}$$

As we saw in Example 1.10 (and 1.14), $\mathcal{G}(2) = 4$, as the 4^{th} term of the sequence is 0. In Example 1.15, we see that the sequence seems to grow very quickly, and – if the sequence does terminate – it does not appear to happen for a low value of i. In fact, for larger values of a, the sequence $(G_i(a))_{i\in\mathbb{N}}$ seemingly gets much larger, much quicker. From this observation, it may seem an absurd suggestion that all Goodstein Sequences, even those for large a, eventually become decreasing sequences. Even more absurd would be the suggestion that every Goodstein Sequence terminates after a finite number of terms. However, it is precisely this which Goodstein's Theorem says – which we shall now see.

2 Goodstein's Theorem

2.1 Statement of the Theorem

From the examples given in subsection 1.2, one may hypothesise that perhaps there exists some natural number n such that the Goodstein Sequence for any $m \in \mathbb{N}$ greater than n diverges to infinity. This seems like a sensible hypothesis, as we have seen an example of a small $a \in \mathbb{N}$ such that the sequence decreases, and we have seen a larger value for $a \in \mathbb{N}$ whose Goodstein Sequence increases very quickly.

Contrarily though, Goodstein's Theorem – stated and proven by Goodstein (1944) – states a perhaps unexpected result, which is much the opposite to the prediction above.

Theorem 2.1 (Goodstein's Theorem)**.** For every $a \in \mathbb{N}$, the Goodstein Sequence $(G_i(a))_{i\in\mathbb{N}}$ for a is finite in length. That is, there exists some $k \in \mathbb{N}$ such that $G_k(a) = 0$, meaning that – by Proposition 1.11 – the Goodstein Sequence for a terminates at the k^{th} term, and $\mathcal{G}(a) = k$.

In fact, many mathematicians have discovered and proven relations which allow us to calculate the value of $\mathcal{G}(a)$ based on the value of a. The earliest of these discoveries is that of Kirby and Paris (1982), which recognises that $\mathcal{G}$ has a growth-rate similar to that of the *Hardy hierarchy* H_{ε_0}.[1]

Table 1 gives the value for i such that $G_i(a) = 0$ – that is, the length of the Goodstein sequence for $a \in \mathbb{N}$.

a	$\mathcal{G}(a)$
1	2
2	4
3	6
4	$3 \cdot 2^{402653211} - 2$
5	$> 10^{10^{10^{19728}}}$
$\vdots$	$\vdots$

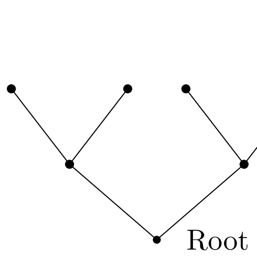
Table 1: The lengths of the Goodstein Sequences for a up to 5.

[1] These were introduced by Hardy (1904), and occur in computability theory. We shall not discuss these further in this paper.

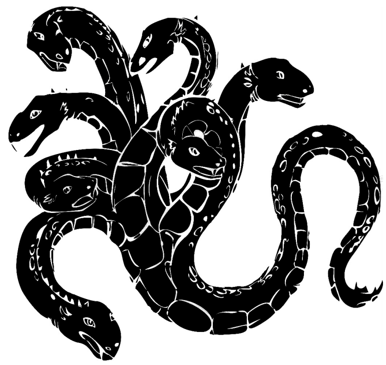
2.2 An Equivalent Construction (Hydra Game)

In 1982, Kirby and Paris (1982) presented *Hydra Game*, which is observed as an equivalent construction to Goodstein Sequences, with an accompanying theorem, equivalent to Goodstein's Theorem but in the context of Hydra Game.

Definition 2.2. A *Hydra* is a finite tree, composed of a finite number of straight edges, each joining two vertices, such that every vertex is connected by a unique path to a "root" node at the bottom of the tree.



(a) An example of a Hydra, as defined by Kirby and Paris (1982).



(b) An illustration of the mythical creature *Hydra*. Source: Deposit Photos.

Figure 1: Graphical representations of Hydras.

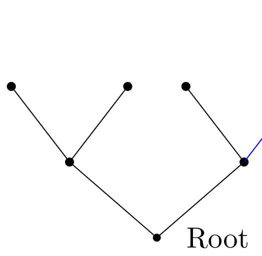
We see in Figure 1 that mathematical tree concept of a Hydra bears resemblance to the Hydra from Greek mythology – hence its name. In fact, Kirby and Paris (1982) presents the Hydra fully analogically to Greek myth of Hercules slaying the Hydra.

Kirby and Paris (1982) defines the head of the Hydra to be a *top node* together the single edge joined to it (analogous to the head and neck of the mythical Hydra), and all other intermediate edges and vertices are called "segments" and "nodes" respectively.

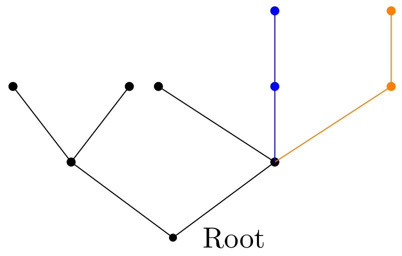
At stage $i \in \mathbb{N}$ in a battle between Hercules and the Hydra, Hercules cuts off one head from the Hydra, and the Hydra grows i new heads according to rules given by Kirby and Paris (1982):

> "*From the node that used to be attached to the head which was just chopped off, traverse one segment towards the root until the next node is reached. From this node sprout n replicas of that part of the hydra (after decapitation) which is 'above' the segment just traversed, i.e., those nodes and segments from which, in order to reach the root, this segment would have to be traversed. If the head just chopped off had the root as one of its nodes, no new head is grown.*"

Example 2.3. If we begin with the Hydra from Figure 1a, and cut the segment (neck) marked below in red, then the rule quoted above from Kirby and Paris (1982) gives the new Hydra to the right as a result:

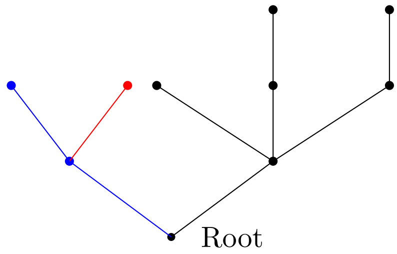


A starting Hydra, with the head we will be cutting off at stage 1 marked in red.

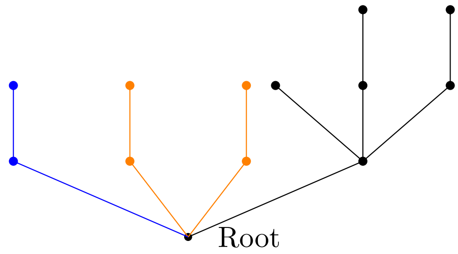


The same Hydra, but after after the head marked in red has been cut off.

We can see that the *sub-Hydra*[2], coloured blue, from the *parent* node of the node from which a head has been severed, is duplicated once, stemming from the same node (the duplication is marked in orange). Now, at stage 2, we shall cut off another head – again marked in red below.



The Hydra after stage 1, with the head we will chop off at stage 2 marked in red.



The same Hydra, but after stage 2 – where the head marked in red has been cut off.

After the second decapitation (stage 2), we see that a similar duplication to above occurs, except we have duplicated the *sub-Hydra* marked in blue two times, instead of once – to reflect this being stage two of the battle.

At any arbitrary stage i, the process is exactly the same: we decapitate one head, and then duplicate the *sub-Hydra* stemming from the *parent* node of the node from which the head has been severed i times.

It is easy to see from this example that the number of heads on the Hydra has potential to grow very quickly at each stage, and thus one may recognise that this seems very similar to a Goodstein Sequence in that, at each stage, the sequence grows by an amount determined by the term number $i \in \mathbb{N}$, and we subtract one.

[2]We shall define a *sub-Hydra* as a section of a Hydra which forms a smaller Hydra in its own right.

A result follows, which says that Hercules can win the battle after a finite number of decapitations – meaning that despite the number of heads on the Hydra increasing at a seemingly colossal rate, eventually – after some finite number of steps – the number of heads will reduce to zero and the Hydra will die (analogous to the Goodstein Sequence terminating). In fact, what is more is that Hercules will *always* win the battle, regardless of the strategy he adopts in choosing heads to chop off. This is precisely the theorem given by Kirby and Paris (1982), which can be recognised as analogous to Goodstein's Theorem:

Theorem 2.4. Every strategy is a winning strategy.

With it being analogous to Goodstein's Theorem, it also possesses the same characteristics as Goodstein's Theorem. That is, it is proven by the same method (as that given in Section 4), and – more significantly – it is also unprovable in Peano Arithmetic. Again, this can be proven in the same way by which we shall show that Goodstein's Theorem is unprovable by Peano's axioms of arithmetic, in Section 6.

Part II

A Proof of Goodstein's Theorem

"*A set is a Many that allows itself to be thought of as One.*"

- Georg Cantor, as quoted in *Platonism and Forms of Intelligence.*[3]

Whilst the setup for Goodstein Sequences and Goodstein's Theorem is fairly simple, the proof is much more complex and relies on several concepts from Set Theory, such as ordinal arithmetic and transfinite induction. We shall thus see an introduction to these concepts, which will lead to a proof of Goodstein's Theorem in Section 4.

3 An Introduction to Ordinal Arithmetic

In order to construct a proof of Goodstein's Theorem, we must first develop the idea of transfinite ordinals such to construct a parallel sequence to a given Goodstein Sequence – from which we can deduce a proof of Goodstein's Theorem. We begin by considering the axioms of Set Theory, as given in the early twentieth century by German mathematicians Ernst Zermelo and Abraham Fraenkel, which will allow us to define ordinal numbers.

3.1 The Zermelo-Fraenkel Axioms for Set Theory

As noted by O'Connor and Robertson (2014), Ernst Zermelo gave the first axiomatisation of Set Theory in 1908. However, in 1921, Abraham Fraenkel noted that for an infinite set Z_0, the existence of the set $\{Z_0, \mathcal{P}(Z_0), \mathcal{P}(\mathcal{P}(Z_0)), \dots\}$ could not be proved using Zermelo's original axioms (Ebbinghaus and Peckhaus, 2015). As a result, there followed a proposal of an amended set of axioms which were published by Fraenkel in 1922 (Ebbinghaus and Peckhaus, 2015), and Fraenkel's amended set of axioms, the ZF (Zermelo-Fraenkel) axioms, became widely accepted within the mathematical community, and are still the most commonly used today (Roitman, 1990).

Definition 3.1 (The Axioms of ZF Set Theory, as stated by Jech, 2003)**.**

1. **Axiom of Extensionality**: If X and Y have the same elements, then $X = Y$.
2. **Axiom of Pairing**: For any a, b, there exists a set $\{a, b\}$ that contains exactly a and b.

[3] Dillon and Zovko (2012).

3. **Axiom Schema of Separation**: If P is a property with parameter p, then for any X and p, there exists a set $Y = \{u \in X : P(u,p)\}$ which contains those $u \in X$ which have property P.

4. **Axiom of Union**: For any X, there exists a set $Y = \bigcup X$, the union of all elements in X.

5. **Axiom of Power Set**: For any X, there exists a set $Y = \mathcal{P}(X)$, the set of all subsets of X.

6. **Axiom of Infinity**: There exists an infinite set.

7. **Axiom Schema of Replacement**: If a class F is a function, then for any X, there exists a set $Y = F(X) = \{F(x) : x \in X\}$.

8. **Axiom of Regularity**: Every non-empty set has a $\ni$-minimal element[4].

Commonly appended to the axioms of ZF is the axiom of choice:

9. **Axiom of Choice**: Every family of nonempty sets has a choice function.

The appending of the axiom of choice (AC for short) to the ZF axioms yields the axiomatic Set Theory ZFC.

Whilst we shall not discuss the axioms of ZF or ZFC in-depth, an understanding of them is important as our proof of Goodstein's Theorem using arithmetic of ordinals is built upon the axioms of ZFC.

3.2 Ordinals

We shall now see an introduction to ordinal numbers[5], whose definition and arithmetic are largely owed to the work of Georg Cantor: a German mathematician, widely regarded as the founding-father of Set Theory (Levy, 1979). We begin by defining a *linear order* on a set S.

Definition 3.2. A binary relation R on a set S is a *linear ordering* of S if:

- $\neg(xRx)$ for all $x \in S$ (x is not related to itself by R);
- If xRy and yRz, then xRz, for any $x, y, z \in S$ (The relation R is transitive);
- Exactly one of the following holds for every $x, y \in S$:

  1. xRy; 2. yRx, or; 3. $x = y$.

[4] An element $x \in X$ is $\ni$-*minimal* if and only if there is no $y \in X$ such that $y \in x$.

[5] Largely based on chapters 2 and 4 of Levy (1979), and chapter 2 of Jech (2003).

Example 3.3. An example of a linear ordering is the binary relation $<$ on the set $\mathbb{R}$, as given any three elements $x, y, z \in \mathbb{R}$, we have $x \nless x$ as $x = x$, if $x < y$ and $y < z$ it follows that $x < z$, and also, for $x, y \in \mathbb{R}$, either $x < y$, $y < x$, or $x = y$.

We shall also define the notions or *well-ordering* and *transitivity* in order to define an ordinal.

Definition 3.4. A linear ordering R on a set S is a *well-ordering* if in every non-empty subset $X \subseteq S$, there is an R-minimal element $x \in X$. That is, an element $x \in X$ such that there is no other element $y \in X$ with yRx.

Definition 3.5. A set S is *transitive* if and only if $X \subseteq S$ for every $X \in S$. That is,

$$S \text{ is transitive} \iff (Y \in X, X \in S \rightarrow Y \in S).$$

Example 3.6. If we consider the set $S = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}$, we have the elements $\emptyset$, $\{\emptyset\}$, and $\{\emptyset, \{\emptyset\}\}$. Let us label these elements as such:

- $\emptyset = 0$;
- $\{\emptyset\} = 1$;
- $\{\emptyset, \{\emptyset\}\} = 2$.

Then we can see that $0 \in S$ is a subset of S trivially; $1 \in S$ is a subset of S, by taking $1 = \{0\} \subseteq S$; and $2 \in S$ is a subset of S by taking $2 = \{0, 1\} \subseteq S$. Hence, we have that S is a transitive set.

The idea of defining *ordinal numbers* is to develop a way of representing elements of the linearly-ordered set $\mathbb{N}$ of natural numbers as sets, such that any two elements α, β of $\mathbb{N}$ satisfy the linear-order $\alpha < \beta$ if and only if $\alpha \in \beta$ as ordinals.

Definition 3.7. A set is an *ordinal* (or *ordinal number*) if it is well-ordered by $\in$, and it is transitive.

We shall next define a successor function for ordinal numbers, which will allow us to obtain ordinals recursively from other ordinals. Thus, given one ordinal, we may define countably infinitely many more, by repeatedly taking the successor function. With this, we can begin to build a definition for each natural number using ordinals, and subsequently we shall later see that we can derive an ordinal which represents the entire set of natural numbers.

Definition 3.8. If α is an ordinal, then the *successor* ordinal $\alpha + 1$ is defined by the *successor function* $S(\alpha) = \alpha \cup \{\alpha\}$.

With this, we can begin to build a set of ordinals for the natural numbers. By Definition 3.7, it is immediate that $\emptyset$ is an ordinal. As $\emptyset$ has no elements, it can be viewed as $\in$-minimal, and thus similar in characteristic to $0 \in \mathbb{N}$ – which has no elements of $\mathbb{N}$ less than it, so is $<$-minimal in $\mathbb{N}$.

Definition 3.9. We can then begin to build on this using the successor function (Definition 3.8), as such:

$$\begin{aligned}
&0 = \emptyset, \\
&1 = S(\emptyset) = \emptyset \cup \{\emptyset\} = \{\emptyset\}, \\
&2 = S(\{\emptyset\}) = \{\emptyset\} \cup \{\{\emptyset\}\} = \{\emptyset, \{\emptyset\}\}, \\
&3 = S(\{\emptyset, \{\emptyset\}\}) = \{\emptyset, \{\emptyset\}\} \cup \{\{\emptyset, \{\emptyset\}\}\} = \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}, \\
&\quad \vdots
\end{aligned}$$

This definition of the natural numbers as ordinals is owed to Hungarian-American mathematician John von Neumann, as documented in his 1923 publication *On the introduction of transfinite numbers* (van Heijenoort, 1967, pp. 346–354). Using this, we can develop an idea of an ordinal-based notion of representation of the set of natural numbers, $\mathbb{N}$. However, as $\mathbb{N}$ is infinite, things do complicate. We shall thus introduce the notion of a limit ordinal.

Definition 3.10. A *limit ordinal* is an ordinal α such that $\alpha \neq \emptyset$, and there does not exist an ordinal β such that $\alpha = S(\beta)$.

We cannot take the existence of a limit ordinal as fact though, as we cannot simply reach a limit ordinal by recursive application of the successor function to any finite ordinal – by definition. Thus, a limit ordinal representation for $\mathbb{N}$ must be proven.

Proposition 3.11. The class of all finite ordinals (i.e. the class of natural numbers as ordinals) is a set, which is the *least infinite ordinal*.

Proof. Let S be an infinite set, whose existence is specified by the axiom of infinity (Axiom 6 in Definition 3.1). We have that $\emptyset$ is a member of every set, so deduce that $\emptyset = 0 \in S$. By our successor function (Definition 3.8), we have that for every $\alpha \in S$, $\alpha + 1 \in S$ – so every finite ordinal is in S.

If we have the class ω of all finite ordinals (natural numbers as ordinals), it follows that ω is a subclass of S. But by the axiom schema of separation (Axiom 3 in Definition 3.1), we have that any subclass of a subset is a set. Moreover, it is easily observed that every member of ω is an ordinal, making ω both transitive and well-ordered by $\in$, and thus an ordinal itself by Definition 3.7.

As every finite ordinal is a member of ω, it follows by definition of well-ordering that ω is greater than every finite ordinal, and there are no other infinite ordinals in ω. Hence, it follows that ω is the *least infinite ordinal.* $\square$

Lemma 3.12. The set ω – the least infinite ordinal – which contains all finite ordinals is isomorphic to $\mathbb{N}$, the set of natural numbers, as an ordinal.

Proof. By John von Neumann's definition of the natural numbers as ordinals (on page 16), each natural number can be represented by a unique ordinal and thus there is an isomorphism between the set of natural numbers $\mathbb{N}$ and the set of finite ordinals ω. $\square$

Corollary 3.13. ω can be considered as the set $\mathbb{N}$ of natural numbers as an ordinal.

ω is a *transfinite number*, meaning that it is larger than finite.

3.3 Ordinal Arithmetic

We shall now define the operations of addition, multiplication, and exponentiation of ordinals, which – as mentioned in subsection 3.2 – were given by Georg Cantor. This shall lead us to some crucial results from which we shall prove Goodstein's Theorem.

Definition 3.14. Addition of ordinals is defined as such, for all ordinals α, β:

- $\alpha + 0 = \alpha$,
- $\alpha + \gamma = \cup\{\alpha + \beta : \beta < \gamma\}$ if γ is a limit ordinal,
- $\alpha + (\beta + 1) = (\alpha + \beta) + 1$ for all ordinals β.

Definition 3.15. Multiplication of ordinals is defined as such, for all ordinals α, β:

- $\alpha \cdot 0 = 0$,
- $\alpha \cdot \gamma = \cup\{\alpha \cdot \beta : \beta < \gamma\}$ if γ is a limit ordinal,
- $\alpha \cdot (\beta + 1) = \alpha \cdot \beta + \alpha$ for all ordinals β.

Definition 3.16. Exponentiation of ordinals is defined as such, for all ordinals α, β:

- $\alpha^0 = 1$,
- $\alpha^\gamma = \cup\{\alpha^\beta : \beta < \gamma\}$ if γ is a limit ordinal,
- $\alpha^{\beta+1} = \alpha^\beta + \alpha$ for all ordinals β.

Ordinal addition and multiplication are associative and distributive, and exponentiation behaves by the same rules as integer exponentiation. It is important to note however that addition and multiplication of ordinals are not commutative (Jech, 2003). This can be shown by the above specified rules for $\alpha + \omega$ and $\alpha \cdot \omega$, where ω is the least infinite ordinal:

$$\begin{aligned} 1 + \omega &= \omega \\ &\neq \omega + 1 \end{aligned} \qquad \text{and} \qquad \begin{aligned} 2 \cdot \omega &= \omega \\ &\neq \omega \cdot 2 = \omega + \omega. \end{aligned}$$

This leads us to *epsilon numbers*, which play a part in the ordinal proof of Goodstein's Theorem.

Definition 3.17. An *epsilon number* is a transfinite ordinal number ε such that $\omega^{\varepsilon} = \varepsilon$.

The smallest epsilon number is $\varepsilon_0 = \omega^{\omega^{\omega^{\cdot^{\cdot^{\cdot}}}}} = \sup\{0, \omega^0 = 1, \omega^1, \omega^{\omega}, \omega^{\omega^{\omega}}, \dots\}$.

A crucial result from ordinal arithmetic on which our proof of Goodstein's Theorem relies involves the *polynomial representation of ordinals.*

Definition 3.18. Let α be an ordinal number, $n \in \omega$, and let $\epsilon_0, \dots, \epsilon_n$ and $\delta_0, \dots, \delta_n$ be ordinal numbers such that $\epsilon_0 > \epsilon_1 > \cdots > \epsilon_{n-1}$ and $\delta_0, \dots, \delta_{n-1} < \omega$. Then the expression

$$\alpha = \sum_{i=0}^{n-1} \omega^{\epsilon_i} \cdot \delta_i$$

is the *ω-polynomial representation* of α, or the *Cantor Normal Form* of α.

This leads us to our main result from ordinal arithmetic, a theorem of Georg Cantor (as stated by Potter, 2004), which we shall apply in order to develop an ordinal arithmetic proof for Goodstein's Theorem.

Theorem 3.19 (Cantor's Normal Form Theorem)**.** If α is any ordinal, then there exist unique finite sequences $(\delta_i)_{i<n}$ and $(\epsilon_i)_{i<n}$ of ordinals with $\epsilon_0 > \epsilon_1 > \cdots > \epsilon_{n-1}$, such that

$$\alpha = \omega^{\epsilon_0}\delta_0 + \omega^{\epsilon_1}\delta_1 + \cdots + \omega^{\epsilon_{n-1}}\delta_{n-1}.$$

That is, for every ordinal number α, there exists a unique *Cantor Normal Form* for α.

Proof (Based on the proof given by Rubin, 2012). This proof is split into two parts: *existence* and *uniqueness.*

(Existence): For any finite ordinal $\alpha \in \omega$ (i.e. any natural number as an ordinal), it is trivial that there exists a Cantor Normal Form for α, which is given by

$$\alpha = \omega^{\epsilon_0}\delta_0,$$

where $\epsilon_0 = 0$, and $\delta_0 = \alpha$. Thus, we shall consider an ordinal α, such that $\omega < \alpha$, and proceed by induction on α.

We begin with the supposition that every $\beta < \alpha$ has a Cantor Normal Form, and let

$$A = \{\omega^{\epsilon_i} \cdot \delta_i : \omega^{\epsilon_i} \cdot \delta_i \text{ is a } \omega\text{-monomial, and } \omega^{\epsilon_i} \cdot \delta_i \leq \alpha\}.$$

Let $\sup(A) = \omega^{\epsilon} \cdot \delta$ be the maximum monomial[6] in A. If $\alpha = \omega^{\epsilon} \cdot \delta$, then we are done. So suppose $\omega^{\epsilon} \cdot \delta < \alpha$, and let γ be an ordinal number such that

$$\omega^{\epsilon} \cdot \delta + \gamma = \alpha. \tag{3.1}$$

By construction, we have $\omega^{\epsilon} \cdot \delta + \omega^{\epsilon} > \alpha$, and by Definition 3.15, we have

$$\omega^{\epsilon} \cdot \delta + \omega^{\epsilon} = \omega^{\epsilon} \cdot (\delta + 1) > \alpha. \tag{3.2}$$

From equations 3.1 and 3.2, it follows that $\omega^{\epsilon} > \gamma$. Hence, $\gamma < \omega^{\epsilon} < \omega^{\epsilon} \cdot \delta < \beta$, and – by the inductive hypothesis – γ has a Cantor Normal Form

$$\gamma = \sum_{i=0}^{n-1} \omega^{\epsilon_i} \cdot \delta_i, \tag{3.3}$$

where $\epsilon_{n-1} < \epsilon$, as $\gamma < \omega^{\epsilon}$. So we may substitute the Cantor Normal Form for γ (equation 3.3) into equation 3.1, to derive a Cantor Normal Form for α:

$$\alpha = \omega^{\epsilon} \cdot \delta + \sum_{i=0}^{n-1} \omega^{\epsilon_i} \cdot \delta_i.$$

Hence, we have proved the existence of a Cantor Normal Form for every ordinal number.

(Uniqueness): Let $p = \sum_{i=0}^{n-1} \omega^{\epsilon_i} \cdot \delta_i$ and $q = \sum_{i=0}^{m-1} \omega^{\sigma_i} \cdot \rho_i$ be ω-polynomials. Suppose that either $m \neq n$ or $m = n$, and for at least one $i < m, n$, we have $\omega^{\epsilon_i} \cdot \delta_i \neq \omega^{\epsilon_i} \cdot \rho_i$. We have that, without loss of generality, $m \leq n$. Then we consider two cases:

1. $m < n$, and for every $i \in \{1, 2, \ldots, m-1\}$, we have:

$$\sigma_i = \epsilon_{i+(n-m)} \qquad \text{and} \qquad \rho_i = \delta_{i+(n-m)}.$$

2. There is some $0 \leq j \leq m-1$ such that for every $j < i \leq m-1$,

$$\sigma_i = \epsilon_{i+(n-m)} \qquad \text{and} \qquad \rho_i = \delta_{i+(n-m)},$$

and $(\omega^{\sigma_i} \cdot \rho_i) \neq (\omega^{\epsilon_{i+(n-m)}} \cdot \delta_{i+(n-m)})$.

[6] A monomial is a polynomial with only one term.

In Case 1,

$$p \geq \sum_{i=0}^{m-1} \omega^{\sigma_i} \cdot \rho_i + \omega^{\epsilon_{n-m-1}} \cdot \delta_{n-m-1} = q + \omega^{\epsilon_{n-m-1}} \cdot \delta_{n-m-1} > q.$$

In Case 2, we have that as $(\omega^{\sigma_i} \cdot \rho_i) \neq (\omega^{\epsilon_{i+(n-m)}} \cdot \delta_{i+(n-m)})$, either $q < p$, or $p < q$. It follows that two different Cantor Normal Forms cannot be equal, and thus Cantor Normal Forms are unique. $\square$

4 Proof of Goodstein's Theorem using Ordinal Arithmetic

We shall begin the proof of Goodstein's Theorem (Theorem 2.1) by defining a new sequence $(\gamma_i(a))_{i\in\mathbb{N}}$, based on Goodstein Sequences, but with a twist which introduces transfinite ordinals. We shall refer to this as the *Gamma Sequence*.

Definition 4.1. The i^{th} term of the *Gamma Sequence* for $a \in \mathbb{N}$ is obtained by writing the i^{th} term of the Goodstein Sequence for a in hereditary base-$(i+1)$ notation, and performing a shift of base whereby each occurrence of $(i+1)$ is replaced by ω.

This shift of base happens in an identical fashion to the shift of base in Goodstein Sequences, where we replace all occurrences of i with $i+1$, and when we perform such shift, we arrive at an equation in Cantor Normal Form – which we previously saw generates a unique ordinal output.

Example 4.2. We have from Example 1.15 that the first 5 terms of the Goodstein Sequence for 5 are as follows:

$$\begin{aligned}
G_1(5) &= 5 = 2^2 + 1,\\
G_2(5) &= 27 = 3^3,\\
G_3(5) &= 255 = 4^4 - 1,\\
G_4(5) &= 467 = 3\cdot 5^3 + 3\cdot 5^2 + 3\cdot 5 + 2,\\
G_5(5) &= 775 = 3\cdot 6^3 + 3\cdot 6^2 + 3\cdot 6 + 1.
\end{aligned}$$

Using this, we may obtain the first 5 terms of the Gamma Sequence $(\gamma_i(5))_{i\in\mathbb{N}}$, as follows:

$$\begin{aligned}
\gamma_1(5) &= (2^2 + 1 \xrightarrow{2 \mapsto \omega}) \ \omega^\omega + 1,\\
\gamma_2(5) &= (3^3 \xrightarrow{3 \mapsto \omega}) \ \omega^\omega,\\
\gamma_3(5) &= (4^4 - 1 \xrightarrow{4 \mapsto \omega})\omega^\omega - 1,\\
\gamma_4(5) &= (3\cdot 5^3 + 3\cdot 5^2 + 3\cdot 5 + 2 \xrightarrow{5 \mapsto \omega}) \ 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega + 2,\\
\gamma_5(5) &= (3\cdot 6^3 + 3\cdot 6^2 + 3\cdot 6 + 1 \xrightarrow{6 \mapsto \omega}) \ 3\cdot\omega^3 + 3\cdot\omega^2 + 3\cdot\omega + 1.
\end{aligned}$$

By construction, the Gamma Sequence terminates at the same stage that the Goodstein Sequence terminates, but also – by nature of transfinite ordinals being larger than every finite ordinal (i.e. every natural number) – we can also observe the following:

Lemma 4.3. For every $i \in \mathbb{N}$, and for every $a \in \mathbb{N}$, the following inequality holds:

$$G_i(a) \leq \gamma_i(a).$$

Proof. If $G_i(a) \geq i+1$, then writing $G_i(a)$ in hereditary base-$(i+1)$ notation includes at least one term which contains $i+1$. Hence, $\gamma_i(a)$ has at least one term containing ω by construction – which makes $\gamma_i(a)$ transfinite. For every i, $G_i(a) \in \mathbb{N}$, and thus – as an ordinal – $G_i(a) \in \omega$. By definition of ordinal numbers, it follows that $G_i(a) < \omega$, so $G_i(a)$ is finite. It follows now that, in this case, $G_i(a) < \gamma_i(a)$.

If however $G_i(a) < i+1$, then writing $G_i(a)$ in hereditary base-$(i+1)$ notation is the same as writing $G_i(a)$ as an integer. Thus, $\gamma_i(a)$ contains no occurrences of ω and $\gamma_i(a) = G_i(a)$.

Hence, in all cases, we have $G_i(a) \leq \gamma_i(a)$. □

From this, it follows that the Gamma Sequence $(\gamma_i(a))_{i\in\mathbb{N}}$ of a *dominates* the Goodstein Sequence $(G_i(a))_{i\in\mathbb{N}}$ of a, for all $a \in \mathbb{N}$. Thus, we have the following corollary of Lemma 4.3.

Corollary 4.4. $G_i(a)$ exists if and only if $\gamma_i(a)$ exists.

Proof. This follows from the definition of Goodstein Sequences and Gamma Sequences (Definitions 1.8 and 4.1 respectively), and Lemma 4.3. □

This result is significant, as it now suffices to show that the Gamma Sequence $(\gamma_i(a))_{i\in\mathbb{N}}$ converges to 0 for every a in order to prove Goodstein's Theorem.

Lemma 4.5. For every $a \in \mathbb{N}$, and for every $i \in \mathbb{N}$ for which $\gamma_i(a)$ exists, we have

$$\gamma_{i+1}(a) < \gamma_i(a).$$

That is, the Gamma Sequence is strictly decreasing.

Proof. To begin, notice that the following definitions for $\gamma_i(a)$ are equivalent, where $G_i(a)$ is the i^{th} term in the Goodstein Sequence for $a \in \mathbb{N}$, written in hereditary base-$(i+1)$ notation:

$$G_i(a) \xrightarrow{i+1 \;\mapsto\; \omega} = \gamma_i(a),$$
$$G_i(a) \xrightarrow{i+1 \;\mapsto\; i+2} \xrightarrow{i+2 \;\mapsto\; \omega} = \gamma_i(a), \tag{4.1}$$

where "$G_i(a) \xrightarrow{i+1 \;\mapsto\; b}$" denotes changing all occurrences of $i+1$ in $G_i(a)$ to b. So it does not matter what hereditary base we are shifting from when we shift to hereditary base-ω notation. Thus, we can define $\gamma_{i+1}(a)$ as:

$$G_i(a) \xrightarrow{i+1 \;\mapsto\; i+2} \xrightarrow{\textbf{cut}} \xrightarrow{i+2 \;\mapsto\; \omega} = \gamma_{i+1}(a), \tag{4.2}$$

where "$\xrightarrow{\textbf{cut}}$" denotes subtracting 1 from the result to its left. So

$$G_i(a) \xrightarrow{i+1 \mapsto i+2} \xrightarrow{\textbf{cut}} \xrightarrow{i+2 \mapsto \omega} = G_{i+1}(a) \xrightarrow{i+1 \mapsto i+2} \xrightarrow{i+2 \mapsto \omega} = \gamma_{i+1}(a).$$

If we denote the transformation $G_i(a) \xrightarrow{i+1 \mapsto i+2} = c$, then we may simplify equations 4.1 and 4.2 to $c \xrightarrow{i+2 \mapsto \omega} = \gamma_i(a)$ and $c \xrightarrow{\textbf{cut}} \xrightarrow{i+2 \mapsto \omega} = c - 1 \xrightarrow{i+2 \mapsto \omega} = \gamma_{i+1}(a)$ respectively.

In order to complete the proof, we now need to show that for any x, and any b we have $(x \xrightarrow{b \mapsto \omega}) < (x + 1 \xrightarrow{b \mapsto \omega})$. We can do this by induction on y, to show that for every $z < y$, we have $(z \xrightarrow{b \mapsto \omega}) < (y \xrightarrow{b \mapsto \omega})$.

Suppose that for all $y < x + 1$ and $z < y$, the inequality $(z \xrightarrow{b \mapsto \omega}) < (y \xrightarrow{b \mapsto \omega})$ holds. We want to show that $(x \xrightarrow{b \mapsto \omega}) < (x + 1 \xrightarrow{b \mapsto \omega})$. To see this, we shall write $x + 1$ in hereditary base-b notation. That is,

$$x + 1 \xrightarrow{\textbf{h base-}b} = b^{k_1} + b^{k_2} + \cdots + b^{k_{s-1}} + b^{k_s},$$

where $k_i \leq k_{i+1}$, and instead of writing db^k if we have d occurrences of b^k for some k, we instead write $b^{k_i} + b^{k_{i+1}} + \cdots + b^{k_{i+d}}$, where $k_i = k_{i+1} = \cdots = k_{i+d} = k$, to denote d copies of b^k.

We let $p = b^{k_1} + b^{k_2} + \cdots + b^{k_{s-1}}$ and $q = k_s$ (written in hereditary base-b), such that $x + 1 = p + b^q$. With this, we observe that $b^q \leq x + 1$, so $q < x + 1$. Now, we can write

$$(x + 1 \xrightarrow{b \mapsto \omega}) = (p + b^q \xrightarrow{b \mapsto \omega}) = \rho + \omega^\sigma, \tag{4.3}$$

where ρ denotes $(p \xrightarrow{b \mapsto \omega})$, and σ denotes $(d \xrightarrow{b \mapsto \omega})$.

If $q = 0$, then $x + 1 = p + 1$, and $x = p$, so $(x \xrightarrow{b \mapsto \omega}) = \rho < \rho + 1 = (x + 1 \xrightarrow{b \mapsto \omega})$.

If $q > 0$, we can write $x = p + b^q - 1$, and expand this to be

$$x = p + b^{q-1}(b - 1) + b^{q-2}(b - 1) + \cdots + b(b - 1) + (b - 1).$$

So, we have

$$(x \xrightarrow{b \mapsto \omega}) = \rho + \underline{\omega^{(q-1 \xrightarrow{b \mapsto \omega})}(b - 1) + \omega^{(q-2 \xrightarrow{b \mapsto \omega})}(b - 1) + \cdots + \omega(b - 1) + (b - 1)}. \tag{4.4}$$

By the inductive hypothesis, we have that each of the underlined terms in Equation 4.4 is less than ω^σ. So the sum of all of the underlined terms $(\omega^{(q-1 \xrightarrow{b \mapsto \omega})}(b - 1) + \cdots + \omega(b - 1) + (b - 1))$ must also be less than ω^σ.

In particular, we have that $(x \xrightarrow{b \mapsto \omega}) < \rho + \omega^\sigma$, and so it follows from Equation 4.3 that $(x \xrightarrow{b \mapsto \omega}) < (x + 1 \xrightarrow{b \mapsto \omega})$.

Therefore, for every $a \in \mathbb{N}$, and for every $i \in \mathbb{N}$ for which $\gamma_i(a)$ exists, we have

$$\gamma_i(a) > \gamma_{i+1}(a).$$

$\square$

Now, the final building block to the proof of Goodstein's Theorem is the following lemma:

Lemma 4.6. There is no infinite descending sequence of ordinals

$$\varepsilon_0 > \alpha_0 > \alpha_1 > \cdots$$

Proof. By definition, ordinals are well-ordered by $\in$, and so for any ordinals α_i, α_j, we have $\alpha_i < \alpha_j$ if and only if $\alpha_i \in \alpha_j$. If an infinite descending sequence or ordinals existed, then it would follow that there is no $\in$-minimal ordinal – which is absurd, as it gives rise to a contradiction against ε_0 being an ordinal. $\square$

We have now seen that $(\gamma_i(a))_{i\in\mathbb{N}}$ is a decreasing sequence of ordinals, and that there does not exist an infinite decreasing sequence of ordinals – so such a decreasing sequence of ordinals must converge to the ordinal $\emptyset$ (or 0 by Definition 3.9). Hence, it follows that there must exist some $n \in \mathbb{N}$ such that $\gamma_n(a) = 0$ for all $a \in \mathbb{N}$. Combining knowledge of this consequence of Lemma 4.5 with Corollary 4.4, we see that every Goodstein Sequence must terminate after a finite number of steps. Thus, we have proven Goodstein's Theorem (Theorem 2.1).

Part III

Unprovability in Peano Arithmetic

"*For nothing worthy proving can be proven, nor yet disproven.*"

- Alfred Tennyson, as quoted in *An Outline of Set Theory.*[7]

The axiomatisation of areas of mathematics has been of significant importance to mathematicians for thousands of years – with mathematicians as early as Euclid of Alexandria seeking to axiomatise elements of mathematics in Ancient Egyptian times (O'Connor and Robertson, 1999). In the mid-to-late nineteenth century, axiomatisation of arithmetic developed into a prominent research area in the mathematical community, which is owed to the the work of German mathematician Hermann Graßmann. Graßmann proved that many properties of arithmetic could be derived from fundamental facts about the successor operation and induction in his book *Lehrbuch der Arithmetik* (Grassmann, 1861, cited by Wikipedia Contributors, 2022).

In 1889, Italian mathematician Giuseppe Peano published his now famous axioms for arithmetic of the natural numbers, which are still widely regarded as the definitive axioms of arithmetic today. However, as will be discussed in section 7, there exist true statements in mathematics which remain unprovable within certain axiomatic systems, and Goodstein's Theorem is precisely this to Peano Arithmetic.

To allow us to show the unprovability of Goodstein's Theorem in Peano Arithmetic, we shall first see an introduction to symbolic logic. This will provide a foundation from which to understand Peano's axioms for arithmetic, and to be able to prove the inability of such axioms to the unprove of Goodstein's Theorem (Theorem 2.1).

[7] Henle (1986).

5 An Introduction to Symbolic Logic and Model Theory

Thus far, we have seen examples of logical statements and axioms, but we have not yet seen a formal definition of axiomatisation, or an introduction to what axioms are and what it means for a theory to be axiomatisable. In this section, we shall develop a core understanding some relevant concepts in and results of *Mathematical (symbolic) Logic* and *Model Theory*, based on the works of Kirby (2019), Smullyan (1968), and van Dalen (2013), as a foundation to demonstrating the unprovability of Goodstein's Theorem in Peano Arithmetic.

5.1 Languages and Structures

In symbolic logic, we consider a *language* $\mathcal{L}$ on which we base everything we do. In essence, a language in a logical sense is alike to a language in the natural sense of how we communicate with one another. In natural language, we have letters from which we build words, and we construct sentences from such words which we can interpret based on context, and we derive meaning from such sentences. We see now that a language in symbolic logic is very similar to this.

Definition 5.1. A language $\mathcal{L}$ consists of:

- A set of relation symbols (e.g. $<$).
- A set of function symbols (e.g. $+, \cdot$).
- A set of constant symbols (e.g. $0, 1$).
- For each relation and function symbol, an arity.

The *arity* of a relation or function symbol is the number of arguments it takes input from. For example, a binary function symbol such as $+$ takes two arguments, so has arity 2. We could also define a function $f : x \mapsto x + 1$, which has arity 1, as it only takes one argument as input (the value for x). We call this a *unary* function. Similarly, for relation symbols, we can have $<(x, y) = x < y$, a binary relation symbol. Also, for some constant symbol c, we may define the relation symbol $<_c(x) = x < c$ which takes only one argument as input, and so is unary.

A language by itself does not have much meaning, as it does not specify a set (or domain) on which it acts, and thus the symbols within a language do not have any interpretation. We must thus also introduce *structures*. These are essentially a language paired with a set, which gives meaning to the language via an interpretation.

Definition 5.2. An $\mathcal{L}$-structure $\mathcal{S}$ consists of a set S, the domain of the structure, together with interpretations of the symbols in $\mathcal{L}$, as such:

- Each relation symbol R, of arity n, in $\mathcal{L}$, is interpreted as a subset $R^{\mathcal{S}}$ of S^n, where each $r \in R^{\mathcal{S}} \subseteq S^n$ is an n-tuple $(r_1, r_2, \ldots, r_n)$ satisfying the relation R in $\mathcal{S}$.
- Each function symbol f, of arity n, in $\mathcal{L}$, is interpreted as a function $f^{\mathcal{S}} : S^n \to S$.
- Each constant symbol c_i in $\mathcal{L}$ is interpreted as an element $c_i^{\mathcal{S}} \in S$.

For sake of understanding, we may think of an $\mathcal{L}$-structure to a logical language $\mathcal{L}$ as we do a dictionary is to a natural language – it provides a definition for what the elements of the language actually mean, and how they should be interpreted in a given context.

Example 5.3. The language $\mathcal{L}_{\text{s-ring}}$ of semirings is defined as $\langle +, \cdot, 0, 1\rangle$, where $+$ and $\cdot$ are binary function symbols, and 0 and 1 are constant symbols.

Remark. It is important to realise that in the above example (5.3), the symbols 0 and 1 are indeed symbols and are not necessarily equal to the natural numbers 0 and 1 respectively. Usually, the symbol 0 is used to represent the additive identity, and the symbol 1 is used to represent the multiplicative identity element, which do often happen to correspond to the natural numbers 0 and 1, but this is not necessarily implied and does depend on the structure through which we interpret the symbols.

Example 5.4. If we consider the $\mathcal{L}_{\text{s-ring}}$-structure

$$\mathbb{N}_{\text{s-ring}} = \left\langle \mathbb{N}; +^{\mathbb{N}_{\text{s-ring}}}, \cdot^{\mathbb{N}_{\text{s-ring}}}, 0^{\mathbb{N}_{\text{s-ring}}}, 1^{\mathbb{N}_{\text{s-ring}}} \right\rangle,$$

we have interpreted the symbols of the language $\mathcal{L}_{\text{s-ring}}$ by their usual interpretations in $\mathbb{N}$, where $+^{\mathbb{N}_{\text{s-ring}}}$ and $\cdot^{\mathbb{N}_{\text{s-ring}}}$ are the usual addition and multiplication over $\mathbb{N}$, and $0^{\mathbb{N}_{\text{s-ring}}} = 0 \in \mathbb{N}$ and $1^{\mathbb{N}_{\text{s-ring}}} = 1 \in \mathbb{N}$ are the additive and multiplicative identity elements in $\mathbb{N}$ respectively.

Notation. As we will primarily be considering $\mathbb{N}_{\text{s-ring}}$ throughout this document, we shall adopt a minor abuse of notation and simply write $\mathbb{N}_{\text{s-ring}} = \langle \mathbb{N}; +, \cdot, 0, 1\rangle$, omitting the superscript "$\mathbb{N}_{\text{s-ring}}$" on the function and constant symbols in the structure and instead assuming $+, \cdot, 0, 1$ to be their interpretations in $\mathbb{N}_{\text{s-ring}}$.

5.2 Formulas and Sentences

In symbolic logic and model theory, we are concerned with proving whether statements are true or false in certain structures. In order to do this, we must have a way of expressing statements in a way which can be understood by symbolic logic, and we do this with *formulas* in a language $\mathcal{L}$ (called $\mathcal{L}$-formulas), constructed of $\mathcal{L}$-*terms*.

Definition 5.5. *$\mathcal{L}$-terms* are strings of symbols from the language $\mathcal{L}$, defined recursively as:

- Every variable is a term.
- Every constant symbol is a term.
- If f is a function symbol of arity k, and $t_1, \ldots, t_k$ are terms, then $f(t_1, \ldots, t_k)$ is a term.

Only something built of finitely many repetitions of the above three steps in any order is an $\mathcal{L}$-term.

Definition 5.6. An $\mathcal{L}$-formula is defined recursively, as such:

- If t_i, t_j are terms, then $(t_i = t_j)$ is a formula.
- If R is an k-ary (arity k) relation symbol, and $t_1, \ldots, t_k$ are terms, then $R(t_1, \ldots, t_k)$ is a formula.
- If φ, θ are formulas, then $\neg\varphi$ (the negation of φ), $(\varphi \to \theta)$ (φ implies θ), $(\varphi \wedge \theta)$ (φ and θ), and $(\varphi \vee \theta)$ (φ or θ) are formulas.
- If φ is a formula and x is a variable, then $\exists x[\varphi]$ and $\forall x[\varphi]$ (there exists an x such that φ is true, and for all x, φ is true, respectively) are formulas.

Only something built of finitely many repetitions of the above three steps in any order is an $\mathcal{L}$-formula.

When considering axioms and the statement of Goodstein's Theorem, we are interested in *$\mathcal{L}$-sentences*, which are $\mathcal{L}$-formulas with no *free* variables, where a *free* variable is one **not** bound by a quantifier (i.e. $\forall$ or $\exists$).

Example 5.7. The following are examples of formulas and sentences.

1. $(x < 1)$ is a formula, and x is a *free* variable in such as it is not bound within the scope of a quantifier.
2. $\forall x[(x = 0) \vee (0 < x)]$ is a sentence, as the variable x is *bound* by the universal quantifier $\forall$.
3. $\exists x[(x < y) \wedge (0 < x)]$ is a formula, as the variable y is *free* due to it not being quantified (i.e. the instance of y in this formula is not within the scope of $\forall y$ or $\exists y$). The variable x is *bound* though, by the existential quantifier $\exists$.

We shall now introduce some notation to describe the validity of an $\mathcal{L}$-formula (or $\mathcal{L}$-sentence) in a given $\mathcal{L}$-structure.

Definition 5.8. If ψ is a formula with k free variables, and $\overline{s} = (s_1, \ldots, s_k)$ is a k-tuple of elements in the domain S of an $\mathcal{L}$-structure $\mathcal{S}$, then we have $\mathcal{S} \models \psi(\overline{s})$, read "$\mathcal{S}$ *models* $\psi(\overline{s})$", to mean that the formula $\psi(\overline{a})$ is true in the structure $\mathcal{S}$.

If we let the $\mathcal{L}$-sentence from Example 5.7.2 be ψ, we have – as shown above – $\mathbb{N}_{\text{s-ring}} \models \psi$, and $\mathbb{Z}_{\text{s-ring}} \not\models \psi$. That is, $\mathbb{N}_{\text{s-ring}}$ models ψ, whilst $\mathbb{Z}_{\text{s-ring}}$ does not model ψ. As ψ is an $\mathcal{L}$-sentence, it has no free variables – so we do not need to define a tuple of variables from $\mathbb{N}$ or $\mathbb{Z}$, as in Definition 5.8.

As well as being able to say that an $\mathcal{L}$-structure $\mathcal{S}$ models an individual $\mathcal{L}$-sentence, we may also say that it models a collective set of $\mathcal{L}$-sentences. For example, if Γ is a set of $\mathcal{L}$-sentences, then we may write $\mathcal{S} \models \Gamma$ to mean that every sentence in Γ is true in $\mathcal{S}$.

The notion described by Definition 5.8 does not however appeal to provability. For this, we introduce the symbol $\vdash$, as follows.

Definition 5.9. For a set Γ of $\mathcal{L}$-formulas, and some formula φ, we have $\Gamma \vdash \varphi$ (Γ *entails* φ) if φ can be deduced from formulas in Γ.

Now, we see the concepts of consistency and completeness of $\mathcal{L}$-sentences:

Definition 5.10. A set Γ of $\mathcal{L}$-sentences is *consistent* if for every $\mathcal{L}$-sentence $\psi \in \Gamma$, we have $\neg\psi \notin \Gamma$. That is, there are no contradictory $\mathcal{L}$-sentences in Γ.

Definition 5.11. A set Γ of $\mathcal{L}$-sentences is *complete* if for every $\mathcal{L}$-sentence φ, we have either $\Gamma \vdash \varphi$, or $\Gamma \vdash \neg\varphi$. That is, if a set Γ of $\mathcal{L}$-sentences is complete, then any $\mathcal{L}$-sentence is logically equivalent to some $\mathcal{L}$-sentence in Γ.

5.3 Peano's Axioms of Arithmetic

In mathematics, we may consider the theory of certain classes of structures; for example, the theory of rings, or the theory of groups. *Theory* refers to the *deductively closed* [8] set of all $\mathcal{L}$-sentences which are true for rings or groups respectively. Of course, it would be counter-intuitive, never-mind impossible, to list all $\mathcal{L}$-sentences true in these classes of structures when introducing them. Thus, axiomatisation is useful here.

A set of axioms is a finite, countable set of $\mathcal{L}$-sentences which characterises the *theory* T of a class of structures $\mathcal{C}$, and which essentially aims to form a basis from which any statement ϕ which is true in T can be derived. That is, if ϕ can be deduced from the axioms for the theory T of $\mathcal{C}$, then $T \vdash \phi$. If T does in fact accurately portray the

[8] A set Γ of $\mathcal{L}$-sentences is *deductively closed* if for any $\mathcal{L}$-sentence ψ, if $\Gamma \vdash \psi$, then $\psi \in \Gamma$.

characteristics of $\mathcal{C}$, and provides the means to proving facts about the behaviour of $\mathcal{C}$, then we have $\mathcal{C} \models T$.

In 1889, Italian mathematician Giuseppe Peano published *Arithmetices principia nova methodo exposita* – translating from Latin to mean *The principles of arithmetic presented by a new method*. Within such, Peano stated nine axioms for $\mathbb{N}_{\text{s-ring}}$. Today, we only consider a subset of Peano's axioms, as it is noted by van Heijenoort (1967) that some of the original axioms are contained in the underlying logic.

Definition 5.12. [Axioms of Peano Arithmetic] As stated by Kirby (2019), a modernised interpretation of the axioms of Peano Arithmetic are as follows.

1. $\forall x[x + 1 \neq 0]$,
   which says that there exists no natural number whose successor is 0.
2. $\forall x[x \neq 0 \to \exists y[x = y + 1]]$,
   which says that each non-zero natural number is the successor to some other natural number.
3. $\forall xy[x + 1 = y + 1 \to x = y]$,
   which says that if the successor of two natural numbers is equal, then those two natural numbers are equal.
4. $\forall x[x + 0 = x]$,
   which says that 0 is the additive identity element.
5. $\forall xy[x + (y + 1) = (x + y) + 1]$,
   which says that the sum of a natural number and the successor of another natural number is equal to the successor of the sum of the two natural numbers.
6. $\forall x[x \cdot 0 = 0]$,
   which says that multiplying anything by 0 is equal to 0.
7. $\forall[x \cdot (y + 1) = (x \cdot y) + x]$,
   which says that multiplication is distributive.

Peano Arithmetic also includes an *induction schema*, making the complete theory of Peano Arithmetic the closure of logical formulas obtained from the above axioms combined with the following:

Induction Schema: $(\phi(0) \wedge \forall x[\phi(x) \to \phi(x + 1)]) \to \forall x[\phi(x)]$.

The descriptors of each of the axioms stated in Definition 5.12 are given in the context of the natural numbers $\mathbb{N}$, but in truth, there do exist other models of Peano Arithmetic which are not isomorphic to $\mathbb{N}$. These are referred to as *non-standard* models of Peano Arithmetic (Kaye, 1991), whose existence is proven by the Löwenheim-Skolem Theorem – but this transcends relevance to the discussion of this report. Thus, we are not interested in non-standard models in the context of demonstrating the unprovability of Goodstein's Theorem, so we shall just be considering Peano's axioms in the context of the natural numbers (i.e. as interpreted in the structure $\mathbb{N}_{\text{s-ring}}$).

6 Unprovability of Goodstein's Theorem

In proving the unprovability of Goodstein's Theorem (Theorem 2.1) in Peano Arithmetic, we shall consider a more formal expression of the theorem, in the language of symbolic logic. Goodstein's Theorem states that for all $a \in \mathbb{N}$, there is some $i \in \mathbb{N}$ such that $G_i(a) = 0$. To simplify notation, we shall consider the *associated function* $G : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ defined by $g(i, a) = G_i(a)$. Thus, we have the following symbolic *sentence* which is logically equivalent to – and thus characterises – Goodstein's Theorem:

Theorem 6.1 (A symbolic restatement of Theorem 2.1)**.**

$$\forall a \exists i [g(i, a) = 0],$$

where $g(i, a) = G_i(a)$ – the i^{th} term in the Goodstein Sequence for $a \in \mathbb{N}$.

We have seen that Goodstein's Theorem is a true statement about the natural numbers, which we were able to prove by ordinal arithmetic. As such, we may deduce that the negation of Goodstein's Theorem is false, and cannot be proven. Therefore, by showing that Goodstein's Theorem is unprovable, we can actually extend our statement to a stronger one, as stated by Smith (2013):

Theorem 6.2 (Kirby and Paris, 1982)**.** Goodstein's Theorem is undecidable in Peano Arithmetic (if Peano Arithmetic is consistent).

In this section, we shall discuss the key ideas involved in proving Theorem 6.2, beginning with an account of the main result of Kirby and Paris (1982) – which proves that the notion of transfinite induction of ordinals up to ε_0 is necessary in formulating a proof of Goodstein's Theorem. We next explore Gentzen's consistency proof for Peano Arithmetic, which – in conjunction with Gödel's Second Incompleteness Theorem – exhibits Peano Arithmetic's inability to handle transfinite induction up to ε_0 as a corollary (Smith, 2013); thus deducing the consequence that Goodstein's Theorem is undecidable in Peano Arithmetic.

6.1 The Kirby-Paris Theorem

Whilst Theorem 6.2 is the final result deduced from the findings presented by Kirby and Paris (1982), the main result which gives way to this is as follows.

Theorem 6.3 (The Kirby-Paris Theorem; Kirby and Paris, 1982)**.** Induction up to ε_0 is equivalent to Goodstein's Theorem.

Kirby and Paris present a proof of this result which utilises rapidly-growing functions derived from combinatorial statements introduced by Ketonen and Solovay (1981), in order to recognise *indicators*[9] in non-standard models of Peano Arithmetic. The Kirby-Paris Theorem presents the consequence that the unprovability of Goodstein's Theorem in Peano Arithmetic can be derived by a proof that Peano Arithmetic cannot handle induction up to ε_0, and this is precisely what we shall see in the next subsection – as an implication of Gentzen's consistency proof for arithmetic.

6.2 Gentzen's Consistency Proof

As noted by Rathjen (2015) and as we may deduce from the proof we gave of Goodstein's Theorem in Section 4, the proof of Goodstein's Theorem is a consequence of there being no infinitely descending primitive recursive sequences of ordinals, and Theorem 6.3 informs that induction up to ε_0 is required to prove this fact. This subsection considers a proof of the consistency of Peano Arithmetic, which was famously presented by Gentzen (1936), by proof of the arithmetical statement Con(PA) which implies the consistency of Peano Arithmetic, using ε_0-induction.

Theorem 6.4 (Gentzen's Consistency Theorem)**.** Peano Arithmetic is Consistent.

Gentzen's original proof of Theorem 6.4 is difficult and highly technical. As such, instead of giving a formal proof of his consistency theorem, we shall simply outline the key ideas of the proof which lead us to the relevant results for proving the undecidability of Goodstein's Theorem.

A sketch proof of Theorem 6.4. Gentzen's proof begins by noting that the lack of contradiction within proofs derived in Peano Arithmetic relies on the lack of contradiction within certain simpler proofs derived in Peano Arithmetic, which make up the constituent parts of the larger proof (Smith, 2013). He recognises that this fact gives way for a linear ordering of proofs by way of assignment of transfinite ordinal numbers to proofs, correlating to the nature of their dependence on other proofs.

The necessity for the linear ordering of proofs to be transfinite is derived by the simple observation that some proofs depend on an infinite number of smaller proofs. For example, Goodstein's Theorem (Theorem 6.1) is a universal statement (i.e. it is a statement about *all* natural numbers), and as such would be the culmination of an infinite number

[9]Let M be a non-standard model of Peano Arithmetic, with P a property of a subset $\{x \in M : x < n\}$ of M for some $n \in M$. An *indicator* for P in M is a function $F : M^2 \to M$ which satisfies

$$F(a,b) > \mathbb{N} \iff \text{there exists } \{x \in M : x < n\} \subseteq M \text{ with } a \in \{x \in M : x < n\} < b$$
$$\text{and } \{x \in M : x < n\} \text{ has property} P \text{ for all } a,b \in M.$$

of proofs – one for each natural number – that the Goodstein Sequence for each natural number terminates. A finite ordinal could not capture the dependence of the proof of Goodstein's Theorem on infinitely many smaller proofs, and so transfinite ordinal numbers are thus necessary to represent the ordering of proofs according to their complexity with regards to the smaller proofs contained within. The ordinals required to prove the consistency of Peano Arithmetic are thus sums of powers of ω (i.e. Cantor Normal Forms) – so Gentzen's proof relies on transfinite induction up to ε_0.

As detailed by Smith (2013), listing the simpler proofs contained within more complex proofs can be understood as a *reduction* task dealing with proofs encoded by Gödel numbers[10], handled by primitive recursive functions. Peano Arithmetic can deal with both primitive recursive functions and codings of proofs, and so its only short-falling is in its inability to handle transfinite induction up to ε_0. As such, we may appeal to Peano Arithmetic with induction up to ε_0 (PA+I), which replaces Peano's *Induction Schema* with *the rule of quantifier-free induction up to* ε_0 (Simpson, 2009):

> **The rule of quantifier-free induction up to ε_0:**
> From $\phi(0)$ and $\phi(x) \to \phi(x+1)$, deduce $\phi(y)$ for any formula ϕ and any $y < \varepsilon_0$. Additionally, if $y < \varepsilon_0$ is a limit ordinal, and $\varphi(x)$ holds for all $x < y$, then we deduce $\varphi(y)$.

Gentzen finally alludes to our familiar concept of the well-foundedness of ordinal numbers in addressing the derivation of an absurdity (acording to the following lemma) from the aforementioned reduction task to complex proofs.

Lemma 6.5. A theory T is consistent if and only if the empty sequent[11] is not derivable from T.

Assuming for contradiction that PA+I contains proofs P of the empty sequent, and letting α_i be the ordinal representation of the reduction task applied recursively i times to proofs P of the empty sequent, Gentzen derives a sequence of ordinals

$$\alpha_0 > \alpha_1 > \alpha_2 > \cdots > \alpha_n$$

for all n (Rathjen and Sieg, 2020). This says precisely that if PA+I contains proofs of the empty sequent, there exists an infinite descending sequence of ordinal numbers, but this contradicts Goodstein's Theorem, which Kirby and Paris (1982) notes is equivalent to the existence of no such sequence. Thus, PA+I does not derive the empty sequent and so is consistent by Lemma 6.5 – which proves Gentzen's Consistency Theorem. □

[10] See Section 15.1 of Smith (2013) for a comprehensive introduction to Gödel numbering.

[11] The empty sequent is the logical formula ($\to$) – i.e. *nothing* implies *nothing* (Gratzl, 2010).

6.3 Gödel's Second Incompleteness Theorem

As a result of Gentzen's consistency proof, we see that the consistency of Peano Arithmetic is proven in the presence of induction up to ε_0, which Theorem 6.3 informs is necessary to prove Goodstein's Theorem. Therefore, we have that Goodstein's Theorem implies Con(PA) – a formula which expresses the consistency of Peano Arithmetic; so if Peano Arithmetic proves Goodstein's Theorem, then it also proves Con(PA) (thus proving its own consistency).

The final building block to our proof of Theorem 6.2 is owed to the following significant theorem of Kurt Gödel.

Theorem 6.6 (Gödel's Second Incompleteness Theorem[12])**.** For any consistent theory T within which a certain amount of elementary arithmetic can be carried out, the consistency of T cannot be proved in T itself. That is: T cannot prove Con(T).

As a result of Gödel's Second Incompleteness Theorem, it follows immediately that Peano Arithmetic must not prove its own consistency, which we have seen to follow from Goodstein's Theorem by Theorem 6.3 and Gentzen's consistency proof, outlined in subsection 6.2. Thus, bringing this all together, we have proven that if Peano Arithmetic is consistent, then Goodstein's Theorem cannot be proved – making it undecidable in Peano Arithmetic. This concludes our proof of Theorem 6.2.

[12] As stated by Raatikainen (2022).

7 Consequences of Goodstein's Theorem and its Unprovability

To quote Henle (1986), the implications of Goodstein's Theorem which have been explored throughout this report make the theorem "remarkable in many ways". Aside from being a surprising statement in its own right, Goodstein's Theorem's unprovability in Peano Arithmetic makes it a purely arithmetical statement about finite integers which requires a notion of infinite ordinals in order to be proven – making Goodstein's Theorem a purely number theoretic exhibition of the findings of Gödel and Gentzen. As such, there are many implications and further discussions to be had surrounding the consequences of the unprovability (undecidability) of Goodstein's Theorem in Peano Arithmetic.

7.1 The Incompleteness of Peano Arithmetic

Arguably some of the most remarkable results which define our understanding of symbolic logic were given by Kurt Gödel, to whom Theorem 6.6 is attributed. Published along with the aforementioned *Second Incompleteness Theorem* was another incompleteness theorem (Gödel, 1931):

Theorem 7.1 (Gödel's First Incompleteness Theorem[13])**.** *If a theory T is axiomatised and arithmetically sound*[14]*, then there is some L-sentence ϕ such that $T \nvdash \phi$ and $T \nvdash \neg\phi$.*

Barwise (1977) claims that since the publication of Gödel's Incompleteness Theorems, mathematicians were immersed in discovering a strictly arithmetical example of incompleteness in Peano Arithmetic, and it is clear to see that Goodstein's Theorem is precisely this – as first proven by Kirby and Paris (1982). Goodstein's Sequence thus bears huge significance in existing as an example of Gödel's First Incompleteness Theorem. Furthermore, with the reliance of the proof of its unprovability on Gödel's Second Incompleteness Theorem, Goodstein's Theorem truly acts as a testament to the results given by Gödel (1931).

As a result of Goodstein's Theorem as a number theoretic example of the incompleteness of Peano Arithmetic (and subsequently, Gödel's Theorems), questions may be posed around the definition of truth in arithmetic; namely, the nature of the grey area surrounding how we determine the truth of a given statement, and in what language or structure we are able to do so. Prior to knowledge of Goodstein's Theorem, or any other

[13] As stated by Smith (2013).

[14] A theory is *sound* if everything which can be deduced/proven is true.

results independent of Peano Arithmetic, one may suppose that truth follows only from proof – but as we have seen, the truth of Goodstein's Theorem is not supported by a proof in Peano Arithmetic, due to incompleteness.

The notion of truth has been given significant attention over the past century within the study of logic, with Tarski (1936) giving arguably the most influential account and exploration of the concept of truth – stating that there is no first-order, arithmetical $\mathcal{L}$-formula which can express truth in arithmetic, and that we must transcend the expressive power of $\mathcal{L}$, with a metalanguage[15]. However, whilst Tarski's take on truth is interesting, there are more relevant topics for discussion, motivated by our account of Goodstein's Theorem.

Goodstein's Theorem's unprovability and thus the subsequent incompleteness of Peano Arithmetic illustrates that not all *true* arithmetical statements are provable in a consistent theory of arithmetic, and thus the definition of truth in arithmetic becomes subjective. We see this portrayed by the necessity of appealing to another theory in our proof of the unprovability of Goodstein's Theorem in Peano Arithmetic and in the proof of Peano Arithmetic's consistency.

Considerations of how we define *truth* add significant substance to the implications of the unprovability of Goodstein's Theorem in Peano Arithmetic. To both the uninitiated and mathematical researchers alike, the lack of equivalence of provability and truth poses questions of how we should in fact define a *true* theory of arithmetic. Gödel's Incompleteness Theorems and examples such as Goodstein's Theorem show us that no theory is complete, and so there is no "perfect" theory of arithmetic which models arithmetic consistently.

Whilst the decidability of Goodstein's Theorem relies on a foundation of the axioms of ZFC, it is also true that ZFC is capable of proving a lot more than is necessary within the structure of arithmetic. This motivates the question of how much set theory we are really willing to take in order to decide every possible statement of arithmetic. Alas, further questions of consistency and incompleteness follow from taking such a stronger theory for arithmetic – such as the decidability of the consistency of that stronger theory – for example, ZFC, whose absolute consistency is undecidable[16] by Gödel's Second Incompleteness Theorem (Jech, 2003) – as shall be discussed in the next subsection.

[15] A *metalanguage* is a language which is used to describe another language.

[16] By *absolute consistency*, we mean the ability to state with 100% certainty that the theory is consistent – with no reliance on any other undecided consistencies.

7.2 The Consistency of Peano Arithmetic

An inconsistent theory allows provability of un-sound statements, with any derivable contradiction giving way to the provability of yet more absurd statements. For example, if Peano Arithmetic contained an inconsistency, then it may even be possible to prove the negation of Goodstein's Theorem – which would be absurd following the proof given in Section 4, which tells us that Goodstein's Theorem is true.

The equivalence of Goodstein's Theorem to a statement of the consistency of Peano Arithmetic told us that Goodstein's Theorem is unprovable if and only if Peano Arithmetic is consistent, and we assumed the consistency of such throughout in order to derive the unprovability of Goodstein's Theorem. Various proofs of the consistency of Peano Arithmetic have been given (Chow, 2019) – including that of Gentzen (1936) – however there still exists reasonable doubt, and the consistency of Peano Arithmetic is considered an open problem by some, as a result of Gödel's Second Incompleteness Theorem (Theorem 6.6).

Gödel (1931) states that the consistency of a theory – Peano Arithmetic, for example – cannot be proven within the theory itself; thus, one must appeal to a stronger theory to do so. This, of course, relies on the consistency of the chosen stronger theory, which again cannot be proven by itself, and must rely on yet another stronger theory. Chow (2019) remarks that generally, Mathematicians consider the theory of ZFC (see Definition 3.1) to be the foundation of truth in Mathematics, and thus it is typically considered that a mathematical statement holds only if it can be proven in ZFC. In this case, the consistency of Peano Arithmetic is accepted, and thus our assumption of its truth is valid in this sense, however the uncertainty of it due to Gödel's Second Incompleteness Theorem is equally valid, and should be considered in discussing the unprovability of Goodstein's Theorem in Peano Arithmetic.

7.3 Final Remarks

As remarked previously, Goodstein's Theorem is considered with many layers of fascinating consequences. Whilst its main impacts lie in the area of mathematical logic and our understanding of incompleteness, Goodstein's work has found applications in some other unexpected areas as well. For example, Paris and Tavakol (1993) unexpectedly consider the algorithm which generates a Goodstein Sequence as a dynamical system, which – although unrelated to any known naturally occurring dynamical system – exhibits very interesting characteristics, which could perhaps be related to the rate at which the universe has expanded since its inception (Miller, 2001).

Of course, in its more prominent environment though, many appreciate Goodstein's work and its subsequent developments (such as those made by Kirby and Paris, 1982) to be hugely influential and groundbreaking in the field of mathematical logic. As alluded to by Miller (2001), Goodstein's Theorem was the first number theoretic statement proved independent of Peano Arithmetic, so the proof given by Kirby and Paris (1982) cultivated much excitement and further research into the incompleteness of Peano Arithmetic and Goodstein's Theorem. The work of Goodstein has been pivotal in our understanding of results independent of Peano Arithmetic, and the progression of mathematical research in this area has been influenced greatly by subsequent research performed on the work presented by Goodstein (1944).

Rathjen (2015) remarks that although Goodstein made no mention of the implications of his theorem with regards to the incompleteness of Peano Arithmetic, it is clear to see that his intention was to present Goodstein's Theorem as an independence result. von Plato (2016) claims that Goodstein's 1944 paper originally held the title "A Note on Gentzen's Theorem", and allegedly made excessive references to Goodstein's Theorem as an independence result for Peano Arithmetic; but on review by Paul Bernays (Gentzen's doctoral supervisor), heavy criticism was made and Goodstein restructured the paper immensely – removing all reference to the unprovability of Goodstein's Theorem and revising the title to "*On the Restricted Ordinal Theorem*" (Bernays, 1942 cited by Rathjen, 2015). As a result, the remarkable implications of Goodstein's Theorem as an independence result for Peano Arithmetic were not uncovered until almost forty years later, by the work of Kirby and Paris (1982). Rathjen (2015) notes that if Goodstein had have persisted with his claims of the unprovability of Goodstein's Theorem in Peano Arithmetic, he would have been well on his way to proving an independence result for Peano Arithmetic, thus accelerating our understanding of this area of mathematics by what in reality was almost half-a-century.

Since the work of Kirby and Paris (1982) in proving the independence of Goodstein's Theorem from Peano Arithmetic, many subsequent developments have been made, in the form of further study of both Goodstein's Theorem and other independence results for Peano Arithmetic. Cichon (1983) gave an alternative proof to Goodstein's Theorem's unprovability a year later, much shorter than that given by Paris and Kirby, which involved constructing Goodstein Sequences in such a way to be related to the Hardy hierarchy (Hardy, 1904), invoking yet more interest in the area; and Kanamori and McAloon (1987) presented yet another independence result for Peano Arithmetic, relating to finite Ramsey Theory.

Goodstein's Theorem and its implications are fascinating in a range of areas of mathematics, and – as such – are discussed in a wide variety of contexts. For the interested reader, von Plato (2016) gives an interesting insight into the becoming of Goodstein's Theorem – starting with an account of the works of Gödel and Gentzen. For further reading into the implications of Goodstein's Theorem and the Incompleteness of Peano Arithmetic, Kaplan (2012) gives a good account of the classification of non-standard models of Peano Arithmetic using Goodstein's Theorem, and Smith (2013) explores incompleteness in great depth, making reference to Goodstein's Theorem in chapter 23.

Acknowledgements

I would like to thank my supervisor, Dr. David Asperó, for proposing and facilitating this MMath Dissertation, and for his guidance and direction during the course of the project. Moreover, I would like to extend my thanks to the various lecturers I have had during my time studying mathematics at UEA, without whom this project would not have been possible. My thanks go also to all those who gave time to proofread my work, with special thanks to Kioni Broomfield and Alice Lyon for their extensive feedback and suggestions, which went a long way in improving my work.

Bibliography

Barwise, J. (1977). *Handbook of Mathematical Logic*, volume 90 of *Studies in Logic and the Foundations of Mathematics*. North-Holland Publishing Co., Amsterdam. With the cooperation of H. J. Keisler, K. Kunen, Y. N. Moschovakis and A. S. Troelstra.

Bernays, P. (1942). Letter to Goodstein, dated September 1st, 1942. Bernays collection of the ETH Zürich.

Chow, T. Y. (2019). The Consistency of Arithmetic. *Math. Intelligencer*, 41(1):22–30.

Cichon, E. A. (1983). A short proof of two recently discovered independence results using recursion theoretic methods. *Proc. Amer. Math. Soc.*, 87(4):704–706.

Dillon, J. and Zovko, M. (2012). *Platonism and Forms of Intelligence*. De Gruyter.

Ebbinghaus, H. and Peckhaus, V. (2015). *Ernst Zermelo: An Approach to His Life and Work*. Springer Berlin Heidelberg.

Gentzen, G. (1936). Die Widerspruchsfreiheit der reinen Zahlentheorie. *Mathematische Annalen*, 112:493–565.

Gödel, K. (1931). Über formal unentscheidbare Sätze der Principia Mathematica und verwandter Systeme I. *Monatsh. Math. Phys.*, 38(1):173–198.

Goodstein, R. L. (1944). On the restricted ordinal theorem. *J. Symbolic Logic*, 9:33–41.

Grassmann, H. (1861). *Lehrbuch der Mathematik für höhere Lehranstalten*. Number v. 1 in Lehrbuch der Mathematik für höhere Lehranstalten. T.C.F. Enslin.

Gratzl, N. (2010). A Sequent Calculus for a Negative Free Logic. *Studia Logica: An International Journal for Symbolic Logic*, 96(3):331–348.

Hardy, G. H. (1904). A Theorem Concerning the Infinite Cardinal Numbers. *Quarterly journal of Mathematics*, 35:87–94.

Henle, J. M. (1986). *An Outline of Set Theory*. Problem Books in Mathematics. Springer-Verlag, New York.

Jech, T. (2003). *Set Theory*. Springer Monographs in Mathematics. Springer-Verlag, Berlin. The third millennium edition, revised and expanded.

Kanamori, A. and McAloon, K. (1987). On Gödel incompleteness and finite combinatorics. *Annals of Pure and Applied Logic*, 33:23–41.

Kaplan, D. (2012). *A Classification of Nonstandard Models of Peano Arithmetic by Goodstein's Theorem*. Franklin and Mashall College, Lancaster, Pennstlvania.

Kaye, R. (1991). *Models of Peano Arithmetic*, volume 15. Oxford: Clarendon Press.

Ketonen, J. and Solovay, R. (1981). Rapidly growing Ramsey functions. *Ann. of Math. (2)*, 113(2):267–314.

Kirby, J. (2019). *An Invitation to Model Theory*. Cambridge University Press, Cambridge.

Kirby, L. and Paris, J. (1982). Accessible Independence Results for Peano Arithmetic. *Bulletin of the London Mathematical Society*, 14(4):285–293.

Levy, A. (1979). *Basic Set Theory*. Perspectives in Mathematical Logic. Springer.

Miller, J. T. (2001). *On the Independence of Goodstein's Theorem*. University of Arizona.

O'Connor, J. J. and Robertson, E. F. (1999). Euclid of Alexandria — MacTutor History of Mathematics. [Online; accessed 1-February-2022].

O'Connor, J. J. and Robertson, E. F. (2014). Abraham Fraenkel — MacTutor History of Mathematics. https://mathshistory.st-andrews.ac.uk/Biographies/Fraenkel/. [Last accessed 7-February-2022].

Paris, J. and Tavakol, R. (1993). Goodstein algorithm as a super-transient dynamical system. *Physics Letters A*, 180(1):83–86.

Potter, M. (2004). *Set Theory and its Philosophy*. Oxford University Press, New York. A critical introduction.

Raatikainen, P. (2022). Gödel's Incompleteness Theorems. https://plato.stanford.edu/archives/spr2022/entries/goedel-incompleteness. [Last accessed 23-February-2022].

Rathjen, M. (2015). *Goodstein's Theorem Revisited*, pages 229–242. Springer International Publishing, Cham.

Rathjen, M. and Sieg, W. (2020). Proof Theory. https://plato.stanford.edu/archives/fall2020/entries/proof-theory/. [Last accessed 30-April-2022].

Roitman, J. (1990). *Introduction to Modern Set Theory*. Pure and Applied Mathematics (New York). John Wiley & Sons, Inc., New York. A Wiley-Interscience Publication.

Rubin, M. (2012). Ordinal arithmetic, Cantor normal form, Hessenberg sum, rank of $\langle \mathrm{On} \times \mathrm{On}, < \rangle$. https://www.math.bgu.ac.il/~matti/Axiomatic-ST-2012-06--Cantor-Normal-Form--Hessenberg-Sum--Rank-of-alpha-times-beta.pdf. [Last accessed 2-Mar-2022].

Simpson, S. G. (2009). *Subsystems of Second Order Arithmetic*. Perspectives in Logic.

Cambridge University Press, Cambridge; Association for Symbolic Logic, Poughkeepsie, NY, second edition.

Smith, P. (2013). *An Introduction to Gödel's Theorems*. Cambridge Introductions to Philosophy. Cambridge University Press, Cambridge, second edition.

Smullyan, R. M. (1968). *First-Order Logic*. Ergebnisse der Mathematik und ihrer Grenzgebiete, Band 43. Springer-Verlag New York, Inc., New York.

Tarski, A. (1936). The Concept of Truth in Formalized Languages. In Tarski, A., editor, *Logic, Semantics, Metamathematics*, pages 152–278. Oxford University Press.

van Dalen, D. (2013). *Logic and Structure*. Universitext. Springer, London, fifth edition.

van Heijenoort, J. (1967). *From Frege to Gödel. A source book in mathematical logic, 1879–1931*. Harvard University Press, Cambridge, Mass.

von Plato, J. (2016). *Gödel, Gentzen, Goodstein: The Magic Sound of a G-String*, pages 215–227. Princeton University Press.

Wikipedia Contributors (2022). Peano Axioms — Wikipedia, The Free Encyclopedia. https://en.wikipedia.org/w/index.php?title=Peano_axioms. [Last accessed 2-February-2022].